Citrix Secure Private Access

Machine translated content

Disclaimer

Contents

新增功能

June 19, 2024

2024 年 **6** 月 **11** 日

- 策略建模工具

  策略建模工具（访问策略 **>** 策略建模）可帮助管理员在管理员控制台内分析和解决配置问题。有关详细信息，请参阅策略建模工具。

- 支持诊断日志图表中的过滤器

  诊断日志图表中的筛选选项可帮助管理员根据应用程序类型、类别和描述等各种条件细化搜索，从而更轻松地进行日志分析和故障排除。有关详细信息，请参阅诊断日志。

2024 年 **3** 月 **13** 日

- 支持终止活动用户会话并将用户添加到禁用用户列表

  管理员现在可以立即终止所有活动的最终用户会话，并将用户添加到禁用用户列表中。将用户添加到此禁用用户列表将终止所有活跃的 Secure Private Access 应用程序会话并阻止将来的应用程序访问。有关详细信息，请参阅终止活动用户会话并将用户添加到禁用用户列表。

2024 年 **2** 月 **12** 日

- 浏览器和防病毒扫描的普遍可用性

  Device Posture 服务支持的浏览器和防病毒扫描现已正式推出。有关详细信息，请参阅 Device Posture 支持的扫描。

2024 年 **1** 月 **23** 日

- 使用 **Device Posture** 服务进行设备证书检查的正式可用性

  使用 Device Posture 服务进行设备证书检查现已正式推出。有关详细信息，请参阅使用 Device Posture 服务检查设备证书。

2023 年 **12** 月 **20** 日

- 本地 **Secure Private Access** 的正式上市

  本地版 Citrix Secure Private Access 现已正式上市。有关详细信息，请参阅新增功能。

2023 年 10 月 16 日

- **Secure Private Access** 本地解决方案预览功能

  Secure Private Access 本地解决方案现在提供以下内容：

  - 首次设置的管理员用户界面。
  - 用于配置应用程序和访问策略的管理用户界面。
  - 日志控制板。

  有关详细信息，请参阅本地 Secure Private Access。

- **Device Posture** 服务预览功能

  Device Posture 服务现在支持以下检查：

  - IGEL 平台现在支持 Device Posture 服务。
  - Device Posture 服务现在支持地理定位和网络位置检查。

  有关详细信息，请参阅 Device Posture。

2023 年 9 月 11 日

- **Device Posture** 与 **Microsoft Intune** 集成的正式发布版本

  Device Posture 与 Microsoft Intune 集成现已正式上市。有关详细信息，请参阅 Microsoft Intune 与 Device Posture 集成。

2023 年 8 月 30 日

- 管理 **Device Posture** 服务的 **Citrix Endpoint Analysis** 客户端

  EPA 客户端可以与 NetScaler 和 Device Posture 一起使用。与 NetScaler 和 Device Posture 一起使用时，需要进行一些配置更改才能管理 EPA 客户端。有关详细信息，请参阅管理 Device Posture 服务的 Citrix Endpoint Analysis 客户端。

2023 年 8 月 28 日

- **iOS** 平台上的 **Device Posture** 服务支持

  iOS 平台现在支持 Device Posture 服务。有关详细信息，请参阅 Device Posture。

  此功能在预览版中提供。

2023 年 8 月 22 日

- 使用 **Citrix Device Posture** 服务检查设备证书

  Citrix Device Posture 服务现在可以根据企业证书颁发机构检查终端设备的证书，以确定终端设备是否可信，从而启用对 Citrix DaaS 和 Secure Private Access 资源的情境访问 (Smart Access)。有关详细信息，请参阅使用 Device Posture 服务检查设备证书。

  此功能在预览版中提供。

2023 年 8 月 17 日

- **Citrix DaaS Monitor** 上的 **Device Posture** 事件

  现在可以在 DaaS Monitor 上搜索 Device Posture 服务事件和监视日志。有关详细信息，请参阅 Citrix DaaS Monitor 上的 Device Posture 事件。

2023 年 6 月 7 日

- 用于为本地配置 **Secure Private Access** 的工具

  现在，简化的用户界面可用于为本地解决方案配置 Secure Private Access。配置工具可以在 Citrix Virtual Apps and Desktops Delivery Controller 上运行，以快速创建 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 NetScaler Gateway 设置。有关详细信息，请参阅 /zh-cn/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html。

2023 年 5 月 29 日

- 创建具有多个规则的访问策略已正式上线

  您可以创建多个访问规则，并在单个策略中为不同的用户或用户组配置不同的访问条件。这些规则可以分别应用于 HTTP/HTTPS 和 TCP/UDP 应用程序，全部应用于单个策略。有关详细信息，请参阅 配置具有多个规则的访问策略。

  [SPA-746]

2023 年 4 月 10 日

- 应用程序发现

  应用程序发现功能可帮助管理员查看其组织中的内部私有应用程序，例如 Web 应用程序和客户端服务器应用程序（基于 TCP 和 UDP 的应用程序）以及访问这些应用程序的用户。管理员可以通过指定域（通配符域）或 IP 子网的范围来发现应用程序。有关详细信息，请参阅应用程序发现。

  [ACS-2325]

2023 年 3 月 29 日

- 适用于本地部署的 **Secure Private Access** 解决方案

  作为 Citrix StoreFront 和 NetScaler Gateway 客户，您现在可以使用用于本地部署的 Citrix Secure Private Access 解决方案无缝访问 Web 和 SaaS 应用程序以及 Citrix Virtual Apps 和 Virtual Desktops。有关详细信息，请参阅本地 Secure Private Access。

  [SPAOP-1]

2023 年 3 月 7 日

- 配置 **DNS** 后缀

  Citrix Secure Private Access 服务的 DNS 后缀功能可用于以下用例：

  - 通过为后端服务器添加 DNS 后缀域，使 Citrix Secure Access 客户端能够将非完全限定域名（主机名）解析为完全限定域名 (FQDN)。
  - 允许管理员使用 IP 地址（IP CIDR/IP 范围）配置应用程序，以便最终用户可以使用 DNS 后缀域下相应的 FQDN 访问应用程序。

  有关详细信息，请参阅将 FQDN 解析为 IP 地址的 DNS 后缀。

  [ACS-2490]

2023 年 1 月 23 日

- **Device Posture** 服务

  Citrix Device Posture 服务是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求才能获得 Citrix DaaS (Virtual Apps and Desktops) 或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）的访问权限。有关详细信息，请参阅 Device Posture。

  [AAUTH-90]

- **Microsoft Endpoint Manager** 与 **Device Posture** 集成

  除了 Device Posture 服务提供的本机扫描外，Device Posture 服务还可以与其他第三方解决方案集成。Device Posture 与 Windows 和 macOS 上的 Microsoft Endpoint Manager (MEM) 集成在一起。有关详细信息，请参阅 Microsoft Endpoint Manager 与 Device Posture 集成。

  [ACS-1399]

2022 年 12 月 22 日

- 通过 **Citrix Workspace** 应用程序登录的用户支持 **Workspace URL** 的单点登录

  当已经通过 Citrix Workspace 应用程序登录时，Citrix Secure Access 客户端现在支持 Workspace URL 的单点登录。此 SSO 功能通过避免多次身份验证来增强用户体验。有关详细信息，请参阅 Workspace URL 的单点登录支持。

  [ACS-1888]

- 使用访问策略启用对应用程序的访问权限

  要向用户授予对应用程序的访问权限，管理员现在需要创建具有匹配的用户订阅列表的访问策略，以使应用程序可供最终用户使用。以前，管理员必须将用户添加为订阅者才能启用访问权限。有关详细信息，请参阅创建访问策略。

  [ACS-3018]

2022 年 10 月 3 日

- 用于授予应用程序访问权限的访问策略

  应用程序订阅者配置选项已从配置向导的“应用程序”部分中删除。要向用户授予对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。

  [ACS-3018]

- 支持 **UDP** 应用程序

  Secure Private Access 服务现在支持访问 UDP 应用程序。有关详细信息，请参阅 预览功能。

  [ACS-1430]

2022 年 9 月 9 日

- 基于用户风险评分的自适应访问

  管理员现在可以使用 Citrix Analytics for Security (CAS) 提供的用户风险评分配置自适应访问策略。有关详细信息，请参阅 基于用户风险评分的自适应访问。

  [ACS-877]

- 基于用户网络位置的自适应接入

  管理员现在可以根据用户访问应用程序的位置配置自适应访问策略。位置可以是用户访问应用程序的国家或用户的网络位置。有关详细信息，请参阅 基于位置的自适应访问。

  [ACS-99]

- 增强型自适应访问策略生成器

  现在，只有在满足配置的条件后才能访问应用程序。仅订阅应用程序，客户无法访问应用程序。管理员必须添加访问策略，以便除应用程序订阅之外还提供对应用程序的访问权限。此外，用户或组是访问策略中的强制性条件，必须满足该条件才能访问应用程序。有关详细信息，请参阅创建访问策略。

  [ACS-1850]

- 限制将文件上载到 **SaaS/Web** 应用程序

  此功能允许客户管理员控制（允许或限制）谁可以将文件上载到他们的关键业务应用程序。这样，只有授权用户才能将文件上载到应用程序中。有关详细信息，请参阅创建访问策略。

  [ACS-655]

- 增强型控制板

  Secure Private Access 控制面板现在可以详细查看多个用户指标，例如应用程序使用情况、热门应用程序用户、访问次数最多的应用程序、诊断日志等。有关详细信息，请参阅 控制面板。

  [ACS-2480]

- 库弃用

  Secure Private Access 应用程序现在在 Citrix Cloud Library 中不可见。所有配置了 Secure Private Access 的应用程序都位于 Secure Private Access 服务磁贴中的应用程序部分内。这有助于管理员轻松浏览、编辑和配置应用程序。

  [ACS-1546]

- **Secure Private Access** 的审核日志

  Citrix Secure Private Access 服务相关的事件现已捕获在 **Citrix Cloud >** 系统日志中。有关详细信息，请参阅 审核日志。

  [ACS-876]

- 企业 **Web** 和 **SaaS** 应用程序访问的诊断日志

  Citrix Secure Private Access 事件现已与 Citrix Analytics 集成。Citrix Analytics 提供了一个公共终端节点，允许管理员访问和下载事件。这些事件可以通过 PowerShell 脚本进行访问。有关详细信息，请参阅 企业 Web 和 SaaS 应用程序访问的诊断日志。

  [ACS-805]

- 故障排除指南

  管理员可以使用故障排除指南来解决与配置相关的问题。有关详细信息，请参阅 解决应用程序相关问题。

  [ACS-2719]

2022 年 7 月 15 日

- 仅在配置了访问策略时才启用对应用程序的访问

  现在，只有在管理员添加应用程序订阅之外的访问策略后，才会启用对应用程序的访问权限。仅订阅应用程序无法访问应用程序。通过此更改，管理员可以根据用户、位置、设备、风险等上下文实施自适应安全性。管理员必须将现有的应用程序安全控制和访问策略迁移到新的访问策略框架中。有关详细信息，请参阅 迁移应用程序安全控制和访问策略。

  [ACS-1850]

2022 年 6 月 1 日

- 自适应身份验证服务

  自适应身份验证现已正式推出 (GA)。有关自适应身份验证的详细信息，请参阅 自适应身份验证服务。

  [CGS-6510]

2022 年 4 月 4 日

- 品牌重塑变更

  Citrix Secure Workspace Access 服务现已更名为 Citrix Secure Private Access 服务。

  [ACS-2322]

- 管理员指导的工作流程，轻松上手和设置

  Secure Private Access 现在具有全新的简化管理体验，可逐步配置 SaaS 应用程序、内部 Web 应用程序和 TCP 应用程序的零信任网络访问权限。它包括在单个管理控制台中配置自适应身份验证、包括用户订阅在内的应用程序、自适应访问策略和其他应用程序。有关详细信息，请参阅 管理员指导的工作流程，以便于入门和设置。

  此功能现已正式推出 (GA)。

  [ACS-1102]

- **Secure Private Access** 控制面板

  Secure Private Access 控制板可让管理员全面了解其热门应用、顶级用户、连接器运行状况、带宽使用情况，并在单个位置进行消费。这些数据是从 Citrix Analytics 获取的。有关详细信息，请参阅 Secure Private Access 控制面板。

  此功能现已正式推出 (GA)。

  [ACS-1169]

- 直接访问企业 **Web** 应用程序

  客户现在可以直接从 Chrome、Firefox、Safari 和 Microsoft Edge 等原生网络浏览器启用对内部网页应用程序的零信任网络访问 (ZTNA)。有关详细信息，请参阅 直接访问企业 Web 应用程序。

  此功能现已正式推出 (GA)。

- 基于 **ZTNA** 代理的访问 **TCP/HTTPS** 应用程序

  Citrix 客户现在可以对所有客户端-服务器应用程序和基于 IP/端口的资源以及内部 Web 应用程序启用零信任网络访问 (ZTNA)。有关详细信息，请参阅 对客户端-服务器应用程序的支持。

  此功能现已正式推出 (GA)。

  [ACS-970]

- 适用于企业 **Web**、**TCP** 和 **SaaS** 应用程序的自适应访问和安全控制

  Citrix Secure Private Access 服务自适应访问功能提供了全面的零信任网络访问 (ZTNA) 方法，可提供对应用程序的安全访问。自适应访问使管理员能够根据上下文提供用户可以访问的应用程序的精细级别访问权限。这里的“上下文”一词是指：

  - 用户和组（用户和用户组）
  - 设备（台式机或移动设备）
  - 位置（地理位置或网络位置）
  - Device Posture（Device Posture 检查）
  - 风险（用户风险评分）

  有关详细信息，请参阅 企业 Web、TCP 和 SaaS 应用程序的自适应访问和安全控制。

  此功能现已正式推出 (GA)。

  [ACS-878、ACS-879、ACS-882]

- **Secure Private Access** 的审核日志

  Citrix Secure Private Access 服务相关的事件现已捕获在 **Citrix Cloud >** 系统日志中。有关详细信息，请参阅 审核日志。

  此功能现已正式推出 (GA)。

  [ACS-876]

- 企业 **Web** 和 **SaaS** 应用程序访问的诊断日志

  Citrix Secure Private Access 事件现已与 Citrix Analytics 集成。Citrix Analytics 提供了一个公共终端节点，允许管理员访问和下载事件。这些事件可以通过 PowerShell 脚本进行访问。有关详细信息，请参阅 企业 Web 和 SaaS 应用程序访问的诊断日志。

  此功能现已正式推出 (GA)。

  [ACS-805]

- 自适应身份验证服务

  Citrix Cloud 客户现在可以使用 Citrix Workspace 为 Citrix Virtual Apps and Desktops 提供自适应身份验证。自适应身份验证是一项 Citrix Cloud 服务，可为登录 Citrix Workspace 的客户和用户启用高级身份验证。自适应身份验证服务是 Citrix 托管和 Citrix Cloud 托管的 ADC。有关详细信息，请参阅 自适应身份验证服务。

  此功能在预览版中提供。

  [CGS-6510]

2022 年 2 月 16 日

- 支持客户端-服务器应用程序 借助 Citrix Secure Private Access 中对客户端-服务器应用程序的支持，您现在可以消除对传统 VPN 解决方案的依赖，从而为远程用户提供对所有私有应用程序的访问权限。

  有关详细信息，请参阅 对客户端-服务器应用程序的支持-预览

  [ACS-870]

2021 年 10 月 11 日

- **Citrix Gateway** 服务磁贴合并到 **Citrix Cloud** 中的单个 **Secure Private Access** 中

  Citrix Gateway 服务磁贴现已合并到 Citrix Cloud 中的单个 Secure Private Access 中。

  - 所有 Secure Private Access 客户（包括 Citrix Workspace Essentials 和 Citrix Workspace Standard）现在都可以使用单个“Secure Private Access”磁贴来配置 SaaS 和企业 Web 应用程序、增强的安全控制、上下文策略以及 Web 筛选策略。
  - 所有 Citrix DaaS 客户仍然可以从“Workspace 配置”中将 Citrix Gateway 服务作为 HDX 代理启用。但是，从网关服务磁贴启用 Citrix Gateway 服务的快捷方式已被删除。您可以通过 **Workspace** 配置 **>** 访问 **>** 外部连接启用 Citrix Gateway 服务。有关详细信息，请参阅 外部连接。否则，功能没有变化。

  [NGSWS-16761]

2021 年 7 月 30 日

- 基于用户地理位置的企业 **Web** 和 **SaaS** 应用程序的上下文访问和安全控制

  Citrix Secure Private Access 服务现在支持基于用户的地理位置对企业 Web 和 SaaS 应用程序进行上下文访问。

  [ACS-833]

- 从 **Citrix Workspace** 门户中隐藏特定 **Web** 或 **SaaS** 应用程序的选项

  管理员现在可以从 Citrix Workspace 门户中隐藏特定的 Web 或 SaaS 应用程序。当应用程序从 Citrix Workspace 门户中隐藏时，Citrix Gateway 服务在枚举过程中不会返回此应用程序。但是，用户仍然可以访问隐藏的应用程序。

  [ACS-944]

2021 年 **6** 月 **9** 日

- 用于定义路由应用程序流量的规则的路由表

  管理员现在可以使用路由表定义规则，以将应用程序流量直接路由到 Internet 或通过 Citrix Gateway Connector 路由。管理员可以将应用程序的路由类型定义为“外部”、“内部”、“内部旁路代理”或“通过网关连接器的外部”，具体取决于他们想要定义流量的方式。

  [ACS-243]

2021 年 **5** 月 **22** 日

- 对企业 **Web** 和 **SaaS** 应用程序的上下文访问

  Citrix Secure Private Access 服务上下文访问功能提供了全面的零信任访问方法，可提供对应用程序的安全访问。上下文访问使管理员能够提供对用户可以根据上下文访问的应用程序的精细级别访问权限。此处的术语“上下文”是指用户、用户组和用户访问应用程序的平台（移动设备或台式计算机）。

  [ACS-222]

- **Citrix Gateway Connector** 用户界面的品牌重塑

  根据 Citrix 品牌推广准则，Citrix Cloud Gateway Connector 用户界面已重新命名。

  [NGSWS-17100]

2021 年 **5** 月 **1** 日

- 从 **Citrix Secure Private Access** 服务数据存储中删除客户数据

  客户数据（包括备份）将在服务权利到期 90 天后从 Citrix Secure Private Access 服务数据存储中删除。

  [ACS-388]

- 将域从 **Azure AD** 联合到 **Citrix Workspace** 的简化步骤

  现在简化了将域从 Azure AD 联合到 Citrix Workspace 应用程序的步骤，以便在 Citrix Workspace 中更快地加入。现在可以通过单点登录页面在 Citrix Gateway 服务用户界面中执行域联合。

  [ACS-351]

- 连接测试工具的增强功能

  Citrix Gateway Connector 中的连接测试工具得到了增强，可以处理超时错误并生成必要的日志。

  [NGSWS-17212]

2021 年 3 月 15 日

- 平台增强功能

  对平台进行了各种增强功能，以提高将客户的管理员配置传播到 Citrix Gateway Connector 的可靠性。

  [ACS-85]

- 提高了 **Web** 应用的性能

  使用无客户端 VPN 从系统浏览器访问 Web 应用程序时，Web 应用程序的性能已得到改进。

  [NGSWS-16469]

- 启用 **Citrix Gateway Connector** 使用 **TLS1.2 A** 级或以上的密码套件

  Citrix Gateway Connector 现在使用带 A 级或更高级别密码套件的 TLS1.2 来连接到 Citrix Cloud 服务和其他后端服务器。

  [NGSWS-16068]

2020 年 11 月 11 日

- 重命名 **Citrix** 访问控制服务

  访问控制服务现已重命名为 Secure Private Access。

  [NGSWS-14934]

2020 年 10 月 15 日

- 增强的安全选项，可在 **Remote Browser Isolation** 服务中启动 **SaaS** 和企业 **Web** 应用程序

  管理员现在可以使用增强安全选项，选择“始终在 **Citrix Remote Browser Isolation** 服务中启动应用程序”以始终在 Remote Browser Isolation 服务中启动应用程序，无论其他增强的安全设置如何。

  [ACS-123]

2020 年 10 月 8 日

- 为 **Citrix Secure Private Access** 浏览器扩展配置会话超时

  管理员现在可以为 Citrix Secure Private Access 浏览器扩展配置会话超时。管理员可以从 Citrix Gateway 服务用户界面的 管理 选项卡中配置此设置。

  [NGSWS-13754]

- **Citrix Secure Private Access** 浏览器扩展管理设置上的 **RBAC** 控制

  RBAC 控制现在在 Citrix Secure Private Access 浏览器扩展管理设置上强制执行。

  [NGSWS-14427]

2020 年 9 月 24 日

- 通过本地浏览器启用无 **VPN** 访问企业 **Web** 应用程序

  现在，您可以使用 **Citrix Secure Private Access** 浏览器扩展程序通过本地浏览器启用对企业 Web 应用程序的无 VPN 访问。Google Chrome 和 Microsoft Edge 浏览器都支持 **Citrix Secure Private Access** 浏览器扩展程序。

  [ACS-286]

2020 年 7 月 7 日

- 在 **Citrix Gateway Connector** 上验证 **Kerberos** 配置

  现在，您可以使用单点登录部分中的测试按钮来验证 Kerberos 配置。

  [NGSWS-8581]

2020 年 6 月 19 日

- **Citrix Gateway** 服务和 **Citrix Secure Private Access** 服务管理员的只读访问权限

  使用 Citrix Gateway 服务的安全管理员团队现在可以提供精细控制，例如对 Citrix Gateway 服务和 Citrix Secure Private Access 服务的管理员的只读访问权限。

  - 对 Citrix Gateway 服务具有只读访问权限的管理员只能查看应用程序详细信息。
  - 对 Citrix Secure Private Access 服务具有只读访问权限的管理员只能查看内容访问设置。

  [ACS-205]

2020 年 5 月 8 日

- **Citrix Gateway Connector 13.0** 中的新故障排除工具
  - 网络跟踪：您现在可以使用 跟踪 功能来解决 Citrix Gateway Connector 注册问题。您可以下载跟踪文件并与管理员共享以进行故障排除。有关详细信息，请参阅解决 Citrix Gateway Connector 注册问题。

    [NGSWS-10799]
  - 连接性测试：您现在可以使用 连接性测试 功能确认网关连接器配置中没有错误，并且网关连接器能够连接到 URL。有关详细信息，请参阅 登录并设置 Citrix Gateway Connector。

    [NGSWS-8580]

V2019.04.02

- **Citrix Gateway** 连接器到出站代理的 **Kerberos** 身份验证支持 [NGSWS-6410]

  现在，从 Citrix Gateway 连接器到出站代理的流量支持 Kerberos 身份验证。Gateway Connector 使用配置的代理凭据向出站代理进行身份验证。

V2019.04.01

- **Web/SaaS** 应用程序流量现在可以通过企业网络托管的网关连接器进行路由，从而避免了双因素身份验证。如果客户发布了托管在公司网络外部的 SaaS 应用程序，现在将添加支持，以验证该应用程序通过本地网关连接器的流量。

  例如，假设客户拥有受 Okta 保护的 SaaS 应用程序（如 Workday）。客户可能希望，即使实际的 Workday 数据流量不是通过 Citrix Gateway 服务路由的，但通过 Citrix Gateway 服务将通过本地网关连接器路由到 Okta 服务器的身份验证流量。当用户从企业网络内连接到 Okta 服务器时，这有助于客户避免 Okta 服务器进行第二因素身份验证。

  [NGSWS-6445]
- 禁用筛选网站列表和网站分类。如果管理员选择不为特定客户应用这些功能，则可以禁用过滤网站列表和网站分类。

  [NGSWS-6532]
- **Remote Browser Isolation** 服务重定向的自动地理路由。现在已为 Remote Browser Isolation 服务重定向启用自动地理路由。

  [NGSWS-6926]

V2019.03.01

- 在“添加网关连接器”页面中添加了“检测”按钮。检测 按钮用于刷新连接器列表，从而允许新添加的连接器反映在 Web 应用程序连接部分中。

  [CGOP-6358]

- 在“访问控制 **Web** 过滤”类别中添加了一个新类别“恶意和危险”。在“恶意软件和垃圾邮件”组下添加了 访问控制 **Web** 筛选 类别中名为“恶意和危险”的新类别。

  [CGOP-6205]

功能弃用

June 19, 2024

本文将提前告知您正在逐步淘汰的 Secure Private Access 服务功能，以便您可以及时做出业务决策。Citrix 将监视客户使用情况和反馈以确定功能的退出时间。在后续版本中声明可能会有更改，可能不会包括每个弃用的特性或功能。有关产品生命周期支持的详细信息，请参阅 产品生命周期支持政策。

下表列出了已弃用或计划弃用的 Secure Private Access 服务功能。

项目	已在其中宣布弃用的版本	弃用日期	备选
用于访问 Web 应用程序的无客户端 VPN 访问方法	2023 年 1 月	2023 年 10 月 17 日	根据您的用例使用 Citrix Enterprise Browser 或直接访问。有关更多详细信息，请参阅关于弃用无客户端 VPN 访问 Web 应用程序。
基于类别的 Web 筛选	2022 年 12 月	2022 年 12 月 31 日	将保留 Secure Private Access 中每个网站的允许、拒绝或 RBI 重定向功能，以便从 Citrix Enterprise Browser 选择性地访问与工作无关的网站。
限制导航安全控制	2022 年 4 月	2022 年 6 月 15 日	不适用

项目	已在其中宣布弃用的版本	弃用日期	备选
Citrix Gateway Connector	2022 年 5 月	2022 年 9 月 30 日	Connector Appliance。要将网关连接器迁移到 Connector Appliance，请参阅将网关连接器迁移到 Connector Appliance。

关于弃用 **Web** 应用程序访问的无客户端 **VPN**

- 什么是无客户端 VPN 访问方法?

  当通过 Workspace for Web（适用于 HTML5 的 Citrix Workspace 应用程序）访问配置为没有任何增强安全限制的内部网络应用程序时，Citrix Secure Private Access 使用基于 CVPN 的访问方法。

  > 注意：
  >
  > 仅当通过 Workspace for Web（适用于 HTML5 的 Citrix Workspace 应用程序）访问内部应用程序时，才使用无客户端 VPN 访问方法。只有未配置增强安全限制的应用程序才会被屏蔽。

- 我们为什么要弃用这个功能?

  无客户端 VPN 方法使用客户端 URL 重写，这具有某些行业范围的技术限制。在某些情况下，当重写 Web 应用程序中的某些链接时，可能会导致应用程序访问失败。这会导致最终用户体验不佳。为了向我们的客户提供最佳的应用程序访问体验，我们已弃用此功能，并建议改用下面提到的替代方案之一。

- 它将如何影响访问已配置 Secure Private Access 的应用程序的最终用户?

  如果通过 Workspace for Web 访问任何配置但没有增强安全限制的 Web 应用程序，则对该应用程序的访问将被阻止。
  它不会影响最终用户通过 Workspace 应用程序、直接访问、Remote Browser Isolation (RBI) 或 Secure Access Agent 访问应用程序。

- 有哪些替代方案，管理员应该怎么做?

  Citrix Enterprise Browser：使用 Citrix Workspace 应用程序通过 Citrix Enterprise Browser 访问这些应用程序。此方法通过增强的安全设置（例如限制下载、打印限制、水印、限制剪贴板访问）和浏览器管理，提供最佳的最终用户体验。适用于 Citrix Workspace 的 Secure Private Access。
  直接访问：如果您想使用无客户端方法来访问网络应用程序，请使用直接访问方法，通过该方法，可以直接从任何本机浏览器（例如 Chrome）访问应用程序。此方法可用于无法在终端设备上安装 Citrix Workspace 应用程序的用例，也可用于非托管设备。有关更多详细信息，请参阅 直接访问企业 Web 应用程序。

- 它会影响通过 Citrix Workspace 应用程序或 Secure Access Agent 访问的任何现有应用程序吗?

  不，我们仅禁止访问通过 Workspace for Web 访问的 Web 应用程序。此次弃用不会影响通过安装在终端设备上的 Citrix Workspace 应用程序或 Secure Access 客户端访问的任何应用程序。如果通过 Workspace for

Web 或 Citrix Workspace 应用程序的 HTML5 变体访问配置了增强安全限制的网络应用程序，则对这些应用程序的访问将被阻止。

- 还有其他问题吗？

  请联系 Citrix 支持人员。

Citrix Secure Private Access 入门

June 19, 2024

本文档将向您介绍如何首次开始加入和设置 SaaS 应用程序交付。本文档面向应用程序管理员。

系统要求

操作系统支持： Windows 7、8、10 和 Mac 10.11 及更高版本支持 Citrix Workspace 应用程序。

浏览器支持：使用最新版本的 Edge、Chrome、Firefox 或 Safari 浏览器访问工作区。

Citrix Workspace 支持：使用适用于任何桌面平台（Windows、Mac）的 Citrix Workspace 访问工作区。

工作原理

Citrix Secure Private Access 可帮助 IT 和安全管理员管理授权的最终用户对经批准的 SaaS 和企业托管 Web 应用程序的访问。用户标识和属性用于确定访问权限，而访问控制策略用于确定执行操作所需的权限。用户通过身份验证后，访问控制将授权相应级别的访问权限以及与该用户的凭据关联的允许操作。

Citrix Secure Private Access 结合了多种 Citrix Cloud 服务的元素，为最终用户和管理员提供集成的体验。

功能	提供功能的服务/组件
使用一致的用户界面访问应用程序	Workspace 体验/Workspace 应用程序
SSO 到 SaaS 和 Web 应用程序	Citrix Gateway Service Standard
Web 过滤和分类	网页过滤服务
针对 SaaS 的增强安全策略	云端应用程序控制
安全浏览	Remote Browser Isolation 服务
网站访问和风险行为的可见性	Citrix Analytics

开始使用 **Citrix Secure Private Access** 服务

1. 注册 Citrix Cloud。
2. 请求 Secure Private Access 服务权利。
3. 授权后，我的服务下提供了 Secure Private Access 服务。
4. 访问 Secure Private Access 服务 UI。

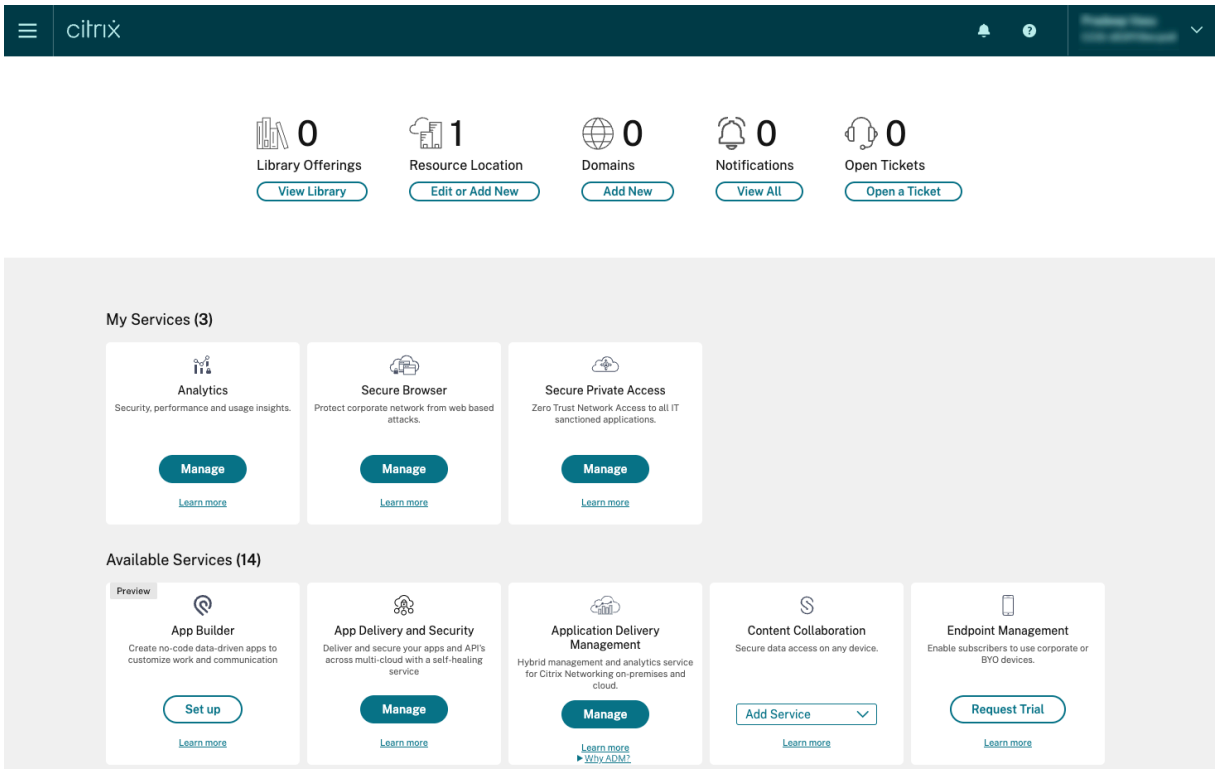
第 1 步：注册 **Citrix Cloud**

要开始使用 Secure Private Access 服务，您必须先创建 Citrix Cloud 帐户或加入由贵公司其他人创建的现有帐户。有关如何继续操作的详细流程和说明，请参阅注册 Citrix Cloud。

步骤 2：申请 **Secure Private Access** 服务权利

要请求 Secure Private Access 服务授权，请在 **Citrix Cloud** 屏幕的“可用服务”部分下，单击“Secure Private Access”磁贴中的“请求试用”选项卡。

有关许可证的详细信息，请参阅 https://www.citrix.com/buy/licensing/product.html。



第 3 步：发布授权，在“我的服务”下提供 **Secure Private Access** 服务

收到 Secure Private Access 服务权利后，“Secure Private Access”服务磁贴将移至“我的服务”部分。

步骤 4：访问 **Secure Private Access** 服务 **UI**

单击磁贴上的 管理 选项卡以访问 Secure Private Access 服务用户界面。

注意：

- 要使最终用户使用 Workspace 和访问应用程序，他们必须下载并使用 Citrix Workspace 应用程序或使用 Workspace URL。您必须将几个 SaaS 应用程序发布到您的工作区才能测试 Citrix Secure Private Access 解决方案。Workspace 应用程序可以从 https://www.citrix.com/downloads 下载。在“查找下载内容”列表中，选择 **Citrix Workspace** 应用程序。
- 如果您配置了出站防火墙，请确保允许访问以下域。

  - *.cloud.com
  - *.nssvc.net
  - *.netscalergateway.net

  有关更多详细信息，请参阅 Cloud Connector 代理和防火墙配置 以及 Internet 连接要求。
- 您只能添加一个 Workspace 帐户。

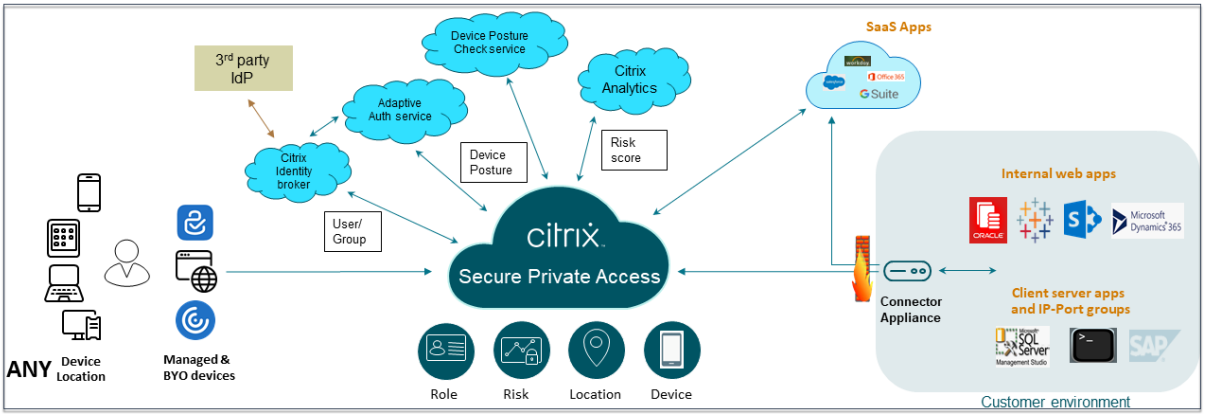
Secure Private Access 服务解决方案概述

June 19, 2024

解决方案概述

传统 VPN 解决方案要求管理最终用户设备，在网络级别提供访问并强制执行静态访问控制策略。Citrix Secure Private Access 为 IT 提供了一组安全控制措施，以防范来自自带设备的威胁，使用户可以选择从任何设备（无论是托管设备还是自带设备）访问经过 IT 批准的应用程序。

Citrix Secure Private Access 为应用程序提供自适应身份验证、单点登录支持和增强的安全控制。Secure Private Access 还提供了在使用 Device Posture 服务建立会话之前扫描最终用户设备的功能。根据自适应身份验证或 Device Posture 结果，管理员可以为应用程序定义身份验证方法。



自适应安全

自适应身份验证为当前请求确定正确的身份验证流程。自适应身份验证可以识别 Device Posture、地理位置、网段、用户组织/部门成员资格。根据获得的信息，管理员可以定义他们希望如何向其 IT 认可的应用程序对用户进行身份验证。这允许组织在所有资源上实施相同的认证策略框架，包括公共 SaaS 应用程序、私有 Web 应用程序、私有客户端服务器应用程序和桌面即服务 (DaaS)。有关详细信息，请参阅 自适应安全。

应用程序访问权限

Secure Private Access 可以在不依赖 VPN 的情况下创建与本地 Web 应用程序的连接。这种无 VPN 的连接使用本地部署的 Connector Appliance。Connector Appliance 为组织的 Citrix Cloud 订阅创建出站控制通道。从那里，Secure Private Access 无需使用 VPN 即可通过通道连接到内部 Web 应用程序。有关详细信息，请参阅 应用程序访问权限。

单点登录

借助自适应身份验证，组织可以提供强大的身份验证策略，以帮助降低用户帐户遭到入侵的风险。Secure Private Access 的单点登录功能对所有 SaaS、私有 Web 和客户端服务器应用程序使用相同的自适应身份验证策略。有关详细信息，请参阅 单点登录。

浏览器安全

Secure Private Access 使最终用户能够使用集中管理和安全的 Enterprise Browser 安全地浏览 Internet。当最终用户启动 SaaS 或私有 Web 应用程序时，会动态做出多个决策，以决定如何最好地为该应用程序提供服务。有关详细信息，请参阅 浏览器安全。

Device Posture

Device Posture 服务允许管理员定义策略，以检查尝试远程访问公司资源的端点设备的状态。根据终端的合规性状态，Device Posture 服务可以拒绝访问或提供对企业应用程序和桌面的限制/完全访问权限。

当最终用户发起与 Citrix Workspace 的连接时，Device Posture 客户端会收集有关端点参数的信息，并与 Device Posture 服务共享这些信息，以确定端点的状态是否符合策略要求。

将 Device Posture 服务与 Citrix Secure Private Access 相集成，可以从任何地方安全访问 SaaS、Web、TCP 和 UDP 应用程序，同时提供 Citrix Cloud 的灵活性和可扩展性。有关详细信息，请参阅 Device Posture。

支持 **TCP** 和 **UDP** 应用程序

有时，远程用户需要访问私有客户端-服务器应用程序，这些应用程序的前端位于端点，后端位于数据中心。组织可以理所当然地围绕这些内部和私有应用程序执行严格的安全策略，这使得远程用户很难在不影响安全协议的情况下访问这些应用程序。

Secure Private Access 服务通过允许 ZTNA 提供对这些应用程序的安全访问来解决 TCP 和 UDP 安全漏洞。用户现在可以使用本机浏览器或通过在其计算机上运行的 Citrix Secure Access 客户端访问所有专用应用程序，包括 TCP、UDP 和 HTTPS 应用程序。

用户必须在其客户设备上安装 Citrix Secure Access 客户端。

- 对于 Windows，可以从 https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html 下载客户端版本（22.3.1.5 及更高版本）。
- 对于 macOS，可以从 App Store 下载客户端版本（22.02.3 及更高版本）。

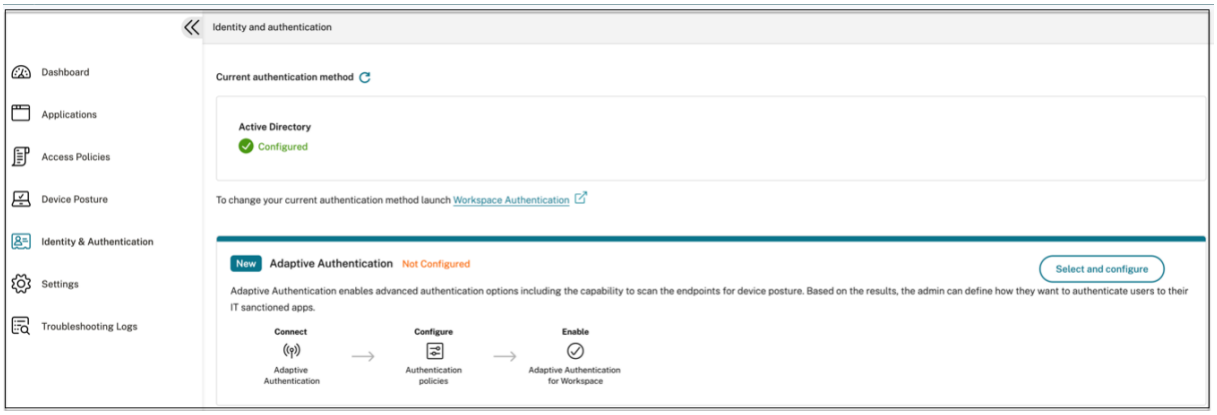
有关详细信息，请参阅 对客户端-服务器应用程序的支持。

设置 **Citrix Secure Private Access**

使用 Secure Private Access 管理控制台启用对 SaaS 应用程序、内部 Web 应用程序、TCP 和 UDP 应用程序的零信任网络访问权限。此控制台包括自适应身份验证的配置、包括用户订阅在内的应用程序和自适应访问策略。

设置身份和身份验证

选择订阅者登录 Citrix Workspace 的身份验证方法。自适应身份验证是一项 Citrix Cloud 服务，可为登录 Citrix Workspace 的客户和用户启用高级身份验证。



有关详细信息，请参阅 设置身份和身份验证。

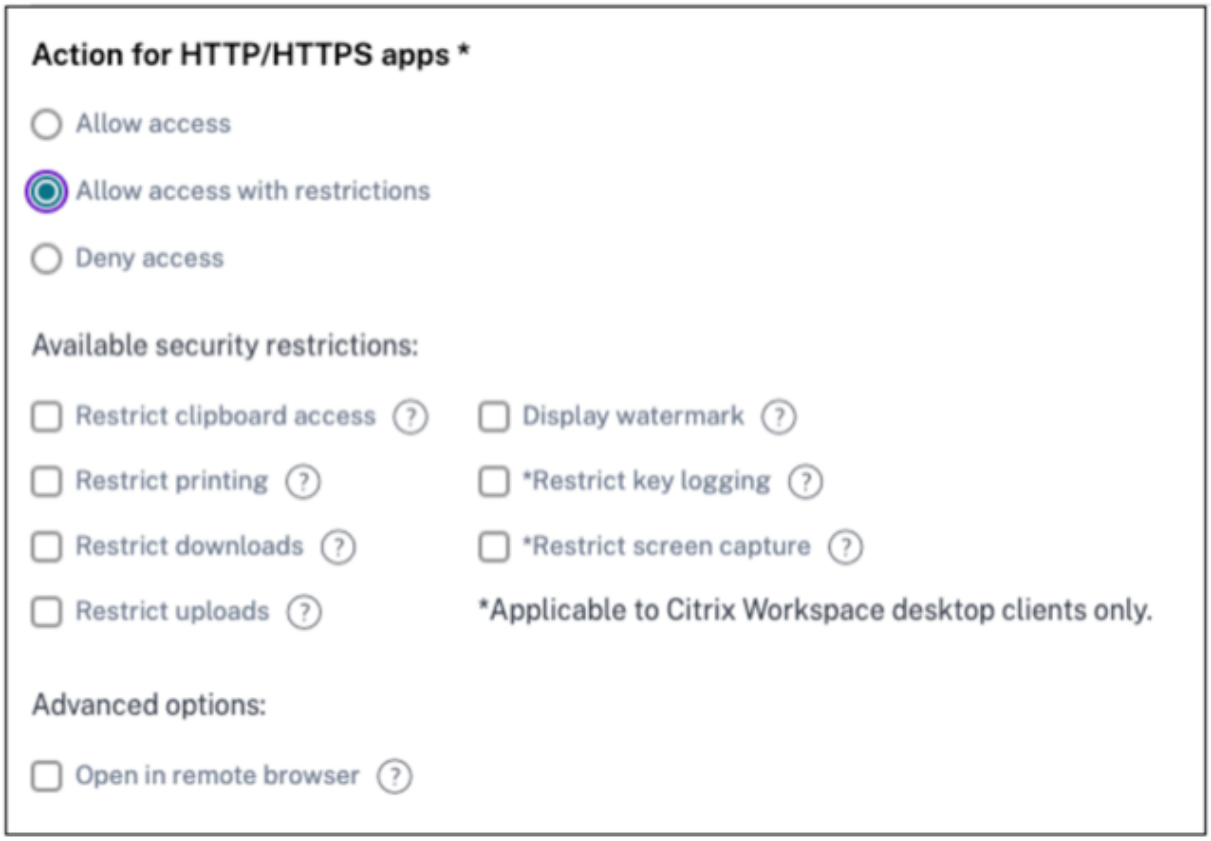
枚举和发布应用程序

选择身份验证方法后，使用管理员控制台配置 Web、SaaS 或 TCP 和 UDP 应用程序。有关详细信息，请参阅 添加和管理应用程序。

启用增强的安全控制

为了保护内容，组织在 SaaS 应用程序中纳入了增强的安全策略。在桌面上使用 Workspace 应用程序时，每个策略都会对 Citrix Enterprise Browser 实施限制，或者在使用 Workspace 应用程序 Web 或移动设备时在 Secure Browser 上实施限制。

- 限制剪贴板访问权限：禁用应用程序和系统剪贴板之间的剪切/复制/粘贴操作。
- 限制打印：禁用从 Citrix Enterprise Browser 中打印的功能。
- 限制下载：禁用用户从应用程序内下载的权限。
- 限制上载：禁用用户在应用程序内上载的功能。
- 显示水印：在用户屏幕上显示水印，显示用户计算机的用户名和 IP 地址。
- 限制按键记录：防范按键记录器。当用户尝试使用用户名和密码登录应用程序时，所有密钥都会在密钥记录器上加密。此外，用户在应用程序上执行的所有活动都受到密钥记录的保护。例如，如果为 Office 365 启用了 App Protection 策略，并且用户编辑 Office 365 Word 文档，则所有按键记录器上的按键都经过加密。
- 限制屏幕截图：禁用使用任何屏幕捕获程序或应用程序捕获屏幕的功能。如果用户尝试捕获屏幕，则会捕获一个空白屏幕。



有关详细信息，请参阅配置访问策略。

启用 **Citrix Enterprise Browser** 以启动应用程序

Secure Private Access 使最终用户能够使用 Citrix Enterprise Browser (CEB) 启动其应用程序。CEB 是一款基于 Chromium 的浏览器，与 Citrix Workspace 应用程序集成在一起，可在 Citrix Enterprise Browser 中访问网络和 SaaS 应用程序，从而实现无缝和安全的访问体验。

可以将 CEB 配置为所有内部托管的 Web 应用程序或具有安全策略的 SaaS 应用程序的首选浏览器或工作浏览器。CEB 允许用户在安全和受控的环境中打开所有已配置的 SaaS/Web 应用程序域。

启用 Citrix Enterprise Browser 管理员可以使用 Global App Configuration Service (GACS) 将 Citrix Enterprise Browser 配置为默认浏览器，以便从 Citrix Workspace 应用程序启动 Web 和 SaaS 应用程序。

通过 **API** 进行配置：

为了进行配置，以下是默认情况下为所有应用程序启用 Citrix Enterprise Browser 的 JSON 文件示例：

```
1 "settings": [
2                   {
3
4                      "name": "open all apps in ceb",
```



