Citrix Workspace

Contents

Citrix Workspace 概述

November 26, 2023

Citrix Workspace 是一种数字化工作区解决方案，可通过任何设备从任何地点提供对应用程序、桌面和内容（资源）的安全、统一访问。这些资源可以是 Citrix DaaS、内容应用程序、本地和移动应用程序、SaaS 和 Web 应用程序以及浏览器应用程序。

Citrix Workspace 原理

Citrix Workspace 聚合和集成 Citrix Cloud 服务，从而可以在一个资源 位置统一访问最终用户（订阅者）可用的所有资源。Citrix Workspace 的最终用户之所以称为订阅者，是因为您为员工“订阅”了通过其工作区向他们提供的服务。

有关 Citrix Workspace 提供的服务的概述，请参阅通过 Citrix Workspace 提供的云托管服务。

订阅者可以在 Citrix Workspace 用户界面 (UI) 中看到您通过这些服务向他们提供的每个资源的完整、统一的视图。有关 Citrix Workspace UI 订阅者体验的更多信息，请参阅管理您的 Workspace 体验。

订阅者可以通过带有 Workspace URL 的浏览器或通过取代 Citrix Receiver 的 Citrix Workspace 应用程序访问您在 **Workspace** 配置中配置和启用的服务。有关用户如何访问其工作区的更多信息，请访问工作 区访问权限。

订阅者使用您在身份 和访问管理中配置、然后在 **Workspace** 配置中启用的主身份 提供程序对其 工作区进行身份验证。然后，系统会自动对订阅者进行身份验证，以访问为 Citrix Workspace 购买的每项云托管服务，这有助于提高安全性并减少可用性挑战。有关配置 Workspace 身份验证的更多信息，请访问 保护工作区。

开始使用概述

Citrix Workspace 是通过 **Citrix Cloud** 控制台设置的，该控制台中有一个 身份识别和访问管理 屏幕和一个名为“工作区 配置”的 **Citrix Workspace** 管理界面。Citrix Workspace 入门涉及以下任务。

1. 确保您已设置为在 **Citrix Cloud** 控制台中实施 Citrix Workspace，您可以在其中执行以下操作：
    - 加入基于云的服务。
    - 组建您的部署团队。
    - 配置您的基础架构和资源。
2. 在身份识别和访问管理中为以下各项定义身份提供商和帐户：
    - Citrix Cloud 管理员。
    - Citrix Workspace 订阅者。
3. 在 **Workspace** 配置中配置您的工作区，包括：

- 内部和外部访问。
- 将您在 Citrix Cloud 控制台中配置的服务集成到工作区中。
- 自定义工作区外观和订阅者登录后的体验。

除此基本设置外，您还有其他安全、隐私和优化选项可供选择。最常见的是：

- 使用 Citrix 联合身份验证服务 (FAS) 在 Citrix Workspace 中配置 DaaS 的单点登录 (SSO)。如果您使用联合身份验证方法，例如 Okta 或 Azure Active Directory，通常会采用 FAS。

有关任务的概述以及部署过程中所需的信息，请参阅 Citrix Workspace 入门。每个步骤都会引导您完成 Citrix Cloud 控制台，并提供有关配置身份提供商和启用服务等任务的说明。通过本演练，还可以快速访问组建部署团队以及配置基础架构和资源所需的技术信息。

通过 **Citrix Workspace** 提供云托管服务

订阅者使用 Citrix Workspace 访问云托管服务提供的资源。现有的 Citrix Cloud 客户可以通过将这些服务随身携带到 Citrix Workspace 解决方案中来过渡到完整的数字化 Workspace 体验。

本节介绍可以为 Citrix Workspace 启用的主要云托管服务，具体取决于您的授权。有关如何配置和启用对已购买服务的访问权限的信息，请访问 Citrix Workspace 入门。有关每个 Citrix Workspace 版本和所包含功能的完整说明，请参阅 Citrix Workspace 功能列表。

Citrix DaaS

Citrix Workspace 是 Citrix DaaS 的多租户、云托管接入点。要设置 Citrix DaaS，请按照 Citrix DaaS 中概述的步骤进行操作。

如果您是本地 Virtual Apps and Desktops 客户，则通过 Citrix Workspace 访问资源有不同的选项。您选择的选项取决于您是要完全迁移到云还是采用混合解决方案，以及是否计划允许外部访问。有关这些选项的更多信息，请访问 使用 Citrix Workspace 交付 DaaS。

SaaS 和 **Web** 应用程序，通过 **Citrix Secure Private Access** 服务进行保护

Citrix Secure Private Access（以前称为 **Secure Workspace Access** 和访问控制服务）提供对集成到 Workspace 中的 Web 和 SaaS 应用程序的单点登录 (SSO)。该服务还允许您管理访问权限和控制策略，根据订阅者的凭据批准对企业托管 Web 应用程序的适当访问级别。

有关 **Citrix Secure Private Access** 服务优势的更多信息，请访问技术简报：Secure Private Access。

Citrix Gateway 服务

Citrix Gateway 服务（以前称为 **NetScaler Gateway** 服务）与 **Citrix Secure Private Access** 一起使用，用于由 Citrix 管理的完全云托管的环境。

Citrix Gateway 服务 通过基于高级策略基础架构提供与 Workspace 的外部连接，为 SaaS 应用程序、虚拟应用程序和桌面提供统一的体验。

按照以下步骤设置 Citrix Gateway 服务，然后测试 Workspace URL 并与订阅者共享，以便为他们提供远程访问权限。有关在 Citrix Gateway 服务中配置 SaaS 应用程序的详细信息，请参阅支持软件即服务应用程序。

Citrix Remote Browser Isolation 服务

将 **Citrix Remote Browser Isolation** 服务集成到您的工作区中，以隔离 Web 浏览并保护企业网络免受基于浏览器的攻击。订阅者导航到 Workspace URL 时，将显示其发布的浏览器，以及在其他 Citrix Cloud 服务中配置的其他应用程序和桌面。

要允许订阅者访问 Remote Browser Isolation，请设置 Remote Browser Isolation，然后测试工作区 URL 并与订阅者共享。

Citrix Endpoint Management

Citrix Endpoint Management 允许您通过对身份、设备、应用程序、数据和网络的严格安全性来管理设备和应用程序策略。新客户和现有客户与 Citrix Workspace 的集成有所不同。有关将 Endpoint Management 与 Citrix Workspace 集成的更多信息，请访问 与 Citrix Workspace 体验集成。

Citrix Analytics

Citrix Analytics 服务可收集所有 Citrix Workspace 订阅者并提供相关见解。根据您的授权，您可以使用不同的 Citrix Analytics 产品。它们是 **Citrix Analytics for Security**、**Citrix Analytics for Performance** 和 **Citrix Analytics**（使用情况）。要了解有关这些服务的更多信息，请访问 Citrix Analytics。

新增功能

November 26, 2023

Citrix 的目标是在新功能和更新可用时向 Citrix Workspace 客户提供这些功能和更新。初始版本应用于 Citrix 内部站点，并逐步应用于客户环境。

有关云规模和服务可用性的服务级别协议的详细信息，请参阅 Citrix Cloud 服务级别协议。要监视服务中断情况和计划内维护，请参阅“服务运行状况”控制板。

Citrix Workspace 中有什么新内容

随时了解 Citrix Workspace 的最新增强和更新，以充分利用我们技术的潜力。通过整合来自 Citrix Workspace 的及时更新，最大限度地提高用户的工作效率并提高他们的交互质量。

- Workspace 平台中的新增功能
- Workspace 用户界面中的新增功能
- Global App Configuration Service 中的新增功能

不同平台上的 **Citrix Workspace** 应用程序

使用以下链接，详细了解适用于您最喜爱的平台的 **Citrix Workspace** 应用程序 的新功能和增强功能。

- Android
- ChromeOS
- HTML5
- iOS
- Linux
- Mac
- Microsoft Teams
- Windows
- Windows 应用商店

此外，请查看 Citrix Enterprise Browser 中的新增功能。

Workspace 平台的新增功能

November 26, 2023

Citrix 的目标是在新功能和更新可用时向 Citrix Workspace 客户提供这些功能和更新。新版本会带来更多的价值，应立即将更新告知客户。

对您而言，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。逐步提供更新可最大限度地提高产品质量和可用性。

有关云规模和服务可用性的服务级别协议的详细信息，请参阅 Citrix Cloud 服务级别协议。要监视服务中断情况和计划内维护，请参阅“服务运行状况”控制板。

2023 年 11 月

配置自定义域-正式上线

自定义域名功能现已正式上线。您可以为工作区配置自定义域，这允许您使用自己选择的域来访问您的 Citrix Workspace 存储。然后，您可以使用此域代替分配的 cloud.com 域，以便从 Web 浏览器和 Citrix Workspace 应用程序进行访问。有关更多信息，请参阅配置自定义域。

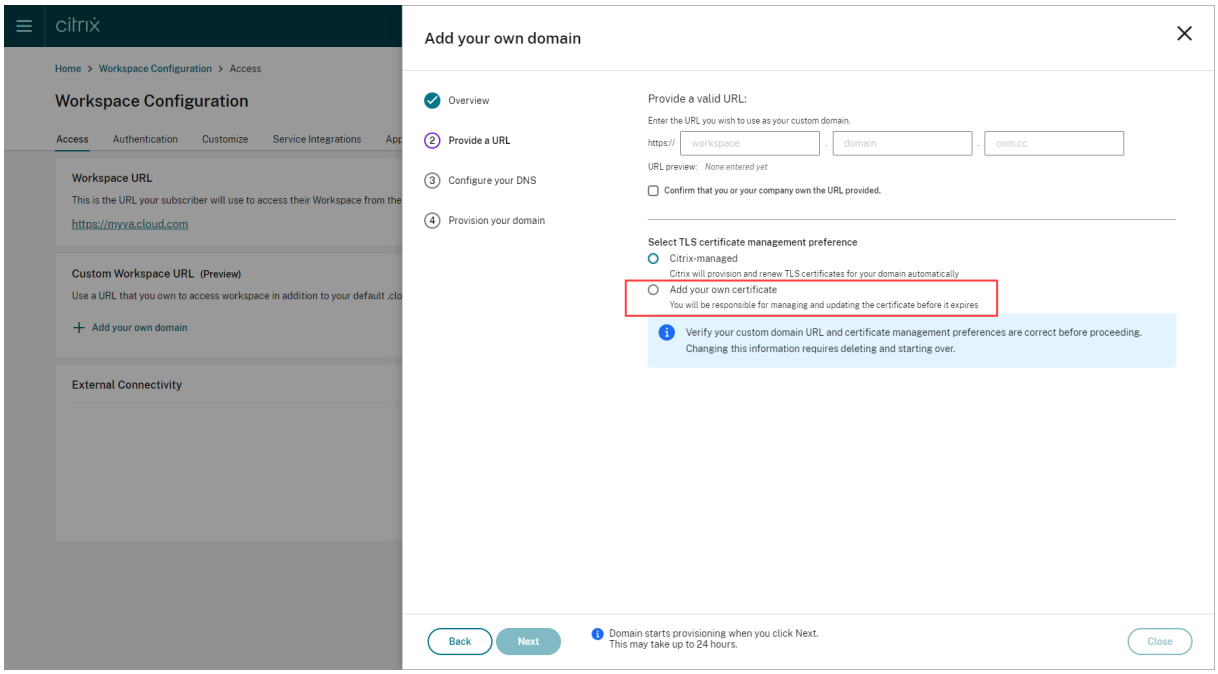
Aug 2023

为自定义域添加您自己的 **TLS** 证书（预览版）

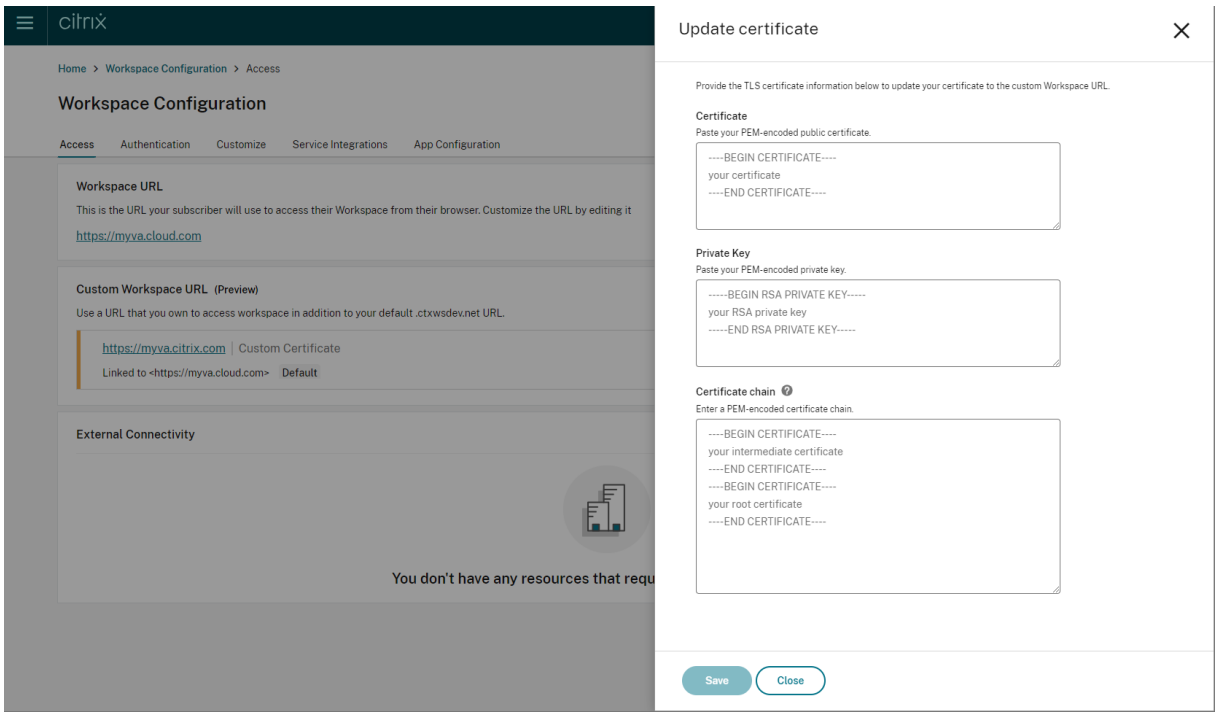
现在，在配置自定义 Workspace URL 时，您可以上载自己的 TLS 证书进行身份验证。在上载证书之前，请确保证书满足以下条件。

- 它应该采用 PEM 编码。
- 它应至少在接下来的 30 天内保持有效。
- 它应专门用于自定义 Workspace URL，不接受通配符证书。
- 证书的公用名称应与自定义域相匹配。
- 证书上的 SAN 应用于自定义域，不允许使用任何其他 SAN。
- 证书的有效期不应超过 10 年。

要添加您的证书，请导航至“提供 **URL**”页面，然后在“选择 **TLS** 证书管理首选项下选择“添加自己的证书”选项。



然后，您可以在“添加自己的证书”页面上添加您的证书。



有关更多信息，请参阅添加自定义域名。

> 注意：
>
> 您可以使用随附的 Podio 表单就此预览功能提供反馈。

2023 年 5 月

配置自定义域（预览版）。您可以为工作区配置自定义域，这允许您使用自己选择的域来访问您的 Citrix Workspace 存储。然后，您可以使用此域代替分配的 cloud.com 域，以便从 Web 浏览器和 Citrix Workspace 应用程序进行访问。有关更多信息，请参阅 配置自定义域（预览）。

March 2023

其他非活动超时设置:。现在，您可以为 Workspace 应用程序的桌面和移动用户启用额外的非活动超时设置。有关更多信息，请参阅自定义安全性和隐私政策。

2022 年 12 月

其他发送自定义公告配置选项:。现在，在将“发送自定义公告”配置为顶部或底部时，您可以将页面放置位置设置为“顶部”或“底部”。有关更多信息，请参阅自定义安全和隐私政策。

支持繁体中文。Citrix Workspace 现已提供繁体中文版本。

2022 年 10 月

支持韩语。Citrix Workspace 现已提供韩语版本。

支持自定义 **Citrix Workspace** 应用程序设置。管理员现在可以使用 Global App Configuration Service 配置适用于 iOS、Android、HTML5、Mac 和 Windows 平台的 Citrix Workspace 应用程序的设置。

2022 年 8 月

改进了 **Workspace** 启动体验。当用户通过 Web 或浏览器启动其工作区时，会触发显示启动状态的通知。如果用户在启动过程中尝试关闭浏览器，系统会提示用户进行确认，并通知正在启动会话。有关更多信息，请参阅 Citrix Workspace 入门。

2022 年 6 月

通过 **Safari** 支持服务连续性。Citrix Workspace Web 扩展可为通过浏览器访问其应用程序和桌面的用户提供服务连续性。有关更多信息，请参阅 浏览器中的服务连续性。

2022 年 5 月

联合身份提供商的新配置选项：启用或禁用联合身份提供商，以允许在登录 Workspace 时提示订阅者进行身份验证。有关更多信息，请参阅 自定义工作区交互。

Workspace 应用程序正式发布的重新身份验证期限：重新身份验证期允许订阅者保持对 Workspace 的登录状态，而无需在每次访问其工作区时都收到登录的提示。通过 Workspace 应用程序登录时，订阅者同意保持登录状态。只要订阅者使用自己的应用程序和桌面，他们就会在重新身份验证期间保持登录状态。有关此功能的详细信息，请参阅 为 Citrix Workspace 应用程序设置重新身份验证期限。

在 **iOS** 上支持服务连续性：适用于 iOS 的 Citrix Workspace 应用程序现在支持服务连续性，正式上市。有关详细信息，请参阅服务连续性。

新的服务连续性错误代码：新的错误代码现已推出，可帮助排除故障的服务连续性连接。有关详细信息，请参阅服务连续性。

2022 年 3 月

在 **Android** 和 **iOS** 上支持服务连续性：适用于 Android 的 Citrix Workspace 应用程序现已正式上市，技术预览版支持适用于 iOS 的 Citrix Workspace 应用程序的服务连续性。有关详细信息，请参阅服务连续性。

2022 年 2 月

支持 **Android** 版 **Citrix Workspace** 应用程序（正式发布）和适用于 **iOS** 的 **Citrix Workspace** 应用程序（技术预览版）的服务连续性：服务连续性允许用户即使在停机期间也能连接到其虚拟应用程序和桌面。现在，适用于 Android 的 Citrix Workspace 应用程序已正式上市，适用于 iOS 的 Citrix Workspace 应用程序在技术预览版中。有关详细信息，请参阅服务连续性。

发送自定义公告和自定义登录策略：现在有两项新功能可供所有客户使用。这些功能允许 Workspace 管理员在 Citrix Workspace 应用程序中显示自己的登录后永久横幅和登录前自定义消息或许可协议。有关更多信息，请参阅 自定义安全和隐私策略。

2021 年 12 月

移除 **Citrix Content Collaboration** 员工和客户用户的默认拆分登录屏幕： Citrix Workspace 现在允许您为客户端和员工用户启用单点登录流程。有关更多信息，请参阅 创建统一的用户登录流程。

使用适用于 **Mac** 的 **Citrix Workspace** 应用程序支持浏览器中的服务连续性： Citrix Workspace Web 扩展使通过浏览器访问其应用程序和桌面的用户可以使用服务连续性。现在，运行适用于 Mac 的 Citrix Workspace 应用程序的设备支持此功能。有关详细信息，请参阅服务连续性。

2021 年 11 月

策略驱动的主题：您可以创建 Workspace 主题并确定其优先级，并将每个主题添加到 **Workspace** 配置中的不同用户组。有关详细信息，请参阅自定义工作区的外观。

2021 年 10 月

电子签名语言支持：除以下语言外，电子签名现在还支持意大利语和巴西葡萄牙语：德语、法语、西班牙语、日语、荷兰语和简体中文。有关详细信息，请参阅 RightSignature 多语言支持。

FAS 支持多个资源位置正式发布： Citrix Workspace 现在支持跨多个资源位置提供对虚拟应用程序和桌面的单点登录。此外，可以将一个资源位置中的 FAS 服务器指定为主服务器或辅助服务器，以便为其他资源位置的 FAS 服务器提供故障切换。有关详细信息，请参阅使用 Citrix 联合身份验证服务对工作区启用单点登录。

2021 年 9 月

Citrix Workspace 推出适用于 **HTML5** 的 **Citrix Workspace** 应用程序：适用于 HTML5 的 Citrix Workspace 应用程序无需在设备上安装任何设备即可在浏览器中提供有关适用于 HTML5 的 Citrix Workspace 应用程序的更多信息，包括新功能，请访问适用于 HTML5 的 Citrix Workspace 应用程序产品文档。

支持浏览器正式发布中的服务连续性： Citrix Workspace Web 扩展使通过浏览器访问其应用程序和桌面的用户可以使用服务连续性。此功能适用于 Windows 设备上的 Google Chrome 和 Microsoft Edge。有关更多信息，请参阅浏览器中的服务连续性。

2021 年 7 月

自定义订阅者许可协议策略：您可以向订阅者提供自定义使用协议策略，以便他们在登录其 Workspace 之前阅读和接受。有关此功能的更多信息，请参阅 配置登录策略。

Workspace 应用程序预览版的重新身份验证期限：重新身份验证期允许订阅者保持对 Workspace 的登录状态，而无需在每次访问其工作区时都收到登录的提示。通过 Workspace 应用程序登录时，订阅者同意保持登录状态。只要订阅者使用自己的应用程序和桌面，他们就会在重新身份验证期间保持登录状态。有关此预览功能的详细信息，请参阅 设置 Citrix Workspace 应用程序的重新身份验证期限。

通过 **Citrix Cloud** 配置网络位置：除了使用 Citrix 提供的 PowerShell 脚本外，您现在还可以通过 Citrix 云管理控制台配置网络位置。有关此功能的更多信息，请参阅使用 直接工作负载连接优化与工作区的连接。

2021 年 6 月

FAS 支持多个资源位置预览： Citrix Workspace 现在支持跨多个资源位置提供对虚拟应用程序和桌面的单点登录。可以将一个资源位置中的 FAS 服务器指定为主服务器或辅助服务器，以便为其他资源位置的 FAS 服务器提供故障切换。有关此预览功能的详细信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录。

支持浏览器技术预览版中的服务连续性： Citrix Workspace Web 扩展为通过浏览器访问其应用程序和桌面的用户提供服务连续性。此技术预览版适用于 Windows 设备上的 Google Chrome 和 Microsoft Edge。有关更多信息，请参阅 浏览器中的服务连续性。

服务连续性通用可用性：即使在 Citrix Cloud 组件或公共和私有云中断期间，服务连续性也允许用户连接到其虚拟应用程序和桌面。有关详细信息，请参阅服务连续性。

Citrix RightSignature 应用程序可用：利用 Citrix 应用程序 (Workspace Premium 和 Premium Plus 附带的电子签名解决方案) 通过 Citrix Workspace 请求对任何设备上的文档有关更多信息，请参阅 配置 Citrix RightSignature 应用程序。

2021 年 5 月

自定义主题技术预览版：为订阅者自定义 Workspace 外观现在支持自定义主题，您可以将这些主题分配给不同的用户组。创建、自定义主题并确定主题的优先级，以便这些用户组中的订阅者在登录时看到相应的工作区主题。有关详细信息，请参阅自定义工作区的外观。

电子签名语言支持：电子签名功能现在支持以下语言：德语、法语、西班牙语、日语、荷兰语和简体中文。有关详细信息，请参阅 RightSignature 多语言支持。

2021 年 2 月

帐户密码更改：订阅者可以在 Citrix Workspace 中更改其域密码。管理员还可以向订阅者提供密码指导，以根据其组织的密码策略创建有效的复杂密码。有关更多信息，请参阅 允许订阅者更改其帐户密码。

December 2020

服务连续性技术预览版：即使在 Citrix Cloud 组件或公共和私有云中断期间，服务连续性也允许用户连接到其 Citrix DaaS。有关详细信息，请参阅服务连续性。

2020 年 10 月

FedRAMP 就绪：在 Citrix Cloud Government 中部署时，Citrix Workspace 处于 FedRAMP 就绪状态 FedRAMP 是一项旨在促进美国政府组织使用的云服务的安全标准的计划。需要 FedRAMP Ready 云服务的美国政府组织现在可以使用 Citrix Workspace 和 Citrix DaaS 服务来交付 DaaS。有关详细信息，请参阅 Citrix Cloud Government。

2020 年 5 月

Citrix Workspace 入门指南： Citrix Workspace 现在包括分步演练，可帮助您快速向最终用户交付工作区。本演练将引导您完成 Citrix Cloud 控制台，以便您配置身份提供商、添加管理员以及启用工作区身份验证和服务。有关任务的概述和所需说明的快速访问权限，请参阅 Citrix Workspace 入门。

2019 年 12 月

网络定位服务：您现在可以确保将从企业网络中启动 Workspace 中的应用程序和桌面的用户直接路由到其 VDA。这绕过了网关，导致更快的 DaaS 会话。有关此服务和设置说明的详细信息，请参阅使用网络定位服务优化与工作区的连接。

最近使用和收藏应用程序的改进：“最近使用”和“收藏夹”首先加载到 Workspace 中，因此用户可以立即启动其常用应用程序和桌面。

工作区用户界面 (UI) 的新增内容

November 26, 2023

以下各节列出了 Workspace UI 当前版本和早期版本中的新功能。

> 注意：
>
> - 有关新 UI 的更多信息，请参阅新建 Workspace 用户界面。
> - 有关活动管理器的更多信息，请参阅 活动管理器。

23.46 中的新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

已知问题

没有新的已知问题。

早期版本

本部分内容提供有关我们支持的早期版本中的新增功能和已修复的问题的信息。

23.45

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

- Google Search 索引已从 Citrix Web 中删除，以防止内部 URL 出现在 Google 的搜索结果中。但是，如果您的 URL 已经被 Google 编入索引，则必须采取措施将其删除。如需更多信息，请参阅从 Google 移除您的站点上托管的页面。

23.44

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.43

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.42

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.41

新增功能

此版本解决了改进整体性能和稳定性的区域。

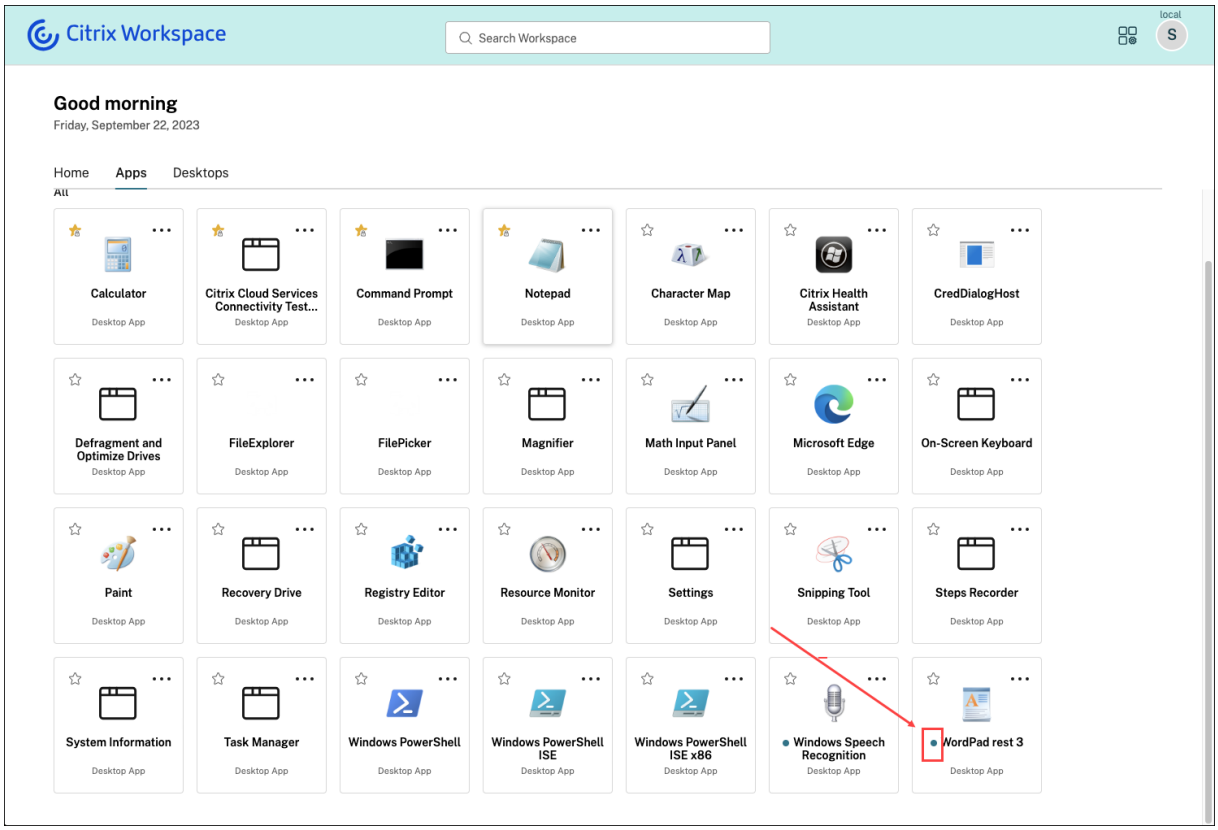
已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.40

新增功能

简化新应用程序的发现　最终用户现在可以轻松发现新添加的应用程序，从而更轻松地浏览和使用最新的应用程序。当管理员向最终用户交付新应用程序时，它会在最终用户的工作区中突出显示，并且应用程序图块上首次显示一个绿点。



已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.39

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.38

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.37

新增功能

全新 **Workspace** 用户界面 **-** 正式上市　新的 Workspace 用户界面现已正式上线。它引入了具有现代外观和感觉的全新 UI 功能，可提供更清晰的视图。用户界面增强适用于 Web、桌面和移动设备。管理员可以通过“Workspace 配置”>“自定义”>“功能”为最终用户启用该功能。有关更多信息，请参阅新建 Workspace 用户界面。

> 注意：
>
> 默认情况下，除非管理员启用，否则新的用户界面开关将在接下来的 6 个月内处于禁用状态。6 个月后，将默认为所有用户启用新用户界面，并且当前的用户界面体验将被弃用。管理员需要在接下来的 6 个月内将其用户过渡到新用户界面。

活动管理器**-**正式发布　活动管理器功能现已在新的云端用户界面中正式推出。活动管理器是一项简单而强大的功能，它使用户能够有效地管理自己的资源。它通过便于在任何设备上对处于活动状态和已断开连接的应用程序和桌面进行快速操作来提高工作效率。管理员可以通过“Workspace 配置”>“自定义”>“功能”>“活动管理器”为其最终用户启用此功能。有关更多信息，请参阅启用活动管理器。

启用后，处于活动状态或处于断开连接状态的应用程序和桌面将显示在“活动管理器”面板上。最终用户可以单击省略号 **(**…) 图标可快速采取行动。

可以对处于活动状态的应用程序和桌面执行以下操作。

- 断开连接：断开远程会话，但应用程序和桌面在后台处于活动状态。
- 注销：注销当前会话。会话中的所有应用程序都已关闭，所有未保存的文件都将丢失。
- 关闭：关闭断开连接的桌面。
- 强制退出：如果出现技术问题，请强行关闭桌面电源。
- 重新启动：关闭桌面并重新启动。

Activity Manager 还允许最终用户与已断开连接的应用程序和桌面进行交互。确保您已升级到最新的 DDC 版本 (115)。有关更多信息，请参阅 已断开连接的应用程序和桌面。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

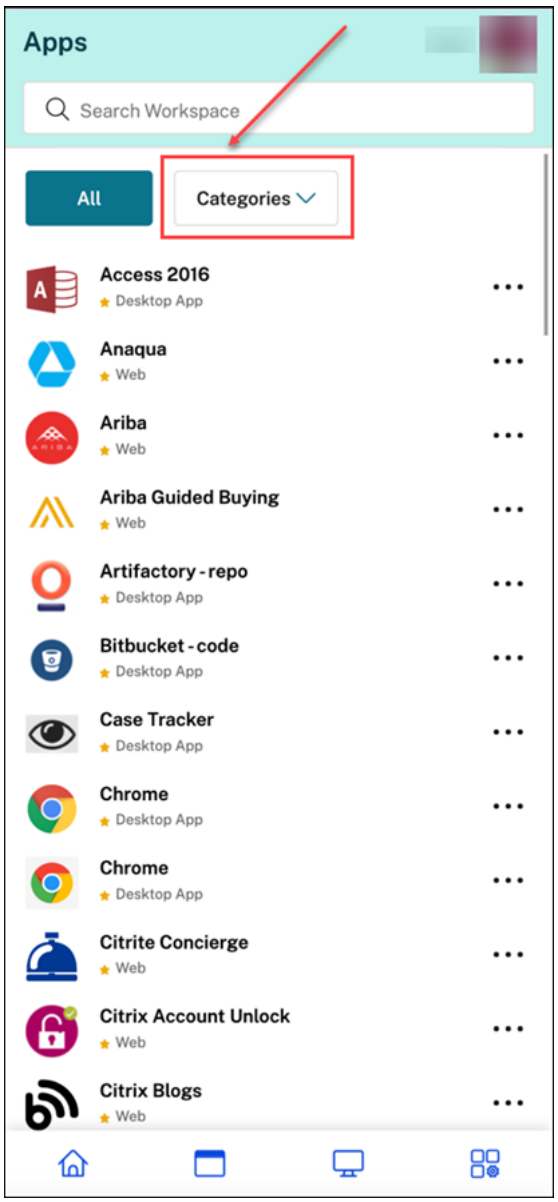
已知问题

- 活动管理器面板显示用户当前登录的所有商店中的活动会话。
- 启用了 App Protection 策略的应用程序不支持活动管理器操作，例如注销、断开连接等。

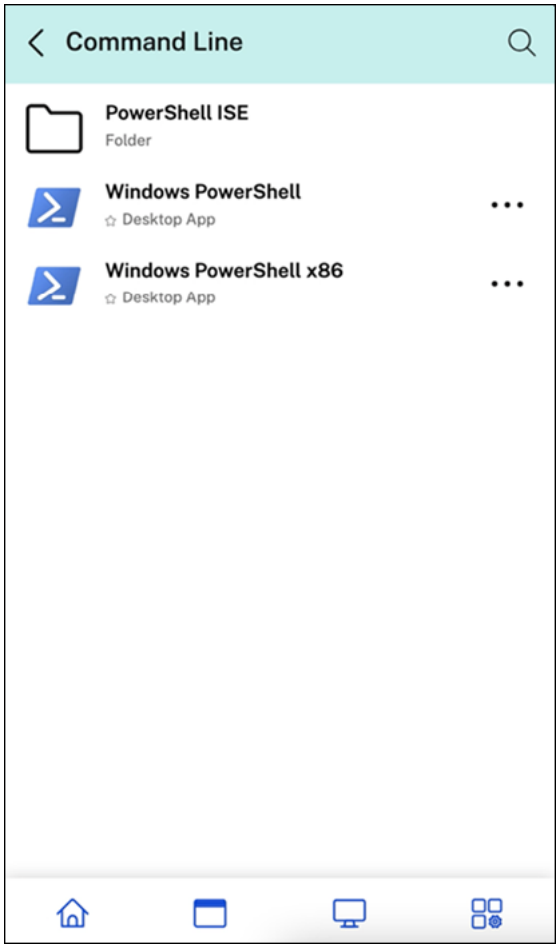
23.36

新增功能

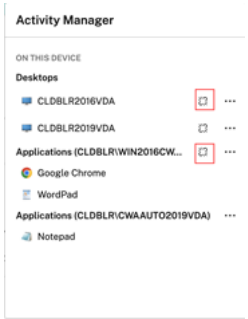
查看移动平台上应用程序的子类别　终端用户现在可以在 Android 和 iOS 设备上查看按类别和子类别整理的应用程序，从而提供便捷的访问和愉快的应用程序浏览体验。要查看类别，请导航至“应用程序”选项卡，然后单击“类别”下拉列表。



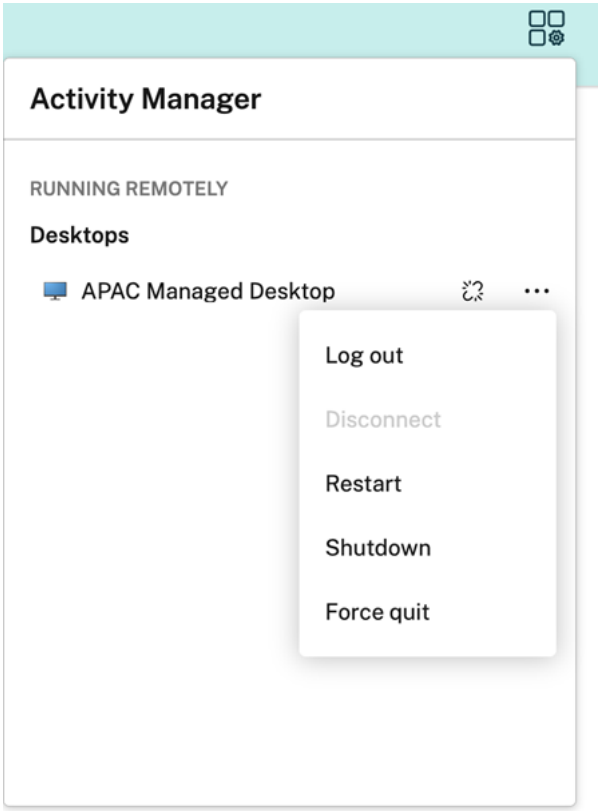
选择相关类别，将根据管理员所做的配置显示可用子类别和应用程序的列表。根据管理员配置，子类别显示为可能包含更多子文件夹或应用程序的文件夹。有关更多信息，请参阅添加文件夹路径



通过任何设备在活动管理器上管理已断开连接的会话　Activity Manager 现在允许最终用户在本地或远程查看以断开连接模式运行的应用程序和桌面，并对其执行操作。可以通过移动设备或台式设备管理会话，从而使最终用户能够随时随地采取行动。对断开连接的会话（例如注销或关闭）采取措施可以优化资源使用并降低能耗。



- 已断开连接的应用程序和桌面显示在“活动管理器”面板上，并以已断开连接的图标表示。
- 已断开连接的应用程序分组在相应的会话下，会话由已断开连接的图标表示。



通过单击省略号按钮，最终用户可以在已断开连接的桌面上执行以下操作：

- 注销：使用此功能从已断开连接的桌面上注销。会话中的所有应用程序都将关闭，所有未保存的文件都将丢失。
- 关机：使用此选项关闭已断开连接的桌面。
- 关机：如果出现技术问题，使用此选项强制关闭已断开连接的台式机的电源。
- 重新启动：使用此选项关闭并重新启动已断开连接的桌面。

有关更多信息，请参阅活动管理器中已断开连接的应用程序和桌面。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.35

新增功能

此版本解决了改进整体性能和稳定性的区域。

已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.34

新增功能

此版本解决了改进整体性能和稳定性的区域。

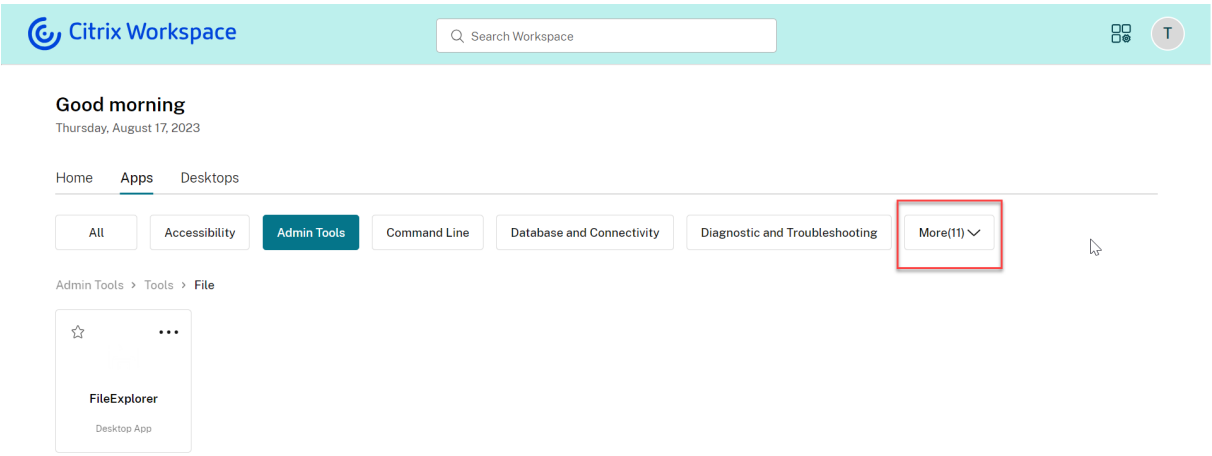
已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.33

新增功能

通过应用分类增强用户体验　最终用户可以在 Workspace 用户界面上查看按类别和子类别组织的应用程序。如果分类涉及两个以上的级别，则最终用户将看到他们的应用程序排列在文件夹结构中。用户可以看到导航痕迹。
当管理员创建的主要类别的数量超过用户屏幕上的可用空间时，用户界面会根据屏幕大小进行调整，并在“更多”下拉列表中动态移动类别。



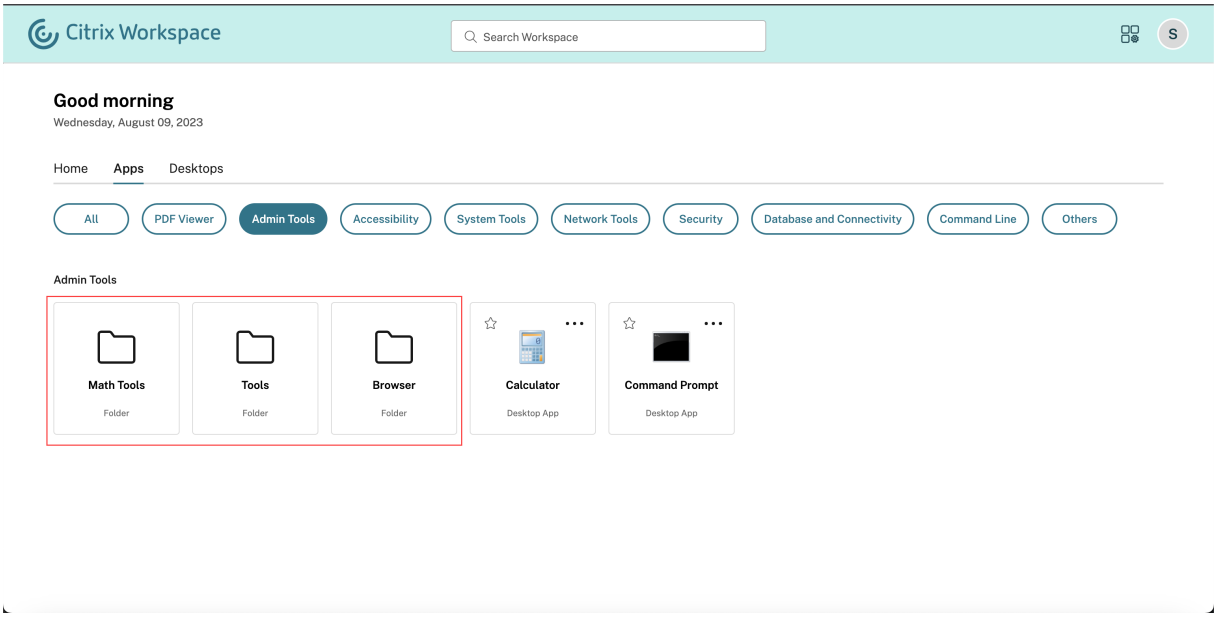
已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.32

新增功能

应用程序分类便于访问　管理员可以交付按类别和子类别整理的应用程序，从而为最终用户提供愉快的应用程序浏览体验。从第二层分类开始，最终用户将看到一个文件夹结构。有条理的多层结构可提供整洁、优化的体验，有助于提高整体用户满意度。有关创建文件夹和子文件夹的更多信息，请参阅创建交付组。



已修复的问题

此版本解决了改进整体性能和稳定性的区域。

23.31

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.30

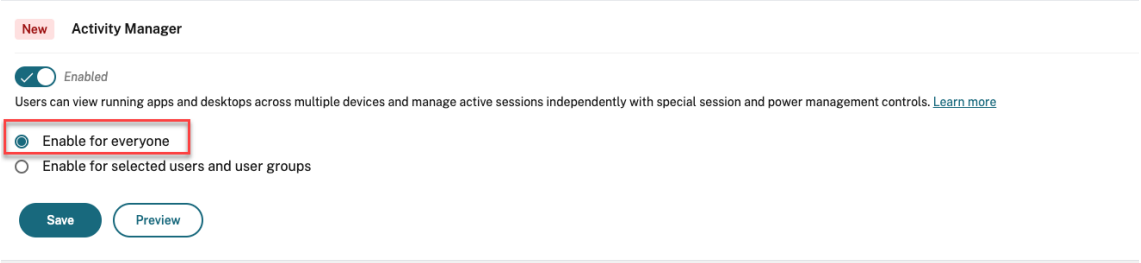
新增功能

管理活动管理器　作为管理员，您现在可以为最终用户启用或禁用“活动管理器”功能。根据组织政策，您可以为所有人或选定的用户和用户组启用该功能。启用后，“活动管理器”面板允许您的最终用户查看其活动应用程序和桌面并与之交互。有关更多信息，请参阅 活动管理器。

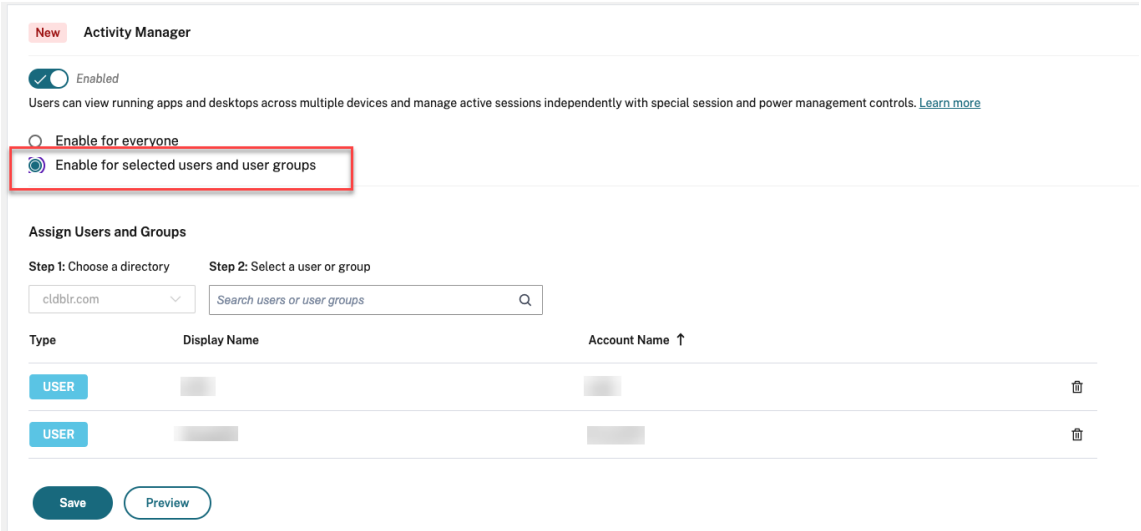
> 注意：
>
> 只有虚拟应用程序和桌面支持此功能。它不适用于 Web 和 SaaS 应用程序。

要启用活动管理器，请执行以下操作：

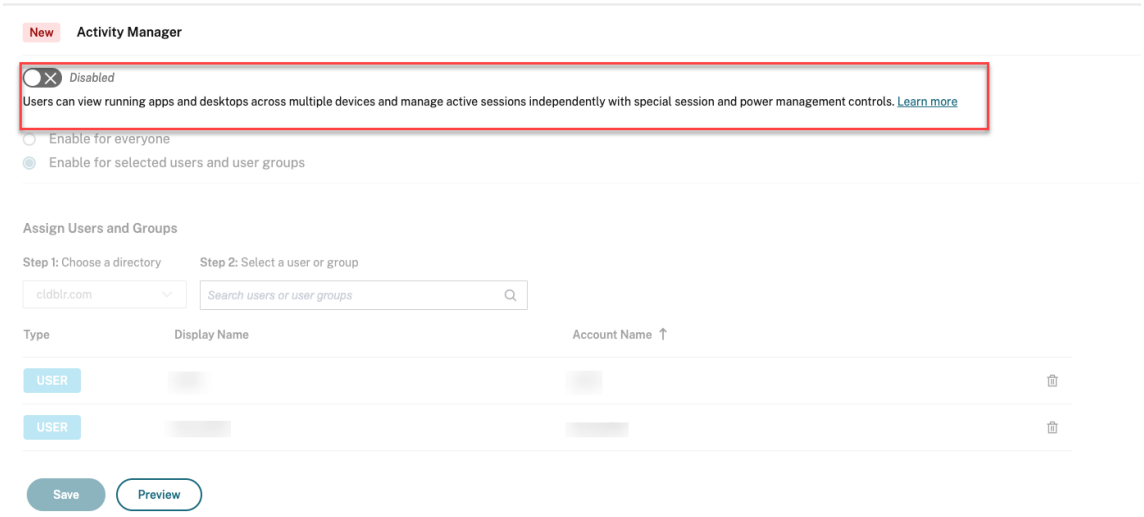
1. 在管理员控制台上，前往“**Workspace** 配置”>“自定义”>“功能”。
2. 在“活动管理器”部分中，打开开关以启用活动管理器。
3. 然后，您可以按如下所示自定义访问权限。
   - 要为所有最终用户启用活动管理器，请选择“为所有人启用”。



   - 要为选定的用户和用户组启用活动管理器，请选择为选定的用户和用户组启用。然后，您可以选择用户或用户组所属的目录。选择相应的目录后，您可以查看相关的用户和用户组。



- 要为所有人禁用“活动管理器”，请关闭开关。



4. 单击保存。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.29

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.28

新增功能

Internet Explorer 的弃用公告　Citrix Workspace UI 版本 23.26 将在 2023 年最后一周之前在 Internet Explorer 可用。Citrix 在 23.26 版本发布后不支持新增功能、缺陷修复或安全修复。此外，管理员会收到升级到支持的浏览器和支持的 LTSR（LTSR2203 或更高版本）的通知。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.27

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

- 通过此修复，实现了错误边界和组件级错误处理。[WSUI-7423]
- 单击省略号图标后，脱机横幅将最小化。[WSUI-7797]

23.26

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

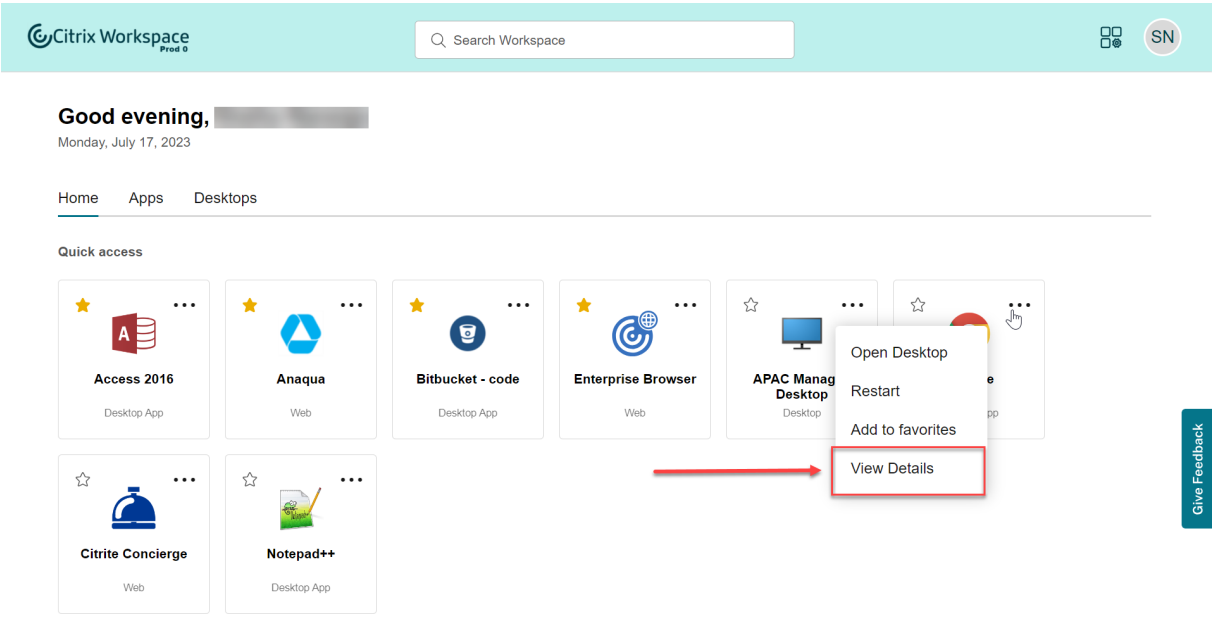
已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.25

新增功能

查看应用程序和桌面的描述　最终用户现在可以查看管理员提供的应用程序和桌面的描述。这些描述有助于理解应用程序或桌面的预期功能。如果存在多个名称相同但配置、位置、环境等不同的应用程序，它们尤其有用。
要查看应用程序或桌面的描述，请单击相应磁贴上的省略号，然后单击“查看详细信息”。



已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.24

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

23.23

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

此版本解决了有助于改进整体性能和稳定性的问题。

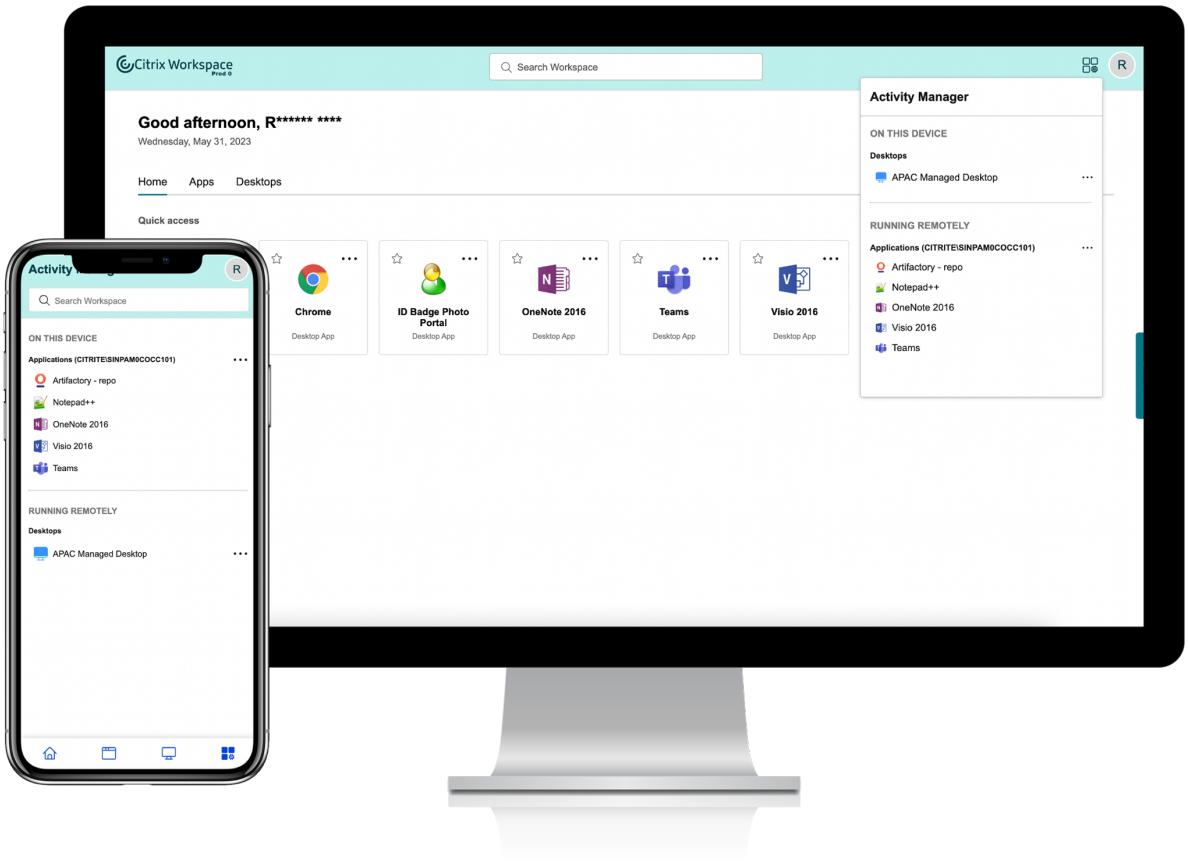
23.22

新增功能

活动管理器简介　现在，您可以通过 Workspace UI 中的单个窗口窗格管理在任何设备上处于活动状态的应用程序和桌面并对其进行快速操作。所有活跃的应用程序和桌面都分组在您当前正在使用的会话中。

活动管理器图标出现在配置文件图标左侧的 Workspace 用户界面窗口中。当您单击该图标时，您会看到以下内容：

- 在“在此设备上”下，应用程序和桌面列表从您正在使用的设备开始。
- 在“远程运行”下的“其他设备上处于活动状态的应用程序和桌面”列表。



有关更多信息，请参阅 活动管理器。

> 注意：
>
> 如果您无法清楚地查看活动管理器图标，请考虑更改在横幅文本和图标颜色设置中选择的颜色。由于横幅与活动管理器图标之间的对比度较低，该图标可能看不清楚。有关更多信息，请参阅配置自定义主题。

已知问题

- 如果会话断开连接，用户将无法从中注销。已断开连接的会话不会显示在“活动管理器”面板上。
- 在适用于 Mac 的 Citrix Workspace 应用程序上，活动管理器面板上显示的活动应用程序和桌面列表列出了来自所有应用商店的活动会话。

23.15

新增功能

新的 **Workspace** 用户界面　Citrix Workspace 应用程序引入了具有现代外观和感觉的新用户界面功能，可提供更清晰的视图。用户界面增强适用于 Web、桌面和移动设备。

增强的首次用户体验　当您首次从浏览器启动下载的 Citrix Workspace 应用程序或 Citrix 时，系统会弹出一个列出相关应用程序的屏幕。这些应用程序由管理员决定，您只需单击一下即可将这些应用程序添加为收藏夹。

增强的搜索体验　增强的搜索功能可让您更快地从搜索引擎中获得结果。搜索 选项允许您在 Workspace 应用程序中进行快速直观的搜索。

管理员相关任务

作为管理员，您可以为订阅者自定义 Workspace 应用程序的用户体验。有关更多信息，请参阅以下部分

- 为用户启用新的 Workspace 体验
- 为用户启用或禁用主屏幕

Global App Configuration Service 中的新增功能

November 26, 2023

以下部分列出了 Global App Configuration Service 当前和早期版本中的新功能。

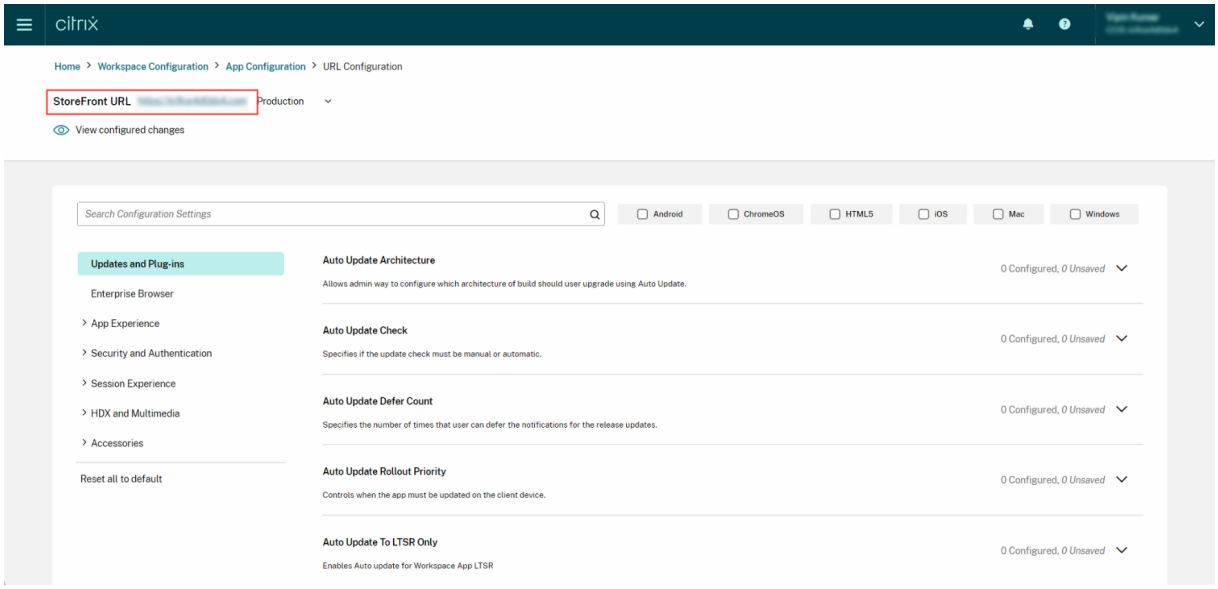
2023 年 10 月 30 日

为本地应用商店配置设置

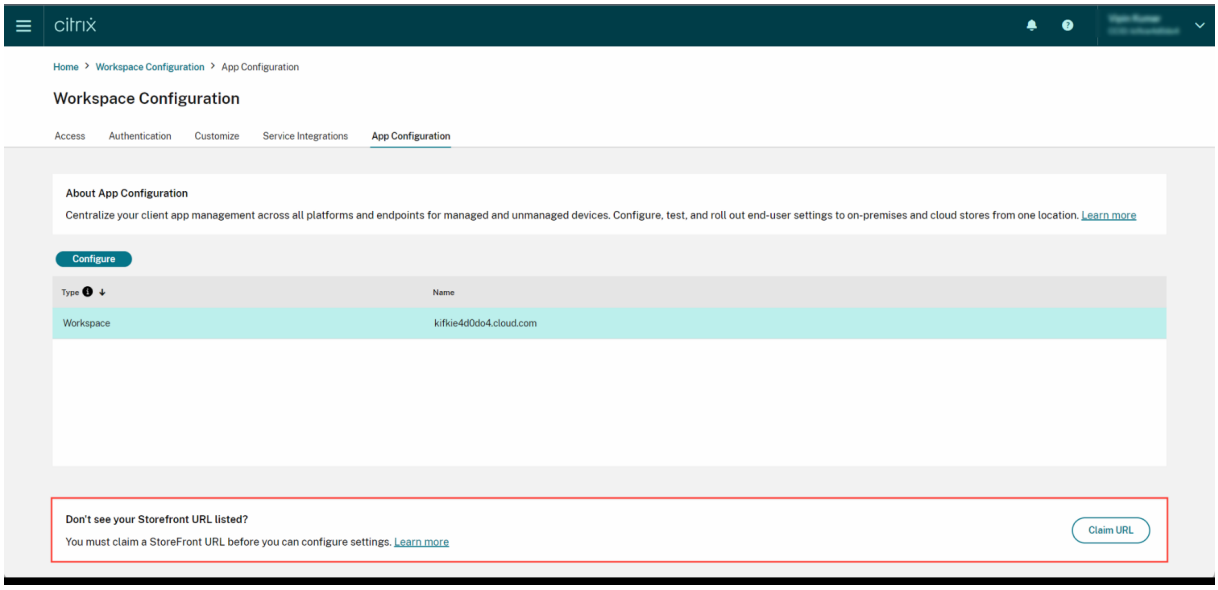
现在，您可以使用 Global App Configuration Service 用户界面来配置本地商店的设置。登录您的 Citrix Cloud 帐户并导航到 **Workspace** 配置 **>** 应用程序配置以开始使用。

> 注意：
>
> 如果您还没有 Citrix Cloud 帐户，请前往 Citrix 入门页面创建一个。

在继续操作之前，请确认您已对 StoreFront URL 提出声明。如果该 URL 已被声明，则会出现以下屏幕，您可以开始为本地商店配置设置。



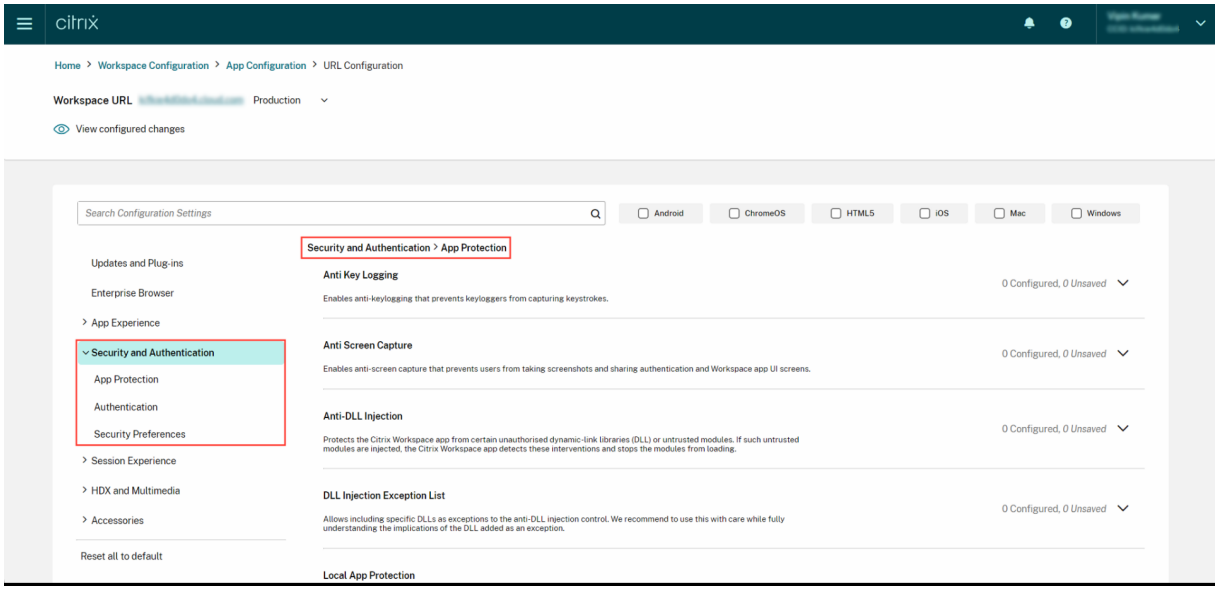
如果您尚未声明 URL，则会看到以下屏幕。单击“为本地应用商店配置设置”部分下的“开始”以声明您的 URL。有关更多信息，请参阅 入门。



2023 年 9 月 28 日

简化设置分类，便于导航

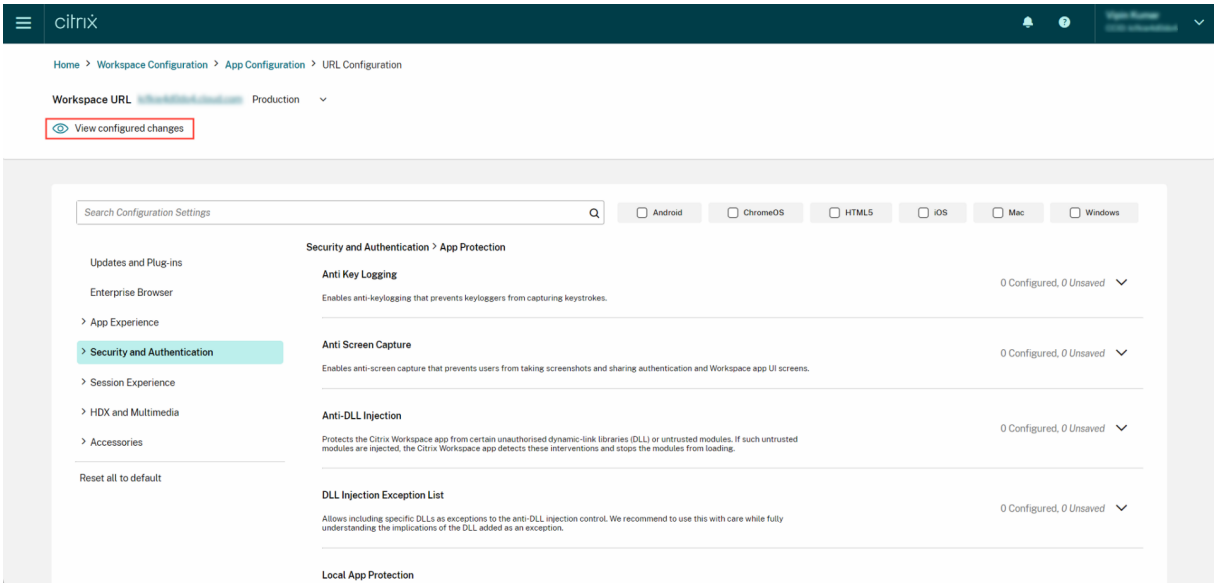
Global App Configuration Service 用户界面已得到增强，可提供用户友好的设置分类。这些设置已根据最终用户的工作流程和主题进行了分类，包括七个主文件夹和多个子文件夹。这个整洁的组织使管理员可以更轻松地在 300 多个设置中导航。



2023 年 7 月 28 日

查看已配置设置的摘要

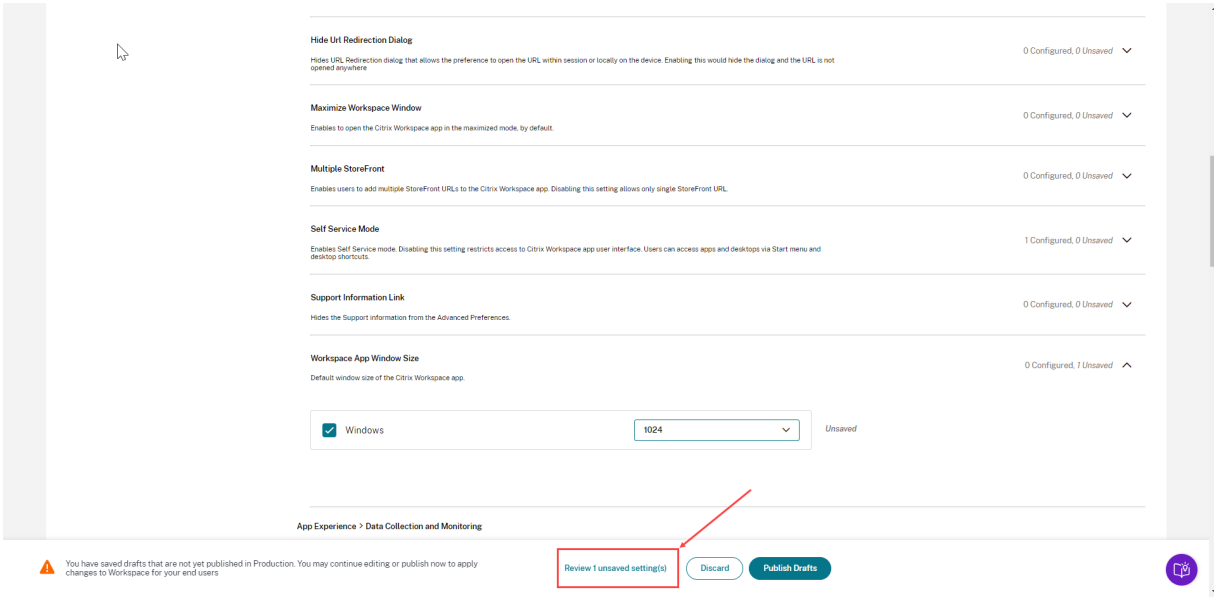
管理员现在可以通过单击“查看已配置的设置”按钮来查看当前配置的摘要。这样就无需单独扩展和查看每个设置。所有已配置设置的合并列表允许管理员对当前配置进行全面审查并衡量用户的影响。



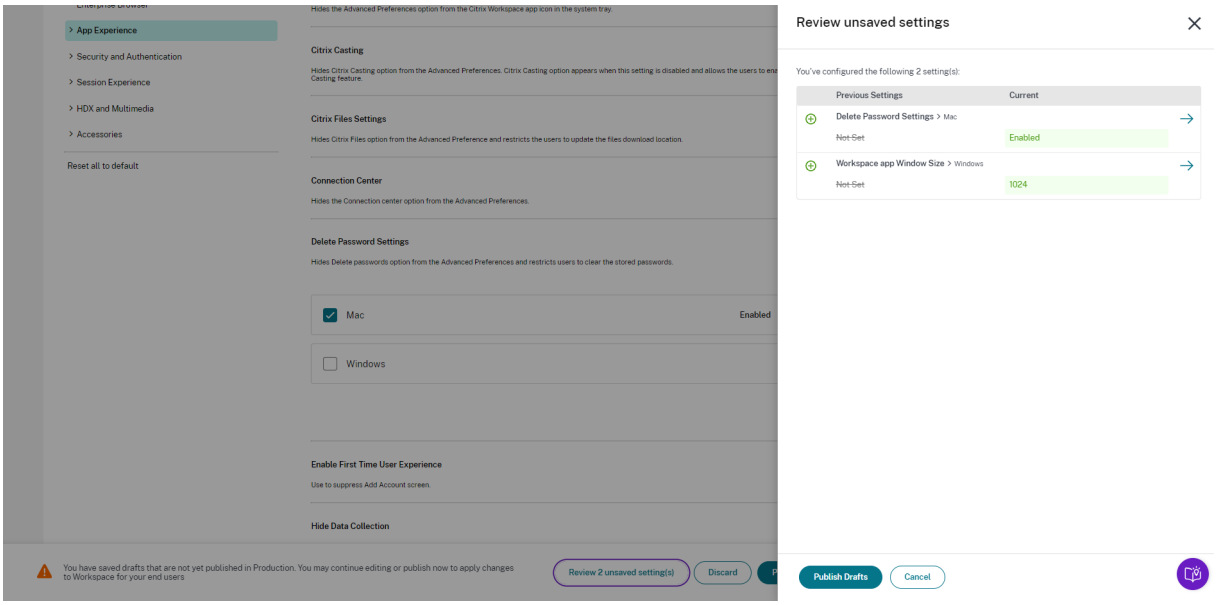
2023 年 6 月 7 日

查看未保存的更改

通过此增强功能，管理员可以在发布配置之前对其未保存的更改进行最终审核。未保存的设置数量显示在用户界面上，管理员可以通过单击“查看未保存的设置”选项来访问此列表。这使管理员能够做出明智的更改并保持数据的准确性。



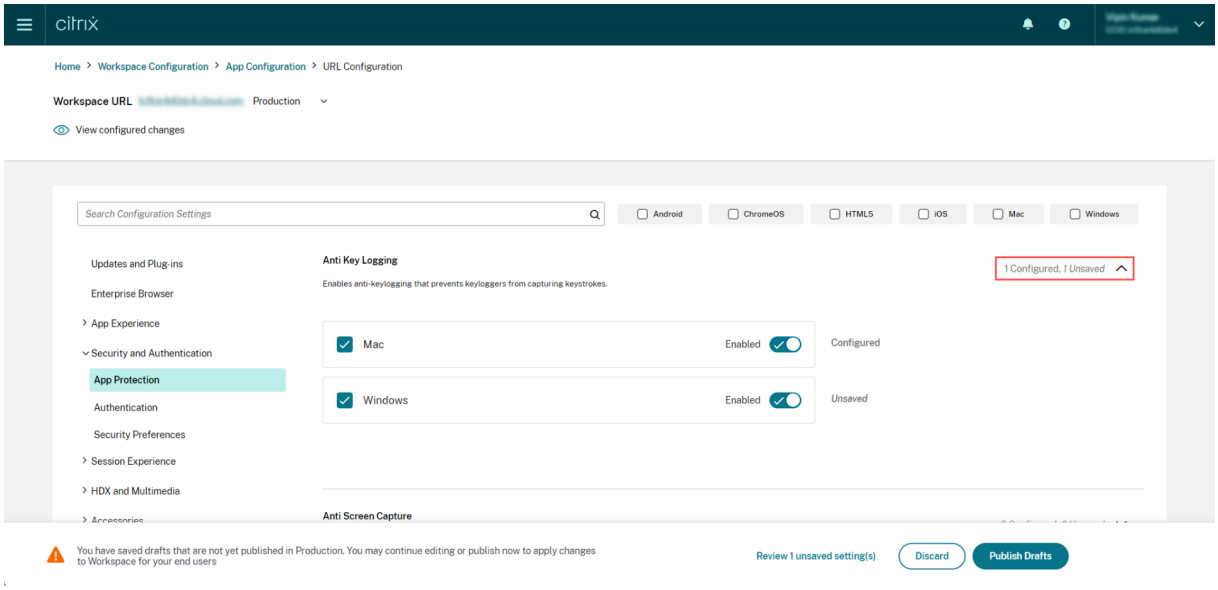
管理员还可以通过单击箭头导航到未保存的设置。



增强的用户界面

管理员现在无需展开即可查看每个设置的状态。现在显示了以下标签，便于在每个步骤中做出明智的决策。

- 已配置：显示已配置该设置的平台（客户端操作系统）的数量。
- 未保存：显示已配置但尚未保存的设置数量



May 23, 2023

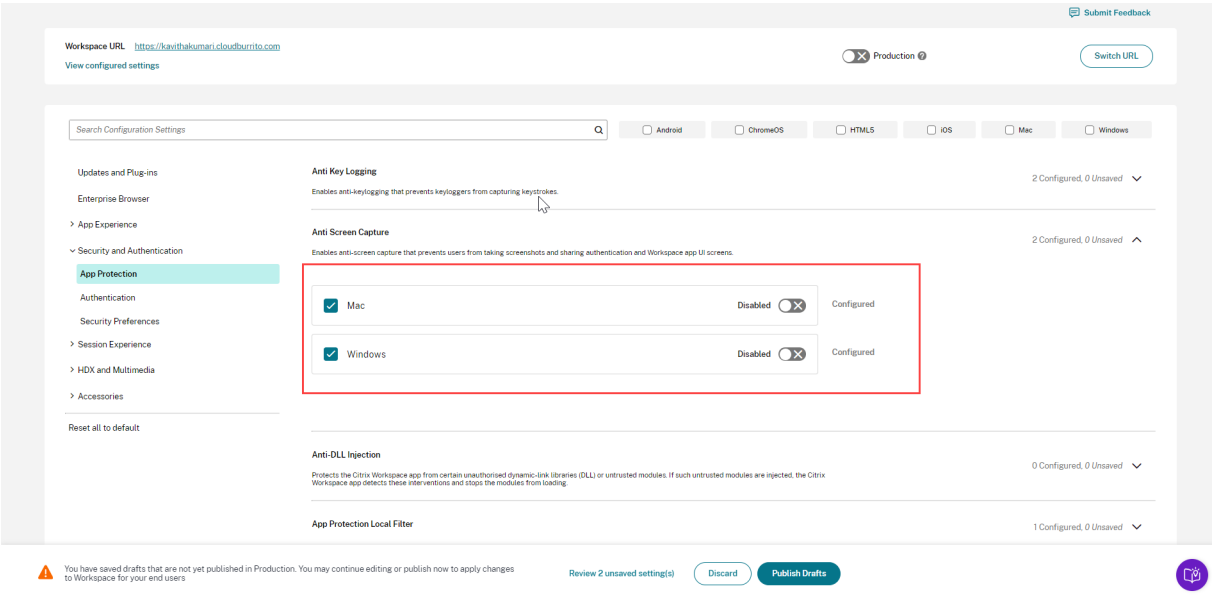
增强的搜索功能

通过此增强功能，搜索体验得到了增强，可提供强大而无缝的体验。管理员现在可以登录云端门户，在应用程序配置页面上轻松找到所需的设置。他们可以使用以下搜索方法。

- 使用设置描述进行搜索
  管理员还可以通过输入在设置描述中找到的关键字来查找设置。这使得搜索方法更加灵活，可以利用与所需设置相关的术语。
- 使用 **API** 设置名称进行搜索
  管理员可以选择通过输入相应的 API 设置名称来搜索设置。此方法允许更精确、更有针对性的搜索，使用户能够快速找到所需的特定设置。

查看每种设置的适用平台

现在，每项设置仅动态显示与其相关且适用的平台。这种智能筛选可确保为用户提供简明而量身定制的选项列表，从而消除不必要的混乱和混乱。



开始使用 **Citrix Workspace**

November 26, 2023

本文从头到尾概述了设置 Citrix Workspace 和相关组件所涉及的主要步骤。有关所涉及阶段的摘要，请参阅 工作流概述。

还有其他方法可以过渡到完整的 Citrix Workspace 体验。最常见的是：

- 通过工作区交付 Citrix Virtual Apps and Desktops。
  - 如果要通过 Workspace 访问本地 Virtual Apps and Desktops 部署中的资源，请参阅混合解决方案的站点聚合。
  - 如果要迁移到云，请参阅 完全迁移到云。

工作流程概述

如果将 Citrix Workspace 设置为新客户，则分为 5 个主要的工作阶段：

1. 为 Citrix Cloud 中的 Citrix Workspace 做好准备。
2. 配置订阅者访问和身份验证。
3. 将服务集成到工作区。
4. 根据企业特定的首选项（例如徽标和安全策略）自定义工作区 。
5. 向订阅者推出 Citrix Workspace。

成功中心 提供其他基于解决方案的指导。

第 **1** 阶段：为 **Citrix Citrix Cloud** 中的 **Citrix Workspace** 做好准备

在配置 Citrix Workspace 之前，您必须注册 Citrix Cloud 并确保满足开始使用 Citrix Workspace 的技术要求。

如果您已经是 Citrix Cloud 客户，并且通过 身份识别和访问管理添加了管理员，则可以跳到 第 2 阶段：配置订阅者访问和身份验证。

第 1 阶段涉及的步骤包括：

1. 注册 Citrix Cloud。
2. 添加具有 Citrix 身份的管理员。
3. 通过以下方式设置基础架构：
    - 创建资源位置
    - 部署 Cloud Connector

配置 Citrix 身份涉及基于时间的一次性密码 (TOTP)。除了 Citrix 身份之外，您还可以配置 Azure AD 身份验证。有关添加管理员和配置管理员身份验证的更多信息，请访问 Citrix Cloud 产品文档中的 管理员 。

第 **2** 阶段：配置订阅者访问和身份验证

第 2 阶段涉及在 **Workspace** 配置中配置访问控制，例如 Workspace URL 和外部连接。

您还可以在身份识别和访问管理中配置一个或多个身份提供者，然后在 **Workspace** 配置中启用其中一个作为订阅者对工作区进行身份验证的主要方式。

> 注意：
>
> 有两种方法可以访问 Citrix Workspace。一种是通过本机安装的 Citrix Workspace 应用程序，该应用程序取代了 Citrix Receiver，可以简单、安全地访问 Citrix Cloud 服务和工作区。访问 Citrix Workspace 的另一种方法是通过带有 工作区 URL的浏览器。默认情况下，工作区 URL 处于启用状态，格式通常为：`https://yourcompanyname.cloud.com`。
>
> 有关更多信息，请访问 工作区访问权限。

配置 **Workspace** 访问权限

您可以在“**Workspace** 配置”**>**“访问权限中配置访问控制。这通常涉及以下任务：

- 配置并启用工作 区 URL。
- 使用 Citrix Gateway 配置外部连接。

完成这两个任务后，Citrix 建议您安装 Citrix Workspace 应用程序，并鼓励订阅者使用 Citrix Workspace 应用程序，以获得一致的工作区体验。

配置工作区的订阅者身份验证

定义订阅者如何通过身份验证以登录其工作区是一个分为两个步骤的过程：

1. 在 身份识别和访问管理中，配置身份提供程序。
2. 在 **Workspace** 配置身份验证中，选择您在第一步中配置的身份提供商提供的身份验证方法之一。

如果您使用的是联合身份提供商，则还可以使用 Citrix 联合身份验证服务 (FAS) 启用 DaaS 的单点登录 (SSO)。

有关配置工作区订阅者身份验证的更多信息，请访问 安全工作区。

第 **3** 阶段：将服务集成到工作区

将您的服务集成到工作区是另外一个分为两部分的过程：

1. 在 Citrix Cloud 中配置您购买的服务。有关服务列表，请访问 Citrix Cloud 服务。
2. 在 **Workspace** 配置 **>** 服务集成中启用对已配置服务的访问权限。有关服务集成的更多信息，请访问 启用和禁用服务。

第 **4** 阶段：自定义工作区

您可以通过以下方式为不同用户自定义工作区的订阅者体验，并满足 **Workspace** 配置中的特定组织要求：

- 自定义工作区的外观，包括徽标和自定义主题。有关自定义工作区外观的说明，请访问 自定义工作区的外观。
- 选择交互选项，例如允许订阅者创建收藏夹和自动启动桌面。有关自定义订阅者与其工作区交互方式的说明，请访问 自定义工作区交互。
- 自定义隐私和安全性，包括设置超时期限、创建登录策略以及允许订阅者在其工作区内更改密码。有关如何自定义 Workspace 隐私和安全策略的说明，请访问 自定义安全和隐私策略。

第 **5** 阶段：向订阅者推出 **Citrix Workspace**

Citrix 建议您通过运营验收测试来验证工作区的完整性，并与我们的 成功中心 联系以规划如何加入订阅者。这一阶段的广泛活动包括：

1. 测试工作区。
    - 确认您可以通过浏览器登录并登录 Citrix Workspace 应用程序。
    - 启动并使用所有可用的应用程序和桌面。
    - 检查是否可以访问可用的文件夹和文件。
    - 检查通知是否显示了预期的操作和活动。
    - 如果启用，请验证您是否可以在移动设备上访问终端节点资源。
2. 入职订阅者。

- 与订阅者沟通 Citrix Workspace 功能。
- 共享浏览器工作 区 URL。
- 指导用户安装 Citrix Workspace 应用程序。

有关测试工作区和加入工作区订阅者的更多信息，请访问 Citrix Workspace 最终用户采用资源。

为 **Citrix Workspace** 做准备

November 26, 2023

本文概述了帮助您为实施 Citrix Workspace 做准备的要求和管理活动。准备 Citrix Workspace 所涉及的步骤包括：

1. 确保您满足 Citrix Cloud 的 系统和连接要求 。
2. 规划您的 Citrix Workspace 的部署和部署 。
3. 登录或注册 Citrix Cloud。
4. 将管理员添加 到 Citrix Cloud 和 Citrix Workspace。
5. 检查您对云托管服务的授权 。
6. 设置 Citrix Workspace 所需的基础架构 。

成功中心 是本文档的重要合作伙伴。Success Center 文章提供了基于解决方案的广泛视角和特定于服务的详细信息。

Citrix Cloud 产品文档为 IT 经理和开发人员提供了有关在 Citrix Cloud 中准备 Citrix Workspace 所涉及的先决条件和活动的更详细指导。

系统和连接要求

Citrix Cloud 是用于查看和管理服务授权以及访问 **Workspace** 配置的控制台。

如果您已针对 Citrix Cloud 进行了设置，则可以跳至 规划部署和部署中概述的步骤。

总而言之，Citrix Cloud 需要以下配置：

- 用于管理工作区订阅者身份验证的 Active Directory 域。
- 每个资源位置至少有两个 Citrix Cloud 连接器。
- 每个 Cloud Connector 都有一台专用计算机。
- 加入您的域的物理机或虚拟机用于托管工作负载和其他组件。

您至少需要两台物理机或虚拟机，因为您无法在托管 Citrix Cloud Connector 的计算机上安装其他组件。

有关 Cloud Connector 要求的信息，请参阅 Citrix Cloud Connector 技术详细信息。有关安装 Cloud Connector 的信息，请参阅 Cloud Connector 安装。

此外，必须联系以下地址才能操作 Citrix Workspace：

- `https://*.cloud.com`
- `https://*.citrixdata.com`

有关 Citrix Cloud 服务所需的可联系地址的完整列表，请参阅 服务连接要求。

规划部署和推出

Citrix 建议您准备 Citrix Workspace 支持和管理计划。使用 成功中心计划 确定目标、定义使用案例、识别风险并制定实施策略，其中包括以下内容：

- 确定业务成果、要添加的服务以及用户组要求。
- 确定为 Citrix Workspace 设置基础设施的技术要求。
- 组建您的 Workspace 团队。将任务分配给交付团队，并将管理员添加到具有 **Workspace** 配置访问权限的 Citrix Cloud 帐户。
- 计划与流程所有者和订阅者的互动。
  - 制定变革战略和沟通计划。
  - 制定培训和强化方法。
  - 进行影响和利益相关者分析。

有关规划 Workspace 部署和部署的更多信息，请参阅成功中心的 成功准备情况清单。

登录或注册 **Citrix Cloud**

如果您以新客户身份注册，请按照 注册 Citrix Cloud 中的说明进行操作。

如果已经为您的组织创建了管理员帐户，则主管理员需要将您添加到公司帐户。有关更多信息，请参阅 添加管理员 。

如果您已经有帐户，请使用您的 citrix.com、我的 Citrix 或 Citrix Cloud 凭据登录 Citrix Cloud。

有关登录或注册 Citrix Cloud 的更多信息，请参阅 Citrix Cloud 服务启动指南。

添加管理员

第一个管理员帐户是通过初始 Citrix Cloud 入职流程创建的。然后，初始管理员可以邀请其他管理员加入 Citrix Cloud。这些新管理员可以使用其现有的 Citrix 帐户凭据或设置新帐户。

邀请管理员

管理员可通过 Citrix Cloud 控制台左侧菜单中的 身份识别和访问管理 添加到您的 Citrix Cloud 帐户。输入要添加的管理员的电子邮件地址，向他们发送带有登录说明的邀请。

将管理员添加到 Citrix Cloud 帐户时，您需要定义适合其在组织中的角色的管理员权限。默认情况下，具有完全访问权限的管理员可以访问 **Workspace** 配置。具有 自定义访问权限 的管理员只能访问您选择的功能和服务。您可以更改邀请的管理员的访问权限。

有关添加（和移除）管理员的更多信息，请参阅 管理员。

设置管理员身份验证

默认情况下，Citrix Cloud 使用 Citrix 身份提供商来管理您的 Citrix Cloud 帐户。Citrix 身份提供程序仅对 Citrix Cloud 管理员进行身份验证。订阅者必须使用 安全工作区中列出的身份提供商之一进行身份验证。

您的 Citrix Cloud 帐户中的每位管理员还必须设置多重身份验证 (MFA)。

注册涉及下载和安装遵循 基于时间的一次性密码 (TOTP) 标准的身份验证应用程序，例如 Citrix SSO。为了顺利注册，Citrix 建议在完成以下步骤之前下载并安装 Citrix SSO。

1. 登录到您的 Citrix Cloud 帐户。
2. 选择您的姓名，然后从下拉菜单中选择 我的个人资料。
3. 选择“登录安全”下的“设置身份验证器应用程序”，接收一封包含步骤 4 所需验证码的电子邮件。
4. 出现提示时，输入 Citrix 通过电子邮件发送给您的验证码和您的帐户密码，然后选择验证。
5. 扫描二维码或在遵循基于时间的一次性密码 (TOTP) 标准的身份验证应用程序（例如 Citrix SSO）中输入密钥。
6. 要确认 MFA 已正确设置，请输入身份验证应用程序中的 6 位数代码，然后选择“验证”。
7. 选择“添加辅助电话”，然后输入 Citrix Support 可以联系到您的电话号码，以验证您的身份，以进行与 MFA 相关的查询。
8. 选择 生成备份代码 以创建一次性使用代码列表，如果您无法访问身份验证器应用程序，则可以使用这些代码。
9. 选择“下载代码”，将包含备份代码的文本文件保存在安全且易于访问的位置。
10. 选中该复选框，然后选中 完成。

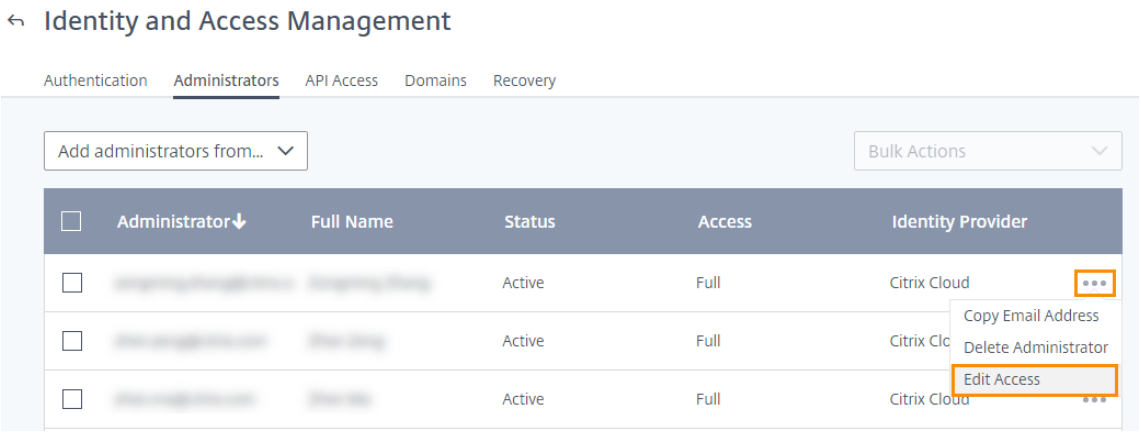
有关设置 MFA 的说明，也可以在知识中心和 Citrix Cloud 产品文档的设置多重身份验证中找到。

也可以选择为管理员设置 Azure Active Directory (AD)。有关 Citrix Cloud 管理员和 Workspace 订阅者可用的身份提供商的更多信息，请访问 身份提供商。

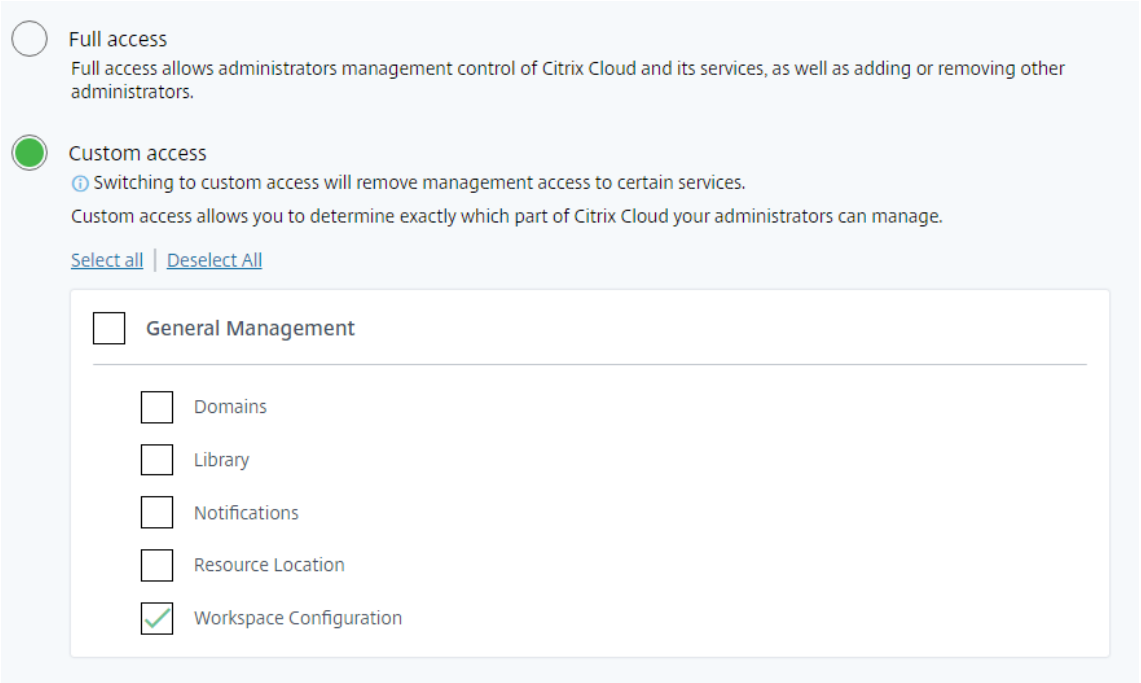
编辑管理员权限

要配置对 **Workspace** 配置的自定义访问权限，请执行以下操作：

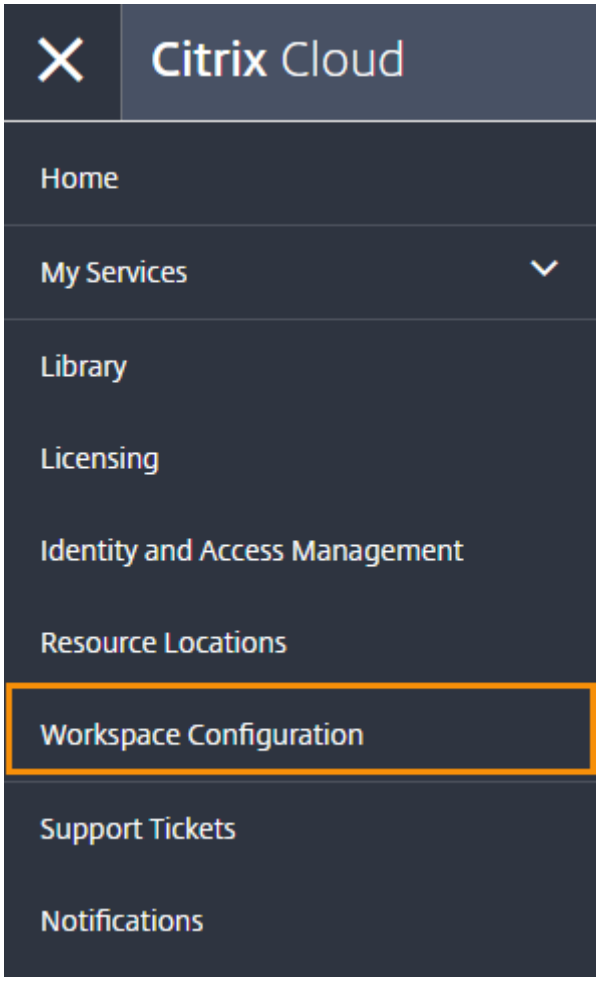
1. 在 **Citrix Cloud** 菜单中，选择身份和访问管理，然后选择管理员。
2. 找到要管理的管理员，选择省略号按钮，然后选择 编辑访问权限。



3. 检查 自定义访问 是否已启用。
4. 要仅启用“**Workspace** 配置”访问权限，请选择“常规管理”下的“**Workspace** 配置”。



启用访问权限后，管理员可以登录 Citrix Cloud 并从 **Citrix Cloud** 菜单中选择 **Workspace** 配置。



> 注意：
>
> 在 Citrix Virtual Apps Essentials 中，创建第一个目录后，可以从 Citrix Cloud 菜单中访问 **Workspace** 配置。

查看您的权利

登录 Citrix Cloud 后，您可以管理您的授权，即您购买的 Citrix 产品和服务。Citrix 产品和服务在 Citrix Cloud 控制面板中以卡片布局显示。您购买和订阅的产品和服务包括 管理 按钮。

如果要尝试一项新服务，可以在 Citrix Cloud 控制面板的相应框中选择 请求试用或请求演示。有关服务试用的更多信息，请访问 Citrix Cloud 服务试用版。

如果您想购买新服务，可以将试用版转换为生产服务，而无需重新配置或创建新帐户。要购买服务，请记下 Citrix Cloud 控制台右上角的组织 ID，然后访问 https://www.citrix.com/product/citrix-cloud。

设置基础架构

设置 Citrix Workspace 所需的基础设施需要通过以下方式将您的资源连接到 Citrix Cloud：

- 在您的环境中部署连接器。
- 正在创建资源位置。

资源位置包含向您的订阅者提供云服务所需的资源。您可以从 Citrix Cloud 控制台管理这些资源。资源位置包含不同的资源，具体取决于您使用的服务。

要创建资源位置，您需要在域中至少安装两个 Cloud Connector。

Citrix Cloud Connector 是一个组件，它为 Citrix Cloud 与您的资源位置之间的通信提供渠道。该通道使用标准 HTTPS 端口 (443) 和 TCP 协议建立与云的连接。不接受任何传入连接。

有关更多信息，请访问 Citrix Cloud Connector。

> 注意：
>
> Workspace 不支持来自使用 PNAgent URL 连接到资源的旧版客户端的连接。如果您的环境包含这些旧版客户端，则必须改为在本地部署 StoreFront 并启用旧版支持。要保护这些客户端连接，请在本地使用 Citrix Gateway 而不是 Citrix Gateway 服务。

下一步：建立您的工作区

现在，您已经为 Citrix Workspace 做好了准备，接下来的步骤如下：

- 配置对工作区的访问权限，包括工作区 URL 和外部连接。
- 使用 安全工作区中的说明配置工作区身份验证。
- 将服务集成到工作区。
- 自定义工作区体验：
  - 自定义工作区的外观。
  - 自定义工作区交互。
  - 自定义安全和隐私政策。

新的 **Workspace** 用户界面

November 26, 2023

全新 Workspace 用户界面 (UI) 降低了视觉复杂性，提供了对基本功能的轻松访问，并根据需要优化您的 Workspace 应用程序的使用和功能，从而带来更好的用户体验。

本文重点介绍了订阅者登录工作区时看到的一些主要功能，并总结了如何访问工作区并与之交互。

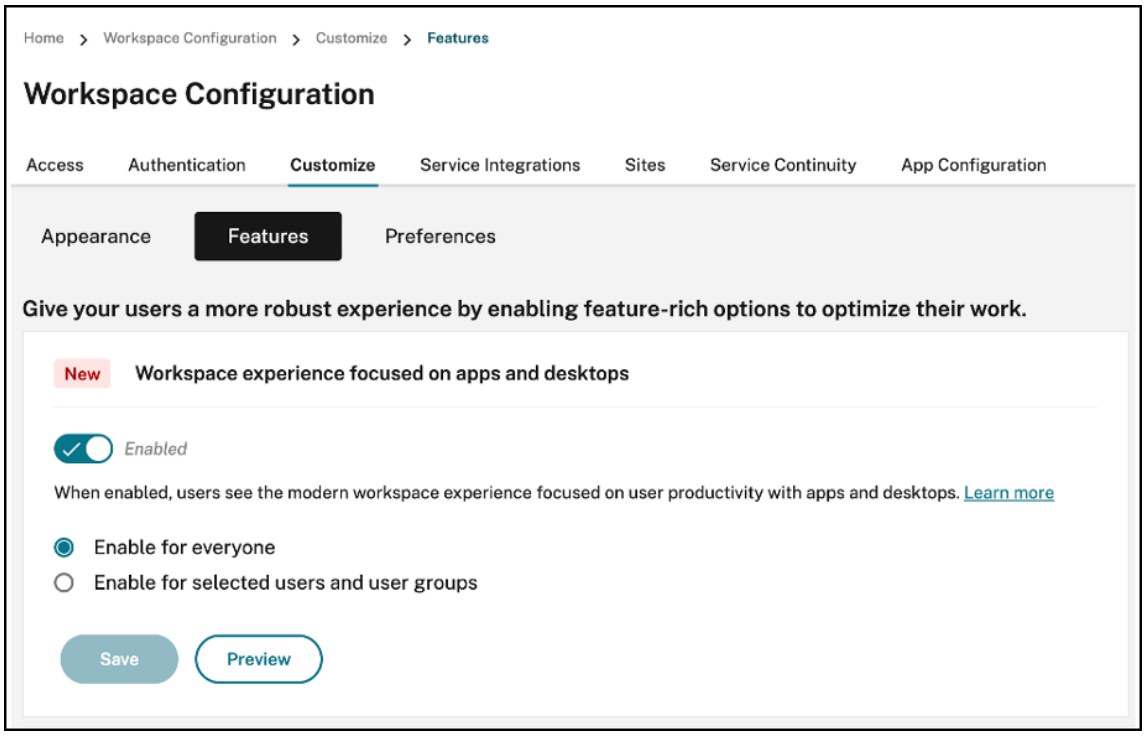
> 注意：
>
> 所有 LTSR 版本的 Citrix Workspace 应用程序都支持新用户界面。它还兼容除了 Internet Explorer（Citrix Workspace UI 版本 23.26 已冻结）之外的所有 Web 浏览器。

启用全新的 **Workspace** 体验

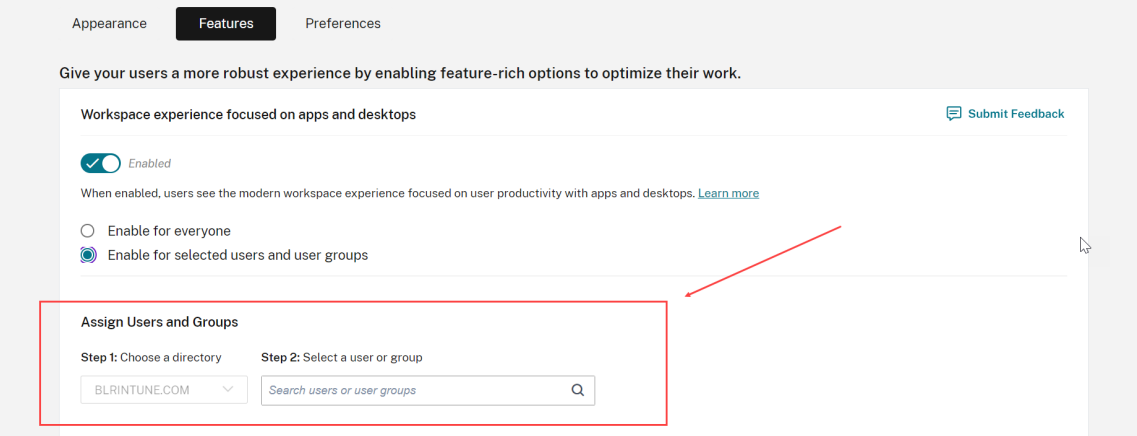
您可以为现有用户启用新的 Workspace 用户界面。启用后，用户可以通过应用程序和桌面体验专注于提高工作效率的现代工作区。

要启用新 UI，请执行以下步骤：

1. 在管理员控制台上，转到 **Workspace** 配置 **>** 自定义 **>** 功能。
2. 在“以应用程序和桌面为重点的 **Workspace** 体验”部分中打开开关。默认情况下，开关处于关闭状态，并且该功能处于禁用状态。
   您还可以选择为所有用户或选定用户启用此功能。



   - To enable the new UI for all end users, select **Enable for everyone**.
   - To enable the new UI for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



3. 单击保存。
4. 重启 Workspace 应用程序。

> 注意：
>
> 更新后的用户界面可能需要大约五分钟才能显示。用户可能会暂时看到旧版本的用户界面。如果在浏览器上打开，用户可能需要刷新页面。

主题、图标和字体

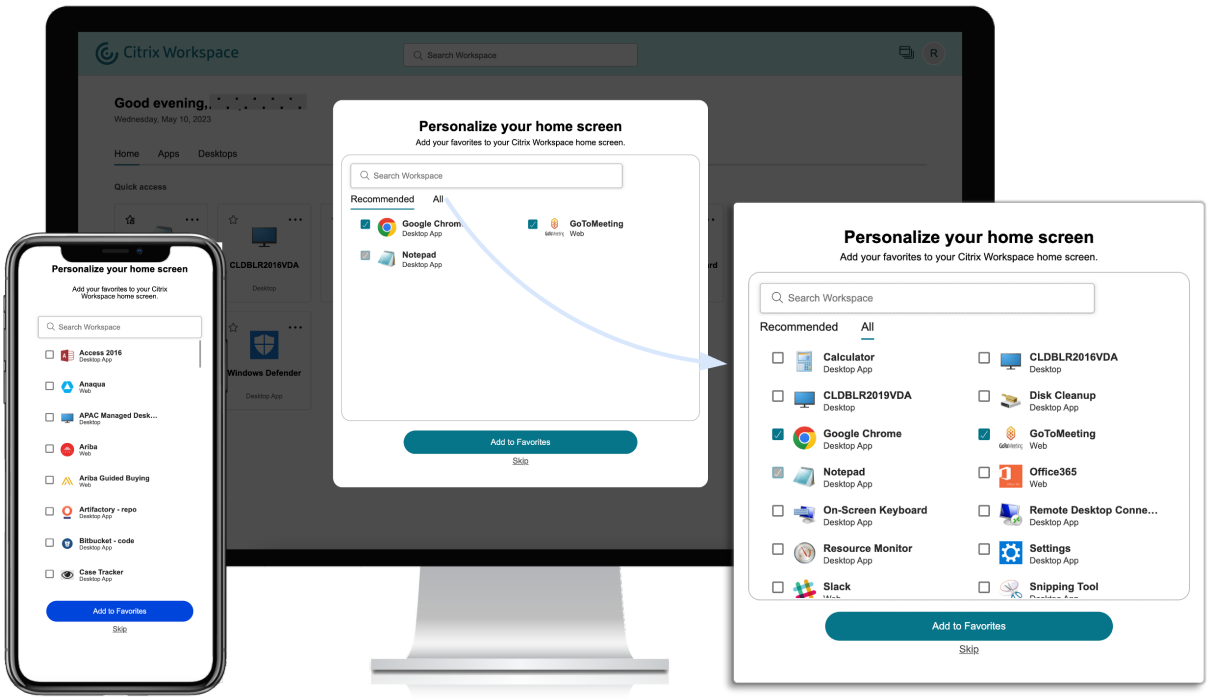
新的颜色主题改善了对比度和一致的调色板。该字体用于所有支持的操作系统上的用户界面。新的图标集具有更多可区分的形状和颜色，旨在提高易读性和视觉清晰度。

Workspace 应用程序的首次用户体验

访问新用户界面时，系统会弹出一个弹出窗口，提示您只需一个简单的步骤即可收藏多个应用程序。

如果您拥有超过 20 个应用程序，并且尚未将任何应用程序添加到“收藏夹”，则会激活首次用户体验。所有浏览器和原生客户端（Mac、Windows、Linux 和 ChromeOS）以及移动设备（iOS 和 Android）都支持这种体验。您可以在第一次登录时看到它。

推荐或必选应用程序显示在首次使用用户屏幕的“推荐”选项卡上，由管理员在 DaaS 控制台上为 Citrix Virtual Apps and Desktops 设置，在 Web 和 SaaS 应用程序的 Secure Private Access 控制台上设置。默认情况下，强制应用程序处于选中状态，并选中禁用。默认情况下，推荐 和自动收藏的应用程序处于选中状态，并为用户选中已启用。您也可以选择其他应用程序进行订阅，或者从所有选项卡中添加到“收藏夹”。所有选定的应用程序都会自动添加到“收藏夹”，并反映在主页上。



当您有五个或更少的应用程序时，在适用于 Windows 的 Citrix Workspace 应用程序上，会出现快速访问桌面快捷方式。

所有显示的应用程序都是为用户订阅的，并创建了相应的桌面快捷方式。

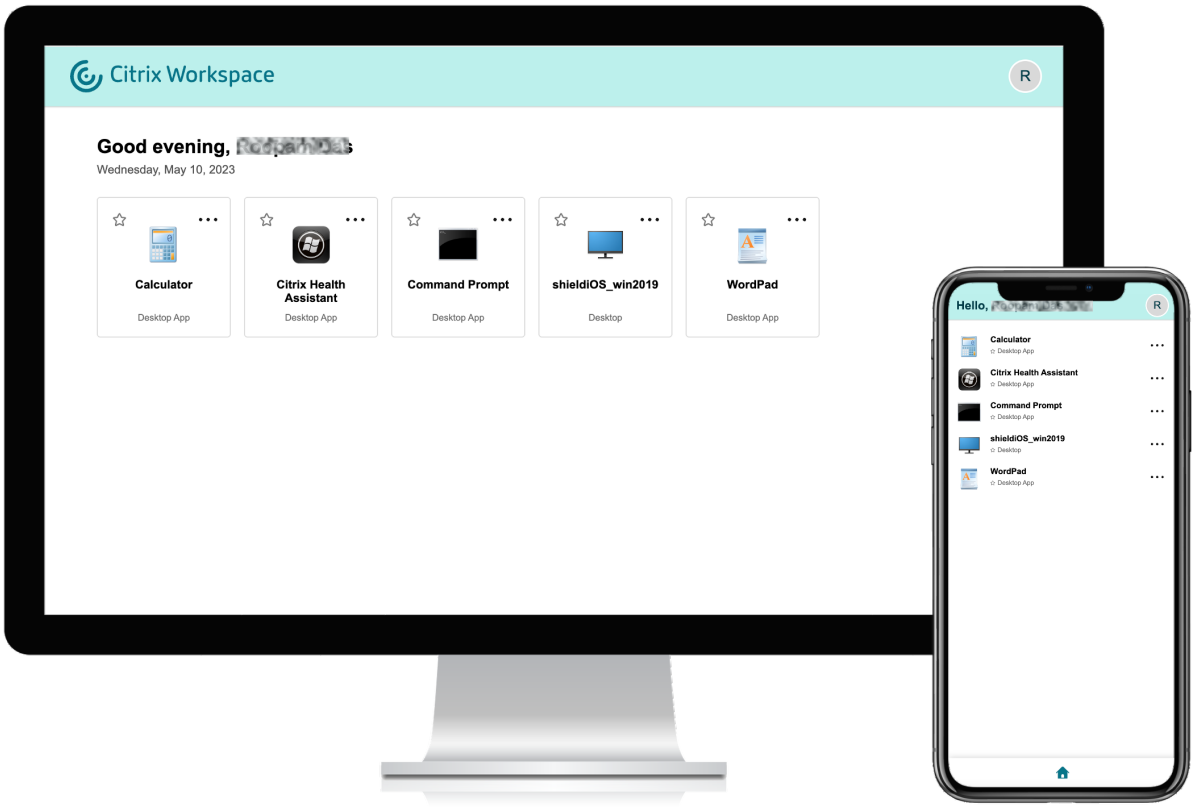
限制

- 在增强 用户个性化服务 以跟踪用户是否为首次用户之前，个性化 屏幕会在每台设备和浏览器中显示一次，在隐身模式下每次出现一次个性化屏幕，除非用户标记为收藏。
- 如果管理员从应用程序中移除必填或推荐标签，则 收藏夹 中的应用程序将不会产生任何影响。
- 如果最终用户未将任何应用程序添加到“收藏夹”，则每次打开 Workspace 应用程序时都会出现“个性化”屏幕。为了避免这种情况，请执行以下操作：
  - End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.
  - Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage** > **Full Configuration** > **Applications**). This prevents the Personalization screen from appearing for all the end-users. For more information, see Customize workspace interactions.