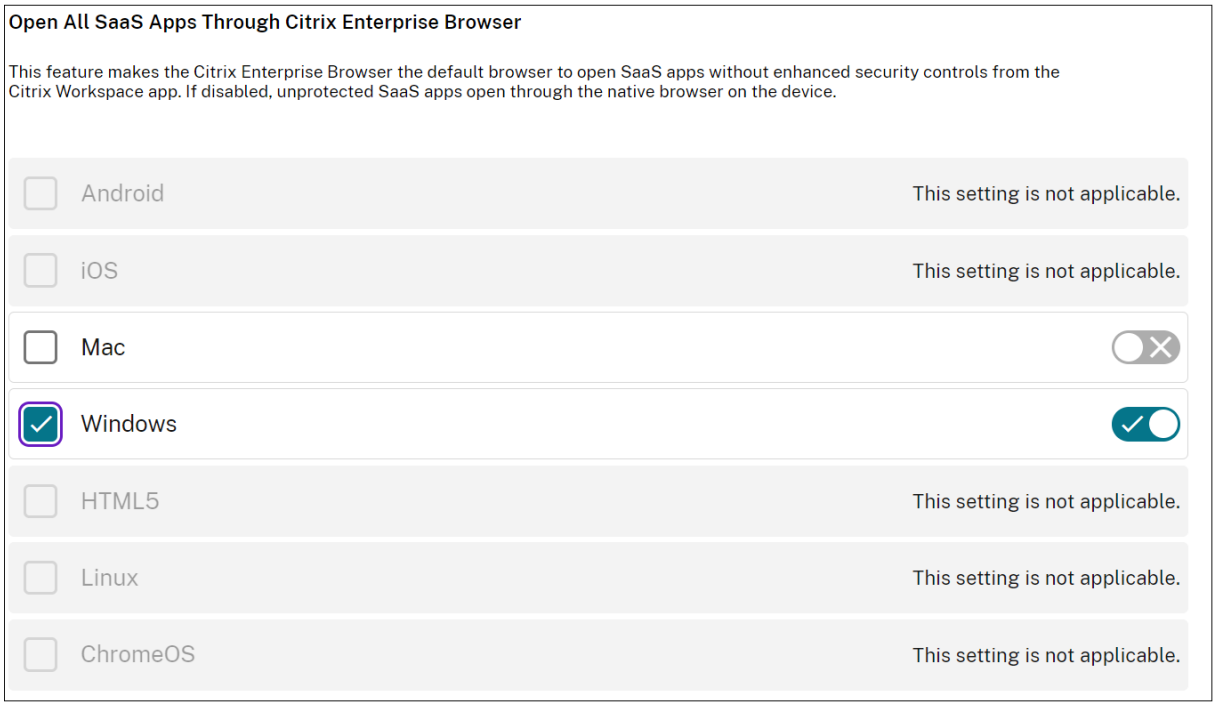
```
                    "value": "true"
                }

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

默认值为 true。

通过 **GUI** 进行配置：

选择必须将 CEB 设置为应用程序启动的默认浏览器的设备。



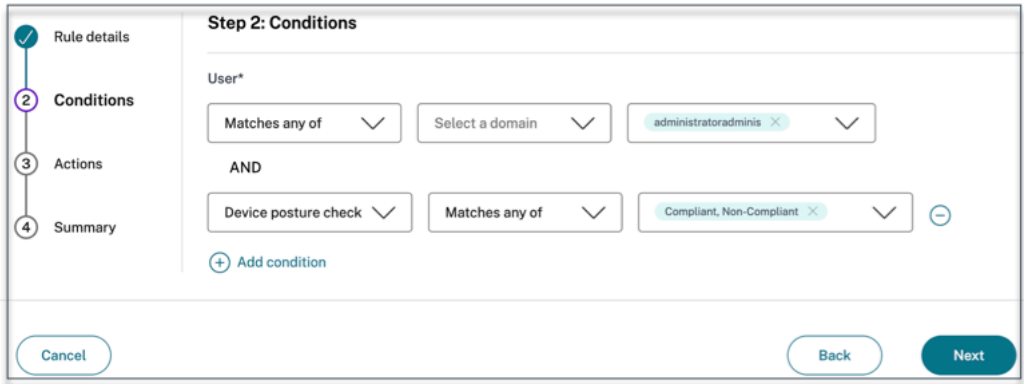
有关详细信息，请参阅通过 GACS 管理 Citrix Enterprise Browser。

使用 **Device Posture** 配置用于上下文访问的标签

Device Posture 验证后，允许设备登录，并将设备归类为合规或不合规。此分类作为 Secure Private Access 服务的标签提供，用于根据 Device Posture 提供上下文访问。

1. 登录 Citrix Cloud。
2. 在 Secure Private Access 图块上，单击管理。
3. 在左侧导航栏中单击“访问策略”，然后单击“创建策略”。
4. 输入策略名称和策略描述。
5. 在 应用程序中，选择必须强制执行此策略的应用程序或一组应用程序。
6. 单击“创建规则”为策略创建规则。

7. 输入规则名称和规则的简要描述，然后单击“下一步”。
8. 选择用户的条件。用户条件是向用户授予应用程序访问权限时必须满足的强制性条件。
9. 单击 **+** 添加 Device Posture 条件。
10. 从下拉菜单中选择 **Device Posture** 检查和逻辑表达式。
11. 在自定义标签中输入以下值之一：



- 合规 - 适用于合规设备
- 不合规 - 适用于不兼容的设备

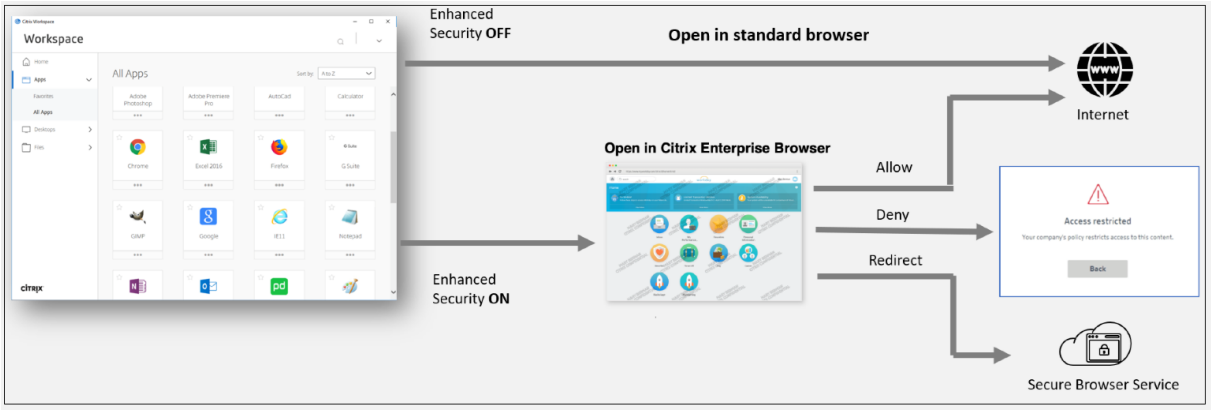
12. 单击下一步。
13. 根据条件评估选择必须应用的操作，然后单击“下一步”。

    摘要页面显示策略的详细信息。
14. 验证详细信息，然后单击完成。

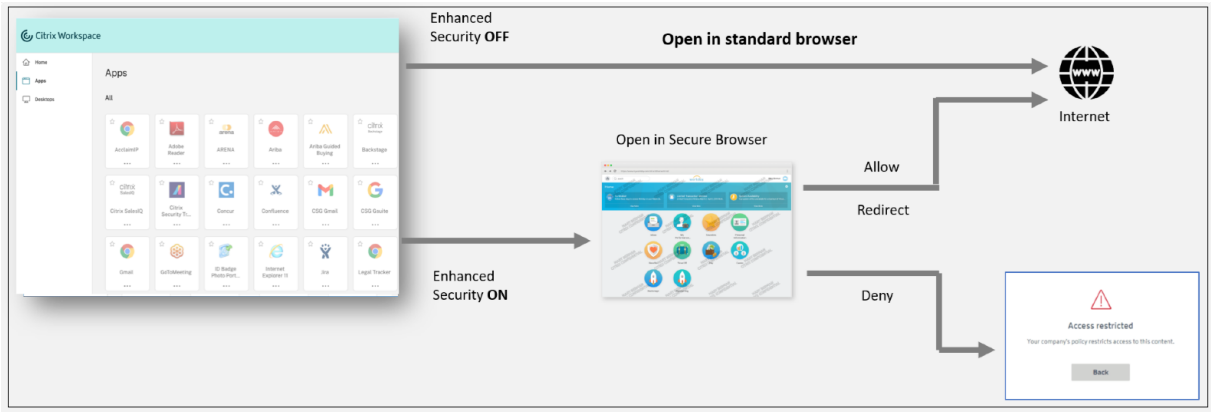
> 注意：
>
> 任何未在访问策略中标记为合规或不合规的 Secure Private Access 应用程序都被视为默认应用程序，无论 Device Posture 如何，均可在所有端点上访问。

最终用户体验

Citrix 管理员有权在 Citrix Secure Private Access 的帮助下扩展安全控制。Citrix Workspace 应用程序是安全访问所有资源的入口点。最终用户可以通过 Citrix Workspace 应用程序访问虚拟应用程序、桌面、SaaS 应用程序和文件。借助 Citrix Secure Private Access，管理员可以控制最终用户如何通过 Citrix Workspace Experience 网页用户界面或原生 Citrix Workspace 应用程序客户端访问 SaaS 应用程序。



当用户在终端上启动 Workspace 应用程序时，他们会看到自己的应用程序、桌面、文件和 SaaS 应用程序。如果用户在禁用增强安全性时单击 SaaS 应用程序，则该应用程序将在本地安装的标准浏览器中打开。如果管理员启用了增强安全性，则 SaaS 应用程序将在 CEB 上的 Workspace 应用程序中打开。SaaS 应用程序和 Web 应用程序中超链接的可访问性是根据未经批准的网站策略进行控制的。有关未经批准的 Web 站点的详细信息，请参阅未经批准的 Web 站点。



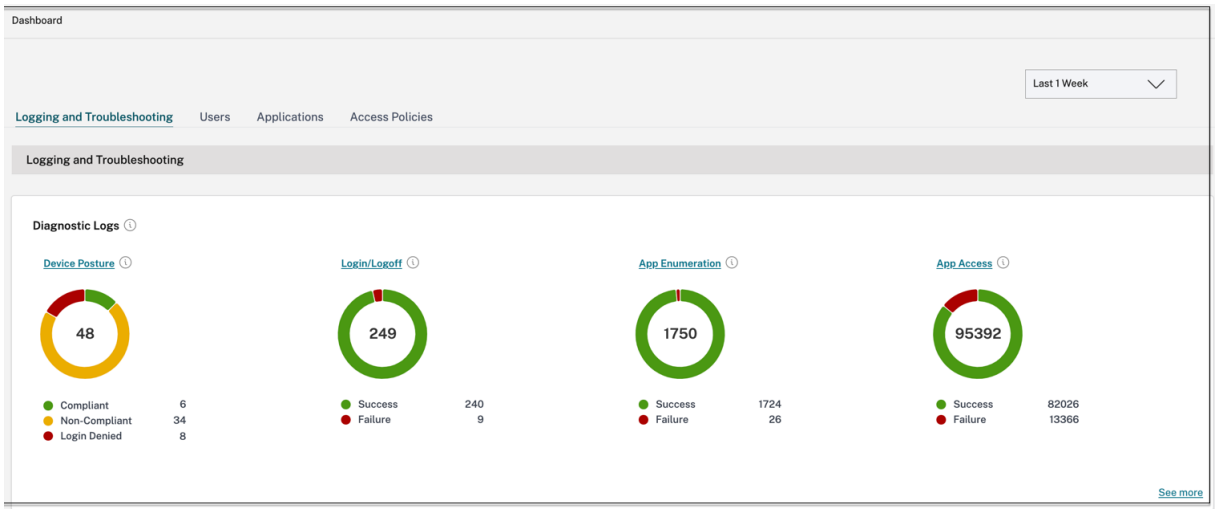
同样，在 Workspace Web 门户中，禁用增强安全性后，SaaS 应用程序将在本机安装的标准浏览器中打开。启用增强安全性后，将在安全的远程浏览器中打开 SaaS 应用程序。用户可以根据未经批准的网站策略访问 SaaS 应用程序中的网站。有关未经批准的 Web 站点的详细信息，请参阅未经批准的 Web 站点。

“分析”控制板

Secure Private Access 服务控制面板显示 SaaS、Web、TCP 和 UDP 应用程序的诊断和使用数据。控制面板让管理员可以在一个地方全面了解其应用程序、用户、连接器运行状况和带宽使用情况，以供使用。这些数据是从 Citrix Analytics 获取的。这些指标大致分为以下几类。

- 记录和故障排除
- 用户
- 应用程序
- 访问策略

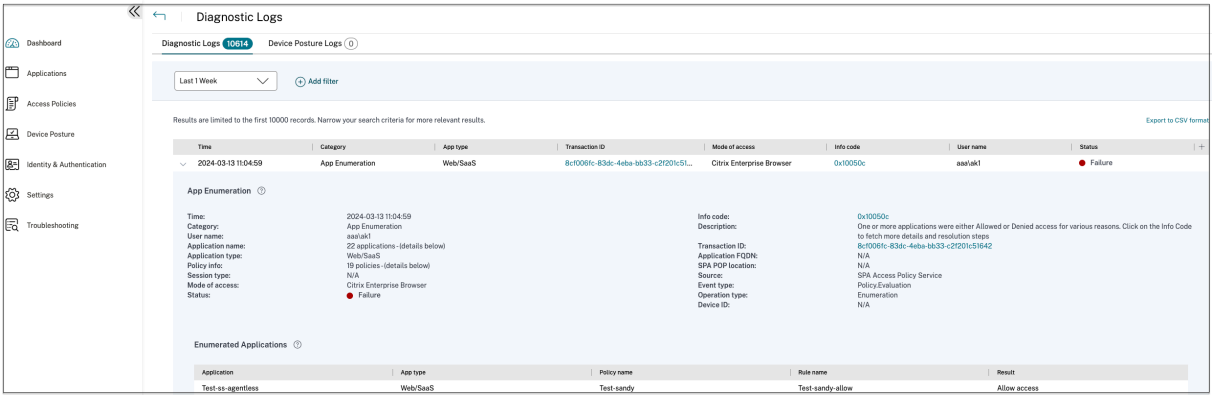
有关详细信息，请参阅 控制面板。



解决应用程序问题

Secure Private Access 仪表板中的诊断日志图表可让您查看与身份验证、应用程序启动、应用程序枚举和 Device Posture 日志相关的日志。

- 信息代码：某些日志事件（例如失败）具有相关的信息代码。单击信息代码会将用户重定向到解决步骤或有关该事件的更多信息。
- 事务 **ID**：诊断日志还显示一个事务 ID，用于关联访问请求的所有 Secure Private Access 日志。一个应用程序访问请求可以生成多个日志，首先是身份验证，然后是工作区应用程序中的应用程序枚举，然后是应用程序访问本身。所有这些事件都会生成自己的日志。事务 ID 用于关联所有这些日志。您可以使用事务 ID 筛选诊断日志，以查找与特定应用程序访问请求相关的所有日志。
  有关详细信息，请参阅解决 Secure Private Access 问题。



示例用例

- 使用零信任方法访问内部应用程序（Web/TCP/UDP），无需在防火墙上打开传入流量

- 通过发现用户访问的应用程序转向零信任方法
- 将对 SaaS 应用程序的访问权限限制为 Citrix Enterprise Browser
- 将对 SaaS 应用程序的访问权限限制为公司拥有的公有 IP 地址
- 增强了 Azure 托管的 SaaS 应用程序的安全性
- 增强了 Office 365 的安全性
- 增强 Okta 应用程序的安全性

参考文章

- Secure Private Access 简介
- 技术简报
- 参考体系结构
- Citrix Enterprise Browser
- 通过 GACS 管理 Citrix Enterprise Browser
- 管理员指导的工作流程，便于入门和设置

参考视频

- 对应用程序的零信任网络访问 (ZTNA)
- 使用 Citrix Secure Private Access 访问私有 Web 应用程序
- 使用 Citrix Secure Private Access 访问公共 SaaS 应用程序
- 使用 Citrix Secure Private Access 访问专用客户端-服务器应用程序
- 使用 Citrix Secure Private Access 保护键盘记录器
- 使用 Citrix Secure Private Access 提供屏幕共享保护
- 最终用户使用 Citrix Secure Private Access 的体验
- 使用 Citrix Secure Private Access 的 ZTNA 与 VPN 的登录体验
- 使用 Citrix Secure Private Access 扫描 ZTNA 与 VPN 端口的对比

相关产品有哪些新内容

- Citrix Enterprise Browser：关于此版本
- Citrix Workspace：新增功能
- Citrix DaaS：新增功能
- Citrix Secure Access 客户端 NetScaler Gateway 客户端

管理员指导的工作流程，便于入门和设置

June 19, 2024

Secure Private Access 服务提供了全新的简化管理员体验，其中包含配置对 SaaS 应用程序、内部 Web 应用程序和 TCP 应用程序的零信任网络访问的分步流程。它包括在单个管理控制台中配置自适应身份验证、包括用户订阅在内的应用程序、自适应访问策略和其他应用程序。

此向导可帮助管理员在入门或经常使用期间实现无错误的配置。此外，还提供了一个新的控制板，可以全面了解总体使用情况指标和其他关键信息。

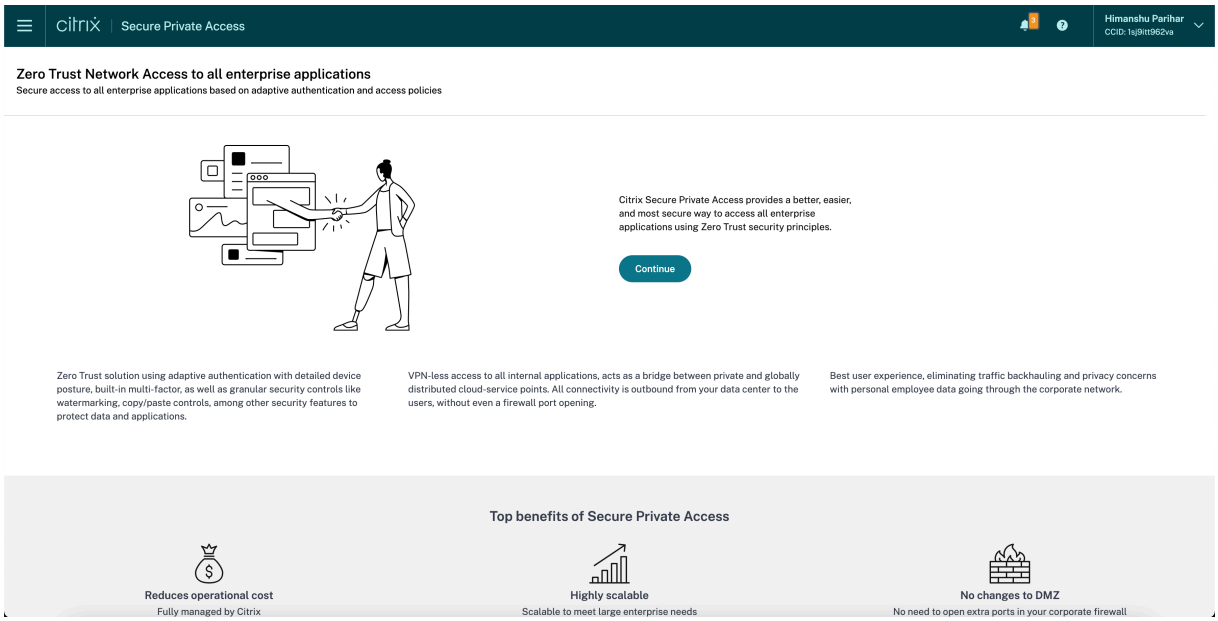
高级步骤包括以下内容：

1. 选择订阅者登录 Citrix Workspace 的身份验证方法。
2. 为用户添加应用程序。
3. 通过创建所需的访问策略来分配应用程序访问权限。
4. 查看应用程序配置。

访问 **Secure Private Access** 管理员指导的工作流程向导

要访问向导，请执行以下步骤。

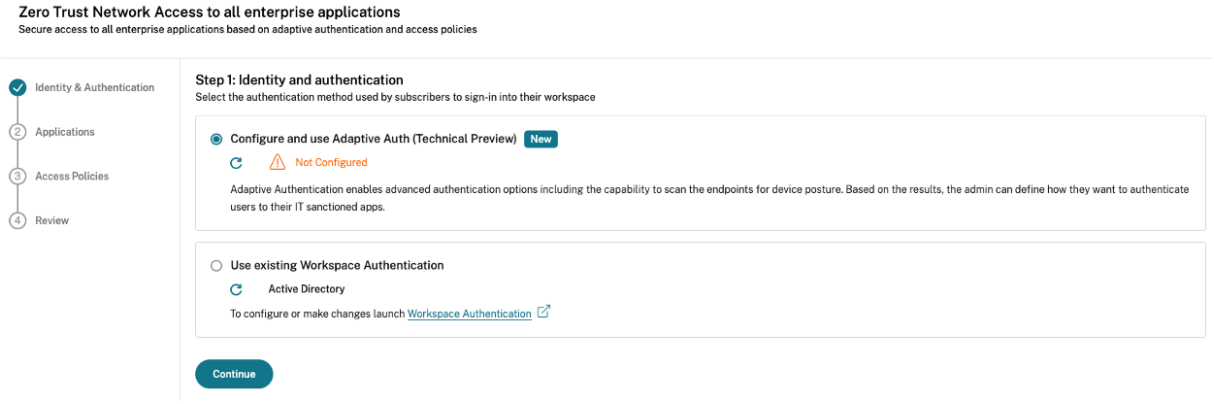
1. 在 **Secure Private Access** 服务图块上，单击“管理”。
2. 在“概述”页面中，单击继续。



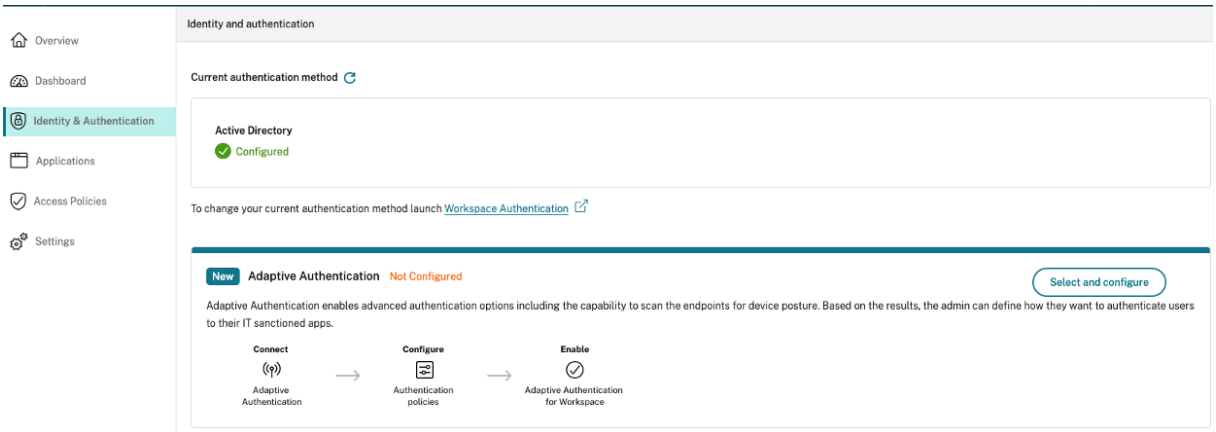
步骤 **1**：设置身份和身份验证

选择订阅者登录 Citrix Workspace 的身份验证方法。自适应身份验证是一项 Citrix Cloud 服务，可为登录 Citrix Workspace 的客户和用户启用高级身份验证。自适应身份验证服务是 Citrix 托管、Citrix 托管、云托管的 Citrix ADC，提供所有高级身份验证功能，如下所示。

- 多重身份验证
- Device Posture 扫描
- 条件身份验证
- 对 Citrix Virtual Apps and Desktops 进行自适应访问
- 要配置自适应身份验证，请选择 配置并使用自适应身份验证（技术预览版），然后完成配置。有关自适应身份验证的更多详细信息，请参阅 自适应身份验证服务。配置自适应身份验证后，如有必要，可以单击 管理 修改配置。



- 如果您最初选择了其他身份验证方法并切换到自适应身份验证，请单击“选择并配置”，然后完成配置。

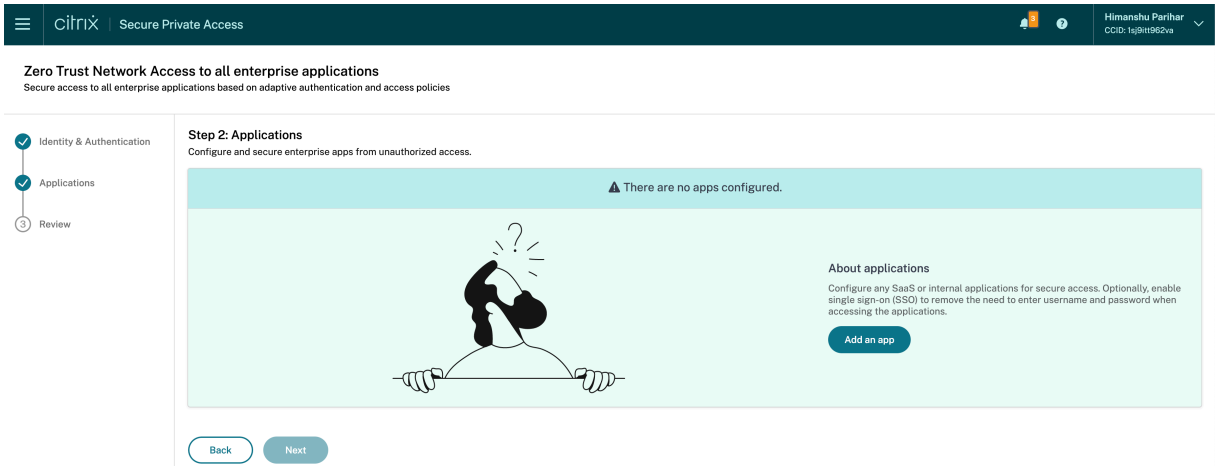


要更改现有身份验证方法或更改现有身份验证方法，请单击 **Workspace** 身份验证。

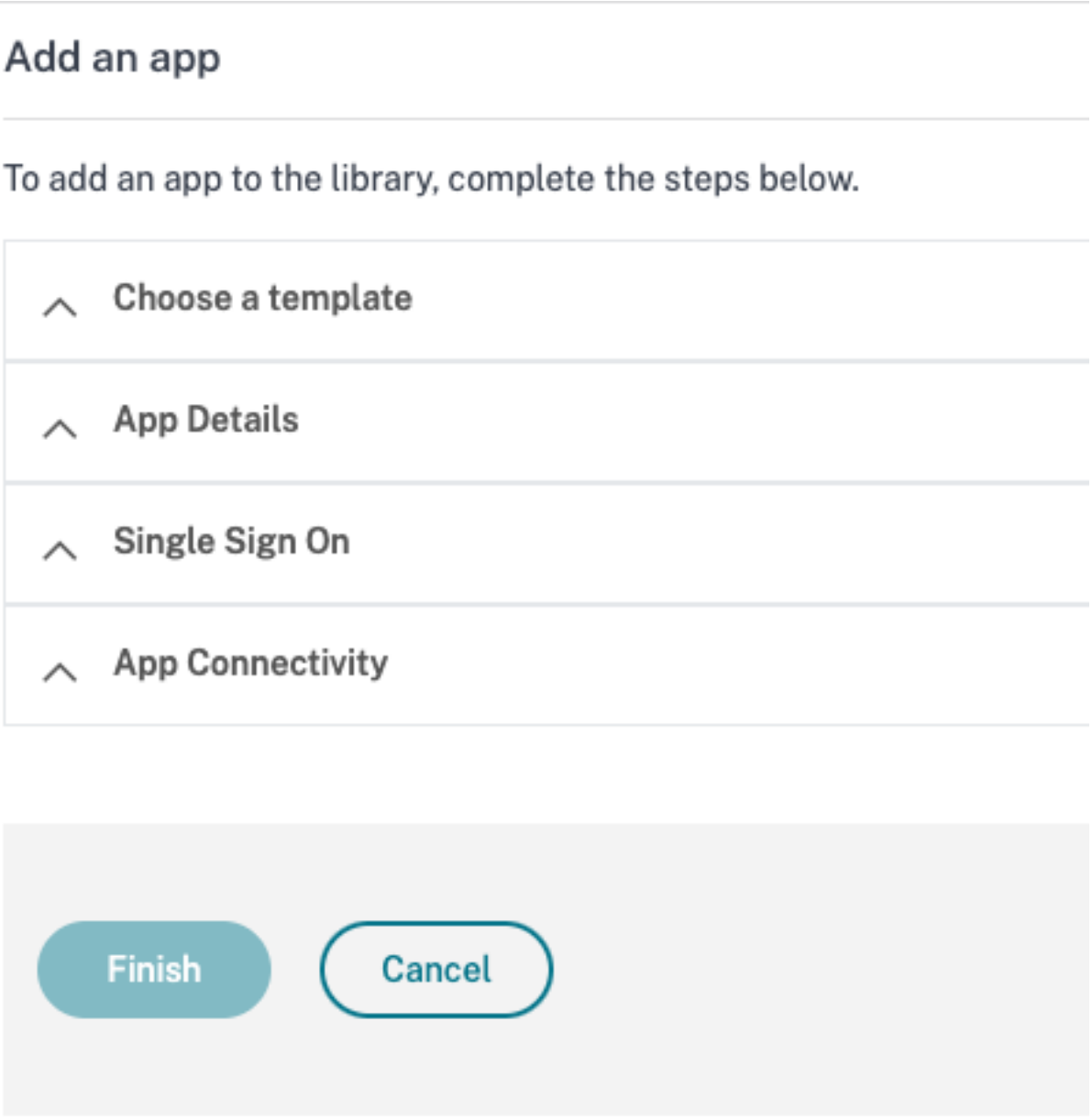
步骤 **2**：添加和管理应用程序

选择身份验证方法后，配置应用程序。对于初次使用的用户，应用程序登录页面不显示任何应用程序。通过单击添加应用程序来 添加应用程序。您可以从此页面添加 SaaS 应用程序、Web 应用程序和 TCP/UDP 应用程序。要添加应用程序，请单击添加应用程序。

添加应用程序后，您可以在此处看到它列出。



完成下图中显示的步骤以添加应用程序。



- 添加企业 **Web** 应用程序
  - 支持企业 Web 应用程序
  - 配置对 Web 应用程序的直接访问
- 添加 **SaaS** 应用程序
  - 支持软件即服务应用
  - 特定于 SaaS 应用服务器的配置
- 配置客户端-服务器应用程序
  - 支持客户端-服务器应用程序

- 启动应用
  - 启动已配置的应用程序 - 最终用户工作流
- 启用管理员的只读访问权限
  - 管理员对 SaaS 和 Web 应用程序的只读访问权限

步骤 **3**：配置具有多条规则的访问策略

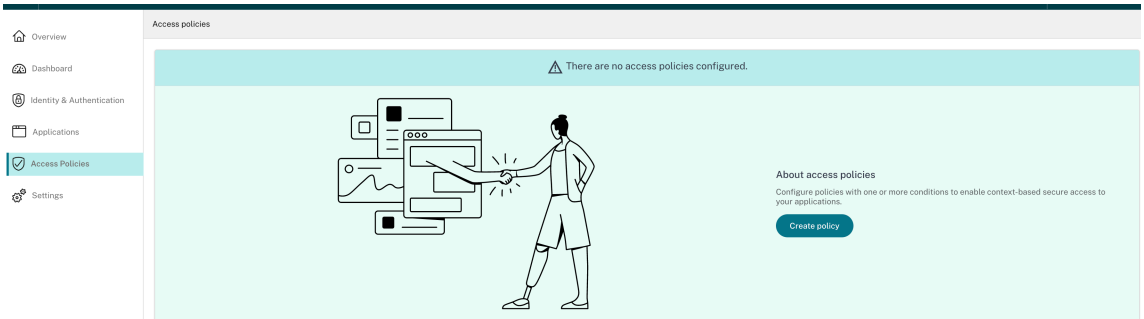
您可以创建多个访问规则，并在单个策略中为不同的用户或用户组配置不同的访问条件。这些规则可以分别应用于 HTTP/HTTPS 和 TCP/UDP 应用程序，全部应用于单个策略。

Secure Private Access 中的访问策略允许您根据用户或用户设备的环境启用或禁用对应用程序的访问。此外，您可以通过添加以下安全限制来启用对应用程序的受限访问：

- 限制剪贴板访问
- 限制打印
- 限制下载
- 限制上载
- 显示水印
- 限制密钥记录
- 限制屏幕截图

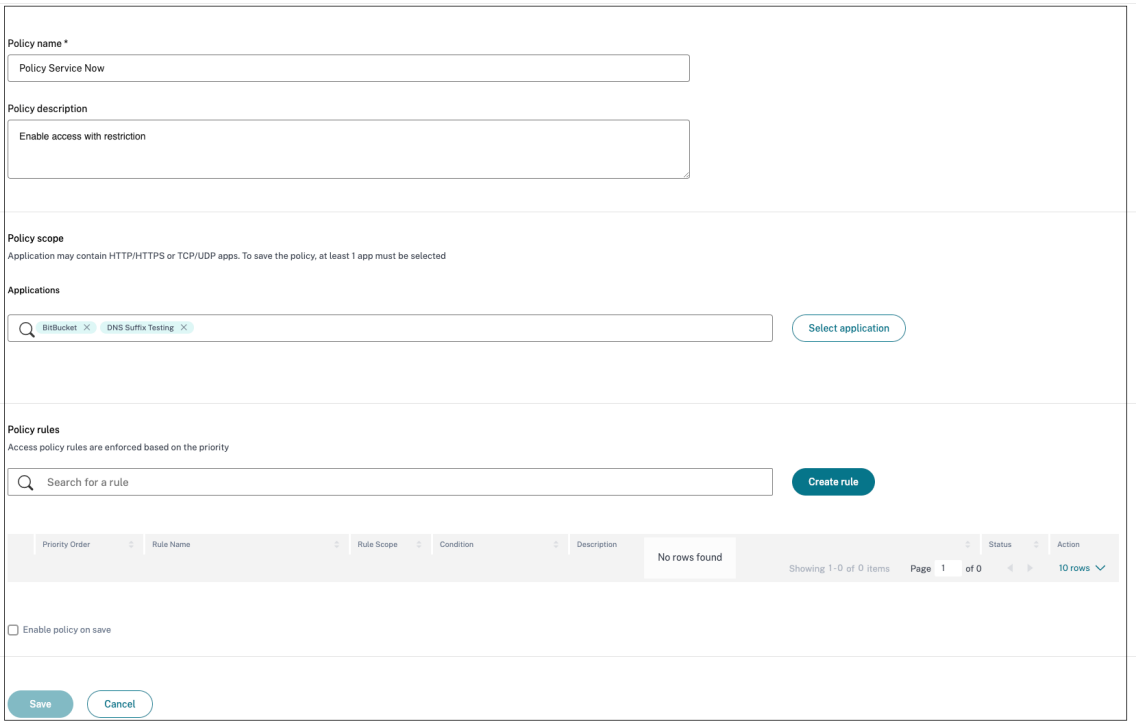
有关这些限制的更多信息，请参阅可用的访问限制选项。

1. 在导航窗格上，单击“访问策略”，然后单击“创建策略”。



   对于首次使用的用户，访问策略 登录页面不显示任何策略。创建策略后，可以看到此处列出的策略。

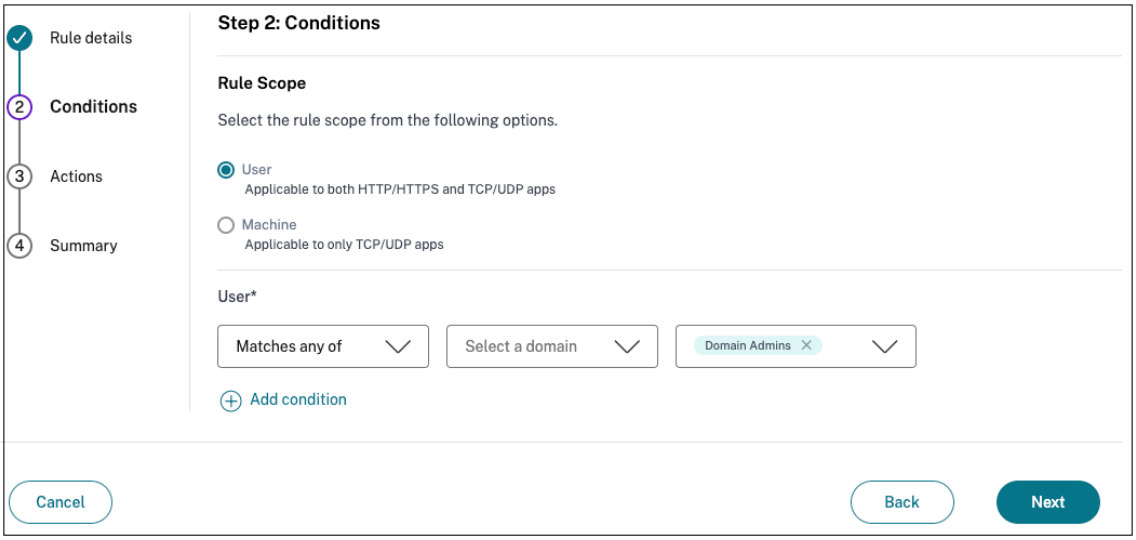
2. 输入策略名称和策略描述。
3. 在 应用程序中，选择必须强制执行此策略的应用程序或一组应用程序。
4. 单击“创建规则”为策略创建规则。



5. 输入规则名称和规则的简要描述，然后单击“下一步”。

6. 选择用户的条件。用户条件是向用户授予应用程序访问权限时必须满足的强制性条件。选择以下选项之一：

   - 匹配任一项 - 仅允许与字段中列出的任何名称相匹配且属于所选域的用户或组进行访问。
   - 不匹配任何项 - 允许除字段中列出并属于选定域的用户或组以外的所有用户或组进行访问。



7. （可选）单击 + 可根据上下文添加多个条件。

   当您基于上下文添加条件时，只有在满足 用户 和基于上下文的可选条件时，才会对策略进行评估的条件应用 AND 运算。您可以根据上下文应用以下条件。

   - 台式机或移动设备 - 选择要为其启用应用程序访问权限的设备。
   - 地理位置 - 选择用户访问应用程序的条件和地理位置。
     - 匹配以下任一项：只有从列出的任何地理位置访问应用程序的用户或用户组才可以访问应用程序。
     - 不匹配：除列出的地理位置的用户或用户组外，所有用户或用户组均已启用访问权限。
   - 网络位置 -选择用户访问应用程序所使用的条件和网络。
     - 匹配以下任一项：只有从列出的任何网络位置访问应用程序的用户或用户组才允许访问应用程序。
     - 不匹配任何项：除列出的网络位置的用户或用户组外，所有用户或用户组均已启用访问权限。
   - **Device Posture** 检查 - 选择用户设备访问应用程序必须满足的条件。
   - 用户风险评分 - 选择风险评分类别，必须根据这些类别向用户提供应用程序访问权限。
   - **Workspace URL** - 管理员可以根据与 Workspace 对应的完全限定域名指定过滤器。
     - 匹配任意一个 - 仅当传入用户连接满足任何已配置的 Workspace URL 时才允许访问。
     - 全部匹配 - 仅当传入用户连接满足所有已配置的 Workspace URL 时才允许访问。

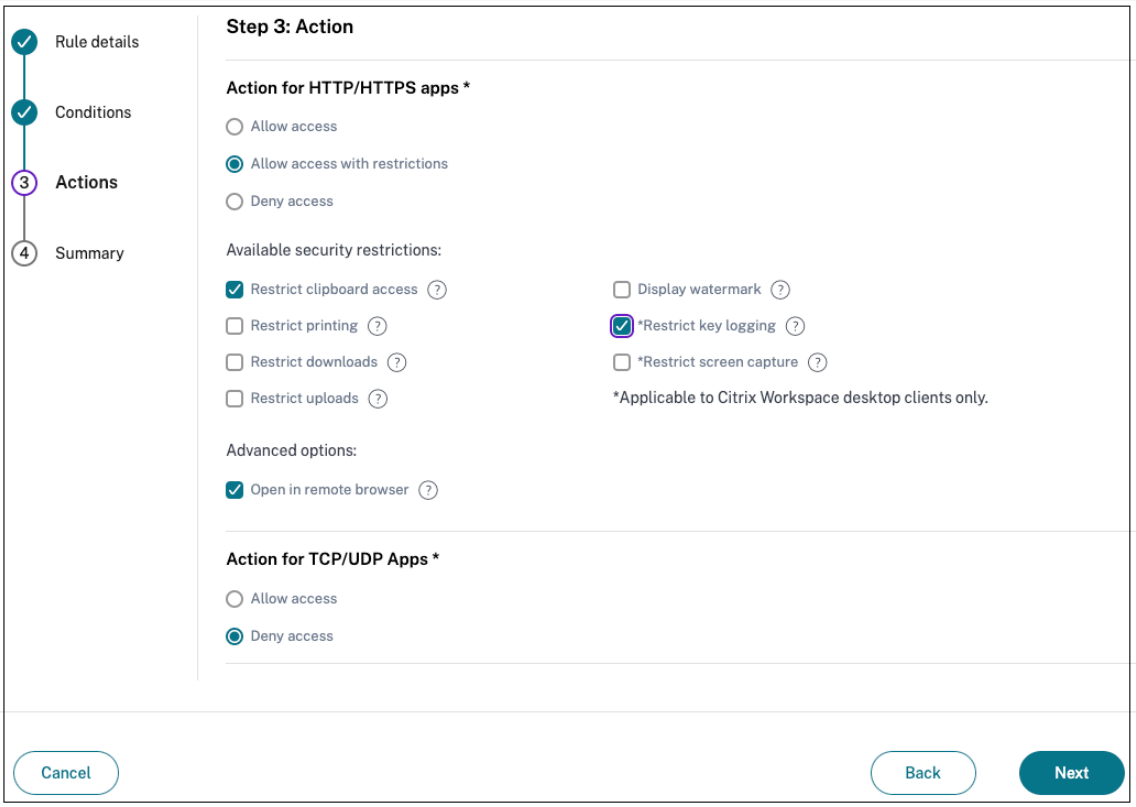
8. 单击下一步。

9. 根据条件评估选择必须应用的操作。

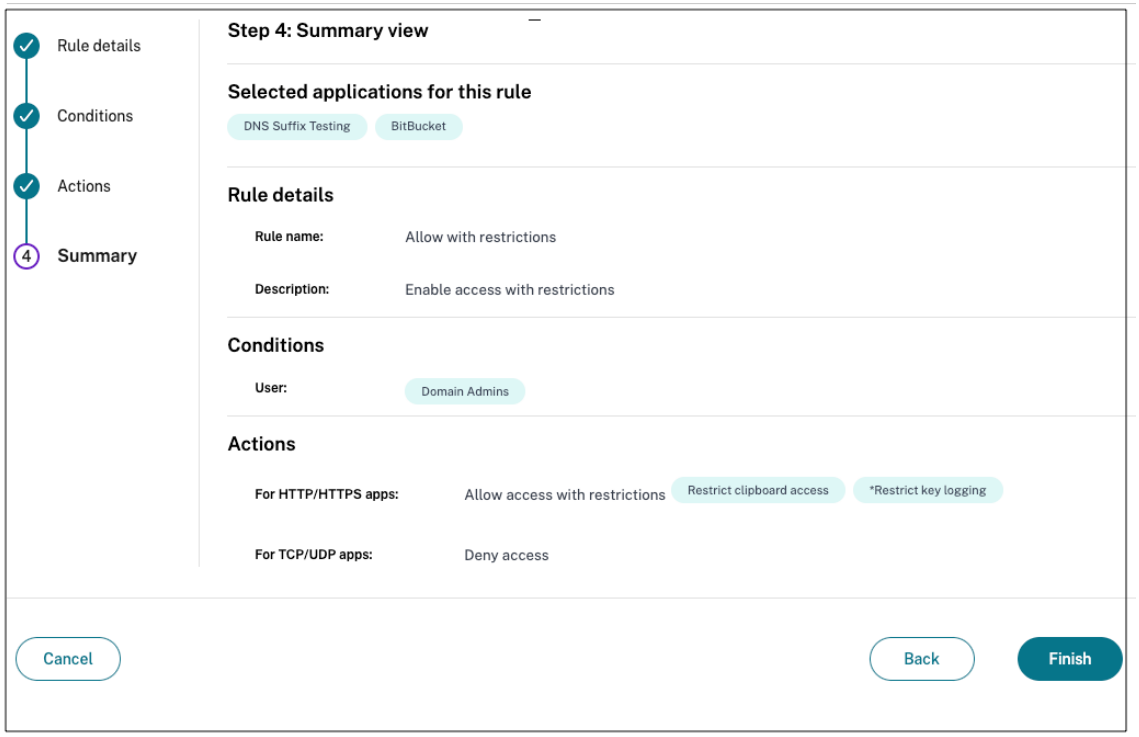
   - 对于 HTTP/HTTPS 应用程序，您可以选择以下选项：
     - 允许访问
     - 允许访问但有限制
     - 拒绝访问

> 注意：
>
> 如果选择“允许有限制的访问”，则必须选择要对应用程序强制执行的限制。有关限制的详细信息，请参阅可用的访问限制选项。您还可以指定是要在远程浏览器还是 Citrix Secure Browser 中打开应用程序。

- 对于 TCP/UDP 访问，您可以选择以下选项：
  - 允许访问
  - 拒绝访问



10. 单击下一步。摘要页面显示策略的详细信息。
11. 您可以验证详细信息，然后单击“完成”。



创建策略后要记住的几点

- 您创建的策略显示在“策略规则”部分下方，默认情况下处于启用状态。如果需要，您可以禁用规则。但是，请确保至少启用一条规则才能使策略处于活动状态。
- 默认情况下，会为策略分配优先顺序。值较低的优先级具有最高优先级。优先级编号最低的规则将首先评估。如果规则 (n) 与定义的条件不匹配，则评估下一个规则 (n+1)，依此类推。

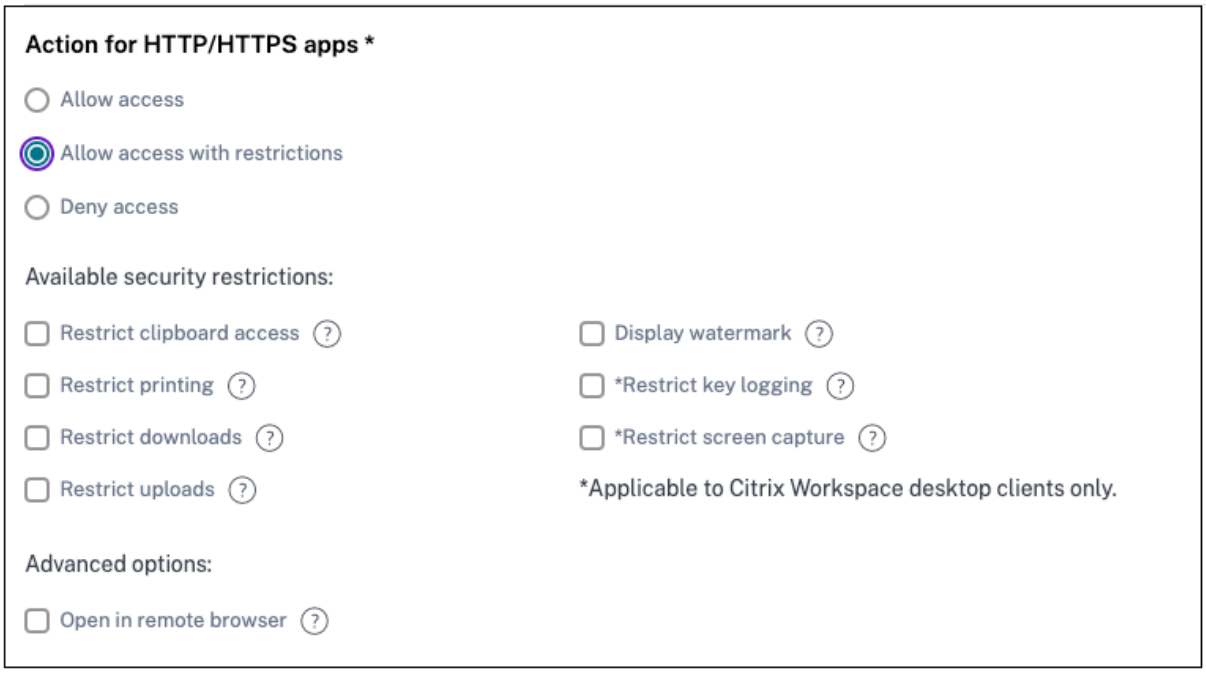
使用优先顺序评估规则示例：

假设您创建了两条规则，即规则 1 和规则 2。
规则 1 分配给用户 A，规则 2 分配给用户 B，然后评估这两条规则。
假设规则 1 和规则 2 都分配给用户 A。在这种情况下，规则 1 的优先级更高。如果规则 1 中的条件得到满足，则应用规则 1 并跳过规则 2。否则，如果规则 1 中的条件未得到满足，则规则 2 将应用于用户 A。

> 注意：
>
> 如果未评估任何规则，则不会向用户枚举应用程序。

可用的访问限制选项

选择“允许有限制的访问”操作时，必须至少选择一项安全限制。这些安全限制是在系统中预定义的。管理员无法修改或添加其他组合。可以为应用程序启用以下安全限制。



- 限制剪贴板访问权限：禁用应用程序和系统剪贴板之间的剪切/复制/粘贴操作。
- 限制打印：禁用在 Citrix Enterprise Browser 中打印的功能。
- 限制下载：禁用用户从应用程序内下载的功能。
- 限制上载：禁用用户在应用程序内上载的权限。
- 显示水印：在用户屏幕上显示水印，显示用户计算机的用户名和 IP 地址。
- 限制按键记录：防范按键记录器。当用户尝试使用用户名和密码登录应用程序时，所有密钥都会在密钥记录器上加密。此外，用户在应用程序上执行的所有活动都受到密钥记录的保护。例如，如果为 Office 365 启用了 App Protection 策略，并且用户编辑 Office 365 Word 文档，则所有按键记录器上的按键都经过加密。

- 限制屏幕截图：禁用使用任何屏幕捕获程序或应用程序捕获屏幕的功能。如果用户尝试捕获屏幕，则会捕获一个空白屏幕。
- 在远程浏览器中打开：在 Citrix Remote Browser 中打开应用程序。
  - 如果选择“在远程浏览器中打开”，并且如果缺少“Secure Private Access”的远程浏览器目录，则会显示以下消息：

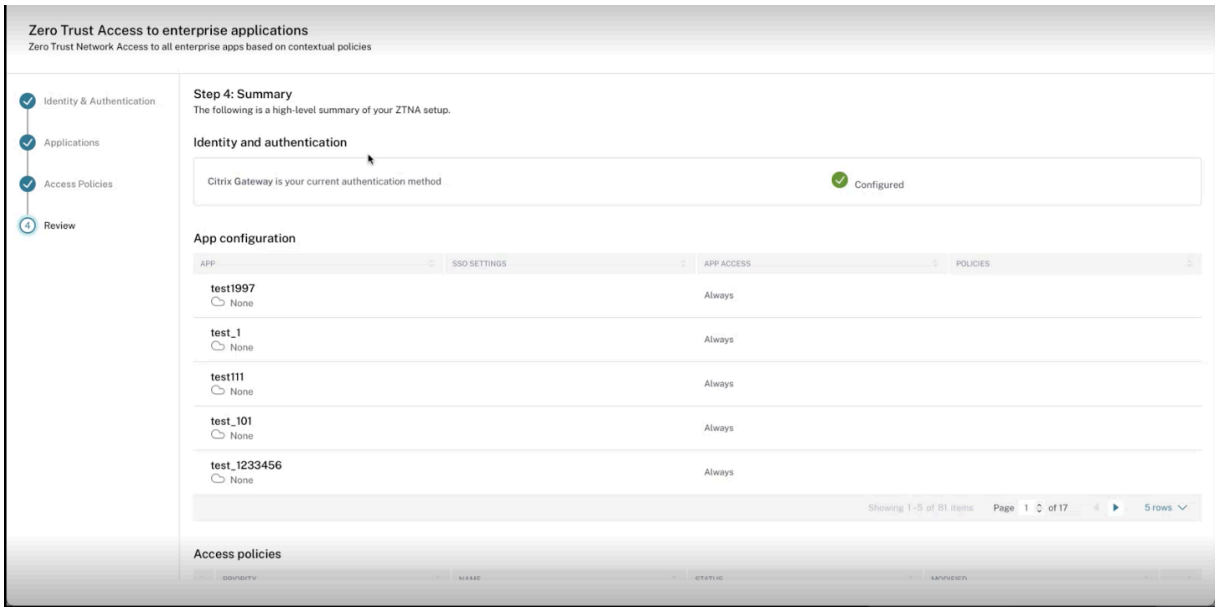
    没有可供托管此应用程序的已发布远程隔离目录。转到 *Remote Browser Isolation* 控制台发布目录。
  - 此外，当您尝试启动 Web 或 SaaS 应用程序时，如果缺少 RBI 目录并且出现以下消息，则应用程序启动将失败：

    尚未创建任何目录来处理此请求。请与您的管理员联系。

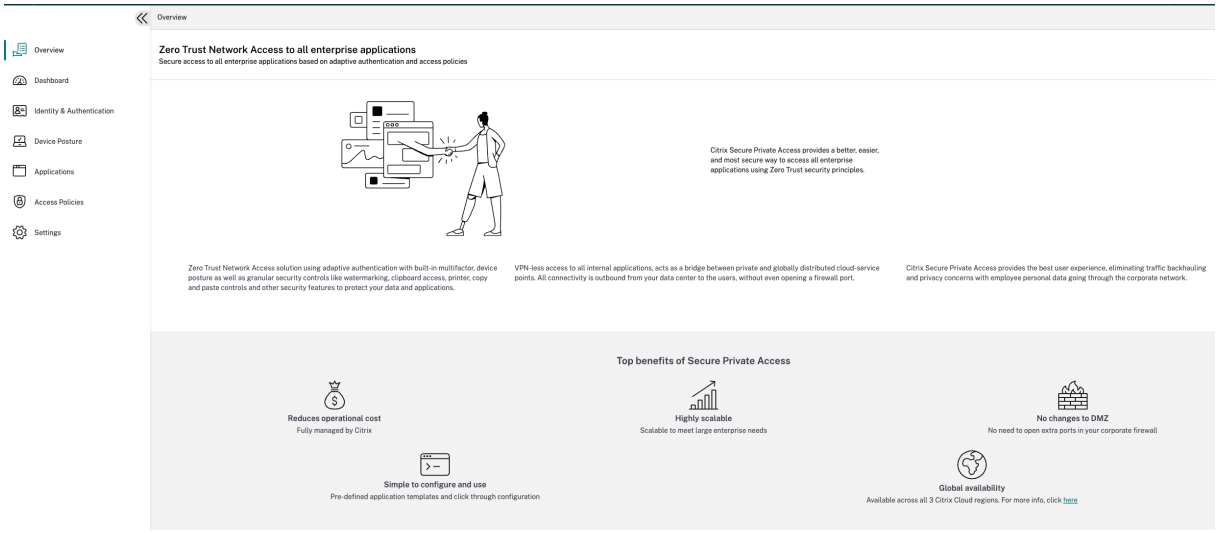
  有关 Citrix Remote Browser Isolation 的更多信息，请参阅 Remote Browser Isolation。

步骤 **4**：查看每种配置的摘要

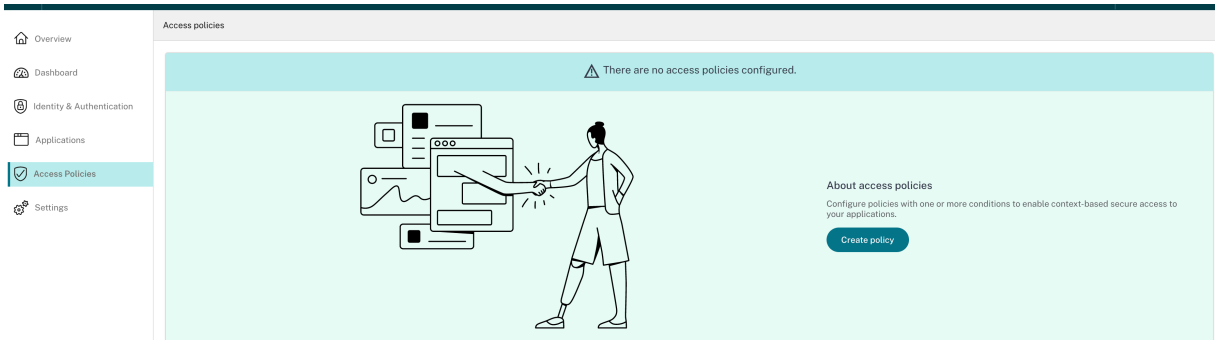
在“审核”页面中，您可以查看完整的应用程序配置，然后单击关闭。



下图显示了完成四步配置后的页面。



> 重要：
>
> - 使用向导完成配置后，您可以直接转到该部分来修改该部分的配置。您不必遵循顺序。
> - 如果您删除了所有已配置的应用程序或策略，则必须重新添加它们。在这种情况下，如果您删除了所有策略，则会显示以下屏幕。



策略建模工具

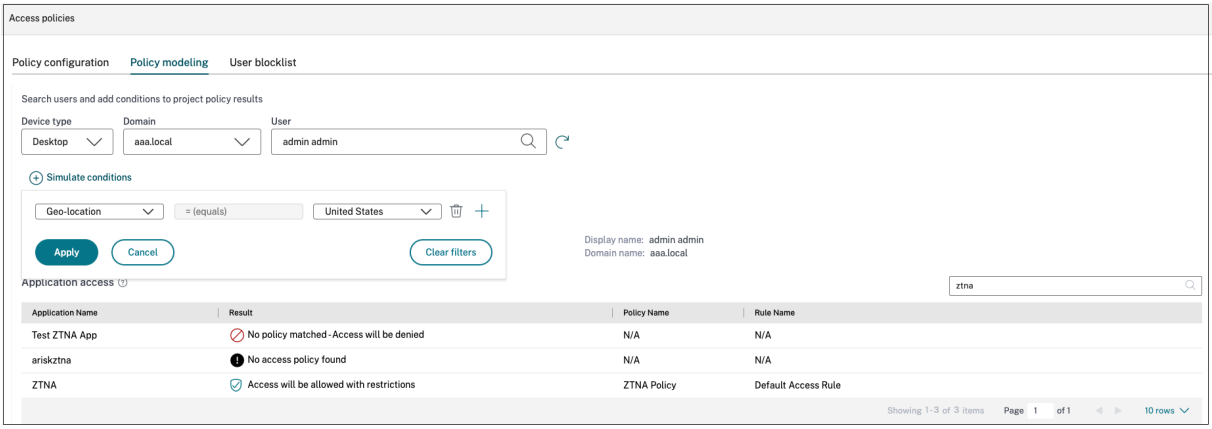
June 19, 2024

管理员可以创建多个策略并将这些策略分配给多个应用程序。因此，管理员可能很难了解其最终用户的应用程序访问结果；也就是说，根据应用程序和访问策略配置允许或拒绝最终用户的访问。策略建模工具（访问策略 **>** 策略建模）通过让管理员完全了解预期的应用程序访问结果（允许/允许但限制/拒绝）来帮助解决这些问题。管理员可以检查特定用户的访问结果，并添加用户条件，例如设备类型、设备状态、地理位置、网络位置、用户风险评分和 Workspace URL。该工具还显示与应用程序相关的策略和规则名称列表。

要分析访问策略配置，请执行以下步骤。

1. 在 Secure Private Access 控制台中，单击“访问策略”，然后单击“策略建模”选项卡。
2. 添加以下详细信息：
    - 设备类型：选择最终用户的设备类型。（默认情况下，桌面处于选中状态。）
    - 域：选择与用户关联的域。
    - 用户：选择要分析应用程序和相关策略的用户名。
3. 您还可以在最终用户及其设备上模拟一组条件/约束。
4. 单击“模拟条件”。
5. 选择条件（设备状态、地理位置、网络位置、用户风险评分和工作区 URL），然后选择关联值。
6. 单击 **+** 号添加其他条件。
7. 单击应用。

所选用户的应用程序、关联策略和规则以表格格式显示。



控制板概述

June 19, 2024

Secure Private Access 服务控制面板显示 SaaS、Web、TCP 和 UDP 应用程序的诊断和使用数据。控制面板让管理员可以在一个地方全面了解其应用程序、用户、连接器运行状况和带宽使用情况，以供使用。这些数据是从 Citrix Analytics 获取的。可以查看预设时间或自定义时间轴的各种实体的数据。对于某些实体，您可以向下钻取以查看更多详细信息。

这些指标大致分为以下几类。

- 记录和故障排除
    - 诊断日志：与身份验证、应用程序启动、应用程序枚举和 Device Posture 检查相关的日志。
- 用户

  - 活跃用户：在所选时间间隔内访问应用程序（SaaS、Web 和 TCP）的唯一用户总数。
  - 上载：在所选时间间隔内通过 Secure Private Access 服务上载的总量数据。
  - 下载量：在所选时间间隔内通过 Secure Private Access 服务下载的数据总量。

- 应用程序：

  - 应用程序：当前配置的应用程序总数（与时间间隔无关）。
  - 应用程序启动次数：在所选时间间隔内每个用户启动的应用程序（应用程序会话）总数。
  - 配置的域：在所选时间间隔内配置的域总数。
  - 已发现的应用程序：已访问但未与任何应用程序关联的唯一单个域名总数

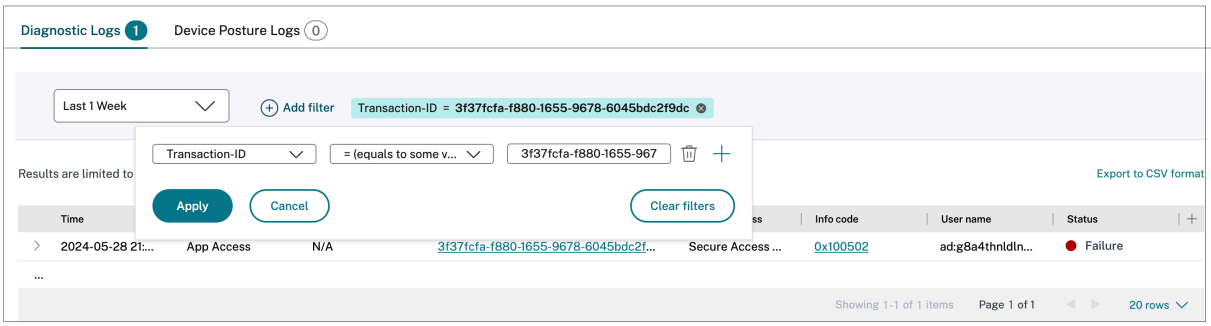
- 访问策略

  - 访问策略：当前配置的访问策略总数（与时间间隔无关）。

诊断日志

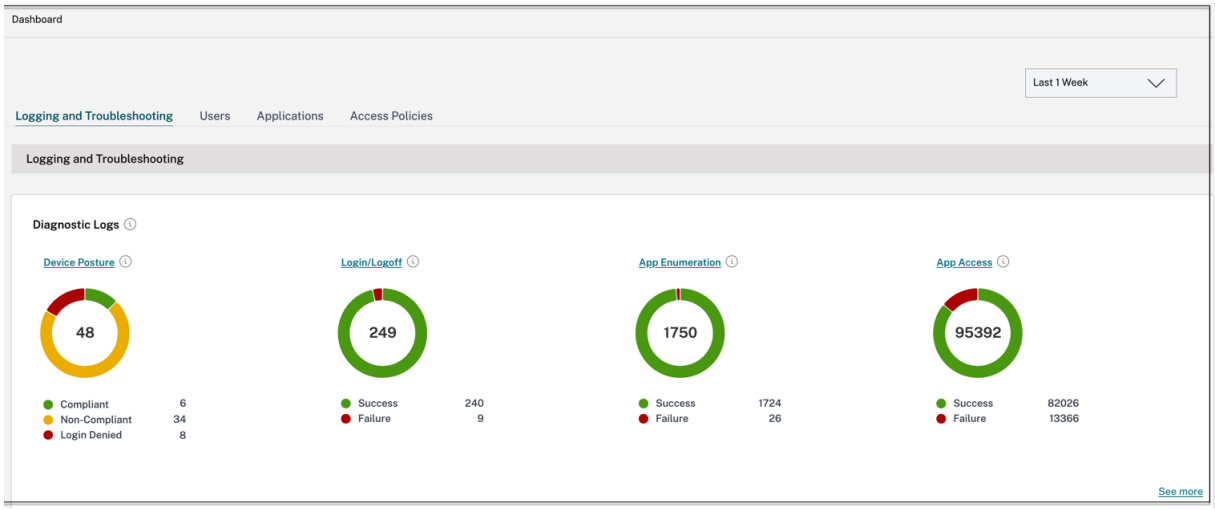
使用诊断日志图表查看与身份验证、应用程序启动、应用程序枚举相关的日志，以及与设备状态相关的日志。您可以单击查看更多链接以查看日志的详细信息。详细信息以表格形式呈现。您可以查看预设时间或自定义时间轴的日志。您可以通过单击 + 符号向图表添加列，具体取决于您要在控制板中看到的信息。您可以将用户日志导出为 CSV 格式。

- 您可以使用“添加过滤器”选项根据应用程序类型、类别、描述等各种条件来细化搜索。例如，在搜索字段中，您可以选择 `Transaction ID`、`=` (`equals to some value`)，并按此顺序输入 `7456c0fb-a60d-4bb9-a2a2-edab8340bb15` 来搜索与该事务 ID 相关的所有日志。有关可与筛选器选项一起使用的搜索运算符的详细信息，请参阅搜索运算符。

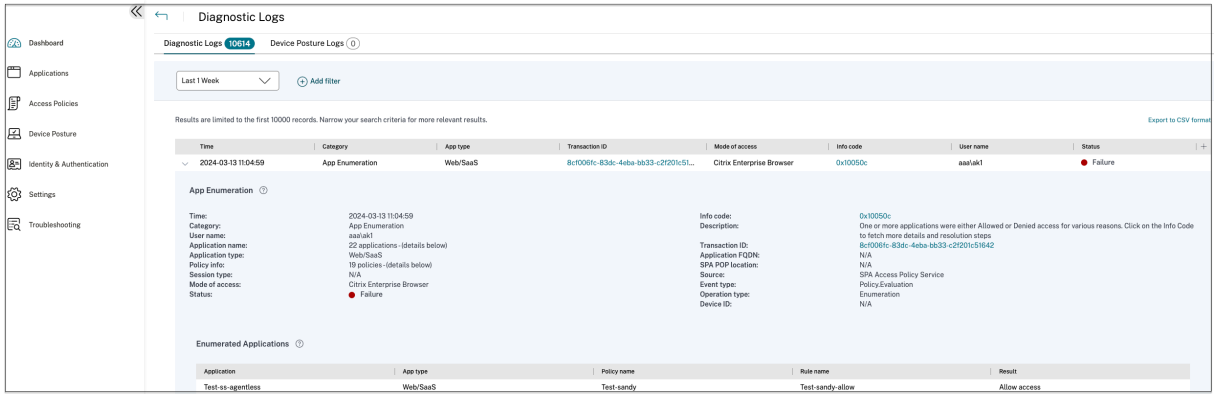


- **Device Posture** 日志：可以根据策略结果（合规、不合规和登录被拒绝）优化搜索。有关 Device Posture 的详细信息，请参阅 Device Posture。

> 注意：
>
> - Secure Private Access 诊断日志控制板中的每个故障事件都有相关的信息代码。有关详细信息，请参阅信息代码。
> - 交易 ID 关联访问请求的所有 Secure Private Access 日志。有关详细信息，请参阅交易 ID。



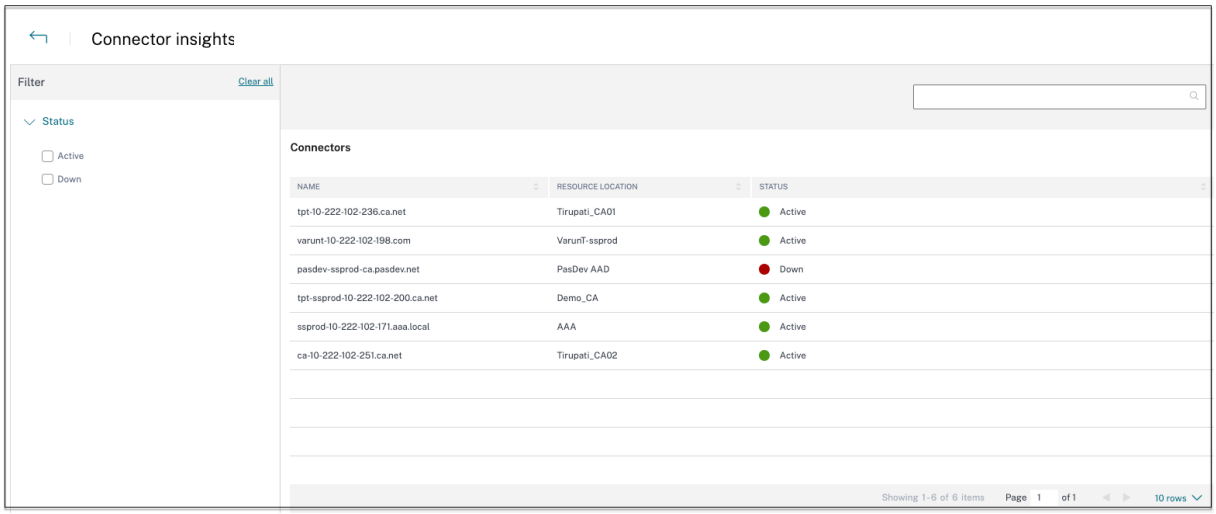
- 您可以单击展开图标 (>) 以查看日志的完整详细信息。
- 诊断日志页面显示访问的每个主要 URL 的嵌入式域。管理员可以通过单击主 URL 中的展开图标 (>) 来查看嵌入式域。管理员可以使用嵌入式域列表来解决与应用程序访问或应用程序呈现相关的问题。例如，如果应用程序配置中遗漏了某个域，则最终用户无法访问特定的应用程序。在这种情况下，管理员可以查看嵌入域列表，识别缺失的域，然后使用缺失的域更新应用程序配置。



> 注意：
>
> - 默认情况下，诊断日志页面显示当周的数据，仅显示最近的 10000 条记录。使用自定义日期搜索和筛选器进一步细化搜索结果。

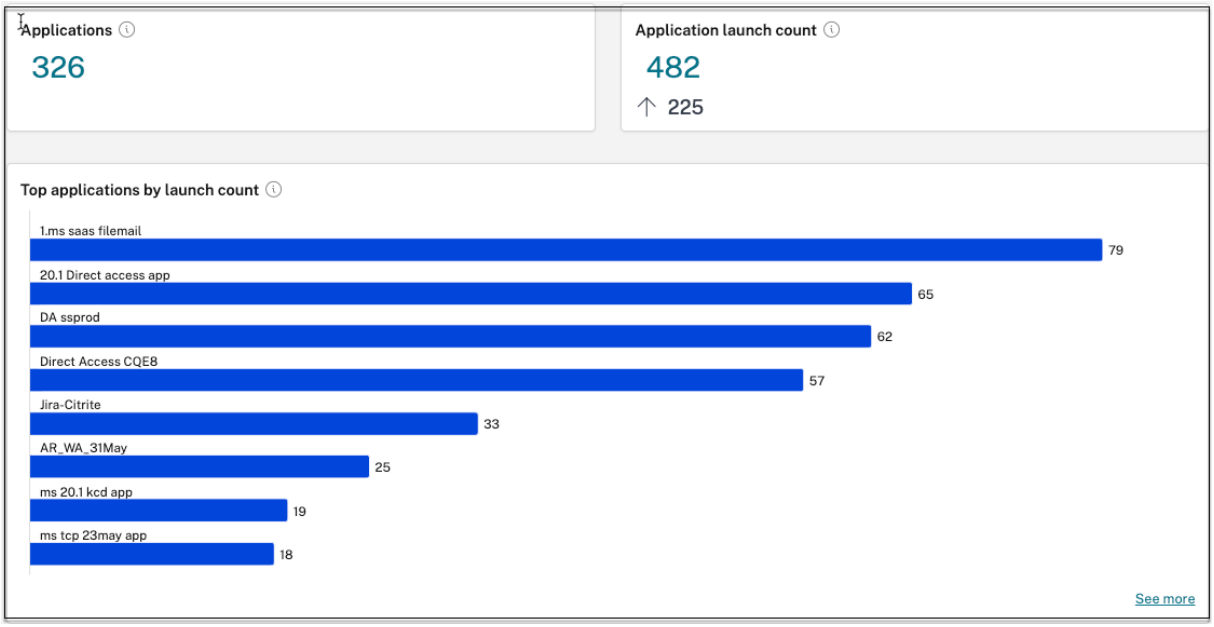
连接器状态

使用 连接器状态 图表可以查看连接器的状态以及部署连接器的资源位置。单击查看更多链接以查看详细信息。在连接器见解页面中，您可以使用过滤器活动或非活动来根据其状态过滤连接器。



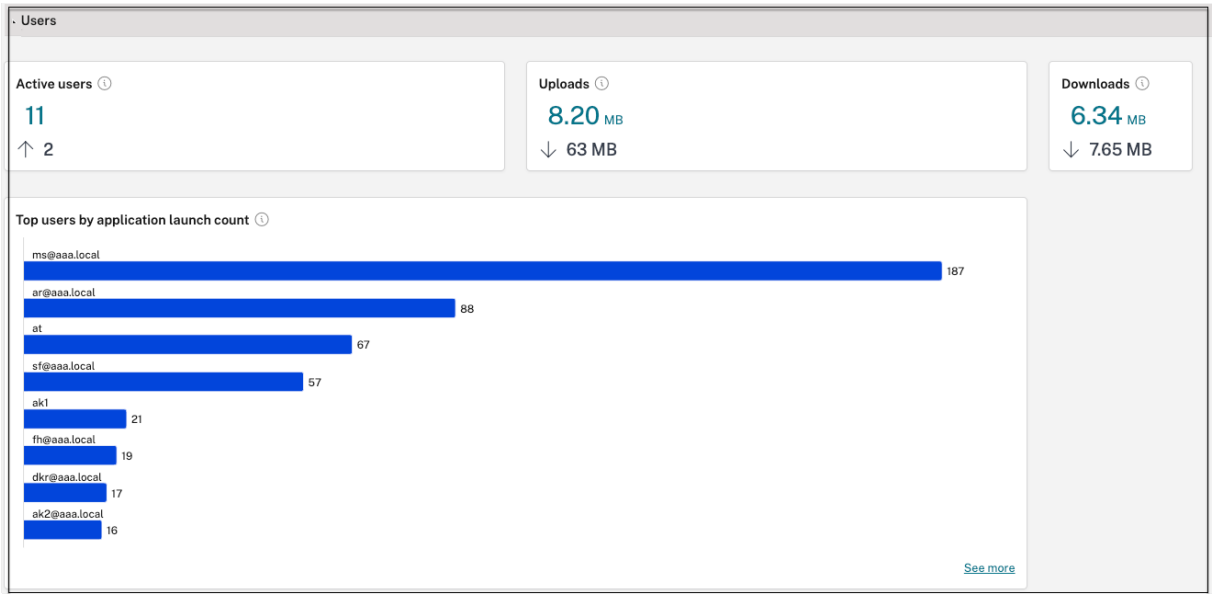
按启动次数排列的热门应用程序

使用 按启动次数 排列的热门应用程序图表根据应用程序的启动次数、上载到应用程序服务器的数据总量以及从应用程序服务器下载的数据总量来查看热门应用程序列表。您可以应用筛选器 **SaaS** 应用程序、**Web** 应用程序或 **TCP/UDP** 应用程序，将搜索范围缩小到特定应用程序。您可以筛选预设时间轴或自定义时间轴的数据。



按应用程序启动次数排列的热门用户

使用 按应用程序排列的热门用户启动次数 图表查看每个用户的数据。例如，用户启动 TCP 应用程序的次数、上载到应用程序服务器的数据总量以及从应用程序服务器下载的数据总量。您可以筛选预设时间轴或自定义时间轴的数据。

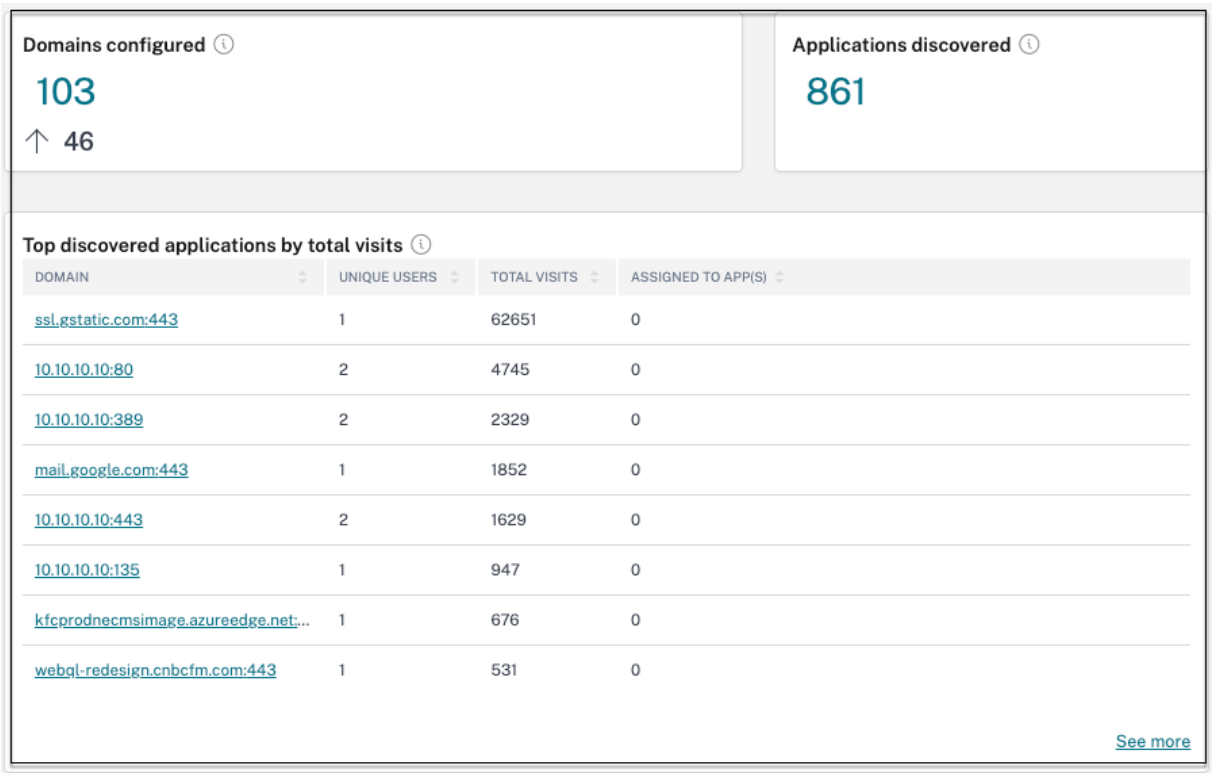


按强制划分的顶级访问策略

使用 按实施排序的顶级访问策略 图表可查看在应用程序上强制实施的访问策略的列表。单击 查看更多 链接可查看与应用程序关联的策略列表以及策略的实施次数。您还可以使用“访问策略”页面中的搜索选项来根据策略名称过滤策略。您还可以使用搜索运算符搜索特定策略，以进一步优化搜索。有关详细信息，请参阅搜索运算符。