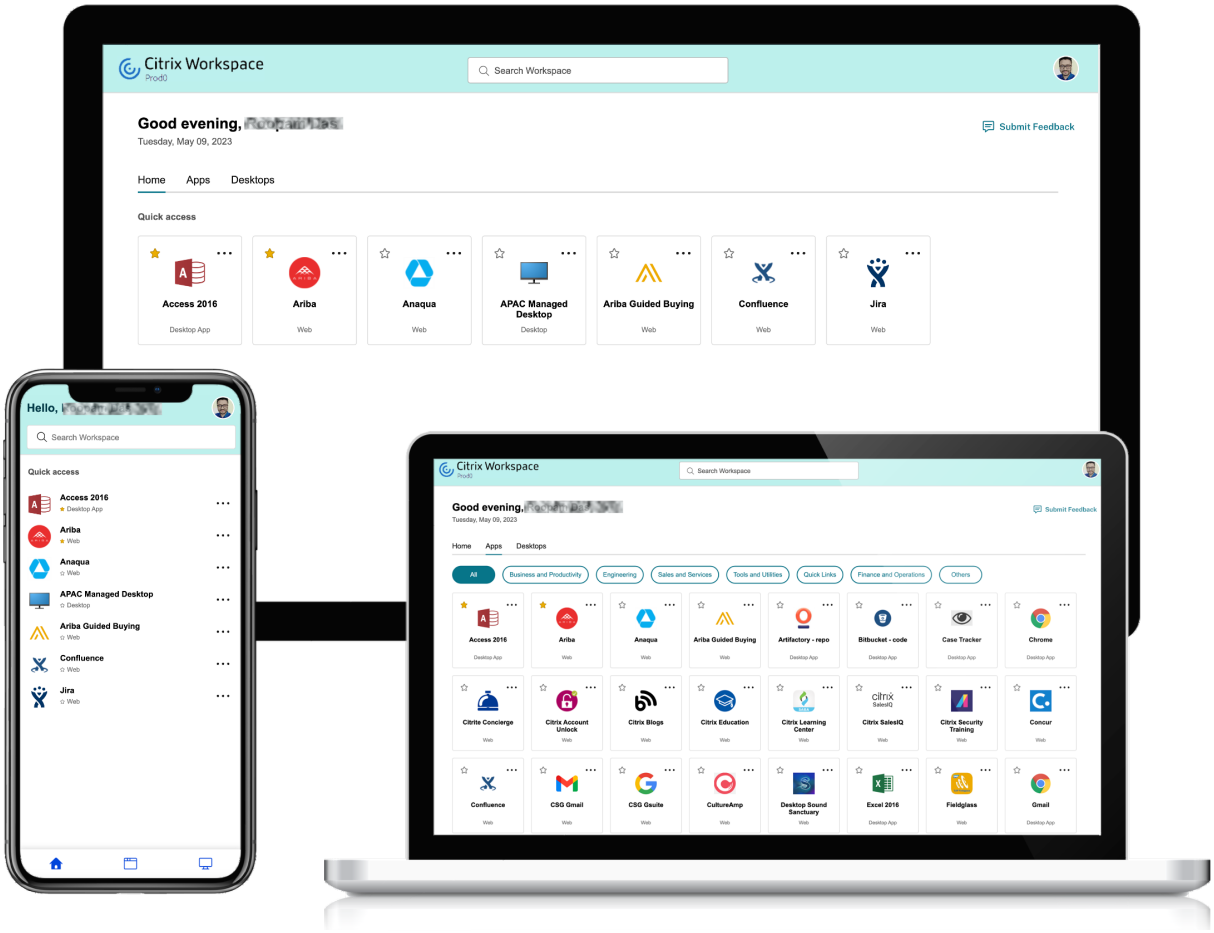
Workspace 视觉和布局改进

新的用户体验的设计侧重于直观的流程和易用性。为了便于使用，您的应用程序、虚拟桌面收藏夹位于用户界面的顶部。Citrix 还有一个新的主页，可以改善您更常用的应用程序和桌面的可导航性。

如果您的应用程序少于 20 个，那么您进入屏幕时会看到一个没有任何选项卡或类别的简单视图。所有应用程序和桌面都显示在同一个页面上。在此屏幕上，您的收藏夹首先显示，然后是按字母顺序排列的所有其他应用程序。所有应用程序都有一个星形图标，您可以使用它来收藏或取消收藏的应用程序。您可以体验到 Workspace 应用程序的这种简单视图，具体取决于您拥有的应用程序数量，而且这些应用程序不受管理员控制。



如果您有超过 20 个应用程序，则在登录时会进入主页。在此屏幕上，所有您最喜欢的应用程序都会首先出现，其次是最近使用的应用程序，仅限五个应用程序。强制 应用程序的星形图标已锁定，您无法将其从“收藏夹”中删除。如果管理员尚未启用主页，则您将进入 应用程序 屏幕。在此屏幕上，您的收藏夹首先出现，然后是按字母顺序排列的所有其他应用程序。如果管理员创建了类别并将应用程序附加到这些类别中，则会出现各种类别，并可以选择要查看的应用程序的类别。



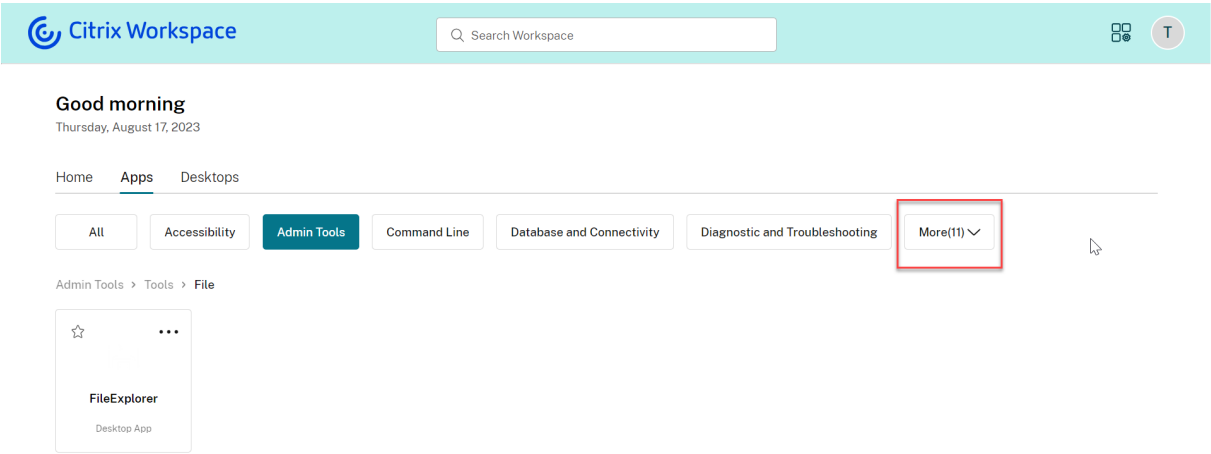
应用程序分类

最终用户可以在 Workspace 用户界面上查看按类别和子类别组织的应用程序。子类别以文件夹结构显示。有条理的多层结构可提供整洁、优化的体验，有助于提高整体用户满意度。

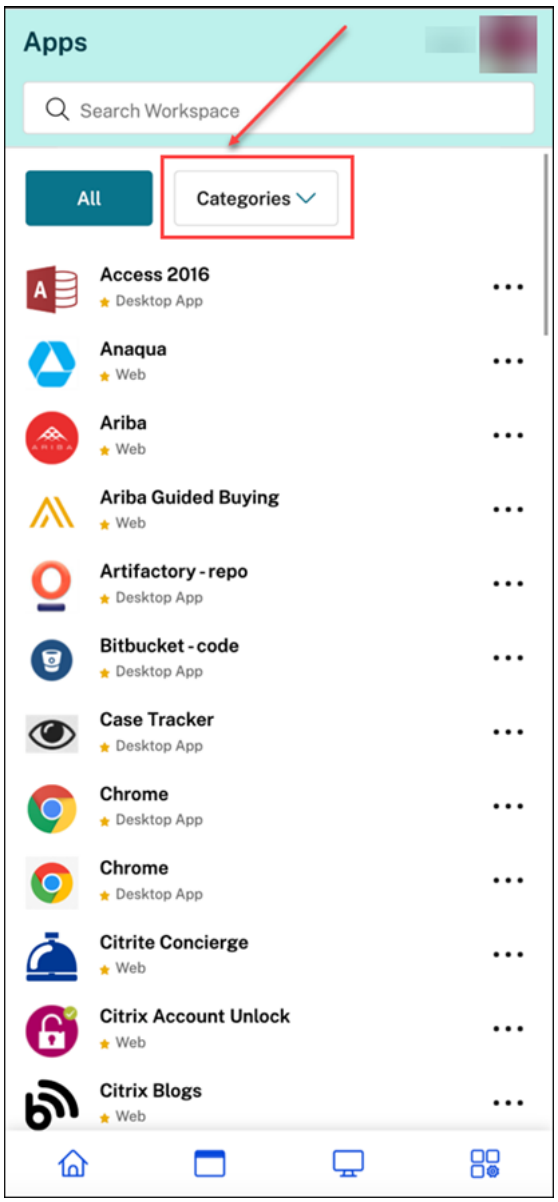
> 注意：
>
> 要使应用程序显示在文件夹结构下，管理员必须添加文件夹路径。有关更多信息，请参阅添加文件夹路径。

当管理员创建的主要类别的数量超过用户屏幕上的可用空间时，用户界面会根据屏幕大小进行调整，并在“更多”下拉列表中动态移动类别。

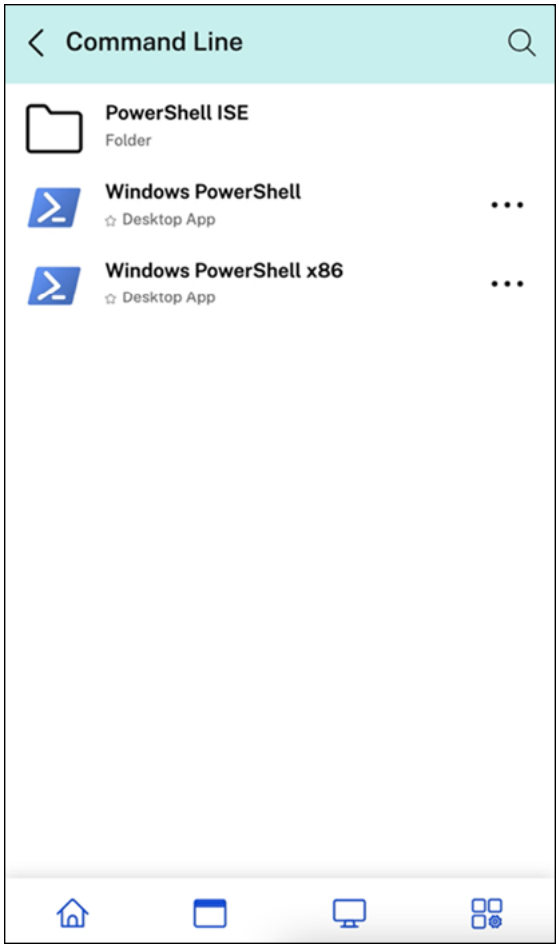
还会向用户显示导航痕迹。



在移动平台上，导航到“应用程序”选项卡，然后单击“类别”下拉列表以查看可用类别的列表。根据管理员配置，子类别显示为可能包含更多子文件夹或应用程序的文件夹。



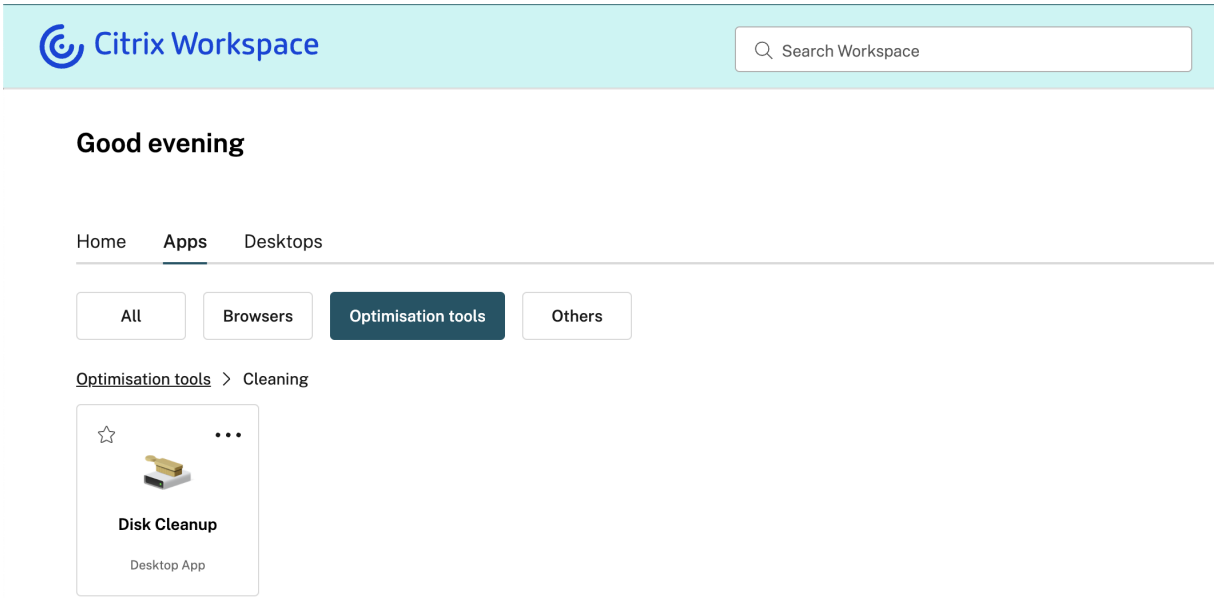
选择相关类别，将根据管理员所做的配置显示可用子类别和应用程序的列表。



添加文件夹路径

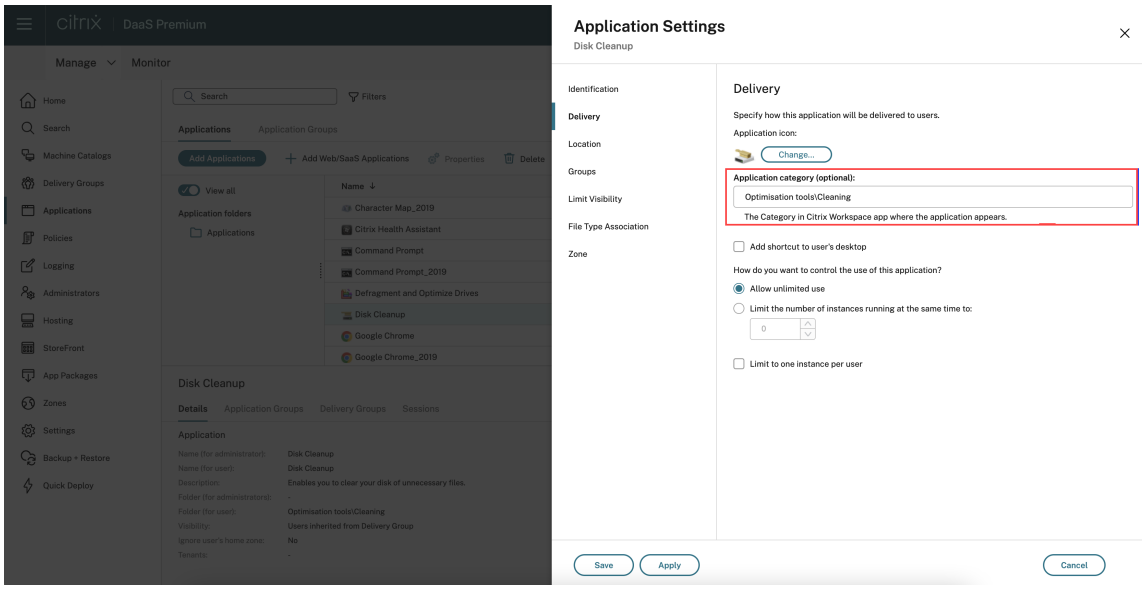
文件夹路径可帮助您定义应用程序的显示类别。它代表屏幕上为最终用户显示的文件夹结构。

例如，假设将文件夹定义为 `Optimisation tools/Cleaning` 的应用程序。现在，要访问此应用程序，最终用户必须转到优化工具 > 清洁，其中优化工具是一个类别，清理是其子类别。



要定义应用程序的文件夹路径，请执行以下操作：

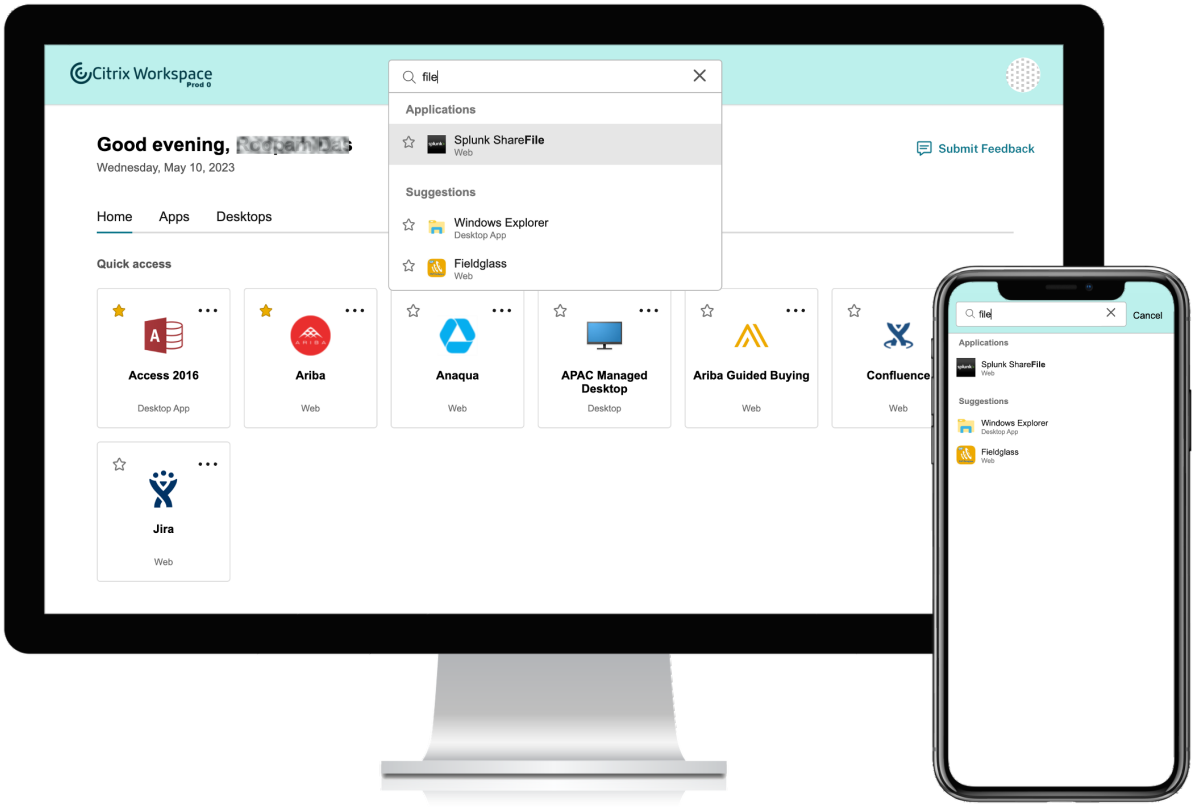
1. 在管理云控制台上导航到 **Citrix DaaS**。
2. 转到“应用程序”并找到该应用程序。
3. 右键单击应用程序，然后选择“属性”。
4. 在“应用程序类别”字段中，定义文件夹路径。



5. 单击保存

增强的搜索功能

增强的搜索功能可让您更快地从搜索引擎中获得结果。为便于使用，搜索 选项出现在工具栏中，允许您在 Workspace 应用程序中进行快速直观的搜索。



它包括以下改进：

- 默认搜索显示最近使用的五个应用程序或桌面
- 使用拼写检查启用搜索，并显示自动完成的结果
- 搜索结果包括基于最近访问的虚拟会话中的应用程序以及 Web 和 SaaS 应用程序
- 按管理员创建的类别进行搜索
- 搜索结果在顶部列出 收藏夹

活动管理器

November 26, 2023

活动管理器是 Citrix Workspace 中一项简单而强大的功能，它使用户能够有效地管理自己的资源。它通过便于在任何设备上对活动应用程序和桌面进行快速操作来提高工作效率。用户可以与其会话进行无缝交互，结束或断开不再需要的会话，从而释放资源并优化移动性能。

“活动管理器”面板显示了不仅在当前设备上处于活动状态的应用程序和桌面的综合列表，还会在任何具有活动会话的远程设备上处于活动状态。用户可以通过单击桌面上个人资料图标旁边和移动设备屏幕底部的“活动管理器”图标来查看此列表。

> 注意：
>
> 如果您无法在较暗的横幅主题中查看 Activity Manager 图标，请考虑更改和测试在横幅文本和图标颜色设置中选择的颜色。由于横幅与活动管理器图标之间的对比度较低，该图标可能看不清楚。有关更多信息，请参阅配置自定义主题。

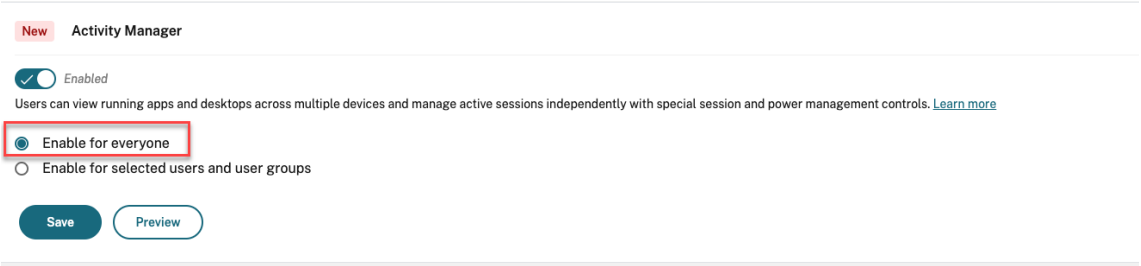
启用活动管理器

作为管理员，您现在可以为最终用户启用或禁用“活动管理器”功能。根据组织政策，您可以为所有人或选定的用户和用户组启用该功能。

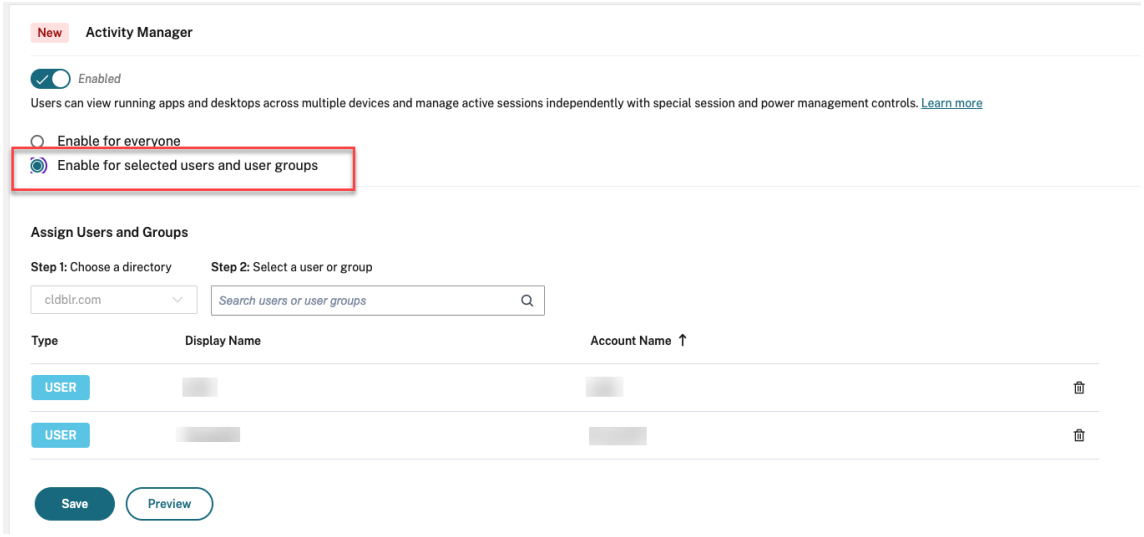
> 注意：
>
> 只能为新用户界面启用活动管理器功能。有关新 UI 的更多信息，请参阅启用全新 Workspace 体验

要启用活动管理器，请执行以下操作：

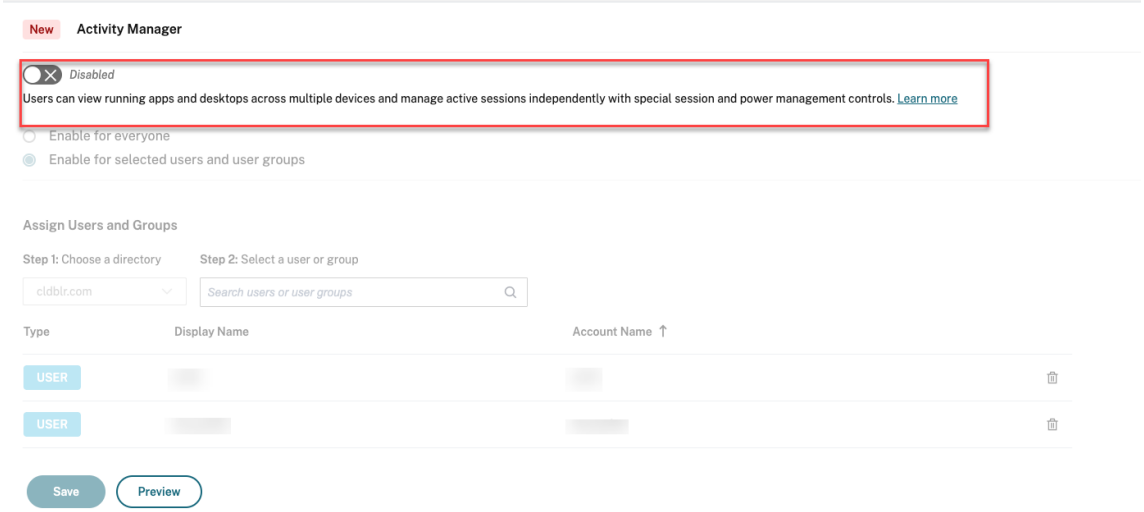
1. 在管理员控制台上，前往“**Workspace** 配置”>“自定义”>“功能”。
2. 在“活动管理器”部分中，打开开关以启用活动管理器。
3. 然后，您可以按如下所示自定义访问权限。
   - 要为所有最终用户启用活动管理器，请选择“为所有人启用”。



   - 要为选定的用户和用户组启用活动管理器，请选择为选定的用户和用户组启用。然后，您可以选择用户或用户组所属的目录。选择相应的目录后，您可以查看相关的用户和用户组。



- 要为所有人禁用“活动管理器”，请关闭开关。



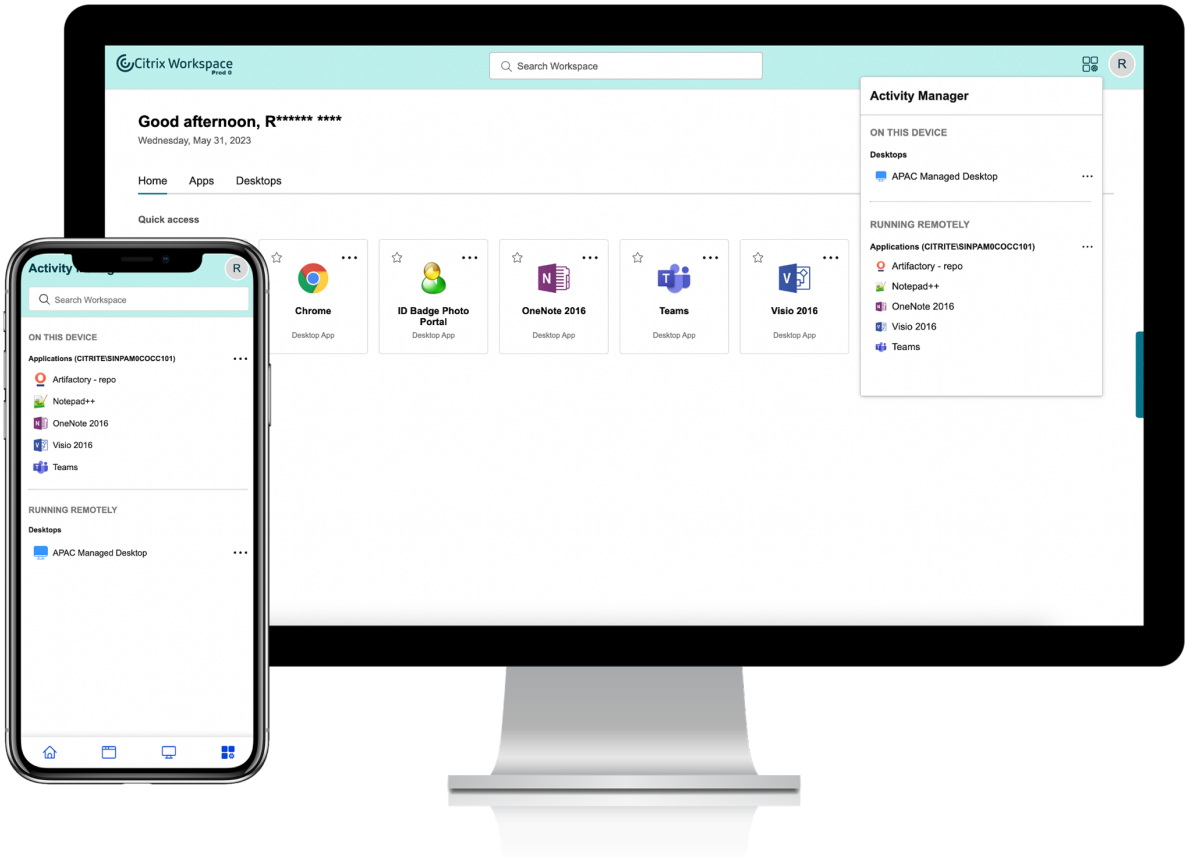
4. 单击保存。

> 注意：
>
> 只有虚拟应用程序和桌面支持此功能。它不适用于 Web 和 SaaS 应用程序。

使用活动管理器

活动管理器中的活动应用程序和桌面按以下方式分组。

- 当前设备上处于活动状态的应用程序和桌面的列表分组在“在此设备上”下。
- 在其他设备上处于活动状态的应用程序和桌面的列表分组在“远程运行”下。

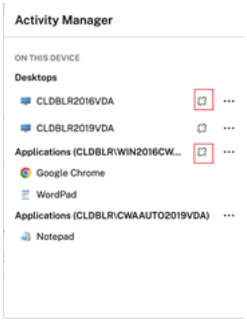


用户可以通过单击相应的省略号 (···) 按钮在应用程序或桌面上执行以下操作。

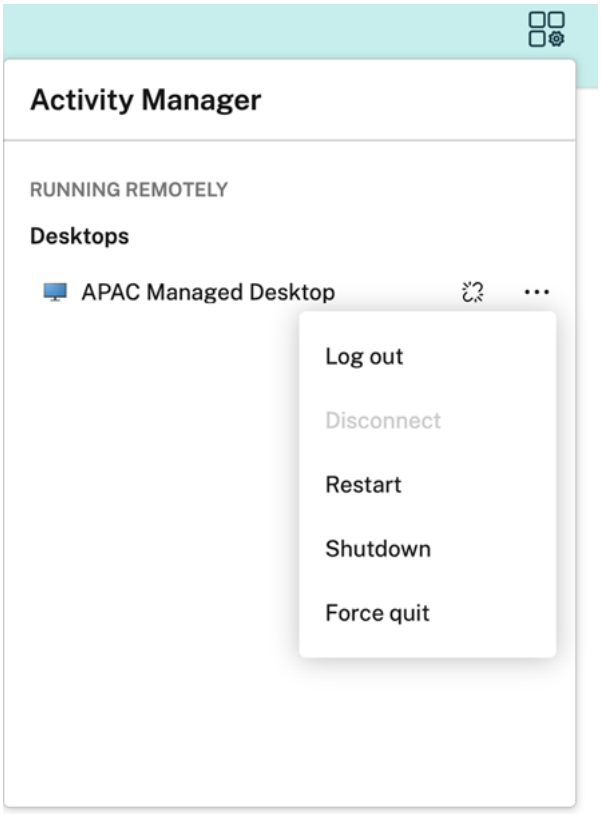
- 断开连接：远程会话已断开连接，但应用程序和桌面在后台处于活动状态。
- 注销：注销当前会话。会话中的所有应用程序都已关闭，所有未保存的文件都将丢失。
- 关闭：关闭断开连接的桌面。
- 强制退出：如果出现技术问题，请强行关闭桌面电源。
- 重新启动：关闭桌面并重新启动。

已断开连接的应用程序和桌面

Activity Manager 现在允许最终用户在本地或远程查看以断开连接模式运行的应用程序和桌面，并对其执行操作。可以通过移动设备或台式设备管理会话，从而使最终用户能够随时随地采取行动。对断开连接的会话（例如注销或关闭）采取措施可以优化资源使用并降低能耗。



- 已断开连接的应用程序和桌面显示在“活动管理器”面板上，并以已断开连接的图标表示。
- 已断开连接的应用程序分组在相应的会话下，会话由已断开连接的图标表示。



通过单击省略号按钮，最终用户可以在已断开连接的桌面上执行以下操作：

- 注销：使用此功能从已断开连接的桌面上注销。会话中的所有应用程序都将关闭，所有未保存的文件都将丢失。
- 关机：使用此选项关闭已断开连接的桌面。
- 关机：如果出现技术问题，使用此选项强制关闭已断开连接的台式机的电源。
- 重新启动：使用此选项关闭并重新启动已断开连接的桌面。

活动管理器上断开连接的会话的行为如下所示。

- 如果您通过浏览器登录到 Citrix Workspace 并断开本地会话的连接，则会话将首先显示在“在此设备上”下。

但是，关闭并重新打开“活动管理器”后，断开连接的会话将移至“远程运行”下。

- 如果您通过本机设备登录 Citrix Workspace 应用程序并断开本地会话，则断开连接的会话将从列表中消失。但是，一旦您关闭并再次重新打开“活动管理器”，则断开连接的会话将移至“远程运行”下方。

使用 Citrix Workspace 交付 DaaS、Virtual Apps and Desktops

November 26, 2023

Citrix Workspace 是一项多租户云服务，它取代了 StoreFront，后者是聚合 Citrix DaaS 应用程序和桌面的单租户本地应用商店。Citrix Workspace 平台是一个云组件，可通过 Citrix Workspace 提供远程工作、可扩展性和自定义所需的工具、服务和功能。

使用 Citrix Workspace 聚合 DaaS 时，您可以使用不同的选项。您选择的选项取决于：

- 无论您是想完全迁移到云还是采用混合解决方案。
- 是否计划允许外部访问 DaaS。

完全迁移到云端

您可以将本地配置迁移到云中，从而允许订阅者通过 Workspace 访问 DaaS，方法是将您的 IT 托管基础设施迁移到 Citrix 托管的环境中。完全迁移到云意味着需要管理的组件更少。

Citrix 建议您使用 自动配置工具 来简化从一个或多个本地站点到云服务的迁移过程。此过程涉及的主要步骤包括以下内容：

1. 确保满足 迁移配置的先决条件。
2. 导出您的本地配置。有关此过程的信息，请访问导出 Citrix Virtual Apps and Desktops 本地配置。
3. 将您的配置导入到云中。有关此过程的信息，请访问 将配置导入到 Citrix DaaS

有关自动配置的更多信息，请访问 迁移到云 和 Tech Zone 部署指南。

混合解决方案的站点聚合

您可以使用现有的本地 Virtual Apps and Desktops 部署过渡到 Citrix Workspace。此过程称为站点聚合，涉及用 Citrix 管理的基础架构替换您的 IT 管理基础架构。

您可以选择站点聚合来缓慢过渡到 Workspace，或者如果您想要一个在云中托管部分（但不是全部）组件的混合解决方案。混合模式允许您与本地资源一起管理云容量，并提供统一的最终用户体验，而无需完全迁移到云。

在通过站点聚合从 StoreFront 转换到 Workspace 之前，必须在您的资源位置安装 Active Directory (AD) 配置和 Cloud Connector。

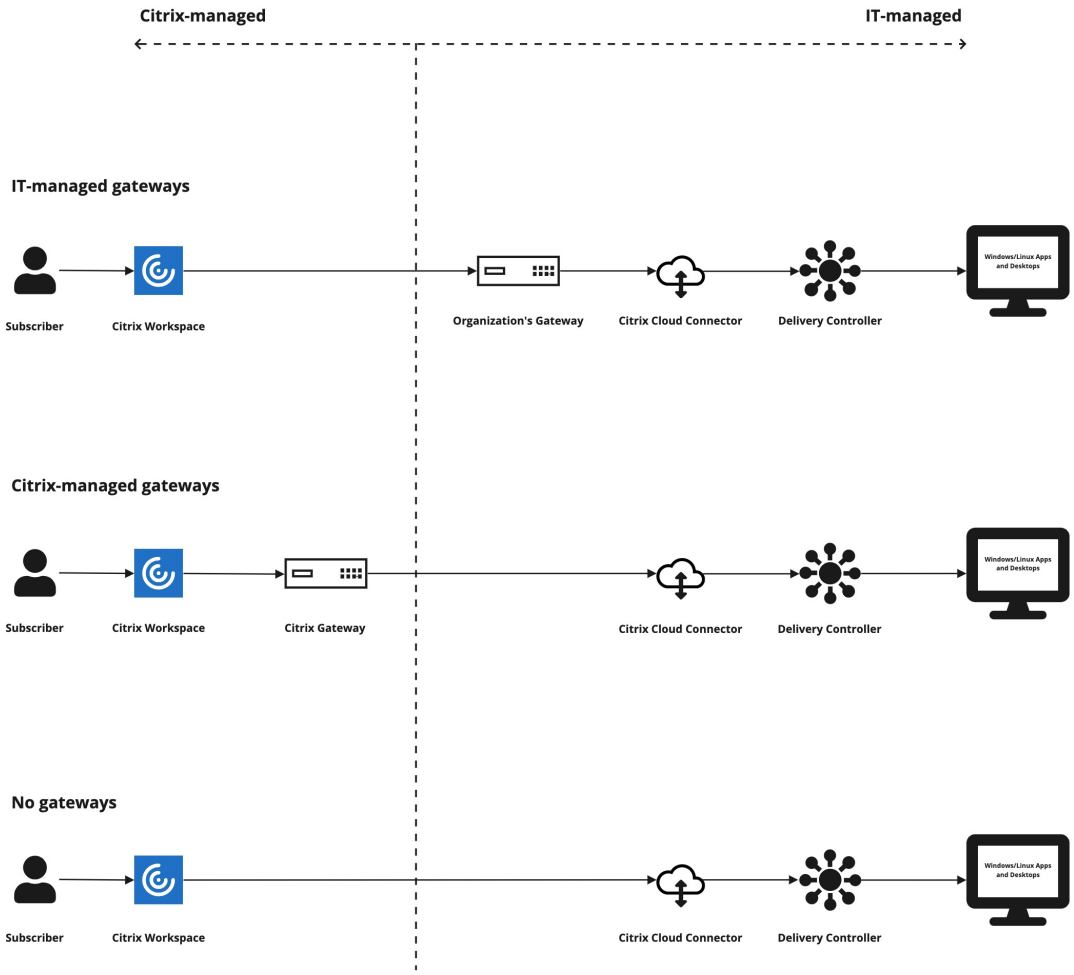
站点聚合涉及三个主要步骤：

1. 探索站点。站点由构成生产部署的组件组成。对于不同的位置和分支机构，您可能有不同的站点。
2. 验证 **Active Directory (AD)** 连接。订阅者必须使用 AD 向 Citrix Workspace 进行身份验证。通过检测安装了 Cloud Connector 的 AD 域，确保订阅者可以进行身份验证。
3. 选择部署类型。此步骤有三种连接选项：
    - IT 管理的网关
    - Citrix 管理的网关
    - 没有网关

有关更多信息，请参阅 连接选项。

连接选项

以下三个选项提供通过 Citrix Workspace 访问 DaaS 的权限，专为不同的业务需求而设计。



连接选项	场景
传统（由 **IT** 管理的）网关	如果您想使用自己的网关与 DaaS 进行外部连接，请选择此选项。这使您能够充分利用当前对本地网关的投资。
Citrix 管理的网关	如果要使用 **Citrix Gateway** 服务 与虚拟应用程序和桌面的外部连接，请选择此选项。客户端和 VDA 之间的 HDX 连接通过 **Citrix Gateway** 服务进行代理。
无网关（仅限内部）	如果您希望订阅者 仅 使用公司网络内的客户端启动 DaaS，请选择此选项。如果选择此选项，订阅者将无法通过外部访问 DaaS。

有关站点聚合过程和所涉及步骤的更多信息，请访问 聚合工作区中的本地虚拟应用程序和桌面。

配置工作区弹性和优化

有关通过 Citrix Workspace 提高 DaaS 效率和可用性的信息，请访问在 Citrix Workspace 中优化 DaaS。Citrix 提供了有关如何执行以下操作的说明：

- 使用直接工作负载连接优化连接。
- 确保停机期间的服务连续性，实现离线弹性。
- 使用 Citrix 联合身份验证服务 (FAS) 配置虚拟应用程序和桌面的单点登录 (SSO)。

配置对工作区的访问权限

November 26, 2023

Citrix 建议使用最新版本的 Citrix Workspace 应用程序访问工作区。Citrix Workspace 应用程序取代了 Citrix Receiver。您也可以使用最新版本的 Microsoft Edge、Google Chrome、Mozilla Firefox 或带有 Workspace URL 的 Apple Safari 访问 Workspace。

本文总结了配置和使用所涉及的步骤：

- 工作 区 URL
- Citrix Workspace 应用程序（以前是 Citrix Receiver）。
- Citrix Gateway 或用于外部连接的 Citrix Gateway 服务。
- 用于对 工作区进行身份验证的身份提供商。

概述

订阅者可以通过带有工作区 URL 的浏览器或通过其设备上安装的 Citrix Workspace 应用程序访问 Citrix Workspace。

工作区 URL 是可自定义的，默认情况下处于启用状态。有关编辑工作区 URL 的说明，请参阅本文中的 工作区 URL 。

Citrix Workspace 应用程序取代 Citrix Receiver 成为本机安装的应用程序，提供对 Workspace 用户界面 (UI) 的访问权限。有关 Citrix Workspace 应用程序和从 Citrix Receiver 过渡的信息，请参阅本文中的 Citrix Workspace 应用程序（以前称为 Citrix Receiver

如果您使用 Citrix Gateway 或 Citrix Gateway 服务配置外部连接，则远程订阅者可以获得对其工作区的外部访问权限。有关启用远程访问工作区的信息，请参阅本文中的 外部连接 。

或者，仅用于内部连接，您可以单独使用 Citrix Workspace 或在本地托管 StoreFront。对于内部连接，端点必须直接连接到 Virtual Delivery Agent (VDA) 的 IP 地址。

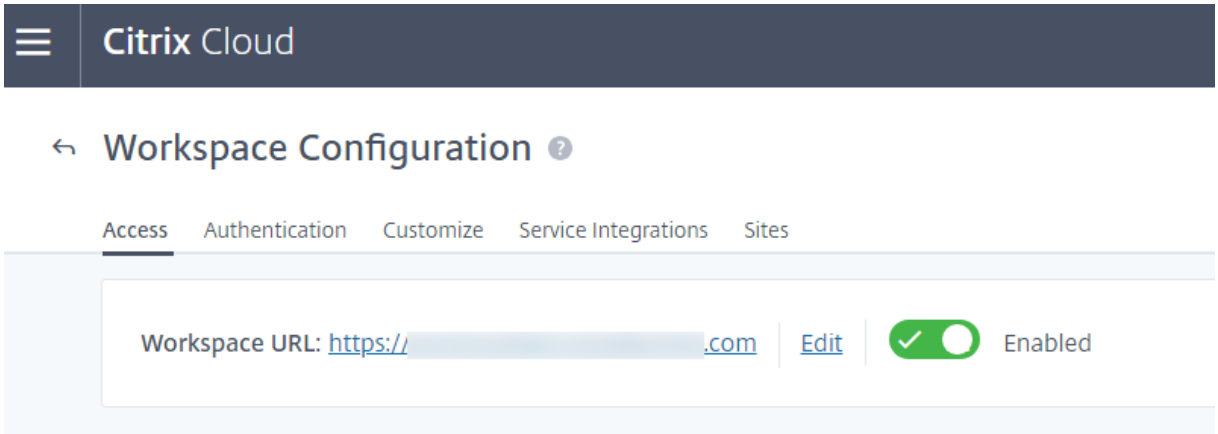
Citrix Workspace 支持越来越多的身份提供商，您可以将其连接到 Citrix Cloud，然后在 **Workspace** 配置中启用，以对工作区的订阅者进行身份验证。有关为 Workspace 订阅者配置 身份验证的信息，请参阅本文中的工作区 身份验证。

Citrix Workspace 还支持以下身份验证选项：

- 令牌是使用 Active Directory 登录工作区时进行身份验证的第二个因素。有关为工作区设置多重身份验证 (MFA) 的更多信息，请参阅 双重身份验证。
- Citrix 联合身份验证服务 (FAS) 可在 Citrix Workspace 中为 DaaS 提供单点登录 (SSO)。有关使用 FAS 设置 SSO 的更多信息，请参阅使用 Citrix 联合身份验证服务为 Workspace 启用单点登录。

Workspace URL

Workspace URL 已准备就绪，可在 **Citrix Cloud > Workspace** 配置 **>** 访问中找到，您可以在其中启用、编辑和禁用 Workspace URL。



自定义工作区 **URL**

工作区 URL 的第一部分是可自定义的。例如，您可以将 URL 从更改 `https://example.cloud.com` 为 `https://newexample.cloud.com`。

只有启用工作区 URL 后，才能更改它。如果 URL 已禁用，则必须先将其重新启用。

要启用 Workspace URL，请导航到“**Workspace** 配置”**>**“访问”，然后选择开关以启用它。重新启用工作区 URL 可能需要 10 分钟才能生效。

Workspace URL 的第一部分代表使用 Citrix Cloud 帐户的组织，并且必须遵守 Cloud Software Group 最终用户协议。滥用第三方知识产权（包括商标）可能会导致 URL 被撤销和重新分配或暂停 Citrix Cloud 帐户。