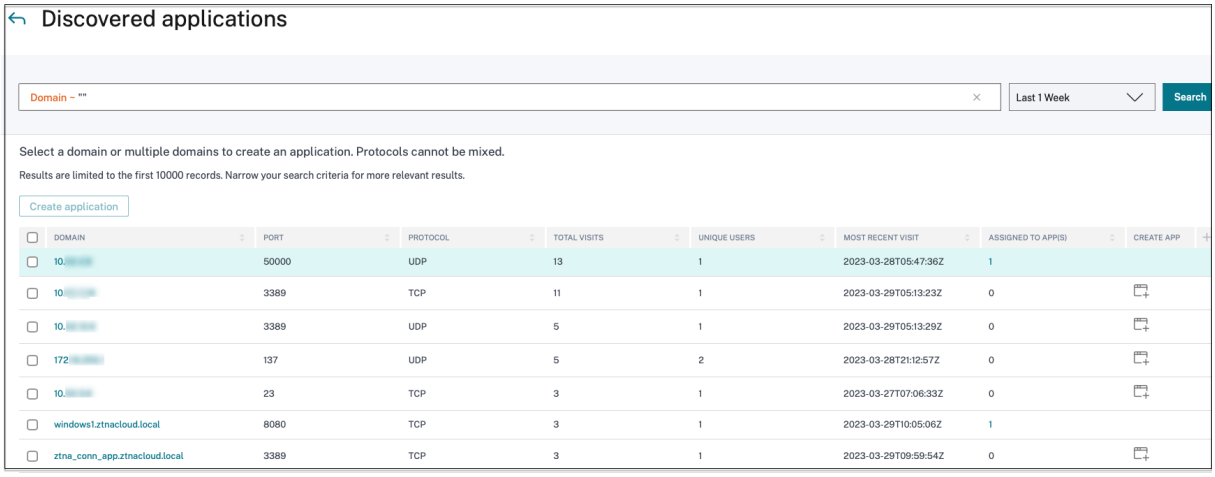
最常发现的应用程序

使用“按总访问量排列的热门已发现应用程序”图表查看在某个时刻曾被访问但未与任何应用程序关联的唯一单个域的列表。这些域是根据这些域的总访问量列出的。管理员可以使用此图表来查看是否有许多用户访问了任何特别感兴趣的域。在这种情况下，管理员可以使用该域创建应用程序，以便于访问。



在图表中，“分配给应用程序”列显示了将此域配置为相关 URL 或目标 URL 值一部分的应用程序总数。单击该数字将显示分配给该域的应用程序。

您可以单击“查看更多”链接以查看有关所有域的更多详细信息。



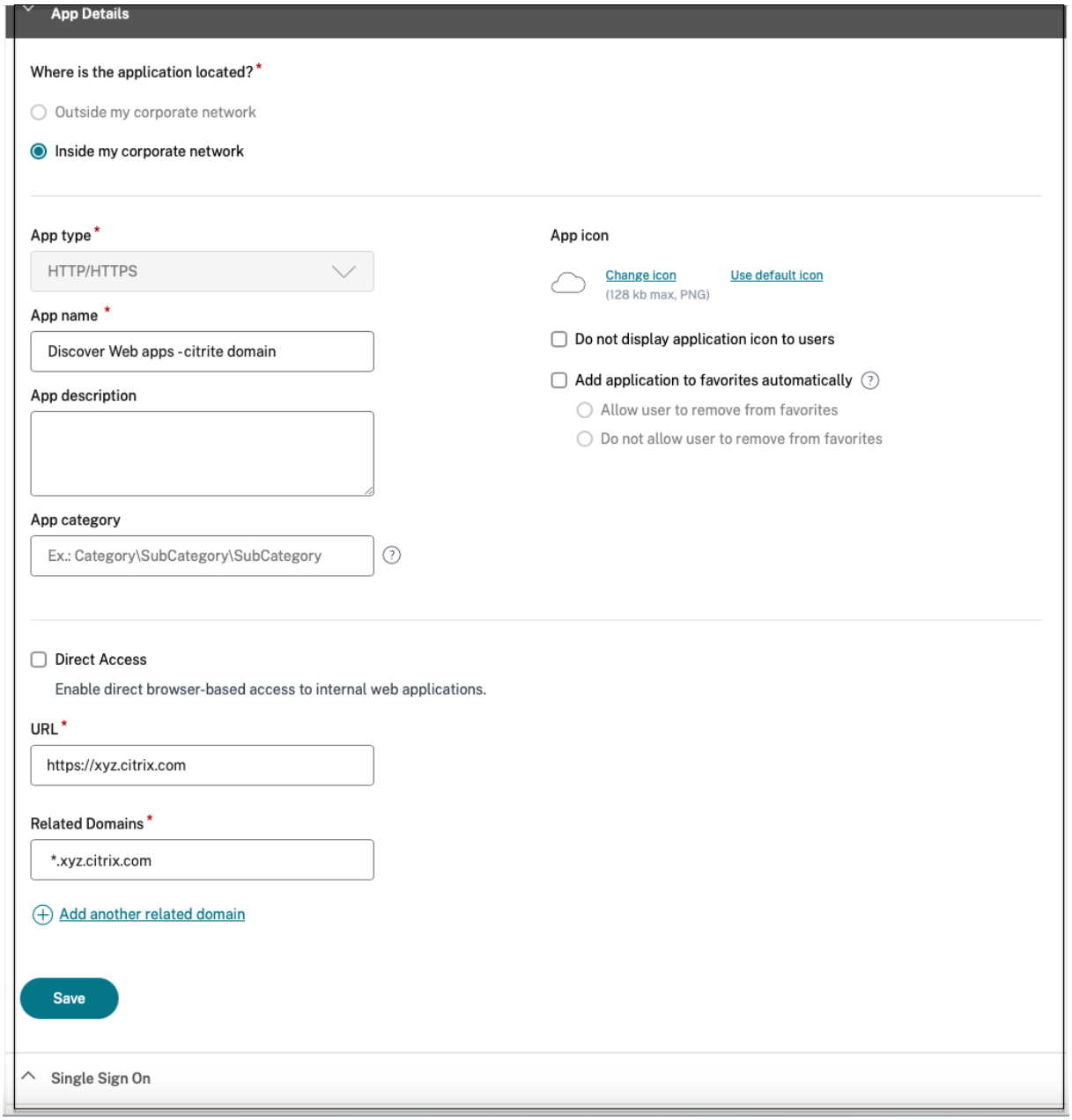
已发现的应用程序页面显示域的详细信息，例如域名、端口、协议、总访问量、唯一用户和最近访问日期。图表中的所有列都是可排序的。您可以使用搜索栏根据域进行搜索。

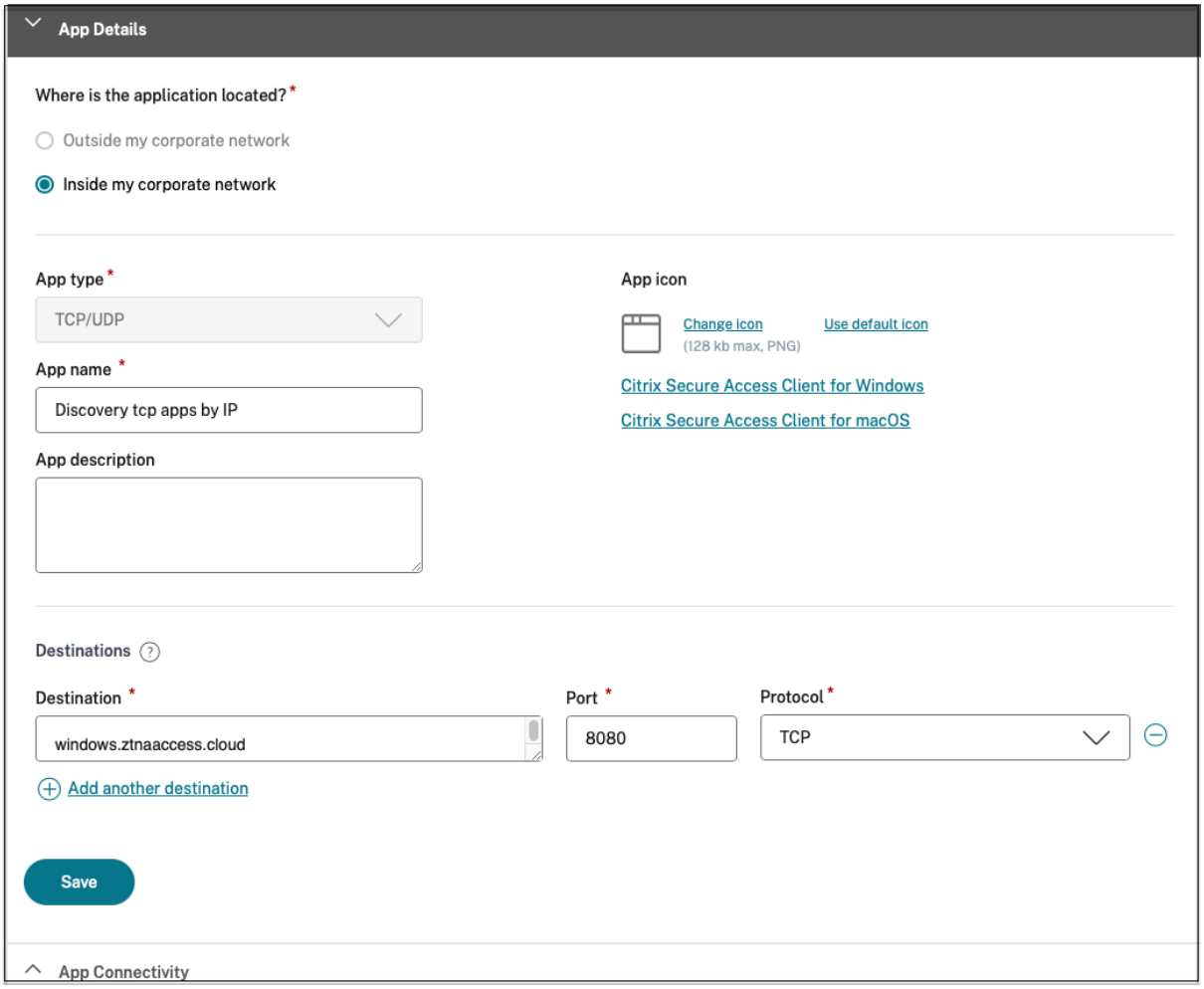
> 注意：
>
> - 这些协议是根据客户使用的标准端口派生的。
> - 已发现域的列表限制为 10000 条记录。

从图表中创建应用程序

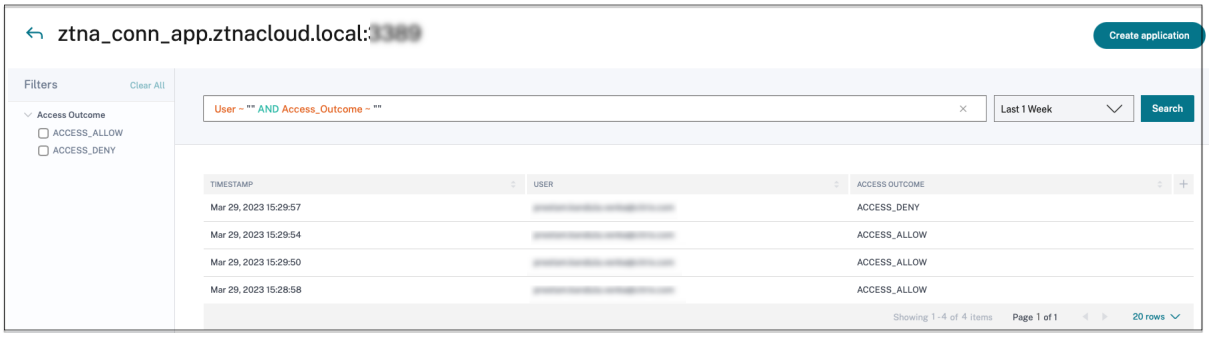
单击与相应域对应的 **+** 图标以创建应用程序。应用程序配置向导弹出。对于已经使用相同的域、端口和协议组合创建应用程序且处于完成状态的行，则不会出现创建应用程序图标。

- 应用程序类型会根据您选择的应用程序协议自动填充。但是，如有必要，您可以更改类型。
- **URL**、相关域、目标、端口、协议 字段中的值都是自动填充的。完成添加应用程序的步骤。有关详细信息，请参阅 管理员指导的工作流程，以便于入门和设置。





您也可以单击唯一域链接以查看更多详细信息并为该域创建应用程序。当您单击域链接时，将显示该域的用户身份验证日志。单击“创建应用程序”按钮。完成添加应用程序的步骤。



搜索运算符

以下是可用于细化搜索的搜索运算符：

- **=**（等于某个值）：搜索与搜索条件完全匹配的日志/策略。

- **!=**（不等于某个值）：搜索不包含指定条件的日志/策略。
- **~**（包含一些值）：搜索与搜索条件部分匹配的日志/策略。
- **!~**（不包含某些值）：搜索不包含某些指定条件的日志/策略。

应用程序发现

January 9, 2024

应用程序发现功能可帮助管理员查看其组织中的内部私有应用程序，例如 Web 应用程序和客户端服务器应用程序（基于 TCP 和 UDP 的应用程序）以及访问这些应用程序的用户。管理员可以通过指定域（通配符域）或 IP 子网的范围来发现应用程序。要在 Citrix Secure Private Access 服务中启用应用程序发现功能，管理员必须配置子网或通配符域，或同时配置两者，需要在这些子网或通配符域中发现和报告应用程序和用户访问权限。管理员使用应用程序配置工作流程来定义广泛的子网和通配符域，并完成与所有应用程序定义配置相同的应用程序访问策略工作流程。

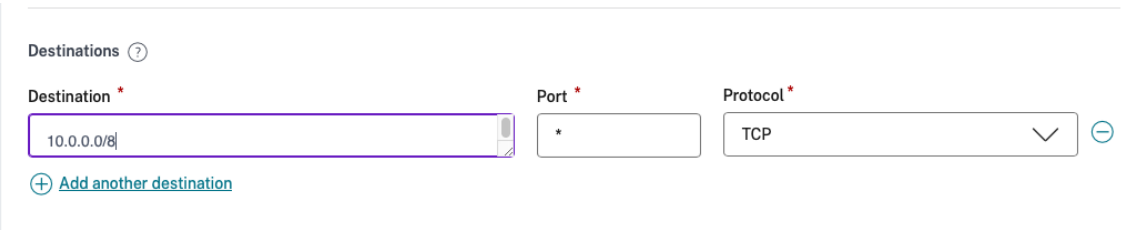
配置应用程序发现

应用程序发现可以通过以下方式之一完成：

- 将系统配置为监视和报告基于 TCP/UDP 的确切 IP 地址目的地和端口。

  指定子网以及 TCP/UDP 协议和端口范围（输入 * 以包括整个范围）。这样可以从安全访问代理发现所有 TCP 和 UDP 应用程序。

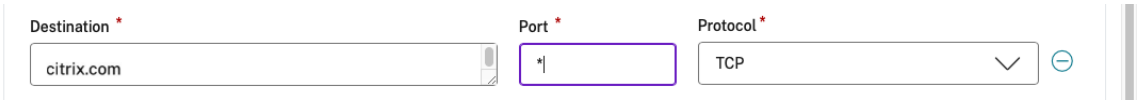
  示例：10.0.0.0/8：TCP：端口 (*)

- 将系统配置为监视和报告使用 TCP 或 UDP 协议访问的应用程序的主机名或完全限定域 (FQDN) 或两者兼而有之。

  指定属于必须监视和报告的 Web 应用程序的通配符域。

  示例：`*.citrix.com : TCP : Port (*)`

- 将系统配置为监视和报告可以从 Citrix Enterprise Browser 访问的完全限定域 (FQDN)。

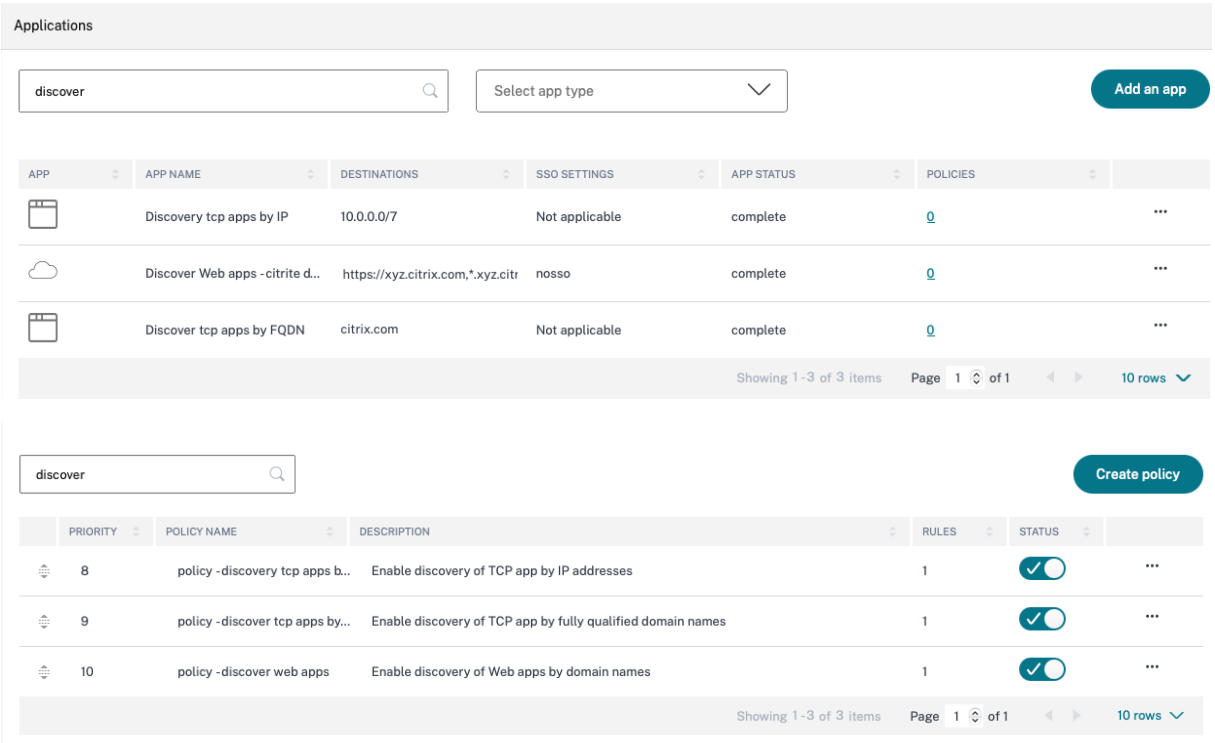
为属于要在其中发现内部 Web 应用程序的域或子域中的 Web 应用程序指定至少一个 FQDN。将相关域配置为包括该应用程序所属的通配符域。

示例：

Web 应用程序 URL：`https://test.citrix.com/`

相关域名：*.citrix.com

> 重要：
>
> - 除了创建应用程序外，您还必须定义允许访问具有已配置域和 IP 子网的应用程序的用户。这是为了防止允许的用户组之外的其他用户组进行未经授权或无意中访问。
> - 在应用程序名称中添加前缀 **Discover**，以表示这是启用发现监视和报告的特殊应用程序配置。此命名可帮助您识别要删除通配符域或 IP 子网或同时删除两者，这样您就可以在几周或一个月后将整个应用程序访问区域缩小到特定的 FQDN 和 IP/端口组合。



创建应用程序和相应的访问策略后，用户可以继续从 Citrix Workspace 应用程序访问应用程序并访问不同的域。要访问 TCP/UDP 应用程序，用户需要使用 Citrix Secure Access 代理。根据应用程序的域和子网配置对来自各种访问方法的应用程序访问进行监视，并在控制板中报告。

应用程序配置和管理

January 9, 2024

使用 Citrix Secure Private Access 服务交付应用程序可为您提供简单、安全、强大且可扩展的解决方案来管理应用程序。在云端交付的应用程序具有以下优势：

- 配置简单 - 易于操作、更新和使用。
- 单点登录—使用单点登录轻松登录。
- 不同 SaaS 应用程序的标准模板-基于模板的流行应用程序配置。这些模板预先填充了配置应用程序所需的大部分信息。仍然必须仅提供特定于买家的信息。

支持企业 **Web** 应用程序

June 19, 2024

通过使用 Secure Private Access 服务交付 Web 应用程序，可以将企业特定应用程序作为基于 Web 的服务进行远程交付。常用的 Web 应用程序包括 SharePoint、Confluence、OneBug 等。

可以使用 Citrix Workspace 使用 Secure Private Access 访问 Web 应用程序。Secure Private Access 服务与 Citrix Workspace 相结合，可为已配置的 Web 应用程序、SaaS 应用程序、已配置的虚拟应用程序或任何其他工作区资源提供统一的用户体验。

SSO 和 Web 应用程序的远程访问可作为以下服务包的一部分提供：

- Secure Private Access Standard
- Secure Private Access Advanced

系统要求

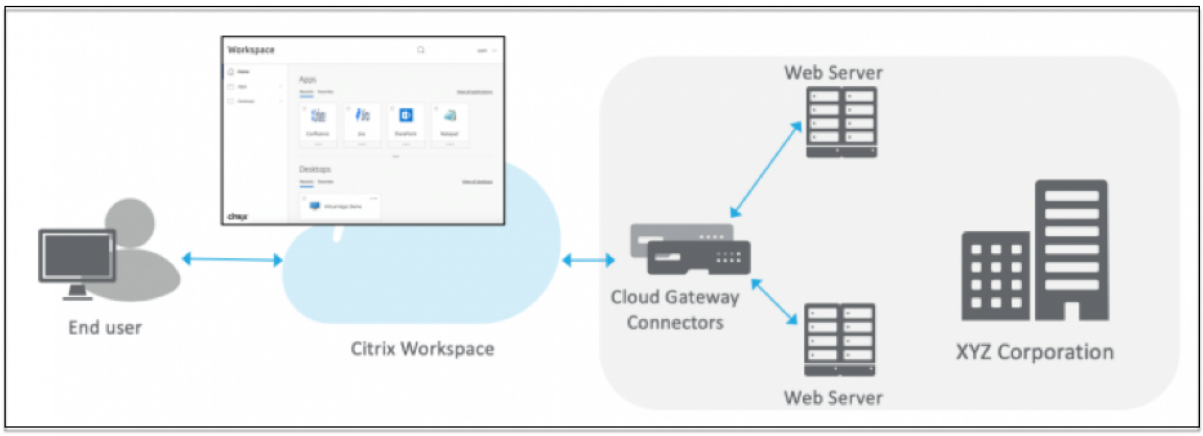
Connector Appliance - 将 Connector Appliance 与 Citrix Secure Private Access 服务结合使用，以支持对客户数据中心中的企业 Web 应用程序进行没有 VPN 的访问。有关详细信息，请参阅使用 Connector Appliance 保护 Workspace 访问的安全。

工作原理

Citrix Secure Private Access 服务使用部署在本地的连接器安全地连接到本地数据中心。此连接器充当本地部署的企业 Web 应用程序与 Citrix Secure Private Access 服务之间的桥梁。这些连接器可以部署在 HA 对中，只需要出站连接。

Connector Appliance 和云中的 Citrix Secure Private Access 服务之间的 TLS 连接可保护枚举到云服务中的本地应用程序。使用无 VPN 的连接通过 Workspace 访问和交付 Web 应用程序。

下图说明了使用 Citrix Workspace 访问 Web 应用程序。



配置 **Web** 应用程序

配置 Web 应用程序涉及以下高级步骤。

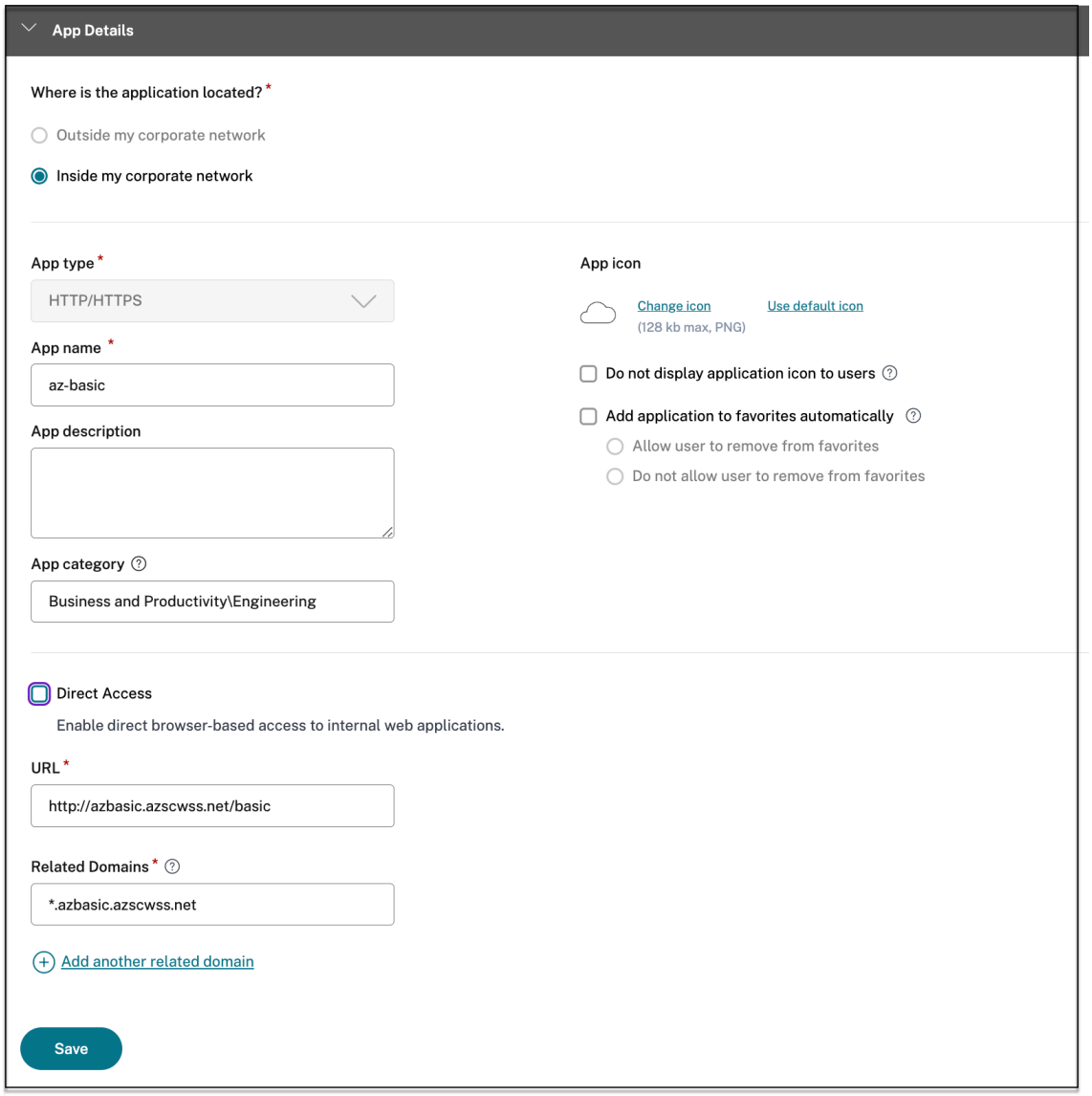
1. 配置应用程序详细信息
2. 设置首选登录方法
3. 定义应用程序路由

配置应用程序详细信息

1. 在“**Secure Private Access**”图块上，单击管理。
2. 在 Secure Private Access 登录页面上，单击继续，然后单击添加应用程序。

   > 注意：
   >
   > 继续按钮仅在您首次使用向导时出现。在后续使用中，您可以直接导航到“应用程序”页面，然后单击“添加应用程序”。

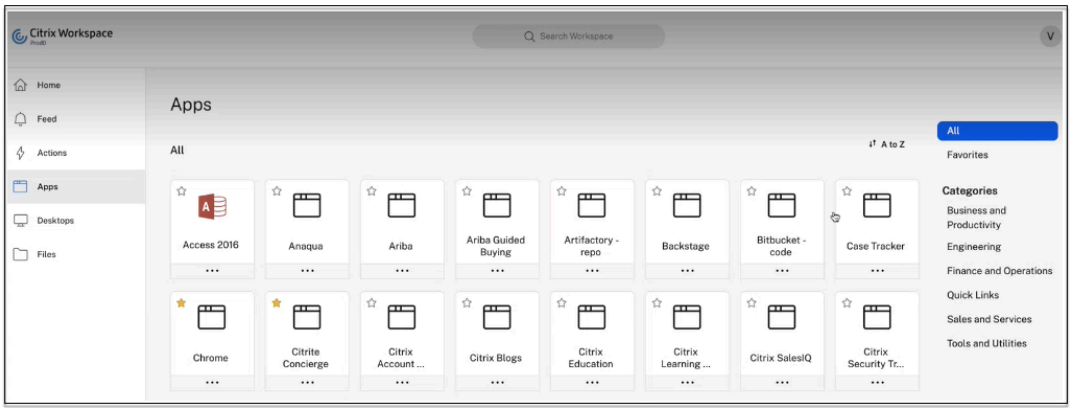
3. 选择要添加的应用程序，然后单击跳过。
4. 在 应用程序位置在哪里？中，选择位置。
5. 在“应用程序详细信息”部分中输入以下详细信息，然后单击下一步。



- 应用程序类型—选择应用程序类型。您可以从 **HTTP/ HTTPS** 或 **UDP/TCP** 应用程序中进行选择。
- 应用程序名称 -应用程序的名称。
- 应用程序描述 - 应用程序的简要描述。您在此处输入的描述将在工作区中显示给您的用户。
- 应用程序类别 - 添加类别和子类别名称（如果适用），您发布的应用程序必须在 Citrix Workspace 用户界面中显示在该类别和子类别下方。您可以为每个应用程序添加新类别，也可以使用 Citrix Workspace 用户界面中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在 Workspace 用户界面中的特定类别下。
  - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
  - 应用程序类别字段适用于 HTTP/HTTPS 应用程序，对于 TCP/UDP 应用程序，则处于隐藏状态。
  - 类别/子类别名称必须用反斜杠分隔。例如，业务与生产力\工程。此外，此字段区分大小写。管理员

必须确保他们定义了正确的类别。如果 Citrix Workspace UI 中的名称与在应用程序类别字段中输入的类别名称不匹配，则该类别将被列为新类别。

例如，如果您在应用程序类别字段中错误地将业务和工作效率类别输入为业务和工作效率类别，则除业务和工作效率类别外，Citrix Workspace UI 中还会列出一个名为业务和工作效率的新类别。



- 应用程序图标—单击更改图标以更改应用程序图标。图标文件大小必须为 128x128 像素。如果不更改图标，则会显示默认图标。

  如果您不想显示应用程序图标，请选择不向用户显示应用程序图标。

- 选择直接访问以允许用户直接从客户端浏览器访问应用程序。有关详细信息，请参阅 直接访问企业 Web 应用程序。

- **URL** —包含您的客户 ID 的 URL。该 URL 必须包含您的客户 ID（Citrix Cloud 客户 ID）。要获取客户 ID，请参阅注册 Citrix Cloud。如果 SSO 失败或您不想使用 SSO，则用户将被重定向到此 URL。

  客户域名 和 客户域 **ID** -客户域名和 ID 用于在 SAML SSO 页面中创建应用程序 URL 和其他后续 URL。

  例如，如果要添加一个 Salesforce 应用程序，则您的域名为 `salesforceformyorg`，ID 为 123754，则应用程序的 URL 为 `https://salesforceformyorg.my.salesforce.com/?so=123754`.

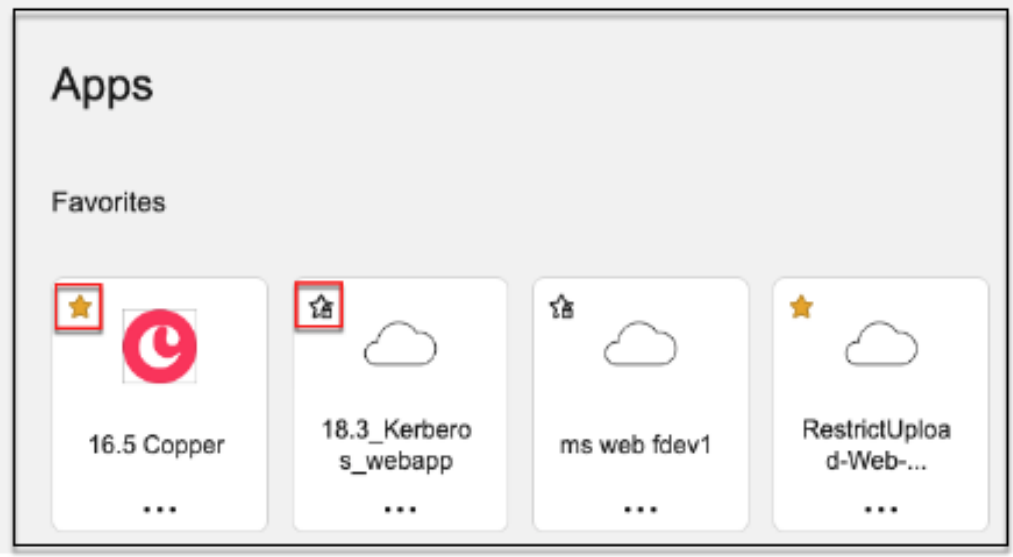
  客户域名和客户 ID 字段特定于某些应用程序。

- 相关域名 - 相关域名将根据您提供的 URL 自动填充。相关域可帮助服务将 URL 识别为应用程序的一部分，并相应地路由流量。您可以添加多个相关域。

- 单击“自动将应用程序添加到收藏夹”，将此应用程序添加为 Citrix Workspace 应用程序中的常用应用程序。

  - 单击“允许用户从收藏夹中删除”，允许应用程序订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。选择此选项时，Citrix Workspace 应用程序中应用程序的左上角会出现一个黄色星形图标。

  - 单击“不允许用户从收藏夹中删除”，以防止订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。选择此选项时，Citrix Workspace 应用程序中应用程序的左上角会出现带有挂锁的星形图标。



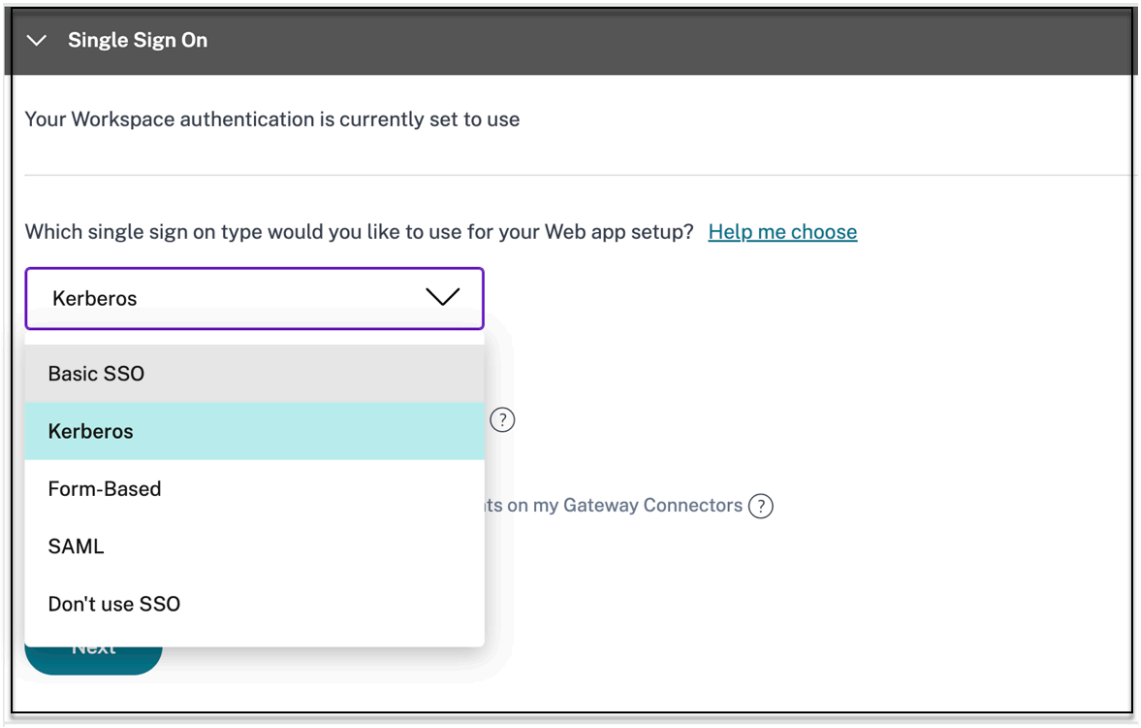
如果您从 Secure Private Access 服务控制台中删除标记为收藏夹的应用程序，则必须从 Citrix Workspace 的收藏夹列表中手动删除这些应用程序。如果从 Secure Private Access 服务控制台中删除这些应用程序，则不会自动从 Workspace 应用程序中删除。

6. 单击“下一步”。

> 重要：
>
> - 要启用基于零信任的应用程序访问权限，默认情况下会拒绝应用程序的访问权限。只有当访问策略与应用程序关联时，才会启用对应用程序的访问权限。有关创建访问策略的详细信息，请参阅创建访问策略。
> - 如果使用相同的 FQDN 或通配符 FQDN 的某些变体配置多个应用程序，则可能会导致配置冲突。为防止配置冲突，请参阅 Web 和 SaaS 应用程序配置的最佳实践。

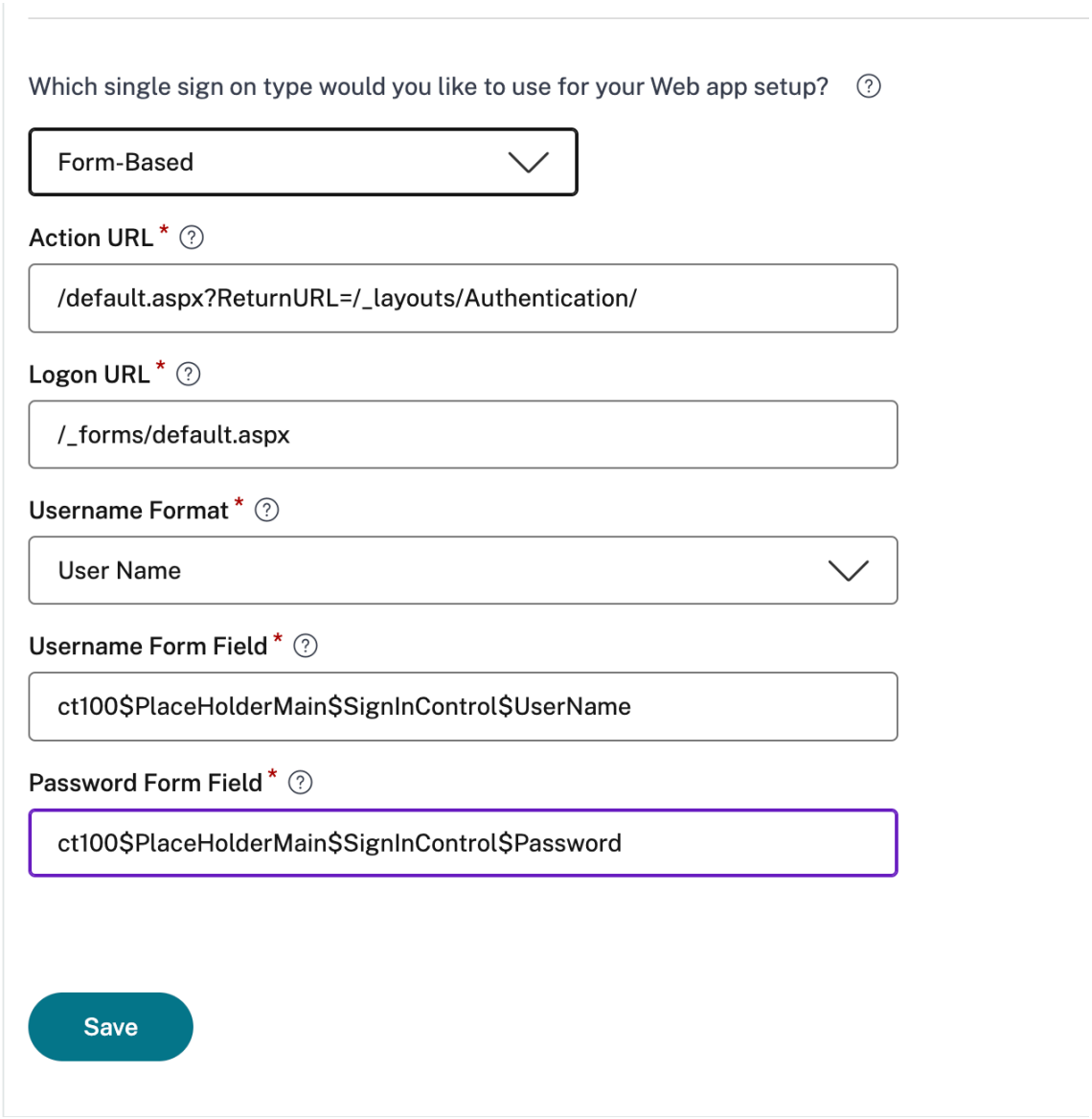
设置首选登录方法

1. 在“单点登录”部分中，选择要用于应用程序的首选单点登录类型，然后单击“保存”。可以使用以下单点登录类型。



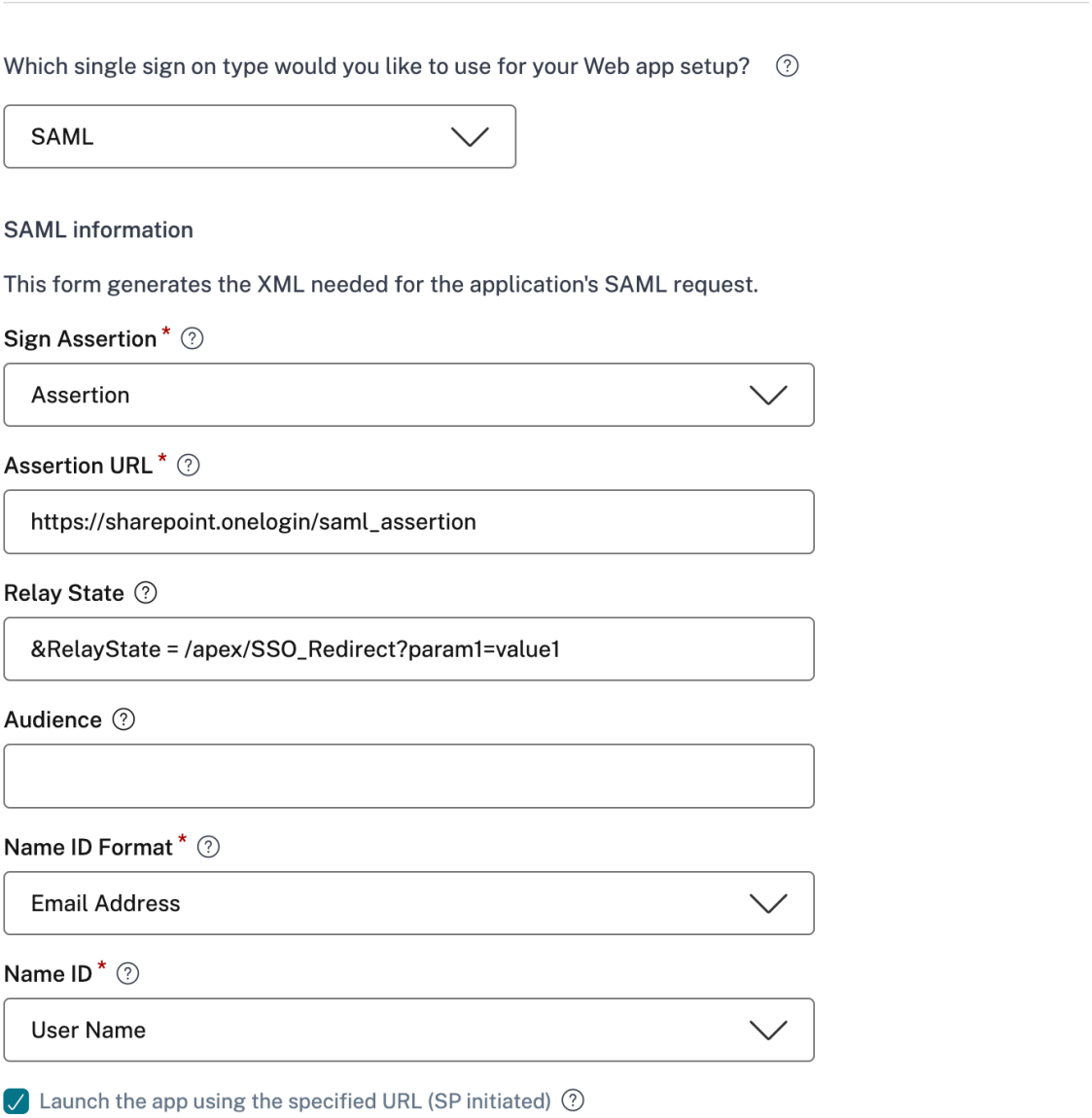
- 基本—如果您的后端服务器向您提出 basic-401 挑战，请选择 基本 **SSO**。您无需为基本 SSO 类型提供任何配置详细信息。
- **Kerberos** —如果您的后端服务器向您提供了协商 401 挑战，请选择 **Kerberos**。您无需为 **Kerberos** SSO 类型提供任何配置详细信息。
- 基于表 单—如果后端服务器向您提供用于身份验证的 HTML 表单，请选择 基于表单。输入基于表单的 SSO 类型的配置详细信息。
- **SAML** -为基于 **SAML** 的 SSO 选择 SAML 进入 Web 应用程序。输入 **SAML** SSO 类型的配置详细信息。
- 不使用 **SSO** —当您 不需要对后端服务器上的用户进行身份验证时，请使用不使用 **SSO** 选项。选择不使用 **SSO** 选项时，用户将被重定向到在应用程序详细信息部分下配置的 URL。

基于表单的详细信息：在“单点登录”部分中输入以下基于表单的配置详细信息，然后单击“保存”。



- 操作 **URL** -键入要向其提交完成的表单的 URL。
- 登录表单 **URL** —键入显示登录表单的 URL。
- 用户名格式 -选择用户名的格式。
- 用户名表单字段—键入用户名属性。
- 密码表单字段—键入密码属性。

SAML：在“单点登录”部分中输入以下详细信息，然后单击“保存”。



- 签名断言 -签名断言或响应可确保在将响应或断言传递给信赖方 (SP) 时消息的完整性。您可以选择断言、响应、两者或无。
- 断言 **URL** —断言 URL 由应用程序供应商提供。SAML 断言被发送到此 URL。
- 中继状态 - 中继状态参数用于识别用户登录并定向到依赖方的联合服务器后访问的特定资源。中继状态为用户生成单个 URL。用户可以单击此 URL 登录到目标应用程序。
- 受众—受众由应用程序供应商提供。此值确认为正确的应用程序生成了 SAML 断言。
- 名称 **ID** 格式—选择支持的名称标识符格式。
- 名称 **ID** —选择支持的名称 ID。

2. 在 高级属性（可选）中，添加有关用户的其他信息，这些信息将被发送到应用程序以做出访问控制决策。

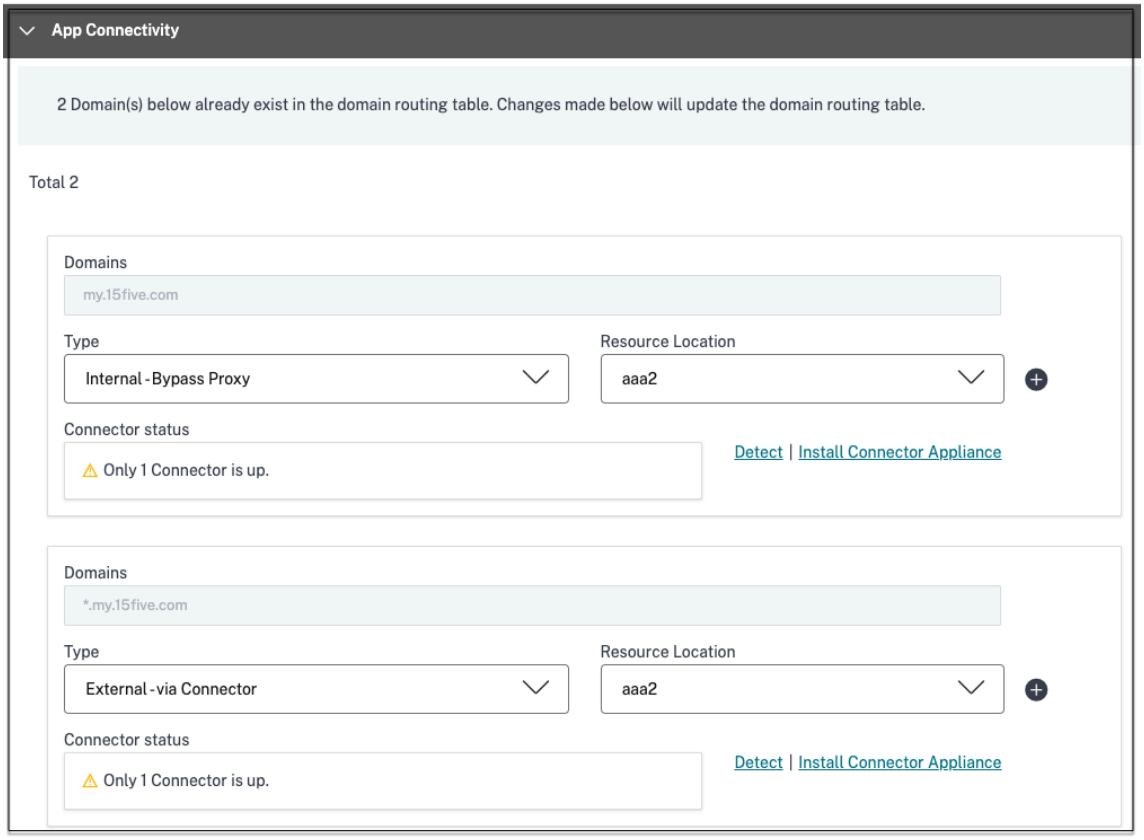
3. 单击 **SAML** 元数据下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用服务器上配置 SSO。

   > 注意：
   >
   > - 您可以复制登录 URL 下的 SSO 登录 **URL**，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
   > - 您还可以从证书列表中下载 证书，并在 SaaS 应用服务器上配置 SSO 时使用该证书。

4. 单击“下一步”。

定义应用程序路由

1. 在“应用程序连接”部分中，如果域必须通过 Citrix Connector Appliance 在外部或内部路由，则可以为应用程序的相关域定义路由。有关详细信息，请参阅在 SaaS 和 Web 应用程序中的相关域相同的情况下路由表以解决冲突。

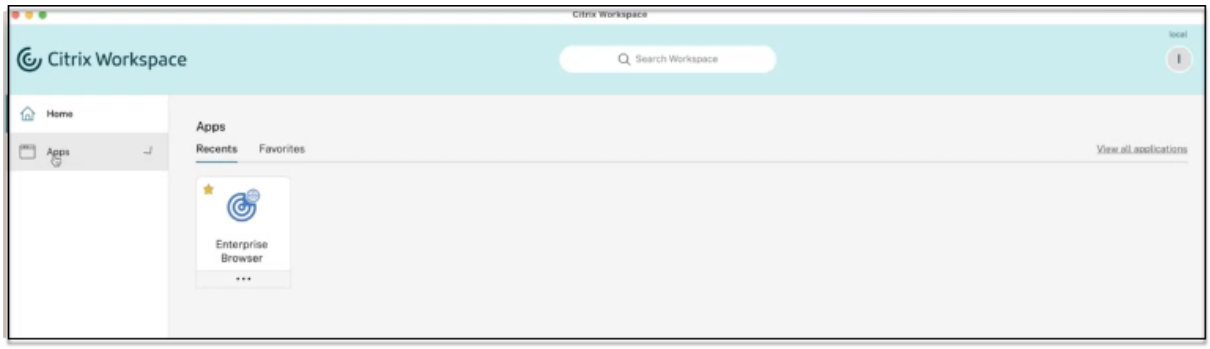


2. 单击“完成”。

   单击完成后，该应用程序将添加到“应用程序”页面。配置应用程序后，您可以从“应用程序”页面编辑或删除该应用程序。为此，请单击应用程序上的省略号按钮，然后相应地选择操作。

   - 编辑应用程序
   - 删除

当您通过 Secure Private Access 服务发布 Web 或 SaaS 应用程序时，如果该应用程序未被隐藏，则 Citrix Enterprise Browser 应用会自动显示在 Citrix Workspace 用户界面中。此外，默认情况下，Citrix Enterprise Browser 也被添加为常用应用程序。最终用户可以在没有 URL 的情况下启动 Workspace Browser，并使用 Workspace Browser 访问内部网站。



> 重要：
>
> - 要向用户授予对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。

适用于 **Secure Private Access** 的 **Connector Appliance**

June 21, 2024

Connector Appliance 是虚拟机管理程序中托管的 Citrix 组件。它充当 Citrix Cloud 与您的资源位置之间的通信渠道，无需任何复杂的网络或基础架构配置即可实现云管理。Connector Appliance 使您能够管理和专注于为用户提供价值的资源。

从 Connector Appliance 到云的所有连接均使用标准 HTTPS 端口 (443) 和 TCP 协议建立。不接受任何传入连接。允许使用以下 FQDN 的 TCP 端口 443 出站：

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

使用 **Connector Appliance** 配置 **Secure Private Access**

1. 在资源位置中安装两个或更多 Connector Appliance。

有关设置 Connector Appliance 的更多信息，请参阅适用于云服务的 Connector Appliance。

2. 要配置 Secure Private Access 以使用 KCD 连接到本地 Web 应用程序，请完成以下步骤来配置 KCD：

   a) 将 Connector Appliance 加入到 Active Directory 域。

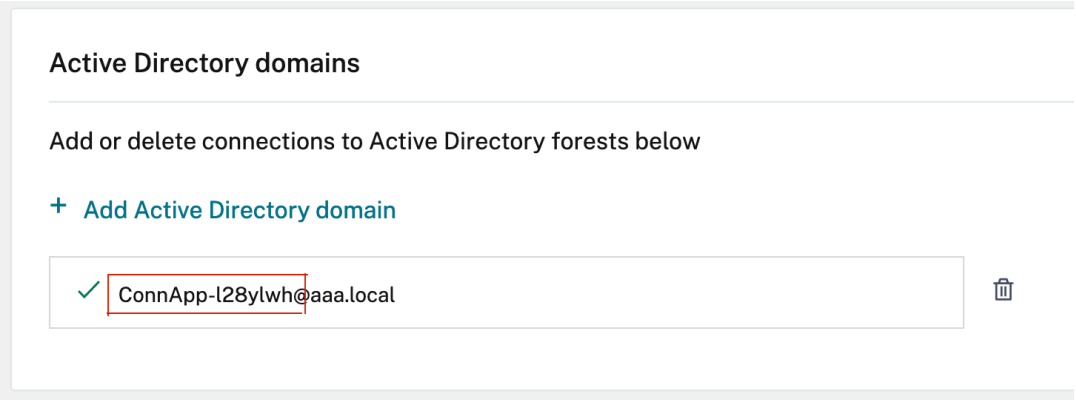
   加入 Active Directory 林后，您可以在配置 Secure Private Access 时使用 Kerberos 约束委派 (KCD)，但它不会启用身份请求或身份验证以使用 Connector Appliance。

   - 使用 Connector Appliance 控制台中提供的 IP 地址连接到浏览器中的 Connector Appliance 管理 Web 页面。
   - 在 **Active Directory** 域名部分，单击 **+** 添加 **Active Directory** 域。

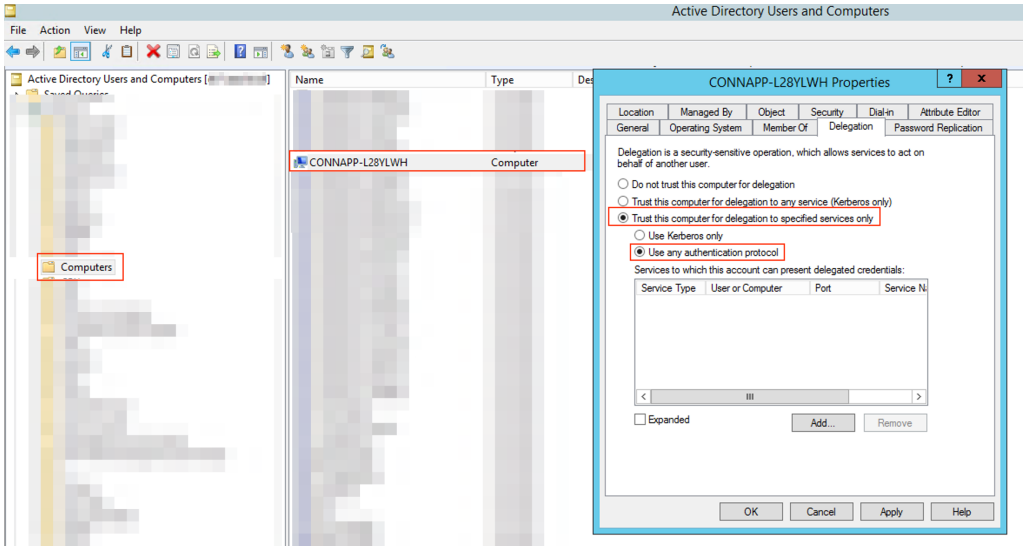
     如果您的管理页面中没有 **Active Directory** 域部分，请联系 Citrix 申请注册预览版。
   - 在“域名”字段中输入 域名。单击添加。
   - Connector Appliance 会检查域。如果检查成功，则会打开“加入 **Active Directory**”对话框。
   - 输入对此域具有加入权限的 Active Directory 用户的用户名和密码。
   - Connector Appliance 会建议计算机名称。您可以选择覆盖建议的名称，并自行提供长度不超过 15 个字符的计算机名称。记下计算机帐户名称。

     此计算机名称是在 Connector Appliance 加入时在 Active Directory 域中创建的。
   - 单击“加入”。

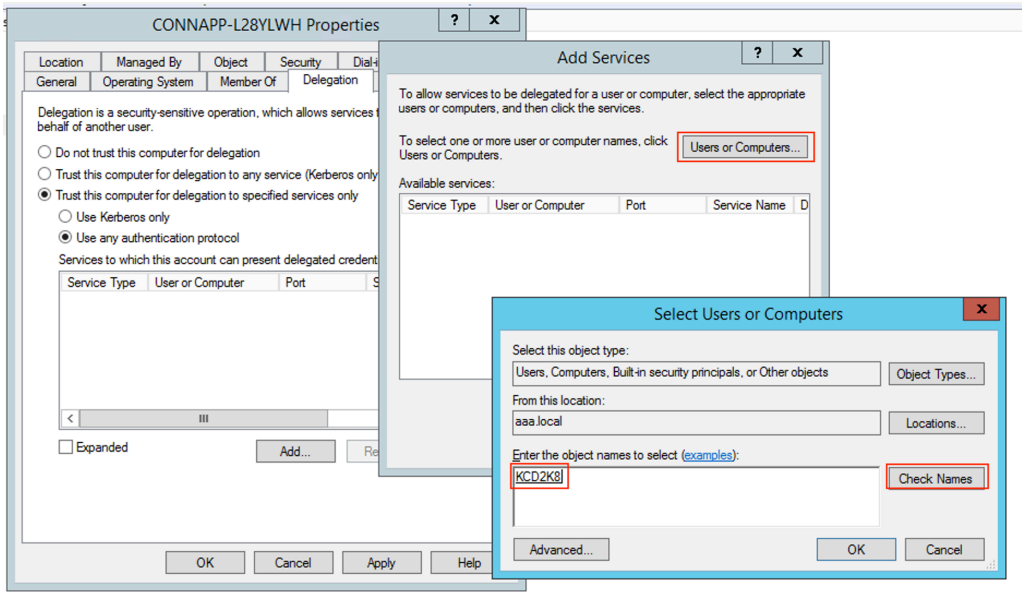
   b) 为没有负载平衡器的 Web 服务器配置 Kerberos 约束委派。



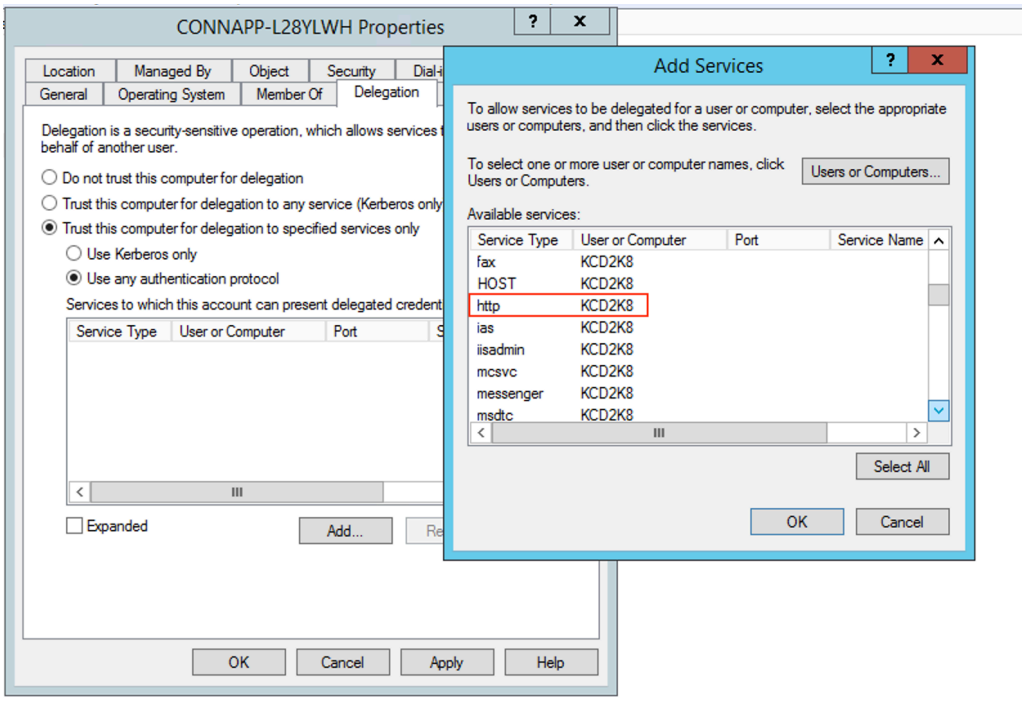
   - 确定连接器装置的计算机名称。您可以从托管位置获取此名称，也可以直接从连接器 UI 中获取此名称。
   - 在 Active Directory 控制器上，查找 Connector Appliance 计算机。
   - 转到 Connector 设备计算机帐户的属性，然后导航到委派选项卡。
   - 选择信任计算机以仅委派给指定的服务。，然后选择 使用任何身份验证协议。



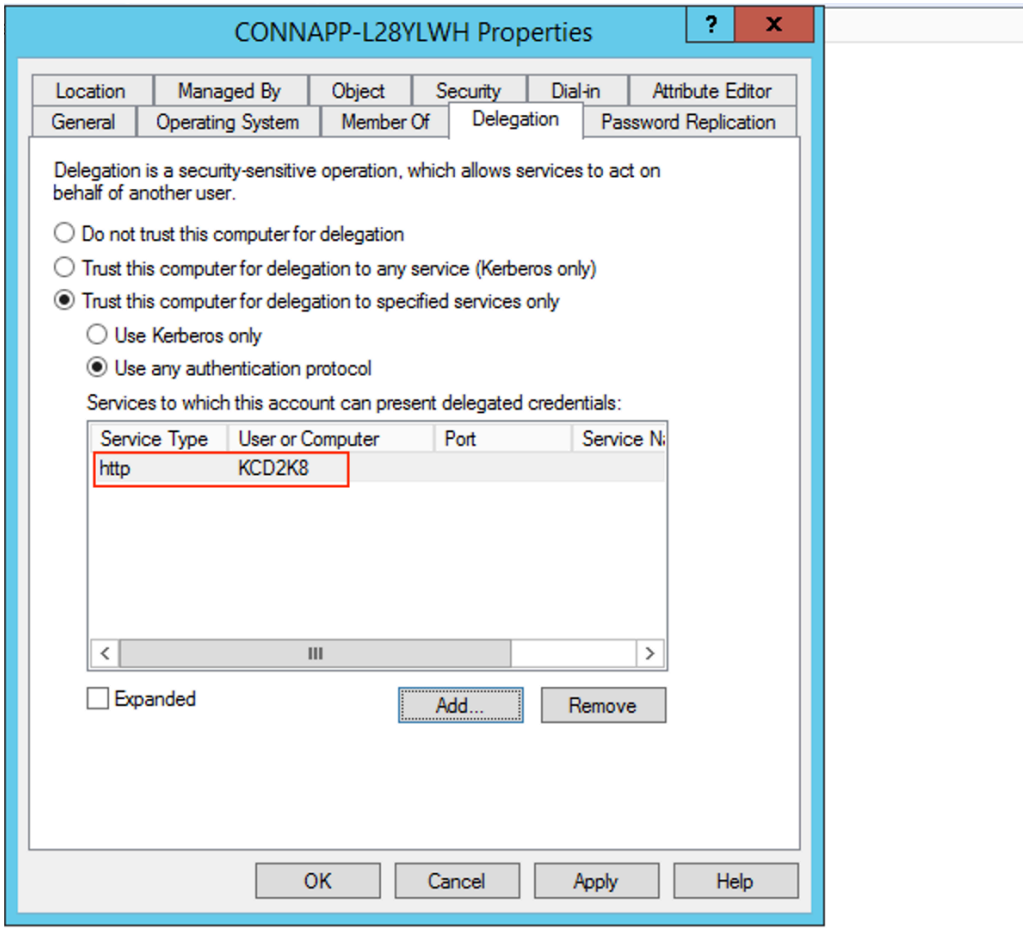
- 单击“添加”。
- 单击用户或 计算机。
- 输入目标 Web 服务器计算机名称，然后单击检查名称。在上图中，**KCD2K8** 是 Web 服务器。



- 单击确定。
- 选择服务类型 **http**。



- 单击确定。
- 单击“应用”，然后单击“确定”。

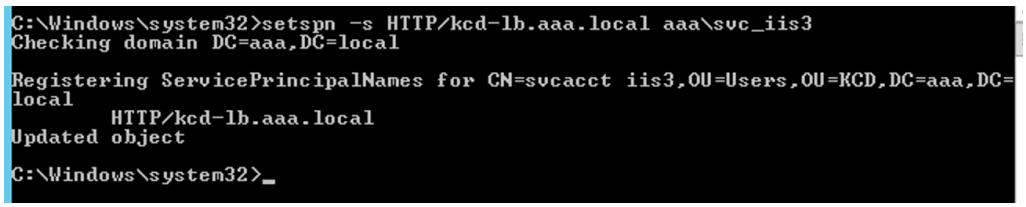


这样就完成了为 Web 服务器添加委派的过程。

c) 为负载平衡器后面的 Web 服务器配置 Kerberos 约束委派 (KCD)。

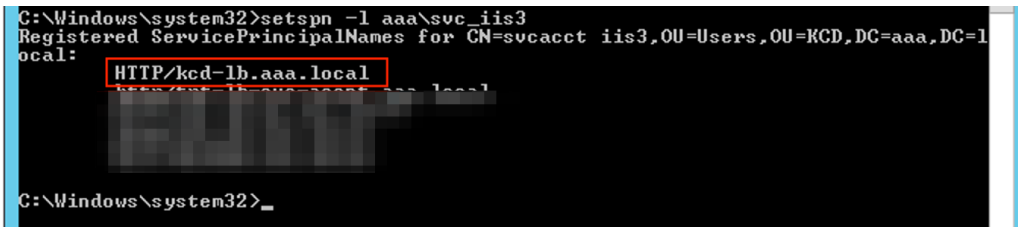
- 使用以下 `setspn` 命令将负载平衡器 SPN 添加到服务帐户。

  `setspn -S HTTP/<web_server_fqdn> <service_account>`

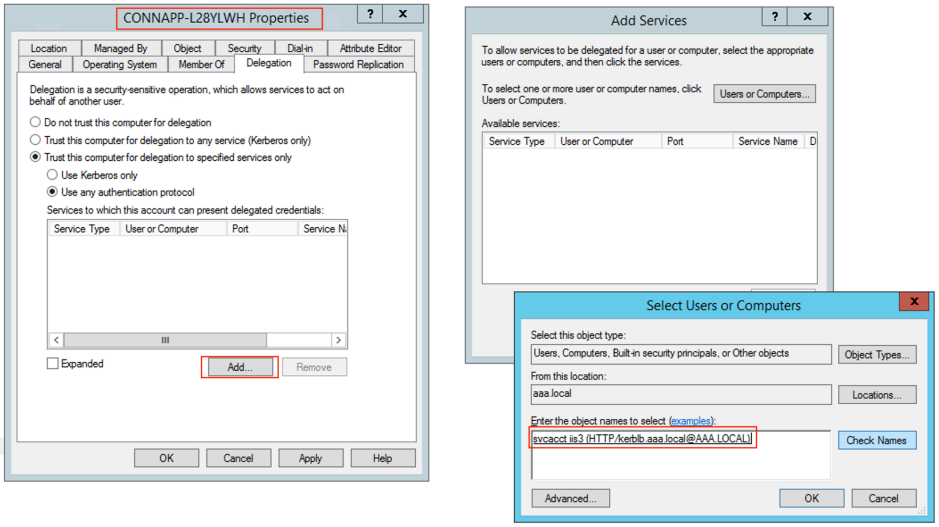


- 使用以下命令确认服务帐户的 SPN。

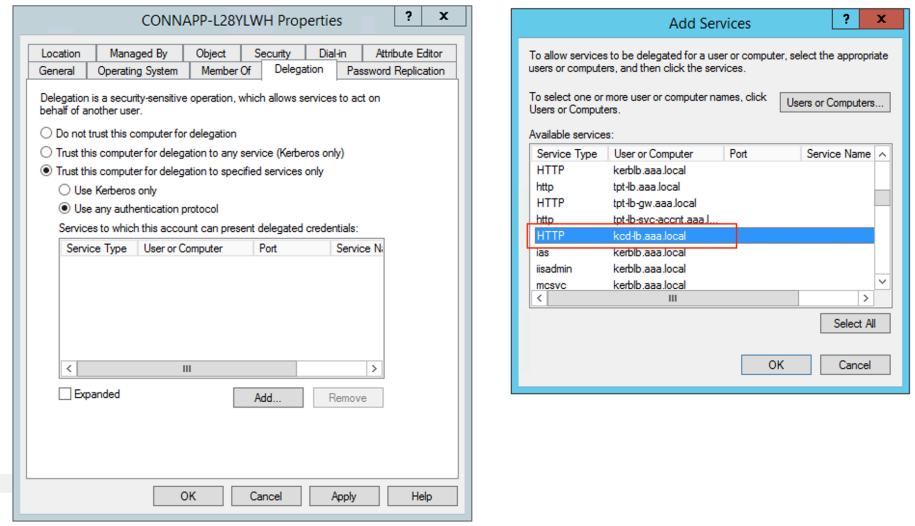
  `setspn -l <service_account>`



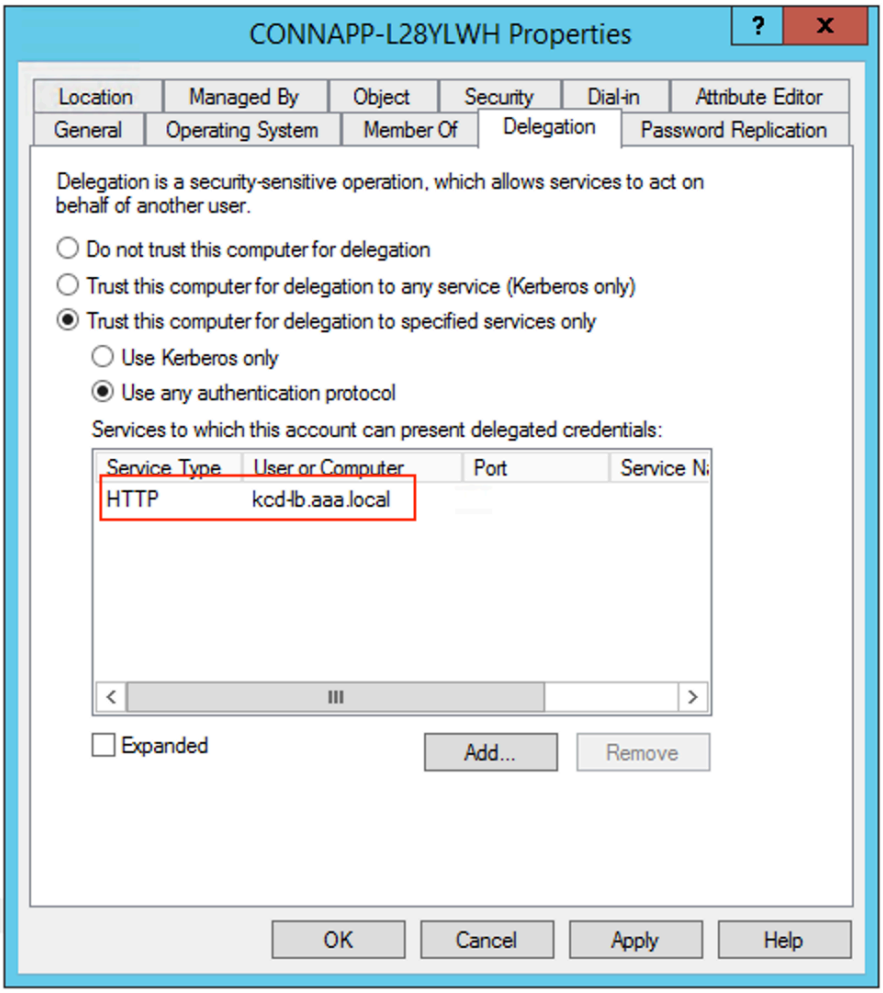
- 为连接器装置计算机帐户创建委派。
  - 按照 为没有负载平衡器的 *Web* 服务器配置 *Kerberos* 约束委派 的步骤来标识 CA 计算机并导航到委派 UI。
  - 在选择用户和计算机中，选择服务帐户（例如 aaa\svc_iis3）。



  - 在服务中，选择条目 **ServiceType: HTTP** 和用户或计算机：Web 服务器（例如，`kcd-lb.aaa.local`）



  - 单击确定。
  - 单击“应用”，然后单击“确定”。

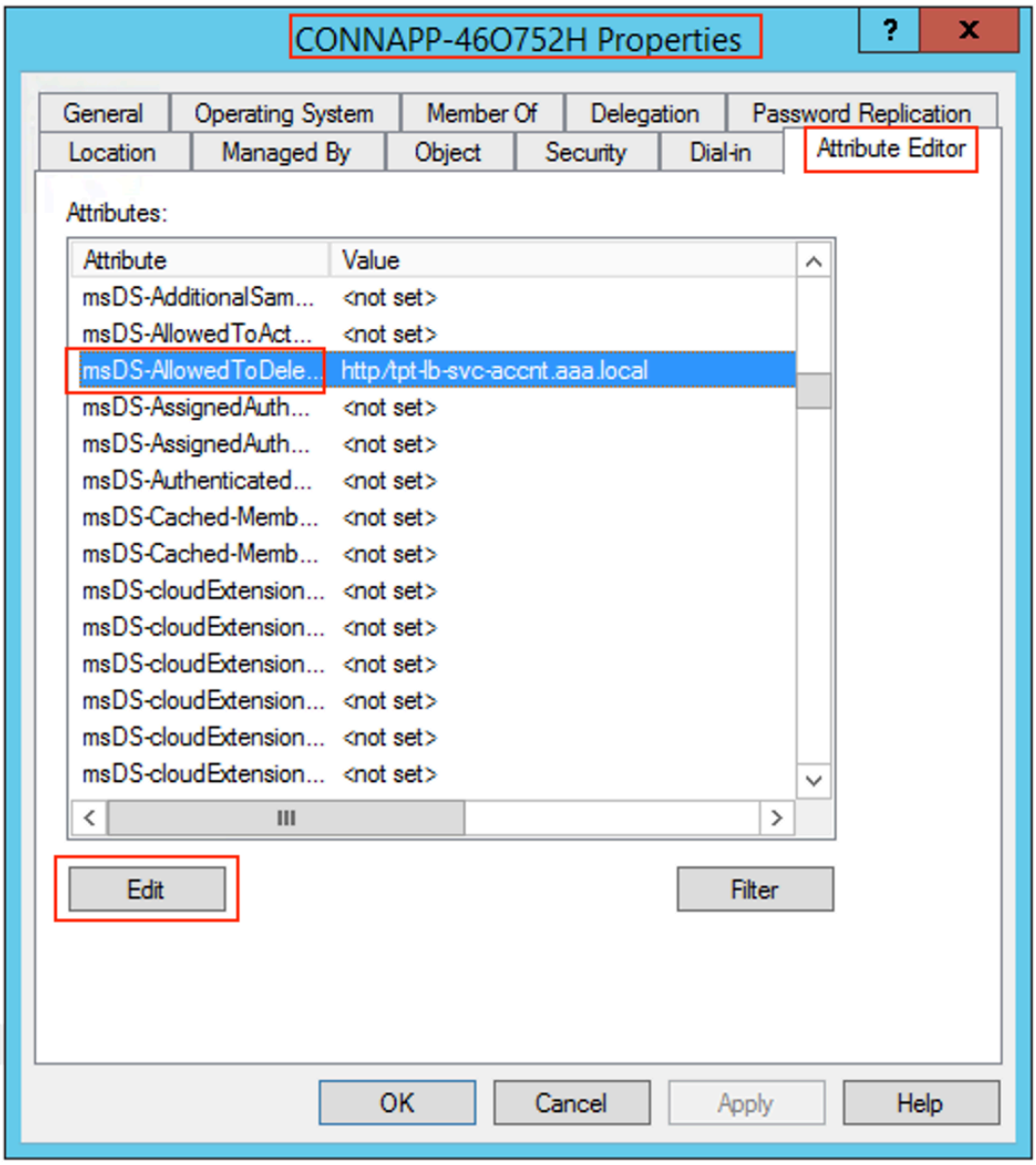


d) 为组托管服务帐户配置 Kerberos 约束委派 (KCD)。

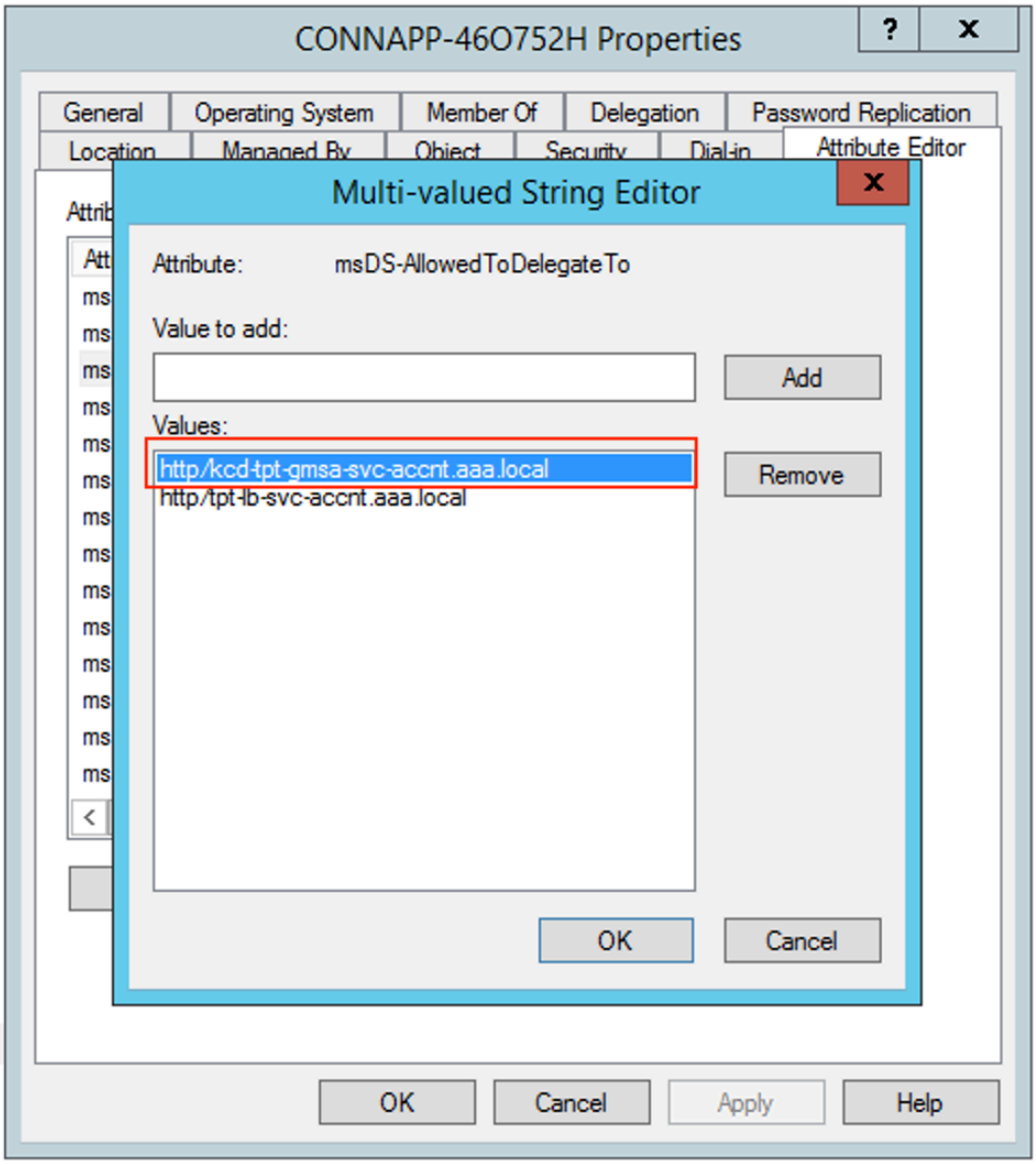
- 将 SPN 添加到组托管服务帐户（如果尚未添加）。
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- 使用以下命令确认 SPN。
  `setspn -l <group_manged_service_account>`

由于在为计算机帐户添加委托条目时无法在 `Users and Computers` 搜索中显示组托管服务帐户，因此无法使用通常的方法为计算机帐户添加委托。因此，您可以通过属性编辑器将此 SPN 作为委派条目添加到 CA 计算机帐户

- 在 Connector 设备计算机属性中，导航到属性编辑器选项卡，然后查找 `msDA-AllowedToDeleteTo` 属性。
- 编辑 `msDA-AllowedToDeleteTo attribute`，然后添加 SPN。



)



)

e) 从 Citrix Gateway 连接器迁移到 Citrix Connector 设备。

- 由于配置网关连接器时已将 SPN 设置为服务帐户，因此如果未配置新的 kerberos 应用程序，则无需为服务帐户添加任何 SPN。您可以通过以下命令查看为服务帐户分配的所有 SPN 的列表，并将它们分配为 CA 计算机帐户的委派条目。