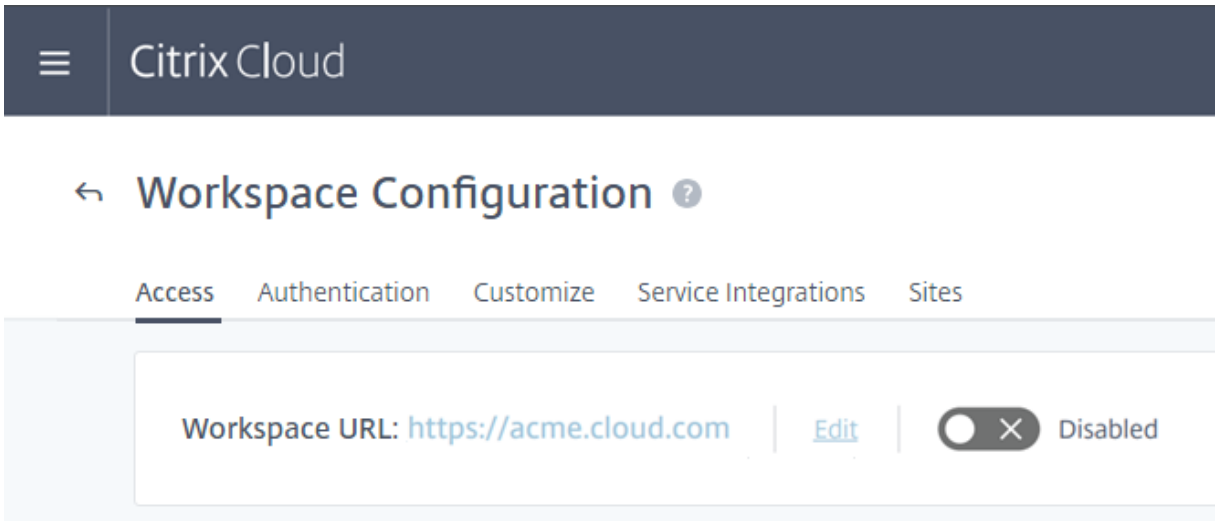
要自定义 URL，请转到 **Workspace** 配置 **>** 访问，然后选择编辑。URL 的可自定义部分：

- 长度必须介于 6 到 63 个字符之间。如果要将 URL 的可自定义部分更改为少于 6 个字符，请在 Citrix Cloud 中打开票证。
- 必须仅由字母和数字组成。
- 不能包含 Unicode 字符。

重命名 URL 时，旧的 URL 会立即被删除，不再可用。告诉订阅者新 URL 是什么，然后手动更新所有本地 Citrix Workspace 应用程序以使用新 URL。

禁用 **Workspace URL**

您可以禁用工作区 URL 以防止用户通过 Citrix Workspace 进行身份验证。例如，您可能希望订阅者使用本地 StoreFront URL 访问资源，或者您可能希望在维护期间阻止访问。



禁用工作区 URL 可能需要 10 分钟才能生效。

禁用工作区 URL 会产生以下影响：

- 所有服务集成均已禁用。订阅者无法从 Citrix Workspace 中的服务访问数据和应用程序。

- 您无法自定义 Workspace URL。必须先重新启用 URL，然后才能对其进行更改。
- 任何访问该 URL 的人都会在其浏览器中收到一条消息，指出找不到工作区或无法加载资源。

Citrix Workspace 应用程序（以前称为 Citrix Receiver

> 重要：
>
> Citrix Receiver 已达到生命周期终止 (EoL)，不再受支持。如果继续使用 Citrix Receiver，则技术支持仅限于生命周期里程碑和定义中描述的选项。有关 Citrix Receiver 按平台划分的 EoL 里程碑的信息，请参阅 Citrix Workspace 应用程序和 Citrix Receiver 的生命周期里程碑

Citrix Workspace 应用程序是本机安装的应用程序，它取代了 Citrix Receiver 访问工作区。

Citrix Workspace 应用程序支持的身份验证方法

下表显示了 Citrix Workspace 应用程序支持的身份验证方法。该表包括与 Citrix Workspace 应用程序所取代的特定版本的 Citrix Receiver 相关的身份验证方法。

Citrix Workspace 应用程序	Active Directory 身份验证	Active Directory 加令牌身份验证	Azure Active Directory 身份验证
适用于 Windows 的 Citrix Workspace	是	是	是（Workspace 应用程序；仅限 Receiver 4.9 LTSR CU2 及更高版本；仅限 Receiver 4.11 CR 及更高版本）
适用于 Linux 的 Citrix Workspace	是	是	是（Workspace 应用程序；仅限 Receiver 13.8 及更高版本）
适用于 Mac 的 Citrix Workspace	是	是	是
适用于 iOS 的 Citrix Workspace	是	是	是
适用于 Android 的 Citrix Workspace	是	是	是（Workspace 应用程序；仅限 Receiver 3.13 及更高版本）

有关各平台的 Citrix Workspace 应用程序中支持的功能的详细信息，请参阅 Citrix Workspace 应用程序功能列表。

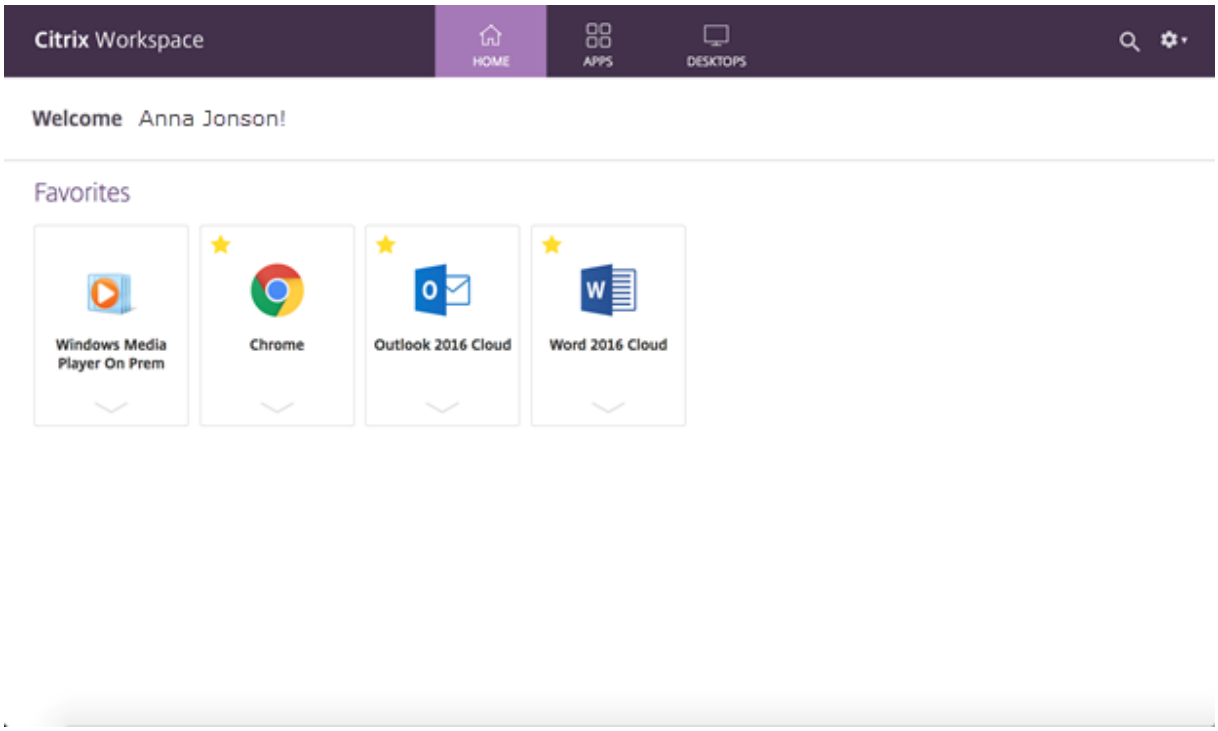
有关 Citrix Receiver 支持 TLS 和 SHA2 的概述，请参阅 CTX23226 支持文章。

从 **Citrix Receiver** 过渡到 **Citrix Workspace** 应用程序

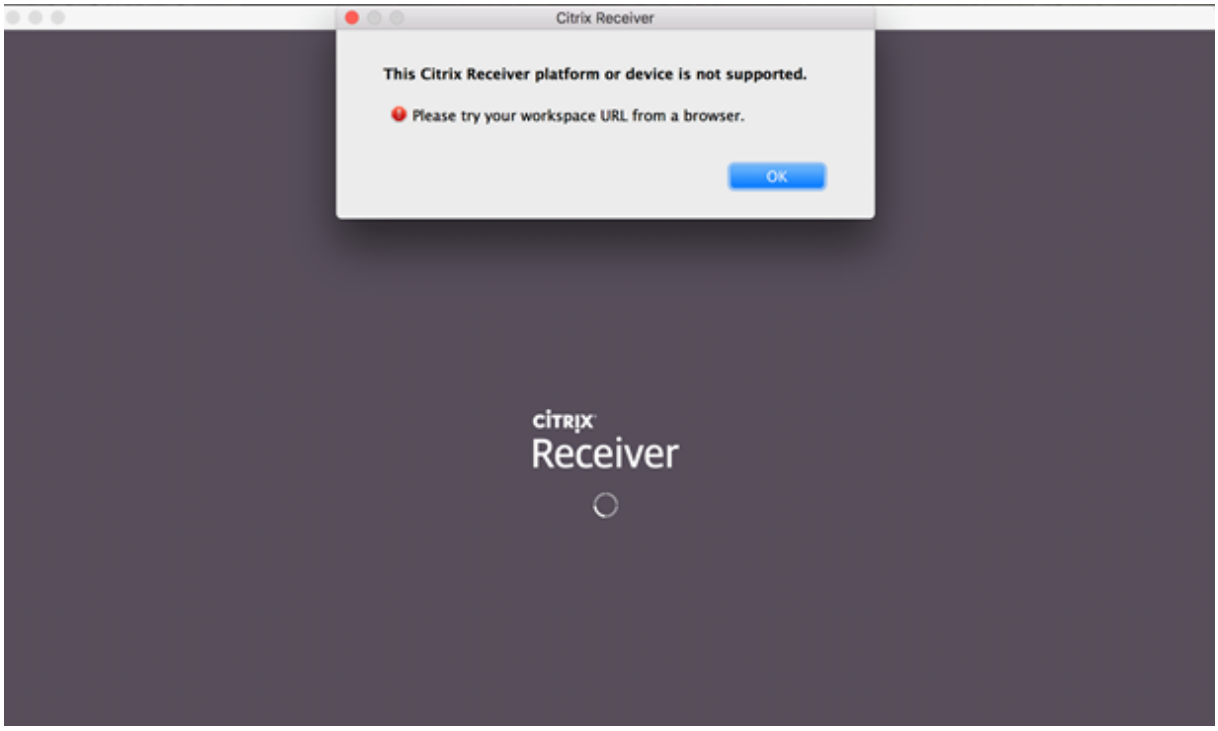
Citrix Workspace 应用程序取代并扩展了 Citrix Receiver 的功能

Citrix Workspace 应用程序通过单点登录 (SSO) 体验为订阅者提供 SaaS、Web 和虚拟应用程序的访问权限。有关工作区订阅者单点登录的信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录。

Citrix Receiver 不支持此访问控制功能。因此，在启用了相同的服务和访问控制的情况下，Citrix Receiver 用户仍然可以看到紫色用户界面，但没有 Web 和 SaaS 应用程序。此外，Citrix Receiver 不支持 文件，订阅者无法通过这种方式访问它们。



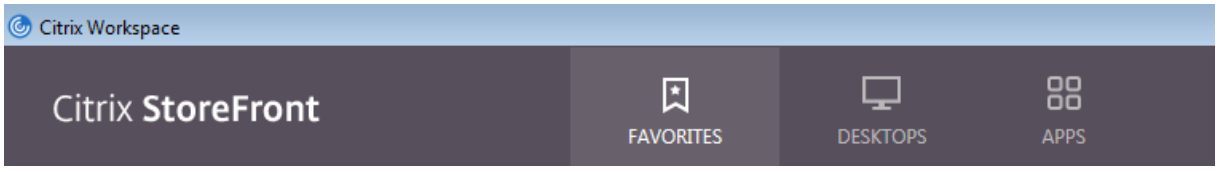
Azure Active Directory (AAD) 也与 Citrix Receiver 不兼容。如果订阅者在启用 AAD 作为身份验证方法时尝试使用 Citrix Receiver 访问 Workspace，他们会看到一条消息，指出该设备不受支持。升级到 Citrix Workspace 应用程序后，他们就可以访问自己的工作区。



升级到 Citrix Workspace 应用程序（或使用 Web 浏览器）的客户将看到新的用户界面。有关此 UI 的订阅者体验的更多信息，请访问管理您的 Workspace 体验。

除了新的用户界面外，Citrix Workspace 应用程序还允许订阅者使用您已启用的所有新功能。订阅者可以通过 Citrix Gateway 服务访问 文件、查看 DaaS 以及访问 Web 和 SaaS 应用程序。

如果您有 StoreFront（本地）部署，从 Citrix Receiver 升级到 Citrix Workspace 应用程序只会更改图标以打开 Citrix Workspace



> 注意：
>
> 使用 Citrix Workspace 应用程序或从 Web 浏览器访问 Workspace 时，Citrix Cloud Government 用户会继续看到其紫色 UI。

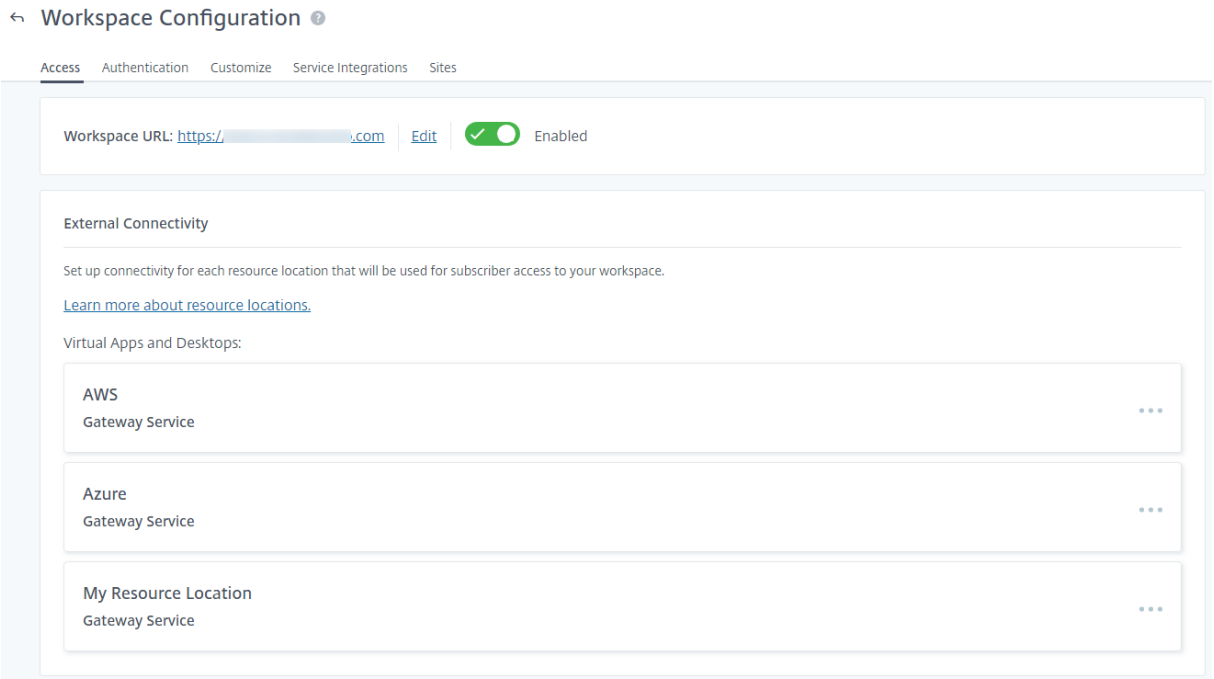
外部连接

通过将 Citrix Gateway 或 Citrix Gateway 服务添加到资源位置，为远程订阅者提供安全访问。

Citrix 支持以下外部连接选项：

- Citrix 托管 Citrix Gateway 和 Citrix ADC
- 您在本地托管 Citrix Gateway 和 Citrix ADC

您可以通过 **Workspace** 配置 **>** 访问 **>** 外部连接或 **Citrix Cloud >** 资源位置添加 Citrix Gateway。



> 注意：
>
> **Workspace** 配置 **>** 访问页面的外部连接部分在 Citrix Virtual Apps Essentials 中不可用。Citrix Virtual Apps Essentials 服务使用 Citrix Gateway 服务，该服务无需额外配置。

工作区身份验证

为订阅者配置工作区身份验证分为两个步骤：

1. 在身份 和访问管理中定义一个或多个身份提供商。有关说明，请访问 身份和访问管理。
2. 在 Workspace 配置中选择一个已 配置的身份提供商作为订阅者登录其工作区时使用的身份验证方法。有关说明，请访问 选择或更改身份验证方法。

在“身份 和访问管理”中配置更多身份 提供程序后，您可以在 **Workspace** 配置 中选择更多选项，以了解订阅者如何登录其工作区。

支持对订阅者进行身份验证的身份提供商

订阅者可以使用以下方法之一对其工作区进行身份验证：

- Active Directory
- Active Directory 加令牌
- Azure Active Directory

- Citrix Gateway
- Okta
- SAML 2.0
- Google

有关支持的工作区订阅者身份验证方法的更多信息，请访问 安全工作区。

Active Directory (AD) 要求您在本地 AD 域中至少安装两个 Citrix Cloud 连接器。有关 Citrix Cloud Connector 的信息，请访问 Citrix Cloud Connector。

AD plus 令牌是用于对工作区订阅者进行身份验证的默认身份提供程序。订阅者使用任何遵循 基于时间的一次性密码 (TOTP) 标准的应用程序（例如 Citrix SSO）生成令牌作为身份验证的第二要素。有关设置基于令牌的双重身份验证的信息，请参阅 双重身份验证。

更改身份提供商

在工作区 配置中，您可以选择身份提供程序作为 **Citrix Workspace** 的主要身份验证方法。您选择的身份提供商必须首先在 身份和访问管理中进行配置。在 **Workspace** 配置 中更改身份提供者不会影响您在身份 和访问管理中配置的身份提供商。

在身份 和访问管理中配置身份 提供程序不会更改登录 Citrix Workspace 的主要身份验证方法。要 更改 登录 Citrix Workspace 的主要身份验证方法，您必须：

1. 在身份 和访问管理中配置新的身份提供程序。
2. 在 **Workspace** 配置中更改身份提供者。

您可以配置和更改 Citrix Workspace 的主要身份验证方法，而不会破坏生产环境。如果要测试新的身份提供商，可以创建测试 Citrix Cloud 组织，也可以计划在订阅者未使用其工作区时更改 **Workspace** 配置 中的身份验证方法。

SaaS 和 **Web** 应用程序的单点登录 **(SSO)**

Citrix Workspace 通过在订阅者登录其工作区后向辅助资源提供单点登录 (SSO) 来提供无缝体验。Citrix Secure Private Access 与 Citrix Gateway 服务一起提供对 SaaS 和 Web 应用程序的 SSO，作为 Citrix Workspace 的集成组成部分。

除了 SSO 功能外，Citrix Secure Private Access 还允许您设置增强的安全策略、配置上下文访问和收集分析。有关 Citrix Secure Private Access 的更多信息，请访问 Citrix Secure Private Access。

单点登录 **(SSO)** 到 **DaaS**

除了 SaaS 和 Web 应用程序外，Active Directory (AD) 和 AD plus Token 已经在订阅者登录其工作区后为 DaaS 应用程序和桌面提供了 SSO。

如果为订阅者对 Citrix Workspace 的初始身份验证选择其他身份提供商，则还可以安装和配置 Citrix 联合身份验证服务 (FAS)。使用 FAS，订阅者只需输入一次凭据即可访问其 DaaS，就像使用 SaaS 和 Web 应用程序一样。

如果您使用以下身份提供商之一进行 Workspace 身份验证，通常会采用 FAS：

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

> 注意：
>
> 根据配置 Citrix Gateway 的方式，可能不需要 FAS 来进行 DaaS 的 SSO。有关配置 Citrix Gateway 的更多信息，请访问 在本地 Citrix Gateway 上创建 OAuth IdP 策略。

有关 FAS 的更多信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录。

更多信息

- 使用 Citrix 联合身份验证服务为工作区启用单点登录
- 参考体系结构：联合身份验证服务
- 技术洞察：联合身份验证服务

配置自定义域

November 26, 2023

为您的 Workspace 配置自定义域允许您使用自己选择的域来访问您的 Citrix Workspace 存储。然后，您可以使用此域代替分配的 cloud.com 域，以便从 Web 浏览器和 Citrix Workspace 应用程序进行访问。

自定义域无法与其他 Citrix Workspace 客户共享。每个自定义域对于该客户来说都必须是唯一的。确保选择不想分配给其他客户的自定义域，除非您愿意稍后删除该自定义域。

在 Citrix Cloud 中禁用 Workspace URL 不会禁用通过自定义域访问 Citrix Workspace。要在使用自定义域时禁用 Citrix Workspace 访问权限，还要禁用自定义域。

支持的场景

方案	受支持	不支持
身份提供商	AD（+Token）、Azure AD、Citrix Gateway、Okta 和 SAML	Google
资源类型	Virtual Apps and Desktops	SaaS 应用程序
访问方法	浏览器（不包括 Internet Explorer）、适用于 Windows、Mac、Linux 和 iOS 应用程序的 Citrix Workspace 应用程序	-
使用情况	Workspace	Cloud Connector 云管理员控制台

它与当前的自定义 **Workspace URL** 有何不同

如果您已经为客户启用了自定义 Workspace URL，则会显示以下视图。

您可以暂时使用此 URL，然后继续执行本文档中的步骤来加载不同的自定义 Workspace URL。将来会被弃用。

如果您想使用相同的 URL，请移除之前的自定义 Workspace URL 并移除所有 DNS 记录以继续。

必备条件

- 您可以选择新注册的域名，也可以选择已经拥有的域名。域名必须采用子域名格式 (your.company.com)。Citrix 不支持只使用根域 (company.com)。
- Citrix 建议您使用专用域作为访问 Citrix Workspace 的自定义域，以便在必要时可以轻松更改它。
- 自定义域不能包含任何 Citrix 商标。在此处查找 Citrix 商标的完整列表。
- 您选择的域必须在公有 DNS 中配置。您的域配置中包含的任何 CNAME 记录名称和值都必须可由 Citrix 解析。

> 注意：
>
> 不支持专用 DNS 配置。

- 域名的长度不应超过 64 个字符。

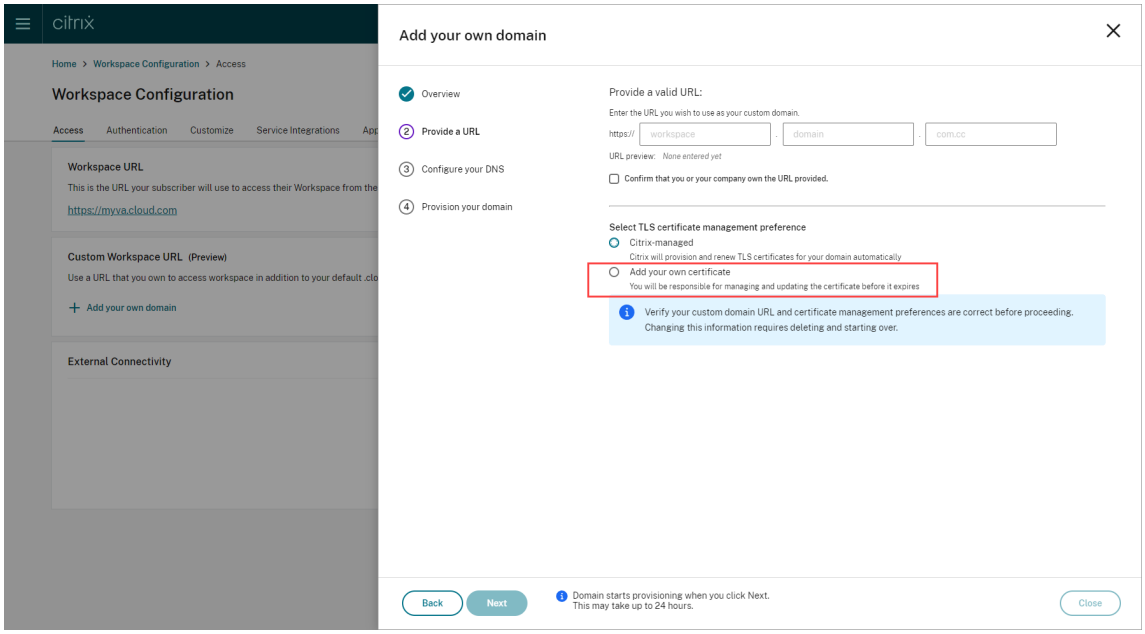
配置您的自定义域

设置自定义域名后，您就无法更改 URL 或证书类型。您只能将其删除。确保您选择的域名尚未在 DNS 中配置。在尝试配置您的自定义域之前，请删除所有现有的 **CNAME** 记录。

如果您使用 SAML 连接到身份提供商，则需要执行额外的步骤才能完成 SAML 配置。有关更多信息，请参阅 SAML。

添加自定义域

1. 登录 Citrix Cloud，网址为 https://citrix.cloud.com。
2. 从 Citrix Cloud 菜单中，选择 **Workspace** 配置，然后选择访问。
3. 在“访问”选项卡的“自定义 **Workspace URL**”下，选择 **+** 添加自己的域。

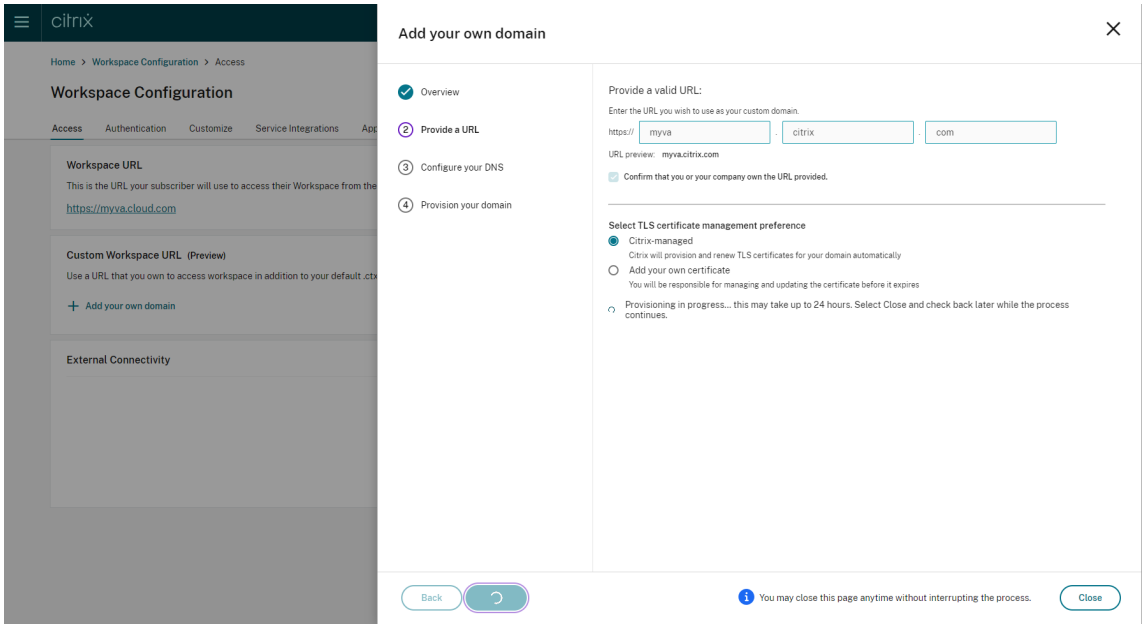


4. 阅读 概览 页面上显示的信息，然后选择 下一步。
5. 在“提供 **URL**”页面中输入您选择的域名。选择“确认您或您的公司拥有所提供的 **URL**”，然后选择您的 TLS 证书管理首选项，确认您拥有指定的域。Citrix 建议采用托管方式，因为证书续订将由您处理。有关更多信息，请参阅提供续订证书。单击下一步。

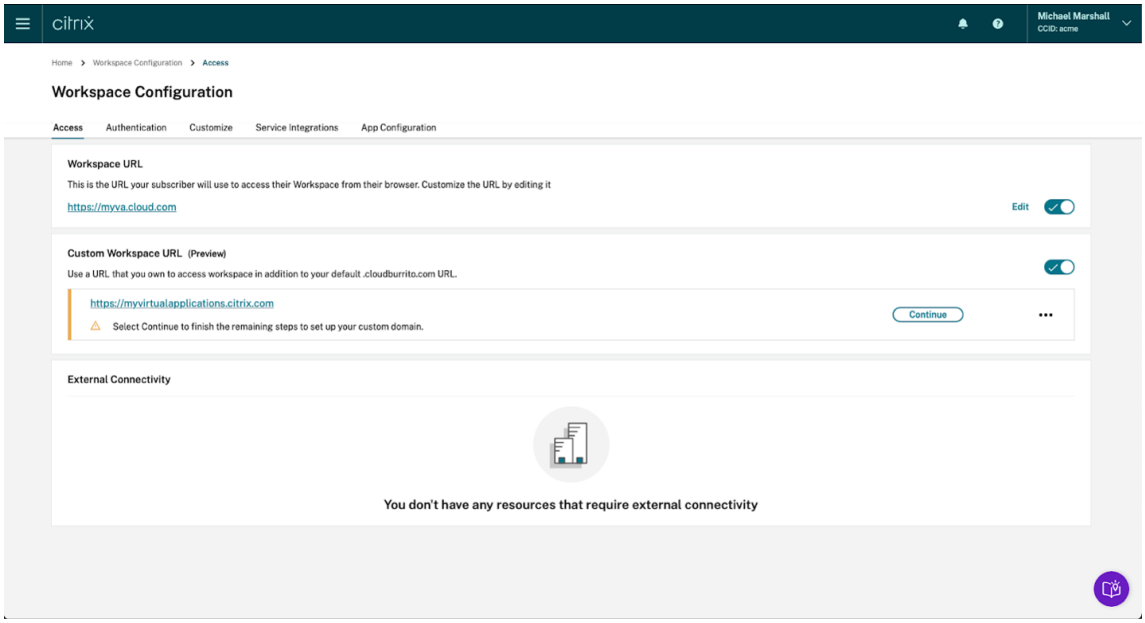
   如果此页面上出现任何警告，请更正突出显示的问题以继续。

   如果您选择提供自己的证书，则说明中还有一个额外的步骤需要完成。

   预配您选择的域需要一些时间。您可以等待页面处于打开状态，也可以在配置进行时将其关闭。



6. 如果您在配置完成时打开“提供 **URL**”页面，“配置您的 **DNS**”页面将自动打开。如果您已关闭页面，请从“访问”选项卡中为您的自定义域选择“继续”按钮。

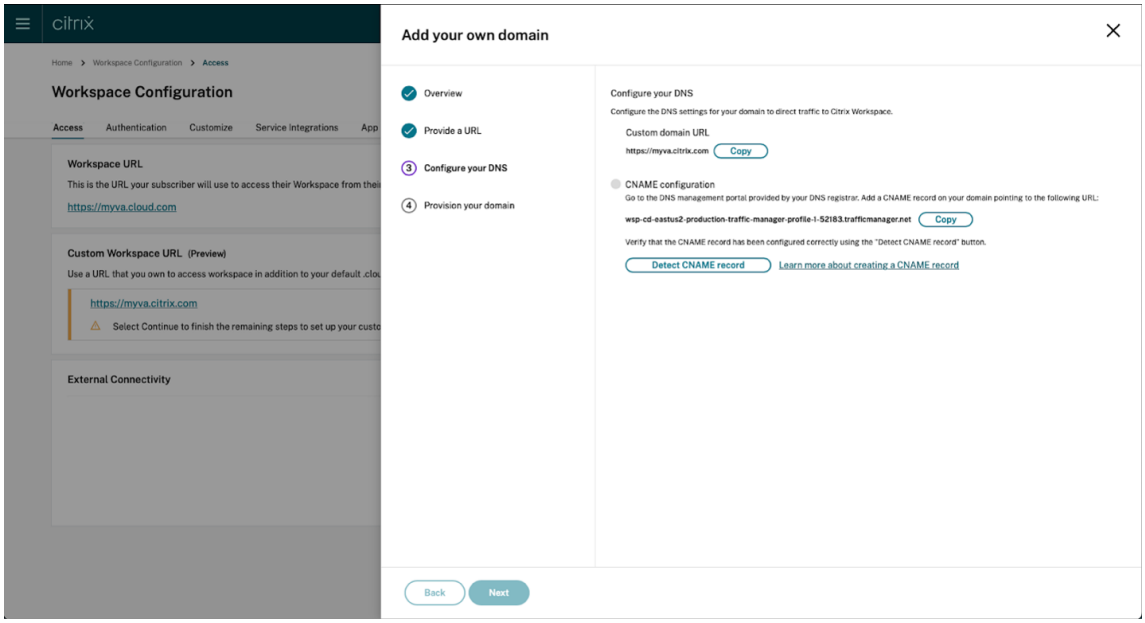


7. 在您的 DNS 注册商提供的管理门户中执行此步骤。为您选择的自定义域添加一个 **CNAME** 记录，该记录指向分配给您的 Azure 流量管理器。

   从“配置您的 **DNS**”页面复制流量管理器的地址。示例中的地址如下所示：

   wsp-cd-eastus2-production-traffic-manager-profile-1-52183.trafficmanager.net

   如果您在 DNS 中配置了任何证书颁发机构授权 (CAA) 记录，请添加一个允许让我们加密为您的域名生成证书的记录。让我们加密是 Citrix 用来为您的自定义域生成证书的证书颁发机构 (CA)。CAA 记录的值必须如下所示：*0 issue “letsencrypt.org”*

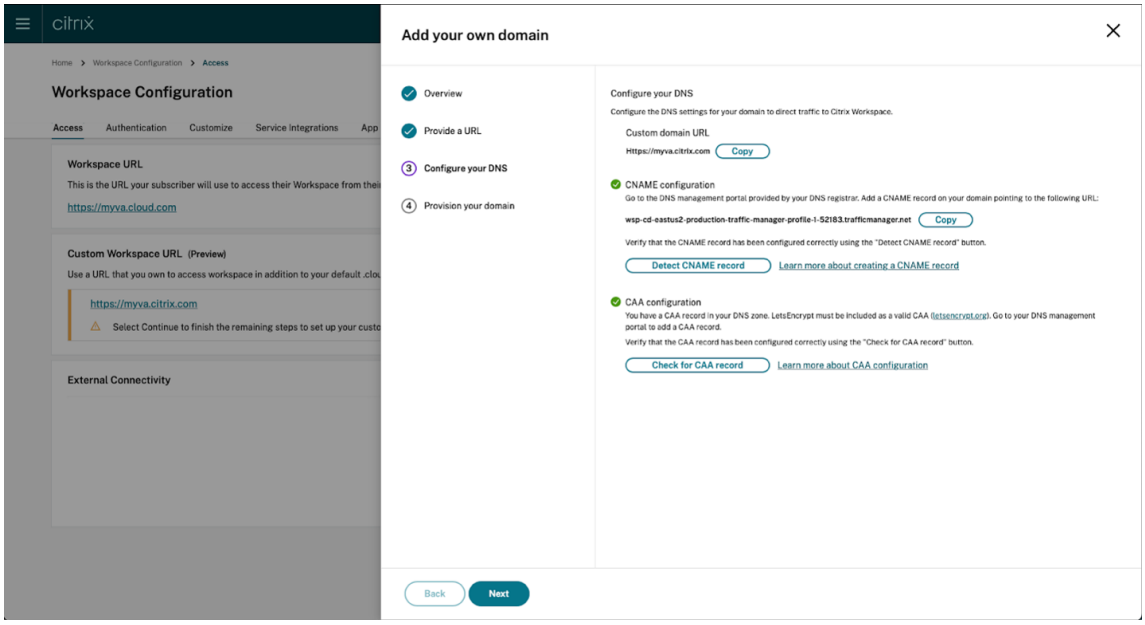


8. 在 DNS 提供商处配置 CNAME 记录后，选择“检测 **CNAME** 记录”以验证您的 DNS 配置是否正确。如果 CNAME 记录配置正确，则 **CNAME** 配置部分旁边会出现绿色勾号。

   如果此页面上出现任何警告，请更正突出显示的问题以继续。

   如果您在 DNS 提供商处配置了任何 CAA 记录，则会出现单独的 **CAA** 配置。选择“检测 **CAA** 记录”以验证您的 DNS 配置是否正确。如果您的 CAA 记录配置正确，则 **CAA** 配置 部分旁边会出现绿色勾号。

   验证您的 DNS 配置后，单击“下一步”。

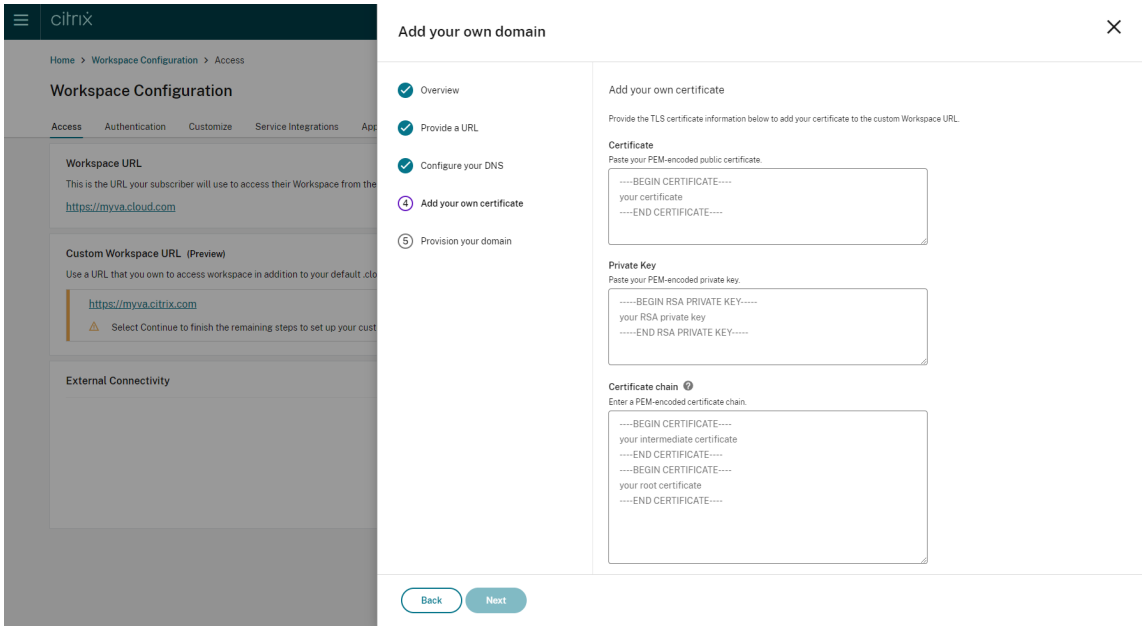


9. 这是一个可选步骤。如果您选择添加自己的证书，请在添加自己的证书页面上填写所需信息。

   如果此页面上出现任何警告，请更正突出显示的问题以继续。

确保证书满足以下条件。

- 它应该采用 PEM 编码。
- 它应至少在接下来的 30 天内保持有效。
- 它应专门用于自定义 Workspace URL，不接受通配符证书。
- 证书的公用名称应与自定义域相匹配。
- 证书上的 SAN 应用于自定义域，不允许使用任何其他 SAN。
- 证书的有效期不应超过 10 年。



> 注意：
>
> Citrix 建议您使用使用安全的加密哈希函数（SHA 256 或更高版本）的证书。您有责任续订证书。如果您的证书已过期或即将过期，请参阅提供续订证书部分。

10. 这是可选步骤。如果您使用 SAML 作为身份提供商，请提供相关配置。在“配置 **SAML**”页面上填写所需信息。

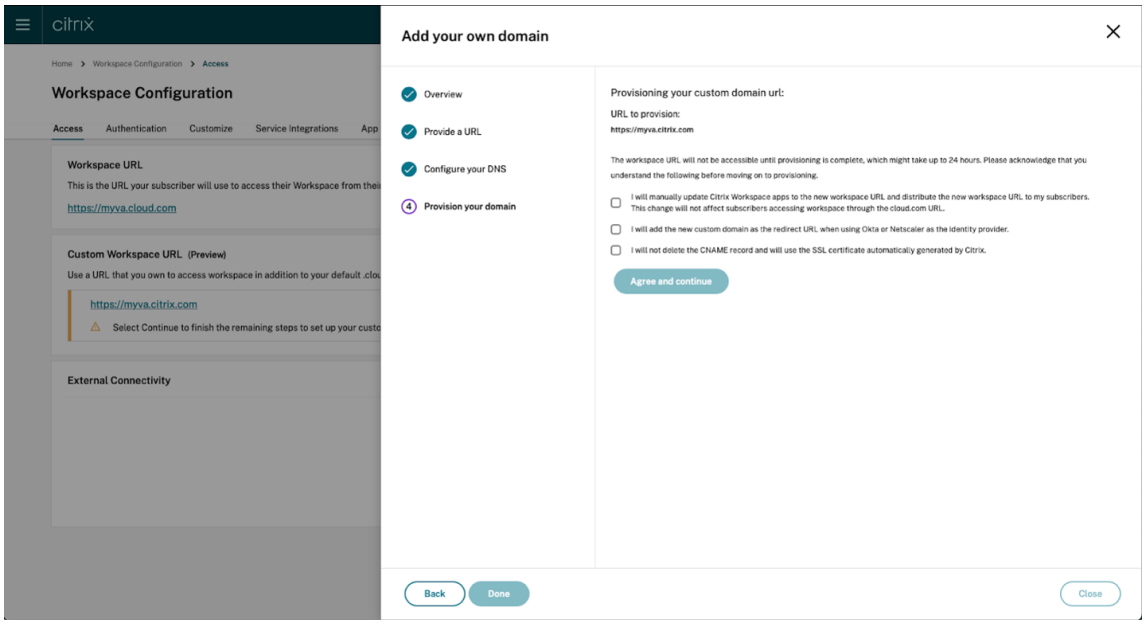
    在身份提供商中配置应用程序时，请使用以下详细信息：

属性	值
受众	`https://saml.cloud.com`
收件人	`https://<your custom domain>/saml/acs`
ACS URL 验证器	`https://<your custom domain>/saml/acs`

属性	值
ACS 消费者 URL	https://<your custom domain>/saml/acs
单一注销 URL	https://<your custom domain>/saml/logout/callback

11. 阅读“提供您的域名”页面上显示的信息，并确认给定的说明。准备好继续时，选择“同意并继续”。

    最后的配置步骤可能需要一些时间才能完成。您可以在操作完成时等待页面处于打开状态，也可以关闭页面。



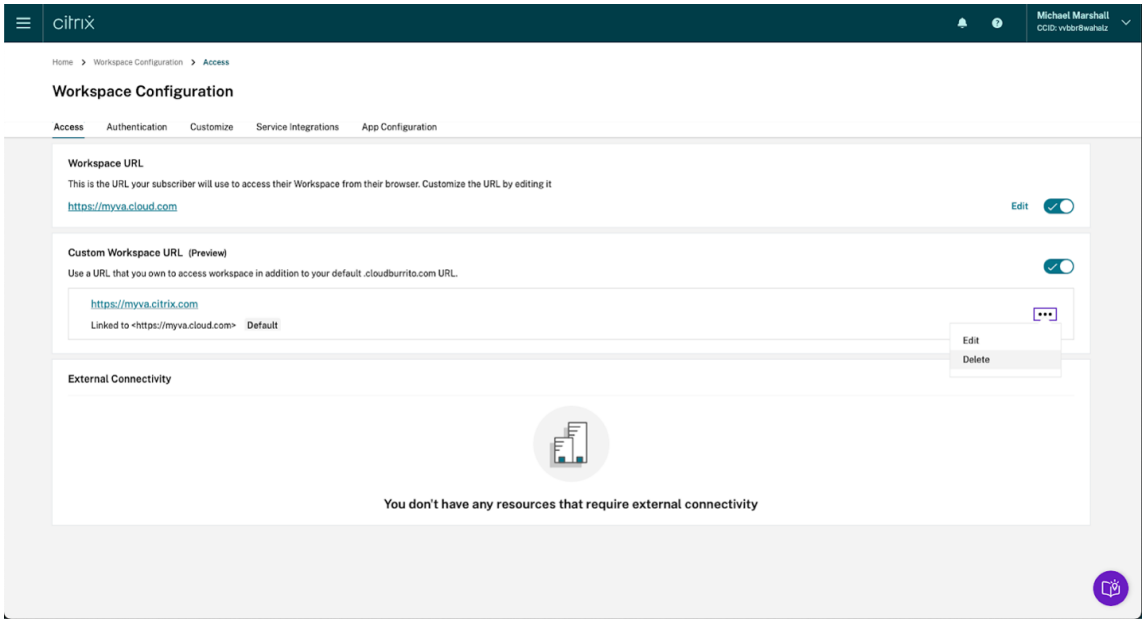
删除自定义域

从客户那里删除自定义域将无法使用自定义域访问 Citrix Workspace。删除自定义域后，您只能使用 cloud.com 地址访问 Citrix Workspace。

删除自定义域名时，请确保从您的 DNS 提供商中删除 CNAME 记录。

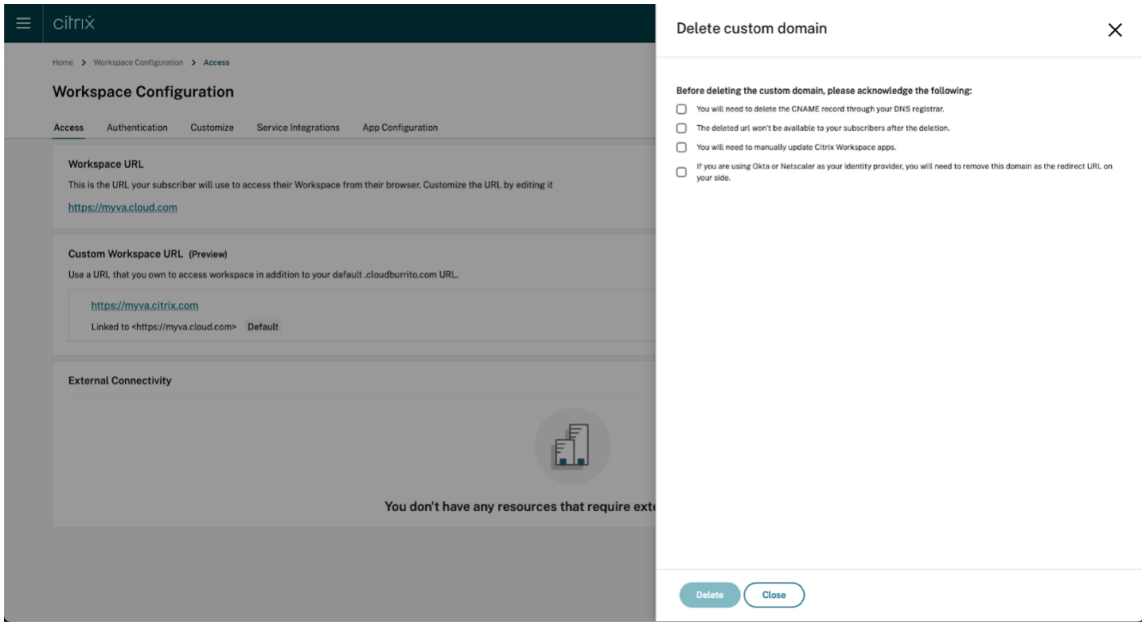
要删除自定义域，

1. 登录 Citrix Cloud，网址为 https://citrix.cloud.com。
2. 从 Citrix Cloud 菜单中，选择 **Workspace** 配置 **>** 访问权限。
3. 展开上下文菜单 **(…)** 在“访问”选项卡上为自定义域，然后选择“删除”。



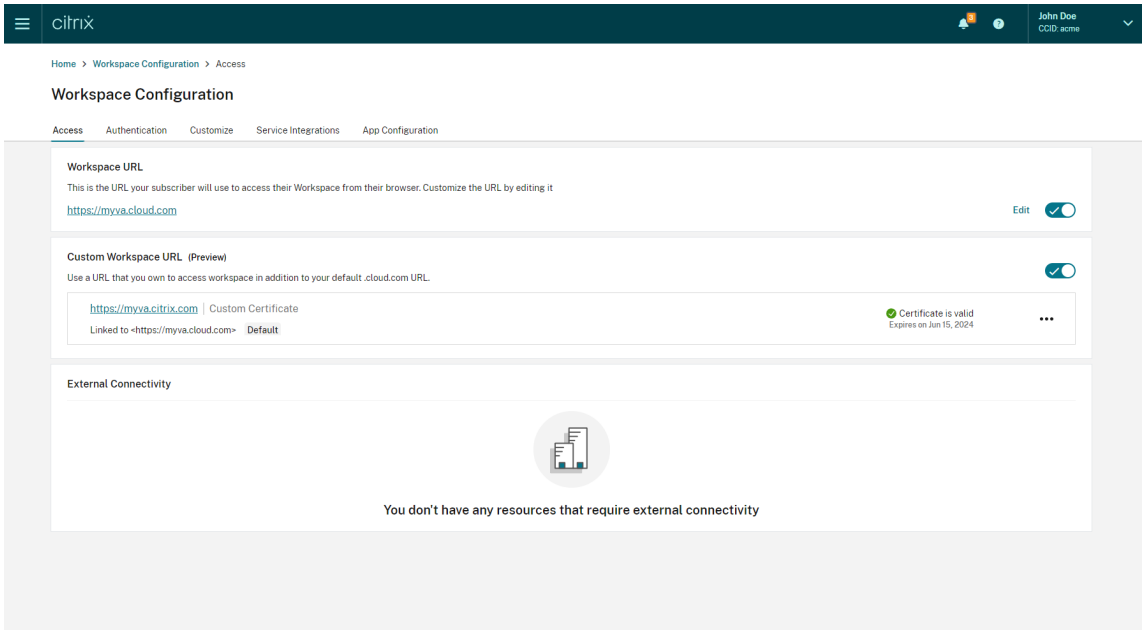
4. 阅读 删除自定义域 页面上显示的信息并确认给定的说明。当您准备好继续时，选择“删除”。

   删除自定义域需要一些时间才能完成。您可以在操作完成时等待页面处于打开状态，也可以关闭页面。

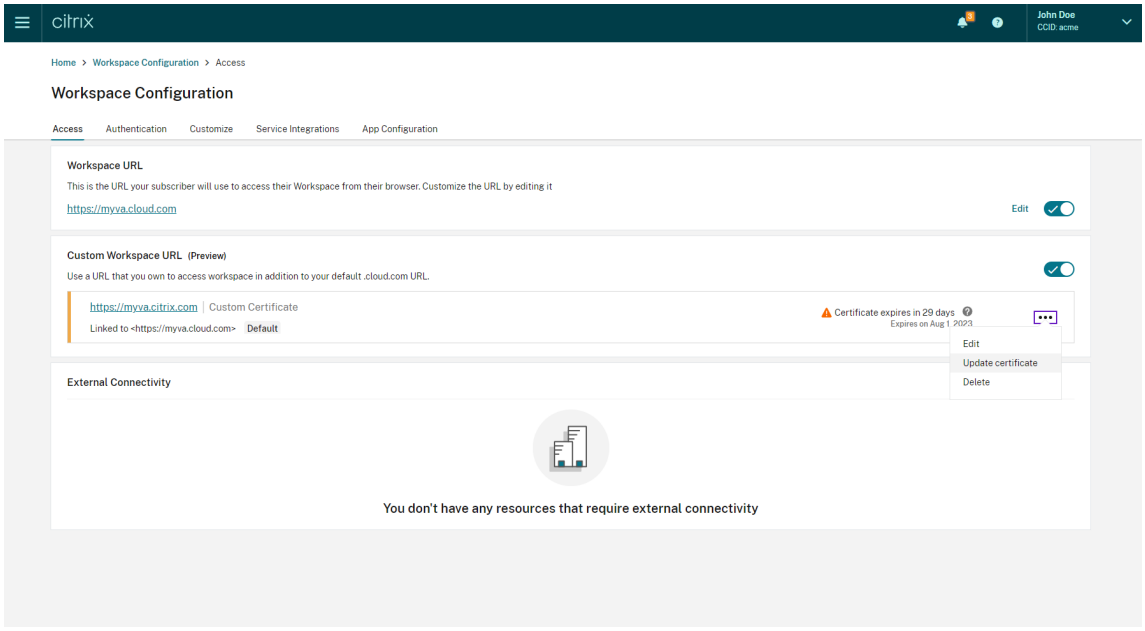


提供续订证书

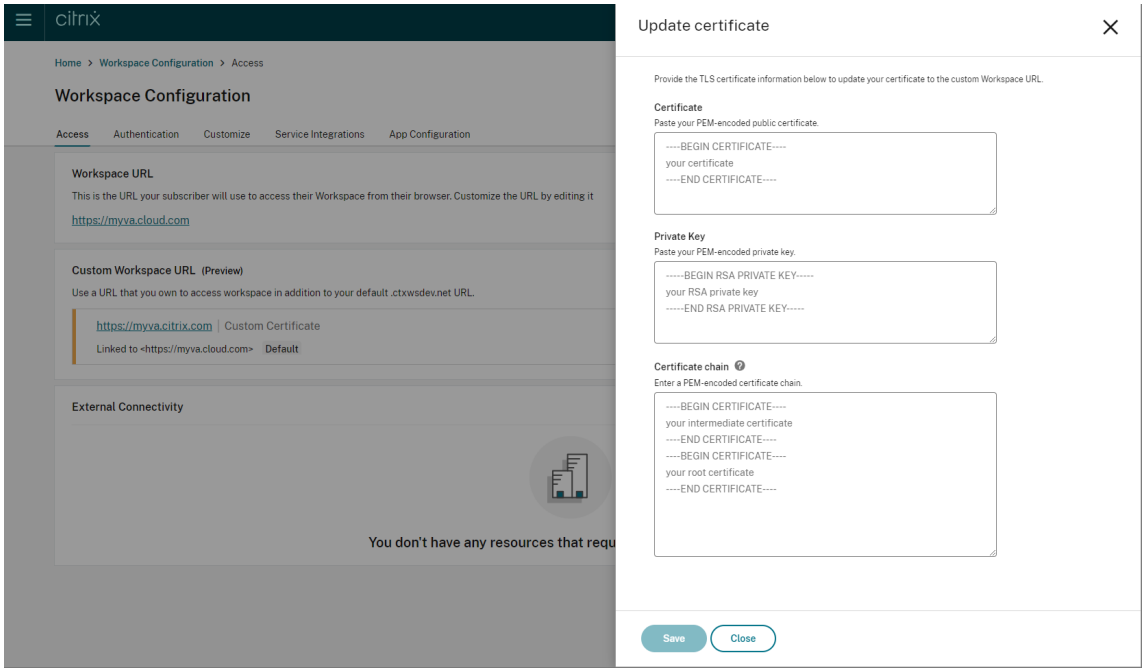
1. 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **Workspace** 配置 > 访问权限。
3. 证书的到期日期将显示在分配给它的自定义域名旁边。



当您的证书将在 30 天或更短时间内到期时，您的自定义域名将显示警告。



4. 在“访问权限”选项卡上展开自定义域的上下文菜单 **(…)** 。选择“更新证书”。



5. 在更新证书页面上输入所需信息，然后保存。

如果此页面上出现任何警告，请更正突出显示的问题以继续。

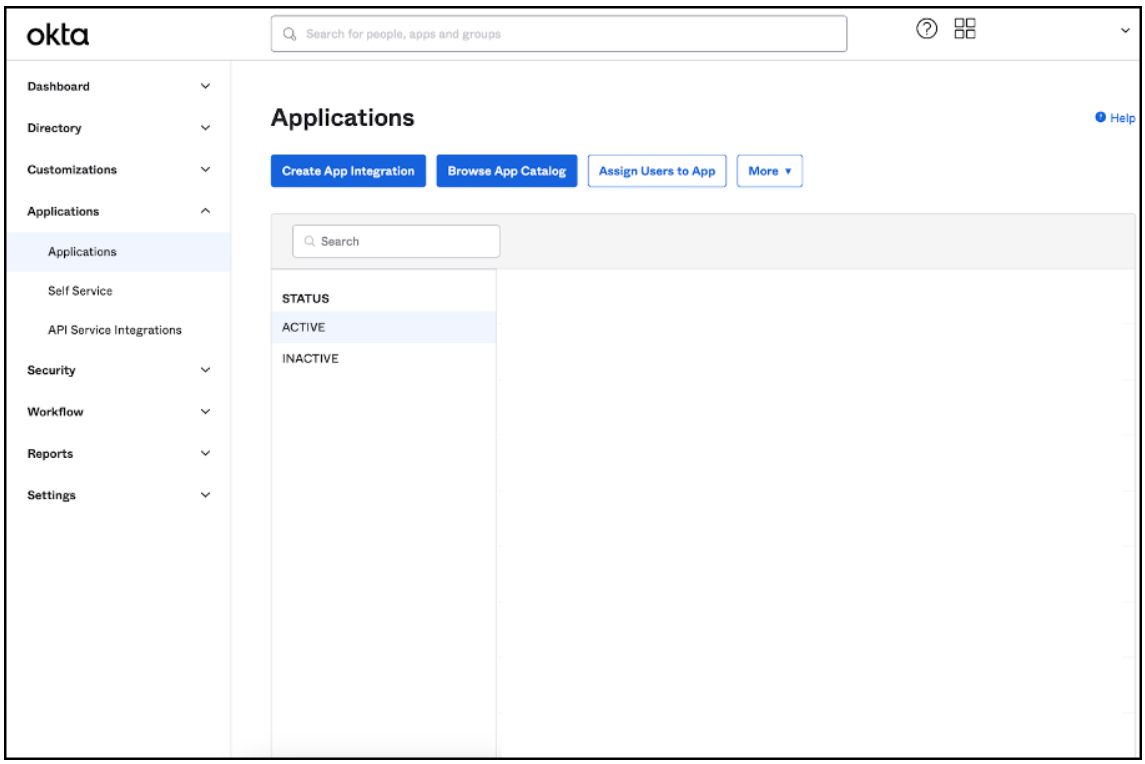
证书必须满足与创建自定义域时相同的要求，可以在此处查看添加自定义域。

配置您的身份提供商

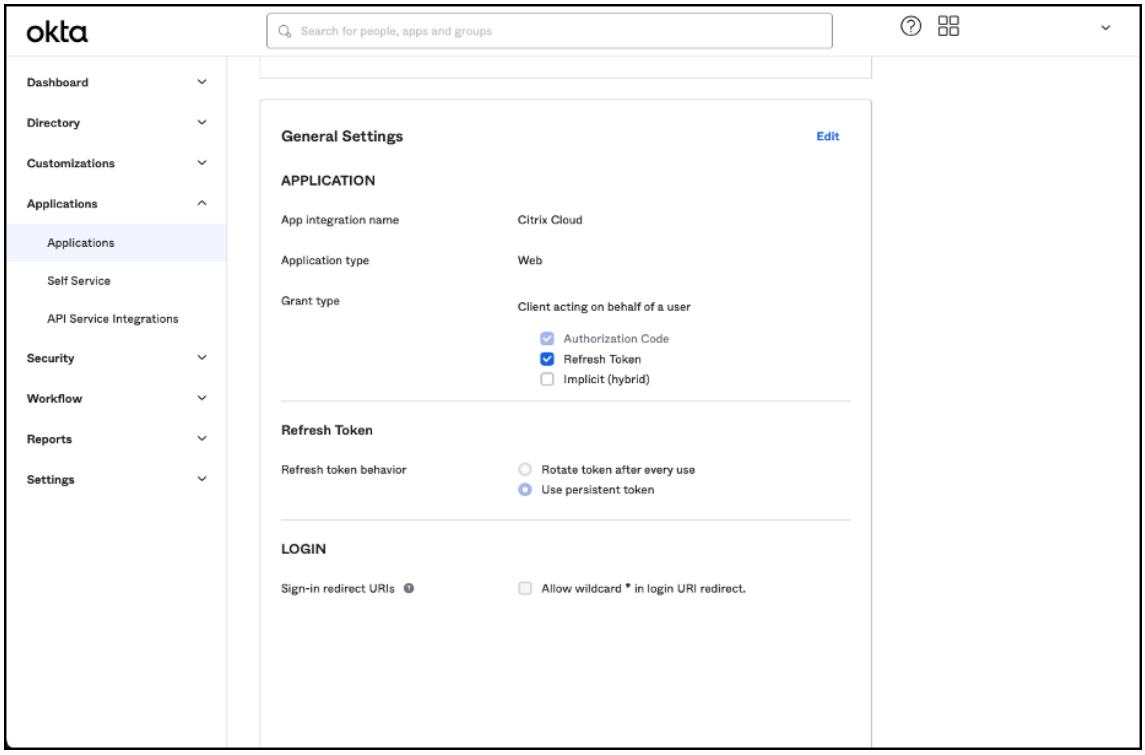
配置 **Okta**

如果您使用 Okta 作为 Citrix Workspace 访问的身份提供商，请执行以下步骤。

1. 登录您的 Okta 实例的管理员门户。此实例包含 Citrix Cloud 使用的应用程序。
2. 展开 应用程序，然后在菜单中选择 应用程序。



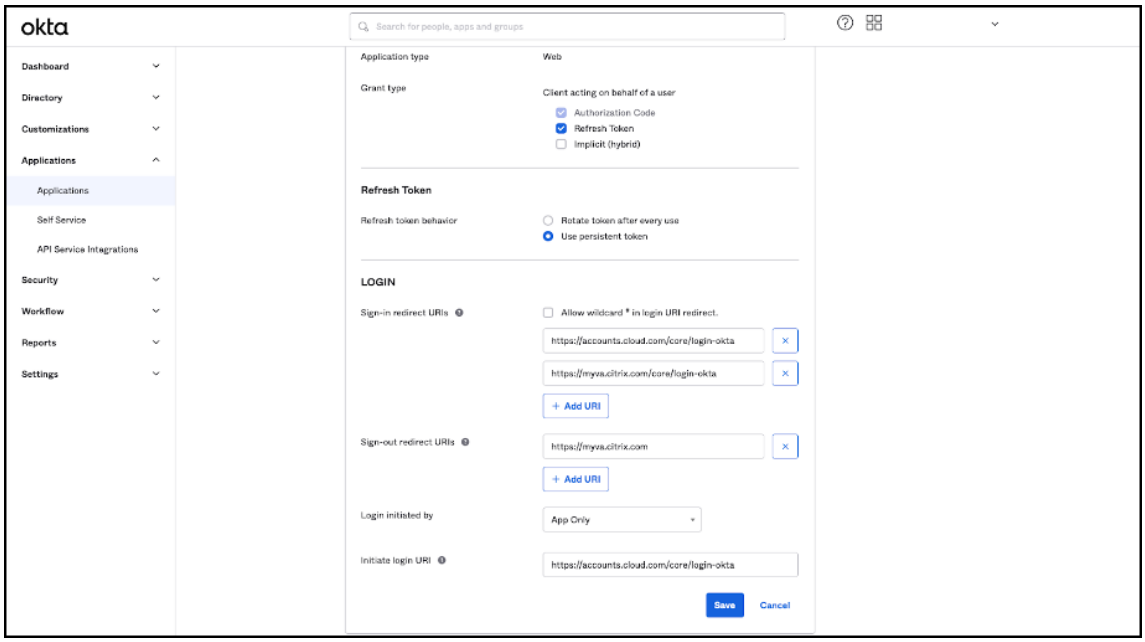
3. 打开链接到 Citrix Cloud 的应用程序。
4. 在“常规设置”部分中选择“编辑”。



5. 在“常规设置”的“登录”部分中，为 登录重定向 **URI** 添加一个新值。添加除任何现有值以外的新值，而不是替

换这些现有值。新值必须采用以下格式：https://your.company.com/core/login-okta

6. 在同一部分中，为注销重定向 **URI** 添加一个新值。添加除任何现有值以外的新值，而不是替换这些现有值。新值必须采用以下格式：https://your.company.com



7. 单击“保存”以存储新配置。

配置 **OAuth** 策略和配置文件

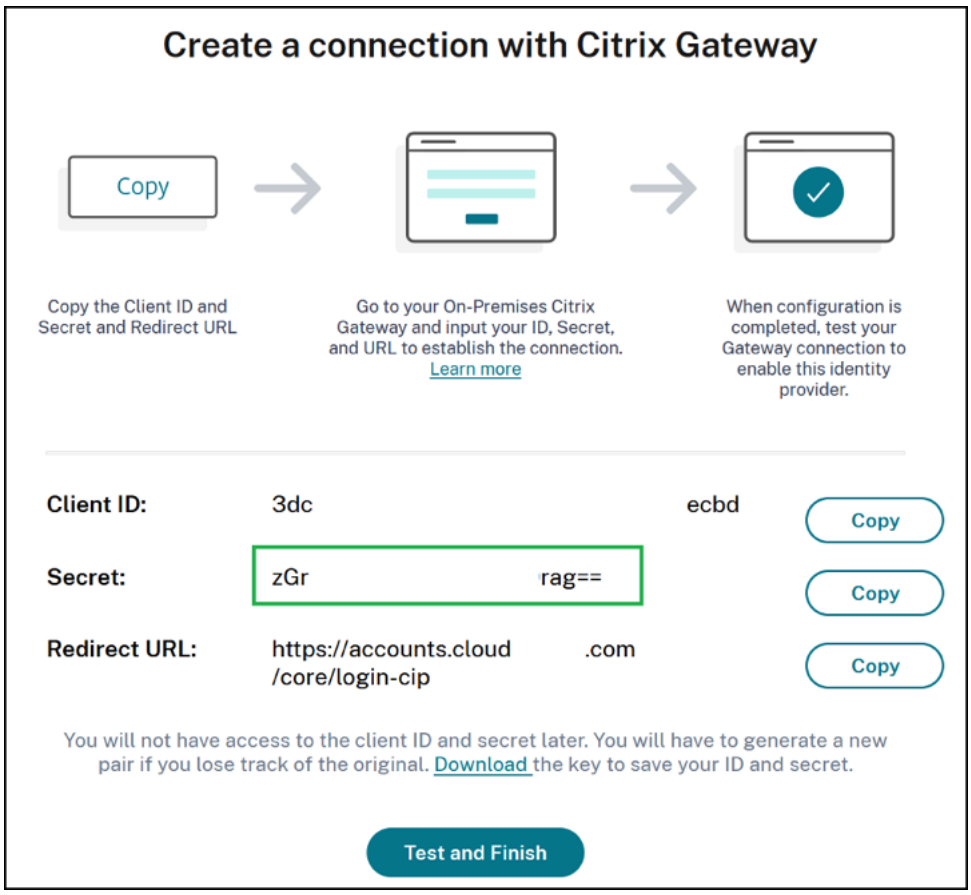
> 重要提示
>
> 将 Citrix Cloud 和 Citrix Gateway 或您的自适应身份验证 HA 配对链接在一起的现有 OAuth 策略和配置文件只有在 OAuth 证书丢失时才必须更新。修改此政策可能会中断 Citrix Cloud 和 Workspaces 之间的联系，并将影响您登录 Workspaces 的能力。

配置 **Citrix Gateway**

Citrix Cloud 管理员有权访问未加密的客户端密钥。这些凭证由 Citrix Cloud 在 Citrix Gateway 链接过程中在“身份和访问管理”**>**“身份验证”中提供。OAuth 配置文件和策略由 Citrix 管理员在连接过程中在 Citrix Gateway 上手动创建。

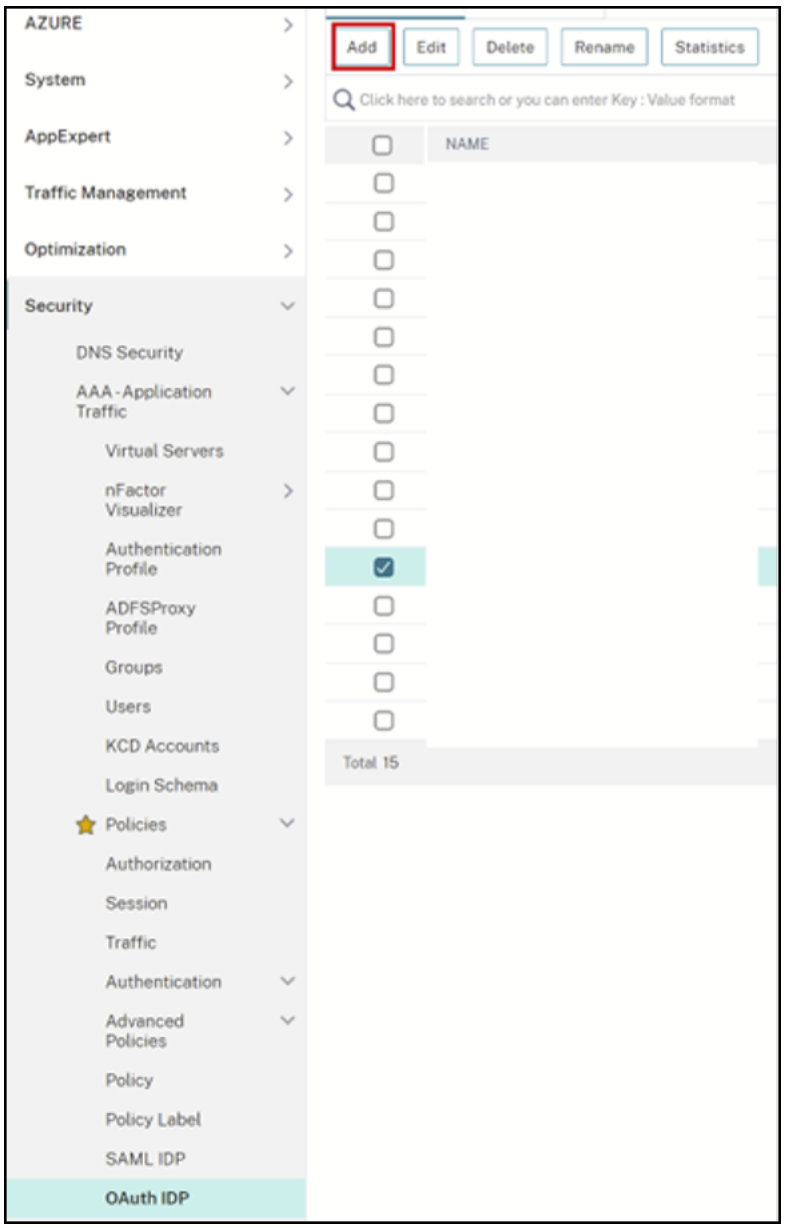
您需要在 Citrix Gateway 连接过程中提供的客户端 ID 和未加密的客户端密钥。这些凭证由 Citrix Cloud 提供并已安全保存。
需要未加密的密钥才能使用 Citrix ADC 接口或命令行接口 (CLI) 创建 OAuth 策略和配置文件。

以下是向 Citrix 管理员提供客户端 ID 和密钥时的用户界面示例。如果 Citrix 管理员在连接过程中未能保存凭证，则在连接 Citrix Gateway 后，他们将无法获得未加密密钥的副本。

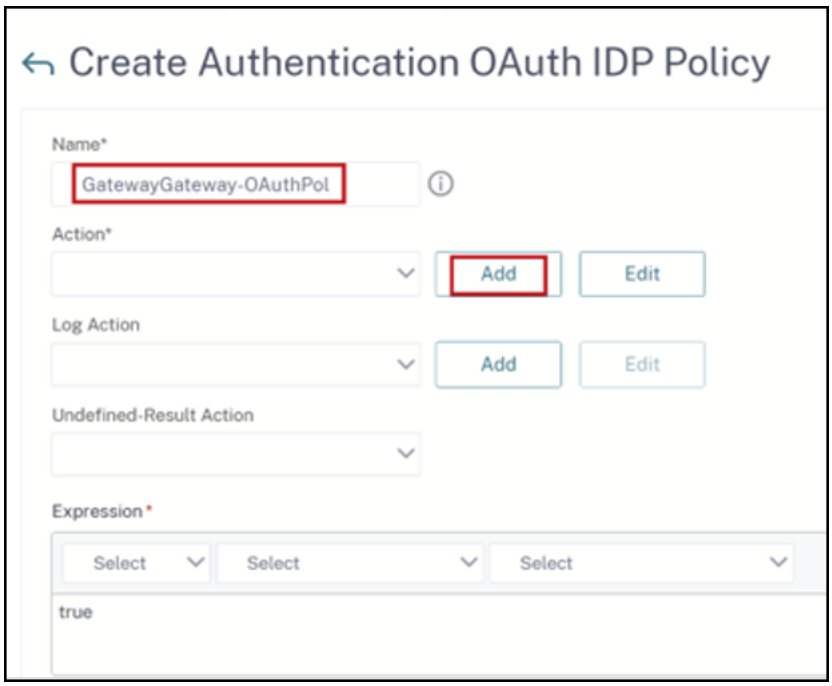


使用 **Citrix Cloud** 执行以下步骤，使用 Citrix Gateway 接口添加额外的 OAuth 配置文件和策略：

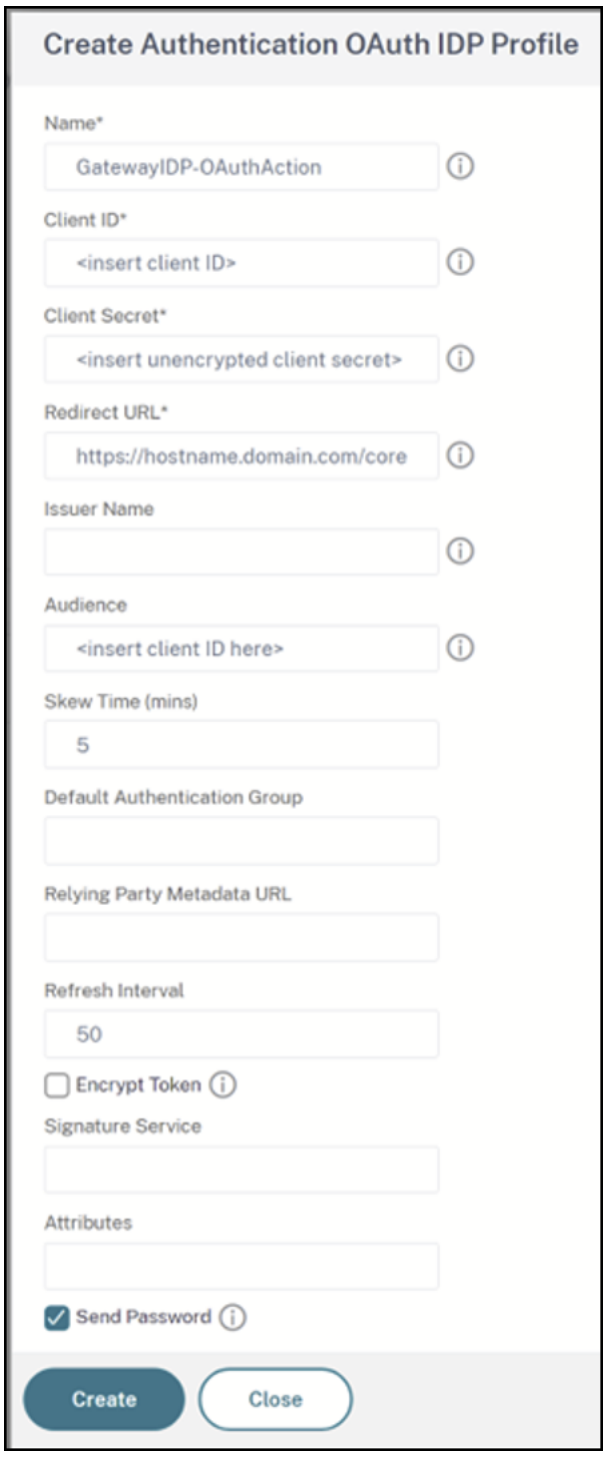
1. 从菜单中选择 安全 **> AAA-**应用程序流量 **> OAuth IDP**。选择现有的 **OAuth** 策略，然后单击“添加”。



2. 出现提示时，修改新 OAuth 策略的名称，使其与上一步中选择的现有策略不同。Citrix 建议在其名称中添加 自定义 *URL* 。



3. 在 Citrix Gateway GUI 上，创建您现有的 OAuth 配置文件
4. 在“操作”旁边的同一 GUI 菜单上，单击“添加”。



5. 在 Citrix Gateway GUI 上，将新的 OAuth 策略绑定到您现有的身份验证、授权和审计虚拟服务器。
6. 导航到“安全”**>**“虚拟服务器”**>**“编辑”。

使用命令行界面 **(CLI)**

> 重要提示
>
> 如果您没有安全保存 OAuth 凭据的副本，则需要断开连接并重新连接 Citrix Gateway，并使用 Citrix Cloud 身份和访问管理提供的新 OAuth 凭据更新现有的 OAuth 配置文件。只有在旧凭证不可恢复时，才使用新凭证更新现有 OAuth 配置文件。除非您别无选择，否则不建议这样做。

1. 使用诸如 PuTTY 之类的 SSH 工具连接到您的 Citrix Gateway 实例。
2. 创建 OAuthProfile 和 OAuthPolicy。添加身份验证 OAuthIDPProfile。

```
"CustomDomain-OAuthProfile"-clientID "<clientID>"-clientSecret "<unencrypted client secret>"-redirectURL "https://hostname.domain.com/core/login-cip"-audience "<clientID>"-sendPassword ON

add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule true -action "CustomDomain-OAuthProfile"
```

3. 将 OAuthPolicy 绑定到正确的身份验证、授权和审计虚拟服务器，其优先级低于现有策略。此实例假设现有策略的优先级为 10，因此新策略使用 20。绑定身份验证虚拟服务器。

```
"CitrixGatewayAAAvServer"-policy "CustomDomain-OAuthPol"-priority 20
```

配置自适应身份验证

> 重要提示
>
> 在自适应身份验证主网关和辅助 HA 网关上，OAuth 配置文件的加密密钥和加密参数不同。确保从主 HA 网关获取加密密钥，并在主 HA 网关上运行这些命令。

Citrix Cloud 管理员无权访问未加密的客户端密钥。OAuth 策略和配置文件由 Citrix 自适应身份验证服务在配置阶段创建。必须使用从 ns.conf 文件中获得的加密密钥和 CLI 命令来创建 OAuth 配置文件。无法使用 Citrix ADC 用户界面执行此操作。使用比绑定到现有身份验证、授权和审计虚拟服务器的现有策略更高的优先级，将新的自定义 URL OAuthPolicy 绑定到您现有的身份验证、授权和审计虚拟服务器。请注意，优先级较低的数字会先进行评估。将现有策略设置为优先级 10，将新策略设置为优先级 20，以确保按正确的顺序对其进行评估。

1. 使用像 PuTTY 这样的 SSH 工具连接到您的自适应身份验证主节点。

```
show ha node
```



```
 Done
> show ha node
1)      Node ID:      0
        IP:     192.168.0.4 (adaptive-auth-1)
        Node State: UP
        Master State: Secondary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: SUCCESS
        Propagation: ENABLED
        Enabled Interfaces : 0/1
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : None
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
        Sync Status Strict Mode: DISABLED
        Hello Interval: 200 msecs
        Dead Interval: 3 secs
        Node in this Master State for: 9:0:15:41 (days:hrs:min:sec)
2)      Node ID:      1
        IP:     192.168.0.7
        Node State: UP
        Master State: Primary
        Fail-Safe Mode: OFF
        INC State: ENABLED
        Sync State: ENABLED
        Propagation: ENABLED
        Enabled Interfaces : 0/1
        Disabled Interfaces : None
        HA MON ON Interfaces : None
        HA HEARTBEAT OFF Interfaces : None
        Interfaces on which heartbeats are not seen : None
        Interfaces causing Partial Failure: None
        SSL Card Status: NOT PRESENT
 Done
```

2. 在包含现有 OAuth 配置文件的主 HA 网关的运行配置中找到该行。

```
sh runn | grep oauth
```

3. 复制 Citrix ADC CLI 的输出，包括所有加密参数。

4. 修改您在上一步中复制的行，并使用它来构建新的 CLI 命令，该命令将允许您使用客户端 ID 的加密版本创建 OAuth 配置文件。这需要包括所有加密参数。

   - 将 OAuth 配置文件的名称更新为 *CustomDomain-OAuthProfile*
   - 将 -redirectURL 更新为 https://hostname.domain.com/core/login-cip

   这是两次更新后的示例。

```
add authentication OAuthIDPProfile "CustomDomain-OAuthProfile"-
clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret <long
 encrypted client Secret> -encrypted -encryptmethod ENCMTHD_3
```



```
-kek -suffix 2023_04_19_09_12_25 -redirectURL "https://hostname
.domain.com/core/login-cip"-audience b1656835-20d1-4f6b-addd-1
a531fd253f6 -sendPassword ON

add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule
true -action "CustomDomain-OAuthProfile"
```

5. 将 OAuthPolicy 绑定到正确的身份验证、授权和审计虚拟服务器，其优先级低于现有策略。所有自适应身份验证部署的身份验证、授权和审计虚拟服务器名称均为 *auth_vs*。此实例假设现有策略的优先级为 10，因此新策略使用 20。

```
bind authentication vserver "auth_vs"-policy "CustomDomain-
OAuthPol"-priority 20
```

已知限制

自定义域解决方案的一些已知限制如下：

Workspace 平台

- 目前，每位客户仅支持一个自定义域。
- 自定义域只能链接到默认 Workspace URL。通过多 URL 功能添加的其他 Workspace URL 不能有自定义域。多 URL 功能目前处于私有技术预览阶段，可能并非所有客户都可用。
- 如果您在先前的解决方案中配置了自定义域，并且正在使用 SAML 或 AzureAD 对 Citrix Workspace 访问权限进行身份验证，则如果不先删除现有自定义域，则无法在新解决方案上配置定制域。

SAML

SAML 支持仅限于以下用例之一：

- SAML 可以专门用于 cloud.com 域名。在这种情况下，SAML 的使用将包括 Citrix Workspace 访问权限和 Citrix Cloud 管理员访问权限。
- SAML 可以专门用于自定义域。

Windows 版 **Citrix Workspace** 应用程序

- 适用于 Windows 的 Citrix Workspace 应用程序版本 2305 和 2307 不支持此功能。更新到最新的支持版本。

安全的工作区

November 26, 2023

作为管理员，您可以选择让订阅者使用以下身份验证方法之一对其工作区进行身份验证：

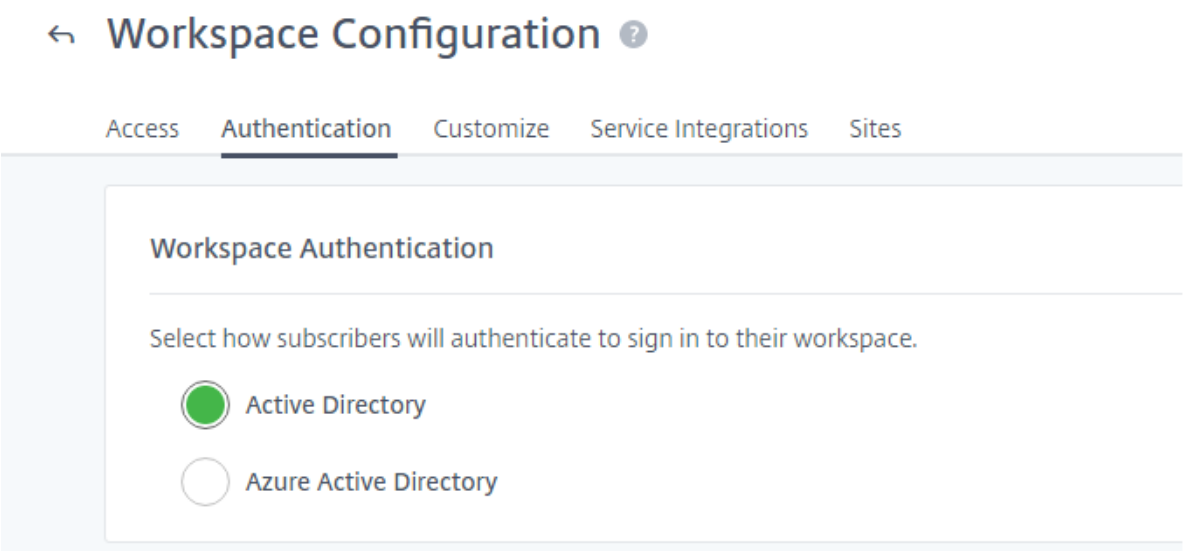
- Active Directory (AD)
- Active Directory 加令牌
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

这些身份验证选项可用于任何 Citrix Cloud 服务。有关更多信息，请参阅 技术简报：Workspace 身份。

Citrix Workspace 还支持使用 Citrix 联合身份验证服务 (FAS) 为 Citrix DaaS 提供单点登录 (SSO)。使用 FAS 的 SSO 消除了订阅者在使用联合身份验证方法登录其工作区后对 DaaS 进行身份验证的需要。有关详细信息，请参阅使用 Citrix 联合身份验证服务对工作区启用单点登录。

选择或更改身份验证方法

配置身份提供程序后，您可以在 **Workspace** 配置 **>** 身份验证 **> Workspace** 身份验证中选择或更改订阅者对其 Workspace 进行身份验证的方式。



> 重要：
>
> 切换身份验证模式可能需要长达五分钟的时间，并会导致订阅者在此期间中断。Citrix 建议将更改限制在低使用率时段。如果您确实有订阅者使用浏览器或 Citrix Workspace 应用程序登录到 Citrix Workspace，请建议他们关闭浏览器或退出应用程序。等待大约五分钟后，他们可以使用新的身份验证方法再次登录。

Active Directory (AD)

默认情况下，Citrix Cloud 使用 Active Directory (AD) 来管理工作区的订阅者身份验证。

要使用 AD，必须在本地 AD 域中至少安装两个 Citrix Cloud 连接器。有关安装 Cloud Connector 的更多信息，请参阅 Cloud Connector 安装。

Active Directory (AD) 加令牌

为了提高安全性，Citrix Workspace 支持基于时间的令牌作为 AD 登录身份验证的第二个因素。

对于每次登录，Workspace 都会提示订阅者从其注册设备上的身份验证应用程序输入令牌。在登录之前，订阅者必须使用遵循基于时间的一次性密码 (TOTP) 标准的身份验证应用程序（例如 Citrix SSO）注册其设备。目前，订阅者一次只能注册一台设备。

有关更多信息，请参阅“技术洞察：身份验证 - TOTP”和“技术洞察：身份验证-推送”。

AD plus 代币的要求

Active Directory 加令牌身份验证有以下要求：

- Active Directory 和 Citrix Cloud 之间的连接，在本地环境中至少安装了两个 Cloud Connector。有关要求和说明，请参阅 将 Active Directory 连接到 Citrix Cloud。
- 在身份和访问管理页面中启用了 **Active Directory +** 令牌身份验证。有关信息，请参阅 启用 Active Directory 加令牌身份验证。
- 订阅者访问电子邮件以注册设备。
- 用于下载身份验证应用程序的设备。

首次注册

订阅者使用注册设备进行 双重身份验证中所述的注册过程来注册其设备。

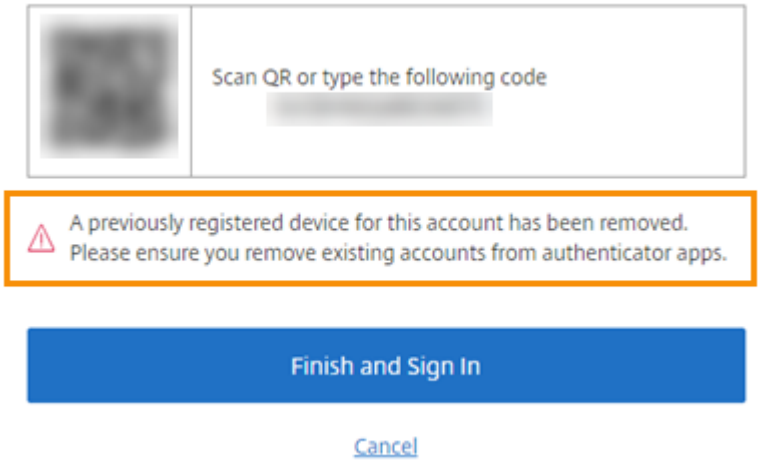
首次登录 Workspace 时，订阅者会按照提示下载 Citrix SSO 应用程序。Citrix SSO 应用程序每 30 秒在已注册的设备上生成一个唯一的一次性密码。

> 重要：
>
> 在设备注册过程中，订阅者会收到一封包含临时验证码的电子邮件。此临时代码仅用于注册订阅者的设备。不支持使用此临时代码作为通过双重身份验证登录 Citrix Workspace 的令牌。只有从已注册设备上的身份验证应用程序生成的验证码才是支持双重身份验证的令牌。

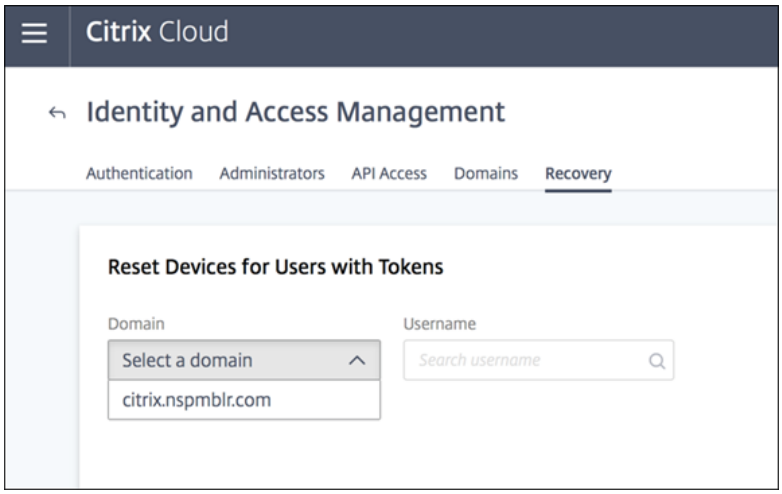
重新注册设备

如果订阅者不再拥有已注册的设备或需要重新注册该设备（例如，从设备中擦除内容后），Workspace 将提供以下选项：

- 订阅者可以使用注册设备进行 双重身份验证中所述的相同注册过程重新注册其设备。由于订阅者一次只能注册一台设备，因此注册新设备或重新注册现有设备会删除之前的设备注册。



- 管理员可以按 Active Directory 名称搜索订阅者并重置其设备。为此，请转到 身份和访问管理 **>** 恢复。在下次登录 Workspace 时，订阅者将经历首次注册步骤。



Azure Active Directory

使用 Azure Active Directory (AD) 管理订阅者对工作区的身份验证有以下要求：

- 具有全局管理员权限的用户的 Azure AD。有关 Citrix Cloud 使用的 Azure AD 应用程序和权限的更多信息，请参阅 适用于 Citrix Cloud 的 Azure Active Directory 权限。
- 在本地 AD 域中安装的 Citrix Cloud Connector。计算机还必须加入同步到 Azure AD 的域。
- VDA 版本 7.15.2000 LTSR CU VDA 或 7.18 当前版本的 VDA 或更高版本。
- Azure AD 和 Citrix Cloud 之间的连接。有关信息，请参阅 将 Azure Active Directory 连接到 Citrix Cloud。

将 Active Directory 同步到 Azure AD 时，同步中必须包含 UPN 和 SID 条目。如果这些条目未同步，Citrix Workspace 中的某些工作流将失败。

> 警告：
>
> - 如果您使用的是 Azure AD，请不要进行 CTX225819中描述的注册表更改。进行此更改可能会导致 Azure AD 用户的会话启动失败。
> - 启用 DSAuthAzureAdNestedGroups 功能后，支持将一个组添加为另一个组的成员（嵌套）。您可以通过向 Citrix 支持部门提交请求来启用 DSAuthAzureAdNestedGroups。

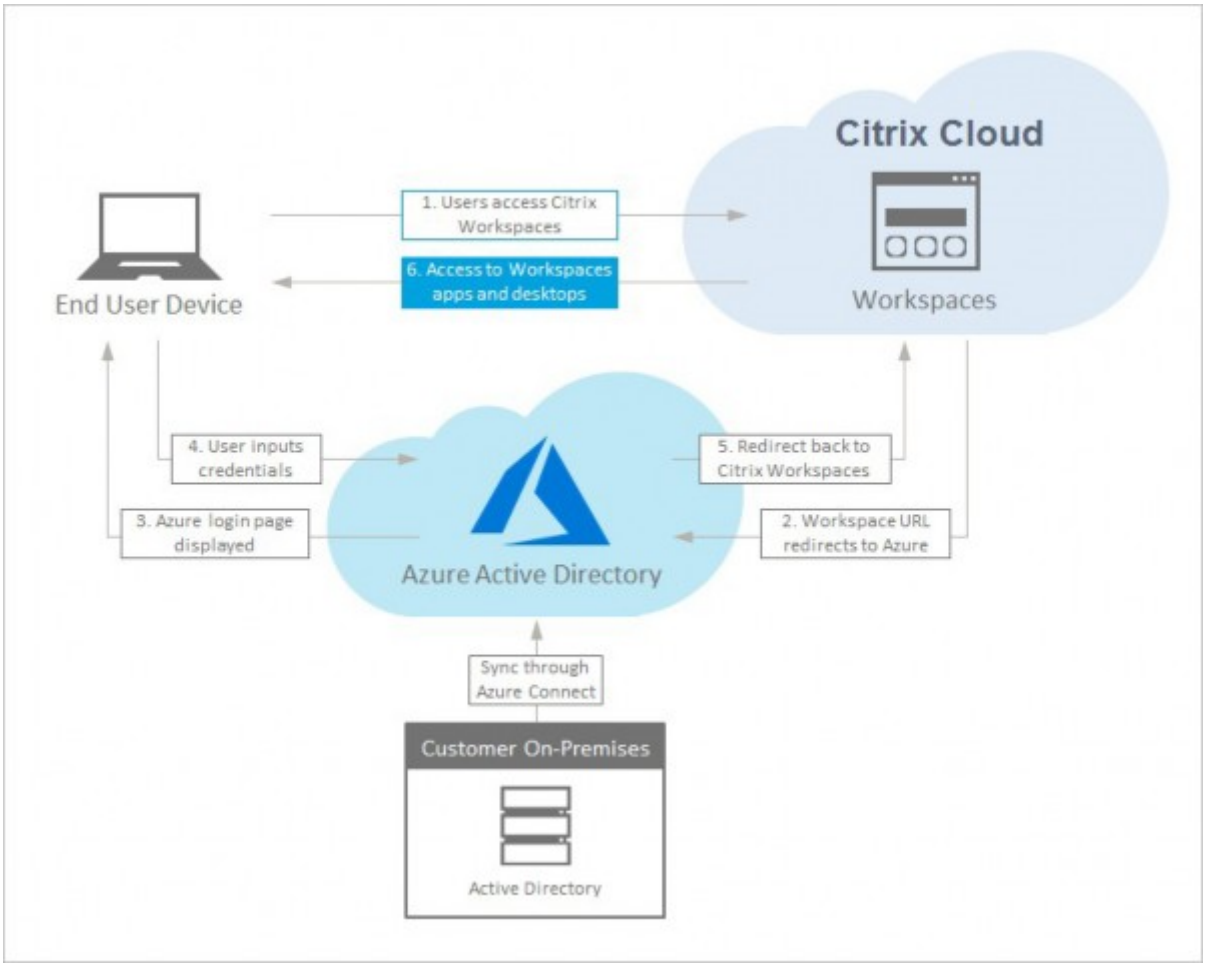
启用 Azure AD 身份验证后：

- 增强安全性：出于安全考虑，启动应用程序或桌面时，系统会提示用户重新登录。密码信息直接从用户的设备流向托管会话的 VDA。
- 登录体验： Azure AD 身份验证提供联合登录，而不是单点登录 (SSO)。订阅者从 Azure 登录页面登录，并且在打开 Citrix DaaS 时可能需要再次进行身份验证。

对于 SSO，请在 Citrix Cloud 中启用 Citrix 联合身份验证服务。有关详细信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录 。

您可以自定义 Azure AD 的登录体验。有关信息，请参阅 Microsoft 文档。在“Workspace 配置”中进行的任何登录自定义（徽标）不会影响 Azure AD 登录体验。

下图显示了 Azure AD 身份验证的顺序。



Citrix Gateway

Citrix Workspace 支持使用本地 Citrix Gateway 作为身份提供程序来管理工作区的订阅者身份验证。有关更多信息，请参阅技术洞察：身份验证 - Citrix Gateway。

Citrix Gateway 的要求

Citrix Gateway 身份验证有以下要求：

- Active Directory 和 Citrix Cloud 之间的连接。有关要求和说明，请参阅 将 Active Directory 连接到 Citrix Cloud。
- 订阅者必须是 Active Directory 用户才能登录其工作区。
- 如果您正在执行联合，则必须将您的 AD 用户同步到联合提供商。Citrix Cloud 需要 AD 属性才能允许用户成功登录。
- 本地 Citrix Gateway：
  - Citrix Gateway 12.1 54.13 Advanced Edition 或更高版本

  - Citrix Gateway 13.0 41.20 Advanced Edition 或更高版本

- 在身份和访问管理页面中已启用 **Citrix Gateway** 身份验证。这将生成在 Citrix Cloud 和本地网关之间创建连接所需的客户端 ID、密钥和重定向 URL。
- 在网关上，使用生成的客户端 ID、密钥和重定向 URL 配置 OAuth IdP 身份验证策略。

有关更多信息，请参阅 将本地 Citrix Gateway 作为身份提供商连接到 Citrix Cloud。

Citrix Gateway 的订阅者体验

启用 Citrix Gateway 身份验证后，订阅者将遇到以下工作流：

1. 订阅者在其浏览器中导航到工作区 URL 或启动 Workspace 应用程序。
2. 订阅者将被重定向到 Citrix Gateway 登录页面，并使用网关上配置的任何方法进行身份验证。此方法可以是 MFA、联合、条件访问策略等。您可以使用 CTX258331中描述的步骤自定义网关登录页面，使其看起来与 Workspace 登录页面相同。
3. 成功进行身份验证后，将显示订阅者的工作区。

Google

Citrix Workspace 支持使用 Google 作为身份提供商来管理订阅者对工作区的身份验证。

对 **Google** 的要求

- 本地 Active Directory 与 Google Cloud 之间的连接。
- 具有 Google Cloud Platform 控制台访问权限的开发者帐号。创建服务帐号和密钥以及启用 Admin SDK API 时需要此帐户。
- 具有 Google Workspace 管理员控制台访问权限的管理员帐号。此帐户是配置域范围委派和只读 API 用户帐户所必需的。
- 您的本地 Active Directory 域与 Citrix Cloud 之间的连接，在“身份和访问管理”页面中启用了 **Google** 身份验证。要创建此连接，您的资源位置中至少需要两个 Cloud Connector。

有关更多信息，请参阅 将 Google 作为身份提供商连接到 Citrix Cloud。

Google 的订阅体验

启用 Google 身份验证后，订阅者将体验以下工作流程：

1. 订阅者在其浏览器中导航到工作区 URL 或启动 Workspace 应用程序。
2. 订阅者将被重定向到 Google 登录页面，并使用 Google Cloud 中配置的方法（例如，多重身份验证、条件访问策略等）进行身份验证。
3. 成功进行身份验证后，将显示订阅者的工作区。

Okta

Citrix Workspace 支持使用 Okta 作为身份提供程序来管理工作区的订阅者身份验证。有关更多信息，请参阅技术洞察：身份验证 - Okta。

Okta 的要求

Okta 身份验证有以下要求：

- 本地 Active Directory 与 Okta 组织之间的连接。
- 配置为与 Citrix Cloud 配合使用的 Okta OIDC Web 应用程序。要将 Citrix Cloud 连接到您的 Okta 组织，必须提供与此应用程序关联的客户端 ID 和客户端密钥。
- 您的本地 Active Directory 域与 Citrix Cloud 之间的连接，在身份和访问管理页面中启用了 **Okta** 身份验证。

有关更多信息，请参阅 将 Okta 作为身份提供商连接到 Citrix Cloud。

Okta 的订阅者体验

启用 Okta 身份验证后，订阅者将体验以下工作流：

1. 订阅者在其浏览器中导航到工作区 URL 或启动 Workspace 应用程序。
2. 订阅者将被重定向到 Okta 登录页面，并使用 Okta 中配置的方法（例如，多因素身份验证、条件访问策略等）进行身份验证。
3. 成功进行身份验证后，将显示订阅者的工作区。

Okta 身份验证提供联合登录，而不是单点登录 (SSO)。订阅者从 Okta 登录页面登录到工作区，并且在打开 Citrix DaaS 时可能需要再次进行身份验证。对于 SSO，请在 Citrix Cloud 中启用 Citrix 联合身份验证服务。有关详细信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录 。

SAML 2.0

Citrix Workspace 支持使用 SAML 2.0 来管理订阅者对工作区的身份验证。您可以使用自己选择的 SAML 提供商，前提是它支持 SAML 2.0。

SAML 2.0 的要求

SAML 身份验证有以下要求：

- 支持 SAML 2.0 的 SAML 提供商。
- 本地 Active Directory 域。
- 两个 Cloud Connector 部署到资源位置并加入到您的本地 AD 域。

- 与您的 SAML 提供商的 AD 集成。

有关为工作区配置 SAML 身份验证的更多信息，请参阅 将 SAML 作为身份提供商连接到 Citrix Cloud。

使用 **SAML 2.0** 的订阅者体验

1. 订阅者在浏览器中导航到 Workspace URL 或启动 Citrix Workspace 应用程序。
2. 订阅者将被重定向到其组织的 SAML 身份提供商登录页面。订阅者使用为 SAML 身份提供程序配置的机制进行身份验证，例如多重身份验证或条件访问策略。
3. 成功进行身份验证后，将显示订阅者的工作区。

Citrix 联合身份验证服务 **(FAS)**

Citrix Workspace 支持使用 Citrix 联合身份验证服务 (FAS) 对 Citrix DaaS 进行单点登录 (SSO)。如果没有 FAS，则会提示使用联合身份提供商的订阅者多次输入凭据以访问其 DaaS。

有关更多信息，请参阅 Citrix 联合身份验证服务 (FAS)。

订阅者注销体验

使用“设置”**>**“注销”完成从 Workspace 和 Azure AD 的注销过程。如果订阅者关闭浏览器而不是使用“注销”选项，他们可能会保持登录到 Azure AD 的状态。

> 重要：
>
> 如果 Citrix Workspace 因不活动而在浏览器中超时，订阅者将保持登录到 Azure AD 的状态。这样可以防止 Citrix Workspace 超时强制关闭其他 Azure AD 应用程序。

更多信息

- 技术简报：工作区单点登录
- 技术见解 - Citrix Workspace
- 概念证明指南 - Citrix Workspace

将服务集成到工作区

November 26, 2023

本文概述了向 Citrix Workspace 添加服务所涉及的步骤，该过程分为两步：

1. 在 Citrix Cloud 中配置单个服务。您可以在 Citrix Cloud Services 中找到各个 Citrix Cloud 服务的列表，这些服务链接到每项服务的说明。
2. 在 **Workspace** 配置 > 服务集成中启用（和禁用）对已配置服务的访问权限。

配置服务

您购买的服务将在 Citrix Cloud 控制面板中以卡片布局显示。您购买的服务包括 管理 按钮。

要配置购买的服务，请执行以下操作：

1. 登录 Citrix Cloud。
2. 在要配置的服务的磁贴中选择 管理。
3. 按照说明设置该服务。

有关云托管服务的简要说明，请 通过 Citrix Workspace 访问云托管服务。

如果您想尝试一项新服务，可以申请试用或演示。有关服务试用的更多信息，请访问 Citrix Cloud 服务试用版。

启用服务

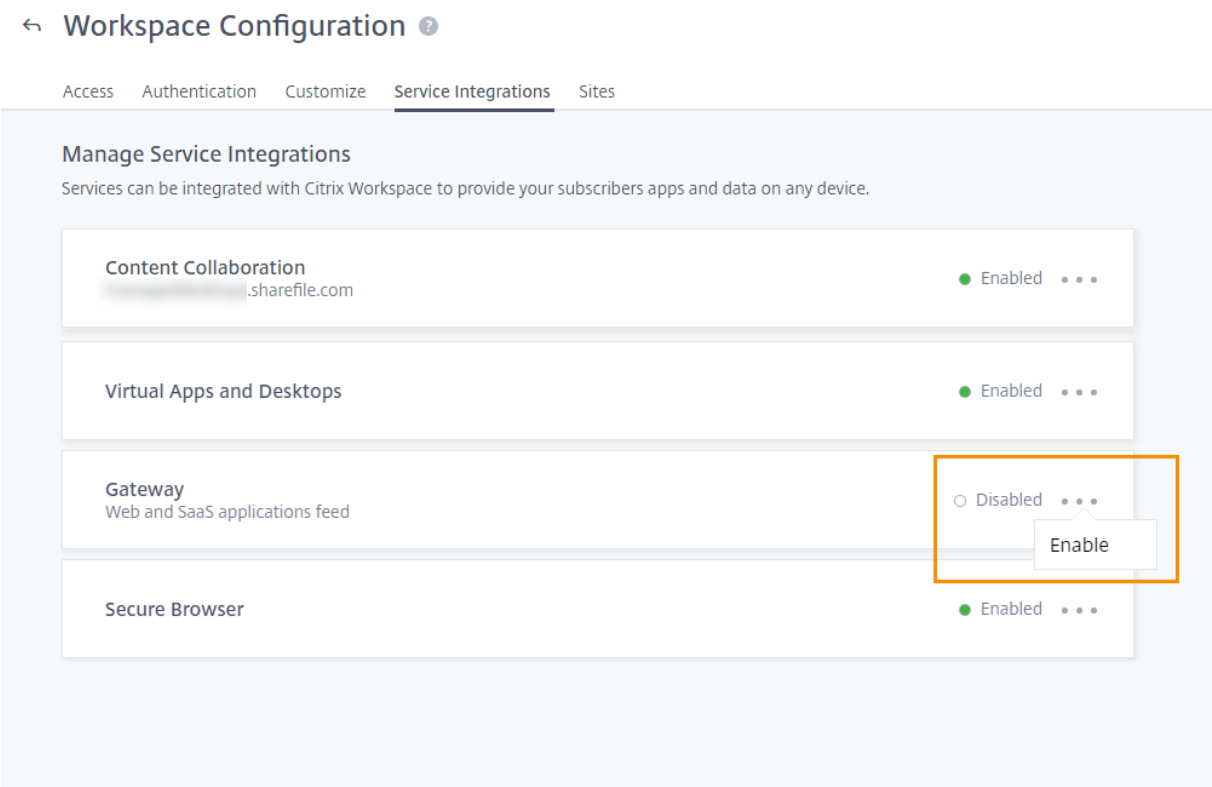
配置服务后，您可以将它们集成到 Citrix Workspace 中。

默认情况下，订阅 **DaaS** 和 **Remote Browser Isolation** 服务会将其启用。默认情况下，您的组织订阅的所有其他新服务都处于禁用状态。

> 注意：
>
> **Citrix Apps Essentials** 服务和 **Citrix DaaS** 在 **Workspace** 配置的服务集成选项卡中均显示为“Citrix DaaS”