```
setspn -l <service_account>
```

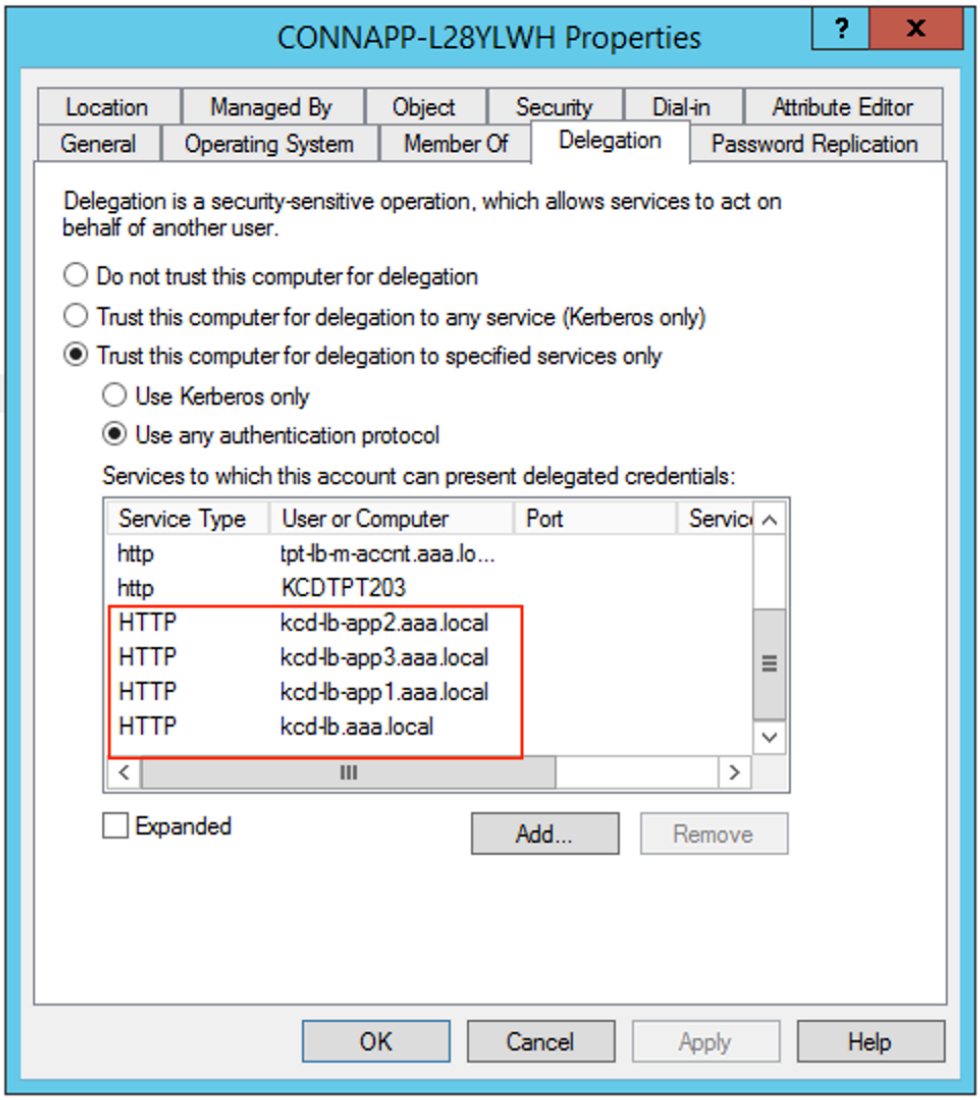


```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

在本示例中，SPN (`kcd-lb.aaa.local`, `kcd-lb-app1.aaa.local`, `kcd-lb-app2.aaa.local`, `kcd-lb-app3.aaa.local`) 是针对 KCD 配置的。

- 将所需的 SPN 作为委派条目添加到连接器装置计算机帐户。有关详细信息，请转至为 *Connector Appliance* 计算机帐户创建委派。



在此示例中，将所需的 SPN 添加为 CA 计算机帐户的委派条目。

注意：这些 SPN 是在配置网关连接器时作为委派条目添加到服务帐户的。当您放弃服务帐户委派时，可以从服务帐户委派选项卡中删除这些条目。

f) 按照 Citrix Secure Private Access 文档设置 Citrix Secure Private Access 服务。在设置过程中，Citrix Cloud 会识别您的 Connector Appliance 是否存在，并使用它们连接到您的资源位置。

- Citrix Secure Private Access 入门
- 配置 Citrix Secure Private Access
- 适用于云服务的 Connector Appliance
- Internet 连接要求。
- 支持企业 Web 应用程序

验证您的 **Kerberos** 配置

如果您使用 Kerberos 进行单点登录，则可以从 **Connector Appliance** 管理页面验证 Active Directory 控制器上的配置是否正确。**Kerberos** 验证 功能使您能够验证 Kerberos 仅领域模式配置或 Kerberos 约束委派 (KCD) 配置。

1. 转到 **Connector Appliance** 管理页面。
   a) 从虚拟机管理程序的 Connector Appliance 控制台中，将 IP 地址复制到浏览器地址栏。
   b) 输入您在注册 Connector Appliance 时设置的密码。
2. 从右上角的“管理”菜单中，选择“**Kerberos** 验证”。
3. 在 **Kerberos** 验证 对话框中，选择 **Kerberos** 验证模式。
4. 指定或选择 **Active Directory** 域。
   - 如果要验证仅限 Kerberos 领域模式的配置，则可以指定任何 Active Directory 域。
   - 如果要验证 Kerberos 约束委派配置，则必须从已加入林中的域列表中进行选择。
5. 指定 服务 **FQDN**。默认服务名假定为 `http`。如果指定“computer.example.com”，则会将其视为与 `http/computer.example.com` 相同。
6. 指定用户名。
7. 如果要验证 Kerberos 仅领域模式配置，请为该用户名指定密码。
8. 单击“测试 **Kerberos**”。

如果 Kerberos 配置正确，则会看到消息 `Successfully validated Kerberos setup`。如果 Kerberos 配置不正确，您会看到一条错误消息，其中提供了有关验证失败的信息。

将网关连接器迁移到 **Connector Appliance**

January 9, 2024

Citrix Gateway 连接器已弃用。Citrix 建议其客户在其环境中使用 Citrix Gateway 连接器，开始为之前由 Citrix Gateway 连接器支持的所有 Secure Private Access 用例部署 Connector Appliance。本主题提供有关将网关连接器迁移到 Connector Appliance 的指南。

将网关连接器迁移到 **Connector Appliance** 的高级步骤

1. 除了网关连接器外，还要在同一资源位置安装 Connector Appliance。
2. 关闭网关连接器并测试现有 Web 应用程序的连接性。检查托管在同一资源位置上的 Web 应用程序是否可访问。
3. 测试完成后，请移除 Citrix Gateway 连接器。

安装 **Connector Appliance**

使用以下步骤安装 Connector Appliance。

1. 登录 Citrix Cloud。
2. 从屏幕左上角的菜单中，选择 资源位置。
3. 单击要添加 Connector Appliance 的资源位置的 Connector Appliance 旁边的加号图标。
4. 选择虚拟机管理程序并单击 下载映像。
5. 在虚拟机管理程序上下载并安装 Connector Appliance。
6. 登录到 Web UI（虚拟机管理程序控制台上提供的 IP 地址）并根据需要设置代理。
7. 单击“注册”按钮并获取短代码。
8. 将短代码粘贴到下载 Connector Appliance 时使用的 Citrix Cloud 用户界面中（步骤 5）。

   Connector Appliance 已注册。

有关详细步骤，请参阅适用于云服务的 Connector Appliance。

常见问题解答

- 如何下载 Connector Appliance?

  下载 Connector Appliance。
- 如何安装 Connector Appliance?

  安装 Connector Appliance。
- 如何注册 Connector Appliance?

  注册 Connector Appliance。

- Connector Appliance 的连接要求是什么?

  Connector Appliance Internet 连接要求。

- Connector Appliance 的系统要求是什么?

  连接器装置系统要求。

- Connector Appliance 是如何更新的?

  Connector Appliance 更新

直接访问企业 **Web** 应用程序

June 19, 2024

现在，客户可以在本地或公共云上托管的企业 Web 应用程序（如 SharePoint、JIRA、Confluence）以及其他应用程序，可以直接从客户端浏览器访问。最终用户不再需要从 Citrix Workspace 体验中启动对其企业 Web 应用程序的访问权限。此功能还允许最终用户通过单击电子邮件、协作工具或浏览器书签中的链接来访问 Web 应用程序。从而为客户提供真正的零占用空间解决方案。

工作原理

- 为已配置的企业 Web 应用程序添加新的 DNS 记录或修改现有 DNS 记录。
- IT 管理员将为已配置的企业 Web 应用程序 FQDN 添加新的公有 DNS 记录或修改现有的公有 DNS 记录，以将用户重定向到 Citrix Secure Private Access 服务。
- 当最终用户启动对已配置的企业 Web 应用程序的访问权限时，应用程序流量将被引导到 Citrix Secure Private Access 服务，然后该服务将代理对该应用程序的访问。
- 请求登陆 Citrix Secure Private Access 服务后，它将检查用户身份验证和应用程序授权，包括上下文访问策略检查。
- 成功验证后，Citrix Secure Private Access 服务将与部署在客户环境（本地或云端）的 Citrix Cloud Connector 设备通信，以允许访问已配置的企业 Web 应用程序。

配置 **Citrix Secure Private Access** 以直接访问企业 **Web** 应用程序

必备条件

在开始之前，您需要满足以下条件才能配置应用程序。

- 应用程序 FQDN

- SSL 证书—要配置的应用程序的公共证书
- 资源位置—安装 Citrix Cloud Connector 设备
- 访问公有 DNS 记录，以便使用 Citrix 在应用程序配置期间提供的规范名称 (CNAME) 对其进行更新。

配置对企业 **Web** 应用程序的直接访问的步骤：

> 重要信息：
>
> 有关应用程序的完整端到端配置，请参阅 管理员指导的工作流程，以轻松上手和设置。

1. 在“Secure Private Access”主页上，单击“继续”。

   > 注意：
   >
   > 继续按钮仅在您首次使用向导时出现。在后续使用中，您可以直接导航到“应用程序”页面，然后单击“添加应用程序”。

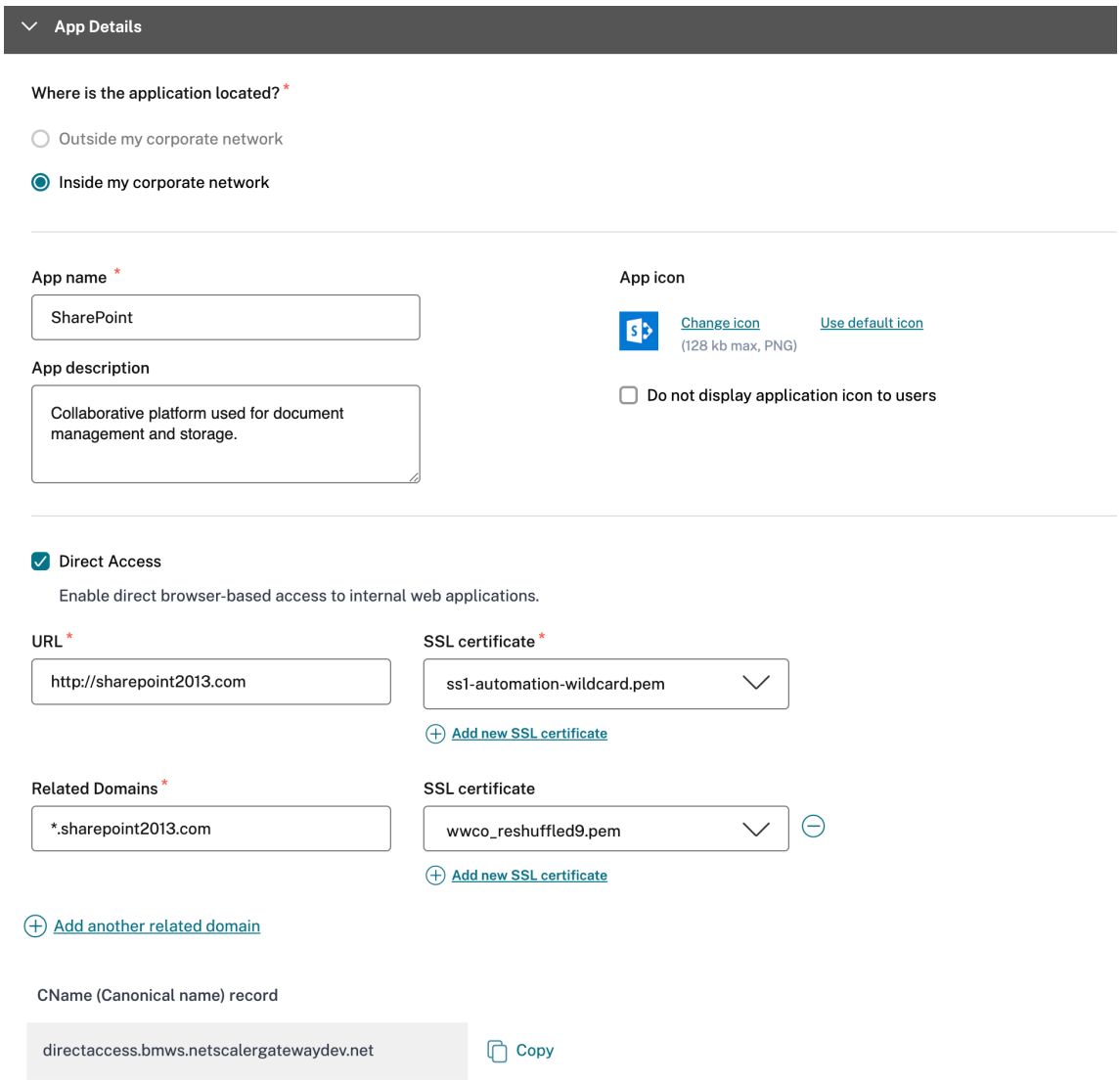
2. 设置身份和身份验证。有关详细信息，请参阅 管理员指导的工作流程，以轻松上手和设置。
3. 继续添加应用程序。有关详细信息，请参阅 添加和管理应用程序。
4. 选择要添加的应用程序，然后单击跳过。
5. 在 应用程序位置在哪里？中，选择位置。
6. 在“应用程序详细信息”部分中输入以下详细信息，然后单击“下一步”。
   - 应用程序类型—选择应用程序类型（HTTP 或 HTTPS）。
   - 应用程序名称 -应用程序的名称。
   - 应用程序描述 - 应用程序的简要描述。您在此处输入的描述将在工作区中显示给您的用户。
   - 应用程序图标—单击更改图标以更改应用程序图标。图标文件大小必须为 128x128 像素。如果不更改图标，则会显示默认图标。

     如果您不想显示应用程序图标，请选择不向用户显示应用程序图标。
7. 选择直接访问以允许用户直接从客户端浏览器访问应用程序。输入以下详细信息。
   - **URL** —后端应用程序的 URL。URL 必须为 HTTPS 格式，管理员必须添加相应的 DNS 条目。
   - **SSL** 证书—从下拉菜单中选择现有的 SSL 证书，或通过单击添加新 SSL 证书来 添加新的 **SSL** 证书。

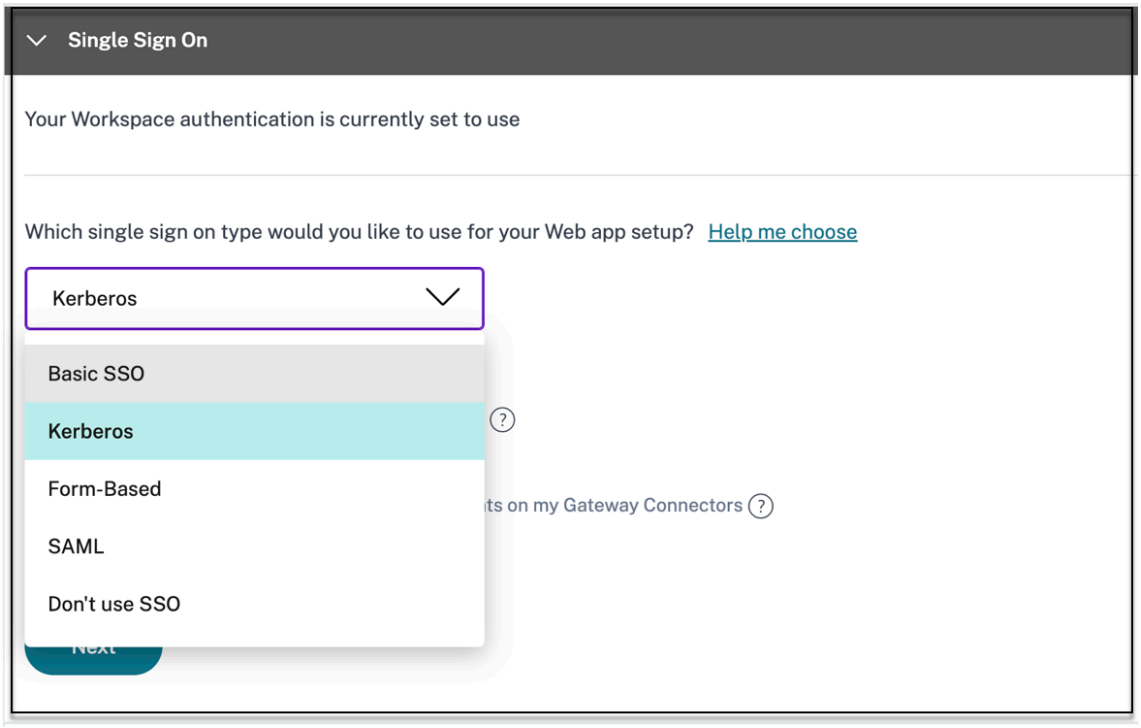
     注意事项：

     - 仅支持公共证书或受信任的 CA 证书。不支持自签名证书。
     - 必须上载完整的证书链。
   - 相关域名 - 相关域名将根据您提供的 URL 自动填充。相关域可帮助服务将 URL 识别为应用程序的一部分，并相应地路由流量。您可以添加多个相关域。您可以将 SSL 证书绑定到每个相关域，这是可选的。

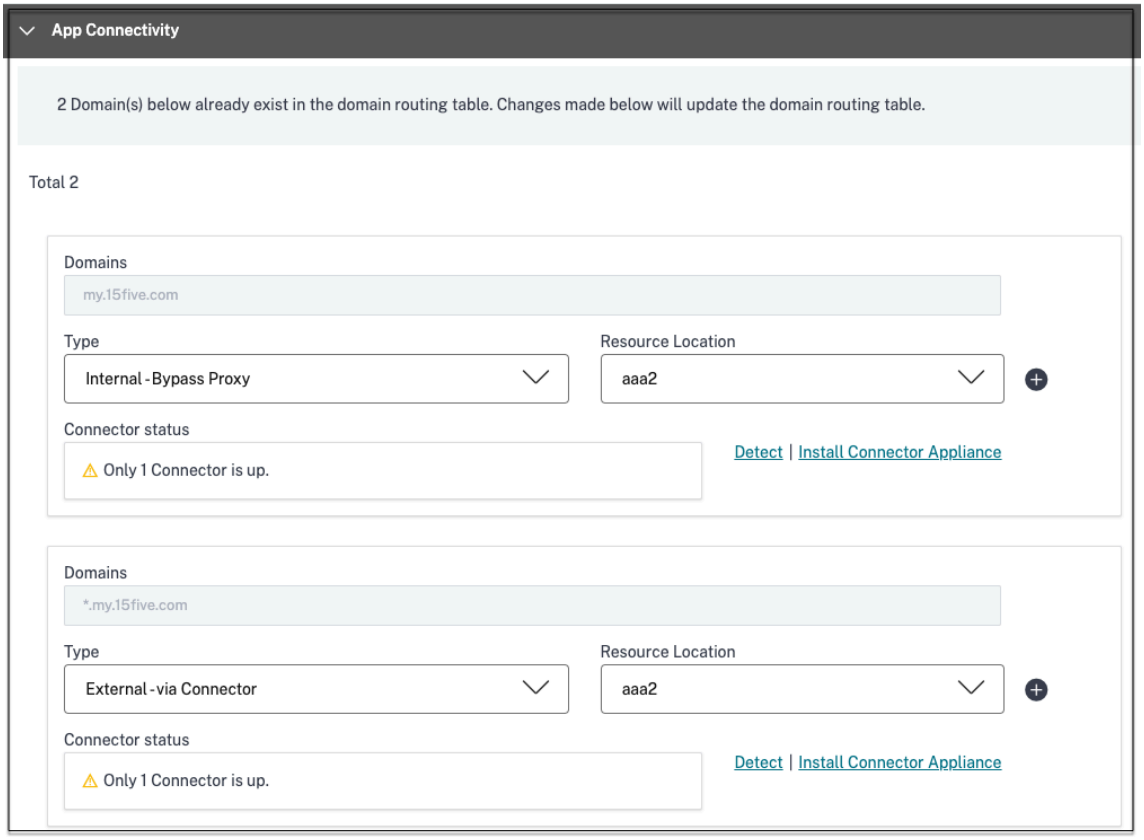
- **CName** 记录—由 Secure Private Access 自动生成。这是必须在 DNS 中输入的值，才能直接访问应用程序。



8. 单击“下一步”。
9. 在“单点登录”部分中，选择要用于应用程序的首选单点登录类型，然后单击“下一步”。



10. 在“应用程序连接”部分中，您可以选择现有资源位置，也可以创建一个资源位置并部署新的 Connector Appliance。要选择现有资源位置，请从资源位置列表中单击其中一个资源位置，例如“我的资源位置”，然后单击“下一步”。有关详细信息，请参阅在 SaaS 和 Web 应用程序中的相关域相同的情况下路由表以解决冲突。



11. 单击完成。该应用程序已添加到应用程序页面。配置应用程序后，您可以在“应用程序”页面中编辑或删除。为此，请单击应用程序上的省略号按钮，然后相应地选择操作。

    - 编辑应用程序
    - 删除

> 重要：
>
> - 要启用基于零信任的应用程序访问权限，默认情况下会拒绝应用程序的访问权限。只有当访问策略与应用程序关联时，才会启用对应用程序的访问权限。有关创建访问策略的详细信息，请参阅创建访问策略。
> - 如果使用相同的 FQDN 或通配符 FQDN 的某些变体配置多个应用程序，则可能会导致配置冲突。为防止配置冲突，请参阅 Web 和 SaaS 应用程序配置的最佳实践。

支持软件即服务应用程序

June 19, 2024

软件即服务 (SaaS) 是一种软件分发模式，可以将软件作为基于 Web 的服务进行远程交付。常用的 SaaS 应用程序包括 Salesforce、工作日、Concur、GoToMeeting 等。

可以使用 Citrix Workspace 使用 Secure Private Access 服务访问 SaaS 应用程序。Secure Private Access 服务与 Citrix Workspace 相结合，可为已配置的 SaaS 应用程序、已配置的虚拟应用程序或任何其他工作区资源提供统一的用户体验。

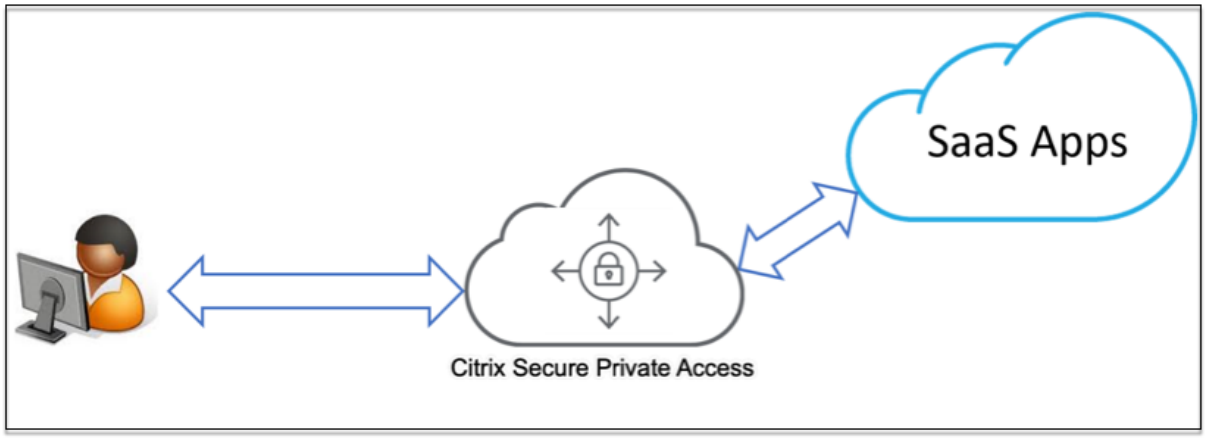
使用 Secure Private Access 服务交付 SaaS 应用程序可为您提供简单、安全、强大且可扩展的应用程序管理解决方案。云上交付的 SaaS 应用程序具有以下优势：

- 配置简单—易于操作、更新和使用。
- 单点登 录—使用单点登录轻松登录。
- 不同应用程序的标准 模板—基于模板的流行应用程序配置。

Secure Private Access 服务如何支持 SaaS 应用程序

1. 客户管理员使用 Secure Private Access 服务用户界面配置 SaaS 应用程序。
2. 管理员向用户提供服务 URL 以访问 Citrix Workspace。
3. 要启动应用程序，用户单击枚举的 SaaS 应用程序图标。
4. SaaS 应用程序信任 Secure Private Access 服务提供的 SAML 断言，并且该应用程序已启动。

> 注意：
>
> - 要向用户授予对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。
> - 配置的 SaaS 应用程序与 Citrix Workspace 中的虚拟应用程序和其他资源一起聚合，以提供统一的用户体验。



配置 SaaS 应用程序

配置 SaaS 应用程序涉及以下高级步骤。

1. 配置应用程序详细信息

2. 设置首选登录方法
3. 定义应用程序路由

配置应用程序详细信息

1. 在“**Secure Private Access**”图块上，单击管理。
2. 单击“继续”，然后单击“添加应用程序”。

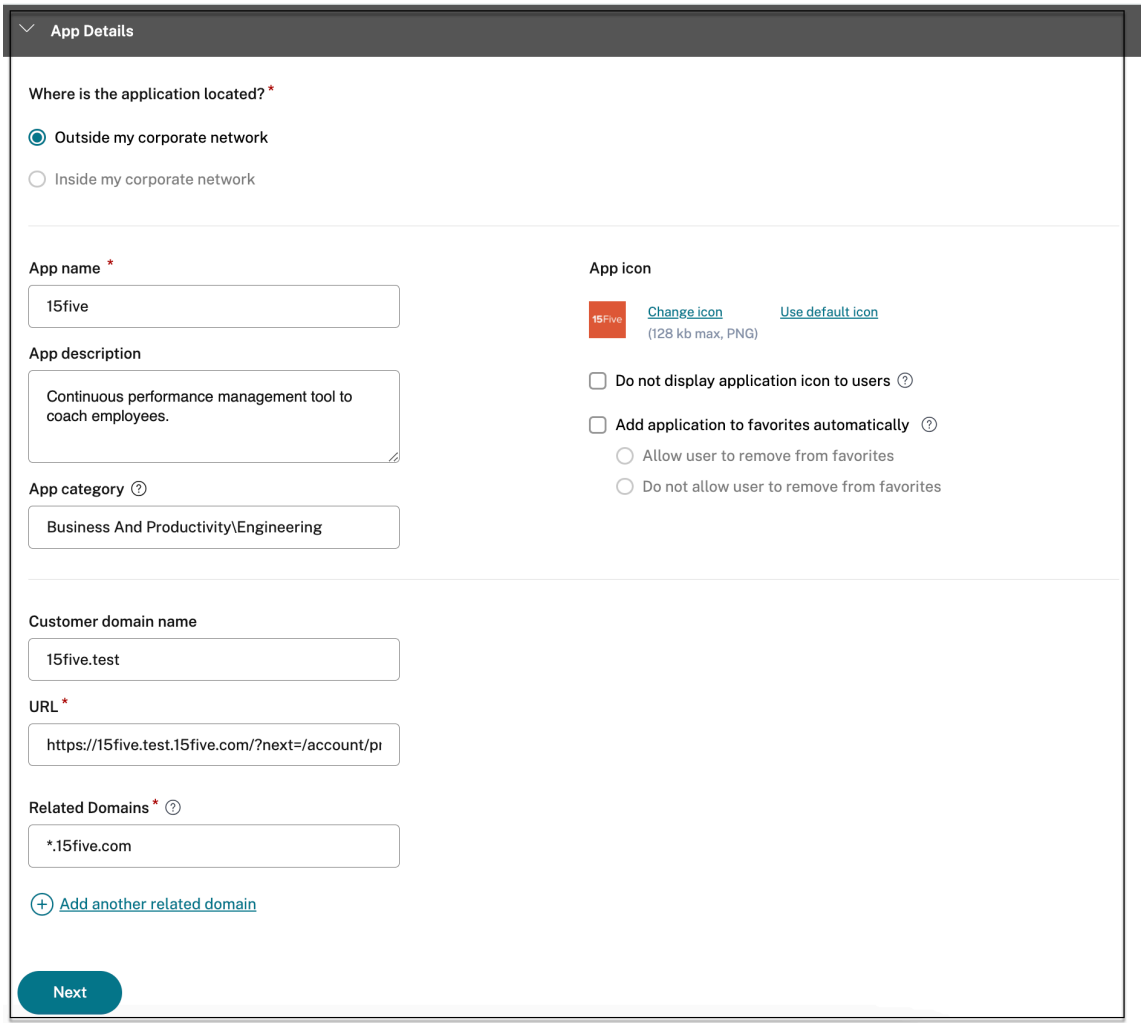
   > 注意：
   >
   > - “继续”按钮仅在您第一次使用向导时出现。在后续使用中，您可以直接导航到“应用程序”页面，然后单击“添加应用程序”。
   > - 您可以通过输入应用程序详细信息来手动添加 SaaS 应用程序，也可以选择一个可用于常用 SaaS 应用程序列表的应用程序模板。该模板预先填充了配置应用程序所需的大部分信息。但是，仍然必须提供特定于客户的信息。有关 SaaS 应用程序配置模板的详细信息，请参阅 SaaS 应用服务器特定配置。

3. 配置应用程序。

   - 要手动输入应用程序详细信息，请单击“跳过”。
   - 要使用模板配置应用程序，请单击“下一步”。

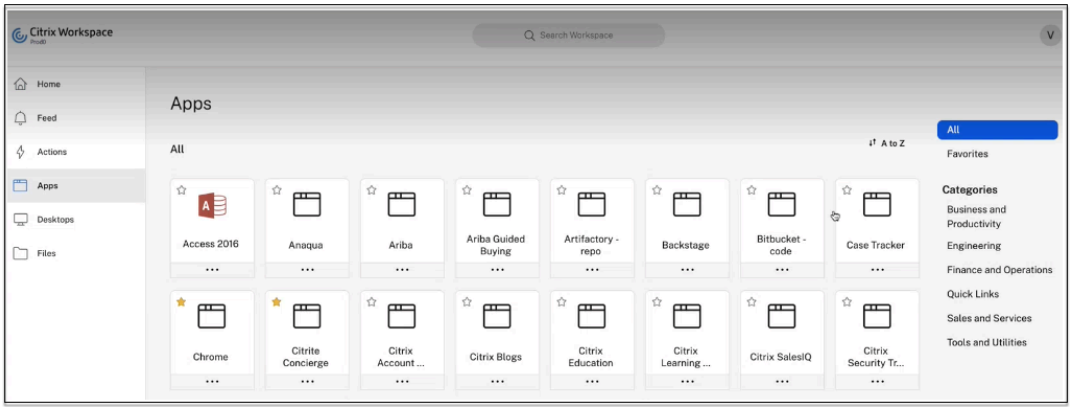
   默认情况下，对于 SaaS 应用程序，启用“企业外部”网络。

4. 在“应用程序详细信息”部分中输入以下详细信息，然后单击下一步。



- 应用程序名称 -应用程序的名称。
- 应用程序描述 - 应用程序的简要描述。您在此处输入的描述将在工作区中显示给您的用户。
- 应用程序类别 - 添加类别和子类别名称（如果适用），您发布的应用程序必须在 Citrix Workspace 用户界面中显示在该类别和子类别下方。您可以为每个应用程序添加新类别，也可以使用 Citrix Workspace 用户界面中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在 Workspace 用户界面中的特定类别下。
  - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
  - 应用程序类别字段适用于 HTTP/HTTPS 应用程序，对于 TCP/UDP 应用程序，则处于隐藏状态。
  - 类别/子类别名称必须用反斜杠分隔。例如，业务与生产力\工程。此外，此字段区分大小写。管理员必须确保他们定义了正确的类别。如果 Citrix Workspace 用户界面中的名称与在应用程序类别字段中输入的类别名称不匹配，则该类别将被列为新类别。

    例如，如果您在应用程序类别字段中错误地将业务和工作效率类别输入为业务和工作效率类别，则除业务和工作效率类别外，Citrix Workspace UI 中还会列出一个名为业务和工作效率的新类别。



- 应用程序图标—单击更改图标以更改应用程序图标。图标文件大小必须为 128x128 像素。如果不更改图标，则会显示默认图标。

  如果您不想显示应用程序图标，请选择不向用户显示应用程序图标。

- **URL** —包含您的客户 ID 的 URL。该 URL 必须包含您的客户 ID（Citrix Cloud 客户 ID）。要获取客户 ID，请参阅注册 Citrix Cloud。如果 SSO 失败或您不想使用 SSO，则用户将被重定向到此 URL。

- 客户域名 和 客户域 **ID** -客户域名和 ID 用于在 SAML SSO 页面中创建应用程序 URL 和其他后续 URL。

  例如，如果要添加一个 Salesforce 应用程序，则您的域名为 `salesforceformyorg`，ID 为 123754，则应用程序的 URL 为 `https://salesforceformyorg.my.salesforce.com/?so=123754`.

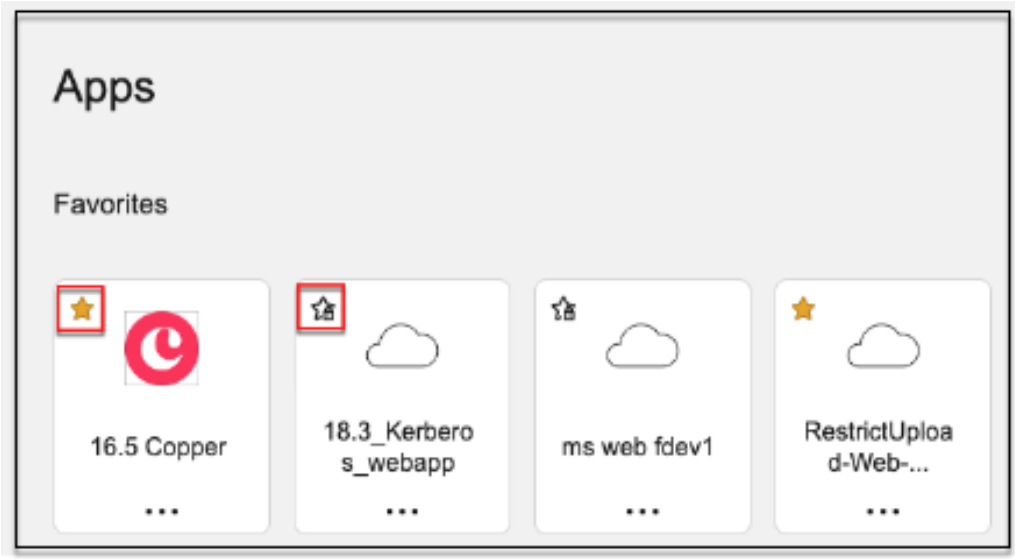
  客户域名和客户 ID 字段特定于某些应用程序。

- 相关域名 - 相关域名将根据您提供的 URL 自动填充。相关域可帮助服务将 URL 识别为应用程序的一部分，并相应地路由流量。您可以添加多个相关域。

- 单击“自动将应用程序添加到收藏夹”，将此应用程序添加为 Citrix Workspace 应用程序中的常用应用程序。

  - 单击“允许用户从收藏夹中删除”，允许应用程序订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。选择此选项时，Citrix Workspace 应用程序中应用程序的左上角会出现一个黄色星形图标。

  - 单击“不允许用户从收藏夹中删除”，以防止订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。选择此选项时，Citrix Workspace 应用程序中应用程序的左上角会出现带有挂锁的星形图标。



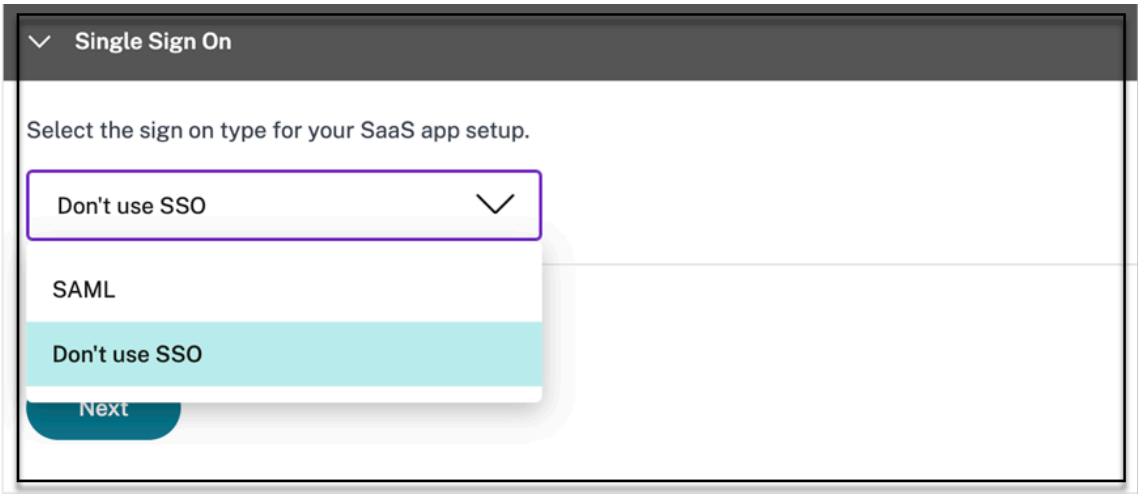
如果您从 Secure Private Access 服务控制台中删除标记为收藏夹的应用程序，则必须从 Citrix Workspace 的收藏夹列表中手动删除这些应用程序。如果从 Secure Private Access 服务控制台中删除这些应用程序，则不会自动从 Workspace 应用程序中删除。

5. 单击“下一步”。

> 重要：
>
> - 要启用基于零信任的应用程序访问权限，默认情况下会拒绝应用程序的访问权限。只有当访问策略与应用程序关联时，才会启用对应用程序的访问权限。有关创建访问策略的详细信息，请参阅创建访问策略。
> - 如果使用相同的 FQDN 或通配符 FQDN 的某些变体配置多个应用程序，则可能会导致配置冲突。为防止配置冲突，请参阅 Web 和 SaaS 应用程序配置的最佳实践。

设置首选登录方法

1. 在“单点登录”部分中，选择要用于应用程序的首选单点登录类型，然后单击“保存”。可以使用以下单点登录类型。

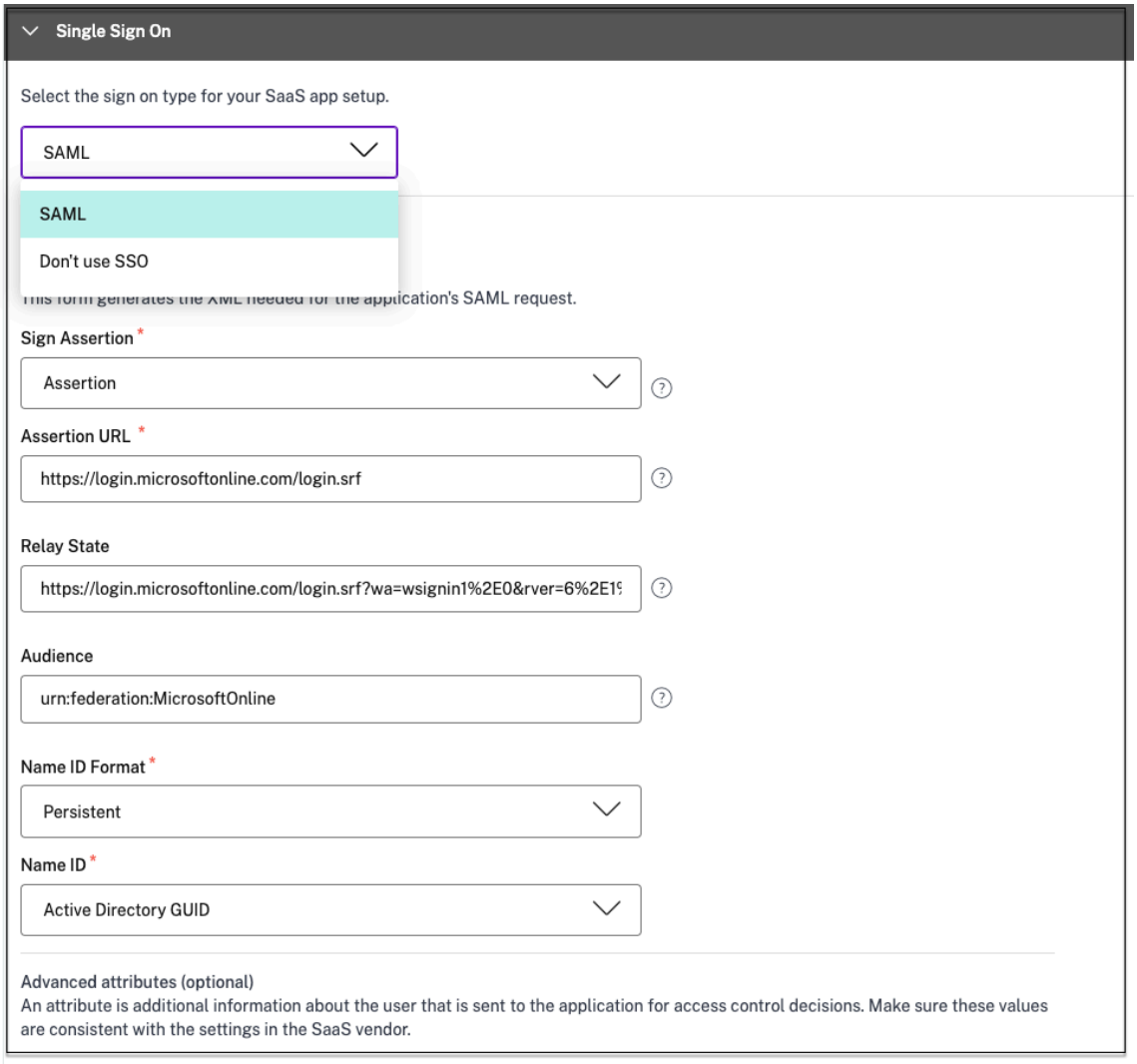


- 不使用 **SSO** —当您 不需要对后端服务器上的用户进行身份验证时，请使用不使用 **SSO** 选项。选择不使用 **SSO** 选项时，用户将被重定向到在应用程序详细信息部分下配置的 URL。
- **SAML** -为基于 **SAML** 的 SSO 选择 SAML 进入 Web 应用程序。输入 **SAML** SSO 类型的配置详细信息。

  在“单点登录”部分中输入以下详细信息，然后单击保存。

  - 签名断言 -签名断言或响应可确保在将响应或断言传递给信赖方 (SP) 时消息的完整性。您可以选择断言、响应、两者或无。
  - 断言 **URL** —断言 URL 由应用程序供应商提供。SAML 断言被发送到此 URL。
  - 中继状态 - 中继状态参数用于识别用户登录并定向到依赖方的联合服务器后访问的特定资源。中继状态为用户生成单个 URL。用户可以单击此 URL 登录到目标应用程序。
  - 受众—受众由应用程序供应商提供。此值确认为正确的应用程序生成了 SAML 断言。
  - 名称 **ID** 格式—选择支持的名称标识符格式。
  - 名称 **ID** —选择支持的名称 ID。
  - 选择 使用特定 **URL**（**SP** 启动）启动应用程序，以覆盖身份提供商启动的流程，仅使用服务提供商启动的流程。

2. 在 高级属性（可选）中，添加有关用户的其他信息，这些信息将被发送到应用程序以做出访问控制决策。



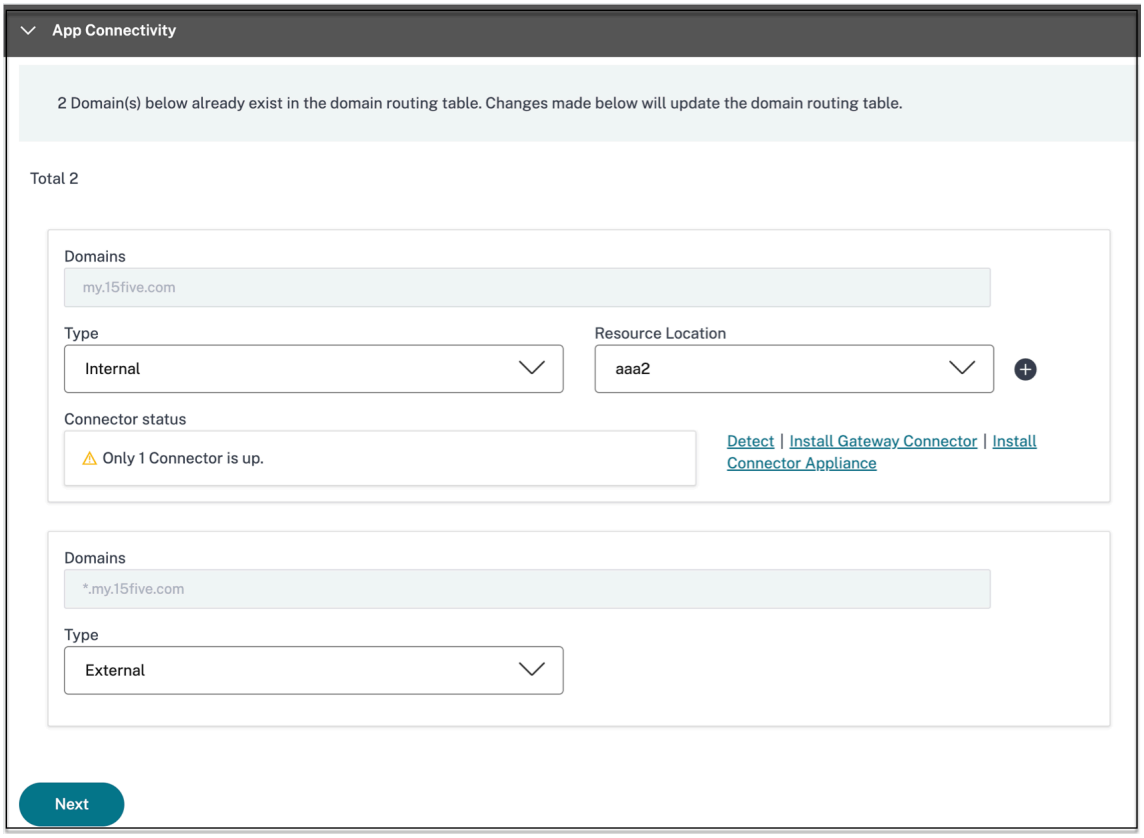
3. 单击 **SAML** 元数据下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用服务器上配置 SSO。

   > 注意：
   >
   > - 您可以复制登录 URL 下的 SSO 登录 **URL**，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
   > - 您还可以从证书列表中下载 证书，并在 SaaS 应用服务器上配置 SSO 时使用该证书。

4. 单击“下一步”。

定义应用程序路由

1. 在应用程序连接部分中，如果必须通过 Citrix Connector Appliance 在外部或内部路由这些域，则为应用程序的相关域定义路由。有关详细信息，请参阅在 SaaS 和 Web 应用程序中的相关域相同的情况下路由表以解决冲突。

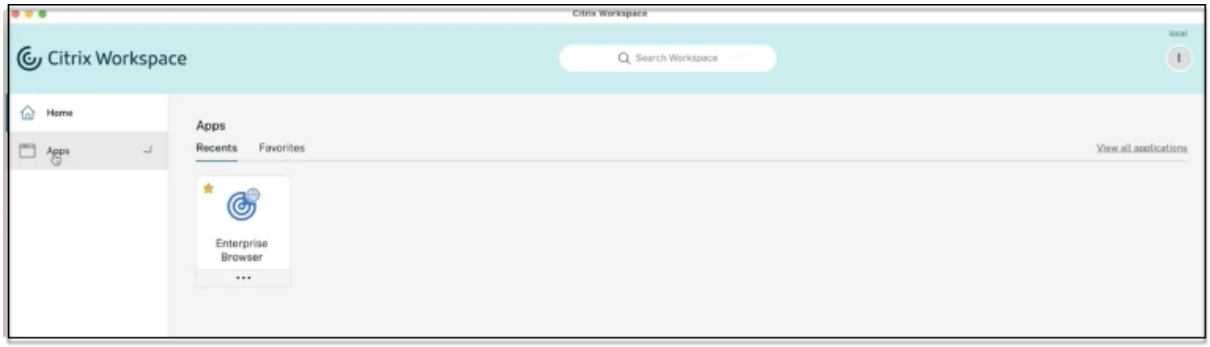


2. 单击“完成”。

   单击完成后，该应用程序将添加到“应用程序”页面。配置应用程序后，您可以从“应用程序”页面编辑或删除该应用程序。为此，请单击应用程序上的省略号按钮，然后相应地选择操作。

   - 编辑应用程序
   - 删除

当您通过 Secure Private Access 服务发布 Web 或 SaaS 应用程序时，如果该应用程序未被隐藏，则 Citrix Enterprise Browser 应用会自动显示在 Citrix Workspace 用户界面中。此外，默认情况下，Citrix Enterprise Browser 也被添加为常用应用程序。最终用户可以在没有 URL 的情况下启动 Workspace Browser，并使用 Workspace Browser 访问内部网站。



引用

有关应用程序的完整端到端配置，请参阅 管理员指导的工作流程，以轻松上手和设置。

支持客户端-服务器应用程序

February 20, 2024

借助 Citrix Secure Private Access，您现在可以使用本机浏览器或通过计算机上运行的 Citrix Secure Access 客户端使用本机客户端应用程序访问所有专用应用程序，包括 TCP/UDP 和 HTTPS 应用程序。

借助 Citrix Secure Private Access 中对客户端-服务器应用程序的额外支持，您现在可以消除对传统 VPN 解决方案的依赖，从而为远程用户提供对所有私有应用程序的访问权限。

预览版功能

支持 DNS 后缀将 FQDN 解析为 IP 地址。

工作原理

最终用户只需在客户端设备上安装 Citrix Secure Access 客户端，即可轻松访问所有经批准的专用应用程序。

- 对于 Windows，可以从 https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html 下载客户端版本（22.3.1.5 及更高版本）。
- 对于 macOS，可以从 App Store 下载客户端版本（22.02.3 及更高版本）。

管理配置—基于 **Citrix Secure Access** 客户端访问 **TCP/UDP** 应用程序

必备条件

确保满足以下要求才能访问 TCP/UDP 应用程序。

- 在 Citrix Cloud 中访问 Citrix Secure Private Access。
- Citrix Cloud Connector - 安装适用于 Active Directory 域配置的 Citrix Cloud Connector，如 Cloud Connector 安装中所述。
- 身份和访问管理-完成配置。有关详细信息，请参阅 身份和访问管理。
- Connector Appliance —Citrix 建议在资源位置的高可用性设置中安装两个 Connector Appliance。连接器可以安装在本地、数据中心虚拟机管理程序或公共云中。有关 Connector Appliance 及其安装的更多信息，请参阅适用于云服务的 Connector Appliance。

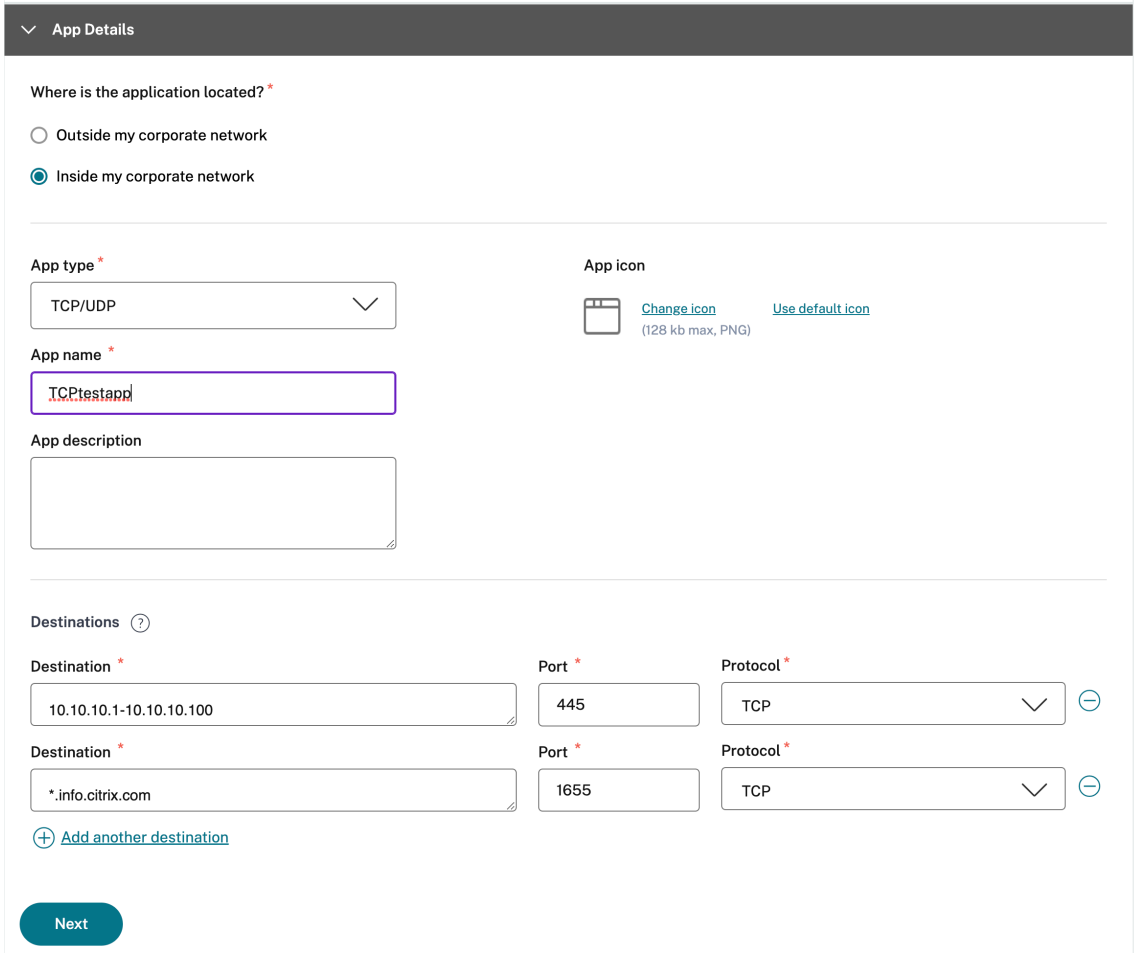
- 对于 TCP/UDP 应用程序，必须使用 Connector Appliance。

> 重要信息：
>
> 有关应用程序的完整端到端配置，请参阅 管理员指导的工作流程，以轻松上手和设置。

1. 在 Citrix Secure Private Access 磁贴上，单击“管理”。
2. 单击继续，然后单击添加应用程序。

   > 注意：
   >
   > 继续按钮仅在您首次使用向导时出现。在后续使用中，您可以直接导航到应用程序页面，然后单击添加应用程序。

   应用程序是目标的逻辑分组。我们可以为多个目标创建一个应用程序-每个目标意味着后端有不同的服务器。例如，一个应用程序可以有一个 SSH、一个 RDP、一个数据库服务器和一个 Web 服务器。您不必为每个目标创建一个应用程序，但一个应用程序可以有多个目的地。
3. 在“选择模板”部分中，单击“跳过”手动配置 TCP/UDP 应用程序。
4. 在“应用程序详细信息”部分中，选择“在我的企业网络中”，输入以下详细信息，然后单击“下一步”。



- 应用程序类型—选择 TCP/UDP。
- 应用程序名称 -应用程序的名称。
- 应用程序图标—将显示应用程序图标。此字段为可选字段。
- 应用程序描述—您要添加的应用程序的描述。此字段为可选字段。
- 目标—驻留在资源位置的后端计算机的 IP 地址或 FQDN。可以按如下方式指定一个或多个目的地。
  - **IP** 地址 **v4**
  - **IP** 地址范围—示例：10.68.90.10-10.68.90.99
  - **CIDR** —示例：10.106.90.0/24
  - 计算机的 **FQDN** 或域名—单一域或通配符域。例如：ex.destination.domain.com、*.domain.com

    > 重要：
    >
    > 即使管理员已使用 IP 地址配置应用程序，最终用户也可以使用 FQDN 访问应用程序。这是可能的，因为 Citrix Secure Access 客户端可以将 FQDN 解析为真实 IP 地址。
    > 下表提供了各种目的地以及如何使用这些目的地访问应用程序的示例：