要为服务启用 Workspace 集成，请执行以下操作：

1. 导航到 工作区配置 > 服务集成。
2. 选择服务旁边的省略号按钮，然后选择 启用。

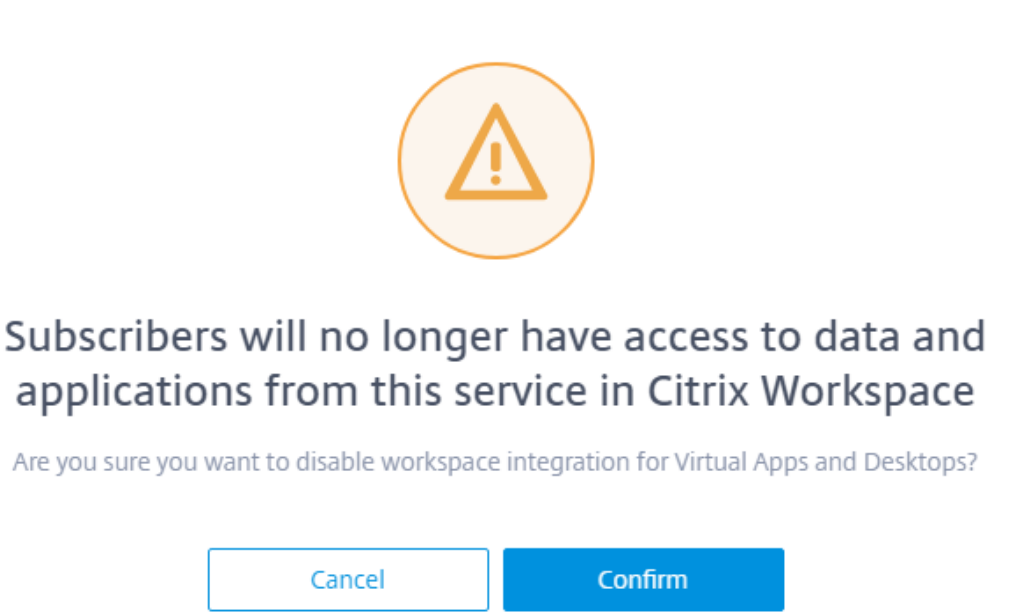


禁用服务

禁用工作区集成会阻止订阅者访问该服务。这不会禁用工作区 URL，但订阅者无法从 Citrix Workspace 中的该服务访问数据和应用程序。

要禁用服务的工作区集成，请执行以下操作：

1. 导航到 工作区配置 > 服务集成。
2. 选择服务旁边的省略号按钮，然后选择 禁用。
3. 出现提示时，选择“确认”以确认订阅者将无法访问该服务中的数据或应用程序。



配置 **Citrix Workspace** 应用程序

November 26, 2023

您可以使用 Global App Configuration Service (GACS) 配置 Citrix Workspace 应用程序。它可以帮助您在托管和非托管设备上管理最终用户的应用程序设置。

可以使用以下方法之一为云环境（Citrix Workspace）和本地（Citrix StoreFront）环境配置设置：

- Global App Configuration Service 用户界面 (UI)：
  - 配置云应用商店的设置
  - 为本地应用商店配置设置
- API：要使用 API 配置设置，请参阅 Citrix Developer。

Windows、Mac、Android、iOS、HTML5 和 ChromeOS 平台支持此服务。

主要好处

Global App Configuration Service 允许您从集中式界面执行以下功能：

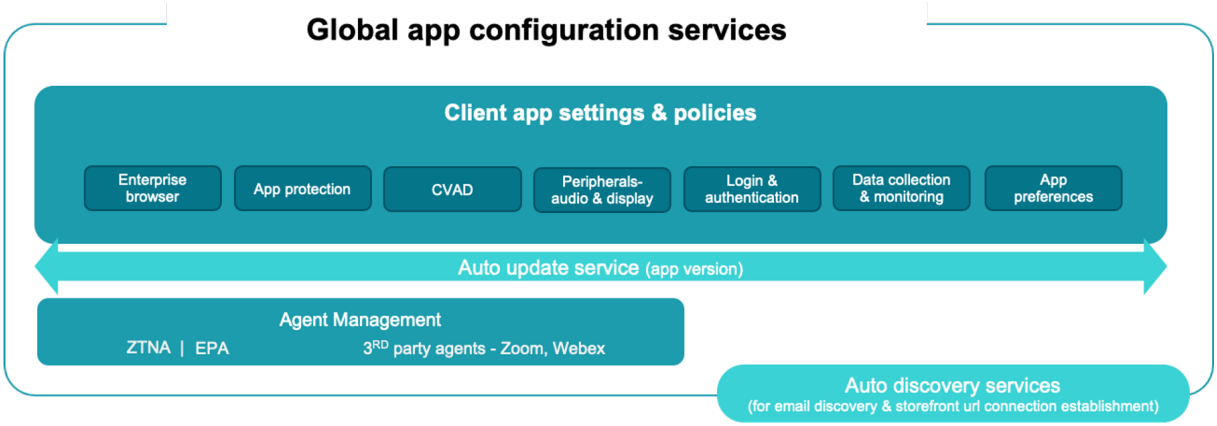
- 为托管和非托管设备配置设置（自带设备）
- 为多个应用商店配置设置

- 更新和管理客户端应用程序代理（例如，Endpoint Analysis、ZTNA）和第三方代理（例如 Zoom、Webex）
- 为最终用户自动更新和管理 Citrix Workspace 应用程序版本
- 在向最终用户推出配置之前对其进行测试

Global App Configuration Service 的工作原理

Global App Configuration Service 是一个 Citrix IP 解决方案，用于配置和管理客户端应用程序设置。它使用以下服务和设置为您的最终用户提供无缝体验。

- 自动发现服务：它将域映射到应用商店 URL，使您的最终用户能够使用他们的电子邮件地址登录。最终用户无需在登录时提供应用商店 URL。
- 自动更新服务和代理管理：为最终用户自动将 Citrix Workspace 应用程序更新到指定版本。您可以灵活地为不同的平台配置不同的应用程序版本。
- 客户端应用程序设置和策略：可以集中配置和设置 Citrix Workspace 应用程序上的所有最终用户设置。它包括登录体验、安全性、身份验证选项、虚拟应用程序、桌面设置等设置。



必备条件

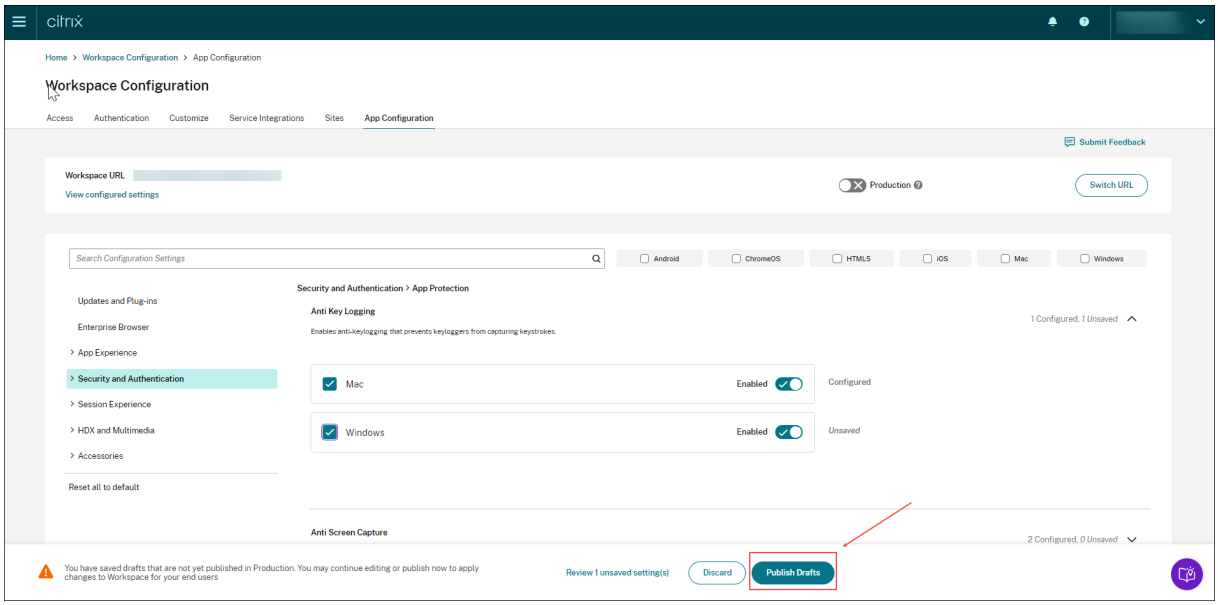
在配置应用程序设置之前，请验证 Citrix Workspace 应用程序版本是否等于或高于指定版本。有关更多信息，请参阅下表。

Citrix Workspace 应用程序平台	支持的最低版本
Windows	当前版本 - 2106、LTSR - 2203.1
Mac	2203.1
iOS	2104
HTML5	2111
ChromeOS	2203

Citrix Workspace 应用程序平台	支持的最低版本
Android	2104

如何使用 **Global App Configuration Service**

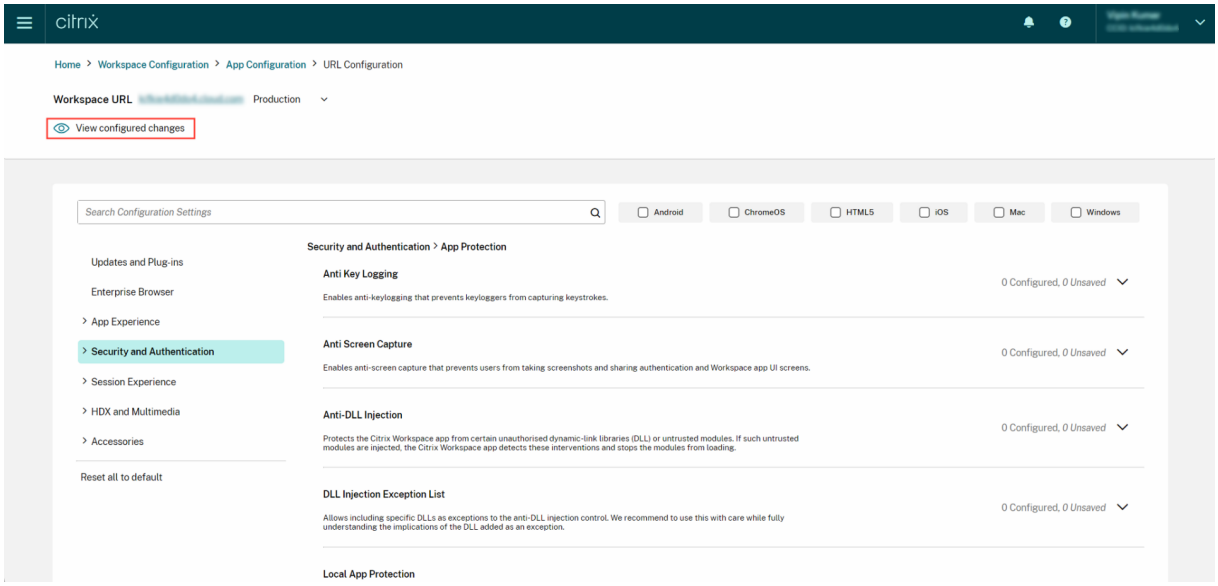
要配置设置，请登录 Citrix Cloud 门户并导航到 **Workspace** 配置 > 应用程序配置。根据贵组织的政策修改应用程序设置。然后，您可以单击“发布草稿”来保存和发布您的设置。



用户界面还提供以下选项，以简化用户体验。

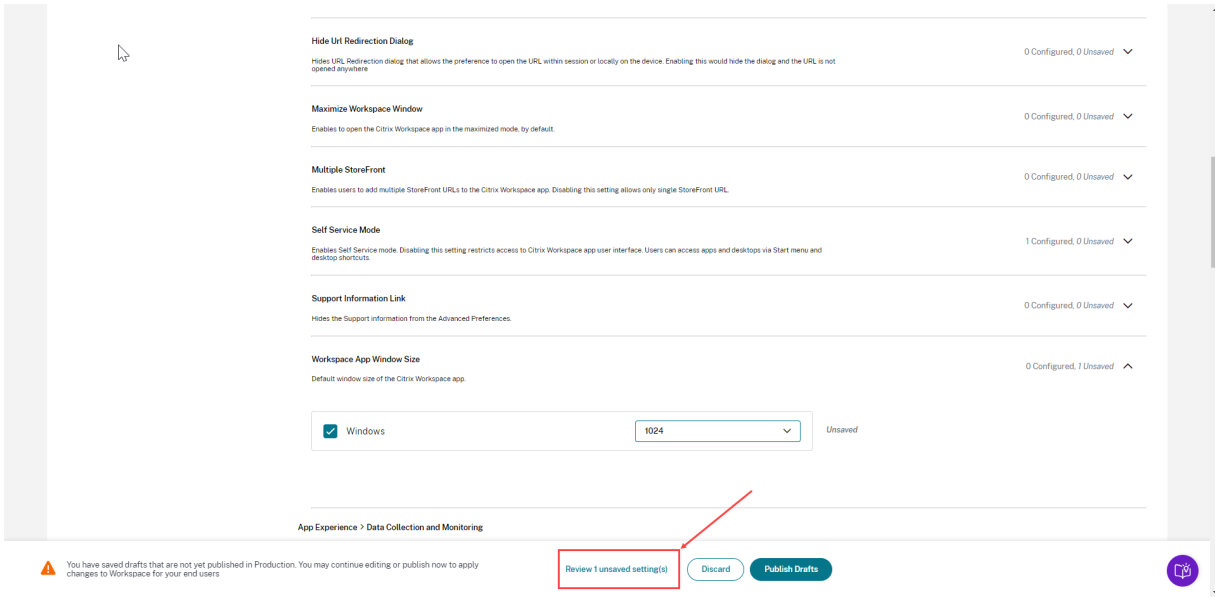
查看已配置设置的摘要

您可以通过单击“查看已配置的设置”按钮来查看当前配置的摘要。这样就无需单独扩展和审查每项设置。所有已配置设置的综合列表允许您全面查看当前配置并衡量用户影响。

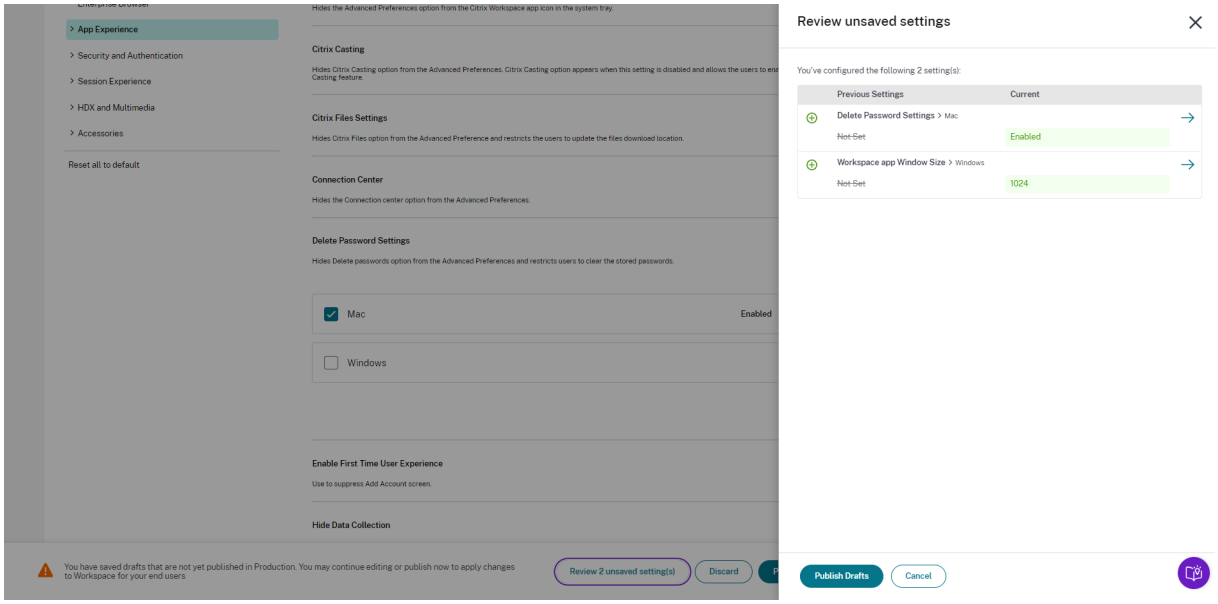


查看未保存的更改

在发布配置之前，请对未保存的更改进行最后审核。未保存的设置数量显示在用户界面上，您可以通过单击“查看未保存的设置”选项来访问此列表。它使您能够做出明智的更改并保持数据的准确性。



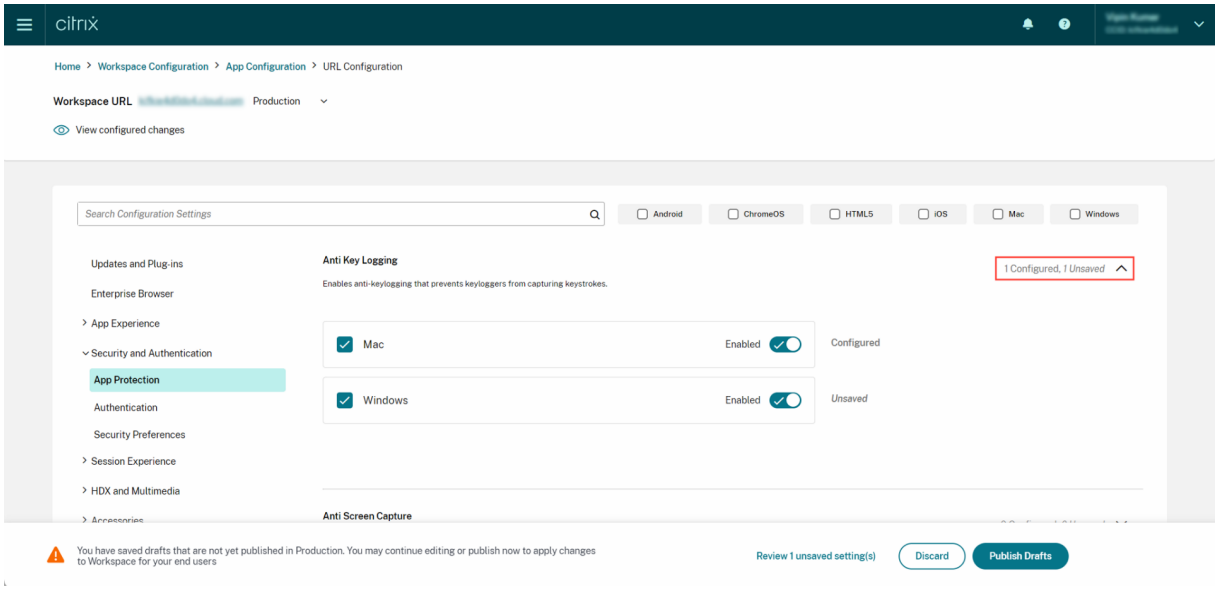
您也可以通过单击箭头导航到未保存的设置。



增强的用户界面

无需扩展即可查看每项设置的状态。现在会显示以下标签，以便在每一步做出明智的决策。

- 已配置：显示已配置该设置的平台（客户端操作系统）的数量。
- 未保存：显示已配置但尚未保存的设置数量



增强的搜索选项

搜索体验已得到增强，可提供强大而无缝的体验。管理员现在可以登录云端门户，在应用程序配置页面上轻松找到所需的设置。他们可以使用以下搜索方法。

- 使用设置描述进行搜索

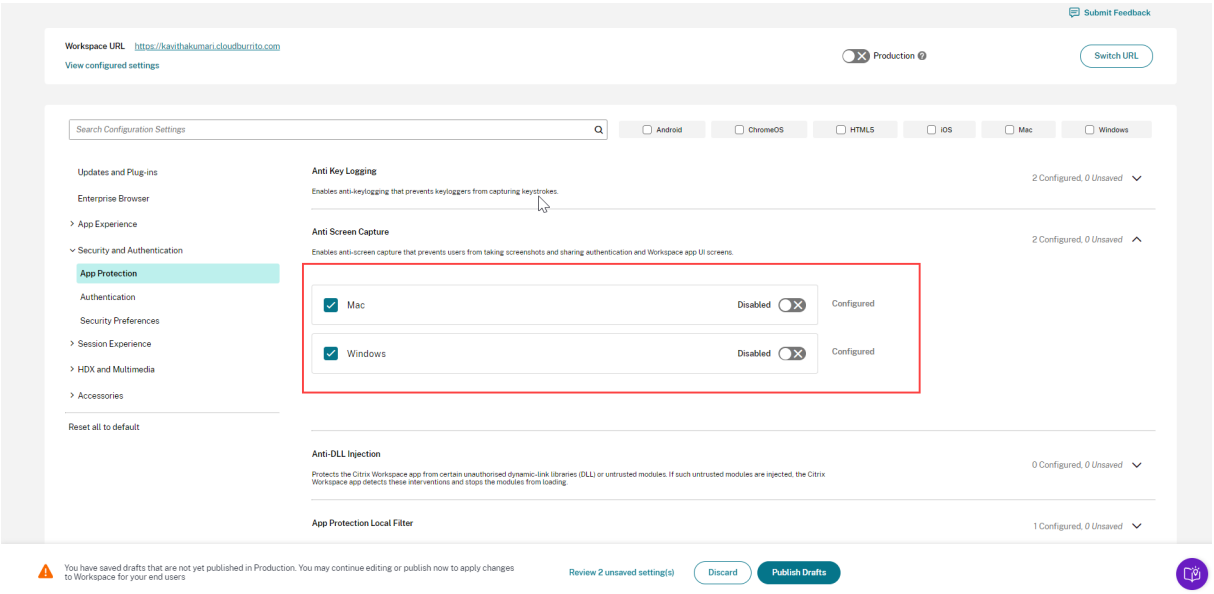
您可以通过输入在设置描述中找到的关键字来查找设置。它允许使用与所需设置相关的术语进行更灵活的搜索方法。

- 使用 **API** 设置名称进行搜索

您可以通过输入相应的 API 设置名称来搜索设置。此方法允许更精确、更有针对性的搜索，使用户能够快速找到所需的特定设置。

查看每种设置的适用平台

现在，每项设置仅动态显示与其相关和适用的平台。这种方法可确保向用户提供简洁且量身定制的选项列表。



获取更新设置的频率

配置发布后，可能需要几个小时才能在客户端更新设置。

- 在同一会话中，设置更新如下。

平台	更新设置所需的最长时间
Windows 版 Citrix Workspace 应用程序	最长 6 小时
适用于 macOS 的 Citrix Workspace 应用程序	最长 6 小时
适用于 HTML5 的 Citrix Workspace 应用程序	最长 3 小时
适用于 ChromeOS 的 Citrix Workspace 应用程序	最长 3 小时
适用于 iOS 的 Citrix Workspace 应用程序	最长 6 小时

平台	更新设置所需的最长时间
适用于 Android 的 Citrix Workspace 应用程序	最长 6 小时

- 对于 Windows 和 macOS，如果最终用户退出并重启其 Citrix Workspace 应用程序，则可以立即更新设置。
- 当最终用户向其 Citrix Workspace 应用程序添加应用商店时，该应用商店的设置会自动更新。

应用设置的优先顺序

除了 Global App Configuration Service 外，还有一些平台专用工具，例如适用于 Windows 的 GPO，可用于配置最终用户设置。
如果通过 Global App Configuration Service 配置的设置与其他平台工具配置的设置之间发生冲突，则按以下顺序应用设置。

平台	应用商店类型	优先顺序
Windows 版 Citrix Workspace 应用程序	StoreFront 和云	组策略对象 **(GPO) > Global App Configuration Service >** 注册表
适用于 Mac 的 Citrix Workspace 应用程序	StoreFront 和云	**MDM > Global App Configuration Service >** 用户默认值
适用于 HTML5 的 Citrix Workspace 应用程序	StoreFront	Global App Configuration Service > Configuration.js
	云	Global App Configuration Service
适用于 ChromeOS 的 Citrix Workspace 应用程序	StoreFront	**Google** 管理策略 **> Global App Configuration Service >** Configuration.js
	云	**Google** 管理策略 **> Global App Configuration Service**
适用于 iOS 的 Citrix Workspace 应用程序	StoreFront 和云	Global App Configuration Service
适用于 Android 的 Citrix Workspace 应用程序	StoreFront 和云	Global App Configuration Service

限制

- Linux 不支持 Global App Configuration Service。
- 在 Windows 和 Mac 上，您不能添加多个支持 Global App Configuration Service 的应用商店。

其他资源

- 关于 Global App Configuration Service 的技术简报
- 常见问题解答：Global App Configuration Service 设置和行为
- 网络研讨会录制文件：如何使用 Global App Configuration Service
- Citrix 功能介绍：Global App Configuration Service

配置云应用商店的设置

November 26, 2023

概述

您可以使用 Global App Configuration Service (GACS) 为云应用商店配置 Citrix Workspace 应用程序设置。它可以帮助管理员在托管和非托管设备上为最终用户配置和管理 Citrix Workspace 应用程序。Windows、Mac、Android、iOS、HTML5 和 ChromeOS 平台支持此服务。

必备条件

- 地址 https://discovery.cem.cloud.us 必须可访问。这是基于电子邮件的发现和 Global App Configuration Service 正常运行所必需的。
- 确认您有权访问 Citrix Cloud 帐户。如果没有，您可以从 https://onboarding.cloud.com/ 中创建帐户。有关更多信息，请参阅注册 Citrix Cloud。
- 验证您是否订阅了 Workspace。

入门

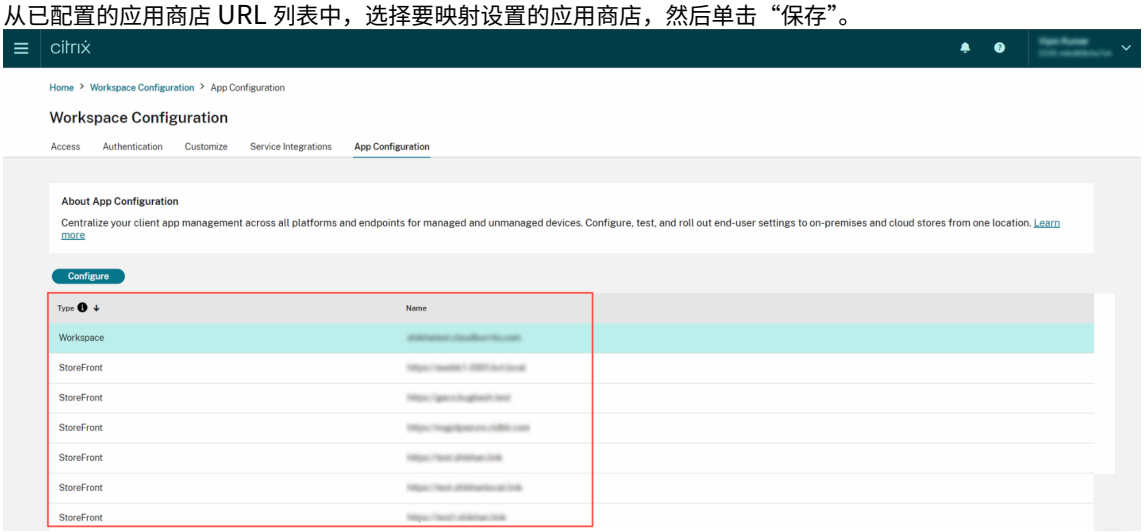
您可以登录您的 Citrix Cloud 帐户并从 **Workspace** 配置 > 应用程序配置中配置设置。
在继续操作之前，请验证您是否具有以下权限。

- **Workspace** 订阅：创建 Workspace URL 需要 Workspace 订阅。如果您没有订阅，则无法添加和配置云应用商店。
  您只能看到配置本地应用商店的选项。
- **Workspace URL**：如果您订阅了 Workspace 但尚未添加 URL，则会显示以下屏幕。您可以单击“配置云应用商店设置”下的“开始”来创建您的 URL。

配置设置

您可以从 Citrix Cloud 门户配置 Citrix Workspace 应用程序的设置。如果已为您的组织配置了多个应用商店，则可以单独配置每个应用商店。

1. 前往 Citrix Cloud 并使用您的 Citrix Cloud 凭据登录。
2. 导航到 **Workspace** 配置 > 应用程序配置。
3. 单击“切换 **URL**”以选择要为其配置设置的应用商店。
4. 从已配置的应用商店 URL 列表中，选择要映射设置的应用商店，然后单击“保存”。



5. 根据您的要求修改首选平台的设置。
6. 单击“发布草稿”以保存设置。

> 注意：
>
> 可能需要几个小时才能将设置更新到 Citrix Workspace 应用程序客户端。有关更多信息，请参阅获取更新设置的频率。

设置基于电子邮件的发现

基于电子邮件的发现服务允许最终用户使用其电子邮件地址自动登录。他们无需提供应用商店 URL。
要为云应用商店启用此服务，您需要执行以下步骤。

1. 声明域
2. 创建域到 URL 的映射

声明域

要声明域，请执行以下操作：

1. 转到 https://adsui.cloud.com。
2. 导航到声明 > 域 > 添加域。
3. 输入您想要声明的域（例如，ace.example.com）。
4. 单击确认。
5. 复制屏幕上显示的 DNS 令牌。
6. 要创建 DNS TXT 记录，请转到服务提供商门户并添加 DNS 令牌。
7. 要开始验证过程，请执行以下操作：
    a) 导航到声明 > 域。
    b) 转到您添加的域名，然后单击省略号菜单。
    c) 选择“验证域”。
    d) 单击“开始 **DNS** 检查”。

验证完成后，您的域名状态将从“待处理”更改为“
已验证”。

创建域到 **URL** 的映射

1. 导航到声明 > 域。
2. 转到您添加的域名，然后单击省略号菜单。
3. 单击“添加其他服务器 **URL**”。
4. 输入您要映射到此域的应用商店 URL。
5. 单击保存。

为本地应用商店配置设置

November 26, 2023

概述

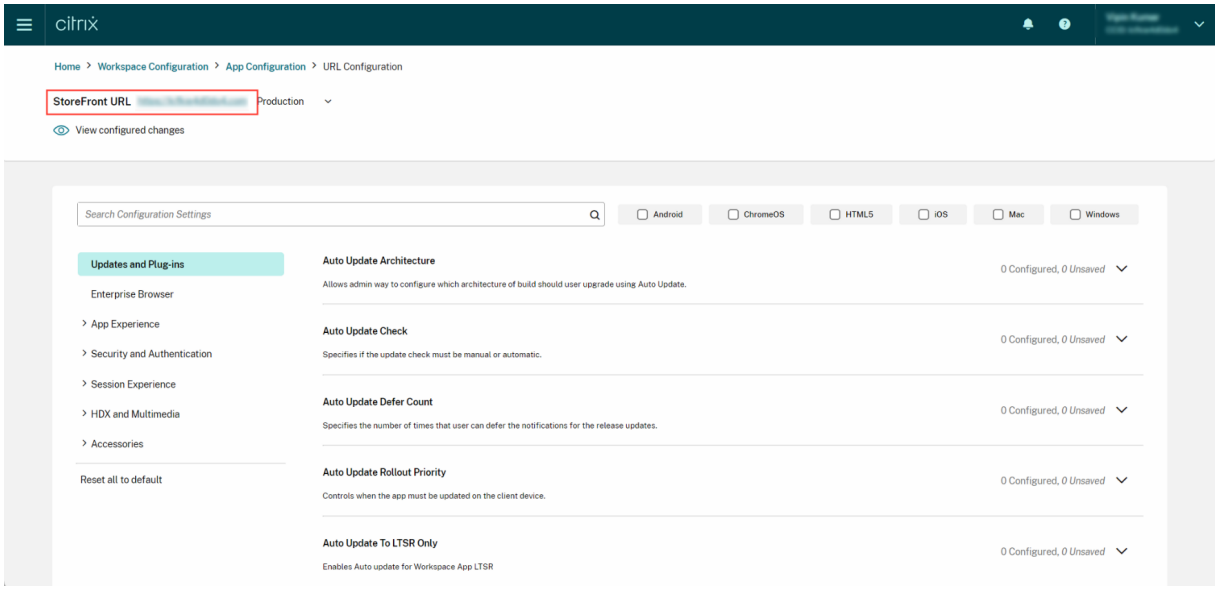
您可以使用 Global App Configuration Service (GACS) 为本地应用商店配置 Citrix Workspace 应用程序设置。它可以帮助您在托管和非托管设备上为最终用户配置和管理 Citrix Workspace 应用程序。Windows、Mac、Android、iOS、HTML5 和 ChromeOS 平台支持 Global App Configuration Service。

必备条件

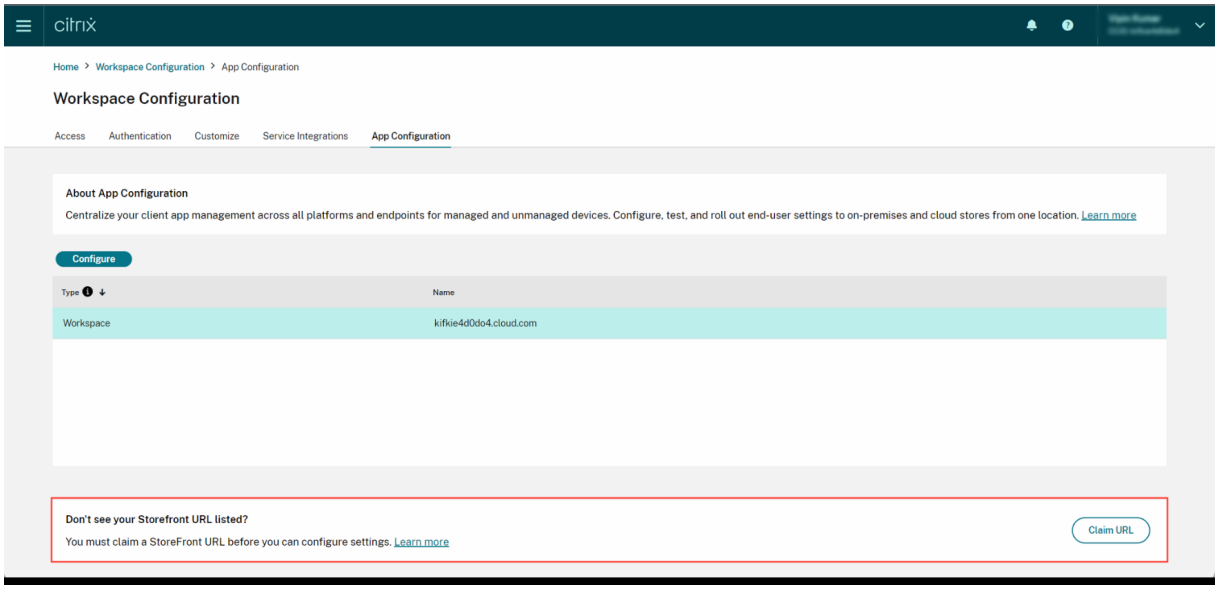
- 地址 https://discovery.cem.cloud.us 必须可访问。这是基于电子邮件的发现和 Global App Configuration Service 正常运行所必需的。
- 确认您有权访问 Citrix Cloud 帐户。如果您还没有帐户，则可以从 https://onboarding.cloud.com/ 中创建一个。有关更多信息，请参阅注册 Citrix Cloud。
- 在本地环境中，必须先声明 URL，然后才能配置设置。有关更多信息，请参阅声明 URL。

入门

要配置本地存储的设置，请登录您的 Citrix Cloud 帐户并导航到 **Workspace** 配置 > 应用程序配置。
如果您声称自己的 StoreFront URL 拥有所有权，则会出现以下屏幕，您可以在其中开始配置设置。有关更多信息，请参阅配置设置部分。



如果您尚未声称自己的 StoreFront URL 的所有权，则会出现以下屏幕，提示您在继续操作之前保护您的 URL。有关更多信息，请参阅为本地商店声明 URL。



声明本地应用商店的 **URL**

在开始为 URL 配置设置之前，必须对 URL 进行声明。

要声明 URL，请执行以下操作：

1. 前往 https://adsui.cloud.com/url 并使用您的 Citrix Cloud 凭据登录。
2. 导航到声明 > **URL** > 添加 **URL**。
3. 输入您要声明的 URL。
4. 单击确认。出现验证弹出窗口。

   > 注意：
   >
   > 如果本地环境未安装 NetScaler Gateway，则您将无法执行验证过程（从步骤 5 开始）。在这种情况下，请按照前面的步骤执行步骤 1 到 4，并联系我们的支持团队，告知您的客户 ID 和您要声明的 URL。

5. 如果您在本地设置中安装了 NetScaler Gateway，则可以使用以下步骤验证您的 URL。

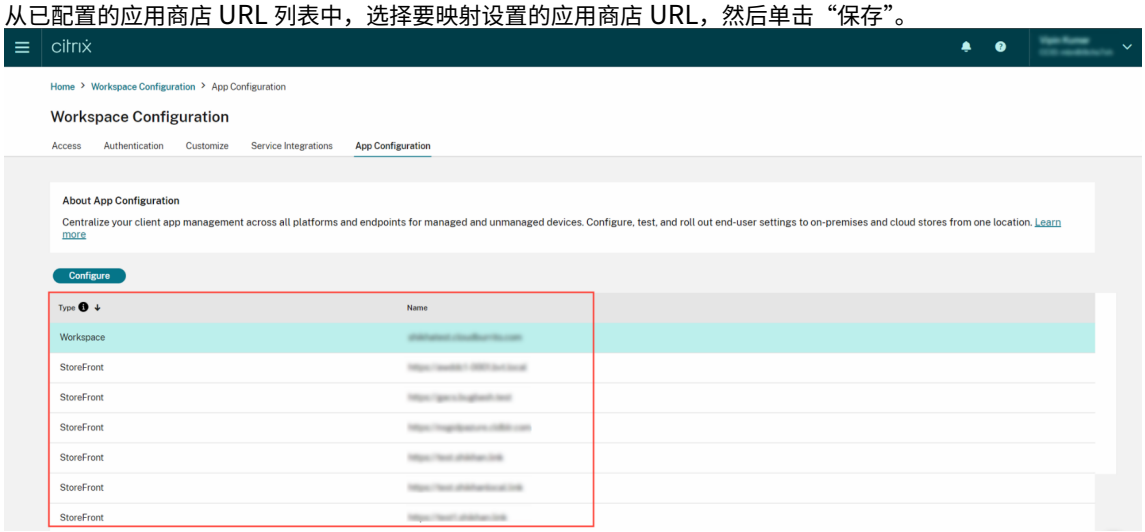
   a) 复制弹出窗口中显示的令牌。
   b) 在 Citrix ADC 中创建和配置响应者操作和响应者策略。
   c) 在全球范围内绑定您的响应者政策。
   d) 转至 `https://<customergatewayurl>/vpn/CitrixClaims` 验证您的响应者策略配置是否正确。
   e) 返回声明 > **URL**，找到您添加的 URL。
   f) 单击已添加 URL 的省略号菜单图标。
   g) 选择“验证 **URL**”。
   h) 单击“开始声明检查”以开始验证过程。

配置完成后，您的域名状态将从“待处理”更改为“已验证”。

配置设置

声明 URL 后，您可以配置 Citrix Workspace 应用程序的设置。如果已为贵公司配置了多个应用商店，则可以分别为每个应用商店配置设置。

1. 前往 Citrix Cloud 门户并使用您的证书登录。
2. 导航到 **Workspace** 配置 > 应用程序配置。
3. 单击“切换 **URL**”以选择要为其配置设置的应用商店。
4. 从已配置的应用商店 URL 列表中，选择要映射设置的应用商店 URL，然后单击“保存”。



5. 根据您的要求修改首选平台的设置。
6. 单击“发布草稿”以保存设置。

> 注意：
>
> 可能需要几个小时才能将设置更新到 Citrix Workspace 应用程序客户端。有关更多信息，请参阅获取更新设置的频率。

设置基于电子邮件的发现

基于电子邮件的发现服务允许最终用户使用其电子邮件地址自动登录。他们无需提供应用商店 URL。
要为云应用商店启用此服务，您需要执行以下步骤。

1. 声明域
2. 创建域到 URL 的映射

声明域

要声明域，请执行以下操作：

1. 转到 自动发现服务。
2. 导航到声明 > 域 > 添加域。
3. 输入您想要声明的域（例如 ace.example.com）。
4. 单击确认。
5. 将屏幕上显示的 DNS 令牌复制到剪贴板。
6. 要创建 DNS TXT 记录，请转到服务提供商门户并添加 DNS 令牌。
7. 要开始验证过程，请执行以下操作：
    a) 导航到声明 > 域。
    b) 转到您添加的域名，然后单击省略号菜单。
    c) 选择“验证域”。
    d) 单击“开始 **DNS** 检查”。

验证完成后，您的域名状态将从“待处理”更改为“已验证”。

> 注意：
>
> 您最多可以声明 10 个域名。如果您想申请超过 10 个域名，请联系 Citrix 支持并提供您的客户 ID 和 URL。

创建域到 **URL** 的映射

1. 导航到声明 > 域。
2. 转到您添加的域名，然后单击省略号菜单。
3. 单击“添加其他服务器 **URL**”。
4. 输入您要映射到此域的应用商店 URL 并保存。

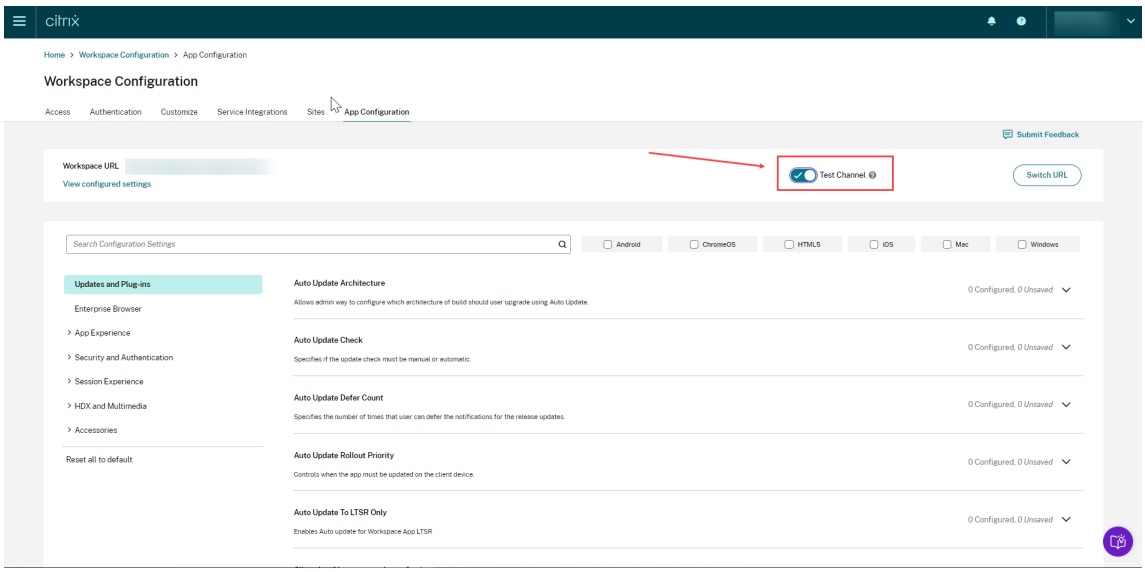
测试频道配置

November 26, 2023

在为最终用户启用配置之前，您可以测试您的配置。它可以帮助您检测和解决部署后可能出现的任何问题。
测试功能显著降低了部署过程中出现中断或错误的可能性，并提高了整体用户满意度。
要测试您的配置，请执行以下操作：

1. 转到云门户并使用您的 Citrix Cloud 凭据登录。

2. 导航到 **Workspace** 配置 > 应用程序配置。
3. 将切换开关切换到 测试频道。默认情况下，它设置为“生产”。



4. 根据您的要求修改首选平台的设置。
5. 然后，您可以单击“发布草稿”以在测试频道中发布您的设置。

> 注意：
>
> Global App Configuration Service 仅支持每个商店两个通道，一个是生产通道（默认），一个是测试通道。

在最终用户设备上配置频道支持

Windows

要测试管理员在 Windows 设备上定义的配置，用户需要创建以下注册表。

```
    Path- HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
    Name- AppConfigChannelName
    Type- REG_SZ
    Value- testrolloutchannel1

<!--NeedCopy-->
```

Mac

要在 Mac 设备上测试管理员定义的配置，用户需要执行以下步骤。

1. 使用以下命令设置 Global App Configuration Service 测试通道的名称：


```
defaults write com.citrix.receiver.nomas GACSChannelName
    testrolloutchannel1

<!--NeedCopy-->
```

2. 使用以下命令重新启动 Citrix Workspace Helper：

```
launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.
    plist

launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.
    plist

<!--NeedCopy-->
```

设备重新启动后，将自动获取测试通道的配置。

iOS

要在 iOS 设备上测试管理员定义的配置，请按以下步骤操作。

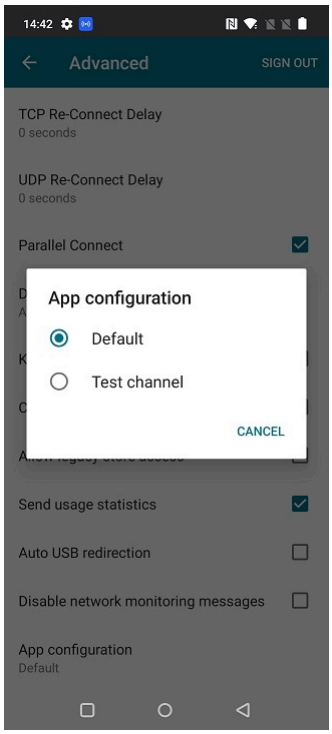
1. 登录 Citrix Workspace 应用程序。
2. 前往“设置”>“高级”>“应用程序配置”。
3. 选择测试频道。
4. 现在，您可以测试管理员定义的配置。

（测试频道）

Android

要在 Android 设备上测试管理员定义的配置，请按以下步骤操作。

1. 登录 Citrix Workspace 应用程序。
2. 前往“设置”**>**“高级”>“应用程序配置”。
3. 选择测试频道。
4. 现在，您可以测试管理员定义的配置。



（测试频道）

管理您的 **Workspace** 体验

November 26, 2023

本文概述了订阅者如何访问和参与其工作区。它讨论了增强 Workspace 体验的自定义选项，并为常见问题提供了解决方案。

Workspace 访问权限

订阅者可以通过两种方式访问 Citrix Workspace：

- 通过带有工作区 URL 的浏览器。

- 使用安装在订阅者设备上的 Citrix Workspace 应用程序。

浏览器访问权限

订阅者在通过浏览器登录时必须使用最新版本的 Edge、Chrome、Firefox 或 Safari。用户可以输入他们的 Workspace URL 来访问他们的工作区。有关更多信息，请参阅 Workspace Browser 兼容性。

默认情况下，工作区 URL 处于启用状态，格式通常为：`https://yourcompanyname.cloud.com`。有关配置 Workspace URL 的信息，请参阅 Workspace URL。

Citrix Workspace 应用程序访问权限

Citrix 建议使用最新版本的 Citrix Workspace 应用程序访问工作区。

Citrix Workspace 应用程序是本机安装的应用程序，它取代了 Citrix Receiver，可跨平台提供一致的 Workspace 用户界面 (UI) 用户体验。Citrix Workspace 应用程序适用于各种操作系统。有关详细信息，请参阅 Citrix Workspace 应用程序 产品文档。

如果您一直在使用 Citrix Receiver，请指导用户升级到 Citrix Workspace 应用程序，以便他们可以使用所有 Workspace 用户界面功能。有关各平台的 Citrix Workspace 应用所支持功能的更多信息，请参阅 Workspace 应用功能列表。

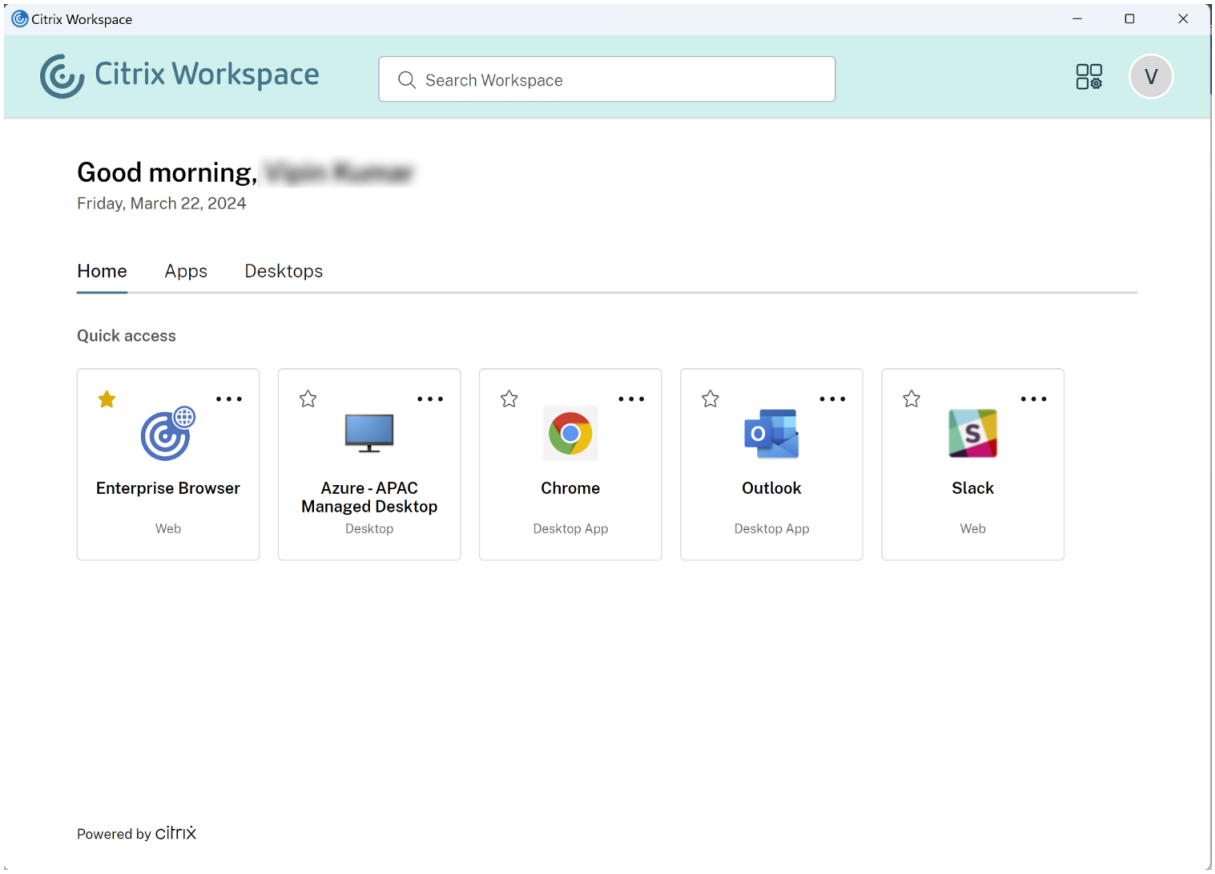
有关如何安装 Citrix Workspace 应用程序的信息，请访问 下载 Citrix Workspace 应用程序。

对于无法安装 Citrix Workspace 应用程序软件的设备，适用于 HTML5 的 Citrix Workspace 应用程序通过兼容 HTML5 的浏览器提供连接。

Workspace 用户界面和功能

新客户。如果您不熟悉 Workspace 体验，订阅者可以在用户界面可用时获得最新版本。

现有客户。如果您使用的是早期版本的 Citrix Workspace 应用程序，则更新后的用户界面可能需要大约五分钟才能显示。您可能会暂时看到旧版本的 UI。



Citrix Workspace 用户界面包含以下功能：

单点登录 **(SSO)**

Citrix Workspace 提供对辅助资源的单点登录 (SSO) 的无缝体验，否则需要其他形式的身份验证。

卡布局

应用程序、桌面、文件、操作和 活动源 以“卡片”布局显示。弹出窗口显示更多详细信息和操作。

设置

订阅者通过选择 Workspace UI 右上角的配置文件图标时出现的菜单访问“设置”。

配置文件图标

订阅者可以将照片上载到他们的配置文件。如果未设置个人头像，则图像默认为基于订阅者的 Active Directory 显示名称的图标。

搜索

用户界面顶部的搜索工具可搜索工作区中的所有资源，并允许订阅者直接从搜索结果中打开应用程序。搜索至少需要三个字符。

“最近”和“收藏夹”视图

订阅者可以在应用程序、桌面和文件的“最 近”和“收藏夹”视图之间进行选择。

您可以配置“收藏夹”，以便在 Works **pace** 配置中将此功能设置为可供订阅者使用或不可用。有关在 Citrix Workspace 中启用和禁用“收藏夹”功能的详细信息，请参阅 允许收藏夹。

双重身份验证（可选）

订阅者必须先注册其设备，然后才能在 Citrix Workspace 中使用双重身份验证。在注册过程中，Workspace 会显示一个二维码，供订阅者使用身份验证应用程序进行扫描。身份验证应用程序必须遵循 基于时间的一次性密码 (TOTP) 标准，例如 Citrix SSO。

> 注意：
>
> 为了顺利完成注册过程，Citrix 建议事先在目标设备上下载并安装 Citrix SSO 。

要注册双重身份验证，请引导订阅者：

1. 打开浏览器，导航到 Workspace 登录页面，然后选择 没有令牌?
2. 按 `domain\username` 格式输入用户名或公司电子邮件地址，然后选择“下一步”。然后，Citrix Cloud 会向订阅者发送一封包含临时验证码的电子邮件。
3. 出现提示时输入验证码和 Active Directory 帐户密码，然后选择“下一步”。

   > 重要：
   >
   > 验证码是一个临时令牌，有效期为 24 小时，仅用于注册用户的设备。订阅者不得使用此代码通过双重身份验证登录其工作区。

4. 在身份验证器应用程序中，扫描二维码或手动输入验证码。
5. 选择“完成 并 登录”以完成注册。

完成注册后，订阅者可以返回 Citrix Workspace 登录页面，输入其 Active Directory 凭据以及身份验证应用程序中显示的令牌。

只有从已注册设备上的身份验证应用程序生成的验证码才是支持双重身份验证的令牌。订阅者不得使用注册过程中发送的临时电子邮件令牌。

自定义工作区

您可以在 Workspace 配置中为不同用户自定义工作区的订阅者体验，以满足特定的组织要求。

- 要在工作区的 活动源 和 操作 卡中配置定向通知，请访问 自定义工作区通知。
- 要自定义工作区的外观（包括徽标和自定义主题），请访问 自定义工作区的外观。
- 要选择订阅者与其工作区的交互方式，例如允许订阅者创建收藏夹和自动启动桌面，请访问自定义工作区交互。
- 要自定义隐私和安全策略，请参阅自定义安全和隐私策略。隐私和安全策略包括超时时间、登录策略和最终用户的密码管理等设置。

故障排除

更改身份验证方法后注销并重新登录

更改身份验证方法后，登录的订阅者可能会看到一条错误消息。订阅者必须注销 Citrix Workspace 并关闭浏览器或 Citrix Workspace 应用程序，然后等待大约 5 分钟才能再次登录。然后，订阅者可以使用新的身份验证方法登录。

有关更多信息，请访问 选择或更改身份验证方法。

更改服务订阅后刷新

如果您已更改服务订阅，则订阅者可能需要手动刷新本地 Citrix Workspace 应用程序。要刷新适用于 Windows 的 Citrix Workspace 应用程序，请执行以下操作：

1. 右键单击 Windows 系统托盘中的 Citrix Workspace 图标，然后选择 高级首选项 **>** 重置 **Citrix Workspace**。
2. 打开适用于 Windows 的 Citrix Workspace 应用程序并选择 帐户 **>** 添加。
3. 输入工作区 URL，然后选择 添加。

您也可以通过浏览器刷新 Citrix Workspace 应用程序。如果从浏览器刷新：

1. 右键单击 Windows 系统托盘中的 Citrix Workspace 图标，然后选择 高级首选项 **>** 重置 **Citrix Workspace**。
2. 在浏览器中输入 Workspace URL 并登录。
3. 从“设置” **>** “帐户设置” **>** “高级” **>** “下载 **Workspace** 配置” 下载配置文件。

这将下载一个扩展名为 **.cr** 的文件，该文件将工作区添加到您的本地 Citrix Workspace 应用程序。

自定义工作区的外观

November 26, 2023

自定义 **Workspace** 用户界面

本节介绍如何通过更新配置 **>** 自定义 **>** 外观中的主题来自定义工作区的外观。

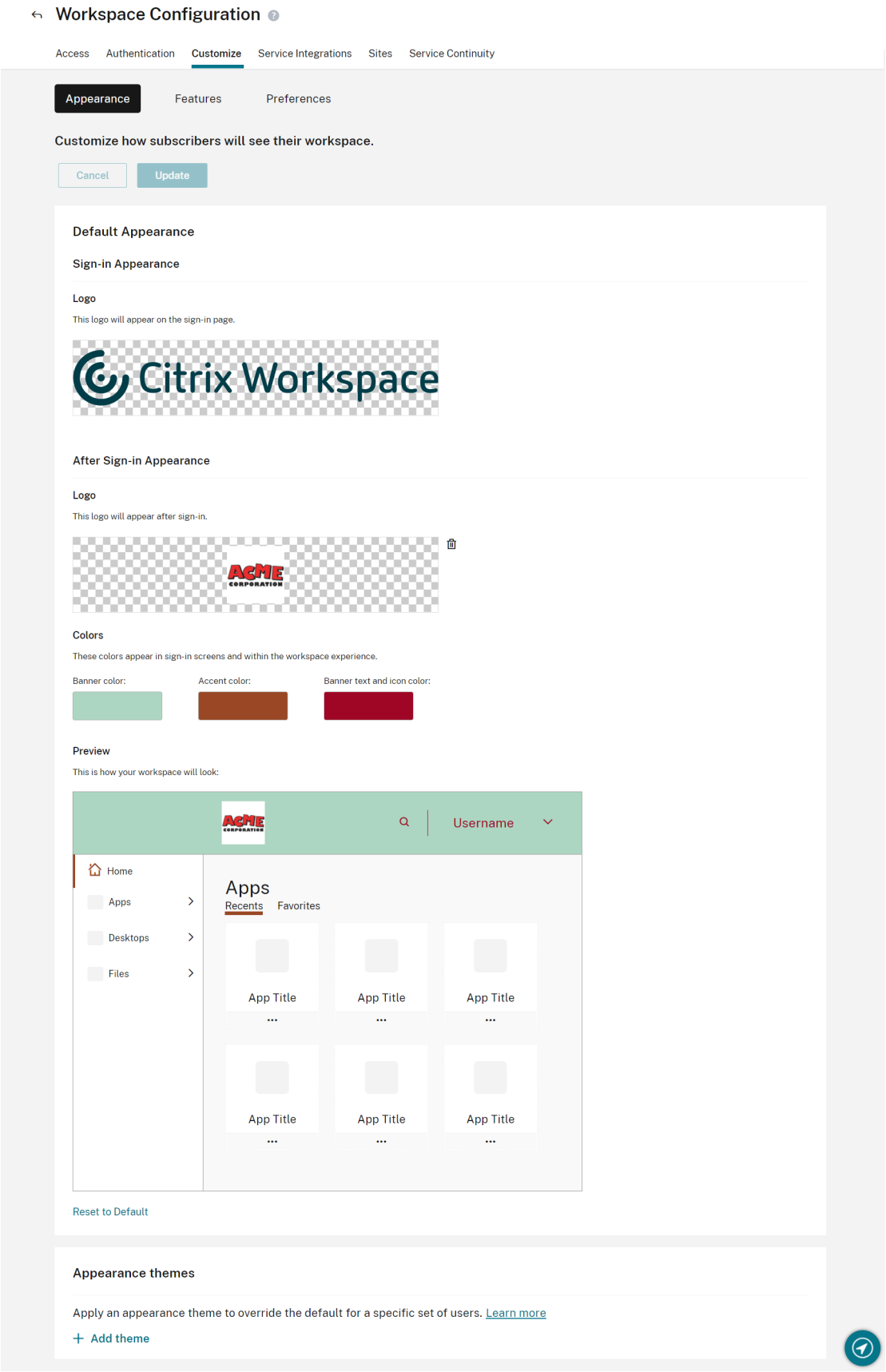
主题允许您配置工作区颜色和徽标。徽标必须符合要求的尺寸，以免出现扭曲或导致错误信息。

徽标	必需的尺寸	最大尺寸	支持的格式
登录徽标	480 x 120 像素	2 MB	JPEG、JPG 或 PNG
登录后徽标	340 x 80 像素	2 MB	JPEG、JPG 或 PNG

选择“保存”后，对工作区外观所做的更改会立即生效。

自定义您的默认主题

默认主题包括登录徽标、工作区徽标以及订阅者在登录后看到的颜色。您可以为默认主题更改其中一个、部分或全部元素。



自定义登录外观

对于登录页面，您只能替换徽标。登录页面的其余部分（包括颜色）不受影响。

对工作区外观所做的更改将立即生效。更新后的用户界面可能需要大约五分钟才能在本地 Citrix Receiver 应用程序中显示。

> 注意：
>
> 登录徽标的更改不会影响使用第三方身份提供商（如 Azure AD 和 Okta）对其工作区进行身份验证的用户。
>
> 有关如何自定义 Azure AD 登录页面的信息，请参阅 Microsoft 文档。有关如何自定义 Okta 托管的登录页面的信息，请参阅 Okta 开发者文档。

您还可以自定义在 Citrix ADC 设备而不是 **Workspace** 配置中配置的本地 Citrix Gateway 登录页面。有关更多信息，请参阅 支持知识中心文章。

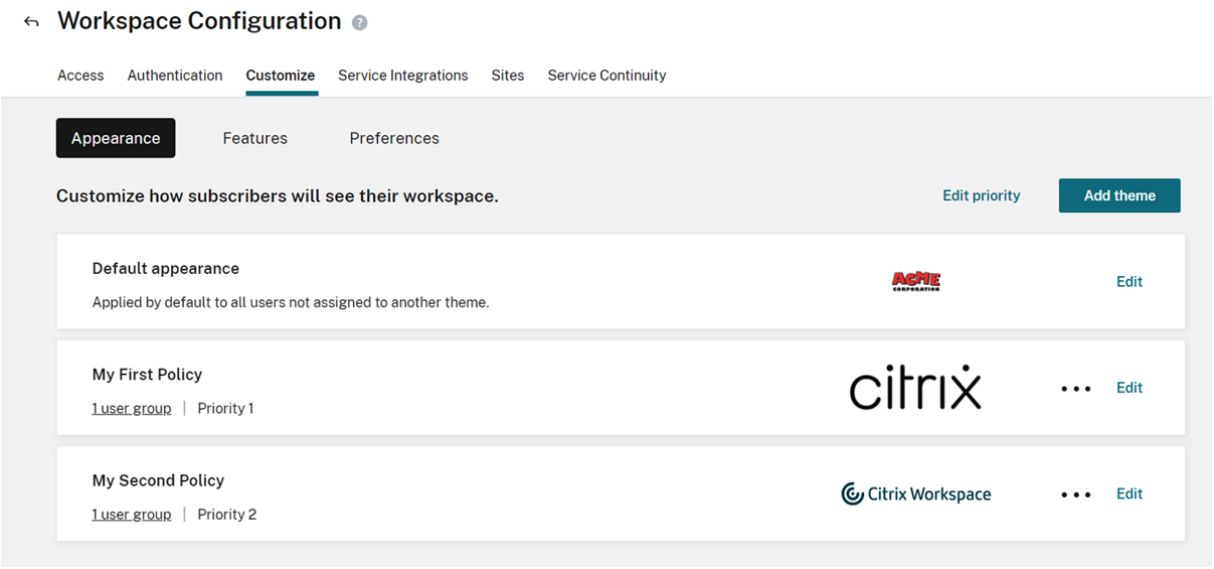
自定义工作区外观

登录徽标不必与订阅者登录后出现在工作区左上角的徽标相同。除了替换工作区徽标外，您还可以定义工作区的横幅、重音以及文本和图标颜色。

创建多个自定义主题

> 重要：
>
> 这是一项 单租户功能。如果您的客户是 Citrix Service Provider 租户，则它必须拥有自己的资源位置、Cloud Connector 和专用 Active Directory 域。目前不支持共享资源位置、Cloud Connector 和专用 Active Directory 域（多租户）的 Citrix Service Provider 租户。

您可以为特定用户组配置多个 Citrix Workspace 主题并确定其优先级。这些自定义主题在默认主题下的单个卡片中列出。如果未设置多个主题，则现有（默认）主题将应用于所有用户。



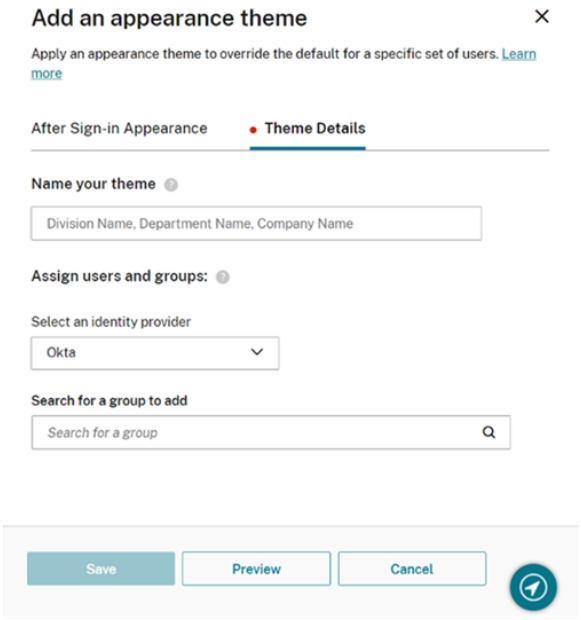
配置自定义主题

要在默认主题下添加您的第一个自定义主题，请选择卡片左下角的默认外观部分下的添加主题。

如果您已经在默认主题下至少有一个自定义主题，请选择现有 主题列表右上角的添加 主题。

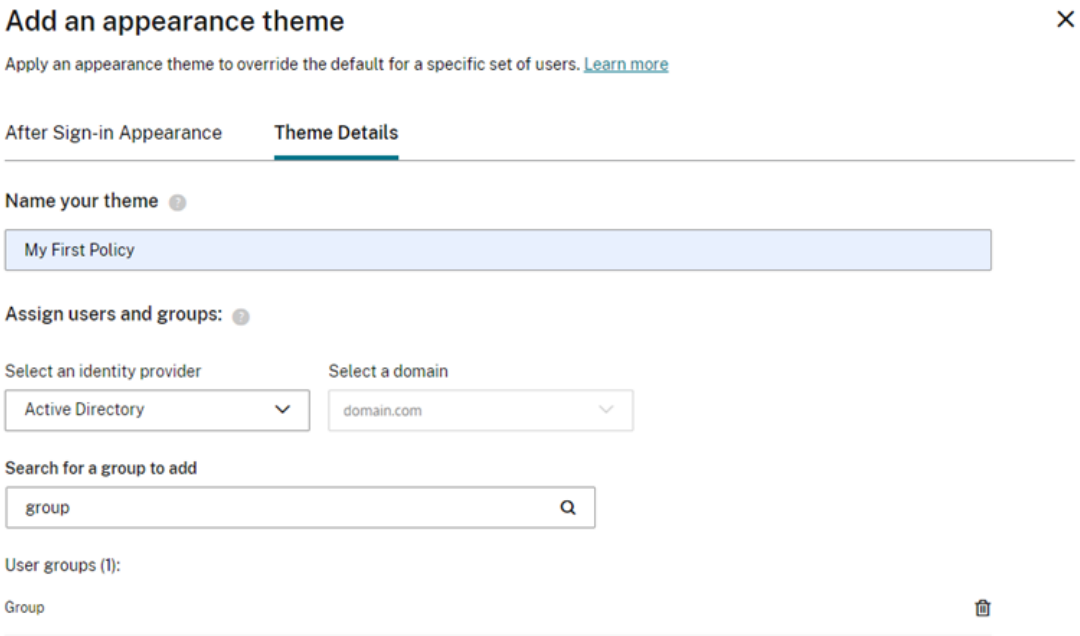
1. 配置您的自定义主题：
    a) 上载您的 徽标（可选）。
    b) 定义横幅、口音、文字和图标 颜色（可选）。

2. 选择主题详细信息并为该主题输入一个有意义的名称。



3. 将用户组分配给主题：

   a) 如果出现提示，请选择身份提供商及其域。
   b) 搜索要添加到自定义主题的用户组。
   c) 选择该组旁边的加号 (+) 按钮。
   d) 对要添加到模版的每个组重复此过程。



4. 选择“预览”以查看订阅者对您的工作区的看法。完成后保存您的模版。

   > 注意：
   >
   > 如果您当前使用的是较旧的紫色用户界面，则 **Workspace** 预览不会显示预览。

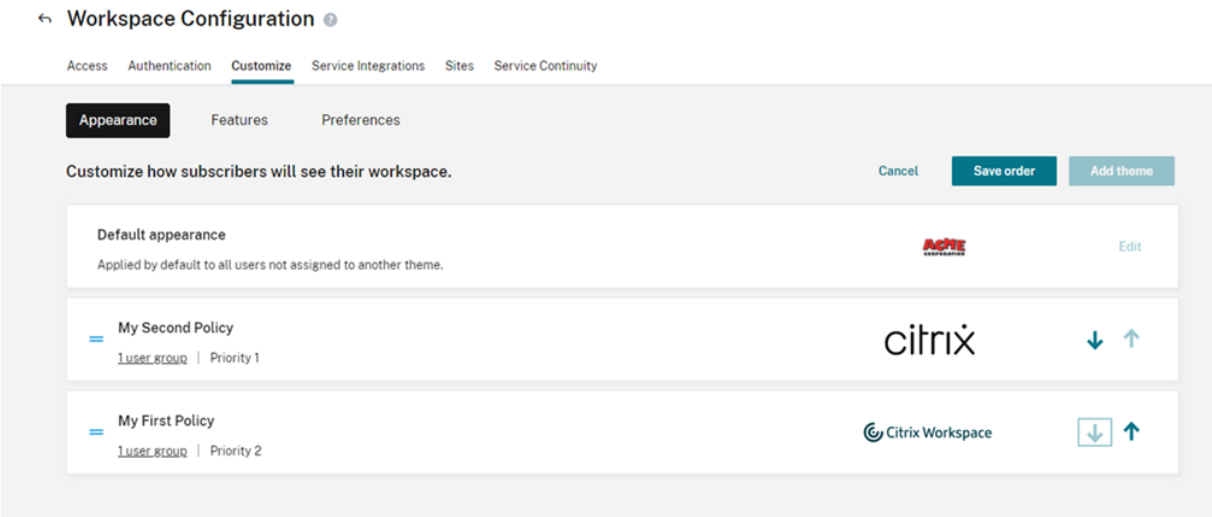
5. 重复步骤 1 到 4 以继续添加新的自定义主题。

优先考虑自定义主题

一个用户可能属于多个用户组，每个用户组可能与不同的主题匹配。您可以通过设置自定义主题相对于彼此的优先级，来定义订阅者在与多个主题匹配时看到哪个主题。

> 重要提示
>
> 要使自定义主题的相对优先级发挥作用，必须在默认主题下配置两个或多个自定义主题。

1. 选择主题列表右上角的“添加主题”旁边的“编辑优先级”。
2. 您可以通过以下两种方式之一对主题的优先级进行重新排序：
   - 使用每个主题右侧的箭头。
   - 使用卡片左侧的手柄在列表中上下拖动单个主题。
3. 重新订购商品后，选择 保存订单。



自定义工作区互动

November 26, 2023

在“**Workspace** 配置”**>**“自定义”**>**“首选项”中自定义订阅者与其工作区的交互方式。

如果要自定义影响登录体验的 Workspace 首选项以符合贵公司的要求，请访问自定义工作区安全和隐私策略。

如果要自定义登录前和登录后工作区外观，请访问 自定义工作区的外观

允许缓存

允许缓存设置可提高通过 Web 浏览器访问 Citrix Workspace 的订阅者的性能。使用支持的 Web 浏览器访问 Citrix Workspace 时，支持缓存。使用本地安装的 Citrix Workspace 应用程序时，缓存不可用。

启用缓存后，某些敏感数据可能会本地存储在用户的设备上。此数据由文件元数据组成，并使用订阅者经过身份验证的身份所独有的密钥进行加密。加密的数据存储在订阅者设备上的 Web 浏览器 `localStorage` 属性中。

如果禁用缓存，则订阅者下次通过其 Web 浏览器登录 Citrix Workspace 时将清除加密数据。此外，订阅者可以通过清除其 Web 浏览器中的浏览数据来手动清除这些数据。

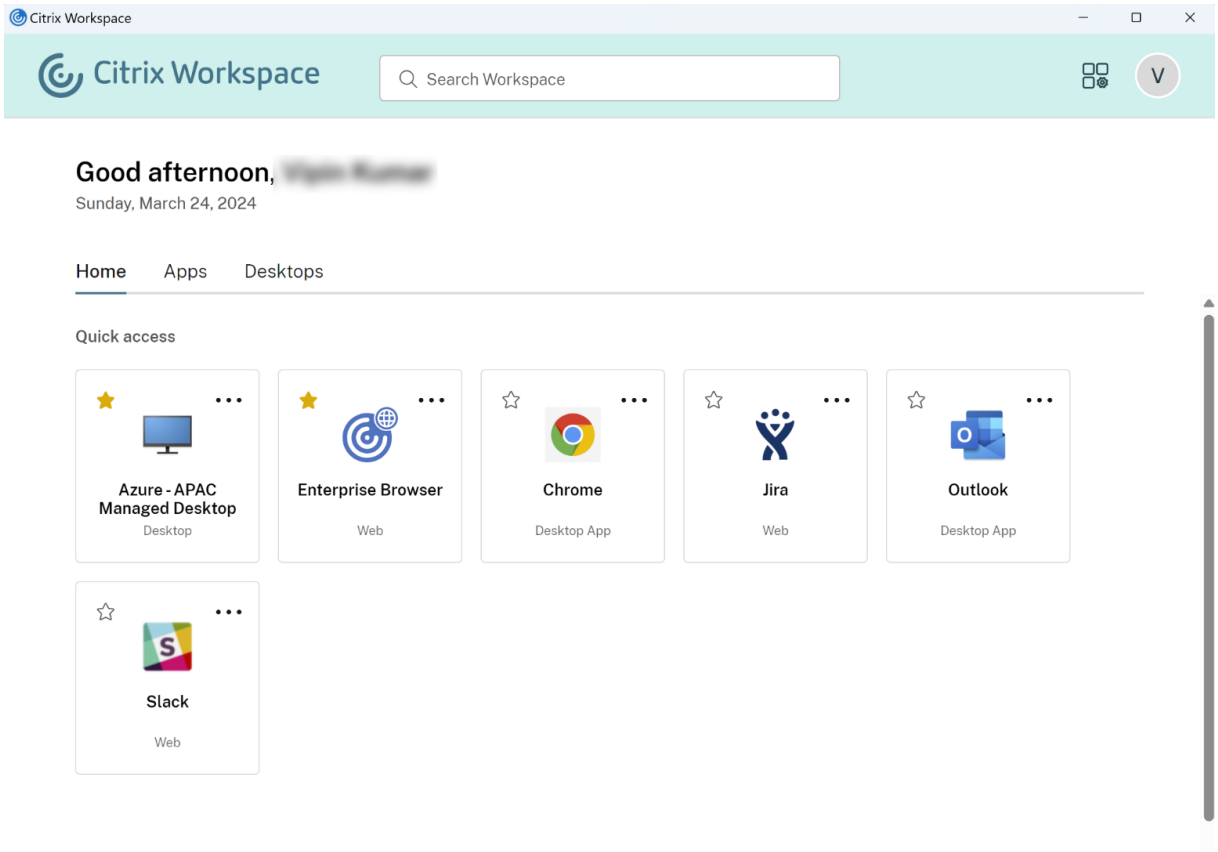
允许收藏

有权访问 **Workspace** 配置 和全新 Workspace 体验的客户可以允许订阅者访问收藏和取消收藏的应用程序和桌面资源。默认情况下，“允许收藏夹”功能处于启用状态。

> 注意：
>
> - 对于一些现有客户（在 2017 年 12 月至 2018 年 4 月期间新使用 Workspace），“允许收藏夹”默认为“禁用”。管理员可以决定何时为其订阅者启用此功能。

允许收藏的订阅者体验

启用（默认）后，订阅者可以使用每张（非强制性）应用程序和桌面卡片左上角的星形图标添加最多 250 个 收藏夹。当星星被收藏时，它会从没有填充变为黄色填充。



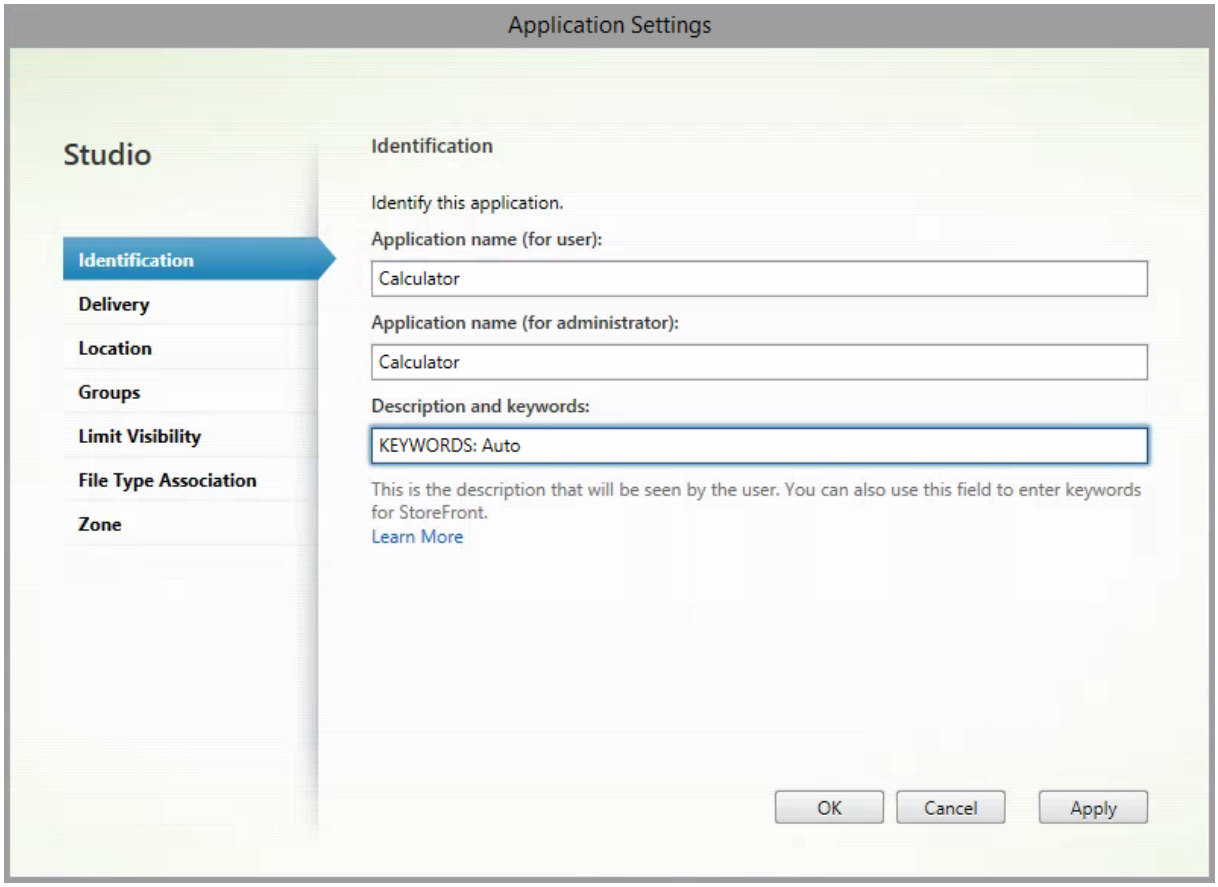
如果订阅者收藏的资源超过 250 个，则“最早的收藏夹”将被删除（或尽可能接近以保留最新的 收藏夹）。

禁用后，Workspace 订阅者看不到应用程序和桌面卡片上的星号，也看不到导航栏中这些资源的“所有应用程序 和 收藏夹”子菜单。应用程序和桌面 收藏夹 不会被删除，如果您重新启用“收藏夹”，则可以恢复。

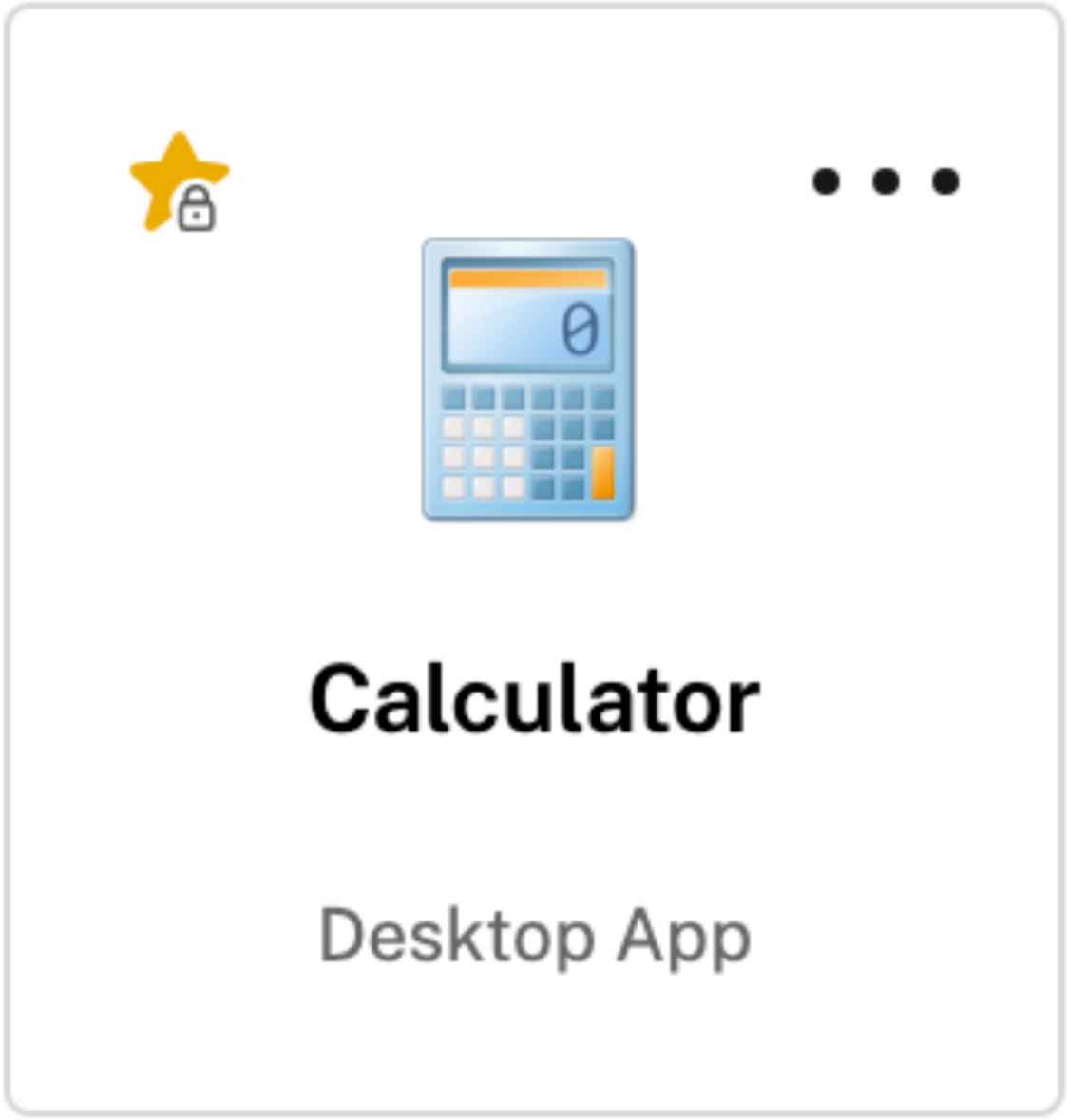
> 注意：
>
> 如果您的订阅者无法访问已配置的桌面，则不会显示侧栏中的桌面选项。

应用程序和桌面关键词

管理员可以使用 Citrix DaaS 中的 `KEYWORDS:Auto` 和 `KEYWORDS:Mandatory` 设置（管理 > 完整配置 > 应用程序）自动为订阅者添加收藏应用程序。



- **KEYWORDS:Auto**。应用程序或桌面将添加为 收藏夹，订阅者可以移除 收藏夹。
- **KEYWORDS:Mandatory**。应用程序或桌面已添加为 收藏夹，订阅者无法移除 收藏夹。强制性应用程序和桌面会显示一个带挂锁的星形图标，表示它不能被取消收藏。



> 注意：
>
> 如果您对应用程序同时使用“必选”和“自动”关键字，则“必选”关键字会覆盖“自动”关键字，并且无法删除收藏的应用程序或桌面。

对于只能访问具有“必选”关键字的应用程序和桌面的订阅者：

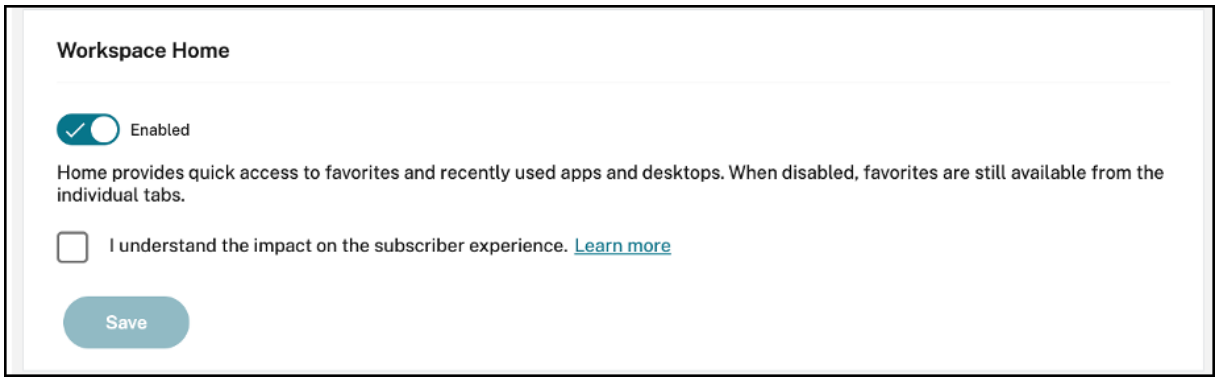
- 订阅者只能在 Workspace 的左侧导航窗格中看到 应用程序 页面。收藏夹页面不显示在左侧窗格中，因为应用程序页面和收藏页面上显示的应用程序没有区别。
- 订阅者在主页上看不到“收藏夹”选项卡。仅显示“最近”选项卡。

为用户启用或禁用主屏幕（预览）

您可以为用户启用或禁用 主页，以改善其应用程序的组织。

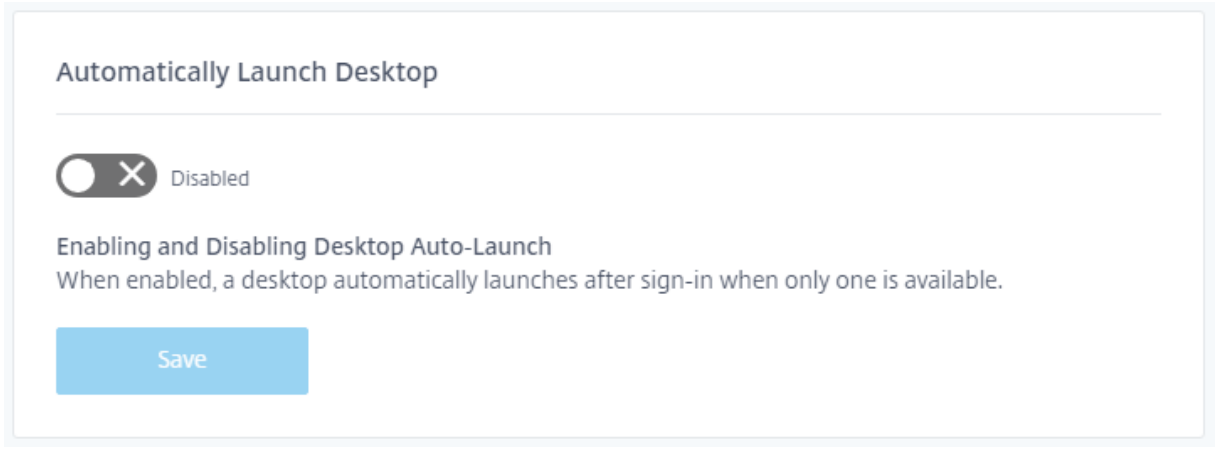
当用户的桌面上有超过 20 个应用程序时，此功能适用。如果用户有 20 个或更少的应用程序，则他们将看到一个没有导航和搜索选项的视图。

要配置设置，请转到 **Workspace** 配置 **>** 自定义 **>** 外观。开启切换后，用户将被导航到 主页。如果您关闭开关，则用户将直接进入 应用程序 页面。默认情况下，开关处于开启状态且该功能处于启用状态。



自动启动桌面

自动启动桌面适用于有权访问 **Workspace** 配置和全新 Workspace 体验的客户。该首选项仅适用于从浏览器访问工作区。



禁用时（默认），该设置会阻止 Citrix Workspace 在订阅者登录时自动启动桌面。订阅者必须在登录后手动启动桌面。

启用后，如果订阅者只有一个可用的桌面，则该桌面将在订阅者登录其工作区时自动启动。

不管 Workspace 控制配置如何，订阅者的应用程序都不会重新连接。

> 注意：
>
> 要让 Citrix Workspace 自动启动桌面，通过 Internet Explorer 访问该站点的订阅者必须将 Workspace URL 添加到本地内部网或可信站点区域。

联合身份提供商会话

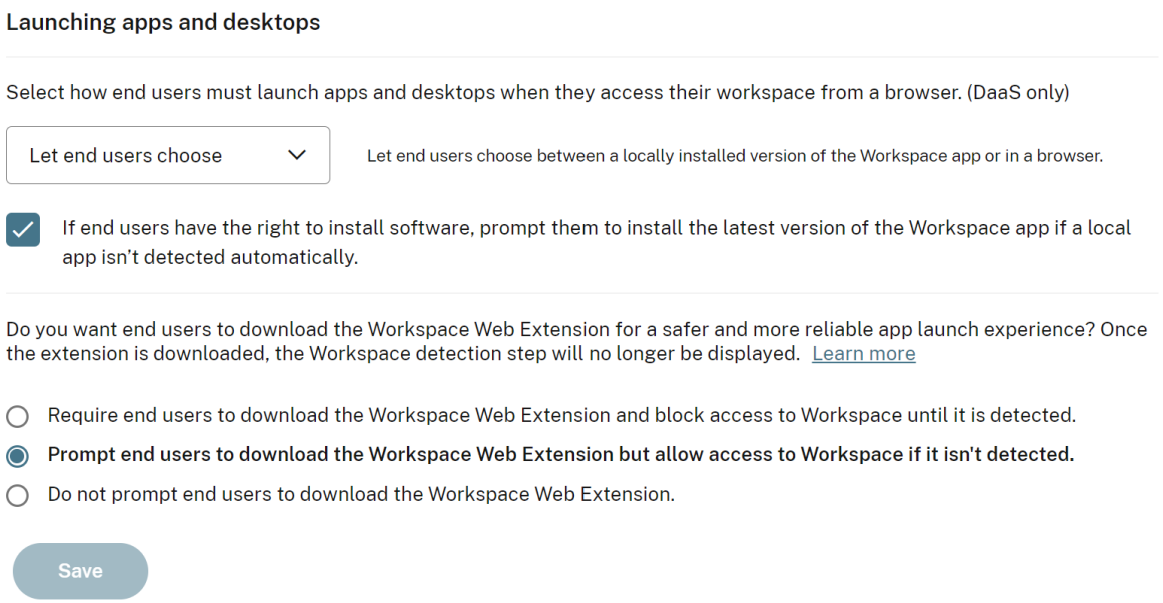
当 Workspace 配置为使用联合身份提供程序时，身份验证会话及其生存期通常由身份提供商控制。联合身份提供商会话 设置允许将控制权移交给服务提供商。启用（默认）后，当需要新的 Workspace 会话时，Workspace 会强制向身份提供者发出登录提示。禁用后，如果通过有效会话访问 Workspace，则不会提示订阅者向身份提供者进行身份验证。

如果启用此设置并且您使用 Azure AD 进行工作区身份验证，则即使订阅者的会话存在有效的 Microsoft 身份验证令牌，也可能会提示订阅者再次登录。有关此场景的更多信息，请参阅 CTX253779。

启动应用程序和桌面

有权访问 **Workspace** 配置和全新 Workspace 体验的客户可以使用“启动应用程序和桌面”设置。此首选项适用于新客户和现有客户。但是，此功能的引入不会更改现有客户的任何设置。

该首选项仅适用于用户打开 **Citrix DaaS** 交付的应用程序和桌面的方式。这可以是 **Citrix DaaS** 服务，也可以是站点聚合功能中的本地。例如，启动应用程序和桌面 不适用于 Citrix Gateway 服务交付的 SaaS 应用程序。



选择以下设置之一：

- 在本机应用程序中（默认）：要求最终用户使用本地安装的 Workspace 应用程序版本。
- 在浏览器中：要求最终用户使用适用于 HTML5 的 Workspace 应用程序的浏览器版本。

- 让用户选择：最终用户可以在本地安装的 Workspace 应用程序版本之间进行选择，也可以在浏览器中启动应用程序和桌面。

如果未自动检测到本地应用程序，在本机应用程序中和允许用户选择的另一个选项会提示用户安装最新版本的 Citrix Workspace 应用程序。如果您的订阅者没有安装软件的权限，请删除此选择。

将 **Microsoft Teams** 与工作区集成

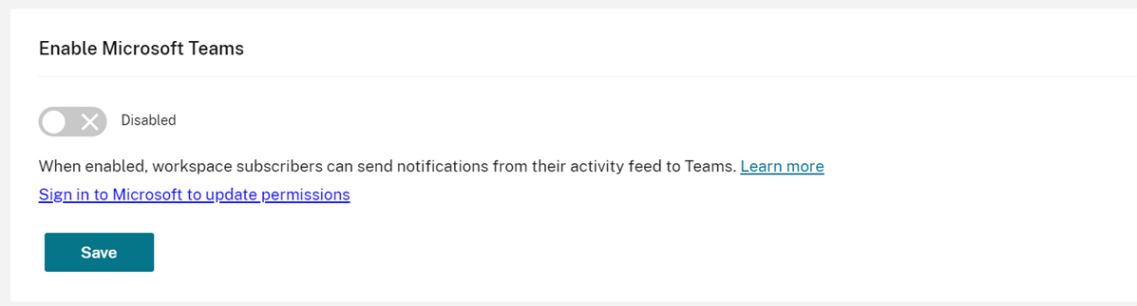
借助 Microsoft Teams 集成，订阅者可以通过 Microsoft Teams 中的渠道与其他订阅者共享其工作区 活动源 中的卡片。

要求

- 您必须是 Citrix Cloud 中的 完全访问 管理员才能启用 Microsoft Teams 集成。具有 自定义访问 权限的管理员没有启用 Microsoft Teams 集成所需的权限。
- 必须在身份 和访问管理中配置 **Azure AD** 身份验证。有关配置 Azure AD 身份验证的更多信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- Microsoft Teams 只能使用一个 Azure AD 实例。如果您配置的 Azure AD 实例已通过其他 Citrix Cloud 帐户启用了 Microsoft Teams，则无法为 Citrix Cloud 帐户启用 Microsoft Teams 集成。
- 必须启用功能切换 **IwsMicrosoftTeams**。
- 必须为工作区启用“操作和活动源”功能。
- Workspace 订阅者必须安装 Microsoft Teams 桌面客户端。

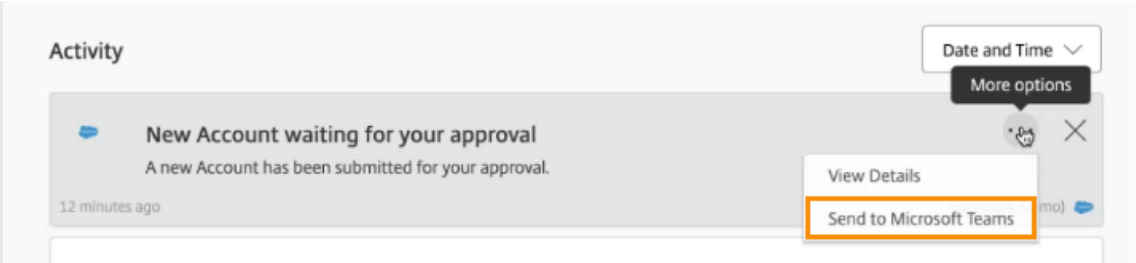
启用 **Microsoft Teams** 集成

1. 登录 Citrix Cloud 后，选择 **Workspace** 配置。
2. 选择“自定义”，然后选择“首选项”选项卡。
3. 在启用 **Microsoft Teams** 下，选择要启用的开关。



4. 选择保存。

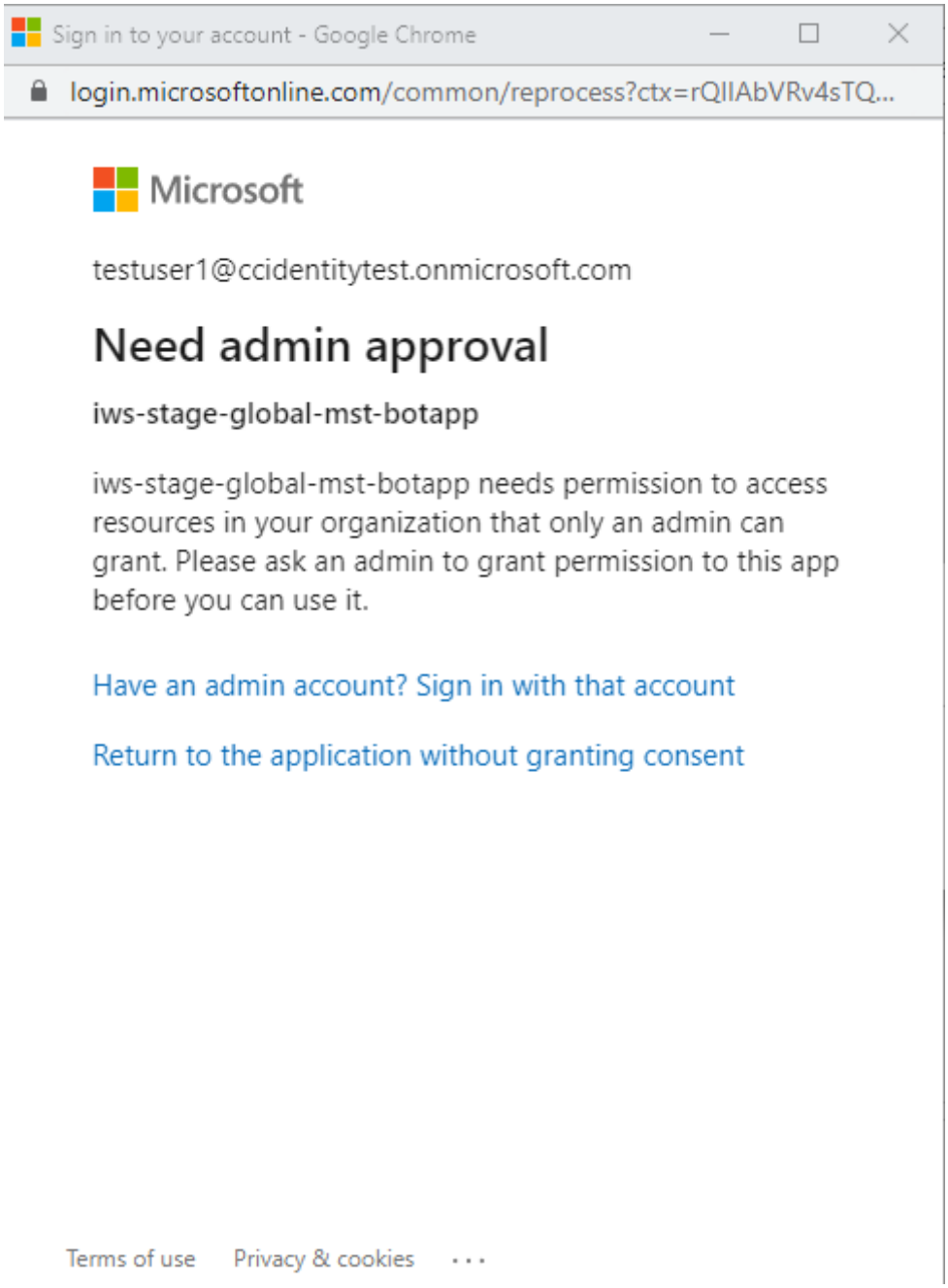
   Workspace 用户现在可以看到发送到 **Microsoft Teams** 选项并从 Workspace 共享卡片。用户可能需要刷新屏幕 (Ctrl+F5)。



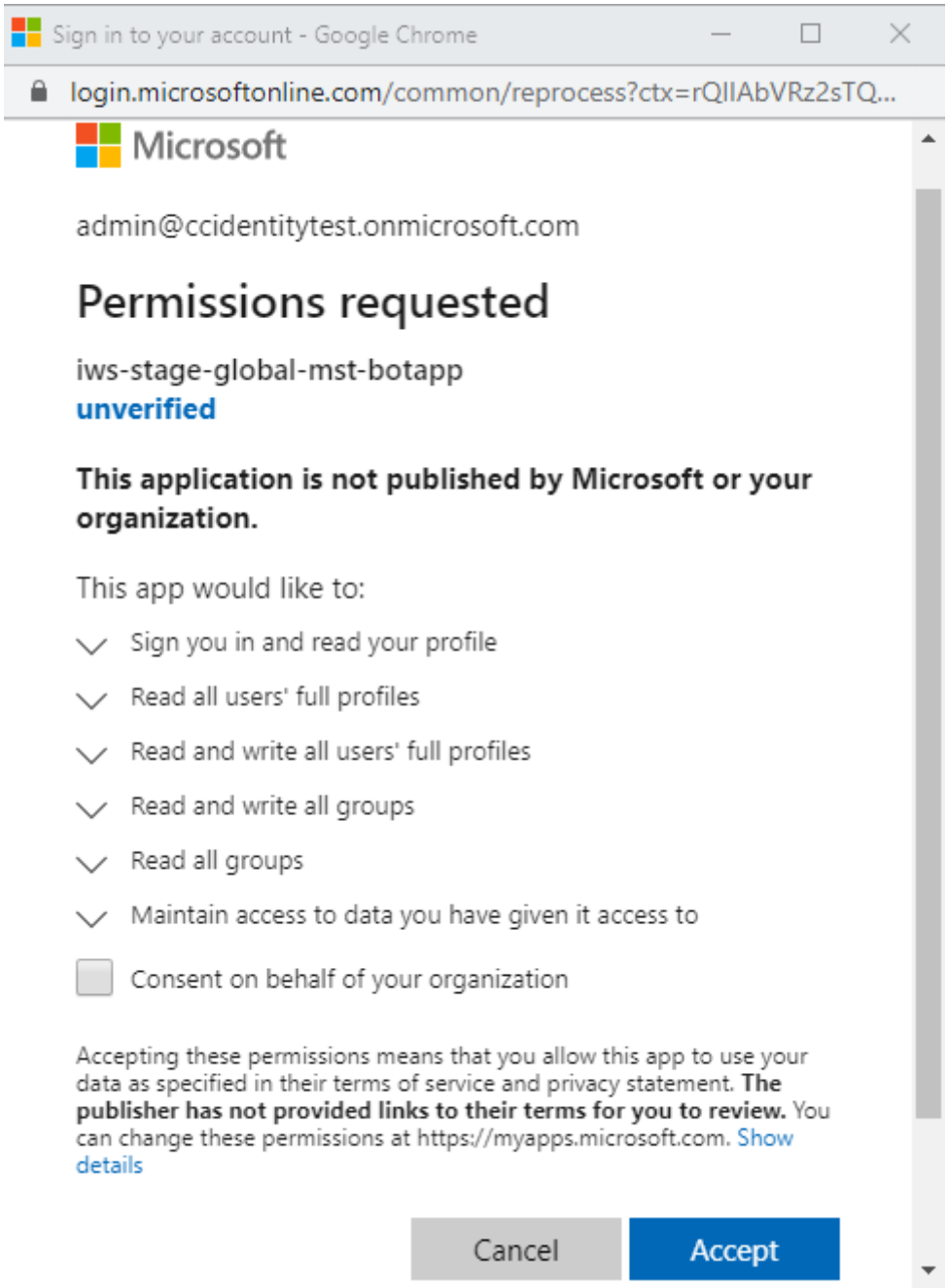
接受 **Workspace** 权限

要启用此集成，还需要执行其他设置步骤。**Microsoft** 管理员 帐户必须接受 Workspace UI 中集成的权限，这样您的组织的用户才能将卡片共享给 Microsoft Teams。

1. 登录任何工作区帐户并尝试共享卡片。
2. 如果 **Microsoft** 管理员 帐户尚未接受与 Microsoft Teams 集成的权限，而您尝试使用非管理员帐户登录，则会显示以下消息：



3. 要接受权限，请选择 是否有管理员帐户？登录到您的管理员帐户使用该帐户登录。要启用 Microsoft Teams 与 Citrix Workspace 的集成，需要以下权限才能访问数据：



4. 当“接受权限”对话框打开时，查看选项。代表贵组织的同意向该管理员的 所有 Workspace 订阅者授予权限。否则，仅授予管理员帐户的权限。
5. 选择 接受。