目的地输入	如何访问应用程序
10.10.10.1-10.10.10.100	最终用户只能通过此范围内的 IP 地址访问应用程序。
10.10.10.0/24	最终用户只能通过 IP CIDR 中配置的 IP 地址访问应用程序。
10.10.10.101	最终用户只能通过 10.10.10.101 访问应用程序
`*.info.citrix.com`	最终用户应该访问 `info.citrix.com` 和 `info.citrix.com`（父域）的子域。例如，`info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` 注意：通配符必须始终是域的起始字符，并且只允许使用一个 *.。
info.citrix.com	最终用户 `info.citrix.com` 只能访问子域，而不能访问子域。例如，`sub1.info.citrix.com` 不可访问。

- 端口—运行应用程序的端口。管理员可以为每个目标配置多个端口或端口范围。

  下表提供了可以为目标配置的端口示例。

端口输入	说明
*	默认情况下，port 字段设置为 “*” （任何端口）。目标支持从 1 到 65535 的端口号。
1300–2400	目标支持从 1300 到 2400 的端口号。
38389	目标仅支持端口号 38389。
22,345,5678	目标支持端口 22、345、5678。
1300–2400, 42000-43000,22,443	端口号范围为 1300 到 2400、42000—43000, 目标支持端口 22 和 443。

> 注意：
>
> 通配符端口 (*) 不能与端口号或端口范围共存。

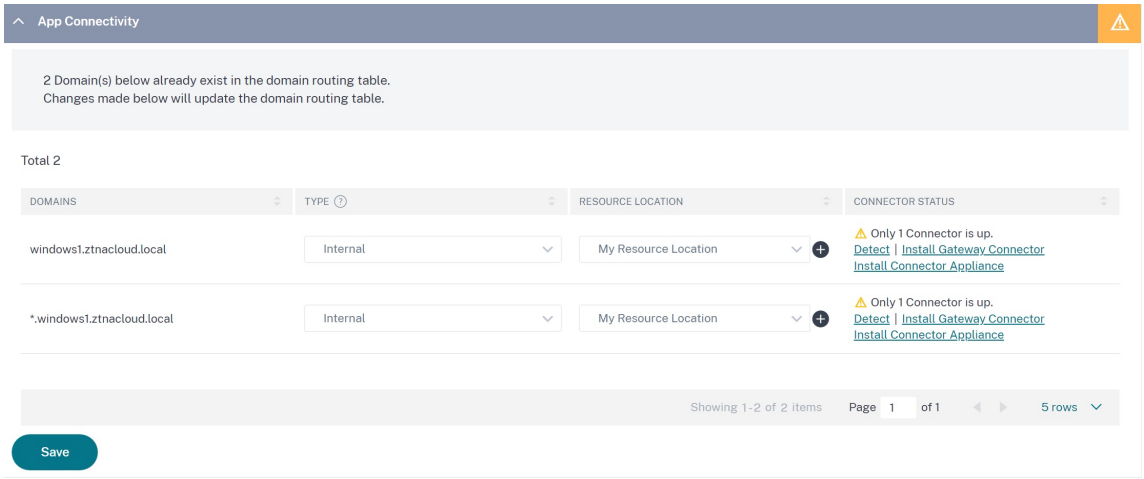
- 协议—TCP/UDP

5. 在应用程序连接部分中，可以使用应用程序域表的迷您版本来做出路由决策。对于每个目标，您可以选择不同的资源位置或相同的资源位置。在上一步中配置的目标将填充在“目标”列下。此处添加的目标也会添加到主“应用程序域”表中。应用程序域表是做出路由决策以将连接建立和流量指向正确的资源位置的真实来源。有关“应用程序域”表和可能的 IP 冲突情形的详细信息，请参阅 应用程序域-*IP* 地址冲突解决方案 部分。
6. 对于以下字段，从下拉菜单中选择输入，然后单击 下一步。

> 注意：
>
> 仅支持内部路由类型。

- 资源位置—从下拉菜单中，必须连接到至少安装了一个 Connector Appliance 的资源位置。

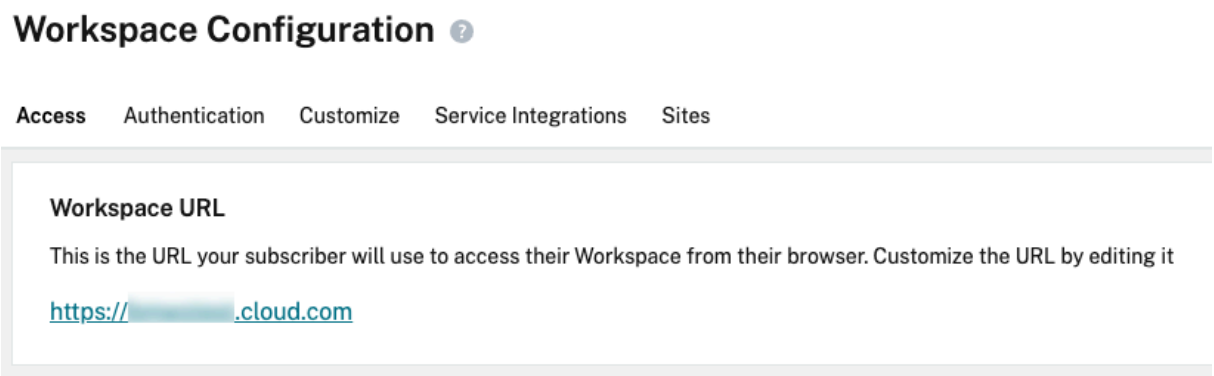
> 注意：
>
> 应用程序连接部分支持 Connector Appliance 安装。您也可以在 Citrix Cloud 门户的“资源位置”部分下进行安装。有关创建资源位置的详细信息，请参阅 设置资源位置。



7. 单击完成。该应用程序已添加到应用程序页面。配置应用程序后，可以从“应用程序”页面编辑或删除应用程序。为此，请单击应用程序上的省略号按钮，然后相应地选择操作。

   - 编辑应用程序
   - 删除

> 注意：
>
> - 要向用户授予对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。
> - 要配置用户所需的身份验证方法，请参阅设置身份和身份验证。
> - 要获取要与用户共享的 Workspace URL，请在 Citrix Cloud 菜单中单击 **Workspace** 配置，然后选择访问选项卡。



管理配置—基于 **Citrix Secure Access** 客户端访问 **HTTP/HTTPS** 应用程序

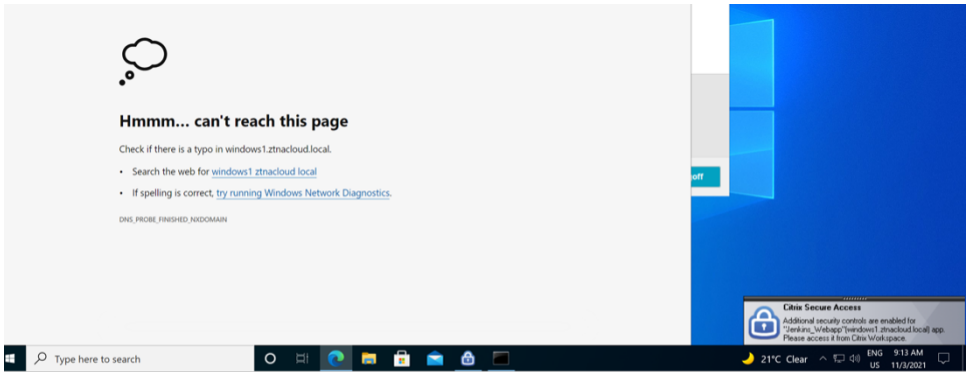
> 注意：
>
> 要使用 Citrix Secure Access 客户端访问现有或新的 HTTP/HTTPS 应用程序，您必须在资源位置安装至少一个（为了高可用性，建议安装两个）Connector Appliance。Connector Appliance 可以安装在本地、数据中心虚拟机管理程序或公有云中。有关 Connector Appliance 及其安装的详细信息，请参阅适用于云服务的 Connector Appliance。

必备条件

- 在 Citrix Cloud 中访问 Citrix Secure Private Access。

注意事项

- 通过增强安全控制强制执行的内部 Web 应用程序无法通过 Citrix Secure Access 客户端进行访问。
- 如果您尝试访问已启用增强安全控制的 HTTP(S) 应用程序，则会显示以下弹出消息。为 **<" app name" (FQDN) >** 应用程序启用了其他安全控制。请从 **Citrix Workspace** 访问。



- 如果要启用 SSO 体验，请使用 Citrix Workspace 应用程序或门户网站访问 Web 应用程序。

配置 HTTP (S) 应用程序的步骤与 支持企业 Web 应用程序中介绍的现有功能相同。

自适应访问 **TCP/UDP** 和 **HTTP (S)** 应用程序

自适应访问使管理员能够根据多种情境因素（例如 Device Posture 检查、用户地理位置、用户角色以及 Citrix Analytics 服务提供的风险评分）来管理对业务关键型应用程序的访问。

> 注意：
>
> - 您可以拒绝访问 TCP/UDP 应用程序，管理员根据用户、用户组、用户访问应用程序的设备以及访问应用程序的位置（国家/地区）创建策略。默认情况下允许访问应用程序。
> - 为应用程序进行的用户订阅适用于为 TCP/UDP 应用程序配置的所有 TCP/UDP 应用程序目的地。

创建自适应访问策略

管理员可以使用管理员指导的工作流向导在 Secure Private Access 服务中配置 SaaS 应用程序、内部 Web 应用程序和 TCP/UDP 应用程序的零信任网络访问权限。

> 注意：
>
> - 有关创建自适应访问策略的详细信息，请参阅 创建访问策略。
> - 有关 Secure Private Access 服务中的 SaaS 应用程序、内部 Web 应用程序和 TCP/UDP 应用程序的零信任网络访问的端到端配置，请参阅管理员指导的工作流程，以便于入门和设置。

注意事项

- 通过 Secure Access 客户端拒绝访问启用了增强安全性的现有 Web 应用程序。将显示一条错误消息，建议您使用 Citrix Workspace 应用程序登录。
- 通过 Citrix Workspace 应用程序基于用户风险评分、Device Posture 检查等的 Web 应用程序的策略配置适用于通过 Secure Access 客户端访问应用程序。
- 绑定到应用程序的策略适用于应用程序中的所有目标。

DNS 解析

Connector Appliance 必须具有 DNS 解析的 DNS 服务器配置。

在 **Windows** 计算机上安装 **Citrix Secure Access** 客户端的步骤

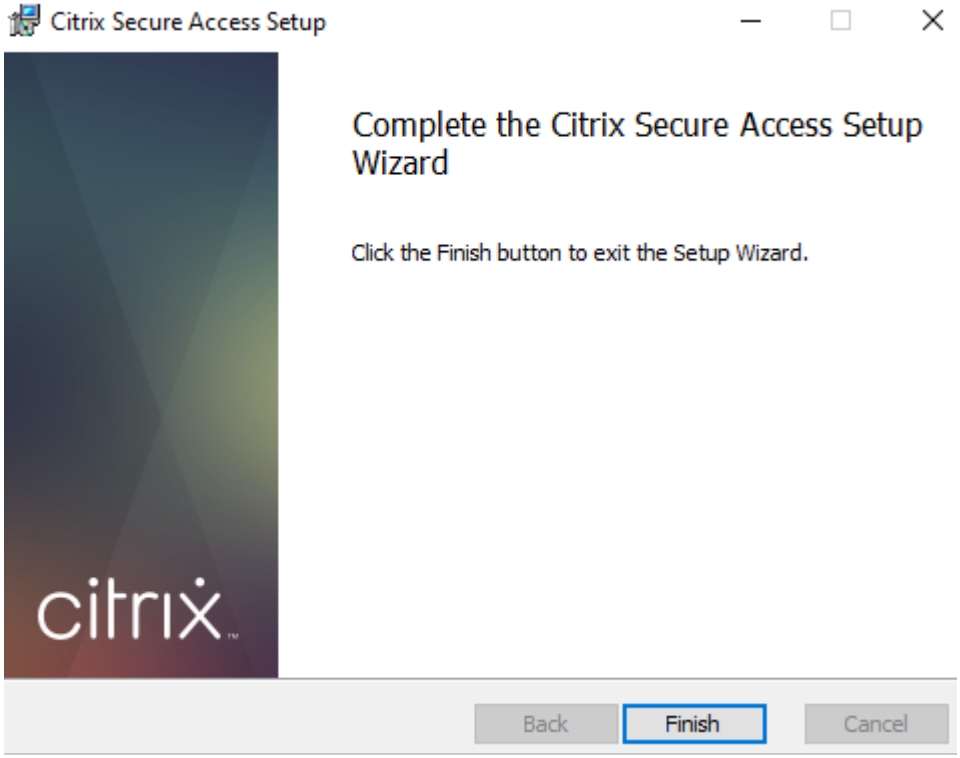
支持的操作系统版本：

Windows –Windows 11、Windows 10、Windows Server 2016 和 Windows Server 2019。

以下是在 Windows 计算机上安装 Citrix Secure Access 客户端的步骤。

1. 从 https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html 下载 Citrix Secure Access 客户端。
2. 单击“安装”在 Windows 计算机上安装客户端。如果您已有 Citrix Gateway 客户端，则会升级同样的客户端。

3. 单击完成以完成安装。



> 注意：
>
> 不支持 Windows 中的多用户会话。

Microsoft Edge 运行时安装步骤

现在，Secure Access 客户端上的身份验证用户界面需要 Microsoft Edge Runtime。
默认情况下，它安装在最新的 Windows 10 和 Windows 11 计算机中。对于早期版本的计算机，请执行以下步骤。

1. 转到以下链接：https://go.microsoft.com/fwlink/p/?LinkId=2124703。
2. 下载并安装 Microsoft Edge。如果用户系统没有安装 Microsoft Edge Runtime，当您尝试连接到 Workspace URL 时，Citrix Secure Access 客户端会提示您安装。

> 注意：
>
> 您可以使用诸如 SCCM 软件或组策略之类的自动解决方案将 Citrix Secure Access 客户端或 Microsoft Edge Runtime 推送到客户端计算机。

在 **macOS** 计算机上安装 **Citrix Secure Access** 客户端的步骤

必备条件：

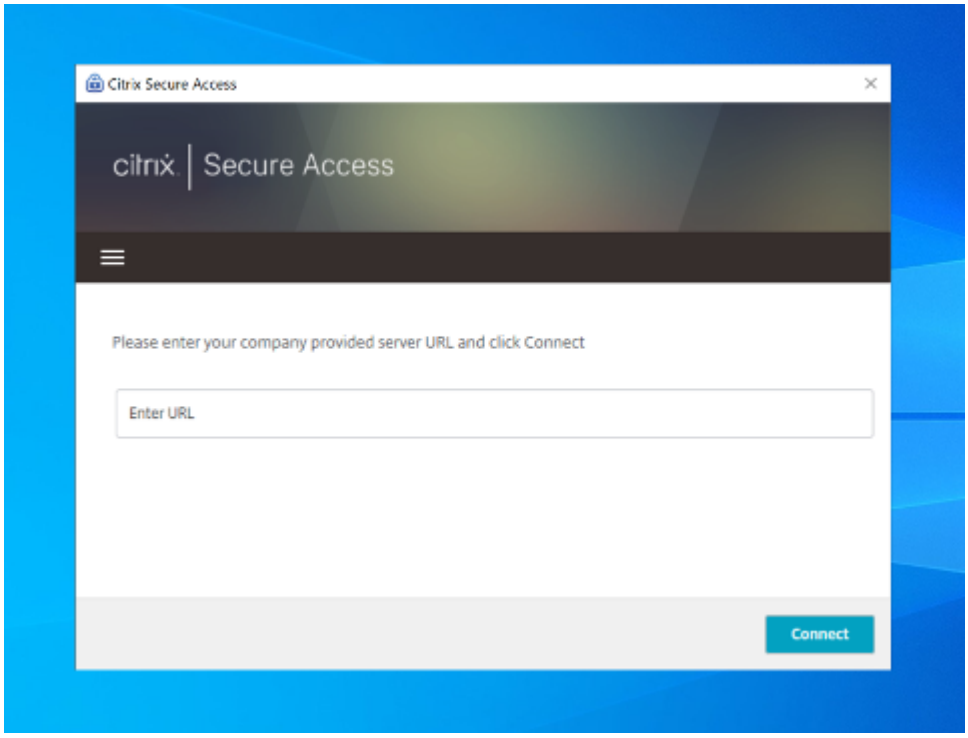
- 从 App Store 下载适用于 macOS 的 Citrix Secure Access 客户端。此应用程序可从 macOS 10.15（Catalina）及更高版本中获得。
- 预览版本仅适用于 macOS Monterey (12.x) 的 TestFlight 应用程序。
- 如果要在 App Store 应用程序和 TestFlight 预览应用程序之间切换，则必须重新创建要用于 Citrix Secure Access 应用程序的配置文件。例如，如果您一直将连接配置文件与一起使用 `blr.abc.company.com`，请删除 VPN 配置文件，然后再次创建相同的配置文件。

支持的操作系统版本：

- macOS：12.x (Monterey)。支持 11.x（Big Sur）和 10.15（Catalina）。
- 移动设备：不支持 iOS 和 Android。

启动已配置的应用程序-最终用户流程

1. 在客户端设备上启动 Citrix Secure Access 客户端。
2. 在 Citrix Secure Access 客户端的 URL 字段中输入客户管理员提供的 Workspace URL，然后单击“连接”。这是一次性活动，URL 已保存以供后续使用。



3. 系统会根据在 Citrix Cloud 中配置的身份验证方法提示用户进行身份验证。

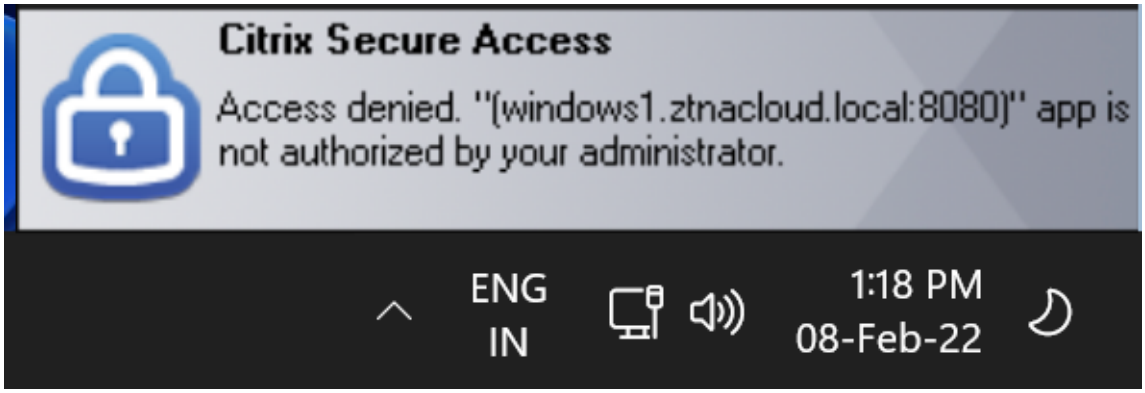
   成功进行身份验证后，用户可以访问配置的私有应用程序。

用户通知消息

在以下情况下会出现弹出式通知消息：

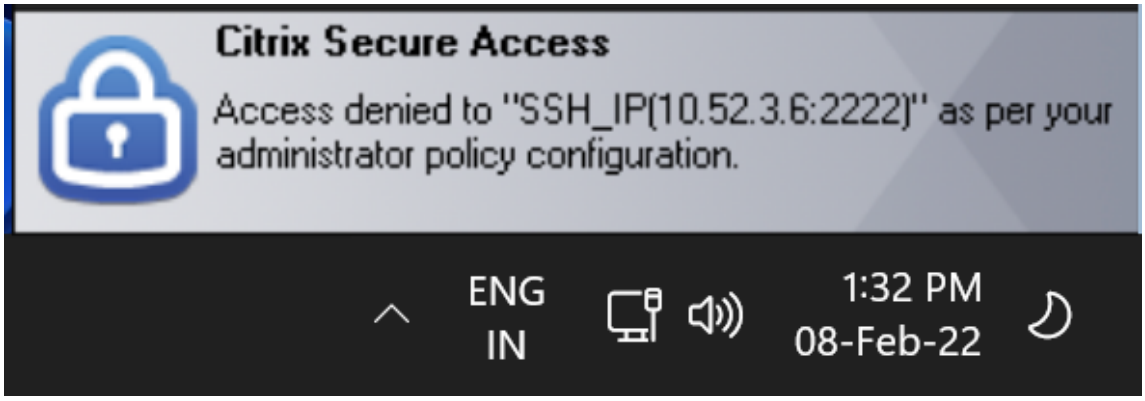
- 该应用程序未获得管理员对用户的授权。

  原因：为访问的目标 IP 地址或 FQDN 配置的应用程序未为登录用户订阅。



- 访问策略评估会导致拒绝访问。

  原因：对目标 IP 地址或 FQDN 的访问被拒绝，因为绑定到应用程序的策略被评估为“拒绝对登录用户的访问”。



- 已为应用程序启用增强的安全控制。

  原因：已对访问目标的应用程序启用了增强的安全控制。该应用程序可以使用 Citrix Workspace 应用程序启动。

其他信息

应用程序域**-IP** 地址冲突解决方案

创建应用程序时添加的目的地将添加到主路由表中。
路由表是做出路由决策以将连接建立和流量指向正确的资源位置的真实来源。

- 目标 IP 地址在资源位置之间必须是唯一的。
- Citrix 建议您避免路由表中的 IP 地址或域重叠。如果您遇到重叠，您必须解决它。

以下是冲突情景的类型。完全重叠 是唯一一种在冲突解决之前限制管理员配置的错误场景。

冲突场景	现有应用程序域条目	来自应用添加的新条目	行为
子集重叠	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	允许；警告信息 - IP 域与现有条目的子集重叠
子集重叠	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	允许；警告信息 - IP 域与现有条目的子集重叠

冲突场景	现有应用程序域条目	来自应用添加的新条目	行为
部分重叠	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	允许；警告信息-IP 域与现有条目部分重叠
部分重叠	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	允许；警告信息-IP 域与现有条目部分重叠
完全重叠	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	错误；<Completely overlapping IP domain's value> IP 域与现有条目完全重叠。请更改现有路由 IP 条目或配置其他目的地
完全重叠	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	错误；<Completely overlapping IP domain's value> IP 域与现有条目完全重叠。请更改现有路由 IP 条目或配置其他目的地
精确匹配	20.20.20.0/29 RL1	20.20.20.0/29	允许；域名路由表中存在域。所做的更改将更新域路由表

> 注意：
>
> - 如果添加的目标导致完全重叠，则在应用程序 详细信息 部分配置应用程序时会显示错误。管理员必须通过修改 应用程序连接 部分中的目标来解决此错误。
>
> 如果“应用程序详细信息”部分没有错误，管理员可以继续保存应用程序的详细信息。但是，在 **App Con** nectivity 部分中，如果目标之间存在子集和部分重叠，或者主路由表中的现有条目重叠，则会显示一条警告消息。在这种情况下，管理员可以选择解决错误或继续配置。
>
> - Citrix 建议保留一个干净的 应用程序域 表。如果 IP 地址域被划分为适当的块而没有重叠，则配置新的路由条目会更容易。

登录和注销脚本配置注册表

当 Citrix Secure Access 客户端连接到 Citrix Secure Access 云服务时，Citrix Secure Private Access 客户端将从以下注册表访问登录和注销脚本配置。

注册表：HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- 登录脚本路径：SecureAccessLogInScript 类型 REG_SZ

- 注销脚本路径：SecureAccessLogOutScript 类型 REG_SZ

发行说明参考

- 适用于 Windows 的 Citrix Secure Access 发行说明
- 适用于 macOS 的 Citrix Secure Access 发行说明
- Citrix Secure Private Access 发行说明

为 **TCP** 和 **UDP** 服务器保留的 **CIDR** 地址

January 9, 2024

管理员可以为 TCP/UDP 服务器配置保留的 CIDR IP 地址。在 DNS 解析过程中，这些 IP 地址在 DNS 响应中共享，而不是实际的 IP 地址。

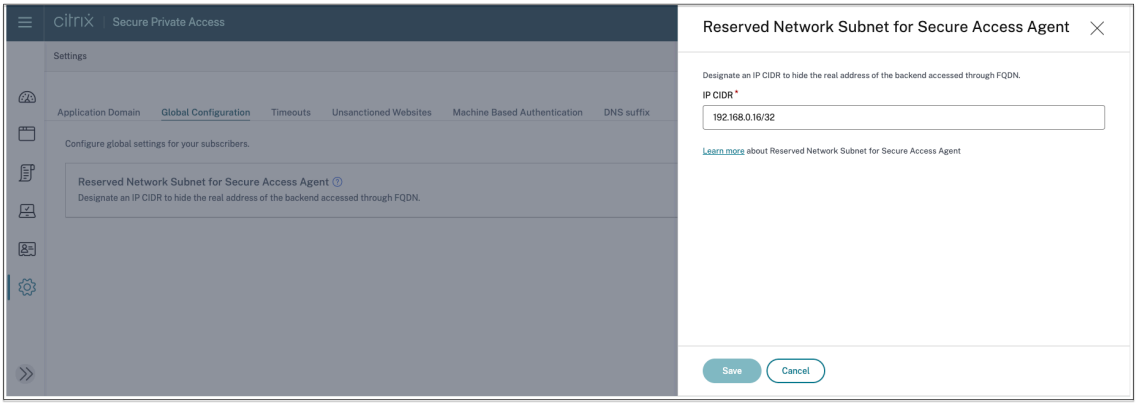
以下是允许的保留 CIDR IP 地址范围：

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> 注意：
>
> 确保保留的 IP 地址不与以下地址冲突：
>
> - 在客户资源位置为 TCP/UDP 应用程序配置的 IP 地址。
> - 客户端的网络子网。

配置保留的 **CIDR IP** 地址

1. 单击“设置”，然后单击“全局配置”。



2. 在“**ecure Access Agent** 的预留网络子网”中，单击“管理”。
3. 在 **IP CIDR** 中，输入专用 IP 地址范围。
4. 单击保存。

用于将 **FQDN** 解析为 **IP** 地址的 **DNS** 后缀

January 9, 2024

DNS 后缀是一种适用于所有最终用户的全局配置。Citrix Secure Private Access 服务的 DNS 后缀功能可用于以下用例：

- 通过为后端服务器添加 DNS 后缀域，使 Citrix Secure Access 客户端能够将非完全限定域名（主机名）解析为完全限定域名 (FQDN)。
- 允许管理员使用 IP 地址（IP CIDR/IP 范围）配置应用程序，以便最终用户可以使用 DNS 后缀域下相应的 FQDN 访问应用程序。

例如，在解析非完全限定域名 “workday” 时，如果配置了 DNS 后缀 “citrix.net”，则操作系统会附加后缀 “citrix.net” 并解析为 “workday.citrix.net”。

如果配置了多个 DNS 后缀，则按顺序解析 DNS 后缀。例如，假设添加了以下后缀：

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

当最终用户键入 “workday” 时，操作系统会尝试按以下顺序解析 FQDN。如果成功使用一个后缀，则跳过其余的后缀。

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> 重要：
>
> - DNS 后缀配置只能使客户端通过为使用 DNS 后缀功能配置的域添加后缀来解析不完全限定的域名。要使最终用户访问 DNS 后缀域下的 FQDN，管理员必须使用 IP 地址、FQDN 或通配符域配置应用程序。有关详细信息，请参阅用例示例中的第 4 点。
> - 如果配置了两个不同的应用程序，一个使用 FQDN，另一个使用 IP 地址，两者都对应同一个后端服务器，则具有 IP 地址的应用程序的策略优先级更高。有关详细信息，请参阅用例示例中的第 5 点。

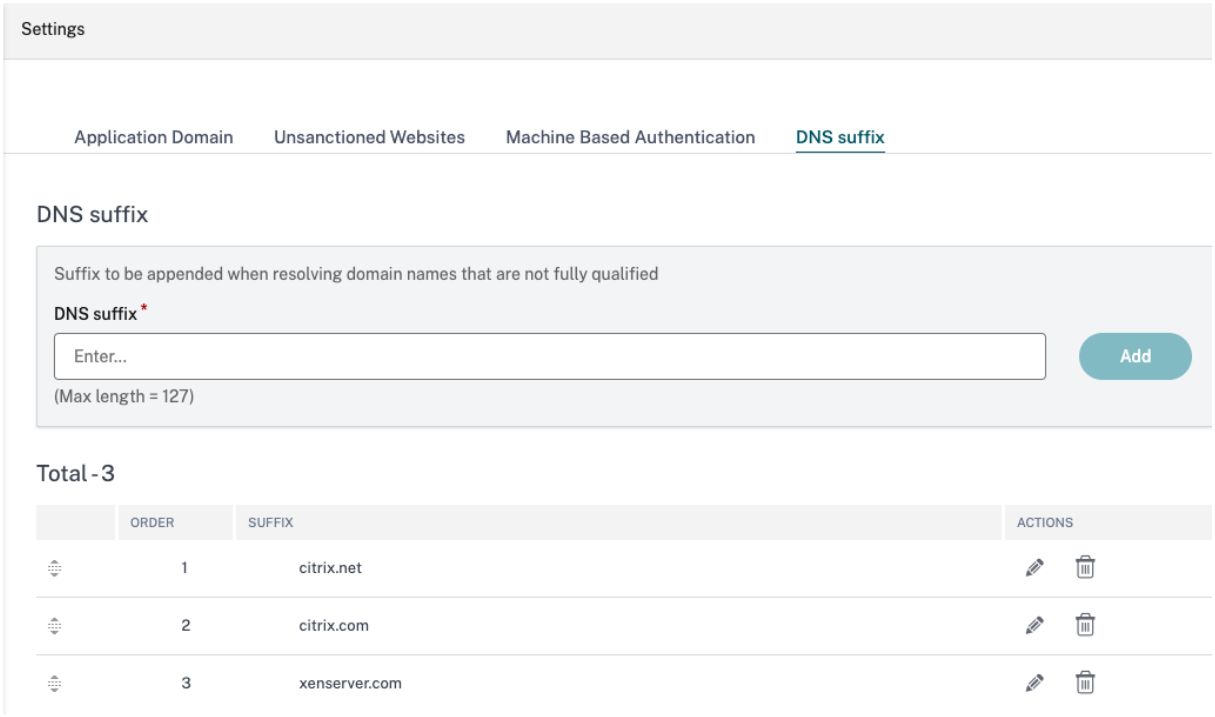
必备条件

- 客户必须有权使用 Secure Private Access Advanced 版才能使用 DNS 后缀功能。
- 请联系 Citrix Product Management 团队以启用 DNS 后缀功能标志。

如何添加 **DNS** 后缀

1. 在“Secure Private Access”磁贴上，单击“管理”。
2. 在“Secure Private Access”登录页面上，单击“设置”，然后单击 **DNS** 后缀。
3. 在 **DNS** 后缀字段中，输入解析非完全限定名称时必须附加的后缀。
4. 单击添加。

后缀是根据添加顺序列出的。管理员可以删除或修改后缀。



示例用例

请注意以下事项：

- 管理员已将 IP 地址 192.0.2.1 分配给客户网络中的一台计算机。
- 计算机的 FQDN（IP 地址为 192.0.2.1）位于“citrix.net”域（例如，workday.citrix.net）。

		DNS 后缀和应用程序配置	最终用户体验
	1	管理员将 DNS 后缀配置为“citrix.net”，并创建一个 IP 地址为 192.0.2.1 的应用程序，将 user1 的访问策略设置为“允许”。	当 user1 尝试连接到“workday”时，FQDN 的后缀是“citrix.net”（workday.citrix.net），IP 地址解析为 192.0.2.1。由于配置了应用程序的 user1 允许 192.0.2.1，因此授予访问权限。 注意：最终用户可以使用 192.0.2.1、workday.citrix.net 或“workday”访问 Workday 应用程序。 如果不配置 DNS 后缀，则通过“workday”和“workday.citrix.net”进行访问将被拒绝。
	2	管理员将 DNS 后缀配置为“citrix.net”，使用 FQDN (workday.citrix.net) 创建应用程序，并将 user1 的访问策略设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”的后缀是“workday” (workday.citrix.net)。最终用户可以访问 Workday，因为应用程序配置了“workday.citrix.net”，并且 user1 的访问策略设置为“允许”。 注意：最终用户可以通过 workday.citrix.net 或“workday”访问 Workday 应用程序。 对 192.0.2.1 的访问被拒绝，因为没有使用此 IP 地址配置任何应用程序。

		DNS 后缀和应用程序配置	最终用户体验
	3	管理员将 DNS 后缀配置为“citrix.net”，使用通配符域“*.citrix.net”创建应用程序，并将 user1 的访问策略设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”的后缀是“workday”(workday.citrix.net)。最终用户可以访问 Workday，因为应用程序配置了“*.citrix.net”，并且 user1 的访问策略设置为“允许”。 注意：最终用户可以使用 workday.citrix.net 或“workday”访问 Workday。
	4	管理员将 DNS 后缀配置为“citrix.net”。没有为使用 FQDN (workday.citrix.net) 或 192.0.2.1 的 user1 配置任何应用程序。	对 192.0.2.1 的访问被拒绝，因为没有使用此 IP 地址配置任何应用程序。 当 user1 尝试连接到“workday”时，客户端将“workday”后缀为“citrix.net”，并将“workday.citrix.net”解析为 192.0.2.1。但是，user1 无法连接到专用服务器 (workday.citrix.net/192.0.2.1)，因为没有为 user1 配置了 192.0.2.1、workday.citrix.net 或 *.citrix.net 的应用程序。

	DNS 后缀和应用程序配置	最终用户体验
5	管理员将 DNS 后缀配置为“citrix.net”。添加 IP 地址为 192.0.2.1 的应用程序，并将 user1 的访问策略设置为“拒绝”。然后添加另一个具有解析为 192.0.2.1 的 FQDN (workday.citrix.net) 的应用程序，并将 user1 的访问策略设置为“允许”。	当 user1 尝试连接到“workday”时，“citrix.net”的后缀是 Workday (workday.citrix.net)，IP 地址解析为 192.0.2.1。但是，由于配置了 IP 192.0.2.1 的应用程序的策略优先于使用 FQDN 配置的应用程序，因此对 Workday 的访问被拒绝。

通过 **Citrix Workspace** 应用程序单点登录 **Citrix Secure Access** 客户端

January 9, 2024

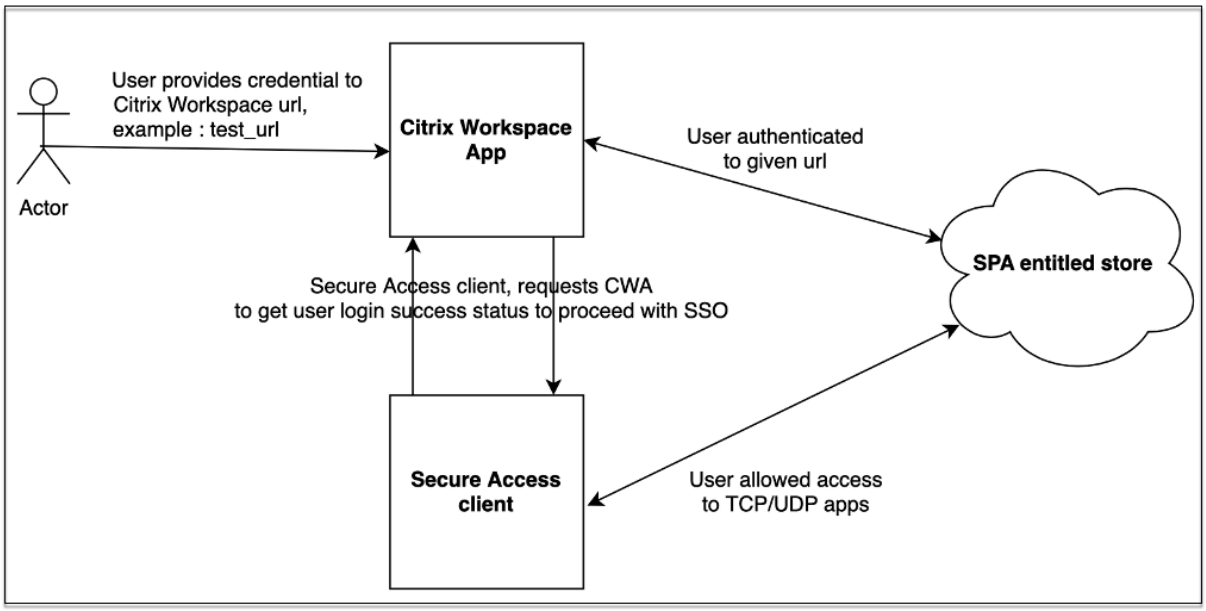
当已经通过 Citrix Workspace 应用程序登录时，Citrix Secure Access 客户端现在支持 Workspace URL 的单点登录。此 SSO 功能通过避免多次身份验证来增强用户体验。

必备条件

- 设备上必须同时安装 Citrix Workspace 应用程序和 Secure Access 客户端。
- 用户必须先登录 Citrix Workspace 应用程序才能在 Citrix Secure Access 客户端中进行自动 SSO。

> 注意：
>
> 只有在 Citrix Workspace 应用程序中配置的主存储区才支持单点登录功能。如果用户登录到主存储以外的任何其他存储，则不会发生 SSO。用户必须手动登录 Citrix Secure Access 客户端。

下图显示了 Citrix Workspace 应用程序和 Citrix Secure Access 客户端之间的 SSO 流程。



Windows 的功能要求

- Citrix Workspace 应用程序版本 - **Citrix Workspace 22.10.5.14 (2210.5)** 或更高版本
- Citrix Secure Access 版本 - **22.10.1.9** 或更高版本
- Citrix Secure Access Windows 注册表 - **EnableCWASSO**

默认情况下，SSO 功能处于禁用状态。要启用此功能，请在最终用户计算机上添加以下注册表。

- 注册表名称 - EnableCWASSO
- 注册表路径 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- 注册表类型 - REG_DWORD
- 注册表值 - 1

> 重要：
>
> 有时，最终用户计算机可能需要重新启动才能成功通过 Citrix Workspace 应用程序建立单点登录。

终止活动用户会话并将用户添加到禁用用户列表中

June 19, 2024

管理员可以立即终止所有活动的最终用户会话，并将用户添加到禁用用户列表中。将用户添加到此禁用用户列表将终止所有活跃的 Secure Private Access 应用程序会话并阻止将来的应用程序访问。

通过 Citrix Enterprise Browser、直接访问、适用于 HTML5 的 CWA 和安全访问代理的所有活动应用程序会话都将被终止和阻止。通过安全访问代理连接的所有资源，例如文件共享、RDP、SSH 会话，也会被终止和阻止。在从禁用用户列表中删除被封锁的用户之前，他们无法启动任何新应用程序。

> 注意：
>
> - 将用户添加到禁用用户列表不会更改或编辑已配置的 Secure Private Access 访问策略。无论配置了什么访问策略，访问都会终止和阻止。用户从列表中删除后，将恢复该用户的现有 Secure Private Access 访问策略。
> - 7 天后，用户将自动从禁用用户列表中删除。
> - 只有对已发布的 Secure Private Access 应用程序的访问权限被阻止。即使将用户添加到阻止列表（基于您的 Web 筛选配置），也可以允许或拒绝通过 Citrix Enterprise Browser 访问 Internet。

用例

您可以在以下场景中使用此功能。

- 员工退出组织或被组织解雇。在这种情况下，管理员通过终止活动的 Secure Private Access 会话并阻止任何未来的应用程序访问来撤消所有 Secure Private Access 应用程序访问权限。
- 设备丢失或被盗。在这种情况下，访问将被阻止，所有当前会话都将终止。情况得到控制后，可以将该用户从禁用用户列表中删除。
- 用户滥用应用程序访问权限。在这种情况下，可以立即撤消用户的访问权限。在将用户添加到列表之前，访问会被阻止。

将用户添加到禁用用户列表

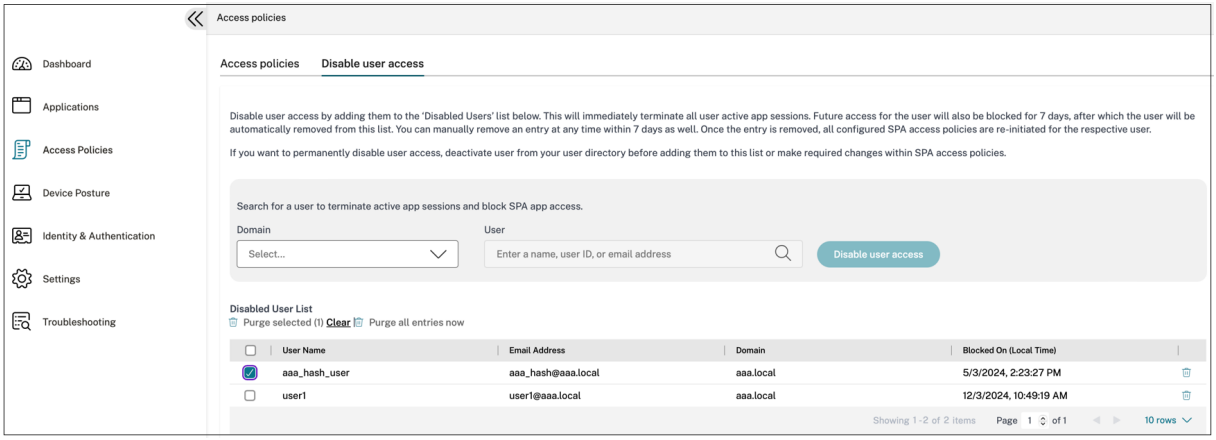
1. 导航到“**Secure Private Access**”**>**“访问策略”，然后单击“禁用用户访问权限”选项卡。
2. 在域中，选择必须禁用访问权限的域。
3. 在用户中，搜索必须添加到禁用用户列表的用户名。将显示所有符合搜索条件的用户名。如果用户从目录服务中移除，则该用户名不会出现在用户列表中。
4. 单击“禁用用户访问权限”。

   该用户被添加到禁用用户列表中。将用户添加到禁用用户列表后，将执行以下操作：

   - 所有活跃的 Secure Private Access 会话都将立即终止。
   - 将来禁止访问所有已发布的 Secure Private Access 应用程序。
   - 即使将用户添加到禁用用户列表后，仍允许通过 Citrix Enterprise Browser 访问 Internet。仅禁止访问已发布的“Secure Private Access”应用程序。
   - 7 天后，所有禁用用户将自动从禁用用户列表中删除。删除后，Secure Private Access 策略优先，访问权限将恢复。

您可以使用“清除所选内容”选项将用户从禁用用户列表中移除。

您可以使用“立即清除所有条目”选项将所有用户从禁用用户列表中移除。



> 建议：
>
> - 要无限期撤消用户的访问权限，请将该用户从相应的目录服务（例如 Active Directory）中移除，然后将其添加到禁用用户列表中。这将终止用户活跃的 Secure Private Access 会话，阻止将来的应用程序访问，一旦用户注销 Workspace，由于目录凭据处于非活动状态，用户将无法再次登录。
> - 7 天后，该用户将自动从禁用用户列表中删除，之后将恢复现有的 Secure Private Access 访问策略。如果您想延长访问封禁期限，请在 7 天后将该用户重新添加到列表中。

用户会话超时

January 9, 2024

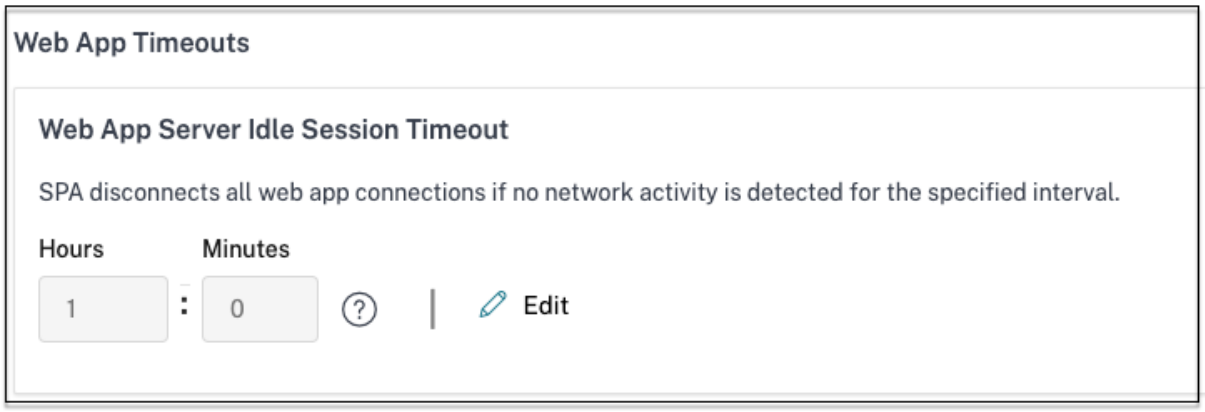
如果在指定时间段内没有网络活动，则可以为 Web 应用程序和 Citrix Secure Access 客户端与最终用户会话配置超时时间。

对于 Citrix Secure Access 客户端，您还可以将 Citrix Secure Access 客户端配置为在该指定时间段内没有用户活动时终止会话。此外，在配置的时间段到期后，无论用户和网络活动如何，您都可以在 Citrix Secure Access 客户端上配置强制断开连接。

Web 应用程序服务器的超时

1. 导航至“设置” **>** “超时”。
2. 在 **Web** 应用程序服务器空闲会话超时中，选择 Web 应用程序会话可以处于空闲状态的持续时间（以小时和分钟为单位）。如果会话保持空闲状态，则 Secure Private Access 服务将在此时间到期后终止会话。

   最短持续时间为 1 小时，最长持续时间可以为 168 小时。默认值为 2 小时。

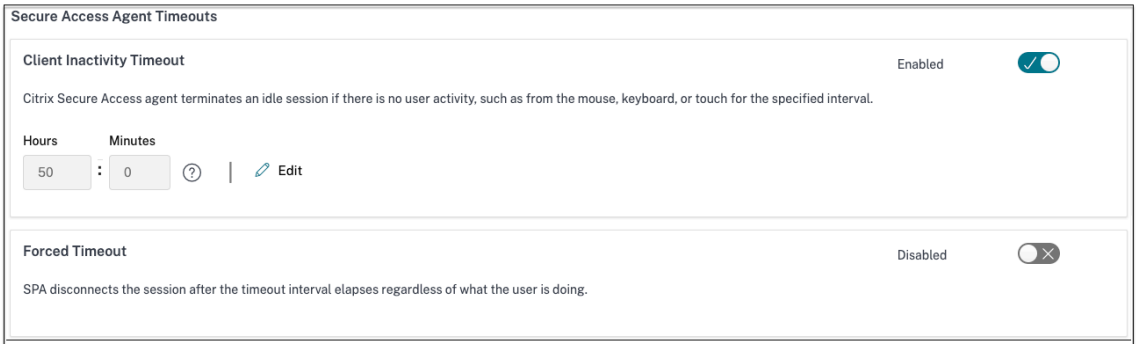


Citrix Secure Access 客户端的超时

您可以为 Citrix Secure Access 客户端配置以下超时：

- 客户端处于非活动状态
- 强制超时

1. 导航至“设置”**>**“超时”。



2. 在 **Secure Access Agent** 超时中，选择要强制执行的超时持续时间（以小时和分钟为单位）。

   - 客户端不活动超时：如果在配置的时间段内没有用户活动（鼠标或键盘），Citrix Secure Access 客户端终止会话的持续时间。默认情况下，此选项处于禁用状态。必须使用切换开关启用该选项才能强制执行配置的超时时间。但是，如果您在保存配置后禁用切换开关，客户端将不启动超时。

     最短持续时间为 5 分钟，最长持续时间为 168 小时。默认值为 8 小时。

   - 强制超时：无论用户或网络活动如何，Citrix Secure Access 客户端终止会话的持续时间。默认情况下，此选项处于禁用状态。必须使用切换开关启用该选项才能强制执行配置的超时时间。但是，如果您在保存配置后禁用切换开关，客户端将不启动超时。

     会话终止前 15 分钟会出现一条通知消息。

     最短持续时间为 1 小时，最长持续时间可以为 168 小时。默认值为 168 小时。

> 注意：
>
> 如果您启用其中多个设置，则第一个到期的超时间隔将关闭用户连接。

将应用程序安全控制和访问策略迁移到新的访问策略框架

January 9, 2024

Citrix 已对在产品中启用应用程序访问进行了更改。以前，应用程序需要订阅向导中应用程序 **>** 应用程序订阅者部分中的用户或用户组才能启用访问权限。今后，至少需要一个访问策略才能启用对应用程序的访问。创建策略时，用户或组条件是向用户授予应用程序访问权限必须满足的强制条件。有关详细信息，请参阅创建访问策略。

此外，应用程序配置中的 增强安全性部分已被弃用。现在，除了高级选项（如通过 Access Policies 在远程浏览器中打开应用程序）之外，您还可以实施精细的安全控制，例如剪贴板限制、下载限制、打印限制。通过此更改，客户可以根据用户、位置、设备、风险等上下文实施自适应安全性。

为了将应用程序的安全控制和访问策略迁移到新的访问策略框架并避免应用程序访问中出现任何停机，Citrix 进行了必要的更改。因此，您可能会注意到策略列表中出现了一些变化，例如：

- 新策略已创建
- 将单个策略拆分为多个策略
- 策略名称前缀为 <System generated policy - App name>

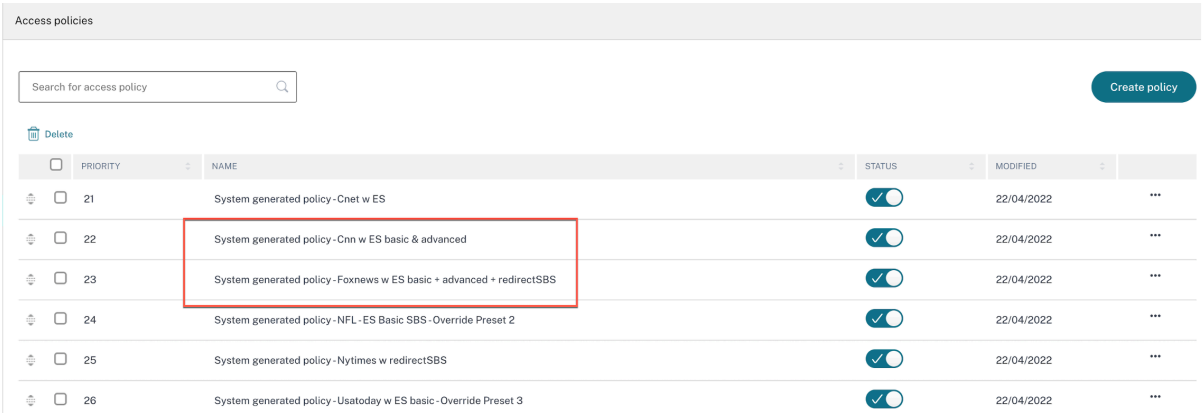
> 注意：
>
> 如果应用程序未添加用户或组，则不会创建新策略。

下表汇总了这些更改。

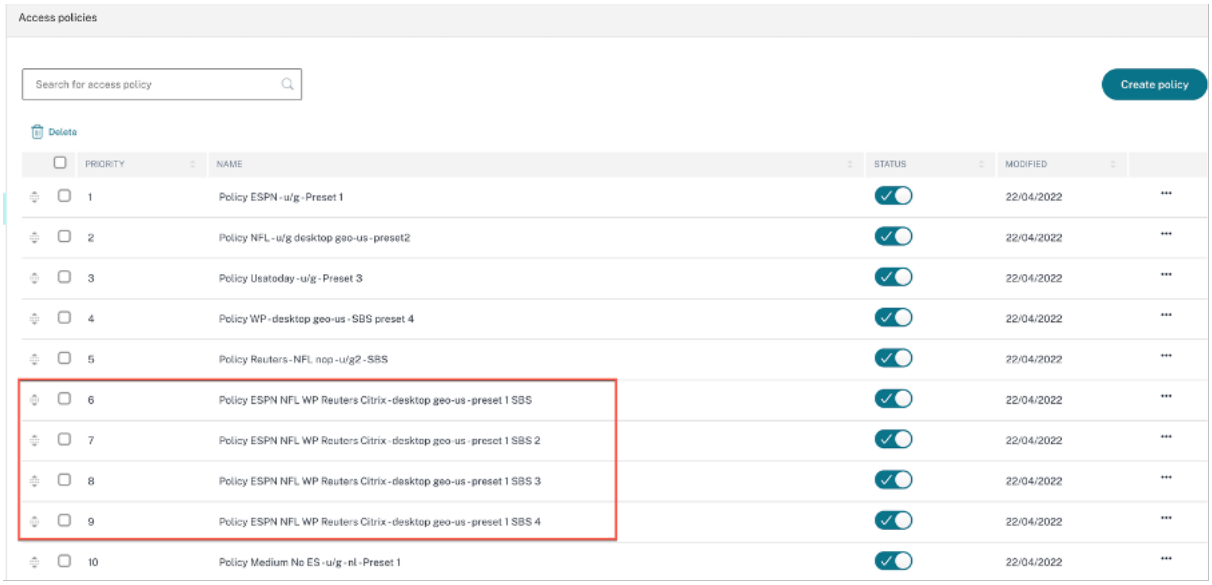
如果您已经配置了…	然后…
应用程序没有任何增强的安全条件	创建新策略，将用户和组作为强制性条件。用户或组源自访问策略。该操作设置为 允许访问。
具有增强安全条件的应用程序	创建新策略，将用户和组作为强制性条件。用户或组源自访问策略。该操作设置为 **Allow with restriction**（允许，但存在限制）。基于之前配置的应用程序级别安全条件。创建策略时会选择相应的安全限制。迁移的策略带有前缀 <System generated policy - App name>。
带预设的访问策略	如果策略已经选择了用户组条件，则会按原样创建新策略，并根据预设在访问策略中选择相应的安全条件。

如果您已经配置了…	然后…
没有用户或组条件的访问策略	由于用户或组是访问应用程序的强制条件，因此为多个应用程序配置的单个策略现在分为多个策略，因为每个应用程序可能有不同的用户或组集。用户或组源自访问策略。对于每个策略，都将用户或组设置为强制性条件。

下图显示了带有 <System generated policy - App name> 前缀的示例策略名称。



下图显示了将单个策略拆分为多个策略的示例。



使用模板配置应用程序

January 9, 2024

通过为常用 SaaS 应用程序配置模板列表，简化了在 Secure Private Access 服务上使用单点登录的 SaaS 应用程序配置。可以从列表中选择要配置的 SaaS 应用程序。

该模板预先填充了配置应用程序所需的大部分信息。但是，仍然必须提供特定于客户的信息。

> 注意：
>
> 以下部分介绍了要在 Secure Private Access 服务上执行的步骤，以便使用模板配置和发布应用程序。后续部分介绍了要在应用服务器上执行的配置步骤。

使用模板配置和发布应用程序

在 **Secure Private Access** 磁贴上，单击管理。

1. 单击“继续”，然后单击“添加应用程序”。

   > 注意：
   >
   > 继续按钮仅在您首次使用向导时出现。在后续用法中，您可以直接导航到应用程序页面，然后单击添加应用程序。

2. 在选择 模板列表中选择要配置的应用程序，然后单击 下一步。
3. 在应用程序详细信息部分中输入以下详细信息，然后单击保存。

   应用程序名称 -应用程序的名称。

   应用程序描述 -应用程序的简要描述。您在此处输入的描述将显示给工作区中的用户。

   应用程序图标—单击更改图标以更改应用程序图标。图标文件大小必须为 128x128 像素。如果不更改图标，则会显示默认图标。

   如果您不想显示应用程序图标，请选择不向用户显示应用程序图标。

   URL —包含您的客户 ID 的 URL。在以下情况下，用户将重定向到此 URL；
   - SSO 失败或
   - 不使用 **SSO** 选项。

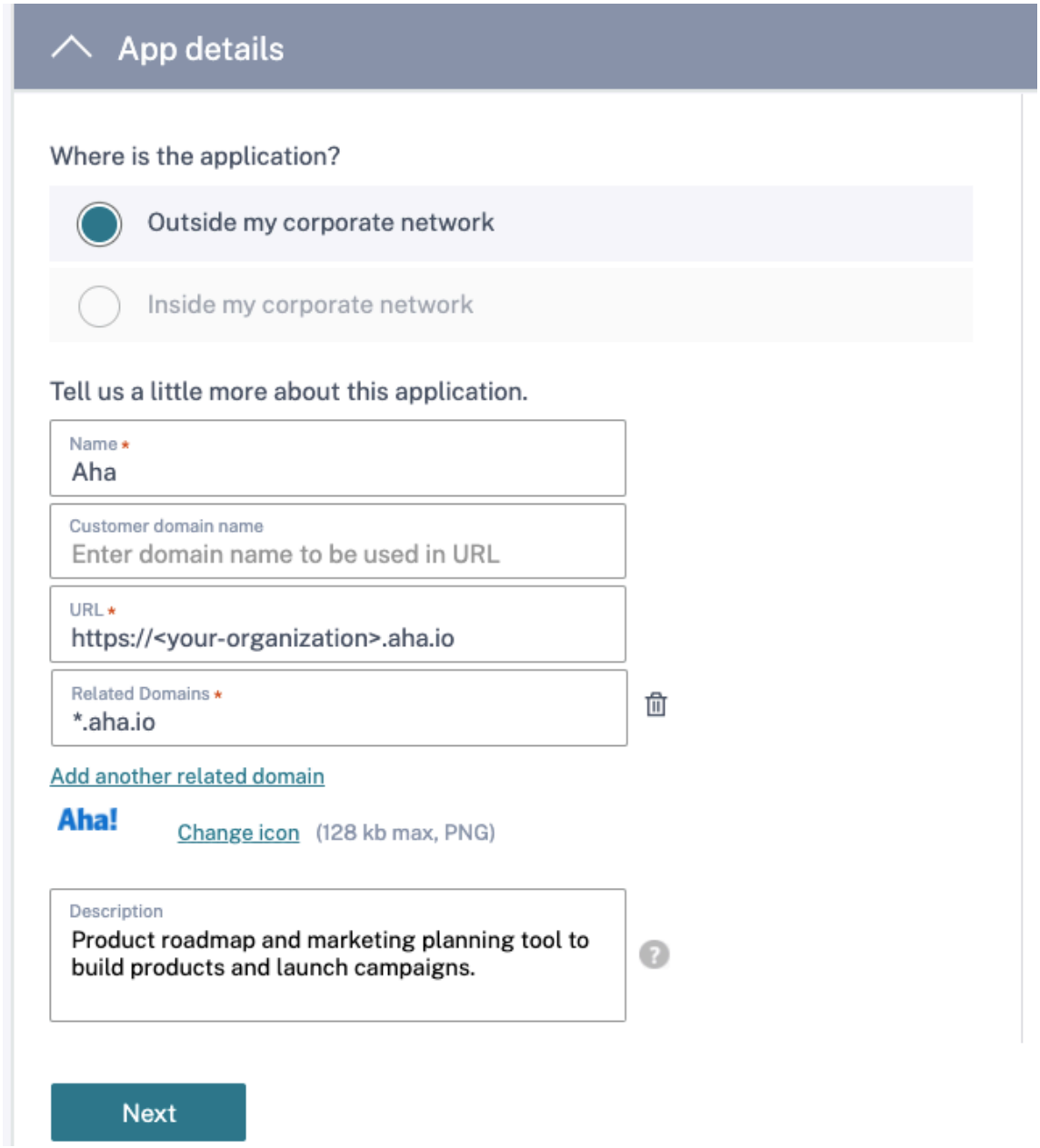
   客户域名 和 客户域 **ID** -客户域名和 ID 用于在 SAML SSO 页面中创建应用程序 URL 和其他后续 URL。

   例如，如果您要添加 Salesforce 应用程序，则您的域名为 `salesforceformyorg` 且 ID 为 123754，那么应用程序 URL 为 `https://salesforceformyorg.my.salesforce.com/?so=123754`.

   客户域名和客户 ID 字段特定于某些应用程序。

相关域—相关域将根据您提供的 URL 自动填充。相关域可帮助服务将 URL 识别为应用程序的一部分，并相应地路由流量。您可以添加多个相关域。

图标—单击 更改图标 可更改应用程序图标。图标文件大小必须为 128x128 像素。如果不更改图标，则会显示默认图标。



4. 在单点登录部分中输入以下 SAML 配置详细信息，然后单击保存。

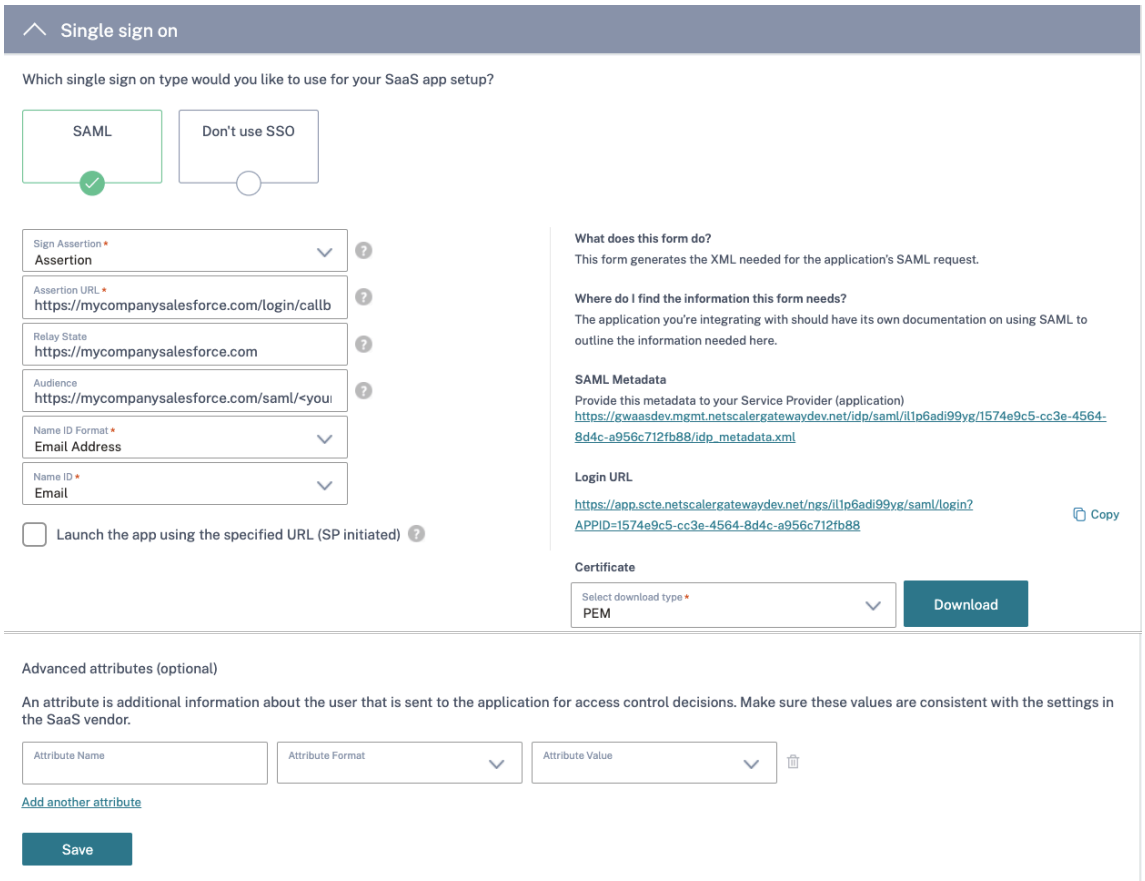
   断言 **URL** —应用程序供应商提供的 SaaS 应用程序 SAML 断言 URL。SAML 断言被发送到此 URL。

   中继状态—中继状态参数用于标识用户登录并定向到信赖方的联合服务器后访问的特定资源。中继状态为用户生成单个 URL。用户可以单击此 URL 登录到目标应用程序。

   受众—断言所针对的服务提供商。

名称 **ID** 格式—支持的用户格式类型。

名称 **ID** —用户格式类型的名称。



注意：

选中“不使用 **SSO**”选项后，用户将被重定向到“应用程序详细信息”部分下配置的 URL。

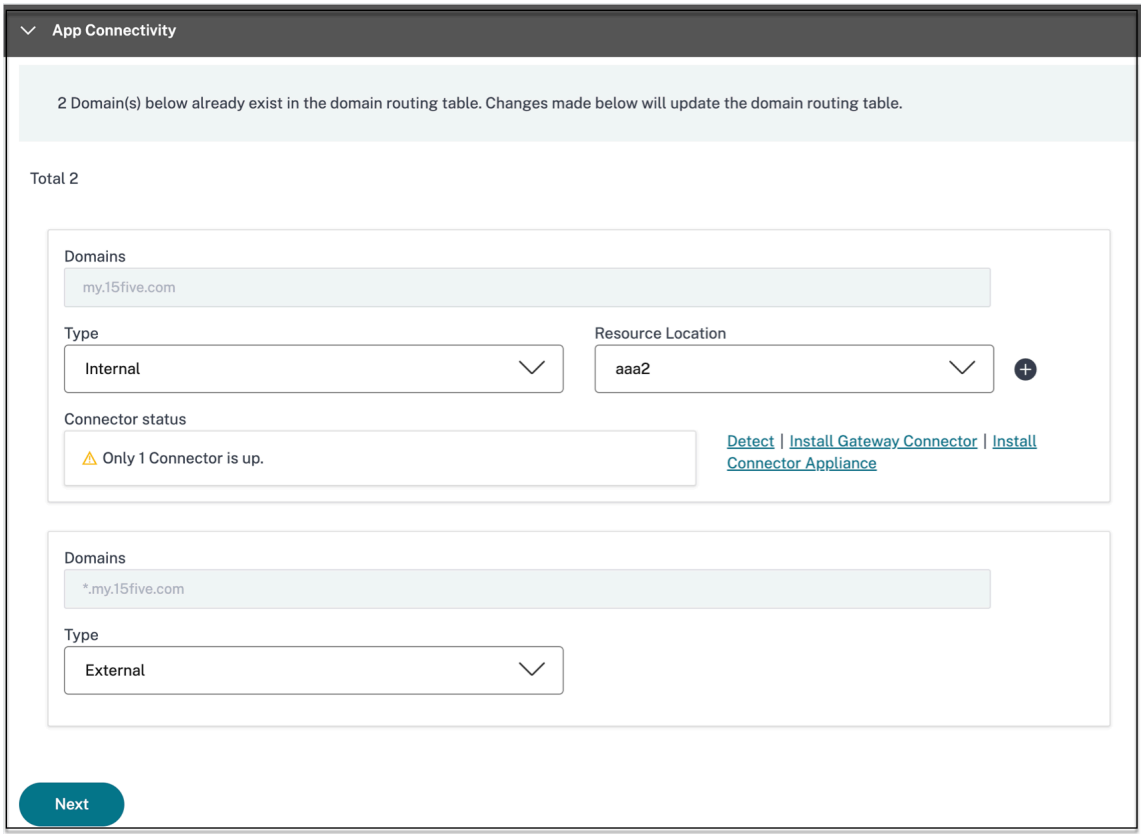
5. 单击 **SAML** 元数据下的链接下载元数据文件。使用下载的元数据文件在 SaaS 应用服务器上配置 SSO。

   注意：

   - 您可以复制登录 URL 下的 SSO 登录 **URL** ，并在 SaaS 应用程序服务器上配置 SSO 时使用此 URL。
   - 您还可以从证书列表中下载 证书，并在 SaaS 应用服务器上配置 SSO 时使用该证书。

6. 单击下一步。

7. 在应用程序连接部分中，如果必须通过 Citrix Connector Appliance 对应用程序的相关域进行外部或内部路由，则为应用程序的相关域定义路由。有关详细信息，请参阅在 SaaS 和 Web 应用程序中的相关域相同的情况下路由表以解决冲突。



8. 单击完成。

   单击完成后，该应用程序将添加到“应用程序”页面。配置应用程序后，可以从“应用程序”页面编辑或删除应用程序。为此，请单击应用程序上的省略号按钮，然后相应地选择操作。

   - 编辑应用程序
   - **Delete**

> 注意：
>
> 要向用户授予对应用程序的访问权限，管理员需要创建访问策略。在访问策略中，管理员添加应用程序订阅者并配置安全控制。有关详细信息，请参阅创建访问策略。

SaaS 应用服务器特定配置

January 9, 2024

以下是指向有关使用模板应用程序服务器特定配置的指南的文档的链接。Citrix 目前支持以下 SaaS 应用程序，并在不断增加对更多应用程序的支持。

- 15Five - 用于指导员工的持续绩效管理工具。

- 10000 ft - 规划增长的项目管理工具。
- 4me -用于内部、外部和外包团队之间协作的服务管理工具。
- Abacus - 实时费用报告软件。
- Absorb - 学习管理工具。
- Accompa - 用于构建产品的需求管理工具。
- Adobe Captivate Prime - 学习管理系统，可跨设备提供个性化的学习体验。
- Aha -用于构建产品和发布活动的产品路线图和营销规划工具。
- AlertOps -用于管理 IT 事件的协作事件响应工具。
- Allocadia -营销绩效管理工具，用于管理组织的营销计划流程。‘
- Ana plan -通过连接数据、人员和计划来帮助组织做出决策的规划工具。
- &frankly - 推动工作场所变革的参与工具。
- Anodot - 一个人工智能平台，可实时监视时间序列数据，检测异常情况并预测业务绩效。
- App Follow -用于加速全球应用增长并提高客户忠诚度的 产品管理工具。
- Assembla -用于软件开发的版本控制和源代码管理工具。
- Automox -用于跟踪、控制和管理修补过程的补丁管理工具。
- Azendoo -供团队交谈和协作的协作工具。
- BambooHR -用于管理员工数据的人力资源管理工具。
- Bananatag -跟踪和安排电子邮件、跟踪文件和创建电子邮件模板的工具
- Base CRM - 用于管理电子邮件、电话和笔记的销售管理工具。
- Beekeeper - 将多个操作系统和通信渠道集成到一个可从台式机和移动设备访问的 Secure Hub 中的工具。
- BitaBIZ - 用于休假和缺勤管理的缺勤和假期计划和沟通工具。
- BlazeMeter - 测试套件。
- Blissbook -用于创建员工手册的策略管理工具。
- BlueJeans -视频会议解决方案。
- Bold360 -用于客户互动的实时聊天工具。
- Bonusly -用于表彰团队贡献的员工认可和奖励管理工具。
- Box -用于管理、共享和访问内容的内容管理和文件共享工具。
- Branch - 一个支持深度链接和移动设备的移动链接平台。
- Brandfolder -用于存储和共享数字资产的数字资产管理工具。

- Breezy HR -招聘软件和申请人跟踪系统。
- Buddy Punch - 用于监视员工出勤的时间管理工具。
- Bugsnag -用于管理应用程序稳定性并报告错误和诊断数据的监视工具。
- Buildkite -持续集成软件开发的基础设施工具。
- Bullseye Locations - 用于在设备上定位商店或经销商的商店定位器工具。
- CA Flowdock-供团队交谈和协作的协作工具。
- CakeHR -用于出勤和绩效管理的人力资源管理工具。
- Cardboard - 用于跟踪混乱信息的协作产品规划工具。
- Citrix Cedexis -适用于大型网站的流量管理工具，可利用数据中心、云提供商和内容交付网络的多供应商采购。
- CipherCloud -为采用基于云的应用程序的企业提供端到端数据保护和高级威胁防护以及全面的合规功能的平台。
- Celoxis -用于创建项目计划、自动化工作和协作的项目管理工具。
- CircleHD -培训、学习和协作工具，用于在组织内共享视频和幻灯片。
- Circonus-用于提供警报、图表、仪表板和机器学习智能的数据分析和监视工具。
- Cisco Umbrella - 提供抵御 Internet 威胁的第一道防线的云安全平台。
- Citrix RightSignature - 一种以电子方式签名文档的解决方案。
- ClearSlide -销售互动工具，允许用户共享内容和销售材料以进行客户互动。
- Cloudability -云成本管理平台，用于提高云环境中的可见性、优化和治理能力。
- CloudAMQP -消息队列工具，用于在进程和其他系统之间传递消息。
- CloudCheckr -成本管理、安全、报告和分析工具，可帮助用户优化其 AWS 和 Azure 部署。
- CloudMonix -用于云和本地资源监视和自动化的工具。
- CloudPassage - 可见性和持续监视工具，可降低网络风险并保持合规性。
- CloudRanger -用于简化 AWS 云的备份、灾难恢复和服务器控制的工具。
- Clubhouse -用于软件开发的项目管理工具。
- Coggle -思维导图 Web 应用程序，用于创建分层结构的文档，如分支树。
- Comm100 -面向客户服务专业人员的客户服务软件和通信工具。
- Confluence-帮助团队协作和共享知识的内容协作工具。
- ConceptShare -校对工具，可以更快、更便宜地交付内容。
- Concur -差旅和费用管理工具，可随时随地管理费用。

- ConnectWise Control -提供远程支持和访问的业务管理工具。
- Contactzilla -用于访问最新联系信息的联系人管理工具。
- ContractSafe -用于跟踪、存储和管理合同的合同管理工具。
- Contentful -用于创建、管理内容并将内容分发到任何平台的软件。
- Convo -用于内部对话的团队沟通和协作工具。
- Copper - CRM 工具。
- Cronitor -用于 cron 作业的监视工具。
- Crowdin -为开发人员提供无缝和持续本地化的解决方案。
- Dashlane -还可以管理数字钱包的密码管理工具。
- Declare - 商务旅行的差旅和费用管理工具。
- Dell Boomi -用于连接云和本地应用程序和数据的集成工具。
- Deskpro -帮助台工具，用于促进票证管理、客户自助和客户反馈。
- Deputy - 劳动力管理工具，用于安排和跟踪员工的时间、任务和沟通。
- DigiCert -网站 SSL 证书的证书管理和故障排除工具。
- Dmarcian -用于过滤垃圾邮件、恶意软件和网络钓鱼的电子邮件监视工具。
- DocuSign -用于保险、医疗和房地产等不同文档的在线签名工具。
- DOME9 ARC-用于管理公共云环境的安全性和合规性工具。
- Dropbox -用于安全共享和存储文件的云存储工具。
- Duo -安全工具，用于提供对应用程序的安全访问。
- Dynatrace -医学实验室服务。
- Easy Projects - 项目管理工具。
- EdApp - 用于工作空间学习的学习管理工具。
- EduBrite -用于创建、交付和跟踪培训计划的学习管理工具。
- Ekarda -电子卡设计工具。
- Envoy - 用于管理人员和包的访客管理工具。
- Evernote -用于记笔记、整理、任务列表和存档的应用程序。
- Expensify -用于支出报告管理、收据跟踪和商务旅行的费用管理工具。
- ezeep -打印基础设施管理工具，可从任何设备、任何位置打印到云中的任何打印机。
- EZOfficeInventory -用于跟踪所有资产和设备的库存管理工具。

- EZRentOut -用于跟踪设备质量和可用性的设备租赁工具。
- Fastly -边缘云平台，用于为更接近用户的应用程序提供服务和保护。
- Favro -组织流程的规划和协作工具。
- Federated Directory - 跨公司联系人目录工具，用于搜索不同公司的公司通讯录。
- Feeder
- Feedly -新闻聚合工具，用于编译来自不同来源的新闻提要。
- FileCloud -为组织提供强大而安全的文件托管和共享平台的软件解决方案。
- Fivetran -帮助分析师将数据复制到云仓库的工具。
- Flatter Files -用于存放图纸和文档的数字平面文件柜，为访问内容提供安全而简单的方法。
- Float -用于项目安排和管理团队利用率的资源规划工具。
- Flock -协作工具。
- Formstack -一个在线表单生成器和数据收集工具。
- FOSSA -内置于 CI/CD 中的 自动开源许可证扫描和漏洞管理工具。
- Freshdesk -帮助支持客户需求的客户支持工具。
- Freshservice -用于简化 IT 运营的 IT 帮助台工具。
- FrontApp -协作工具，可在一个地方管理所有对话。
- Frontify -促进和简化日常品牌、营销和开发运营的平台。
- Fulcrum -移动数据收集平台，可让您轻松构建移动表单并收集数据。
- Fusebill -账单管理和定期计费软件。
- G-Suite -一套用于连接公司人员的智能应用程序。
- GetGuru - 知识管理软件。
- GitBook -用于创建和维护文档的工具。
- GitHub -一种基于 Web 的托管服务，用于使用 Git 控制在企业防火墙后面托管的仓库。
- GitLab -一个完整的 DevOps 平台，作为单个应用程序交付。
- GlassFrog -用于实践 Holacracy 的软件。
- GoodData -嵌入式商业智能和分析平台，提供快速、可靠且易于使用的分析
- GotoMeeting -具有高清视频会议功能的在线会议软件。
- HackerRank -为消费者和企业提供具有竞争力的编程挑战。
- HappyFox -在线帮助台软件和基于 Web 的支持票系统。

- Helpjuice -用于创建和维护知识库的知识管理解决方案。
- Help Scout - 面向客户服务专业人员的客户服务软件和知识库工具。
- Hello sign -电子签名界面，可随时随地在任何设备上启用签名。
- HelpDocs-知识库软件，用于在用户卡住时引导他们。
- Honeybadger -应用程序健康监视工具。
- Harness - 用于持续交付和集成 Java、AWS、GCP、Azure 和裸机中的.NET 应用程序的工具。
- HelpDocs -用于创建权威知识库的工具，用于在用户陷入困境时为其提供指导。
- Helpmonks -用于团队协作的协作电子邮件平台。
- Hoshinplan -在一个画布中可视化战略计划和跟踪状态的工具。
- Hosted Graphite - 用于监视您的网站、应用程序、服务器和容器性能的工具。
- Humanity - 在线员工排程软件，用于管理轮班、日程安排、工资单和时间计时。
- Igloo -数字化工作场所和内联网解决方案提供商，可解决整个组织的 IT 挑战。
- iLobby - 基于云的访客注册管理解决方案。
- Illumio -防止漏洞在数据中心和云环境中传播的安全系统。
- Image Relay -用于安全组织和共享数字文件的数字资产管理和品牌管理软件。
- Informatica -用于 SaaS 应用程序集成的工具，以及用于开发和部署自定义集成服务的平台。
- Intelligent contract - 合同管理软件。
- iMeet Central -面向营销人员、创意机构和企业企业的项目管理软件。
- InteractGo -用于测量系统性能的实时和历史数据的工具。
- iQualify One -提供真实学习体验的学习和管理工具。
- InsideView-用于解决销售、营销和其他业务挑战的数据和智能解决方案。
- Insightly -面向中小型企业的基于云的客户关系管理 (CRM) 和项目管理工具。
- ITGlue -基于云的 IT 文档平台，可帮助 MSP 标准化文档、创建知识库、管理密码和跟踪设备。
- Jitbit -帮助台软件和票务系统，用于管理和跟踪传入的支持请求电子邮件及其相关票证。

JupiterOne -用于创建和管理整个安全流程的软件平台。

- Kanbanize -用于精益管理的在线投资组合看板软件。
- Klipfolio -一个在线仪表板平台，用于为您的团队或客户构建强大的实时业务仪表板。
- Jira -用于规划、跟踪和管理问题和项目的工具。
- Kanban Tool - 可视化管理软件，可提高团队绩效并提高生产力。

- Keeper Security -密码管理器和安全软件来保护您的密码和私人信息。
- Kentik -将大数据应用于网络和性能监视、DDoS 防护和实时临时网络流量分析的工具。
- Kissflow -工作流工具和业务流程工作流管理软件，可自动执行工作流程。
- KnowBe4 -提供安全意识培训和模拟网络钓鱼的工具。
- KnowledgeOwl -知识库和创作工具。
- Kudos - 零售、工作、项目和履行流程系统。
- LaunchDarkly -功能管理平台，使开发和运营团队能够控制功能生命周期。
- Lifesize -视频会议解决方案。
- Litmos -用于员工培训、客户培训、合规培训和合作伙伴培训的学习管理系统。
- LiquidPlanner -适用于您企业的在线项目管理软件。
- LeanKit -基于精益的企业流程和工作管理软件，可帮助企业可视化工作、优化流程并加快交付速度。
- LiveChat -面向企业的实时聊天和帮助台软件。
- LogDNA -在一个集中式日志记录工具中收集、监视、解析和分析来自所有来源的日志的工具。
- Mango -团队协作软件，用于将孤立的应用程序整合和简化到一个平台中。
- Manuscript -一种书写工具，可帮助您规划、编辑和分享您的作品。
- Marke of-帮助营销团队掌握数字营销的艺术和科学的自动化软件。
- Matomo -一个网络分析平台，用于评估访问网站的每个人的整个用户旅程。
- Meisterplan -帮助组织创建项目组合的软件。
- Mingle -一种敏捷的项目管理和协作工具，可为整个团队提供一个组合的工作场所。
- MojoHelpdesk -帮助台软件和票务系统。
- Monday - 团队管理软件可在一个工具中规划、跟踪和协作所有工作。
- Mixpanel -用于跟踪用户与网络和移动设备互动的系统。
- MuleSoft -集成软件，用于连接云端和本地的 SaaS 和企业应用程序。
- MyWebTimesheets -在线时间跟踪系统，用于跟踪花费在各种项目/工作/活动上的时间。
- New Edge -面向混合 IT 的安全应用程序网络服务。
- NextTravel -公司差旅管理软件工具。
- N2F -费用报告管理工具，用于管理您的业务和差旅费用。
- New Relic -用于衡量和监视应用程序和基础设施性能的数字智能平台。
- Nmbrs -面向企业的云人力资源和薪资软件。

- Nuclino -用于实时协作和共享信息的协作软件。
- Office365 - Microsoft 基于云的订阅服务。
- OfficeSpace - 基于云的平台，帮助组织分配工作
- OneDesk -项目管理和帮助台软件，可与客户建立联系并为其提供支持。
- OpsGenie -DevOps 和 IT 运营团队的事件管理平台，用于简化警报和事件解决流程。
- Orginio -一种在线组织结构图创建工具，用于可视化组织结构。
- Oomnitza -用于跟踪和管理资产的 IT 资产管理平台解决方案。
- OpenEye -用于在 Apex 录像机上查看实时和录制的视频的移动应用程序
- Oracle ERP Cloud - 基于云的软件应用程序套件，用于管理企业功能。
- Pacific Timesheet - 基于 Web 的工时表工具，用于工资单、项目时间和费用。
- PagerDuty -数字化运营管理系统。
- PandaDoc -一款适用于 iPhone 用户的移动应用程序，可直接在手机上访问其文档、分析和仪表板。
- Panopta -基础设施监视工具。
- Panorama9 -基于云的 IT 管理平台，用于企业网络监视。
- Papyrs -用于设计自己的内部网页面的编辑器。
- ParkMyCloud -用于连接到 AWS、Azure 服务或 GCP 的单一用途 SaaS 工具。
- Peakon -衡量和提高员工敬业度的工具。
- People HR - 适用于所有关键人力资源职能的 HR 软件系统。
- Pingboard -用于构建组织团队和劳动力规划的组织结构图的工具。
- Pigeonhole Live -互动问答平台。
- Pipedrive -销售 CRM 和管道管理软件。
- PlanMyLeave -休假管理系统，用于管理和跟踪员工的请假。
- PlayVox -客户服务质量监视工具。
- Podbean -播客服务提供商。
- Podio -一种基于 Web 的工具，用于在项目管理工作区中组织团队沟通、业务流程、数据和内容。
- POPin -人群解决平台和移动应用程序，可操作团队参与以解决问题
- Postman -API 开发环境。
- Presscreen -申请人跟踪工具，用于在线和离线发布职位空缺。
- ProductBoard -产品管理工具。

- ProdPad-用于制定产品策略的产品管理软件。
- Proto.io -应用程序原型设计平台，用于创建完全交互式的高保真原型。
- Proxyclick - 基于云的访客管理解决方案，用于管理访客，建立他们的品牌形象并确保安全。
- Pulumi -适用于容器、无服务器、基础设施和 Kubernetes 的云原生开发平台。
- PurelyHR -用于访问员工休假数据的休假管理工具。
- Promapp-业务流程管理（BPM）工具。
- Presscreen - 基于云的申请人跟踪系统，用于在线和离线发布职位空缺。
- QAComplete - 软件测试管理工具。
- Qualaroo -从客户那里获得见解的反馈工具。
- Quality Built, LLC - 保险、金融和建筑行业，提供可靠和创新的第三方质量保证服务。
- Qubole -基于 Amazon 构建的用于大数据分析的自助平台。
- Questetra BPM Suite -基于 Web 的业务流程平台，用于常规工作流程。
- QuestionPro -用于创建调查和问卷的在线调查软件。
- Quandora -基于问答的知识管理解决方案。
- Quip -适用于移动和 Web 的协作生产力软件套件。
- Rackspace -托管云计算服务。
- ReadCube -用于 Web、桌面和移动参考资料管理的工具。
- RealtimeBoard -白板协作工具，组织可以在格式、工具、位置和时区之外进行协作。
- Receptive - 在一个地方收集来自客户、团队和市场的反馈的工具。
- Remedyforce - IT 服务管理和帮助台系统。
- Rtrace -一种应用程序性能管理工具，可提供错误跟踪、数据聚合和自动警报。
- Robin -用于安排会议室和办公桌预订的工作场所体验工具。
- Rollbar -面向开发人员的实时错误警报和调试工具。
- Really Simple Systems - 基于云的 CRM 软件，适用于小型企业管理销售和营销。
- Reamaze -客户支持软件，可在单个平台上通过聊天、社交、短信、常见问题解答和电子邮件支持、吸引和转化客户。
- Resource Guru - 用于安排人员、设备和其他资源的资源管理软件。
- Rtrace-应用程序性能管理，用于集成代码分析、错误跟踪、应用程序日志和指标。
- Roadmunk -用于创建产品路线图的产品路线图软件和路线图工具。

- Runscope -用于创建、管理和运行功能性 API 测试和监视器的工具。
- Salesforce —用于管理客户联系信息、集成社交媒体并促进实时客户协作的 CRM 工具。
- SalesLoft -销售互动平台，可实现高效和增加收入的销售
- Salsify -产品体验管理（PXM）平台。
- Samanage -用于 IT 服务管理的工具。
- Samepage -用于管理在线项目的协作软件。
- Screencast-O-Matic —用于截屏和编辑视频的工具。
- ScreenSteps —创建以屏幕截图为中心的可视文档的工具。
- SendSafely —用于安全交换文件和电子邮件的加密平台。
- Sentry -开源错误跟踪软件。
- ServiceDesk Plus -IT 服务台的工具。
- ServiceNow -用于创建数字工作流程的云平台。
- SharePoint —用于文档管理和存储的协作平台。
- Shufflrr -用于创建、更新、共享和广播演示文稿的演示文稿管理工具。
- Sigma Computing —一种用于探索、分析和可视化数据的分析工具。
- Signavio —一种业务流程建模工具。
- Skeddly -用于自动化 AWS 资源的工具。
- Skills Base - 用于跟踪和记录员工绩效和技能的人才管理工具。
- Skyprep -用于培训客户和员工的学习管理系统（LMS）。
- Slack -用于交流和共享信息的协作工具。
- Slemma -用于从多个数据集创建数据报告的数据分析工具。
- Sli.do -用于会议、活动和会议的交互工具。
- SmartDraw -用于制作流程图、组织图、思维导图、项目图表和其他商业视觉对象的图表工具。
- SmarterU -用于培训客户和员工的学习管理系统（LMS）。
- Smartsheet -用于分配任务、跟踪项目进程、管理日历和共享文档的协作工具。
- SparkPost - 电子邮件投递服务。
- Split - 账单拆分申请。
- Spoke - 用于提交服务票证的服务台工具。
- Spotinst - 一个 SaaS 优化平台，可帮助公司购买和管理云基础设施容量。

- SproutVideo -托管商业视频的平台。
- Stackify -故障排除工具，通过包括前缀和回溯在内的一套工具提供支持。
- StatusCast - 托管页面，让您的员工和客户了解停机时间和网站维护情况。
- StatusDashboard - 用于托管状态仪表板和向客户广播事件通知的通信平台。
- Status Hero - 用于跟踪球队状态更新和每日进球的工具。
- StatusHub -托管服务状态页面的平台。
- Statuspage - 用于传达状态和事件的工具。
- SugarCRM -适用于 Salesforce 自动化、营销活动、客户支持、协作、移动 CRM、社交 CRM 和报告的 CRM 工具。
- Sumo Logic -专注于安全性、运营和 BI 用例的数据分析软件。
- Supermood -用于实时收集员工反馈的人力资源平台。
- Syncplicity -用于共享和同步文件的工具。
- Tableau -用于创建交互式数据可视化的工具。
- TalentLMS -学习管理系统（LMS），用于促进在线研讨会，课程和其他培训计划。
- Tallie —用于捕获和上载收据、生成支出报告以及自定义支出详细信息的工具。
- Targetprocess -适用于 Scrum、看板、SAFe 等的敏捷项目管理软件。
- Teamphoria -提供实时员工敬业度指标、员工评论和认可的软件。
- TeamViewer -用于远程控制、桌面共享、在线会议、网络会议和计算机之间文件传输的专有软件应用程序。
- Tenable.io -提供数据以识别、调查和优先修复 IT 环境中的漏洞和错误配置的工具。
- Testable - 用于创建行为实验和调查的工具。
- TestingBot -为实时和自动测试提供各种浏览器版本的工具。
- TestFairy -移动测试平台，为公司提供移动会话的视频录制、日志和崩溃报告。
- TextExpander -通信工具，用于在键入时插入电子邮件存储库中的文本片段和其他内容。
- TextMagic -用于与客户联系的消息传递服务。
- ThousandEyes - 用于监视网络基础设施、排查应用程序交付故障和绘制互联网性能的工具
- Thycotic Secret server - 用于管理密码的帐户管理软件工具。
- TimeLive —提供时间表和跟踪时间的工具。
- Tinfoil Security -用于检查漏洞的安全解决方案软件。
- Tisotech -允许客户发现、建模和分析其数字化企业的工具。
- Trumba -用于发布在线、交互式活动日历的工具。

- TwentyThree -视频营销平台，用于将视频集成并添加到营销堆栈中。
- Twilio -一个用于通信的开发人员平台。
- Ubersmith -用于基于使用情况的计费、报价、订单管理、基础设施管理和服务台票务解决方案的业务管理软件。
- UniFi -具有语音、Web 协作和视频会议功能的通信和协作软件。
- UPTRENDS —用于跟踪网站正常运行时间和性能的网站监视
- UserEcho -社区论坛工具，可帮助企业管理客户反馈。
- UserVoice -产品反馈管理软件，使企业能够做出数据驱动的产品决策。
- VALIMAIL -用于验证合法电子邮件并阻止网络钓鱼攻击的电子邮件身份验
- Veracode -源代码分析器和代码扫描程序可保护企业免受网络威胁和应用程序后门的侵害。
- Velpic -旨在简化工作场所培训的学习管理系统（LMS）。
- VictorOps - 事件管理软件，用于提供 DevOps 可观察性、协作和实时警报。
- VIDIZMO -企业直播和点播视频流软件。
- Visual Paradigm -用于团队协作的可视化建模和图表绘制在线平台。
- Vtiger -CRM 工具，使销售，支持和营销团队能够组织和协作。
- WaveMaker —用于构建和运行自定义应用的软件。
- Weekdone -为公司创建经理仪表板和团队管理服务的工具。
- Wepow -通过移动和视频面试解决方案连接招聘人员、求职者和雇主的工具。
- When I Work - 用于员工安排和时间跟踪的工具。
- WhosOnLocation —用于跟踪人员通过站点和区域的流量的工具。
- Workable - 申请人跟踪系统。
- Workday -用于财务管理、人力资源和规划的工具。
- Workpath -管理组织目标和绩效的工具。
- Workplace - Facebook 的协作工具，帮助员工通过熟悉的界面进行交流。
- Workstars -社交和同伴员工认可计划的平台。
- Workteam -用于跟踪员工时间和出勤的工具。
- Wrike -社交项目管理和协作软件。
- XaitPorter -用于投标和建议书以及其他商业文档的文档共同创作软件。
- Ximble -用于员工安排和时间跟踪的工具。
- XMatters -具有警报软件的协作平台，该软件与其他工具集成，可创建无缝流程和有效的沟通。

- Yodeck -通过网络或移动设备远程管理屏幕的工具。
- Zendesk -用于请求客户服务和记录支持票证的软件。
- Ziflow -创意制作团队的工具。
- Zillable —具有通信功能的协作平台。
- Zing tree -用于创建交互式决策树和故障排除程序的工具包。
- ZIVVER -允许从您熟悉的电子邮件程序安全传输电子邮件和文件的工具。
- Zoho -业务应用程序套件。
- Zoom-具 有语音、网络协作和视频会议功能的通信和协作软件。
- Zuora -一种基于订阅的软件，使公司能够启动、管理和转型为订阅业务。

启动已配置的应用程序 - 最终用户工作流

January 9, 2024

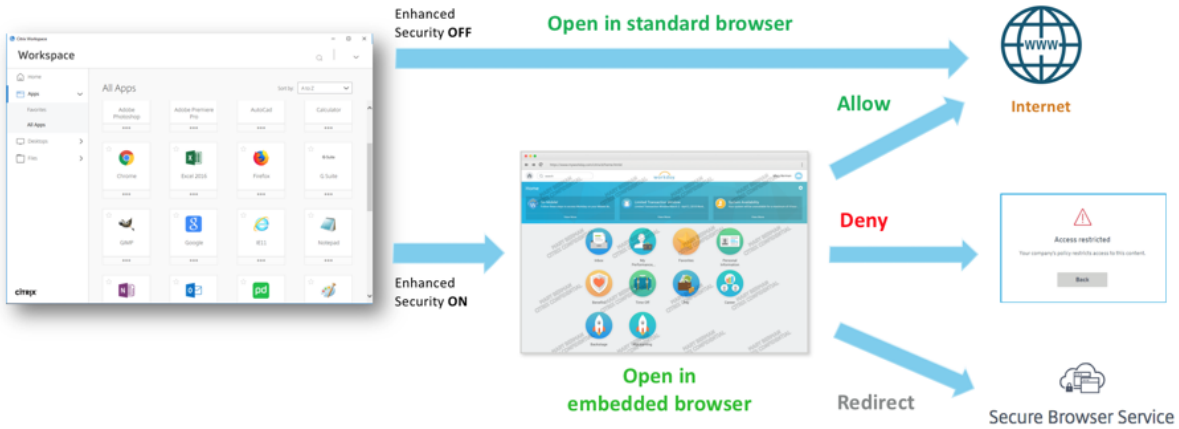
作为最终用户，您必须执行以下操作：

1. 从 https://www.citrix.com/downloads 下载 Citrix Workspace 应用程序。在“查找下载”列表中，选择 **Citrix Workspace** 应用程序。
2. 登录并搜索您的 SaaS 应用程序。单击该应用程序以启动它。

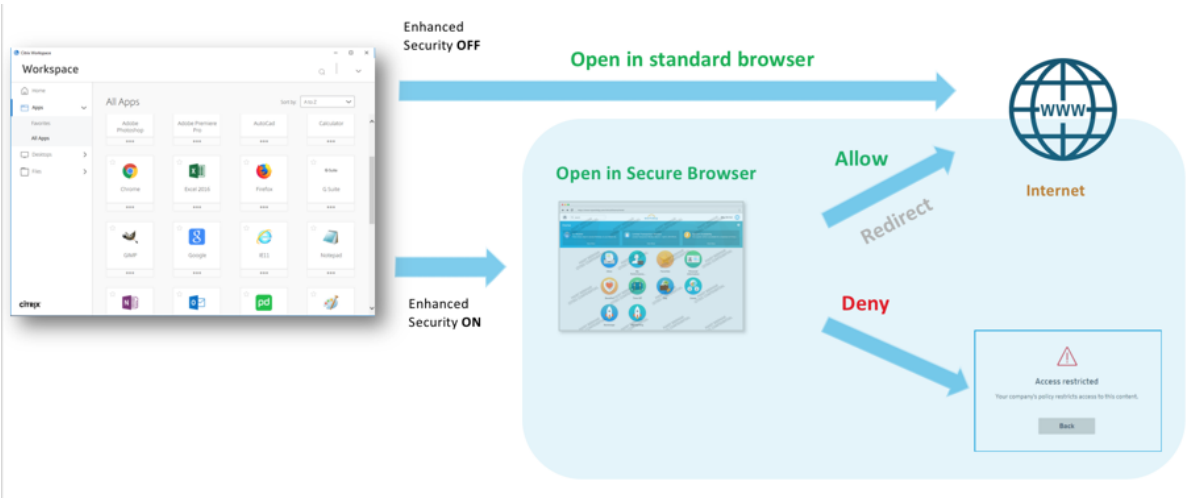
现在，您可以在 Citrix Workspace 应用程序中或 Citrix Workspace Web 门户中使用 SaaS 应用程序。

根据管理员配置的设置，您的 SaaS 应用程序会在 Workspace 应用程序中使用浏览器引擎打开，或者您将被重定向到安全浏览器。

下图显示了 Citrix Workspace 应用程序的高级流程。



下图显示了 Citrix Workspace Web 门户的高级流程。



管理员对 **SaaS** 和 **Web** 应用程序的只读访问权限

January 9, 2024

组织通常由多个管理员组成，必须向管理员提供不同级别的访问权限。使用 Secure Private Access 服务的安全管理员团队可以提供精细控制，例如对管理员的只读访问权限。可以向不添加或修改应用程序的管理员提供只读访问权限，以查看应用程序详细信息。具有只读访问权限的 Secure Private Access 服务管理员无法执行以下任务。

- 添加企业 Web 或 SaaS 应用程序。
- 在现有或新的资源位置添加新的 Connector Appliance。

如何为管理员提供只读访问权限

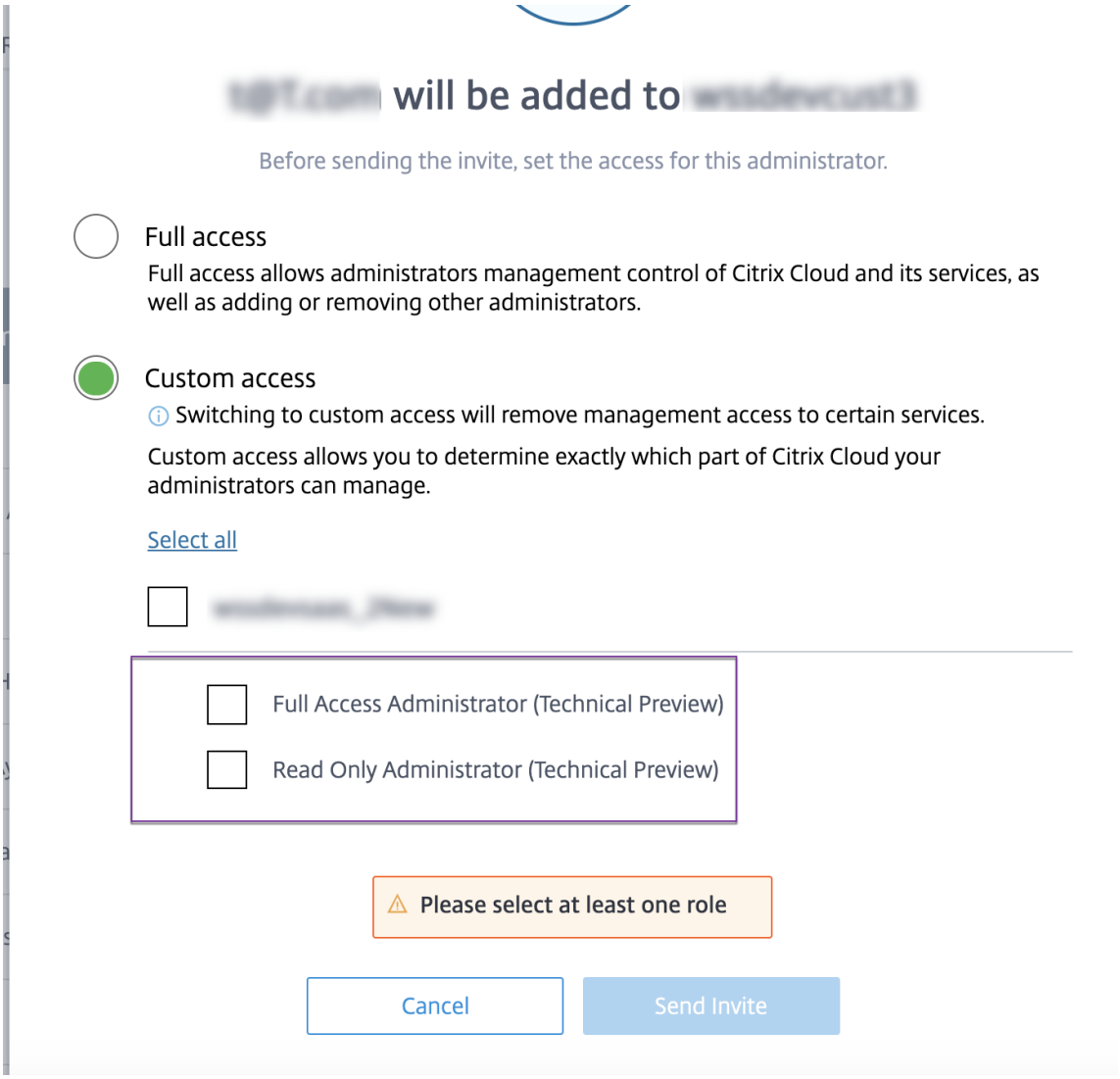
登录 Citrix Cloud 后，从菜单中选择身份和访问管理。
在“身份和访问管理”页面上，单击“管理 员”。控制台将显示帐户中当前的所有管理员。

添加具有只读访问权限的管理员

1. 在添加管理员中，选择要从中选择管理员的身份提供商。有时，Citrix Cloud 可能会提示您先登录身份提供程序（例如 Azure Active Directory）。
2. 如果选择了 **Citrix Identity**（Citrix 身份），请输入用户的电子邮件地址，然后单击 **Invite**（邀请）。
3. 如果选择了 Azure Active Directory，请键入要添加的用户的名称，然后单击“Invite”（邀请）。
4. 选择 **Custom access**（自定义访问权限）。此时将显示以下选项：

- 选择完全访问权限管理员（技术预览版）—提供完全访问权限。
- 只读管理员（技术预览版）—提供只读访问权限。

5. 选择 只读管理员（技术预览版）。



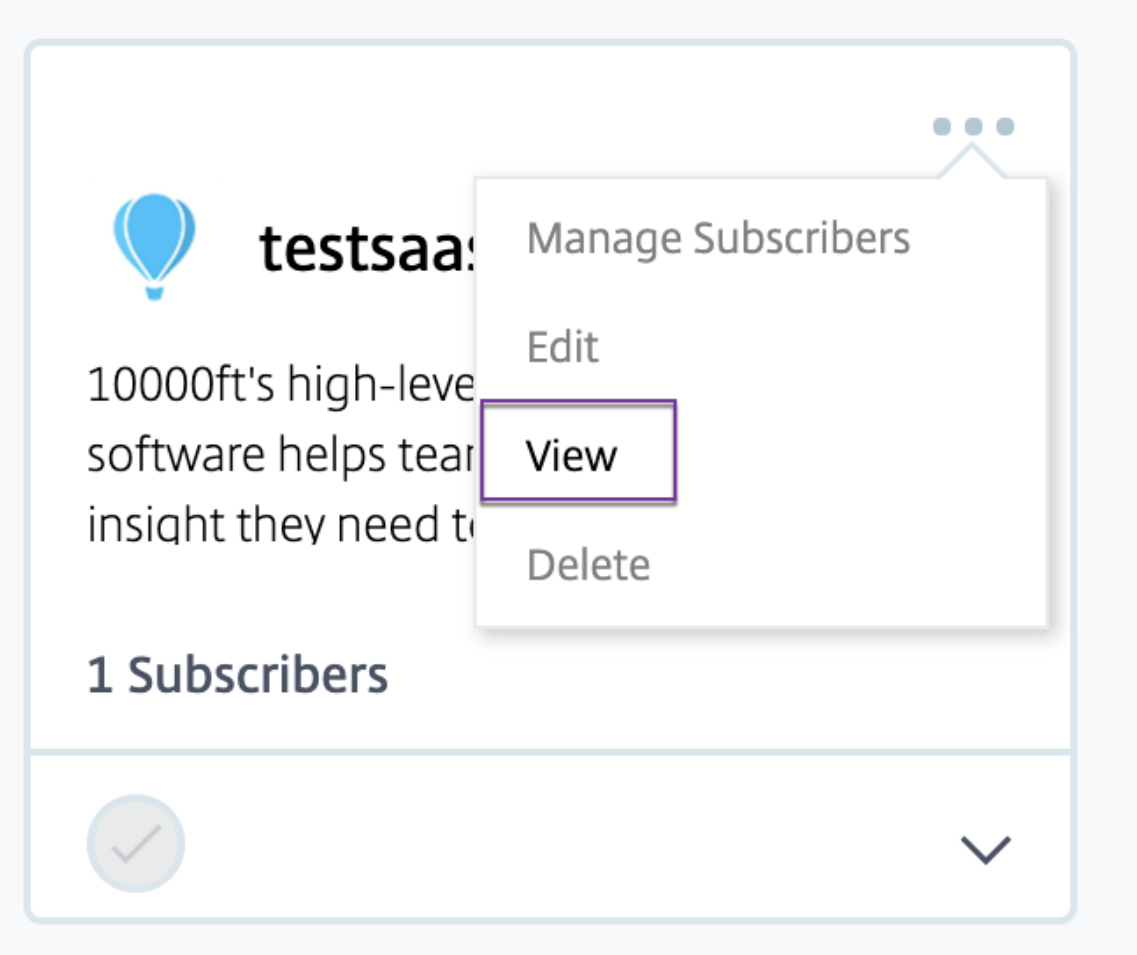
6. 单击发送邀请。

> 重要：
>
> - 向 Citrix Gateway 服务管理员提供只读管理员访问权限时，还必须从常规管理列表中为这些管理员启用库。只有这样，才能为管理员启用应用程序的查看选项。
> - 对于具有只读管理员访问权限的用户，添加 **Web /SaaS** 应用程序按钮已禁用。

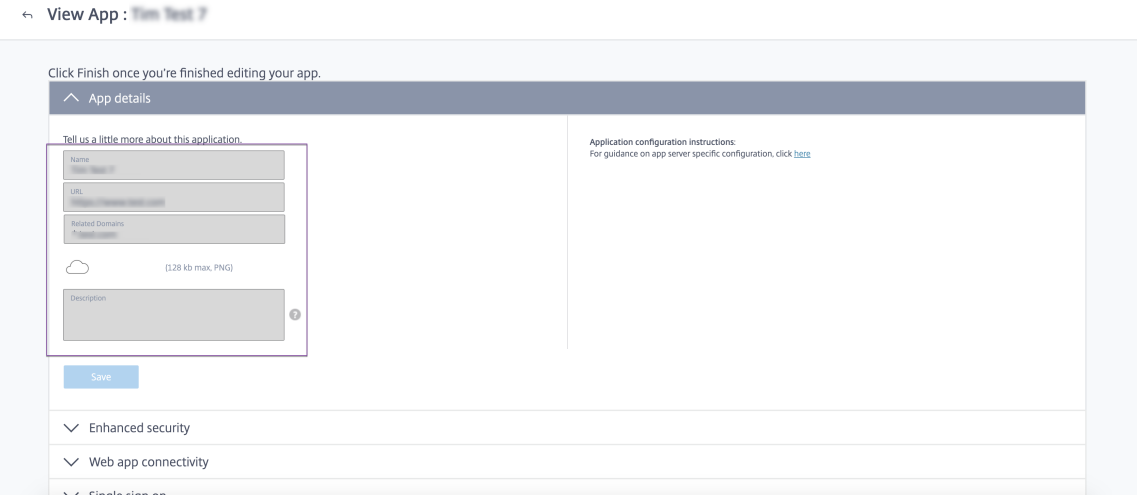
在管理员具有只读访问权限时查看应用详细信息

1. 登录 Citrix Cloud 后，从菜单中选择 资源库。

2. 选择要查看详细信息的应用程序，然后单击 省略号。
   仅启用“查看”选项。所有其他选项都已禁用。



3. 单击“查看”。



Web 和 SaaS 应用程序配置的最佳实践

June 19, 2024

已发布和未发布应用程序的应用程序访问权限取决于在 Secure Private Access 服务中配置的应用程序和访问策略。

在 Secure Private Access 中访问已发布和未发布的应用程序

- 访问已发布的 **Web** 应用程序和相关域：
  - 当最终用户访问与已发布的 Web 应用程序关联的 FQDN 时，只有在为用户明确配置了访问策略“允许”或“有限制地允许”操作时，才允许访问。

    > 注意：
    >
    > 建议不要让多个应用程序共享同一个应用程序 URL 域或相关域以实现精确匹配。如果多个应用程序共享同一个应用程序 URL 域或相关域，则将根据精确的 FQDN 匹配和策略优先级提供访问权限。有关详细信息，请参阅访问策略匹配和优先级。

  - 如果没有任何访问策略与已发布的应用程序相匹配，或者应用程序与任何访问策略均不关联，则默认情况下，对该应用程序的访问将被拒绝。有关访问策略的详细信息，请参阅访问策略。
- 访问未发布的内部 **Web** 应用程序和外部 **Internet URL**：

  为了启用零信任，Secure Private Access 拒绝访问与应用程序无关且未为应用程序配置访问策略的内部 Web 应用程序或内联网 URL。要允许特定用户访问，请确保为 Intranet Web 应用程序配置了访问策略。

  对于未在 Secure Private Access 中配置为应用程序的任何 URL，流量会直接流向 Internet。

  - 在这种情况下，对内联网 Web 应用程序 URL 域的访问将直接路由，因此访问会被拒绝（除非用户已经在内联网内）。
  - 对于未发布的 Internet URL，访问权限基于为未经批准的应用程序（如果启用）配置的规则。默认情况下，在 Secure Private Access 中允许此访问。有关详细信息，请参阅为未经批准的网站配置规则。

访问策略匹配和优先级排序

Secure Private Access 在匹配应用程序以获得访问权限时执行以下操作：

1. 将正在访问的域名与应用程序 URL 的域名或相关域进行匹配以获得精确匹配。
2. 如果找到配置了完全匹配的 FQDN 的 Secure Private Access 应用程序，则 Secure Private Access 将评估为该应用程序配置的所有策略。
   - 策略按优先顺序进行评估，直到用户上下文匹配为止。操作（允许/拒绝）是根据优先顺序匹配的第一个策略应用的。

- 如果没有任何策略匹配，则默认情况下访问会被拒绝。

3. 如果找不到精确的 FQDN 匹配项，则 Secure Private Access 会根据最长匹配项（例如通配符匹配）对域进行匹配，以查找应用程序和相应的策略。

   示例 **1**：考虑以下应用程序和策略配置：

应用程序	应用程序 URL	相关域
Intranet	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

策略名称	优先级	用户和关联应用程序
PolicyA	高	Eng-User5（内联网）
PolicyB	低	HR-User4 (Wiki)

   如果 `HR-User4` 访问 `app.intranet.local`，则会发生以下情况：

   a) Secure Private Access 会在所有策略中搜索与正在访问的域名完全匹配的内容，在这种情况下为 `app.intranet.local`。
   b) Secure Private Access 会查找 `PolicyA` 并检查条件是否匹配。
   c) 由于条件不匹配，Secure Private Access 在此停止，不会继续检查通配符是否匹配，尽管 `PolicyB` 本来可以匹配（因为在 Wiki 应用程序的相关域 `*.intranet.local` 中 `app.intranet.local` 确实匹配）并给出了访问权限。
   d) 因此 `HR-User4` 被拒绝访问维基应用程序。

   示例 **2**：考虑以下应用程序和策略配置，其中在多个应用程序中使用同一个域：

应用程序	应用程序 URL	相关域
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

策略名称	优先级	用户和关联应用程序
PolicyA	高	Eng-User5 (App1)
PolicyB	低	HR-User7 (App2)

当用户 `Eng-User5` 访问时 `app.intranet.local`，App1 和 App2 都将根据精确的 FQDN 匹配进行匹配，因此 `Eng-User5` 用户可以通过 `PolicyA` 进行访问。

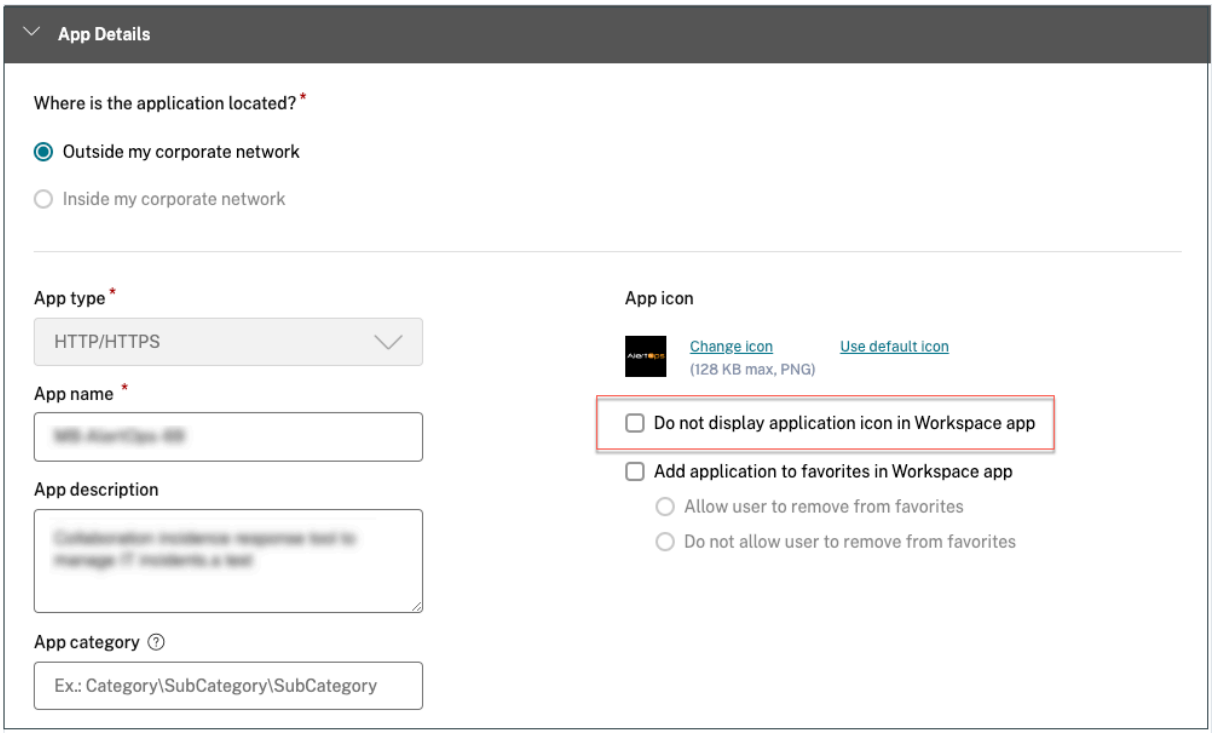
但是，如果 App1 改为将 `*.intranet.local` 作为相关域，则访问 `Eng-User5` 将被拒绝，因为 `app.intranet.local` 本来是完全匹配的 `PolicyB`，而用户 `Eng-User5` 没有访问权限。

应用程序配置最佳实践

IDP 域必须有自己的应用程序

我们建议不要在您的内联网应用程序配置中将 IDP 域添加为相关域，而应采取以下措施：

- 为所有 IDP 域创建单独的应用程序。
- 创建策略以允许所有需要访问 IDP 身份验证页面的用户访问权限，并将该策略保持为最高优先级。
- 将此应用程序（通过选择“不向用户显示应用程序图标”选项）从应用程序配置中隐藏，这样它就不会在工作区中枚举。有关信息，请参阅配置应用程序详细信息。



> 注意：
>
> 此应用程序配置仅允许访问 IDP 身份验证页面。对单个应用程序的进一步访问权限仍然取决于各个应用程序的配置及其各自的访问策略。

示例配置：

1. 将所有常见 FQDN 配置到自己的应用程序中，并在适用的情况下将它们分组在一起。

   例如，如果您有一些使用 Azure AD 作为 IdP 的应用程序，并且需要配置 `login.microsoftonline.com` 和其他相关域 (`*.msauth.net`)，那么请执行以下操作：

   - 使用 `https://login.microsoftonline.com` 作为应用程序 URL，`*.login.microsoftonline.com` 和 `*.msauth.net` 作为相关域，创建单个通用应用程序。

2. 配置应用程序时选择“不向用户显示应用程序图标”选项。有关详细信息，请参阅配置应用程序详细信息。
3. 为通用应用程序创建访问策略，并允许所有用户访问。有关详细信息，请参阅配置访问策略。
4. 为访问策略分配最高优先级。有关详细信息，请参阅优先顺序。
5. 验证诊断日志，以确认 FQDN 与应用程序匹配以及策略是否按预期执行。

相同的相关域不得是多个应用程序的一部分

相关域名必须是应用程序独有的。配置冲突可能会导致应用程序访问问题。如果使用相同的 FQDN 或通配符 FQDN 的某种变体配置了多个应用程序，则可能会遇到以下问题：

- 网站停止加载或可能显示空白页面。
- 当您访问 URL 时，可能会出现“阻止访问”页面。
- 登录页面可能无法加载。

因此，我们建议在单个应用程序中配置唯一的相关域。

错误的配置示例：

- 示例：在多个应用程序中复制相关域

  假设您有 2 个应用程序都需要访问 Okta（example.okta.com）：

应用程序	应用程序 URL 域	相关域
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

策略名称	优先级	用户和关联应用程序
拒绝 App1 给 HR	高	App1 的用户组 HR
授予所有人访问 App1 的权限	中	允许访问用户组 Everyone to App1
授予所有人访问 App2 的权限	低	允许访问用户组“所有人”对 App2 的访问权限

配置问题：尽管目的是向所有用户授予对 App2 的访问权限，但用户组 HR 无法访问 App2。HR 用户组被重定向到 Okta，但由于第一个拒绝访问 App1（也与 App2 具有相同的相关域 `example.okta.com`）的策略而被卡住。

这种情况对于诸如 Okta 之类的身份提供商来说非常常见，但也可能发生在具有共同相关域的其他紧密集成的应用程序中。有关策略匹配和优先级的详细信息，请参阅访问策略匹配和优先级划分。

上述配置的建议：

1. 从所有应用程序中移除 example.okta.com 作为相关域名。
2. 仅为 Okta 创建新应用（应用 URL 为 `https://example.okta.com`，相关域为 `*.okta.com`）。
3. 在工作区中隐藏此应用程序。
4. 为策略分配最高优先级，以消除任何冲突。

最佳实践：

- 应用程序的相关网域不得与其他应用程序的相关网域重叠。
- 如果发生这种情况，必须创建一个新发布的应用程序以覆盖共享的相关域，然后应相应地设置访问权限。
- 管理员必须评估此共享相关域是否需要在 Workspace 中显示为实际应用程序。
- 如果应用程序不得出现在 Workspace 中，则在发布应用程序时，选择“不向用户显示应用程序图标”选项以将其隐藏在 Workspace 中。

深度链接 **URL**

对于深度链接 URL，必须将内联网应用程序 URL 域添加为相关域：

示例：

内联网应用程序配置了 `https://example.okta.com/deep-link-app-1` URL 作为主应用程序 URL 域，相关域具有 Intranet 应用程序 URL 域，即 `*.issues.example.net`。

在这种情况下，使用 URL `https://example.okta.com` 分别创建 IdP 应用程序，然后将相关域名设置为 `*.example.okta.com`。

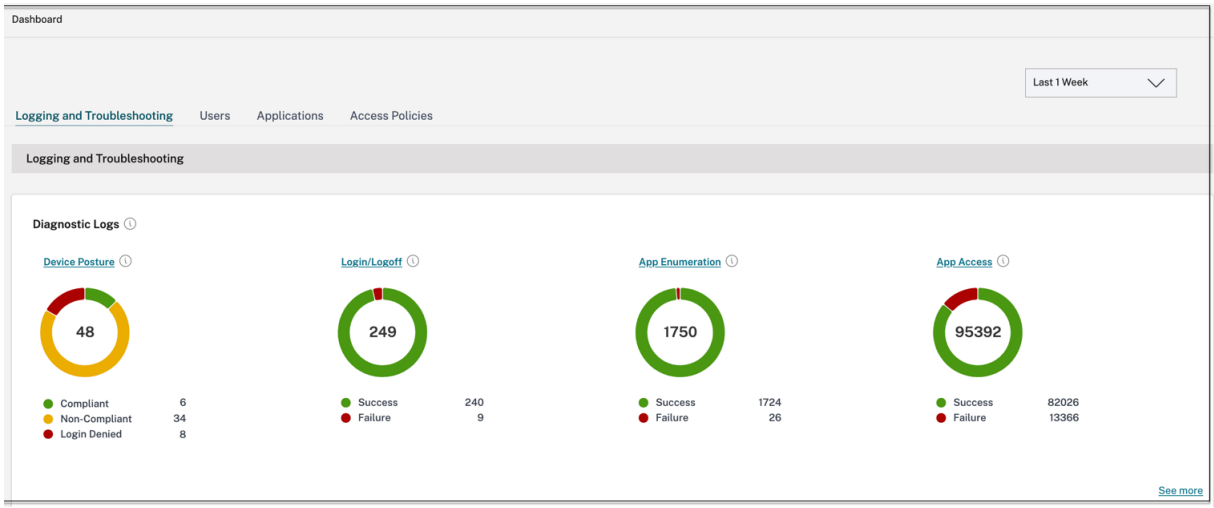
诊断日志

June 19, 2024

Secure Private Access 服务控制面板显示 SaaS、Web、TCP 和 UDP 应用程序的诊断和使用数据。使用诊断日志图表查看与身份验证、应用程序启动、应用程序枚举相关的日志，以及与设备状态相关的日志。您可以单击查看更多链接以查看日志的详细信息。详细信息以表格形式呈现。您可以查看预设时间或自定义时间轴的日志。您可以通过单击 + 符号向图表添加列，具体取决于您要在控制板中看到的信息。您可以将用户日志导出为 CSV 格式。

- 您可以使用“添加过滤器”选项根据应用程序类型、类别、描述等各种条件来细化搜索。例如，在搜索字段中，您可以单击 `Transaction ID`、`= (equals to some value)`，然后输入 `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`，搜索与该事务 ID 相关的所有日志。有关可与筛选器选项一起使用的搜索运算符的详细信息，请参阅搜索运算符。
- **Device Posture** 日志：可以根据策略结果（合规、不合规和登录被拒绝）优化搜索。有关 Device Posture 的详细信息，请参阅 Device Posture。

> 注意：
>
> - Secure Private Access 诊断日志控制板中的每个故障事件都有相关的信息代码。有关详细信息，请参阅信息代码。
> - 交易 ID 关联访问请求的所有 Secure Private Access 日志。有关详细信息，请参阅交易 ID。



> 注意：
>
> - 默认情况下，诊断日志页面显示当周的数据，仅显示最近的 10000 条记录。使用自定义日期搜索和筛选器进一步细化搜索结果。

审核日志

February 20, 2024

与 Secure Private Access 服务相关的事件现在可以在 **Citrix Cloud >** 系统日志中捕获。管理员在 Citrix Secure Private Access 服务中执行的所有事件都将发送到 Citrix Cloud 并在系统日志中捕获。管理员事件可以但不限于以下内容：

- 配置 Web 或 SaaS 应用程序
- 订阅应用
- 删除应用
- 配置自适应访问策略

下图显示了系统日志中与 Secure Private Access 相关的事件。有关导出事件、检索特定时间段的事件、转发日志事件和数据保留等详细信息，请参阅 系统日志。

适用于企业 **Web**、**TCP** 和 **SaaS** 应用程序的自适应访问和安全控制

June 19, 2024

在当今不断变化的形势下，应用程序安全对任何企业都至关重要。做出具有上下文意识的安全决策，然后启用对应用程序的访问权限可在允许用户访问的同时降低相关风险。

Citrix Secure Private Access 服务自适应访问功能提供了一种全面的零信任访问方法，可提供对应用程序的安全访问。自适应访问使管理员能够根据上下文提供用户可以访问的应用程序的精细级别访问权限。这里的“上下文”一词是指：

- 用户和组（用户和用户组）
- 设备（台式机或移动设备）
- 位置（地理位置或网络位置）
- Device Posture（Device Posture 检查）
- 风险（用户风险评分）

自适应访问功能将自适应策略应用于正在访问的应用程序。这些策略根据上下文确定风险，并做出动态访问决策，授予或拒绝对企业 Web、SaaS、TCP 和 UDP 应用程序的访问权限。

工作原理

要授予或拒绝对应用程序的访问权限，管理员需要根据用户、用户组、用户访问应用程序的设备、用户访问应用程序的位置（国家/地区或网络位置）以及用户风险评分来创建策略。

自适应访问策略优先于在 Secure Private Access 服务中添加 SaaS 或 Web 应用程序时配置的特定于应用程序的安全策略。每个应用程序级别的安全控制被自适应访问策略覆盖。

自适应访问策略在三种情况下进行评估：

- 在 Secure Private Access 服务的 Web、TCP 或 SaaS 应用程序枚举期间—如果拒绝此用户访问应用程序，则用户无法在工作区中看到此应用程序。
- 启动应用程序时—枚举应用程序后，如果将自适应策略更改为拒绝访问，则用户无法启动该应用程序，即使之前枚举了该应用程序。
- 在 Citrix Enterprise Browser 或 Remote Browser Isolation 服务中打开应用程序时，Citrix Enterprise Browser 会强制执行某些安全控制。这些控制措施由客户强制执行。启动 Citrix Enterprise Browser 时，服务器会评估用户的自适应策略并将这些策略返回给客户端。然后，客户端在 Citrix Enterprise Browser 中本地强制执行策略。

创建包含多个规则的自适应访问策略

您可以创建多个访问规则，并在单个策略中为不同的用户或用户组配置不同的访问条件。这些规则可以分别应用于 HTTP/HTTPS 和 TCP/UDP 应用程序，全部应用于单个策略。

Secure Private Access 中的访问策略允许您根据用户或用户设备的环境启用或禁用对应用程序的访问。此外，您可以通过添加以下安全限制来启用对应用程序的受限访问：

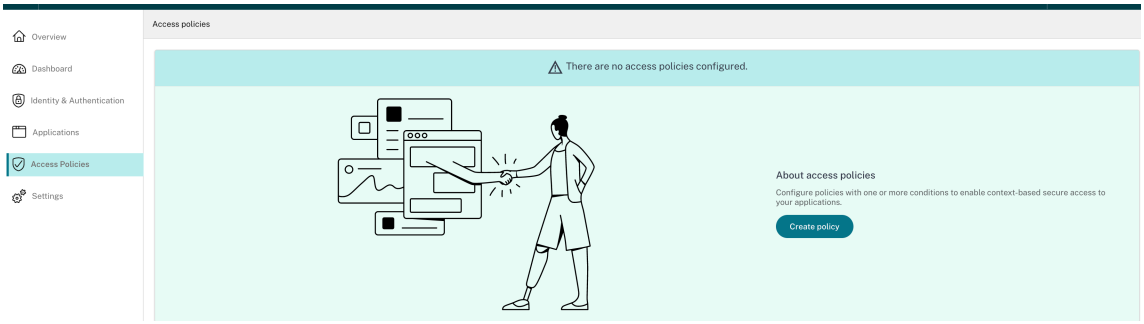
- 限制剪贴板访问
- 限制打印
- 限制下载
- 限制上载
- 显示水印
- 限制密钥记录
- 限制屏幕截图

有关这些限制的更多信息，请参阅可用的访问限制选项。

在配置访问策略之前，请确保您已完成以下任务。

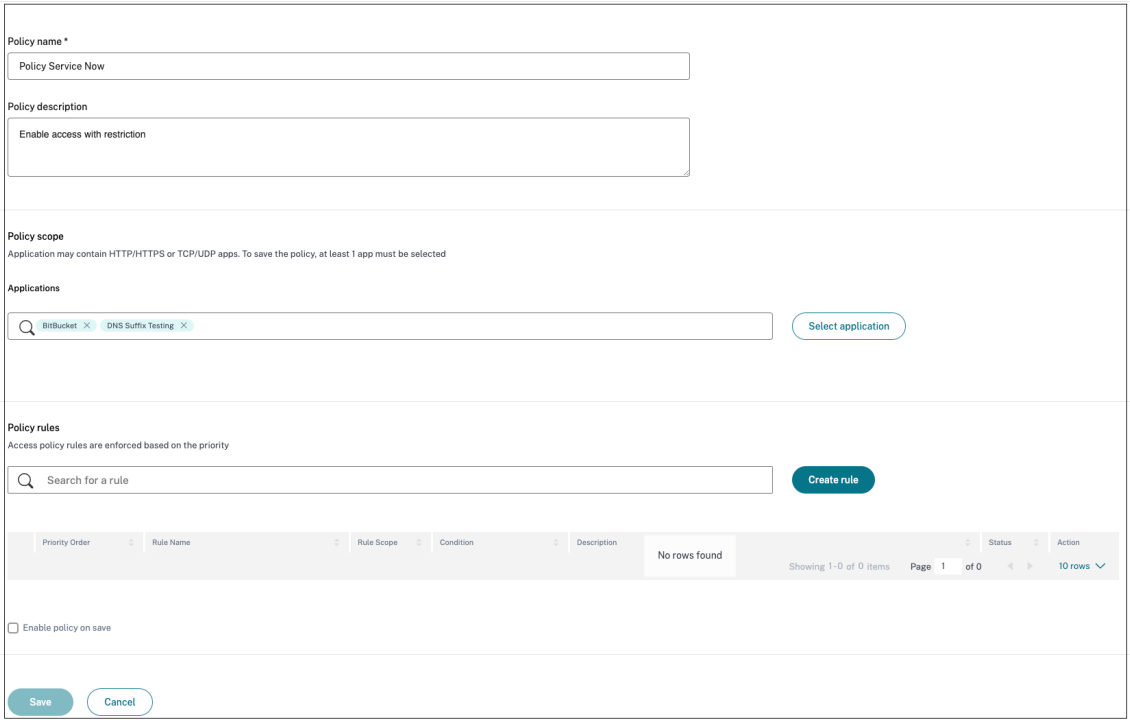
- 设置身份和身份验证
- 已配置的应用程序

1. 在导航窗格上，单击“访问策略”，然后单击“创建策略”。



对于首次使用的用户，访问策略 登录页面不显示任何策略。创建策略后，可以看到此处列出的策略。

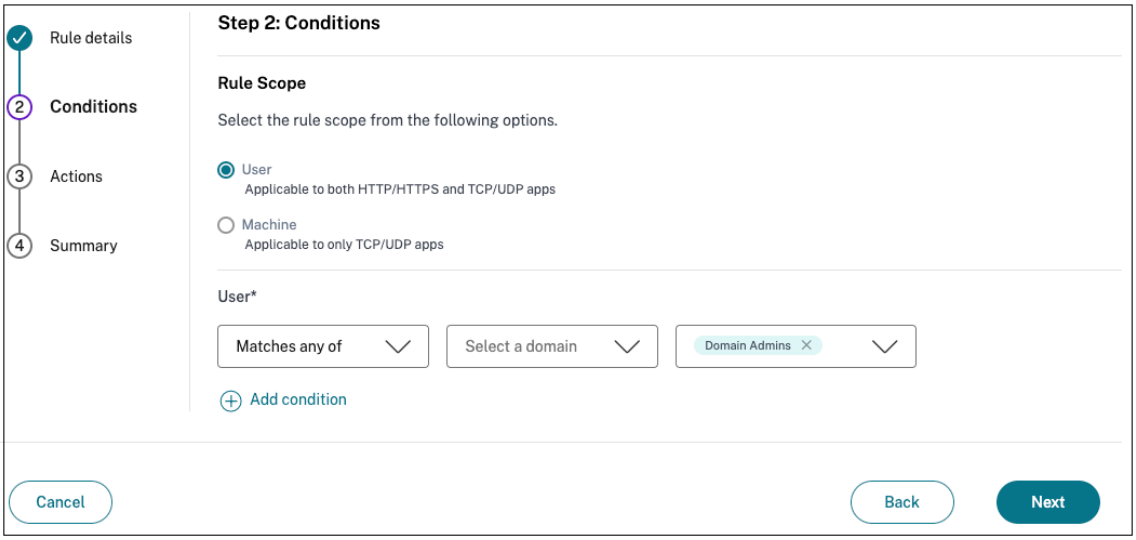
2. 输入策略名称和策略描述。
3. 在 应用程序中，选择必须强制执行此策略的应用程序或一组应用程序。
4. 单击“创建规则”为策略创建规则。



5. 输入规则名称和规则的简要描述，然后单击“下一步”。

6. 选择用户的条件。用户条件是向用户授予应用程序访问权限时必须满足的强制性条件。选择以下选项之一：

   - 匹配任一项 - 仅允许与字段中列出的任何名称相匹配且属于所选域的用户或组进行访问。
   - 不匹配任何项 - 允许除字段中列出并属于选定域的用户或组以外的所有用户或组进行访问。



7. （可选）单击 + 可根据上下文添加多个条件。

   当您根据上下文添加条件时，只有在满足用户 * 和可选的基于上下文的条件时，才会对策略进行评估的条件应用 AND 运算。您可以根据上下文应用以下条件。

   - 台式机或移动设备 - 选择要为其启用应用程序访问权限的设备。
   - 地理位置 - 选择用户访问应用程序的条件和地理位置。
   - 网络位置 -选择用户访问应用程序所使用的条件和网络。
   - **Device Posture** 检查 - 选择用户设备访问应用程序必须满足的条件。
   - 用户风险评分 - 选择风险评分类别，必须根据这些类别向用户提供应用程序访问权限。

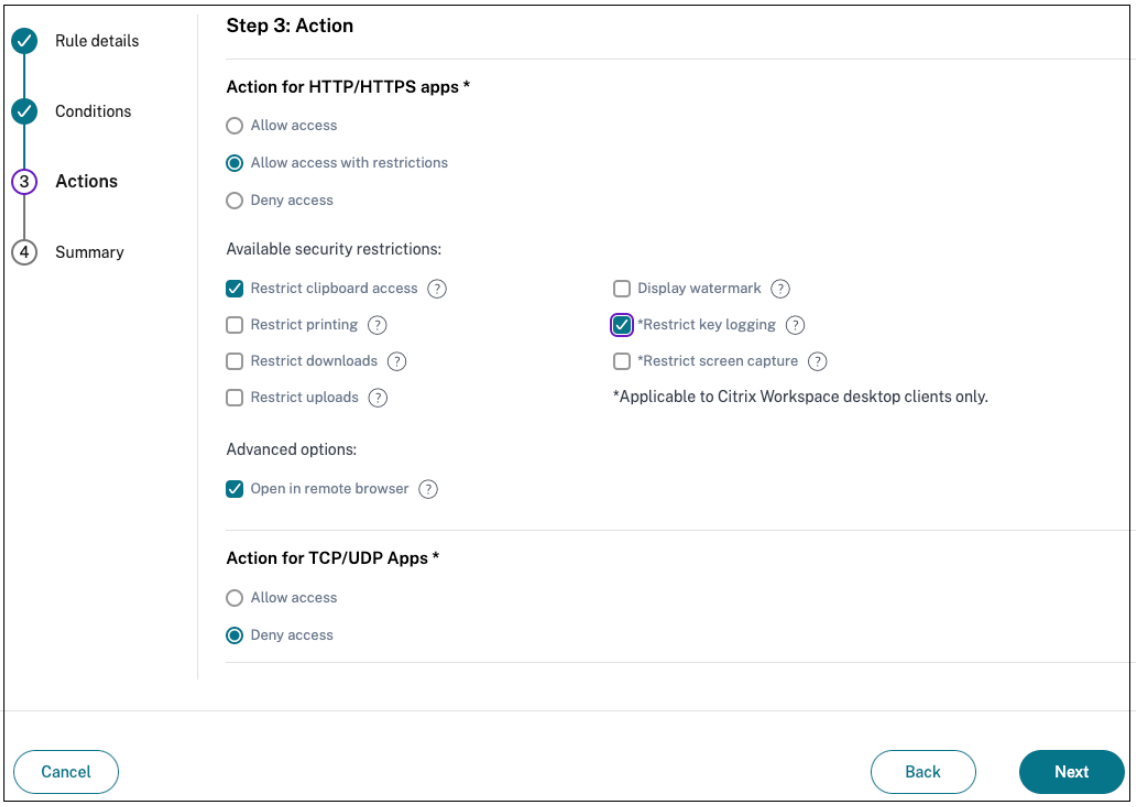
8. 单击下一步。

9. 根据条件评估选择必须应用的操作。

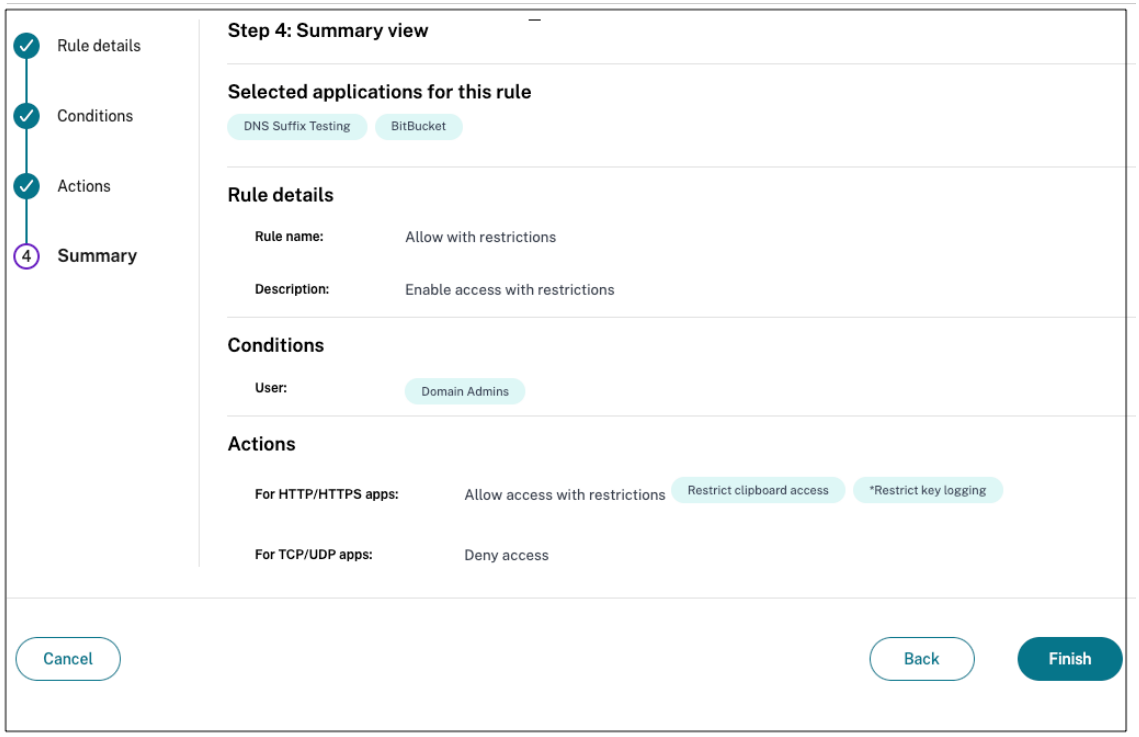
   - 对于 HTTP/HTTPS 应用程序，您可以选择以下选项：
     - 允许访问
     - 允许访问但有限制
     - 拒绝访问

     > 注意：
     >
     > 如果选择“允许有限制的访问”，则必须选择要对应用程序强制执行的限制。有关限制的详细信息，请参阅可用的访问限制选项。您还可以指定是要在远程浏览器还是 Citrix Secure Browser 中打开应用程序。

   - 对于 TCP/UDP 访问，您可以选择以下选项：
     - 允许访问
     - 拒绝访问

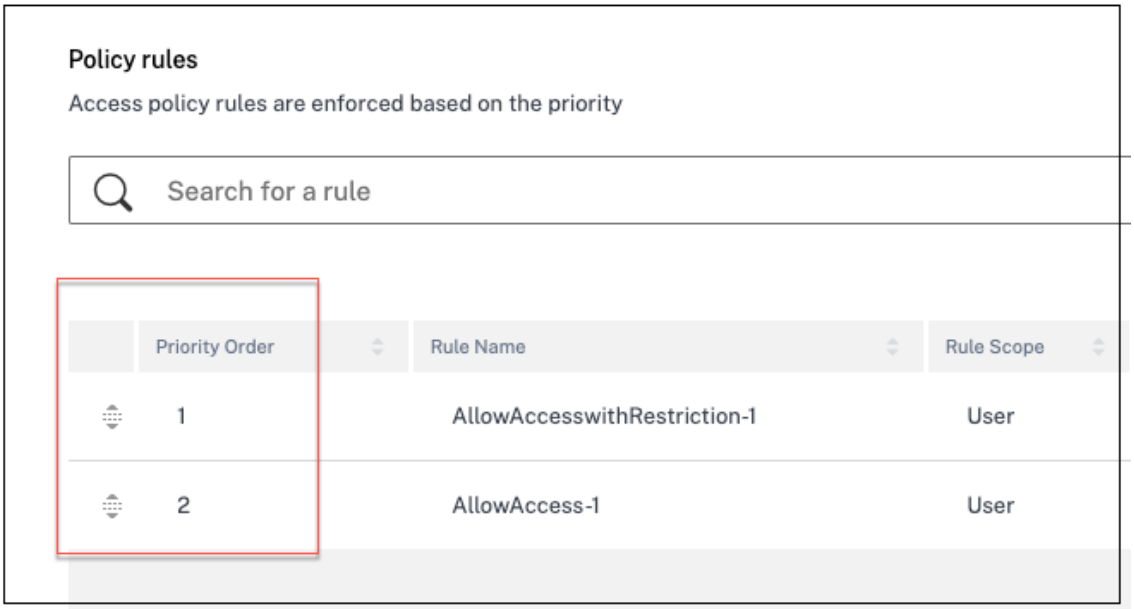


10. 单击下一步。摘要页面显示策略的详细信息。
11. 您可以验证详细信息，然后单击“完成”。



创建策略后要记住的几点

- 您创建的策略显示在“策略规则”部分下方，默认情况下处于启用状态。如果需要，您可以禁用规则。但是，请确保至少启用一条规则才能使策略处于活动状态。
- 默认情况下，会为策略分配优先顺序。值较低的优先级具有最高优先级。优先级编号最低的规则将首先评估。如果规则 (n) 与定义的条件不匹配，则评估下一个规则 (n+1)，依此类推。



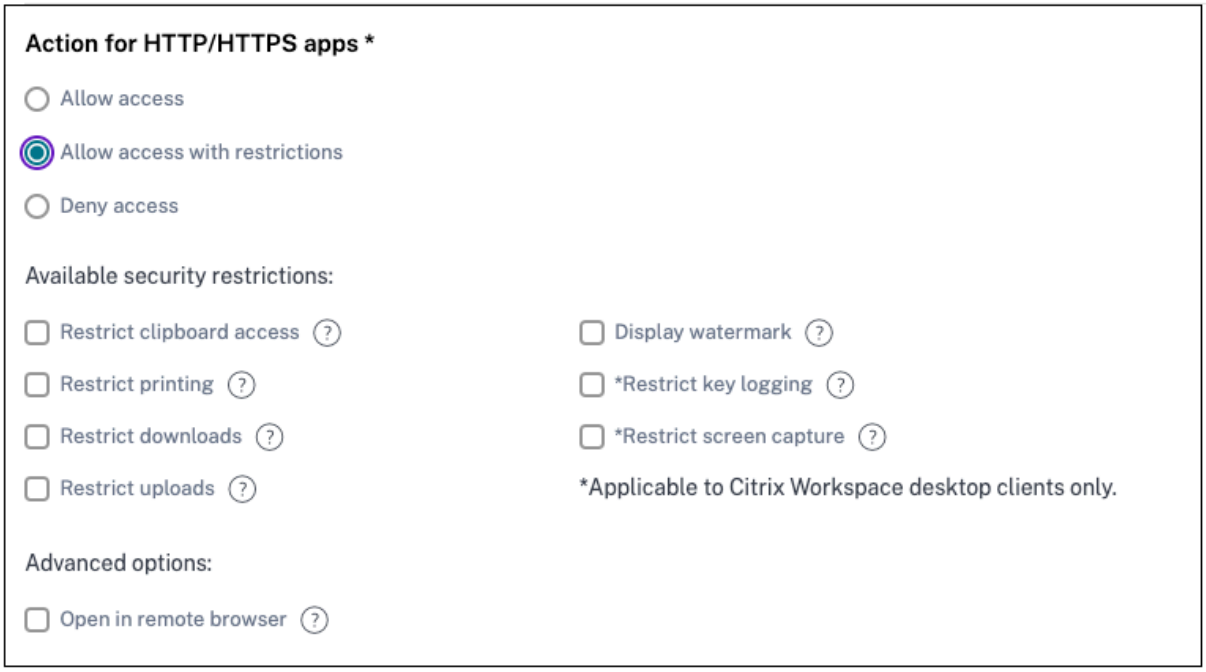
使用优先顺序评估规则示例：

假设您已经创建了两条规则，即规则 1 和规则 2。
规则 1 分配给用户 A，规则 2 分配给用户 B，然后评估这两条规则。
假设规则 1 和规则 2 均分配给用户 A。在这种情况下，规则 1 的优先级更高。如果规则 1 中的条件得到满足，则应用规则 1 并跳过规则 2。否则，如果规则 1 中的条件未得到满足，则规则 2 将应用于用户 A。

> 注意：
>
> 如果未评估任何规则，则不会向用户枚举应用程序。

可用的访问限制选项

选择“允许有限制的访问”操作时，必须至少选择一项安全限制。这些安全限制是在系统中预定义的。管理员无法修改或添加其他组合。可以为应用程序启用以下安全限制。

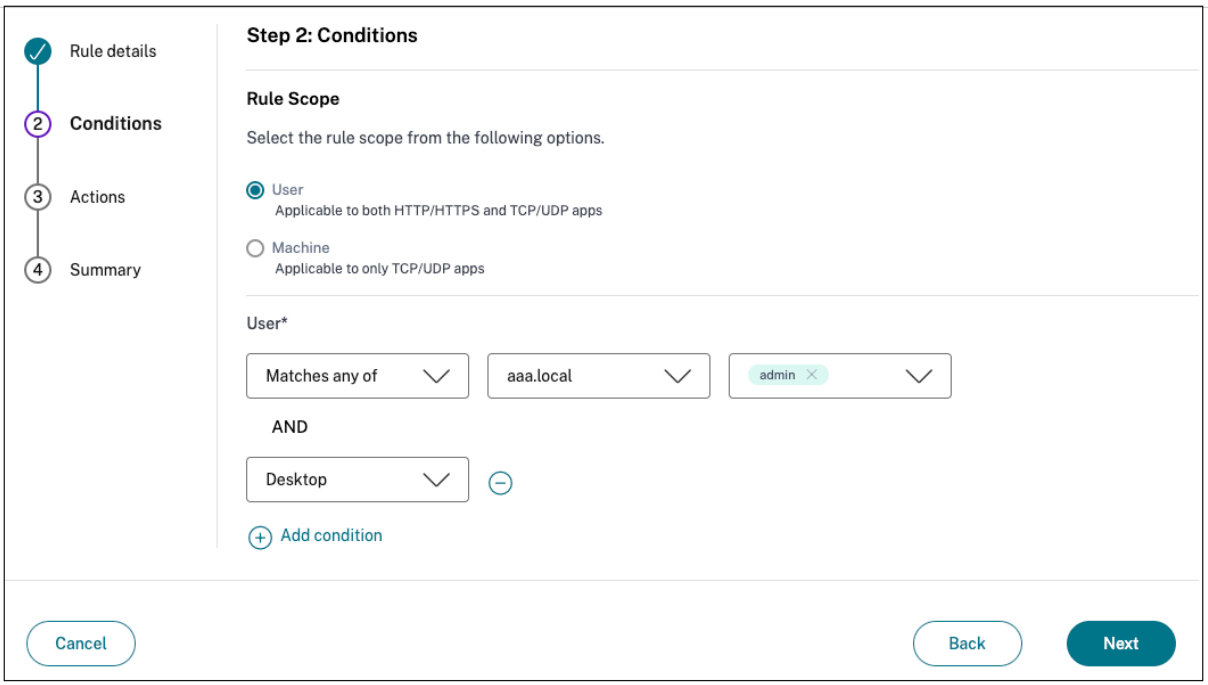


- 限制剪贴板访问权限：禁用应用程序和系统剪贴板之间的剪切/复制/粘贴操作。
- 限制打印：禁用在 Citrix Enterprise Browser 中打印的功能。
- 限制下载：禁用用户从应用程序内下载的功能。
- 限制上载：禁用用户在应用程序内上载的权限。
- 显示水印：在用户屏幕上显示水印，显示用户计算机的用户名和 IP 地址。
- 限制按键记录：防范按键记录器。当用户尝试使用用户名和密码登录应用程序时，所有密钥都会在密钥记录器上加密。此外，用户在应用程序上执行的所有活动都受到密钥记录的保护。例如，如果为 Office 365 启用了 App Protection 策略，并且用户编辑 Office 365 Word 文档，则所有按键记录器上的按键都经过加密。
- 限制屏幕截图：禁用使用任何屏幕捕获程序或应用程序捕获屏幕的功能。如果用户尝试捕获屏幕，则会捕获一个空白屏幕。

基于设备的自适应访问

要根据用户访问应用程序的平台（移动设备或台式计算机）配置自适应访问策略，请使用创建具有多规则的自适应访问策略过程并进行以下更改。

- 在“步骤 **2**：条件”页面中，单击“添加条件”。
- 选择“台式机”或“移动设备”。
- 完成策略配置。



基于位置的自适应访问

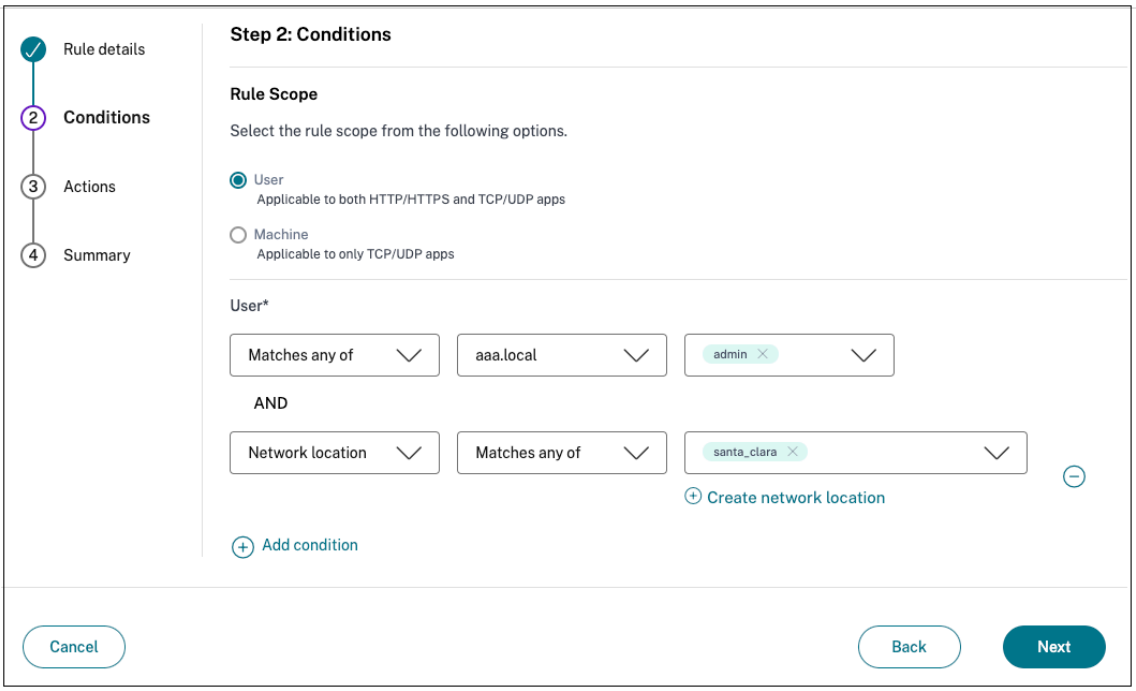
管理员可以根据用户访问应用程序的位置配置自适应访问策略。该位置可以是用户访问应用程序所在的国家/地区，也可以是用户的网络位置。网络位置是使用 IP 地址范围或子网地址定义的。

要根据位置配置自适应访问策略，请使用经过以下更改的 [创建具有多规则的自适应访问策略程序。

- 在“步骤 **2**：条件”页面中，单击“添加条件”。
- 选择 地理位置 或 网络位置。
- 如果您配置了多个地理位置或网络位置，请根据需要选择以下位置之一。
  - 匹配任一 -地理位置或网络位置与数据库中配置的任何地理位置或网络位置匹配。
  - 不匹配任何 -地理位置或网络位置与数据库中配置的地理位置或网络位置不匹配。

  注意：

- 如果选择 地理位置，则使用国家/地区数据库的 IP 地址评估用户的源 IP 地址。如果用户的 IP 地址映射到策略中的国家/地区，则应用该策略。如果国家/地区不匹配，则跳过此自适应策略并评估下一个自适应策略。
- 对于 网络位置，您可以选择一个现有的网络位置或创建一个网络位置。要创建新的网络位置，请单击创建网络位置。
- 确保您已从 **Citrix Cloud > Citrix Workspace >** 访问 **>** 自适应访问启用自适应访问。如果没有，则无法添加位置标签。有关详细信息，请参阅启用自适应访问。
- 您也可以从 Citrix Cloud 控制台创建网络位置。有关详细信息，请参阅 Citrix Cloud 网络位置配置。



- 完成策略配置。

基于 **Device Posture** 的自适应访问

您可以配置 Secure Private Access 服务，使用 Device Posture 标签强制执行访问控制。在 Device Posture 验证后允许设备登录后，可以将该设备归类为兼容或不合规。此信息可作为 Citrix DaaS 服务和 Citrix Secure Private Access 服务的标签提供，用于根据 Device Posture 提供上下文访问。

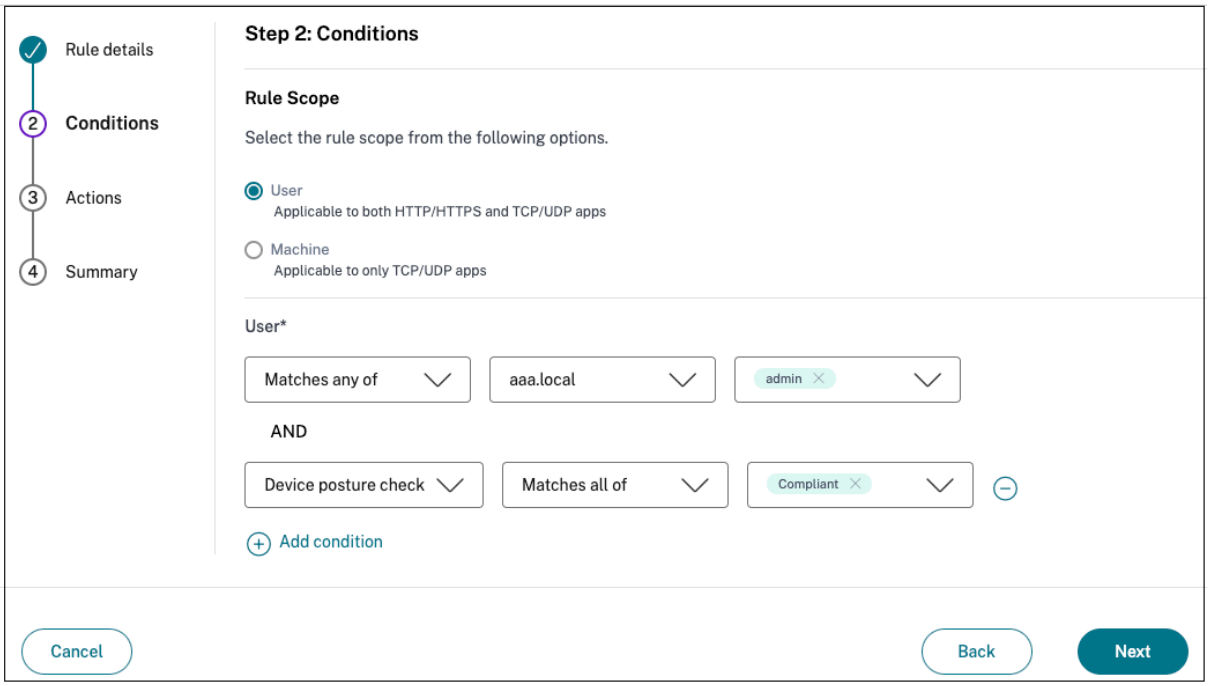
有关 Device Posture 服务的完整详细信息，请参阅 Device Posture。

要根据 Device Posture 配置自适应访问策略，请使用 具有多规则的自适应访问策略 过程并进行以下更改。

- 在“步骤 **2**：条件”页面中，单击“添加条件”。
- 从下拉菜单中选择 **Device Posture** 检查和逻辑表达式。

- 在自定义标签中输入以下值之一：
  - 合规 - 适用于合规设备
  - 不合规 - 适用于不兼容的设备

> 注意：
>
> 设备分类标签的输入方式必须与之前捕获的语法相同，即初始上限（合规和不合规）。否则，Device Posture 策略将无法按预期运行。



基于用户风险评分的自适应访问

> 重要提示：
>
> 此功能仅在客户拥有 Security Analytics 权限时才可用。

用户风险评分是一种评分系统，用于确定与企业中的用户活动相关的风险。风险指示器分配给看起来可疑或可能对组织构成安全威胁的用户活动。当用户的行为偏离正常情况时，会触发风险指示器。每个风险指标都可以有一个或多个与之相关的风险因素。这些风险因素可帮助您确定用户事件中的异常类型。风险指示器及其相关的风险因素决定用户的风险评分。风险评分是定期计算的，在操作和风险评分更新之间存在延迟。有关详细信息，请参阅 Citrix 用户风险指示器。

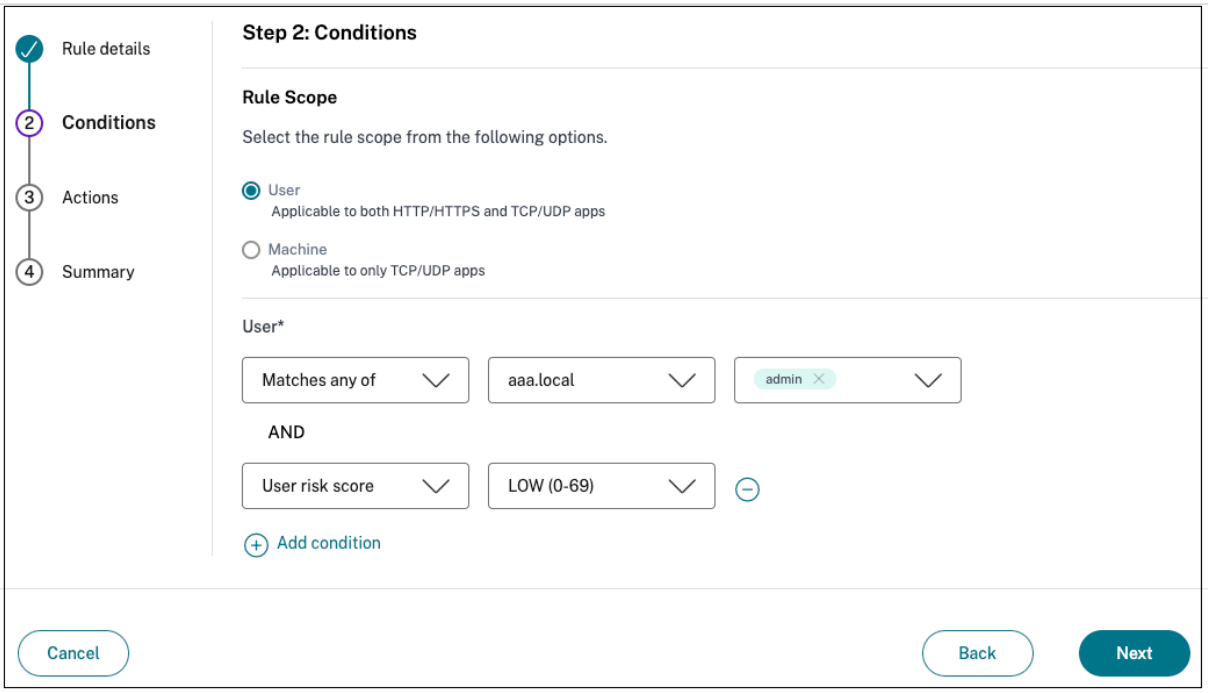
要使用风险评分配置自适应访问策略，请使用 具有多规则的自适应访问策略 过程并进行以下更改。

- 在“步骤 **2**：条件”页面中，单击“添加条件”。
- 选择 用户风险评分，然后选择风险状况。

- 从 CAS 服务中提取的预设标签
  - 低 1—69
  - 中 70—89
  - 高 90—100

> 注意：
>
> 风险分数 0 不被视为风险等级为“低”。

- 阈值类型
  - 大于或等于
  - 小于或等于
- 一个数字范围
  - 范围



用于解决由相同相关域产生的冲突的路由表

January 9, 2024

Citrix Secure Private Access 服务的应用程序域功能使客户能够做出路由决策，允许通过 Connector Appliance 在外部或内部路由应用程序的相关域。

考虑到客户在 SaaS 应用程序和内部 Web 应用程序中配置了相同的相关域。
例如，如果 Okta 是 Salesforce（SaaS 应用程序）和 Jira（内部 Web 应用程序）的 SAML IdP，则管理员可能会在这两个应用程序的配置中配置 `*.okta.com` 为相关域。这会导致冲突，最终用户会遇到不一致的行为。在这种情况下，管理员可以定义规则，根据要求通过 Connector Appliance 在外部或内部路由这些应用程序。

应用程序域功能还允许管理员配置 Connector Appliance，使其绕过客户的 Web 代理服务器访问内部 Web 服务器。这些绕过策略以前是通过在 Connector Appliance 上运行 NSCLI 命令来手动配置的。

路由表的工作原理

管理员可以通过 Connector Appliance 将应用程序的路由类型定义为“外部”、“内部”或“外部”，具体取决于他们想要如何定义流量。

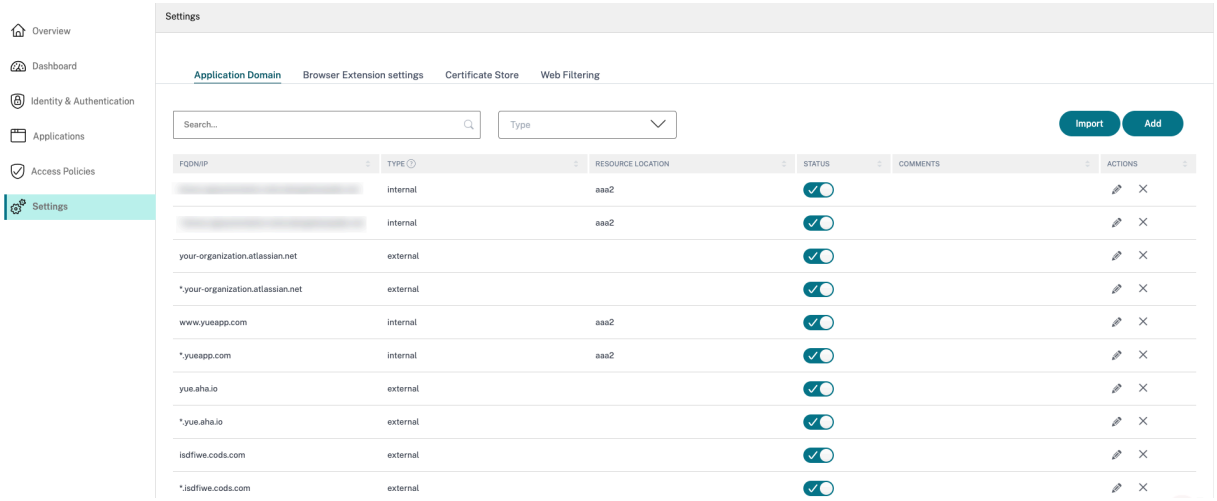
- 外部—流量直接流向互联网。
- 内部—流量通过 Connector Appliance 传输。
  - 对于 Web 应用程序，流量在数据中心内流动。
  - 对于 SaaS 应用程序，流量通过 Connector Appliance 路由到网络外部。
- 内部—绕过代理 - 域流量通过 Citrix CloudConnector 设备路由，绕过客户在 Connector Appliance 上配置的 Web 代理。
- 外部 **(**通过连接器**)** - 应用程序是外部应用程序，但流量必须通过 Connector Appliance 传输到外部网络。

> 注意：
>
> - 路由条目不会影响在应用程序上配置的安全策略。
> - 如果管理员不打算使用路由表中的条目，或者相应的应用程序未按预期运行，管理员可以直接禁用该条目，而不是将其删除。
> - 无论应用程序类型如何，特定客户的所有 Connector Appliance 都将获得 SSO 设置。以前，特定应用程序的 SSO 设置与资源位置相关联。

主路由表

主路由表可从 **Secure Private Access** 磁贴访问。

1. 登录 Citrix Cloud 帐户。
2. 在 Secure Private Access 图块上，单击管理。
3. 在导航窗格中，单击“设置”。此时将显示“应用程序域”页面。



主路由表显示以下列。

- **FQDN/IP**：需要为其配置流量路由类型的 FQDN 或 IP 地址。
- 类型：应用程序类型。添加应用程序时选择的内部、外部或外部 **(**通过连接器**)** 。

  > 重要提示：
  >
  > 如果存在冲突，则会为表格中的相应行显示一个警报图标。要解决冲突，管理员必须单击三角形图标，然后在主表中更改应用程序类型。

- 资源地点：“内部”类型的工艺路线的资源地点。如果未分配资源位置，则相应应用程序的“资源位置”列中会显示一个三角形图标。当您将鼠标悬停在图标上时，将显示以下消息。

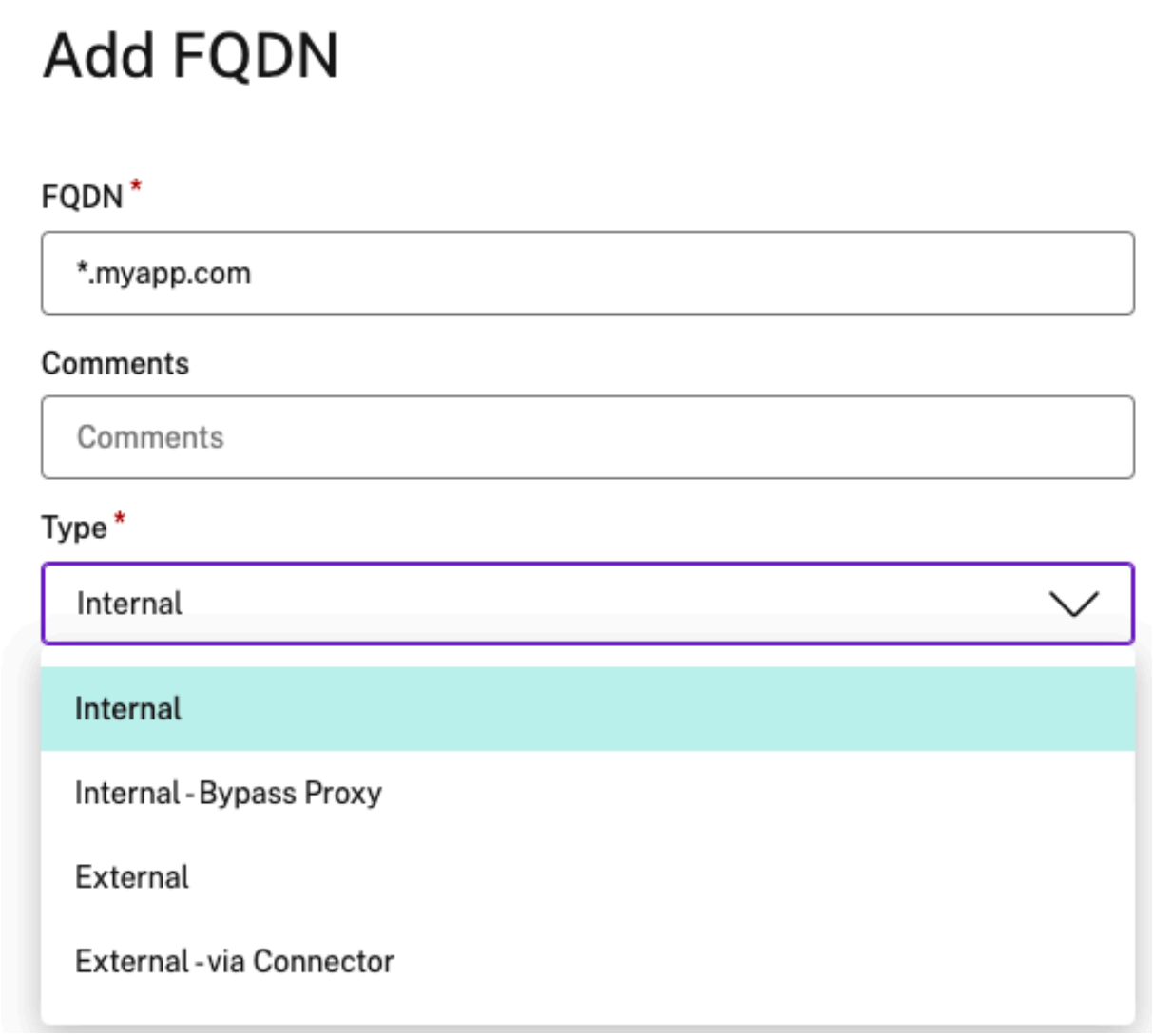
  缺少资源位置。确保资源位置与此 *FQDN* 关联。

- 状态：状态列中的切换开关可用于禁用路由条目的路由，而无需删除应用程序。将切换开关转为“关”时，路径条目不会生效。此外，如果存在完全匹配的 FQDN，管理员可以选择要启用或禁用的路由。
- 注释：显示注释（如果有）。
- 操作：编辑图标用于添加资源位置或更改路径条目的类型。删除图标用于删除路由。

将 **FQDN** 添加到应用程序域表

管理员可以将 FQDN 添加到应用程序域表中，然后为其选择适当的路由类型。

1. 单击应用程序域页面中的 添加。
2. 输入 FQDN 名称，然后为 FQDN 选择适当的路由类型。



迷您路由表

应用程序域表的迷您版本可用于在应用程序配置期间做出路由决策。Citrix Secure Private Access 服务用户界面的“应用程序连接”部分中提供的迷您路由表。

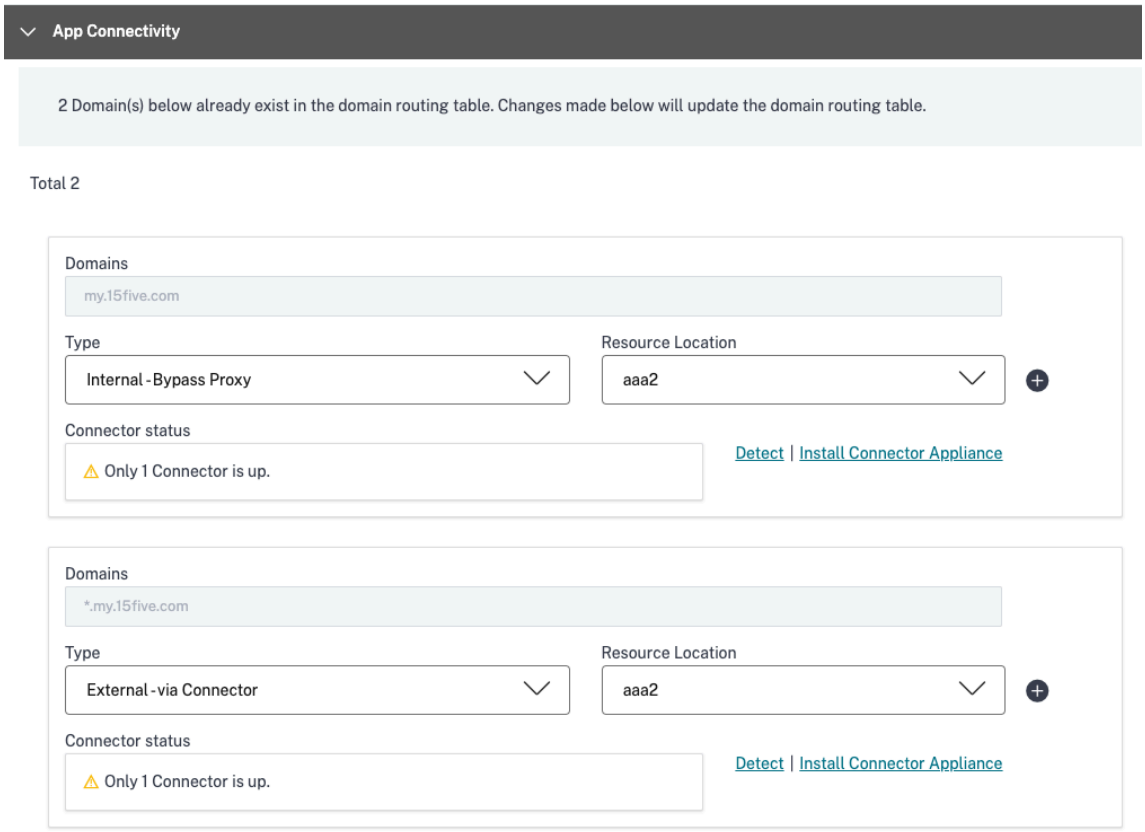
向迷您路由表添加路由

在 Citrix Secure Private Access 服务中添加应用程序的步骤与支持软件即服务应用程序和支持企业 Web 应用程序主题中所述的步骤相同，但以下两项更改除外：

1. 完成以下步骤：
    - 选择一个模板。
    - 输入应用详细信息。

- 根据需要选择增强的安全详细信息。
- 选择单点登录方法（如果适用）。

2. 单击 应用程序连接。-应用程序域表的迷您版本可用于在应用程序配置期间做出路由决策。



- 域：域 列显示特定应用程序的一行或多行。第一行显示管理员在添加应用程序详细信息时输入的实际应用程序 URL。其他行是在添加应用程序详细信息时输入的所有相关域。如果应用程序 URL 和相关域名相同，则它们将显示在一行中。

如果选择了 SAML SSO，则一行显示 SAML 断言 URL。

- 类型：选择以下选项之一。
  - 外部—流量直接流向互联网。
  - 内部—流量通过 Connector Appliance 传输，应用程序被视为 Web 应用程序。
    - 对于 Web 应用程序，流量在数据中心内流动。
    - 对于 SaaS 应用程序，流量通过 Connector Appliance 路由到网络外部。
  - 内部—绕过代理 - 域流量通过 Citrix Cloud Connector 设备路由，绕过客户在 Connector Appliance 上配置的 Web 代理。
  - 外部 **(**通过连接器**)** - 应用程序是外部应用程序，但流量必须通过 Connector Appliance 传输到外部网络。
- 资源位置：为应用程序选择“内部”类型时自动填充资源位置。如果需要其他资源位置，请更改它。

- **Connector Appliance** 状态：当您为应用程序选择内部类型时，自动填充以及资源位置。

未经批准的 **Web** 站点

June 19, 2024

未在 Secure Private Access 中配置的应用程序（内联网或 Internet）被视为“未经批准的 Web 站点”。默认情况下，如果没有为所有内联网 Web 应用程序配置应用程序和访问策略，Secure Private Access 会拒绝访问这些应用程序。

对于所有其他未配置应用程序的 Internet URL 或 SaaS 应用程序，管理员可以使用管理控制台中的设置 **>** 未经批准的 **Web** 站点选项卡，允许或拒绝通过 Citrix Enterprise Browser 进行访问。管理员还可以将访问重定向到远程浏览器隔离 (RBI) 环境，以防止基于浏览器的攻击。如果管理员配置了将 URL 重定向到 RBI，则会发生以下操作。

1. Secure Private Access 会转换域。
2. 然后，Citrix Enterprise Browser 将这些 URL 发送回 Secure Private Access。
3. Secure Private Access 将这些 URL 重定向到远程浏览器隔离服务。

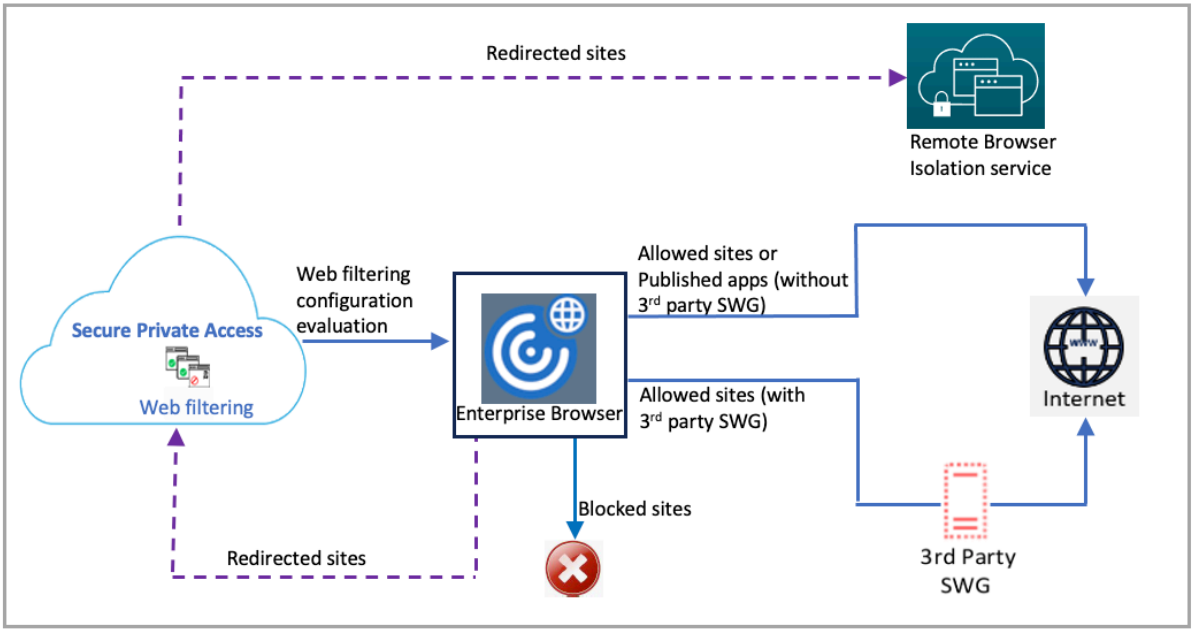
您可以使用通配符（例如 `*.example.com`）来控制对该网站中所有域名以及该网域内所有页面的访问权限。

> 注意：
>
> 默认情况下，设置配置为允许通过 Citrix Enterprise Browser 访问所有 Internet URL 或 SaaS 应用程序。

未经批准的 **Web** 站点是如何运作的

1. 完成 URL 分析检查以确定该 URL 是否为 Citrix 服务 URL。
2. 然后检查该 URL 以确定它是企业 Web 应用程序 URL 还是 SaaS 应用程序 URL。
3. 然后检查该 URL，以确定它是否被识别为被屏蔽的 URL，或者是否必须将其重定向到 Secure Browser 会话，或者是否允许访问该 URL。

下图说明了最终用户流量。

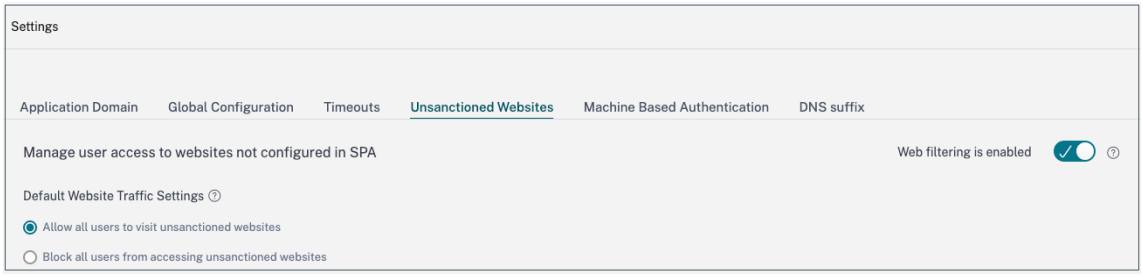


当请求到达时，将执行以下检查并采取相应的操作：

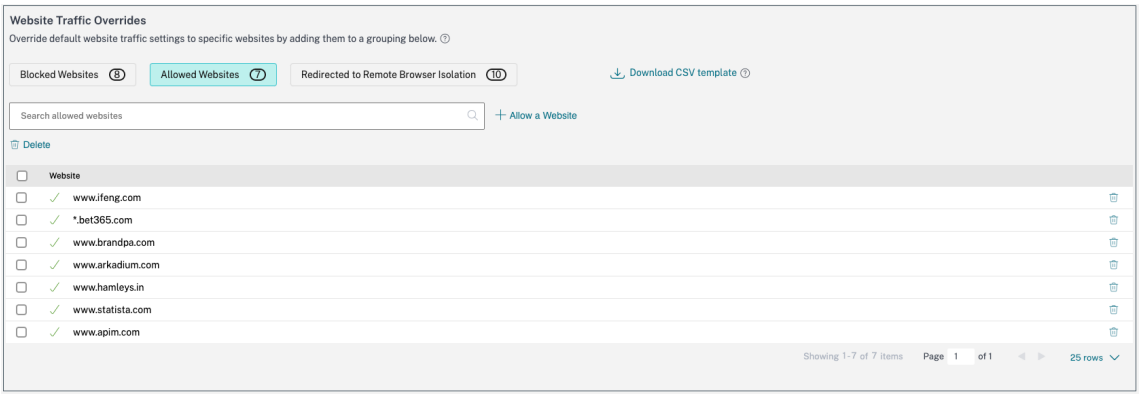
1. 请求是否与全局允许列表匹配?
   a) 如果匹配，则用户可以访问请求的网站。
   b) 如果不匹配，则检查网站列表。
2. 请求是否与配置的网站列表匹配?
   a) 如果匹配，则以下顺序确定操作。
      i. 阻止
      ii. 重定向
      iii. 允许
   b) 如果不匹配，则应用默认操作 (ALLOW)。无法更改默认操作。

为未经批准的 **Web** 站点配置规则

1. 在 Secure Private Access 控制台中，单击设置 **>** 未经批准的 **Web** 站点。



> 注意：
>
> - 默认情况下，网络过滤功能处于启用状态，允许访问所有未经批准的 Internet URL。
> - 您可以将设置更改为阻止所有用户访问未经批准的 **Web** 站点，以阻止所有用户通过 Citrix Enterprise Browser 访问任何 Internet URL。



您还可以通过将特定 URL 添加到被封锁的网站、允许的网站或重定向到远程浏览器隔离列表来更改特定 URL 的设置。

例如，如果您在默认情况下封锁了对所有未经批准的 URL 的访问权限，并且只想允许访问几个特定的 Internet URL，则可以通过执行以下步骤来实现：

a) 单击“允许的网站”选项卡，然后单击“允许使用网站”。

b) 添加必须允许访问的网站地址。您可以手动添加网站地址，也可以拖放包含该网站地址的 CSV 文件。

c) 单击“添加 **URL**”，然后单击“保存”。

该 URL 将添加到允许的网站列表中。

> 注意：
>
> 默认情况下，付费的远程浏览器隔离标准服务客户（组织）每年可使用 5,000 小时。在更长的时间内，他们必须购买 Secure Browser 加载项包。您可以跟踪 Remote Browser Isolation 服务的使用情况。有关详细信息，请参阅以下主题：
>
> - 管理和监视远程隔离浏览器
> - 远程浏览器隔离。

ADFS 与 Secure Private Access 集成

January 9, 2024

声明规则对于控制声明渠道中的声明流程是必要的。声明规则还可用于在声明规则执行过程中自定义声明流程。有关声明的更多信息，请参阅 Microsoft 文档。

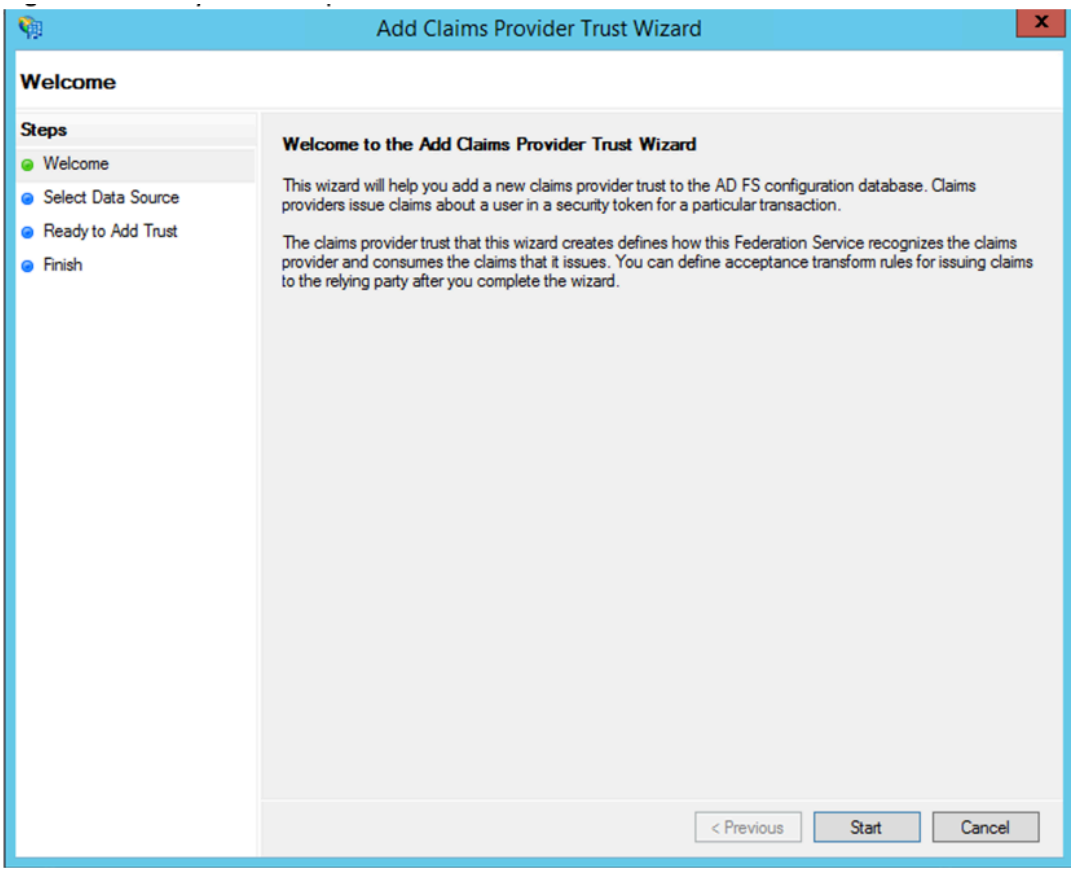
要将 ADFS 设置为接受来自 Citrix Secure Private Access 的声明，必须执行以下步骤：

1. 在 ADFS 中添加声明提供商信任。
2. 在 Citrix Secure Private Access 上完成应用程序配置。

添加声明提供商对 **ADFS** 的信任

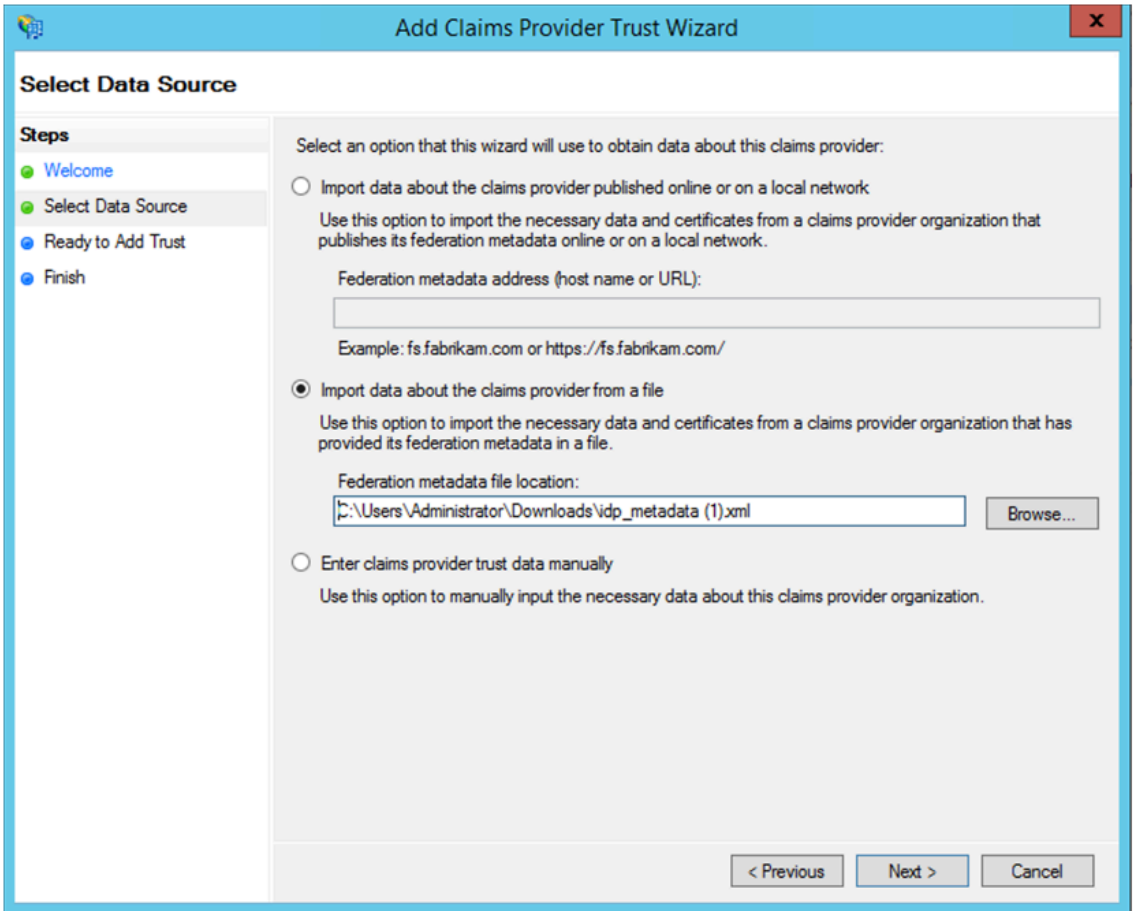
1. 打开 ADFS 管理控制台。转到 **ADFS >** 信任关系 **>** 声明提供商信任。

   a) 右键单击并选择添加声明提供商信任



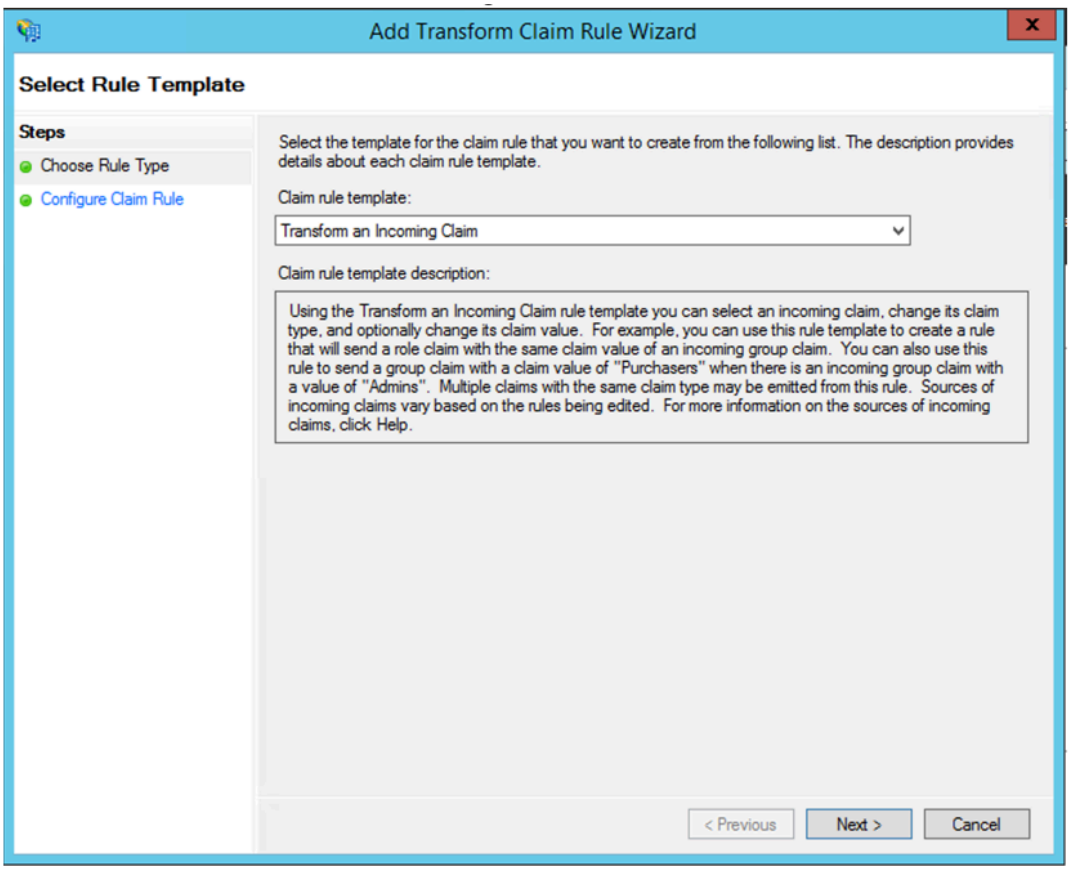
   b) 在 Secure Private Access 中添加用于联合到 ADFS 的应用程序。有关详细信息，请参阅 Citrix Secure Private Access 上的应用程序配置。

> 注意：
>
> 首先添加应用程序，然后从应用的 SSO 配置部分中下载 SAML 元数据文件，然后将元数据文件导入 ADFS。

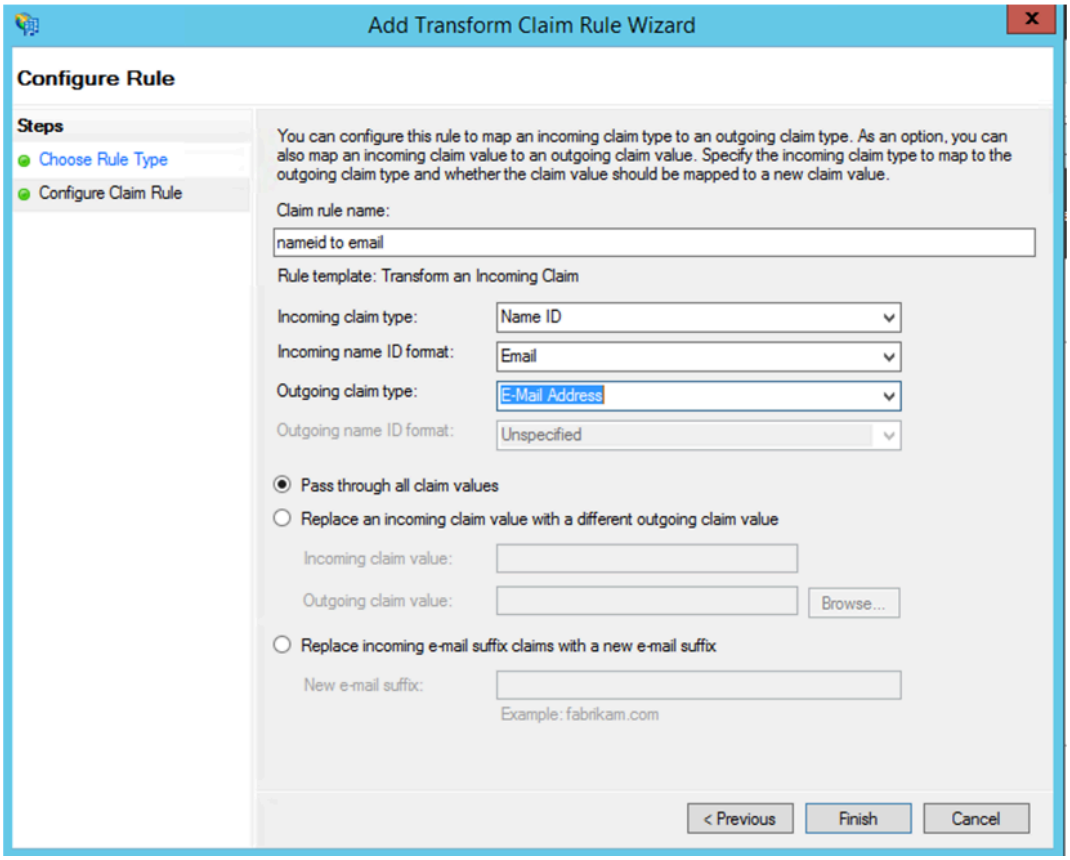


a) 完成以下步骤以完成添加声明提供商信任。添加完声明提供者信任后，将显示一个用于编辑声明规则的窗口。

b) 使用转换传入的声明添加声明规则。



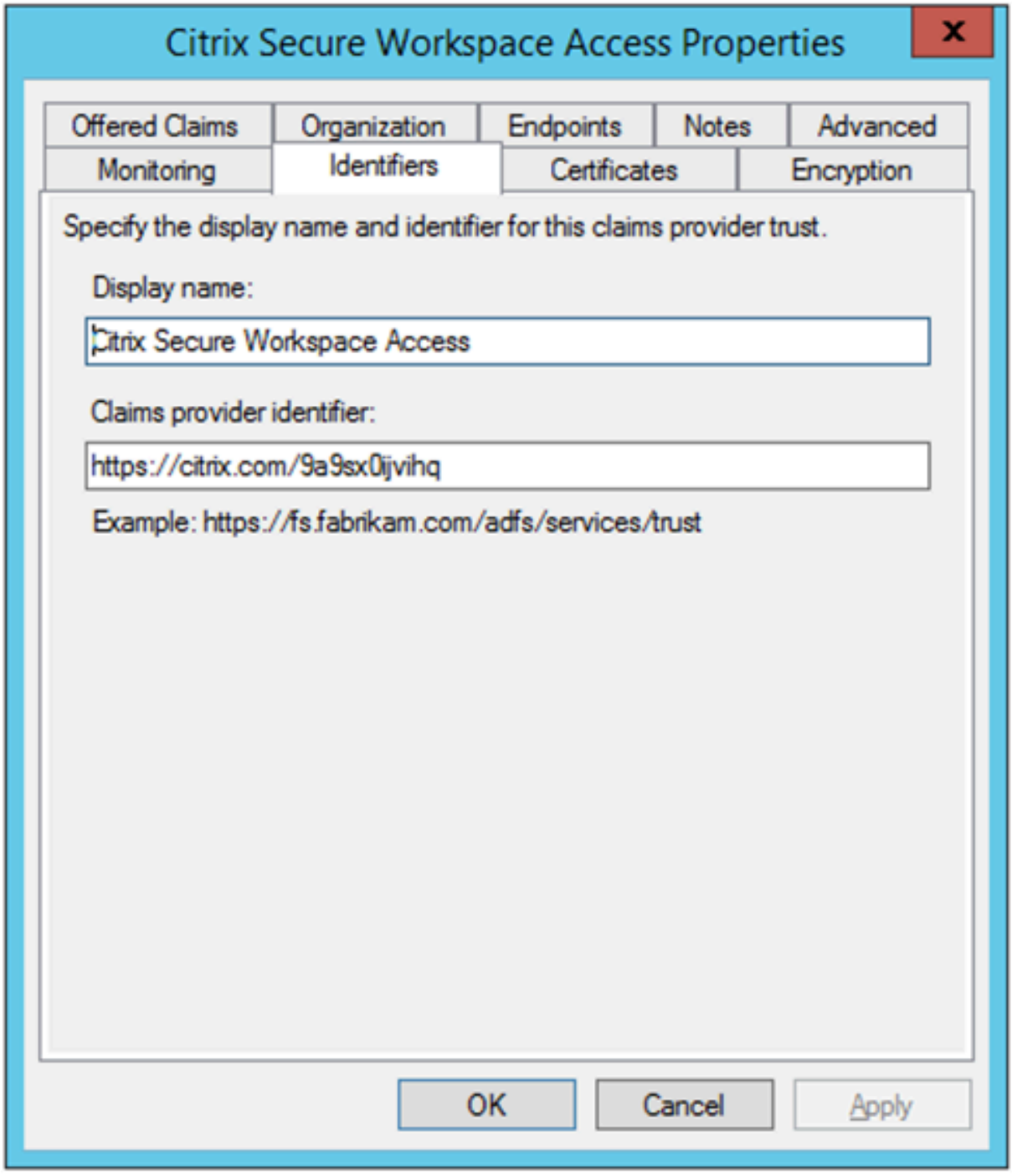
c) 如下图所示完成设置。如果您的 ADFS 接受其他声明，则使用这些声明并在 Secure Private Access 中相应地配置 SSO。



现在，您已配置声明提供程序信任，以确认 ADFS 现在信任适用于 SAML 的 Citrix Secure Private Access。

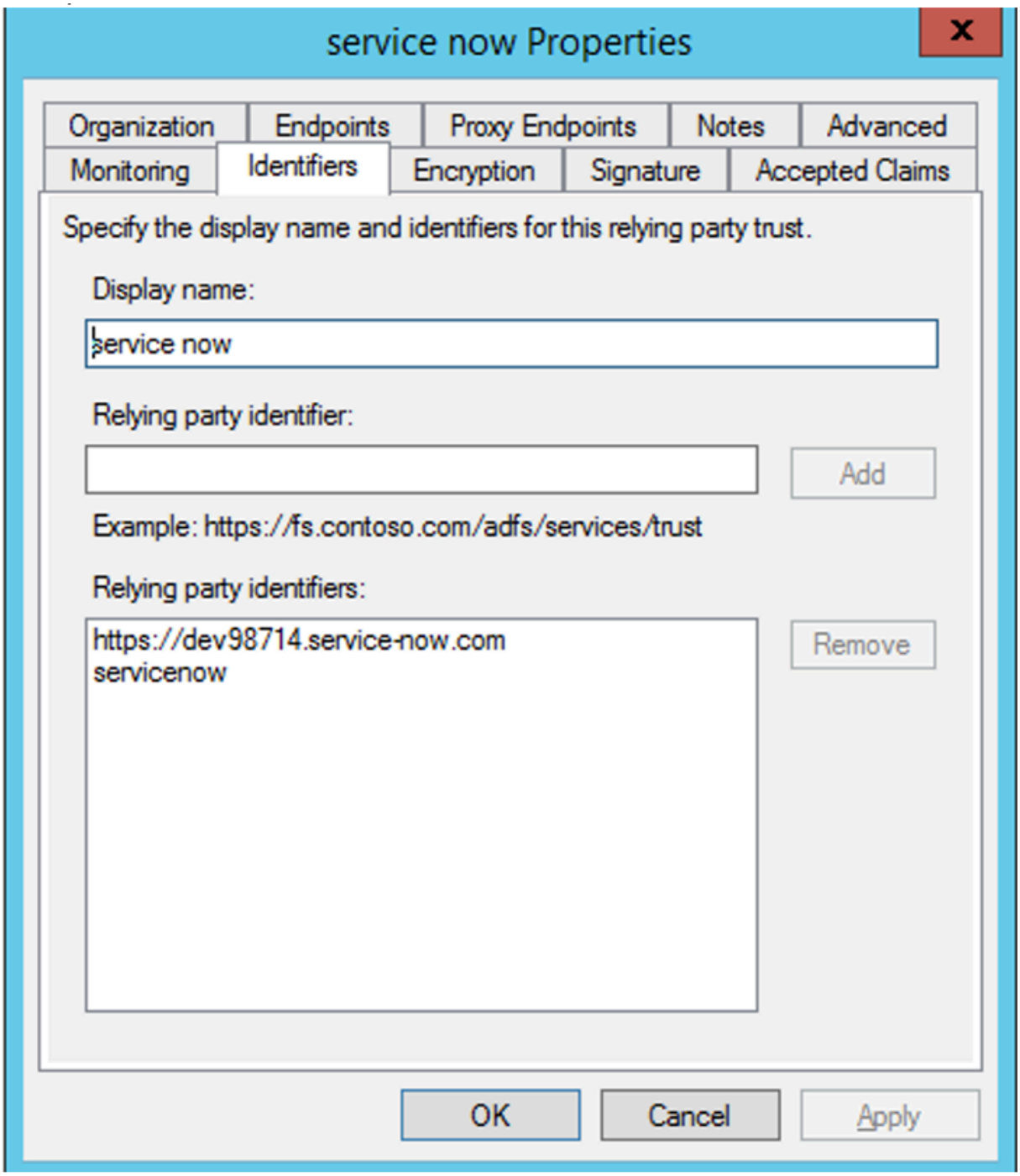
声明提供商信任 **ID**

记下您添加的声明提供商信任 ID。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。



中继方标识符

如果您的 SaaS 应用已使用 ADFS 进行身份验证，那么您必须已经为该应用添加了中继方信任。在 Citrix Secure Private Access 中配置应用程序时需要此 ID。



在 **IdP** 启动的流中启用中继状态

RelayState 是 SAML 协议的一个参数，用于识别用户在登录并定向到依赖方的联合服务器后访问的特定资源。如果 ADFS 中未启用 RelayState，则用户在向需要它的资源提供商进行身份验证后会看到错误。

对于 ADFS 2.0，必须安装更新 KB2681584 （更新汇总 2）或 KB2790338 （更新汇总 3）才能提供 RelayState 支持。ADFS 3.0 内置了 RelayState 支持。在这两种情况下，RelayState 仍然需要启用。

在 **ADFS** 服务器上启用 **RelayState** 参数

1. 打开文件。
   - 对于 ADFS 2.0，请在记事本中输入以下文件：%systemroot%\ inetpub\ adfs\ ls\ web.config
   - 对于 ADFS 3.0，请在记事本中输入以下文件：%systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.c
2. 在 microsoft.identityServer.web 部分中，为 useRelyStateForIdpInitiatedSignOn 添加一行，然后保存更改：
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - 对于 ADFS 2.0，运行 `IISReset` 以重新启动 IIS。
3. 对于这两个平台，请重新启动 Active Directory 联合身份验证服务 (`adfssrv`)`service`.
   注意事项：如果您有 Windows 2016 或 Windows 10，请使用以下 PowerShell 命令启用它。
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

链接到命令- https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

Citrix Secure Private Access 上的应用程序配置

您可以配置 IdP 启动的流程或 SP 启动的流程。在 Citrix Secure Private Access 中配置 IdP 或 SP 启动的流程的步骤相同，不同之处在于对于 SP 启动的流程，必须在 **UI** 中选中使用指定的 **URL**（**SP** 启动）启动应用程序 复选框。

IdP 启动的流程

1. 在设置 IdP 启动的流程时，配置以下内容。
   - 应用程序 **URL** —使用以下格式作为应用程序 URL。
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```
   - **ADFS FQDN** —ADFS 设置的 FQDN。

- **RP ID** —RP ID 是您可以从中继方信托中获得的 ID。它与中继方标识符相同。如果是 URL，则会进行 URL 编码。
- **IDP ID** —IdP ID 与声明提供商信任 ID 相同。如果是 URL，则会进行 URL 编码。

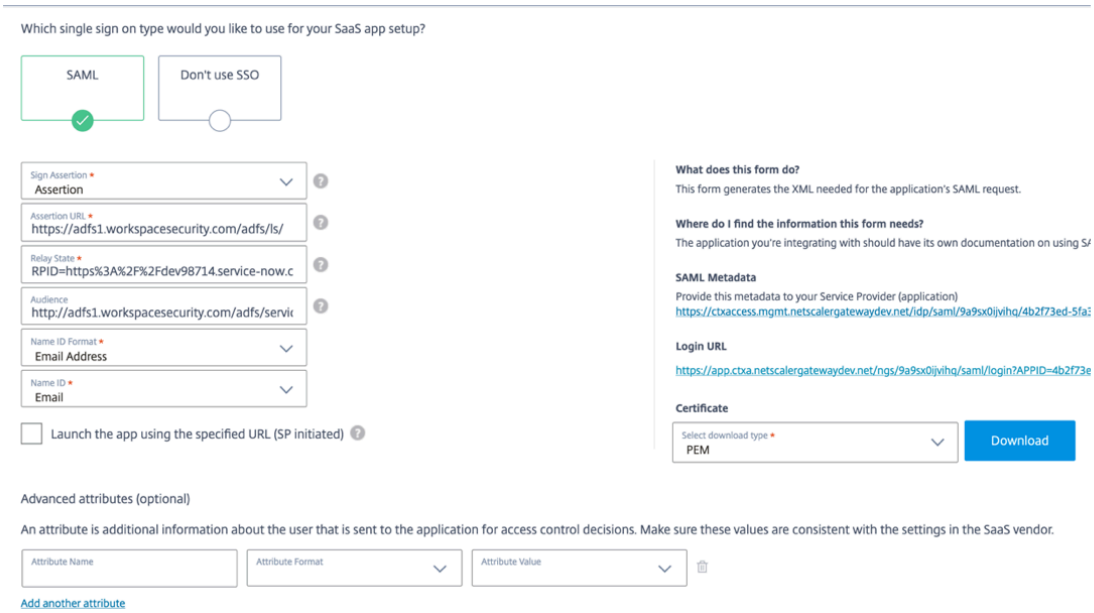
  示例： https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. SAML SSO 配置。

   以下是 ADFS 服务器的默认值。如果任何值发生了更改，请从 ADFS 服务器的元数据中获取正确的值。ADFS 服务器的联合元数据可以从其联合身份验证元数据端点下载，该端点可从 **ADFS >** 服务 **>** 端点了解该端点。

   - 断言 **URL** —`https://<adfs fqdn>/adfs/ls/`
   - 中继状态—中继状态对 IdP 启动的流非常重要。点击这个链接来正确构造它- `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     示例: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
   - 观众—`http://<adfsfqdn>/adfs/services/trust`
   - 有关其他 SAML SSO 配置设置，请参阅下图。有关详细信息，请参阅https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html



3. 将应用程序保存并订阅给用户。

SP 启动的流

对于 SP 启动的流程，请按照 **IDP** 启动的流程 部分中捕获的设置进行配置。此外，启用使用 指定的 **URL** 启动应用程序（**SP** 启动）复选框。

解决 **Secure Private Access** 问题

June 19, 2024

使用本主题来解决一些应用程序配置、身份验证和 SSO 或应用程序访问相关的问题。从 Secure Private Access 诊断日志的“信息代码”列中复制信息代码，然后在此页面上搜索该代码以找到相应的故障排除步骤。以下是一些常见问题解答，可帮助您更好地使用本主题。

常见问题解答

什么是 Secure Private Access 诊断日志?

在哪里可以找到 Secure Private Access 日志?

我可以在 Secure Private Access 诊断日志中找到哪些详细信息?

Secure Private Access 诊断日志中捕获了哪些事件?

如何使用 Secure Private Access 故障排除主题来解决我遇到的故障?

什么是信息代码？我在哪里找到他们?

什么是交易 ID？我该如何使用它?

Secure Private Access 的所有 PoP 地点在哪里?

如果我无法使用信息代码和错误查找表来解决我的故障，该怎么办?

信息代码查询表

以下错误查找表全面概述了用户在使用 Secure Private Access 服务时可能遇到的各种错误。

信息代码	说明	解决方案
0x180006、0x1800B7	应用程序启动失败，因为已超出应用程序 FQDN 长度	应用程序启动失败，因为已超出应用程序 FQDN 长度
0x180022	由于身份验证服务已关闭，应用程序启动失败	由于身份验证服务已关闭，应用程序启动失败

信息代码	说明	解决方案
0x180001、0x18001A、0x18001B、0x18008A 0x1800A9、0x1800AA、0x1800AB、0x1800AC 0x1800AD、0x1800AE、0x1800AF、0x1800B0 0x1800B1、0x1800B2、0x1800B3、0x180048	单点登录错误、Citrix Cloud 和本地连接器之间建立连接失败、SAML SSO 失败、应用程序 FQDN 无效	应用程序访问被拒绝
0x1800EF	连接 Connector Appliance 时出现问题	连接 Connector Appliance 时出现问题
0x18009D	DNS 查找/连接失败	Secure Browser 服务 - DNS 查找/连接错误
0x1800A0、0x1800A2、0x1800A3、0x1800A5 0x1800A6、0x1800A5	由于无法连接到后端 Web 应用程序，Web 应用程序启动失败	由于无法连接到后端 Web 应用程序，Web 应用程序启动失败
0x1800BC、0x1800BF	用户无权访问 Web/SaaS 应用程序	用户无权访问 Web/SaaS 应用程序
0x1800BD	用户无权访问用于 DirectAccess 的 Web/SaaS 应用程序	用户无权访问用于 DirectAccess 的 Web/SaaS 应用程序
0x1800D0	获取应用程序配置时 Citrix Secure Access 代理会话启动失败	获取应用程序配置时 Citrix Secure Access 代理会话启动失败
0x1800CD、0x1800CE、0x1800D6、0x1800EA	获取应用程序配置时 Citrix Secure Access 代理会话启动失败，Citrix Secure Access 代理应用程序在策略评估期间启动失败，Citrix Secure Access 代理应用程序启动失败	客户端请求格式不正确
0x1800DE	在策略评估期间，Citrix Secure Access 代理应用程序启动失败	在策略评估期间，Citrix Secure Access 代理应用程序启动失败
0x180055、0x1800DF、0x1800E3	应用程序受上下文策略限制，由于策略配置，访问被拒绝	一个或多个应用程序未在用户控制面板中列出
0x1800EB	由于不支持 IPv6，Citrix Secure Access 代理应用程序启动失败	由于不支持 IPv6，Citrix Secure Access 代理应用程序启动失败
0x1800EC、0x1800ED	由于 IP 地址无效，Citrix Secure Access 代理应用程序启动失败	由于 IP 地址无效，Citrix Secure Access 代理应用程序启动失败
0x10000001、0x10000002、0x10000003、0x10000004	由于网络问题，Citrix Secure Access 客户端登录失败	Citrix Secure Access 客户端存在网络连接可访问性问题

信息代码	说明	解决方案
0x10000006	由于中间有代理，Citrix Secure Access 客户端登录失败	代理服务器干扰客户端与服务的连接
0x10000007	由于证书颁发机构不可信，Citrix Secure Access 客户端登录失败	观察到不可信的服务器证书问题
0x10000008	由于证书无效，Citrix Secure Access 客户端登录失败	观察到服务器证书无效问题
0x1000000A	由于配置问题，Citrix Secure Access 客户端登录失败	登录失败，因为用户的配置为空
0x1000000B	由于连接失败，Citrix Secure Access 客户端登录失败	网络或最终用户终止了连接
0x10000010	由于会话过期，Citrix Secure Access 客户端登录失败	由于会话已过期，配置下载失败
0x10000013	由于配置列表庞大，Citrix Secure Access 客户端登录失败	Citrix Secure Access 客户端登录失败
0x11000003	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	由于会话已过期，控制通道建立失败
0x11000004	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	控制信道建立失败
0x11000005	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	控制信道建立失败
0x11000006	由于控制通道创建失败，Citrix Secure Access 客户端登录失败	由于网络问题，控制信道建立失败
0x12000001	Citrix Secure Access 客户端注销失败，因为会话已经过期	会话终止时无法注销
0x12000002	Citrix Secure Access 客户端注销失败，因为会话已经超时	会话被强制终止
0x13000001	由于会话过期，应用程序访问失败	由于会话已过期，应用程序启动失败
0x13000002	由于许可证不足，应用程序访问失败	由于许可证问题，应用程序启动失败
0x13000003、0x13000008、0x001800DF	由于禁止访问，应用程序访问失败，TCP/UDP 应用程序启动根据策略被拒绝	由于服务拒绝访问，应用程序启动失败
0x13000004、0x13000005	由于服务器不可用，应用程序访问失败	应用程序启动失败，因为客户端无法访问服务
0x13000007	由于访问策略被禁用或用户未订阅，应用程序访问失败	由于策略评估和配置验证失败，应用程序启动失败

信息代码	说明	解决方案
0x13000009	由于缺少路由条目，应用程序访问失败	由于应用程序域表中的问题，应用程序启动失败
0x1300000B	客户端关闭了连接	客户关闭了与 Secure Private Access 服务的连接
0x1300000C	通过 ZTNA 进行的 FQDN 解析失败	无法通过 DNS 服务器解析 FQDN
0x001800D3	登录时应用程序配置下载失败	未能获取已配置的应用程序目标列表
0x001800D9、0x001800DA	TCP/UDP 应用程序启动在解析策略评估响应期间失败，TCP/UDP 应用程序启动失败，策略评估期间的结果无效	应用程序配置问题
0x001800DB	TCP/UDP 应用程序启动失败，资源位置配置无效	资源位置问题
0x13000006、0x001800DC、0x001800DD	由于为应用程序配置了不支持的增强安全策略，TCP 应用程序启动失败；由于为 TCP 应用程序配置了不支持 Secure Browser 服务重定向，TCP 应用程序启动失败	增强的安全策略绑定到 HTTP 应用程序
0x001800DE	TCP/UDP 应用程序启动失败，因为没有找到目标的应用程序配置	找不到应用程序
0x001800EA	由于目标 FQDN 太长，TCP 应用程序启动失败	主机名长度超过 256 个字符
0x001800ED	由于目标 IP 无效，TCP 应用程序启动失败	IP 地址无效
0x001800EF	在与专用 TCP 服务器建立连接期间，TCP 应用程序启动失败	无法建立端到端连接
0x001800F5	由于 IPV6 地址的原因，UDP 应用程序启动失败	在应用程序请求中收到的 IPv6
0x001800F9	由于客户端连接中断，UDP 流量无法传送	UDP 流量未能传输
0x001800FF	UDP 数据流量传输失败	UDP 数据流量传输失败
0x10000401	Citrix Rendezvous 服务器拨号失败	由于网络连接问题，应用程序启动失败
0x10000402、0x1000040C	无法注册 Connector Appliance，UDP 网络连接初始化失败	Connector Appliance 未能注册到 Secure Private Access 服务
0x10000403、0x10000404、0x10000407、0x1000040A	连接错误，控制数据包传输失败，读取网关服务时出错控制数据包解析失败，写入网关服务时出错	连接 Connector Appliance 问题

信息代码	说明	解决方案
0x1000040B、0x1000040F、0x10000410 0x10000405、0x10000408、0x10000409、0x1000040D 0x1000040E，0x10000412	后端无法访问、UDP 数据包传输失败、UDP 数据包接收失败、写入后端时出错、后端关闭连接	Connector Appliance 和后端专用 TCP/UDP 服务器的连接问题
0x10000406	DNS 解析失败	Connector Appliance 无法解析 FQDN 的 DNS
0x10000411	网关服务关闭了连接	专用服务器连接已终止
0x10000413	确定连接断开原因时出错	无法连接或发送数据到私有服务 IP 或 FQDN
0x100508	用户上下文与访问规则条件不匹配	没有匹配的策略条件
0x100509	访问策略与应用程序无关	没有与应用程序相关的访问策略
0x10050C	用户可能有权使用的多个应用程序的策略评估结果	应用程序枚举信息
0x00180101	TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目	TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目
0x00180102	TCP/UDP 应用程序启动失败，因为连接器不正常	TCP/UDP 应用程序启动失败，因为连接器不正常
0x00180103	UDP/DNS 请求失败，因为无法访问连接器	UDP/DNS 请求失败，因为无法访问连接器
0x20580001	由于 NGS Cookie 已过期，无法加载页面	由于 NGS Cookie 已过期，无法加载页面
0x20580002	由于网络故障，访问策略提取失败	由于网络故障，访问策略提取失败
0x20580003	解析 JSON 网络令牌时访问策略提取失败	解析 JSON 网络令牌时访问策略提取失败
0x20580004	网络无法获取访问策略的详细信息	网络无法获取访问策略的详细信息
0x20580005	获取公共证书时策略提取失败	获取公共证书时策略提取失败
0x20580007	验证 JWT 签名时策略提取失败	验证 JWT 签名时策略提取失败
0x20580008	验证公共证书时策略提取失败	验证公共证书时策略提取失败
0x2058000A	无法确定存储环境以形成策略 URL	无法确定存储环境以形成策略 URL
0x2058000B	未能获得访问策略提取请求的响应	未能获得访问策略提取请求的响应

信息代码	说明	解决方案
0x2058000C	由于辅助 DS 身份验证令牌过期，访问策略提取失败	由于辅助 DS 身份验证令牌过期，访问策略提取失败
0x10200002	Connector Appliance 未注册	Connector Appliance 未注册
0x10200003	无法连接到 Connector Appliance	无法连接到 Connector Appliance
0x10000301	连接到 Citrix SPA 服务失败	连接到 Citrix Secure Private Access 服务失败
0x10000303、0x10000304	无法访问代理服务器	无法访问代理服务器
0x10000305	代理服务器身份验证失败	代理服务器身份验证失败
0x10000306	无法访问已配置的代理服务器	无法访问已配置的代理服务器
0x10000307	收到来自后端服务器的错误响应	收到来自后端服务器的错误响应
0x10000005	无法向目标 URL 发送请求	无法向目标 URL 发送请求
0x10000107	无法处理 SSO	无法处理 SSO
0x10000108、0x1000010B	无法处理 SSO，无法确定 SSO 设置	无法处理 SSO，无法确定 SSO 设置
0x10000101、0x10000102、0x10000103、0x10000104	FormFill SSO 失败，表单应用程序配置不正确	FormFill SSO 失败，表单应用程序配置不正确
0x1000010A	FormFill SSO 失败，表单应用程序配置不正确	FormFill SSO 失败，表单应用程序配置不正确
0x10000202	Kerberos SSO 失败	Kerberos SSO 失败
0x10000203	无法处理身份验证类型的 SSO	无法处理身份验证类型的 SSO
0x10000204	Kerberos SSO 失败但回退到 NTLM	Kerberos SSO 失败但回退到 NTLM
0x14000001	在 Citrix Workspace 应用程序中配置了多个具有 ZTNA 权限的帐户	在 Citrix Workspace 应用程序中配置了多个具有 ZTNA 权限的帐户

解决步骤

以下部分提供了大多数信息代码的解析步骤。对于未捕获解析步骤的代码，请联系 Citrix 支持人员。

一个或多个应用程序未在用户控制面板中列出

信息代码： 0x180055、0x1800DF、0x1800E3

由于上下文策略设置，某些用户或设备可能无法看到应用程序。诸如信任因素（Device Posture 或风险评分）之类的参数可能会影响应用程序的可访问性。

1. 从 `reasons` 列中为诊断日志 csv 文件中的错误代码 `0x18005C` 复制事务 ID。
2. 修改 csv 文件中的 `prod` 列过滤器，以显示名为 `SWA.PSE` 或 `SWA.PSE.EVENTS` 的组件中的事件。此筛选器仅显示与策略评估相关的日志。
3. 在 `reason` 列中搜索评估的策略有效负载。此负载显示用户订阅的所有应用程序的用户上下文的评估策略。
4. 如果策略评估显示该用户的应用程序被拒绝，可能的原因可能是：
    - 策略中的匹配条件不正确-检查 Citrix Cloud 中的应用程序策略配置
    - 策略中的匹配规则不正确-检查 Citrix Cloud 中的应用程序策略配置
    - 策略中的默认规则匹配不正确-这是一个漏洞案例。相应地调整条件。

用户无权访问 **Web/SaaS** 应用程序

信息代码： 0x1800BC、0x1800BF

用户可能点击了用户可能没有订阅的应用程序链接。

确保用户订阅了应用程序。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并转到订阅选项卡。
3. 确保目标用户在订阅列表中有一个条目。

后端应用程序性能缓慢

信息代码：0x18000F

在某些情况下，由于资源位置的连接器可能已关闭，或者后端服务器本身可能没有响应，客户网络不稳定。

1. 确保 Connector Appliance 在地理位置上靠近后端服务器，以排除网络延迟。
2. 检查后端服务器的防火墙是否未阻止 Connector Appliance。
3. 检查客户端是否正在连接到最近的云 POP。

    例如，`nslookup nssvc.dnsdiag.net` 在客户端上，答案中的规范名称表示特定于地理位置的服务器，例如 `aws-us-w.g.nssvc.net`.

应用程序启动失败，因为已超出应用程序 **FQDN** 长度

信息代码： 0x180006、0x1800B7

应用程序 FQDN 的长度不得超过 512 个字符。在应用程序配置页面中检查应用程序 FQDN。确保长度大小不超过 512 字节。

1. 转到管理控制台上的应用程序选项卡。
2. 查找 FQDN 超过 512 个字符的应用程序。
3. 编辑应用程序并修复应用程序 FQDN 长度。

已超出应用程序详情长度

信息代码： 0x18000E

检查策略是否阻止应用程序访问。

1. 转到访问策略。
2. 查找应用程序有权限的策略。
3. 查看最终用户的策略规则和条件。

应用程序访问被拒绝

信息代码：0x180001、0x18001A、0x18001B、0x18008A、0x1800A9、0x1800AB、0x1800AC、0x1800AD、0x1800AE、0x1800AF、0x1800B0、0x1800B1、0x1800B2、0x1800B3、0x180048

这与情境策略有关，在这种策略中，策略拒绝为给定用户提供应用程序。

检查策略是否阻止应用程序访问

1. 转到访问策略。
2. 查找应用程序有权限的策略。
3. 查看最终用户的策略规则和条件。

未列举应用程序

由于策略拒绝或未启用 Secure Private Access 集成，枚举列表中可能缺少应用程序。

- 如果必须为某些应用程序启用访问权限，但您看到的应用程序为零，请尝试启用 Secure Private Access 集成。
  - 登录 Citrix Cloud。
  - 从汉堡菜单中选择“**Workspace** 配置”，然后单击“服务集成”。
  - 单击“Secure Private Access”中的省略号按钮，然后单击“启用”。
- 如果已经启用了 Secure Private Access 集成，请将其禁用，然后再次启用以查看是否有任何应用程序。

连接 **Connector Appliance** 时出现问题

信息代码： 0x1800EF

由于与本地连接器的 TCP 连接不可用，应用程序路由失败。

查看来自控制器组件的事件

1. 在诊断日志 csv 文件中查找错误代码 0x1800EF 的 transaction ID。
2. 在 csv 文件中过滤与事务 ID 匹配的所有事件。
3. 此外，筛选 csv 文件中匹配的 prod 列 SWA.GOCTRL。

   如果您看到包含 connectType 消息 multiconnect::success? 的事件，则：

   - 这表明通道建立请求已成功中继到控制器。
   - 检查日志消息中的 Resource Location 是否正确。如果不正确，请在 Citrix 管理门户的应用程序配置部分中修复资源位置。
   - 检查日志消息中的 VDA Ip and Port 是否正确。VDA IP 和端口表示后端应用程序 IP 和端口。如果不正确，请在 Citrix 管理门户的应用程序配置部分中修复应用程序 FQDN 或 IP 地址。
   - 如果您没有发现任何前面提到的问题，请继续查看 连接器事件 。

   如果您看到带有 connectType 消息的事件 connect::failure 或 multiconnect::success，那么；

   - 检查此日志消息的建议修复是否显示- Check if connector is still connected to same pop。这表示资源位置的连接器可能已关闭。继续查看 连接器事件。
   - 如果未看到前面提到的消息，请联系 Citrix 客户支持。

   如果您看到带有 connectType 消息的事件 IntraAll::failure，请联系 Citrix 客户支持。

查看连接器组件中的事件

1. 在诊断日志 csv 文件中查找错误代码 0x1800EF 的 transaction ID。
2. 在 csv 文件中过滤与事务 ID 匹配的所有事件。
3. 同时筛选 csv 文件中匹配的 prod 列 SWA.ConnectorAppliance.WebApps。
4. 如果您看到包含 status 作为 failure 的事件，则：

   - 查看每个失败事件的 reason 消息。
   - UnableToRegister 表示连接器无法成功注册到 Citrix Cloud。请联系 Citrix 支持部门。
   - IsProxyRequiredCheckError、ProxyDialFailed、ProxyConnectionFailed、ProxyAuthenticationFailure 或 ProxiesUnReachable 表示连接器无法通过代理配置解析后端 URL。检查代理配置是否正确。
   - 有关进一步调试的信息，请参阅 连接器 SSO 事件。

单点登录错误

对于单点登录，将在应用程序启动期间从应用程序配置中提取和应用不同的 SSO 属性。如果该特定用户没有属性或者属性不正确，则单点登录可能会失败。确保配置看起来正确。

1. 转到访问策略。
2. 查找应用程序有权限的策略。
3. 查看最终用户的策略规则和条件。

表单 SSO、Kerberos 和 NTLM 等 SSO 方法由本地连接器执行。查看连接器中的以下诊断日志。

查看连接器组件中的 **SSO** 事件

1. 在匹配 `SWA.ConnectorAppliance.WebApps` 的 csv 文件中过滤 `component name`。
2. 您是否看到状态为“失败”的事件？
   - 查看每个失败事件的消息。
   - `IsProxyRequiredCheckError`、`ProxyDialFailed`、`ProxyConnectionFailed`、`ProxyAuthenticationFailure` 或 `ProxiesUnReachable` 表示连接器无法通过代理配置解析后端 URL。检查代理配置是否正确。
   - `FailedToReadRequest` 或 `RequestReceivedForNonSecureBrowse` 或 `UnableToRetrieveUserCredentials` 或 `CCSPolicyIsNotLoaded` 或 `FailedToLoadBaseClient` 或 `ProcessConnectionFailure` 或 `WebAppUnSupportedAuth` 表示通道出现故障。请联系 Citrix 支持部门。
   - `UnableToConnectTargetServer` 表示无法从连接器访问后端服务器。再次检查后端配置。
   - `IncorrectFormAppConfiguration` 或 `NoLoginFormFound` 或 `FailedToConstructForLo` 或 `FailedToLoginViaFormBasedAuth` 表示基于表单的身份验证失败。查看 Citrix 管理门户中应用程序配置中的表单 SSO 配置部分。
   - `NTLMAuthNotFound` 表示基于 NTLM 的身份验证失败。查看 Citrix 管理门户中应用程序配置中的 NTLM SSO 配置部分。
   - 有关进一步的调试，请参阅 连接器事件。

由于身份验证服务已关闭，应用程序启动失败

信息代码： 0x180022

Secure Private Access 允许管理员配置第三方身份验证服务，例如传统的 Active Directory、AAD、Okta 或 SAML。这些身份验证服务中断可能会导致出现此问题。

检查第三方服务器是否已启动且可访问。

SAML SSO 失败

信息代码：0x18008A、0x1800A9、0x1800AA、0x1800AB、0x1800AC、0x1800AD、0x1800AE、0x1800AF、0x1800B0、0x1800B1、0x1800B2、0x1800B3

在 IdP 启动应用程序时，用户在启动应用程序时会面临身份验证失败，或者在 SP 启动时可能会看到无法访问的链接。检查 Secure Private Access 服务端的 SAML 应用程序配置以及服务提供商配置。

Secure Private Access 配置：

1. 转到应用程序选项卡。
2. 寻找有问题的 SAML 应用程序。
3. 编辑应用程序，然后转到单点登录选项卡。
4. 请检查以下字段。

    - 断言 URL
    - 中继状态
    - 受众
    - 名称 ID 格式、名称 ID 和其他属性

服务提供商配置：

1. 登录到服务提供商。
2. 转到 **SAML** 设置。
3. 检查 IdP 证书、受众和 IdP 登录 URL。

如果配置看起来正确，请联系 Citrix 支持部门。

应用程序 **FQDN** 无效

信息代码： 0x180048

客户管理员可能提供了无效的 FQDN 或后端服务器上的 DNS 解析失败的 FQDN。

在这种情况下，最终用户会在网页上看到错误。检查应用程序设置。

SaaS 应用程序验证　检查是否可以从网络访问该应用程序。

Web 应用程序验证

1. 转到应用程序选项卡。
2. 编辑有问题的应用程序。
3. 转到 应用程序详细信息 页面。
4. 检查 URL。该 URL 必须可在内联网或 Internet 中访问。

Secure Browser 服务 **- DNS** 查找**/**连接失败

信息代码： 0x18009D

通过 Remote Browser Isolation 服务获得的浏览体验不正常。检查最终用户正在尝试连接的后端服务器。

1. 转到后端服务器，检查它是否已启动并正在运行，是否能够接收请求。

2. 如果它正在停止与后端服务器的连接，请检查代理设置。

> 注意：
>
> Citrix Remote Browser Isolation 服务以前称为 Secure Browser 服务。

CWA Web-Web 应用程序的 **DNS** 查找/连接错误

信息代码： 0x1800A0、0x1800A2、0x1800A3、0x1800A5、0x1800A6、0x1800A7

在公司网络内运行的 Web 应用程序的浏览体验不佳。

1. 筛选无法解析的 FQDN 的诊断日志。
2. 检查企业网络内部后端服务器的可访问性。
3. 检查代理设置，查看连接器是否被阻止访问后端服务器。

直接访问-错误配置为 **Web** 应用程序

由于 Web 应用程序流量始终通过连接器路由，因此在它们上配置直接访问会导致应用程序访问错误。

检查路由域表和应用程序配置之间是否存在冲突的配置。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并检查是否启用了直接访问。
3. 检查路由域表中的应用程序 FQDN 是否已标记为内部。

用户无权访问用于 **DirectAccess** 的 **Web/SaaS** 应用程序

信息代码： 0x1800BD

应用程序配置禁止直接访问来自基于浏览器的客户端的流量。

确保用户订阅了应用程序。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并检查无代理访问配置。

增强的安全策略 **- Secure Browser** 服务配置错误

信息代码： 0x1800C3

看到的行为不符合策略规则的预期。查看上下文访问策略。

1. 转到策略选项卡。
2. 检查与应用程序相关的策略。
3. 查看这些策略的规则。

增强的安全策略-策略配置错误

看到的行为不符合策略规则的预期。检查增强的安全设置。

1. 转到应用程序。
2. 单击访问策略选项卡。
3. 检查 可用安全限制：部分中的设置。

获取应用程序配置时 **Citrix Secure Access** 代理会话启动失败

信息代码： 0x1800D0

Citrix Secure Access 应用程序无法成功建立通往 Citrix Cloud 的完整通道。

1. 查看 TCP/UDP 应用程序的路由域配置。
2. 确保最大条目数完全在 16k 限制之内。

TCP/UDP 应用程序-格式错误的客户端请求

信息代码： 0x1800CD、0x1800CE、0x1800D6、0x1800EA

VPN 通道未建立，或者某些 FQDN 可能未通过通道传输。

1. 确保请求不是由中间的代理捏造或重建的。
2. 疑似中间人袭击。

TCP/UDP 应用程序 **- Secure Browser** 服务重定向配置错误

信息代码： 0x1800DD

Remote Browser Isolation 服务重定向只能应用于 Web 应用程序，不能应用于 TCP/UDP 应用程序。查看 Secure Private Access 服务 GUI 中的应用程序配置。

> 注意：
>
> Citrix Remote Browser Isolation 服务以前称为 Secure Browser 服务。

在策略评估期间，**Citrix Secure Access** 代理应用程序启动失败

信息代码： 0x1800DE

确保 Citrix Secure Access 客户端通过通道传输的所有内部 FQDN 在路由域表中都有相应的条目。

由于不支持 **IPv6**，**Citrix Secure Access** 代理应用程序启动失败

信息代码： 0x1800EB

查看路由域条目。确保表中没有 IPV6 条目。

由于 **IP** 地址无效，**Citrix Secure Access** 代理应用程序启动失败

信息代码：0x1800EC，0x1800ED

查看路由域条目。确保 IP 地址有效且指向正确的后端。

Citrix Secure Access 客户端存在网络连接可访问性问题

信息代码： 0x10000001、0x10000002、0x10000003、0x10000004

1. 检查客户端计算机网络是否可访问。如果网络可以访问，请联系 Citrix 支持人员并提供客户端调试日志。
2. 检查代理或防火墙是否阻塞了网络。

要收集客户端调试日志，请参阅如何收集客户端日志。

代理服务器干扰客户端与服务的连接

信息代码： 0x10000006

1. 检查客户端计算机网络是否可访问。
2. 检查客户端中的代理配置是否正确。
3. 如果两者都没有问题，请联系 Citrix 支持人员提供客户端调试日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

观察到不可信的服务器证书问题

信息代码： 0x10000007

联系 Citrix 支持部门，检查服务器证书是否由有效 CA 正确生成。

观察到服务器证书无效问题

信息代码： 0x10000008

联系 Citrix 支持人员，检查服务器证书是自签名证书、已过期证书还是来自不可信来源。

登录失败，因为用户的配置为空

信息代码： 0x1000000A

1. 确保至少配置了一个 TCP/UDP/HTTP 应用程序。有关详细信息，请参阅添加和管理应用程序。
2. 确保“应用程序域”表（“**Secure Private Access**” **>** “设置” **>** “应用程序域”）不为空或未禁用所有条目。在 TCP/UDP/HTTP 应用程序中配置的目的地将自动添加到此表中。

建议不要删除或禁用活动的 TCP/UDP/HTTP 应用程序的目标或 URL。

连接被网络和/或最终用户终止

信息代码： 0x1000000B

在 ZTNA 会话连接期间，检查网络是否中断或最终用户是否取消了连接。

由于会话已过期，配置下载失败

信息代码： 0x10000010

在 ZTNA 会话配置下载请求期间，VPN 会话可能已过期。尝试重新登录 Citrix Secure Access 客户端。

Citrix Secure Access 客户端登录失败

信息代码： 0x10000013

由于配置大小超过最大配置限制，Citrix Secure Access 客户端无法登录。

1. 在 **Secure Private Access >** 设置 **>** 应用程序域中查看 TCP/UDP 应用程序的路由域配置
2. 确保条目数量不大。如果条目列表很大，请禁用或删除未使用的目的地。

   如果目标列表预计超过 1000 个，请尝试通过更新 ConfigSize 注册表项来增加最大配置下载大小。有关详细信息，请参阅 Citrix Gateway VPN 客户端注册表项。

由于会话已过期，控制通道建立失败

信息代码： 0x11000003

由于会话已过期，建立 DNS 请求的控制通道出现故障。

在控制通道设置期间，ZTNA 会话可能已过期。

尝试重新登录 Citrix Secure Access 客户端。

控制信道建立失败

信息代码： 0x11000004

建立 DNS 请求的控制通道已失败。

- 保持资源位置健康：

1. 登录 Citrix Cloud。
2. 从汉堡菜单中单击“资源位置”。
3. 在相应的资源位置对 Connector Appliance 运行运行状况检查。
4. 如果这不能解决问题，请尝试重新启动连接器虚拟机。

- 维护 **HA Connector Appliance**：

1. 登录 Citrix Cloud。
2. 从汉堡菜单中单击“资源位置”。
3. 确保预期的资源位置至少有两个 Connector Appliance。

请务必满足以下各项条件：

- 资源位置 LAN 处于工作状态。
- 中间没有防火墙或代理来阻止 Connector Appliance 连接到服务或后端服务器。
- 客户端网络运行正常。
- 后端私有服务器已启动并正在运行。
- DNS 服务器已启动并正在运行。
- FQDN 是可解析的。

如果您符合上述建议，请执行以下操作。

1. 从诊断日志中获取此错误的交易 ID。
2. 在 Secure Private Access 控制面板中筛选与交易 ID 匹配的所有事件。
3. 检查客户端或 Connector Appliance 或服务诊断日志中是否出现任何与事务 ID 匹配的错误。然后相应地采取适当的操作。
4. 检查在应用程序域表（**Secure Private Access >** 设置 **>** 应用程序域）中为目标选择的资源位置是否正确。
5. 检查应用程序是否配置了正确的端口、IP 范围和域。有关详细信息，请参阅添加和管理应用程序。

如果您仍然无法解决问题，请联系 Citrix 支持部门，提供与事务 ID 和客户端日志相对应的错误代码。

要收集客户端调试日志，请参阅如何收集客户端日志。

控制信道建立失败

信息代码： 0x11000005

控制通道（用于 DNS 请求）建立失败。

1. 检查 Secure Private Access 服务许可证授权。
2. 如果未获得授权，请联系 Citrix 支持部门检查许可证。

有关详细信息，请参阅 https://www.citrix.com/buy/licensing/product.html。

由于网络问题，控制信道建立失败

信息代码： 0x11000006

由于网络问题，控制通道（用于 DNS 请求）建立失败。

1. 检查 Secure Private Access 服务是否可访问。
2. 如果无法访问，请使用错误代码和客户端日志与 Citrix 支持部门联系。

要收集客户端调试日志，请参阅如何收集客户端日志。

由于 **IIP** 不足，控制信道建立失败

信息代码： 0x11000007

由于 IIP 不足，控制通道（用于 DNS 请求）建立失败。

请联系 Citrix 支持部门，提供错误代码和客户端日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

会话终止时无法注销

出现此问题可能是因为客户端计算机（键盘或鼠标）的空闲时间超过了配置的超时时间。

信息代码： 0x12000001

尝试重新登录 Citrix Secure Access 客户端。

会话被强制终止

当达到配置的强制超时时，会话将被强制终止。

信息代码： 0x12000002

尝试重新登录 Citrix Secure Access 客户端。

由于会话已过期，应用程序启动失败

信息代码： 0x13000001

1. ZTNA 会话在应用程序启动期间已过期。
2. 尝试重新登录 Citrix Secure Access 客户端。

由于许可证问题，应用程序启动失败

信息代码： 0x13000002

1. 检查 Secure Private Access 服务许可证是否有效。
2. 如果未获得授权，请联系 Citrix 支持部门检查许可证。

有关详细信息，请参阅 https://www.citrix.com/buy/licensing/product.html。

由于服务拒绝访问，应用程序启动失败

信息代码： 0x13000003、0x13000008、0x001800DF

根据用户和应用程序的策略配置，应用程序启动被拒绝。

确保满足以下条件。

- 多个应用程序（HTTP、HTTPS、TCP、UDP）中不使用相同的目的地
- 多个应用程序上没有重叠的目的地。
- 访问策略绑定到应用程序。

还要检查为被拒绝的应用程序配置的策略的条件和操作。然后查看策略条件和操作。

有关详细信息，请参阅 访问策略。

应用程序启动失败，因为客户端无法访问服务

信息代码： 0x13000004、0x13000005

1. 检查 Secure Private Access 服务是否可访问。
2. 再次启动应用程序。
3. 如果长时间无法访问该应用程序，请使用错误代码和客户端日志与 Citrix 支持人员联系。

要收集客户端调试日志，请参阅如何收集客户端日志。

由于策略评估和配置验证失败，应用程序启动失败

信息代码： 0x13000007

由于 Secure Private Access 服务未能通过策略评估和配置验证，应用程序启动失败。

找不到访问目的地的应用程序。

由于服务拒绝访问，应用程序启动失败。

由于应用程序域表中的问题，应用程序启动失败

信息代码： 0x13000009

应用程序启动失败，因为应用程序域表中没有访问目标的条目。

在“**Secure Private Access**”**>**“设置”**>**“应用程序域”中检查应用程序的路由条目配置是否正确。

客户关闭了与 **Secure Private Access** 服务的连接

信息代码： 0x1300000B

1. 检查最终用户是否手动关闭了连接。
2. 如果不是，请联系 Citrix 支持部门，提供错误代码和客户端日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

无法通过 **DNS** 服务器解析 **FQDN**

信息代码： 0x1300000C

当 Connector Appliance 无法解析 FQDN 的 DNS 时，就会出现此问题。

1. 在 DNS 服务器中检查相应应用程序 FQDN 的 DNS 条目。
2. 确保在 Connector Appliance 中配置了适当的 DNS 服务器。有关详细信息，请参阅 Connector Appliance 管理页面上的配置网络设置。

找不到应用程序

信息代码： 0x001800DE

您可能无法找到用户访问目标的应用程序。如果应用程序域表中缺少目标到资源位置的映射，则可能会出现这种情况。

- 确保为访问的目标配置 TCP/UDP 或 HTTP 应用程序。
- 确保用户订阅了所访问目标的应用程序。

1. 转到管理门户中的应用程序。
2. 编辑应用程序并转到订阅选项卡。
3. 确保目标用户在订阅列表中有一个条目。
4. 确保 应用程序域 表有目标和相应的资源位置。

未能获取已配置的应用程序目标列表

信息代码： 0x001800D3

- 确保至少配置了一个 TCP/UDP/HTTP 应用程序。有关详细信息，请参阅添加和管理应用程序。
- 确保应用程序域表（**Secure Private Access >** 设置 **>** 应用程序域）页面不为空或未禁用所有条目。在 TCP/UDP/HTTP 应用程序中配置的目的地将自动添加到此表中。建议不要在应用程序域表中删除或禁用活动 TCP/UDP/HTTP 应用程序的目标或 URL。

应用程序配置问题

应用程序配置包含特殊字符或某些策略配置问题。

信息代码： 0x001800D9、0x001800DA

请务必满足以下各项条件：

- 应用程序配置不包含不支持的字符。
- 目标 IP 地址或 IP 地址范围或 IP CIDR 是有效的。
- 应用程序目标已在应用程序域表（**Secure Private Access >** 设置 **>** 应用程序域）中启用。
- 策略已配置并绑定到相应的应用程序。
- 访问策略配置正确。

资源位置问题

信息代码： 0x001800DB

- 确保配置了资源位置。
    1. 在 Citrix Cloud 汉堡菜单中，选择资源位置。
    2. 确保配置了预期的资源位置并且资源位置处于活动状态。
- 确保在应用程序域表（**Secure Private Access >** 设置 **>** 应用程序域）中为目标选择了正确的资源位置。

在 TCP/UDP/HTTP 应用程序中配置的目的地将自动添加到此表中。建议不要在“应用程序域”表中删除或禁用活动 TCP/UDP/HTTP 应用程序的目标或 URL。

增强的安全策略绑定到 **HTTP** 应用程序

信息代码： 0x001800DC、0x001800DD、0x13000006

绑定了增强安全策略的 HTTP 应用程序可通过 Citrix Secure Access 客户端进行访问。

- 确保 TCP/UDP 和 HTTP 应用程序不使用相同的目的地。
- 如果为 HTTP/HTTPS 应用程序启用了增强的安全策略，则建议仅通过 Citrix Workspace 应用程序或 Citrix Remote Browser Isolation 服务访问该应用程序。
- 禁用 HTTP/HTTPS 应用的增强安全控制，以便通过 Citrix Secure Access 客户端访问该应用。
  - 转到 Secure Private Access 管理门户。
  - 单击“应用程序”选项卡，搜索访问的目标 HTTP/HTTPS 应用程序的策略名称。
  - 单击“访问策略”选项卡，搜索之前确定的策略名称。
  - 选择策略并单击“编辑”。
  - 将操作从“允许有限制的访问”更改为“允许访问”。

有关配置的详细信息，请参阅 添加和管理应用程序。

> 注意：
>
> Citrix Remote Browser Isolation 服务以前称为 Secure Browser 服务。

主机名长度超过 **256** 个字符

信息代码： 0x001800EA

在应用程序启动请求中收到的主机名超过 256 个字符。

建议 FDQN 字符不要超过 256 个字符。

IP 地址无效

信息代码： 0x001800ED

在应用程序启动请求中收到的 IP 地址无效。

建议仅从客户端访问有效的私有 IP 地址。

无法建立端到端连接

信息代码： 0x001800EF

无法在客户端和资源位置中配置的服务器之间建立端到端连接。

- 确保资源位置处于活动状态。
  - 在 Citrix Cloud 汉堡菜单中，选择资源位置。
  - 在相应的资源位置对 Connector Appliance 运行运行状况检查。
  - 如果这不能解决问题，请重新启动连接器虚拟机。
- 保持高可用性 Connector Appliance
  - 在 Citrix Cloud 汉堡菜单中，选择资源位置。
  - 确保资源位置至少有两个 Connector Appliance。
- 请务必满足以下各项条件：
  - 资源位置 LAN 处于工作状态。
  - 中间没有防火墙或代理阻止 Connector Appliance 访问服务或后端服务器。
  - 客户端网络运行正常。
  - 后端私有服务器运行良好。
  - DNS 服务器运行正常。
  - FQDN 是可解析的。

如果这些没有问题，请执行以下操作：

1. 从诊断日志中获取此错误的交易 ID。
2. 在 Secure Private Access 服务控制面板中筛选与交易 ID 匹配的所有事件。
3. 从 Secure Private Access 服务控制面板中检查与交易 ID 对应的诊断日志，然后相应地采取相应的措施。
4. 检查是否在应用程序域表（**Secure Private Access >** 设置 **>** 应用程序域）中选择了正确的资源位置作为目标。
5. 检查应用程序是否配置了正确的 IP 地址、端口和 FQDN（**Secure Private Access >** 应用程序）。

如果这些步骤都不能解决问题，请联系 Citrix 支持并提供与事务 ID 相关的错误代码并收集客户端日志。

要收集客户端调试日志，请参阅如何收集客户端日志。

在应用程序请求中收到的 **IPv6**

信息代码： 0x001800F5

在不支持的应用程序请求中收到的 IPv6。目前，仅支持 IPv4。

编辑应用程序以修复应用程序 IP 地址问题。

1. 转到 Secure Private Access 管理门户。
2. 单击应用程序选项卡。
3. 搜索应用程序，然后单击“编辑”。

有关详细信息，请参阅 添加和管理应用程序。

UDP 流量未能传输

信息代码： 0x001800F9

由于客户端连接中断，UDP 流量无法传输

1. 检查客户端会话是否处于活动状态。
2. 注销然后重新登录。

UDP 数据流量传输失败

信息代码： 0x001800FF

- 在 Secure Private Access 服务控制面板中查找错误代码的交易 ID 并筛选与交易 ID 匹配的所有事件。
- 检查与事务 ID 匹配的其他组件中是否出现任何错误。如果在其他组件中发现问题，则采取相应的措施。
- 如果这不能解决问题，请联系 Citrix 支持部门，提供错误代码和相应的交易 ID。

由于网络连接问题，应用程序启动失败

信息代码： 0x10000401

由于 Connector Appliance 和 Secure Private Access 服务之间的网络连接问题，应用程序启动失败

1. 检查 Connector Appliance 的公共 Internet 连接。
2. 检查是否有任何代理或防火墙规则阻止了连接。
3. 如果有任何代理导致了问题，请绕过代理，然后再次尝试启动应用程序。
4. 检查 Connector Appliance 运行状况（**Citrix Cloud >** 资源位置）。

有关网络设置的详细信息，请参阅 Connector Appliance 的网络设置。

Connector Appliance 未能注册到 **Secure Private Access** 服务

信息代码： 0x10000402，0x1000040C

1. 转到 Connector Appliance 管理页面并查看连接器摘要。
2. 如果连接器状态不佳，则转到管理门户中的资源位置。
3. 在相应的资源位置对 Connector Appliance 运行运行状况检查。
4. 如果运行状况检查失败，请重新启动连接器虚拟机。
5. 检查连接器摘要并再次运行运行状况检查。

有关网络设置的详细信息，请参阅 Connector Appliance 的网络设置。

连接 **Connector Appliance** 问题

信息代码：0x10000403、0x10000404、0x10000407、0x1000040A、0x1000040B、0x1000040F、0x10000410

- 在交易 ID 中查找错误代码。
- 在 Secure Private Access 控制面板中筛选与交易 ID 匹配的所有事件。
- 检查与事务 ID 匹配的其他组件中是否出现任何错误（如果找到），相应的解决方法与该错误代码相匹配。
- 如果在其他组件中未发现错误，请执行以下操作：
  - 转到 Connector Appliance 管理页面。
  - 下载诊断报告。有关详细信息，请参阅 生成诊断报告。
  - 捕获数据包跟踪。有关详细信息，请参阅 验证您的网络连接。
- 请联系 Citrix 支持部门，提供此诊断报告和数据包跟踪信息以及错误代码和交易 ID。

Connector Appliance 和后端专用 **TCP/UDP** 服务器的连接问题

信息代码： 0x10000405、0x10000408、0x10000409、0x1000040D、0x1000040E、0x10000412

Connector Appliance 与后端专用 TCP/UDP 服务器存在连接问题。

- 检查最终用户尝试连接的后端服务器是否已启动并正在运行并且能够接收请求。
- 从公司网络内部检查后端服务器的可访问性。
- 检查代理设置，查看连接器是否被阻止访问后端服务器。
- 如果请求基于 FQDN 的应用程序，请在 DNS 服务器中检查相应应用程序的 DNS 条目。

Connector Appliance 无法解析 **FQDN** 的 **DNS**

信息代码： 0x10000406

- 在 DNS 服务器中检查相应应用程序 FQDN 的 DNS 条目。
- 确保在 Connector Appliance 中配置了适当的 DNS 服务器。有关详细信息，请参阅 Connector Appliance 管理页面上的配置网络设置。

专用服务器连接已终止

信息代码： 0x10000411

与专用服务器的连接由客户端或 Secure Private Access 服务终止。

1. 检查最终用户是否已关闭应用程序。
2. 检查与该日志的交易 ID 相匹配的其他诊断日志，并相应地采取相应的操作。

3. 再次启动应用程序。
4. 如果这不能解决问题，请联系 Citrix 支持部门，提供错误代码和交易 ID。

无法连接或发送数据到私有服务 **IP** 或 **FQDN**

信息代码： 0x10000413

- 专用服务器连接已终止
- Connector Appliance 和后端专用 TCP/UDP 服务器的连接问题。
  查看路由域条目。确保 IP 地址有效且指向正确的后端。

没有匹配的策略条件

信息代码： 0x100508

用户上下文与分配给应用程序的策略中定义的访问规则条件不匹配。

更新策略配置以匹配用户的上下文。

没有与应用程序相关的访问策略

信息代码： 0x100509

1. 在 Citrix Secure Private Access 服务 GUI 中，单击左侧导航栏中的访问策略。
2. 确保访问策略与相应的应用程序相关联。
3. 如果访问策略与应用程序无关，请为该应用程序创建访问策略。有关详细信息，请参阅创建访问策略。
4. 如果这不能解决问题，请联系 Citrix 支持部门。

未找到 **FQDN** 或 **IP** 地址的应用程序配置

信息代码： 0x10050A

未找到与传入的 FQDN 或 IP 地址请求匹配的应用程序。因此，该应用程序被归类为未发布的应用程序。如果这不是预料之中的，请执行以下操作。

1. 转到 Secure Private Access 服务管理门户。
2. 点击左侧导航栏上的 应用程序。
3. 搜索应用程序，然后单击“编辑”。
4. 向应用程序添加 FQDN 或 IP 地址。您可以添加确切的域、IP 地址或通配符域。

   注意：在“**Secure Private Access**”**>**“设置”**>**“应用程序域”中添加 FQDN 或 IP 地址并不能解决此问题。它必须作为应用程序配置的一部分进行添加。

应用程序枚举信息

信息代码： 0x10050C

此代码捕获了用户可能有权使用的多个应用程序的策略评估结果。应用程序访问可能由于以下原因而被拒绝：

- 用户上下文与分配给应用程序的策略中定义的访问规则条件不匹配-有关详细信息，请参阅不匹配策略条件。
- 没有与应用程序关联的访问策略-有关详细信息，请参阅不与应用程序关联的访问策略。
- 与应用程序关联的策略配置为拒绝访问—在这种情况下，无需按预期执行任何操作。
- 执行访问策略时出现意外内部错误。有关详细信息，请联系 Citrix 支持部门。

TCP/UDP 应用程序启动失败，因为应用程序域表中缺少路由条目

信息代码： 0x00180101

如果应用程序配置存在但路由条目丢失或之前已删除，则可能会出现此问题。

为访问的目标添加路由条目（**Secure Private Access >** 设置 **>** 应用程序域）。

TCP/UDP 应用程序启动失败，因为连接器不正常

信息代码： 0x00180102

如果所有连接器均未启动/响应新连接，则可能会出现此问题。

在相应的资源位置对 Connector Appliance 运行运行状况检查。

由于无法访问连接器，**UDP/DNS** 请求失败

信息代码： 0x00180103

如果 UDP/DNS 流量无法到达连接器，则可能会出现此问题。

在相应的资源位置对 Connector Appliance 运行运行状况检查。

由于 **NGS cookie** 已过期，无法加载页面

信息代码： 0x20580001

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

由于网络故障，访问策略提取失败

信息代码： 0x20580002

1. 检查 URL 和网络连接。
2. 重新启动浏览器，然后尝试再次打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持部门。

解析 **JSON** 网络令牌时访问策略提取失败

信息代码：0x20580003

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

网络无法获取访问策略的详细信息

信息代码：0x20580004

1. 检查访问策略是否已启用。
2. 重新启动浏览器，然后尝试再次打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持部门。

获取公共证书时策略提取失败

信息代码： 0x20580005

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

验证 **JSON** 网络令牌的签名时策略提取失败

信息代码： 0x20580007

1. 检查网络时间和用户设备时间是否同步。
2. 重新启动浏览器，然后尝试再次打开应用程序。
3. 如果这不能解决问题，请联系 Citrix 支持部门。

验证公共证书时策略提取失败

信息代码： 0x20580008

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

未能确定形成策略 **URL** 的存储环境

信息代码： 0x2058000A

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

未能获得访问策略提取请求的响应

信息代码： 0x2058000B

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

由于辅助 **DS** 身份验证令牌过期，访问策略提取失败

信息代码： 0x2058000C

1. 重新启动浏览器，然后尝试再次打开应用程序。
2. 如果这不能解决问题，请联系 Citrix 支持部门。

Connector Appliance 未注册

信息代码： 0x10200002

检查 Connector Appliance 的注册。

有关详细信息，请参阅向 Citrix Cloud 注册您的 Connector Appliance。

无法连接到 **Connector Appliance** 设备

信息代码： 0x10200003

Connector Appliance 无法在 Citrix Cloud 和资源位置之间进行通信。

检查连接器注册。

有关详细信息，请参阅向 Citrix Cloud 注册您的 Connector Appliance。

连接到 **Citrix Secure Private Access** 服务失败

信息代码： 0x10000301

检查 Connector Appliance 的网络设置。有关详细信息，请参阅 Connector Appliance 的网络设置。

无法访问代理服务器

信息代码： 0x10000303、0x10000304

检查代理服务器设置，并确保 Connector Appliance 可以访问代理服务器设置。有关详细信息，请参阅向 Citrix Cloud 注册您的 Connector Appliance。

代理服务器身份验证失败

信息代码： 0x10000305

检查代理服务器凭据，并确保在 Connector Appliance 中正确配置了这些凭据。有关详细信息，请参阅注册您的 Connector Appliance 之后。

无法访问已配置的代理服务器

信息代码： 0x10000306

检查 Connector Appliance 网络设置、防火墙设置或代理服务器设置。有关详细信息，请参阅以下主题：

- Connector Appliance 的网络设置
- 向 Citrix Cloud 注册您的 Connector Appliance
- Connector Appliance 通信

收到来自后端服务器的错误响应

信息代码： 0x10000307

如果不是预期的代码，请检查后端 Web 服务器的 HTTP 状态码。

无法向目标 **URL** 发送请求

信息代码： 0x10000005

检查目标 URL 或检查 Connector Appliance 的网络设置。有关详细信息，请参阅 Connector Appliance 的网络设置。

无法处理 **SSO**

信息代码： 0x10000107

无法从 Citrix Cloud 检索应用程序配置数据。

检查 Connector Appliance 网络设置，确保已配置 NTP 服务器且没有时差问题。有关详细信息，请参阅 Connector Appliance 的网络设置。

连接到 **Citrix Secure Private Access** 服务失败

信息代码： 0x10000108、0x1000010B

检查 Connector Appliance 的网络设置。有关详细信息，请参阅 Connector Appliance 的网络设置。

无法处理 **SSO**，无法确定 **SSO** 设置

信息代码： 0x1000010A

检查 SSO 配置，确保 Connector Appliance 可以访问服务器。

FormFill SSO 失败，表单应用程序配置不正确

信息代码： 0x10000101、0x10000102、0x10000103、0x10000104

检查 SSO 表单应用程序配置，并确保在应用程序设置中正确配置了用户名、密码、操作和登录 URL 字段。

Kerberos SSO 失败

信息代码： 0x10000202

检查后端服务器和域控制器上的 Kerberos SSO 设置。还要检查备用 NTLM 身份验证设置。

有关 Kerberos SSO 设置，请参阅验证您的 Kerberos 配置。

无法处理身份验证类型的 **SSO**

信息代码： 0x10000203

检查 Secure Private Access 服务和后端服务器中的 SSO 设置。有关 Secure Private Access 服务，请参阅设置首选登录方法。

Kerberos SSO 失败但回退到 **NTLM**

信息代码： 0x10000204

从域控制器检索 Kerberos 票证失败。作为辅助身份验证，Connector Appliance 已尝试使用备用 NTLM 身份验证。

要成功启用 Kerberos 身份验证，请检查后端服务器和域控制器上的 Kerberos SSO 设置。

有关详细信息，请参阅验证您的 Kerberos 配置。

在 **Citrix Workspace** 应用程序中配置了多个具有 **ZTNA** 权限的帐户

信息代码： 0x14000001

在 Citrix Workspace 应用程序中仅配置一个授权为 ZTNA 的帐户。

如何收集客户端日志

- **Windows** 客户端：
  1. 打开应用程序并确保已启用日志记录。
  2. 现在连接到 Secure Private Access 服务并重复您面临的问题。
  3. 在应用程序中，转到“日志”，然后单击“收集日志文件”。这将生成日志文件。
  4. 将日志文件保存在客户端计算机的桌面上。
- **Mac** 客户端：
  1. 打开应用程序并转到日志 **>** 详细。
  2. 清除日志并继续重现问题。
  3. 返回 日志 **>** 导出日志。这将创建一个包含日志文件的 zip 文件。

常见问题解答

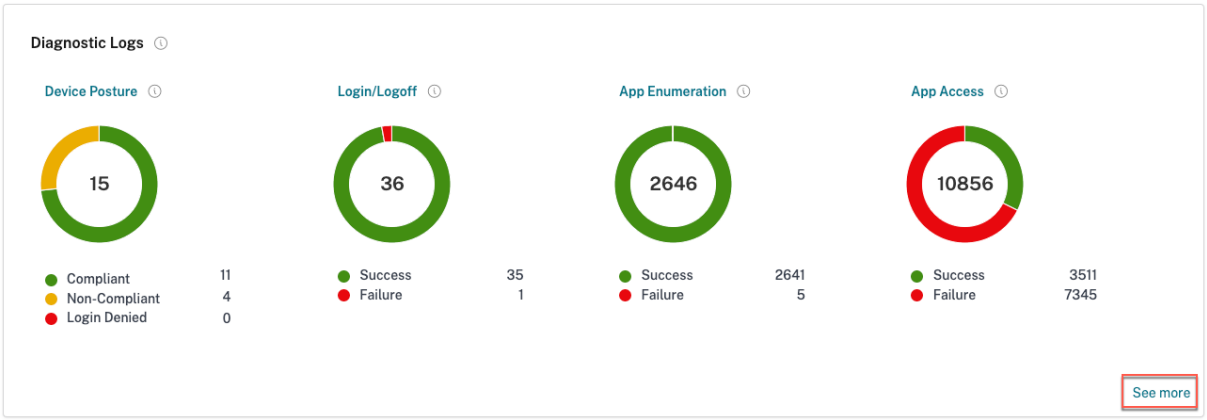
什么是 **Secure Private Access** 诊断日志

Secure Private Access 诊断日志捕获用户访问任何应用程序（Web/SaaS/TCP/UDP）时发生的所有事件。这些日志捕获 Device Posture、应用程序身份验证、应用程序枚举和应用程序访问日志。

在哪里可以找到 **Secure Private Access** 日志

1. 登录 Citrix Cloud。
2. 在“Secure Private Access 服务”图块上，单击“管理”。

3. 在管理员用户界面左侧导航栏中单击“控制面板”。
4. 在“诊断日志”图表中，单击“查看更多”链接。



我可以在 **Secure Private Access** 诊断日志中找到哪些详细信息

默认情况下，Secure Private Access 用户日志控制板提供以下详细信息。

- 时间戳 -以 UTC 为单位的事件时间。
- 用户名 -访问应用程序的最终用户的用户名。
- 应用程序名称 -访问的应用程序/应用程序的名称。
- 策略信息 -显示事件期间触发的一个或多个访问策略的名称。
- 状态 -显示事件、成功或失败的状态。
- 信息代码 - 查看有关信息代码的更多信息。
- 描述 -显示失败的原因或有关该事件的更多详细信息。
- 应用程序 **FQDN**：访问的应用程序的 FQDN
- 事件类型 - 显示与所执行操作相关的事件类型。
- 操作类型 -显示生成日志的操作。
- 类别 -根据事件的类型，有三个类别可用。即应用程序身份验证、应用程序枚举或应用程序访问权限。这些选项也可用作筛选选项。您可以使用这些选项根据所面临问题的类型筛选日志。
- 交易 **ID** - 了解如何使用交易 ID
  单击控制面板最右侧的 + 按钮可以获取以下详细信息：
- **SPA PoP** 位置 - 显示应用程序访问期间使用的 Secure Private Access 服务 PoP 位置的名称/ID。请参阅 Secure Private Access PoP 位置

Secure Private Access 诊断日志中捕获了哪些事件

Secure Private Access 诊断日志会捕获以下事件：

- **Device Posture**：最终用户 Device Posture。这些日志捕获有关 Device Posture 结果的信息。根据您的设备状态策略，设备是否被视为合规、不合规或被拒绝访问。

- 登录/注销：有关最终用户登录 Citrix Secure Access 客户端或注销状态以及工作区（内部或外部提供商）身份验证的事件。
- 应用程序枚举：在 Secure Private Access 服务中，管理员配置的访问策略决定哪个用户可以访问哪个应用程序。在 Citrix Workspace 应用程序中，最终用户不可见（未枚举）被拒绝的应用程序。这些事件可帮助您了解根据在 Secure Private Access 服务中配置的访问策略允许或拒绝用户访问哪些应用程序。
- 应用程序访问：根据所选时间间隔内配置的访问策略，最终用户应用程序/端点访问、允许/拒绝状态、单点登录状态和连接状态的事件。

如何使用 **Secure Private Access** 故障排除主题来解决我遇到的故障

1. 获取您正在尝试解决的失败的信息代码。
2. 在错误查找表中查找信息代码。
3. 按照为该信息代码提供的解决步骤进行操作。

什么是信息代码？我在哪里找到他们

某些日志事件（例如故障）有相关的信息代码。在错误查找表中搜索此信息代码以查找解决步骤或有关该事件的更多信息。

什么是交易 **ID**？我该如何使用它

交易 ID 关联访问请求的所有 Secure Private Access 日志。一个应用程序访问请求可以生成多个日志，首先是身份验证，然后是工作区应用程序中的应用程序枚举，然后是应用程序访问本身。所有这些事件都会生成自己的日志。事务 ID 用于关联所有这些日志。您可以使用事务 ID 筛选诊断日志，以查找与特定应用程序访问请求相关的所有日志。

Secure Private Access 的所有 **PoP** 地点在哪里

以下是“Secure Private Access PoP”位置列表。

PoP 名称	区域	地理区域
az-us-e	Azure east	弗吉尼亚州
az-us-w	Azure 西部	加利福尼亚
az-us-sc	Azure 中南部	德克萨斯州
az-aus-e	Azure 澳大利亚东部	新南威尔士州
az-eu-n	Azure 北欧	爱尔兰
az-eu-w	Azure 的西欧	荷兰

PoP 名称	区域	地理区域
az-jp-e	Azure 日本东部	东京、埼玉
az-bz-s	Azure 巴西南部	圣保罗州
az-asia-se	Azure 东南亚	新加坡
az-uae-n	Azure 阿联酋北部	迪拜
az-in-s	Azure 印度南部	钦奈
az-asia-hk	Azure 东亚	中国香港特别行政区

如果我无法使用信息代码和错误查找表来解决我的故障，该怎么办

请联系 Citrix 支持部门。

引用

- 添加 **Web** 应用程序
  - 支持企业 Web 应用程序
  - 配置对 Web 应用程序的直接访问
- 添加 **SaaS** 应用程序
  - 支持软件即服务应用
  - 特定于 SaaS 应用服务器的配置
- 配置客户端-服务器应用程序
  - 支持客户端-服务器应用程序
- 创建访问策略
  - 创建访问策略
- 路由表
  - 路由表