自定义安全和隐私政策

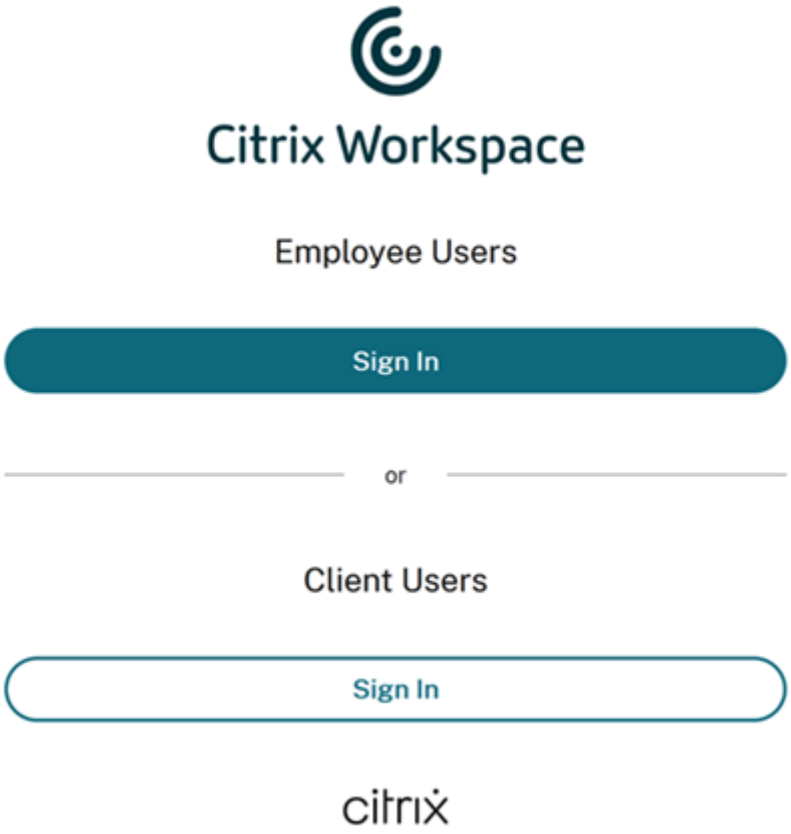
November 26, 2023

本文提供有关如何在配置完 Workspace 访问和身份验证后自定义登录体验的指导。

有关配置工作区访问权限和身份验证所涉及的步骤的概述，请访问 配置访问权限。有关如何配置工作区订阅者身份验证的信息，请访问 安全工作区。

创建统一的用户登录流程

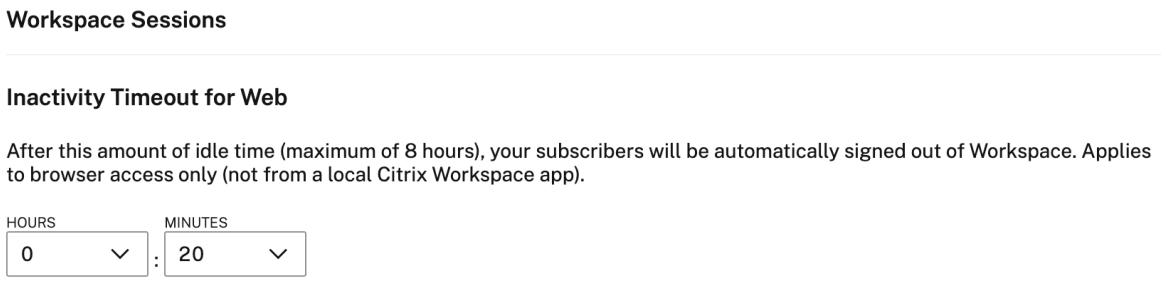
员工用户和客户端（外部）用户的默认登录体验是分屏模式。



要移除分屏，请导航到 **Workspace** 配置 **>** 身份验证 **>** 统一用户登录流程，然后选择 启用。启用此功能可为所有用户提供相同的登录选项。

为 **Web** 和 **Workspace** 应用程序桌面和移动设备设置非活动超时时间

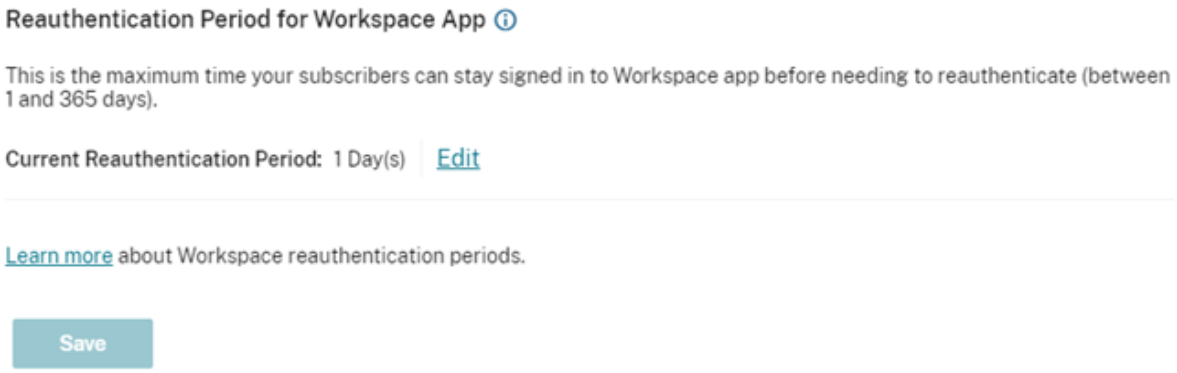
使用 **Workspace** 配置 **>** 自定义 **>** 首选项中的 **Web** 不活动超时设置来指定订阅者自动注销 Citrix Workspace 之前允许的空闲时间（最长 8 小时）。您还可以通过选择相应的配置框为台式机和移动设备上的 Workspace 应用程序启用非活动超时功能。



与断开 DaaS 会话连接的手动注销不同，订阅者在超时后由于不活动而保持与 DaaS 会话的连接。

为 **Citrix Workspace** 应用程序设置重新身份验证期限

使用 **Workspace** 配置 **>** 自定义 **>** 首选项中的 **Workspace** 应用程序的重新身份验证期限设置来指定订阅者在需要再次登录之前可以保持登录 Citrix Workspace 应用程序的时间长度。



默认情况下，此设置要求订阅者每 24 小时（一天）登录一次。您可以指定更长的重新身份验证期限，最长为 365 天。较长的重新身份验证期限需要订阅者同意才能保持登录状态。2021 年 9 月 27 日之后配置的用户，订阅者需要有 30 天的时间才能再次登录。

在您设置的重新身份验证期限内，订阅者将保持登录状态，除非他们一次不活跃 14 天或更长时间。如果订阅者在 14 天或更长时间内处于非活动状态，则系统会在下次尝试访问其工作区时提示他们重新进行身份验证。

通过下载此 PowerShell 脚本 并按照下载中包含的说明操作，可以使订阅者的会话失效。使会话失效后，订阅者必须在接下来的 24 小时内对其工作区重新进行身份验证。

如果您需要将 Citrix Workspace 应用程序的重新身份验证期限设置为少于 24 小时，则可以通过 PowerShell 执行此操作。
有关详细信息，请参阅配置 InactivityTimeoutInMinutes 的步骤。

支持的 **Workspace** 应用程序客户端

以下版本的 Citrix Workspace 应用程序支持此功能：

- 适用于 Windows 的 Workspace 应用程序 2106 或更高版本
- 适用于 Mac 的 Workspace 应用程序 2106 或更高版本
- 适用于 iOS 的 Workspace 应用程序 21.6.5 或更高版本
- 适用于 Android 的 Workspace 应用程序 21.6.0 或更高版本

支持的身份验证方法

以下身份验证方法支持保持对 Citrix Workspace 应用程序的登录状态：

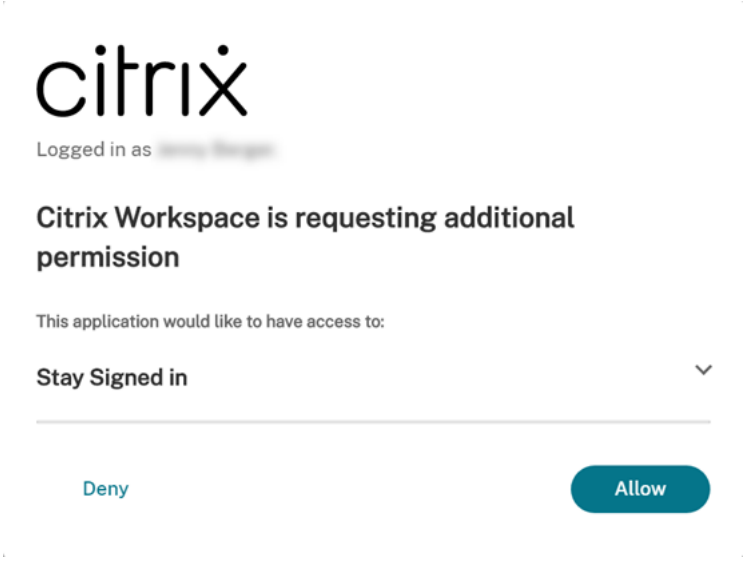
- Active Directory

- Active Directory 加令牌
- Azure Active Directory
- Citrix Gateway
- Okta

> 注意：
>
> 要获得与使用 Okta 或 Azure Active Directory 的 Citrix DaaS 客户相同的体验，请配置 Citrix 联合身份验证服务 (FAS)。有关 FAS 的更多信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录。

保持登录状态的订阅者体验

当订阅者在其设备上登录 Workspace 时，Workspace 会提示他们同意保持登录状态。



当订阅者选择“允许”时，他们在重新身份验证期间保持登录状态。如果订阅者的设备在四天内未检测到任何活动，系统会自动提示订阅者重新进行身份验证。登录 Citrix Workspace 应用程序后，只要他们在设备上使用应用程序和桌面，重新身份验证期限就会一直有效。

如果订阅者选择 拒绝，Workspace 会提示订阅者再次登录。之后，Workspace 会提示订阅者在 24 小时后再次登录。

如果订阅者的密码发生更改，则订阅者必须注销并通过 Citrix Workspace 应用程序重新登录，才能继续使用重新身份验证期。

允许订阅者更改其帐户密码

> 注意：
>
> 此功能正在逐步向客户推出。在部署过程完成之前，您可能看不到该功能。

> Citrix 的目标是在新功能和产品更新可用时向 Citrix Workspace 客户提供这些功能和产品更新。对您而言，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。逐步提供更新有助于确保产品质量并最大限度地提高可用性。

Workspace 配置 **>** 自定义 **>** 首选项中的“允许更改帐户密码”设置控制订阅者是否可以从 Citrix Workspace 中更改其域密码。您还可以向订阅者提供指导，以便他们可以根据贵组织的密码策略创建有效的密码。

启用（默认）后，订阅者可以根据贵组织的 Active Directory 设置随时更改其密码。如果禁用，Workspace 会在密码过期时提示订阅者更改密码，但他们无法在 Workspace 中更改未过期的密码。

支持的身份验证方法

- Active Directory
- Active Directory 加令牌

支持的 **Workspace** 应用程序客户端

以下版本的 Citrix Workspace 应用程序支持此功能：

- 适用于 Windows 的 Workspace 应用程序 2101 或更高版本
- 适用于 Mac 的 Workspace 应用程序 2012 或更高版本
- 适用于 Chrome 的 Workspace 应用程序 2010 或更高版本
- 适用于 HTML5 的 Workspace 应用程序 2101 或更高版本
- 适用于 Android 的 Workspace 应用程序 21.1.0 或更高版本

订阅者在使用最新版本的 Edge、Chrome、Firefox 或 Safari 网络浏览器访问工作区时也可以使用此功能。

旧版本的 Citrix Workspace 应用程序和适用于 Linux 的 Citrix Workspace 应用程序不支持此功能。

密码指导

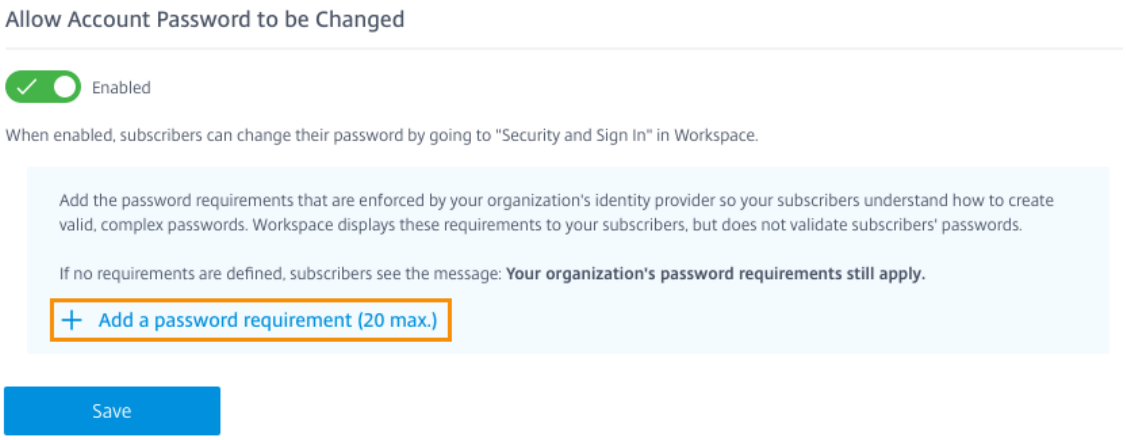
您最多可以添加 20 个密码要求，以满足贵组织的安全策略并由身份提供商强制执行。当订阅者从 Workspace 的“帐户设置”页面更改密码时，Workspace 会将这些要求显示为指南。如果您未添加任何密码要求，Workspace 会显示消息“您所在组织的密码要求仍然适用。”

> 重要：
>
> Citrix Workspace 不会验证订阅者输入的新密码。如果订阅者试图通过 Workspace 将其有效密码更改为无效密码，您的身份提供商会拒绝新密码。现有密码未更改。

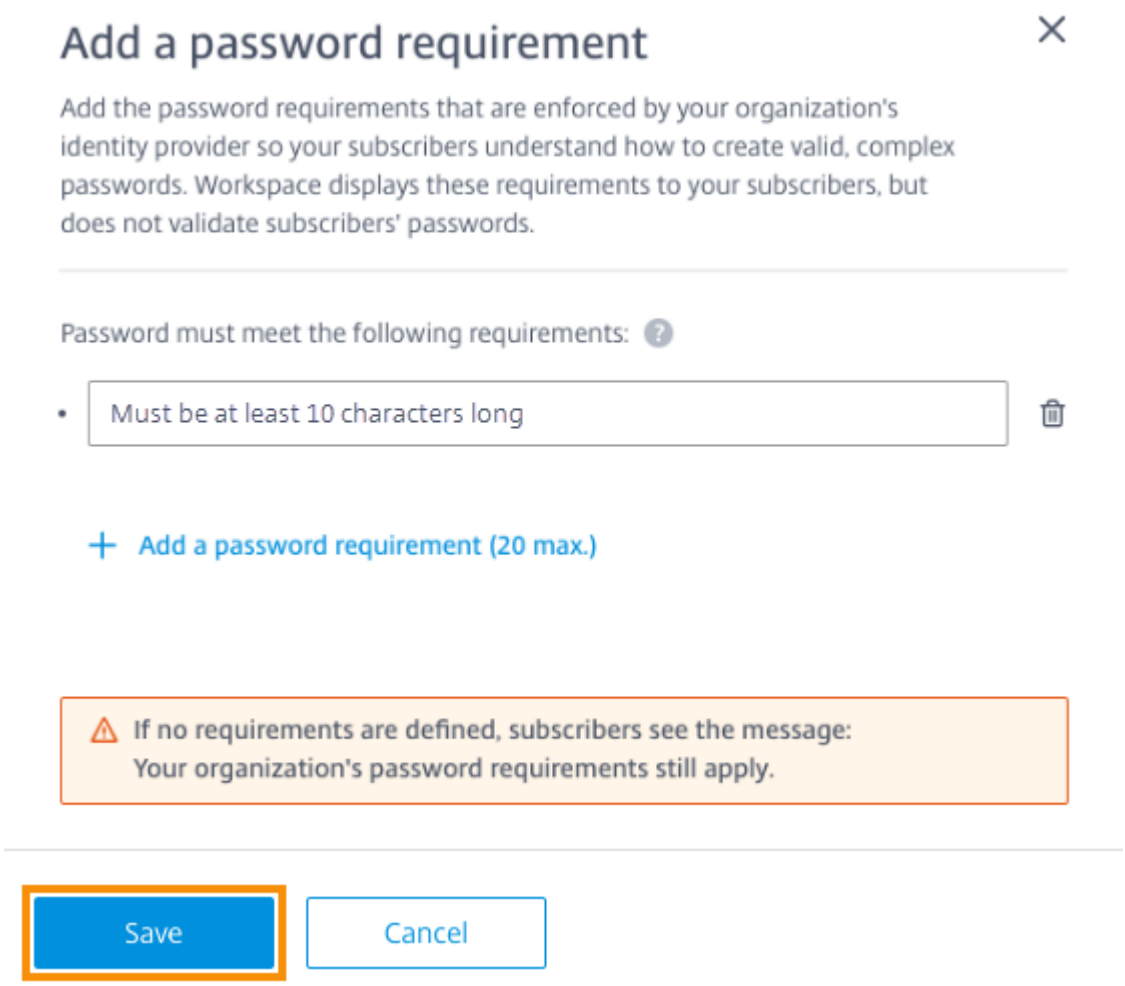
要添加密码要求，请执行以下操作：

1. 导航到 **Workspace** 配置 **>** 自定义 **>** 首选项。

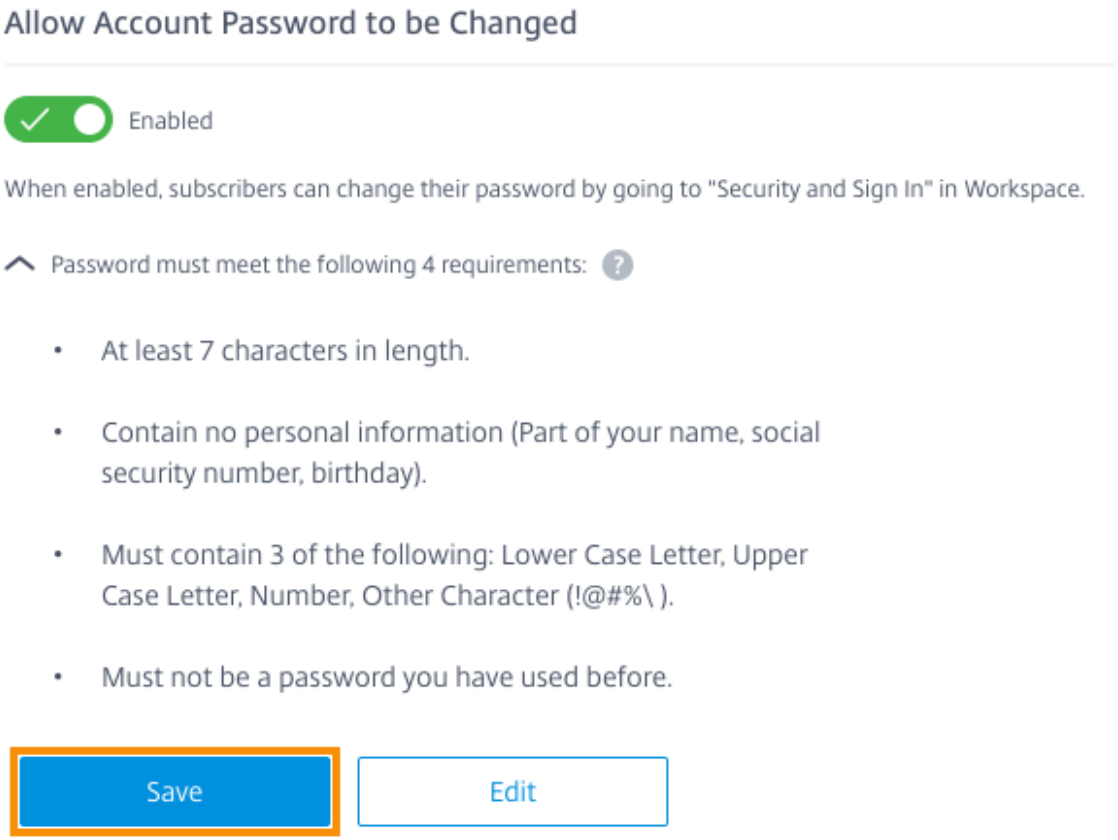
2. 在“允许更改帐户密码”下，检查该设置是否已启用。如果禁用，请启用该设置。
3. 选择“添加密码要求”。



4. 输入符合贵组织对有效密码的安全要求的要求。例如，您可以指定密码必须为特定的字符长度。选择 添加密码要求可在 订阅者更改密码时为其添加更多项目。



5. 添加完需求后，选择 保存。
6. 再次选择“保存”以保存所有设置更改。

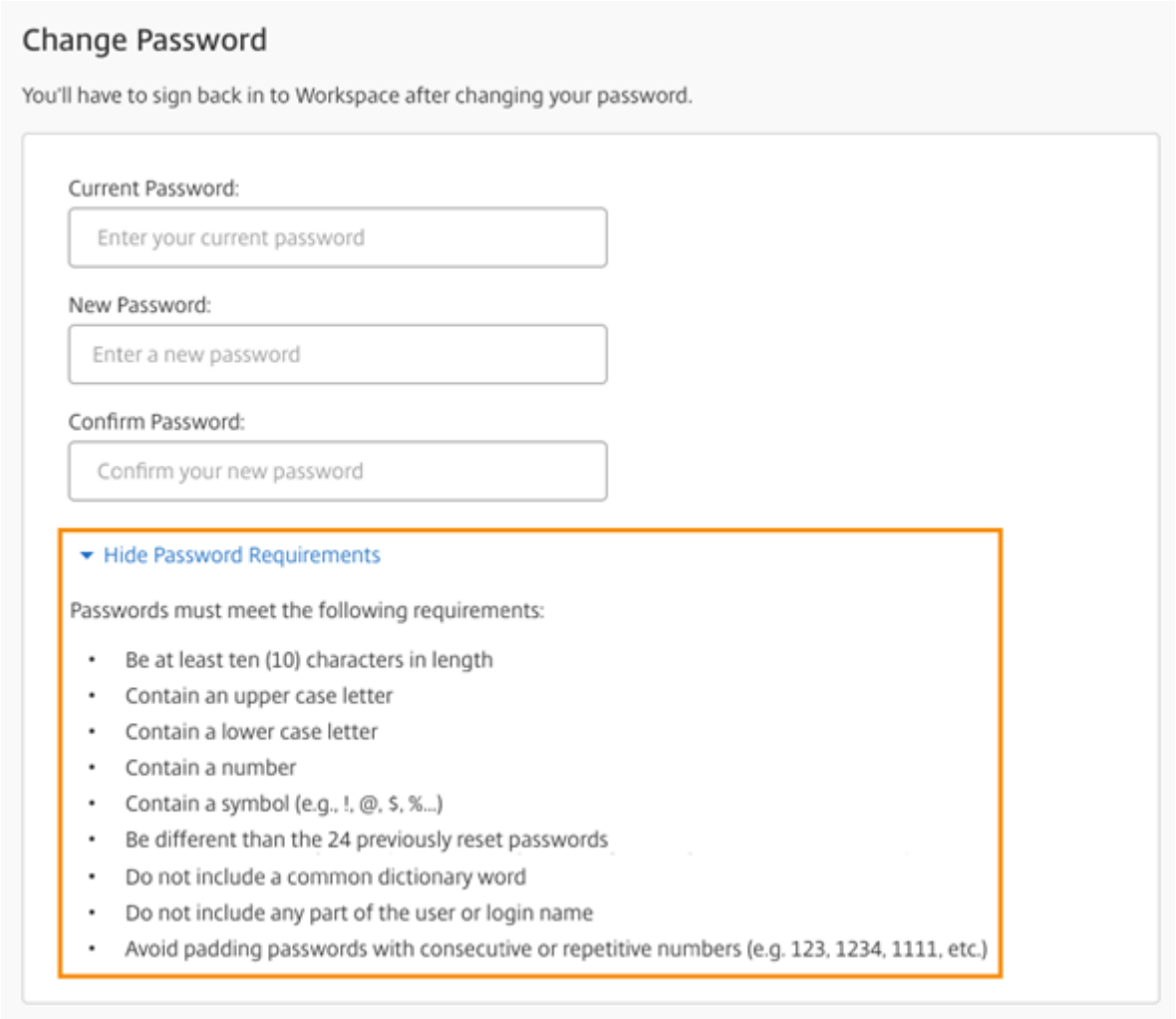


更改密码时的订阅者体验

> 提示：
>
> 要提高订阅者对该功能的认识，请考虑在内部知识库中包含一项建议，让订阅者通过 Workspace 更改其域密码。下载此 PDF 文件，了解可以在自己的通讯和知识库文章中包含的说明。

启用“允许更改帐户密码”后，订阅者可以通过前往“帐户设置”>“安全和登录”在 Workspace 中更改密码。

选择查看密码要求以显示您在 **Workspace** 配置中输入的所有要求。



订阅者在更改密码后会自动从 Workspace 注销，并且必须使用新密码重新登录。

发送自定义公告

发送自定义公告以显示您选择的限时消息，例如即将到来的维护窗口。

自定义公告显示在所有客户端（包括网络和移动设备）中的所有订阅者。订阅者登录后会看到该消息。订阅者无法忽略此公告，但他们可以在移动设备上将其隐藏。

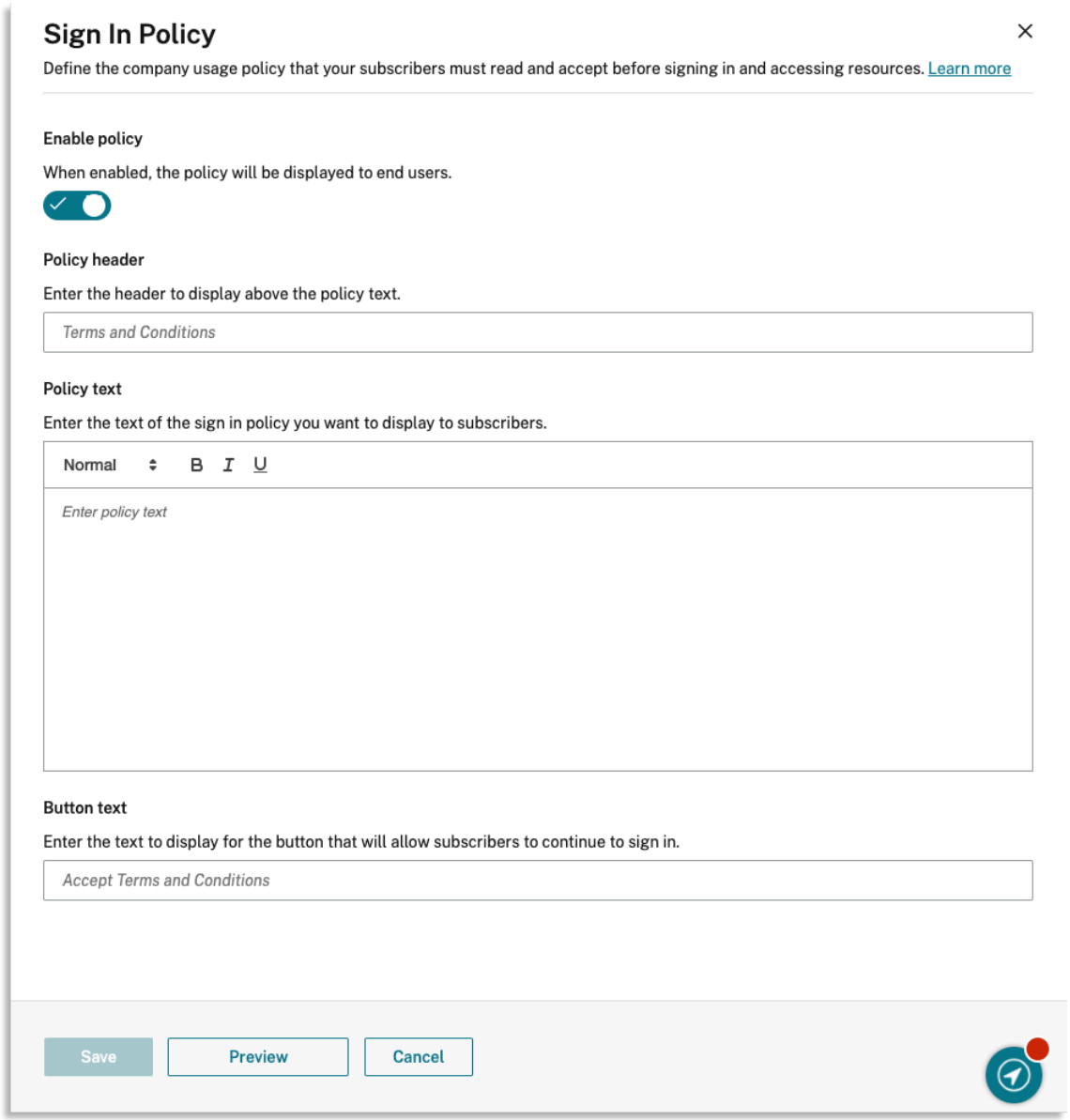
1. 从 **Citrix Cloud** 菜单中，选择 **Workspace** 配置 **>** 自定义 **>** 首选项 **>** 发送自定义公告 **>** 配置。
2. 输入要显示的消息的标题和文本，然后选择向订阅者显示消息的日期、时间和位置（顶部或底部）。
3. 要查看您的消息在订阅者面前的显示效果，请选择“预览”。
4. 完成后，选择“保存”。

配置登录策略

创建自定义登录策略，以便在订阅者登录其工作区时通知其组织的最终用户许可协议 (EULA)。

启用和配置后，登录策略将显示在所有客户端（包括 Web 和移动设备）中。订阅者可以在登录时看到登录策略。订阅者不能绕过该策略，必须接受该策略才能登录其工作区。

1. 从 **Citrix Cloud** 菜单中，选择 **Workspace** 配置 **>** 自定义 **>** 首选项。
2. 在“登录策略”部分中，选择“配置”。如果存在策略，则该按钮将改为显示“编辑”。
3. 使用启用策略下的开关启用该功能。
4. 在 策略标题中，输入策略的标题。
5. 输入订阅者在登录前必须同意的策略文本。如果需要，请在同一文本框中添加其他语言的本地化文本。
6. 输入按钮的名称，订阅者必须选择该名称才能同意该策略。



7. 选择“预览”以查看订阅者的政策是什么样子。

8. 完成后，选择“保存”。

> 注意
>
> 如果您将 Citrix Gateway 配置为 Workspace 身份提供商，则可能已经将登录策略作为 AAA 和 nFactor 身份验证流程的一部分。Citrix 建议您仅配置一个登录策略，作为现有 nFactor 身份验证流程的一部分或使用 Citrix Cloud 管理控制台在流程之外配置。

在 Citrix Workspace 中优化 DaaS

October 12, 2023

您可以使用以下选项提高 DaaS 应用程序和桌面的效率和可用性：

- 通过 站点聚合，向 Workspace 订阅者提供现有的本地虚拟应用程序和桌面部署。
- 使用 直接工作负载连接优化连接，这涉及在 Citrix Cloud 中配置网络位置。
- 确保停机期间的服务连续性，实现离线弹性。
- 使用 Citrix 联合身份验证服务 (FAS) 配置单点登录 (SSO) 到 DaaS。

站点聚合

站点聚合允许您将本地虚拟应用程序和桌面部署添加到 Workspace 中，以便订阅者可以访问这些资源以及云托管资源。

有关站点聚合的更多信息，请参阅在工作区中聚合本地虚拟应用程序和桌面。

有关可扩展性限制的更多信息，请参阅 Workspace 平台可扩展性限制。

直接工作负载连接

直接工作负载连接使用网络位置在内部和外部路由之间切换，指向托管您的虚拟应用程序和桌面的虚拟机。

使用直接工作负载连接，您可以允许公司网络内的客户端切换到直接启动 Citrix DaaS。直接启动不需要通过网关代理客户端和 VDA 之间的 HDX 连接。直接工作负载连接需要至少一个内部网络位置。

有关更多信息，请访问 使用直接工作负载连接优化连接。

服务连续性

服务连续性可确保订阅者在 Citrix Cloud 中断时继续通过 Citrix Workspace 应用程序访问关键应用程序和桌面。

服务连续性将连接租约存储在安装了 Citrix Workspace 应用程序的客户端磁盘上。客户端访问 Workspace 存储区时，会定期刷新连接租约。然后，客户端可以启动可以在中断之前访问的 Citrix DaaS。有关更多信息，请访问 服务连续性。

Citrix 联合身份验证服务 (FAS)

Citrix Workspace 支持使用 Citrix 联合身份验证服务 (FAS) 对 Citrix DaaS 进行单点登录 (SSO)。FAS 允许使用联合身份提供程序（如 Azure AD 或 Okta）的订阅者在登录其工作区时仅输入一次凭据。如果没有 FAS，则会提示使用联合身份提供商的订阅者多次输入凭据以访问其虚拟应用程序和桌面。

将 FAS 与 Workspace 一起使用有以下要求：

- 按照 FAS 产品文档的 要求 部分所述配置的 FAS 服务器。
- 您的 FAS 服务器与 Citrix Cloud 之间的连接，通过 FAS 安装程序中的“连接到 **Citrix Cloud**”选项创建。
- 内部部署 Active Directory 域与 Citrix Cloud 之间的连接，在 **Workspace** 配置中启用了 FAS。

有关实施 FAS 的信息，请参阅 使用 Citrix 联合身份验证服务为工作区启用单点登录。

聚合工作区中的本地虚拟应用程序和桌面

November 26, 2023

您可以将站点（Virtual Apps and Desktops 部署）添加到 Citrix Workspace，以便订阅者可以使用现有应用程序和桌面。添加站点后，订阅者可以在登录其工作区时访问其所有虚拟应用程序和桌面以及文件和其他资源。此过程称为站点聚合。

站点聚合适用于所有 Citrix Workspace 版本。有关每个 Workspace 版本中包含的功能的详细信息，请参阅 Citrix Workspace 功能列表。

支持的环境

以下 Citrix 产品的本地部署支持站点聚合：

- Virtual Apps and Desktops 7 1808 或更高版本
- XenApp 和 XenDesktop 7.0 到 7.18

运行旧版 XenApp 或 XenApp 和 XenDesktop 的本地站点不支持与 Citrix Workspace 配合使用。

> 重要：
>
> XenApp 和 XenDesktop 7.x 包括生命周期终止 (EoL) 版本。7.14 之前的 XenApp 和 XenDesktop 版本将于 2018 年 6 月 30 日停产。使用 XenApp 和 XenDesktop 7.x 的 EoL 版本对站点聚合的支持取决于成功枚举和启动您的 StoreFront 部署中的资源。

要将站点聚合与包含 Citrix 联合身份验证服务 (FAS) 的本地部署结合使用，您的站点必须使用以下 Citrix 产品版本之一：

- Virtual Apps and Desktops 7 1808 或更高版本
- XenApp 和 XenDesktop 7.16 到 7.18

将 FAS 与 Citrix Workspace 配合使用需要连接到 Citrix Cloud。将 FAS 服务器更新到最新版本的 FAS 软件，以便您可以连接到 Citrix Cloud。有关详细信息，请参阅使用 Citrix 联合身份验证服务对工作区启用单点登录。

Workspace 平台可扩展性限制

以下可扩展性限制适用于 Workspace 平台：

极限类型	SLI 指标	SLO 阈值限制
使用限制	所有聚合的本地 Citrix 虚拟应用程序和桌面站点的并发最终用户	500
额外的后端/前端集成限制	本地 Citrix 虚拟应用程序和桌面站点的数量	4

> 注意：
>
> 如果后端/前端集成站点的数量超过四个，则站点的响应时间可能会很慢。本地站点也不提供服务连续性或 LHC 支持。

任务概述

将本地站点添加到 Citrix Workspace 时，添加站点 向导将引导您完成以下任务：

1. 发现您的站点并选择要使用的资源位置。
2. 检测安装了 Cloud Connector 的 Active Directory 域。
3. 指定要在 Citrix Cloud 和您的站点之间使用的连接。

资源位置为访问您的站点的所有用户指定域和连接方法。在此过程中，Citrix Cloud 将测试连接性，以验证您的站点是否可通过 Cloud Connector 访问。然后，Citrix Cloud 将显示您的资源位置的列表。如果您的资源位置未安装 Cloud Connector，请下载并安装所需的软件。

对于外部连接，您可以使用自己的 Citrix Gateway 或 Citrix Gateway 服务。要仅允许与您的站点位于同一网络上的用户访问应用程序，请指定仅限内部访问。

必备条件

Cloud Connector

Cloud Connector 允许 Citrix Cloud 定位您的站点并与之通信。为了尽量减少中断，Citrix 建议在将站点添加到 Citrix Workspace 之前安装 Cloud Connector。

为了实现高可用性，Citrix 建议至少在两 (2) 台服务器上安装 Citrix Cloud Connector 软件。这些服务器必须：

- 满足 Cloud Connector 技术详情中描述的系统要求。
- 未安装其他 Citrix 组件。
- 不是 Active Directory 域控制器。
- 不是一台对您的资源位置基础架构至关重要的机器。
- 加入您的网站域。如果用户在多个域中访问您站点的应用程序，请在每个域中至少安装两个 Cloud Connector。
- 连接到可以联系您的站点的网络。
- 连接到互联网。有关详细信息，请参阅系统和连接要求。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。

Web 代理配置

如果您的环境中有 Web 代理，请检查 Cloud Connectors 是否可以验证与站点中的 XML 服务的连接。将站点内的每个 XML 服务器添加到每个 Cloud Connector 上的绕过代理列表中。请勿使用通配符或 IP 地址，因为 Cloud Connector 仅支持处理 FQDN。

1. 将 XML 服务器添加到旁路代理列表中：
   a) 在 Cloud Connector 上，选择开始，然后键入 **Internet** 选项。
   b) 选择“连接”选项卡，然后选择“局域网设置”。
   c) 在“代理服务器”下，选择“高级”。
   d) 在“例外”下，使用小写字母添加站点中每个 XML 服务器的 FQDN。如果这些条目使用混合大小写或大写字母，则站点聚合可能会失败。有关更多信息，请参阅 Citrix 支持知识中心中的 CTX272160 。
2. 导入该列表，以便 Cloud Connector 服务可以使用它们。在命令提示符处键入 `netsh winhttp import proxy source=ie`。
3. 从服务控制台中，在托管 Cloud Connector 的每台计算机上重新启动所有 Citrix Cloud 服务，或者重新启动每台计算机。

Active Directory

站点聚合支持使用本地 Active Directory 的站点。

Azure Active Directory 配置　要将使用 Azure Active Directory 的站点添加到 Citrix Workspace，请将您的站点配置为信任 XML 服务请求。有关详细说明，请参阅以下文章：

有关 XenApp 和 XenDesktop 7.x 以及 Virtual Apps and Desktops 7 1808 的信息，请参阅 CTX236929。

> 重要：
>
> 如果将 Azure Active Directory、Okta、SAML 或其他联合身份提供程序与工作区和站点聚合一起使用，则系统会提示用户对他们启动的每个应用程序进行身份验证。
>
> FAS 为使用联合身份验证启动资源提供了单点登录 (SSO) 体验。要为订阅者启用 SSO，请使用您为添加站点而配置的相同资源位置注册一个或多个 FAS 服务器。

Active Directory 信任　如果您在 Active Directory 中有单独的用户林和资源林，则在添加本地站点之前，必须在每个林中安装 Cloud Connector。Citrix Cloud 在站点发现过程中通过 Cloud Connector 检测到这些森林。然后，您可以使用林的用户和资源为用户创建工作区。

限制：

添加站点时，在定义资源位置时不能使用单独的用户林和资源林。由于 Cloud Connector 不参与可能建立的任何跨林信任，因此 Citrix Cloud 无法通过这些林中的 Cloud Connector 发现您的站点。在定义为用户提供不同连接选项的辅助资源位置时，可以使用这些林。有关更多信息，请参阅 为不同的连接选项添加 IP 范围。

站点聚合不支持不受信任的林。尽管 Citrix Cloud 和 Citrix Workspace 支持来自不受信任林的用户，但在通过站点聚合添加本地站点后，这些用户将无法使用 Citrix Workspace。只有位于站点信任的林中的用户才能登录和使用 Citrix Workspace。如果来自不受信任林的用户尝试登录 Citrix Workspace，他们会收到错误消息“您的登录已过期。请重新登录以继续。

与 **Workspace** 资源的内部和外部连接

在将站点添加到 Citrix Workspace 的过程中，您可以指定是否要向用户提供对可用资源的内部或外部访问权限。如果您打算仅允许内部用户通过 Citrix Workspace 访问您的站点，则用户必须与站点位于同一网络上才能访问应用程序。

如果您打算允许外部用户访问这些资源，则有以下选项：

- 使用现有的 Citrix Gateway 处理本地站点与 Citrix Cloud 之间的流量。在将站点添加到 Citrix Workspace 之前，必须将 Citrix Gateway 配置为使用 Cloud Connector 作为 Secure Ticket Authority (STA) 服务器。相关说明，请参阅 CTX232640。
- 使用 Citrix Gateway 服务允许 Citrix 为您处理站点与 Citrix Cloud 之间的流量。您可以在添加站点时激活服务试用版并配置服务。如果您已经注册了 Citrix Gateway 服务，则当您选择此选项时，Citrix Cloud 会检测到您的订阅。

> 注意：
>
> 要使 Citrix Cloud 检测到您的 Citrix Gateway 服务订阅，您必须使用注册 Citrix Gateway 服务时使用的相同 OrgID。有关 Citrix Cloud 中的 OrgID 的更多信息，请参阅 什么是 OrgID?

站点发现的凭据和端口

在将站点添加到 Citrix Workspace 的过程中，Citrix Cloud 会发现您的站点并检查您指定的控制器是否可用。在添加本地站点之前，请检查以下各项：

- 您具有最低 只读 权限的 Citrix 管理员凭据。在站点发现过程中，Citrix Cloud 会提示您提供这些凭据。Citrix Cloud 不会存储这些凭据，也不会使用它们来更改您的站点。

在没有站点凭据的情况下启用站点发现　仅限 **XenApp** 和 **XenDesktop 7.x** 以及 **Virtual Apps and Desktops 7 1808**：如果出于安全原因不想提供站点凭据，则可以允许 Citrix Cloud 在不提示输入站点凭据的情况下发现您的站点。在将站点添加到 Citrix Workspace 之前，请先完成此任务。

1. 在站点的域中至少安装两个 Cloud Connector。
2. 创建 Active Directory 安全组，然后将域中的 Cloud Connector 添加到该安全组。
3. 重新启动 Cloud Connector。
4. 在 Studio 中，至少向安全组授予 只读 权限。

任务 **1**：发现站点

在此步骤中，您将提供 Citrix Cloud 定位站点和选择资源位置所需的信息。资源位置为访问您的站点的所有用户指定域和连接选项。如果您需要在站点的域中安装 Cloud Connectors，现在就可以安装了。如果您已经安装了 Cloud Connectors，则可以在出现提示时选择它们。

1. 从 Citrix Cloud 菜单中，导航到 **Workspace** 配置 **>** 站点 **>** 添加站点。
2. 选择要添加的本地站点的类型并继续。

   Citrix Cloud 会尝试发现域中的任何资源位置和 Cloud Connector，并显示一个列表供您选择。
3. 执行以下操作之一：

   - 如果站点的域中没有安装 Cloud Connector，请选择安装连接器。Citrix Cloud 会提示您下载 Cloud Connector 软件并完成安装向导。
   - 如果安装了 Cloud Connector，Citrix Cloud 会在检测到它们的域中显示连接器。选择要添加到 Citrix Workspace 的资源位置。此资源位置将成为默认资源位置。
   - 如果您安装了 Cloud Connector，但它们未显示，请选择检测。
4. 选择要用于发现站点的资源位置和 Cloud Connector 对。
5. 在 输入服务器地址中，添加站点中控制器的 IP 地址或 FQDN，然后选择 发现

   > 注意：

> 如果使用 FQDN，则必须有一条指向要发现的 Delivery Controller 的 DNS 记录。
>
> 对于 XenApp 和 XenDesktop 7.x 站点，Citrix Cloud 会自动发现 XML 服务器端口。

6. 如果出现提示，请输入站点的 Citrix 管理员凭据。

   Citrix Cloud 会测试连接以验证您的站点是否可访问。发现可能需要几分钟才能完成，具体取决于站点的类型和大小。

7. 如果出现成功消息，表明已成功发现该站点，请选择“继续”。

任务 **2**：验证 **Active Directory** 连接

在 验证 **Active Directory** 连接中，Citrix Cloud 将显示与您的站点一起使用的域以及这些域中是否安装了 Cloud Connector。

如果域中没有 Cloud Connector，则该域中的用户将无法使用 Citrix Workspace 访问在那里发布的应用程序。如果您的域中只有一个 Cloud Connector，则有两种选择：

- 通过选择安装连接器来安装更多 Cloud Connector。
- 继续不安装更多 Cloud Connectors ，只需选择我了解高可用性要求在每个域中安装两个连接器。

如果已将本地用户分配给站点中的应用程序，请选择 下载用户列表 **(.csv)**。

验证 Active Directory 连接后，选择 继续。

任务 **3**：配置连通性

在此步骤中，您将指定是要允许外部用户还是仅允许内部用户通过 Citrix Workspace 访问您的站点。内部连接要求您的用户与您的站点和托管已发布资源的 VDA 位于同一网络上。对于外部连接，您可以使用现有的本地 Citrix Gateway，也可以使用云托管的 Citrix Gateway 服务。

在选择 连接类型 **>** 配置连接中选择以下选项之一：

- 添加现有网关：选择此选项可使用现有的 Citrix Gateway 提供外部访问权限。
- **Citrix Gateway** 服务：选择此选项可激活服务试用版或将现有订阅用于站点。
- 仅限内部：如果不需要其他配置，请选择此选项。

如果选择了“添加现有网关”，请执行以下操作：

1. 选择 编辑，然后输入 Citrix Gateway 的公共 URL。
2. 确认 Citrix Gateway 已配置为使用 Cloud Connector 作为 STA 服务器，如 CTX232640 中所述。
3. 选择“测试 **STA**”，然后在测试成功时选择“继续”。如果测试不成功，请参考 CTX232517 进行故障排除。

如果选择了 **Citrix Gateway** 服务，但您的 Citrix Cloud 帐户未将该服务作为服务试用版或购买启用，则可以选择 启动 **60** 天试用。Citrix Cloud 为您启用该服务作为试用版。如果该服务是在较早时间启用的，Citrix Cloud 将检测该服务并显示任何剩余的试用天数。

完成上述任务后，选择 继续。

任务 **4**：确认站点聚合

在此步骤中，您将确认站点聚合，其中包括检查 XML 端口、XML 服务器、Active Directory 域以及之前选择的连接类型。

Citrix Cloud 最多显示它可以连接的五个 XML 服务器。如果您的站点中有多个 XML 服务器，但只显示了一个 XML 服务器，Citrix Cloud 将显示警报。要解决此问题，请参阅 CTX232516。

1. 在“确认站点聚合”中，查看 XML 端口、XML 服务器、Active Directory 域以及之前选择的连接类型。
2. 选择“保存并完成”。“站点”页面显示您新添加的站点。

如果要指定不同的 XML 服务器，则可以在选择“保存并完成”后编辑站点以更改这些值。

任务 **5**：管理服务集成

添加第一个站点后，必须启用 Virtual Apps and Desktops 本地站点的 服务集成，默认情况下处于禁用状态。在您启用网站之前，订阅者无法看到来自该网站的资源。

1. 导航到 **Workspace** 配置 **>** 服务集成 **> Virtual Apps and Desktops** 本地 站点，然后选择省略号以打开站点操作菜单。
2. 启用服务集成，以便订阅者可以登录其工作区并查看站点中的资源。

更改您的站点配置

重新发现您的网站

如果将交付控制器添加到站点或更改 XML 端口，则可以通过重新发现过程验证站点是否仍可在 Citrix Workspace 中访问。

1. 导航到“**Workspace** 配置”**>**“站点”，选择要更新的站点的省略号，然后选择“编辑站点”。
2. 在 服务器地址中，键入站点中 Delivery Controller 的 IP 地址或 FQDN，然后选择 重新发现。

添加或修改 **XML** 服务器

将站点添加到 Citrix Workspace 时，Citrix Cloud 会自动检测站点中的 XML 服务器，并在配置中最多显示五个 XML 服务器。您可以根据需要从站点配置中添加和删除 XML 服务器，最多可显示五个 XML 服务器。

添加 **XML** 服务器

1. 导航到“**Workspace** 配置”**>**“站点”，选择要更新的站点的省略号，然后选择“编辑站点”。
2. 在“**XML** 服务器”部分中，输入 XML 服务器端口，然后根据需要选择“使用 **SSL**”。
3. 选择一种连接方式：
   - 负载平衡：此选项允许 Citrix Cloud 从列表中随机选择一个 XML 服务器。
   - 故障转移：此选项允许 Citrix Cloud 按列出的 XML 服务器在列表中显示的顺序使用它们。只有列表中的第一个 XML 服务才会用于启动，除非该服务不可用，然后使用第二个服务器。您可以通过拖放每台服务器来对列表重新排序。
4. 选择 保存更改。

如果在添加 XML 服务器时遇到错误，请参阅 CTX232516 了解故障排除步骤。

为不同的连接选项添加 **IP** 范围

如果您的 VDA 或会话主机位于不同的子网中，则可以为每个 IP 范围指定具有不同连接类型的 IP 范围。每个 IP 范围也可以具有与其关联的不同资源位置。例如，对于用户在内部进行连接的欧盟计算机可能有一个 IP 范围，对于用户通过 Citrix Gateway 进行连接的欧盟计算机可能有一个 IP 范围，对于用户通过 Citrix Gateway 服务进行连接的美国计算机，可能有一个 IP 范围。

1. 导航到“**Workspace** 配置”**>**“站点”，选择要更新的站点的省略号按钮，然后选择“编辑站点”。
2. 在 连接 部分中，选择 添加具有不同连接选项的 **IP** 范围，然后输入 CIDR 格式的 IP 范围。

要为 IP 范围创建资源位置，请执行以下操作：

1. 选择“添加新的资源位置”，然后输入用户友好的名称。
2. 在 选择连接中，选择是要提供仅限内部访问还是允许使用 Citrix Gateway 或 Citrix Gateway 服务进行外部访问。

要将现有资源位置分配给 IP 范围，请执行以下操作：

1. 选择“选择现有资源位置”
2. 选择要使用的资源位置。
3. 如果您选择的资源位置仅安装了一个 Cloud Connector ，请选择我了解高可用性要求在一个资源位置安装两个连接器。
4. 选择添加。

添加更多 **Active Directory** 域

如果您在站点中有 Active Directory 用户的更多域中安装 Cloud Connector，则可以在 Citrix Workspace 中检查它们是否已添加到您的站点配置中。

1. 导航到“**Workspace** 配置”**>**“站点”，选择要更新的站点的省略号，然后选择“编辑站点”。
2. 在“Active Directory”下，选择“刷新”。

禁用站点

如果您不想再向 Citrix Workspace 中的用户提供本地站点，可以将其禁用。您可以禁用单个本地站点或已添加到 Citrix Workspace 的所有本地站点。

禁用站点后，用户将无法通过 Citrix Workspace 访问这些站点中的本地应用程序。但是，这些站点的配置将保留。如果稍后重新启用站点，则会保留该站点的默认资源位置、域、XML 服务器和连接设置。

禁用本地站点

1. 导航到“**Workspace** 配置”**>**“站点”，选择要禁用的站点的省略号，然后选择“禁用”。
2. 此时将显示一条确认消息。再次选择“禁用”。

禁用所有本地站点

要禁用“站点”页面上的所有 站点，请禁用所有本地 Virtual Apps and Desktops 站点的 Workspace 服务集成。有关说明，请参阅 禁用服务的工作区集成。

要重新启用单个本地站点或稍后添加其他站点，必须先在服务集成页面上为所有站点重新启用 Workspace 服务集成。

从 **Citrix Workspace** 中删除站点

如果您不再希望在 Citrix Workspace 中配置本地站点，则可以删除该站点。删除站点时，只会删除 Citrix Workspace 中该站点的配置。Citrix Cloud 不会更改您的站点。

要删除站点，请导航到“**Workspace** 配置”**>**“站点”，选择要移除的站点的省略号，然后选择“删除”。

使用直接工作负载连接优化工作区的连接

November 26, 2023

借助 Citrix Cloud 中的直接工作负载连接，您可以优化工作区中应用程序和桌面的内部流量，从而加快 HDX 会话的速度。通常，内部和外部网络上的用户都通过外部网关连接到 VDA。此网关可能位于组织内部或作为 Citrix 提供的服务并添加到 Citrix Cloud 中的资源位置。直接工作负载连接允许内部用户绕过网关直接连接到 VDA，从而减少内部网络流量的延迟。

要设置 Direct Workload Connection，您需要与客户端在您的环境中启动应用程序和桌面的位置相对应的网络位置。使用网络定位服务 (NLS) 为这些客户端所在的每个办公地点添加一个公共地址。有两种配置网络位置的选项：

- 使用 Citrix Cloud 中的 网络位置 菜单选项。
- 使用 Citrix 提供的 PowerShell 模块 。

网络位置与内部用户连接的网络的公共 IP 范围相对应，例如您的办公室或分支机构位置。Citrix Cloud 使用公有 IP 地址来确定启动虚拟应用程序或桌面的网络是公司网络的内部网络还是外部网络。如果用户从内部网络连接，Citrix Cloud 会将连接直接路由到 VDA，而绕过 NetScaler Gateway。如果订阅者在外部连接，Citrix Cloud 会通过 NetScaler Gateway 将他们路由，然后通过 Citrix Cloud Connector 将会话流量定向到内部网络中的 VDA。如果使用 Citrix Gateway 服务并启用了 Rendezvous 协议，则 Citrix Cloud 会通过网关服务将外部用户路由到内部网络中的 VDA。漫游客户端（如便携式计算机）可能会使用这些网络路由中的任何一个，具体取决于启动时客户端是在公司网络内部还是外部。

> 重要：
>
> 如果您的环境包括 Citrix DaaS Standard for Azure 和本地 VDA，则配置直接工作负载连接会导致从内部网络启动失败。

Remote Browser Isolation、Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials 资源启动始终通过网关路由。配置直接工作负载连接不会提高这些启动的性能。

要求

网络要求

- 企业网络和访客 Wi-Fi 网络必须有单独的公有 IP 地址。如果您的公司和访客网络共享公有 IP 地址，则访客网络上的用户无法启动 DaaS 会话。
- 使用内部用户连接的网络的公有 IP 地址范围。这些网络中的内部用户必须直接连接到 VDA。否则，当 Workspace 尝试将内部用户直接路由到 VDA 时，虚拟资源的启动将失败，这是不可能的。
- 尽管 VDA 通常位于本地网络中，但您也可以使用托管在公共云（如 Microsoft Azure）内的 VDA。客户端启动必须具有网络路由，以便在不被防火墙阻止的情况下联系 VDA。这需要使用从本地网络到 VDA 所在的虚拟网络的 VPN 隧道。

TLS 要求

配置网络位置时，必须在 PowerShell 中启用 TLS 1.2。要强制 PowerShell 使用 TLS 1.2，请在使用 PowerShell 模块之前使用以下命令：

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```


Workspace 要求

- 您在 Citrix Cloud 中配置了工作区。
- Citrix DaaS 已在 **Workspace** 配置 **>** 服务集成中启用。

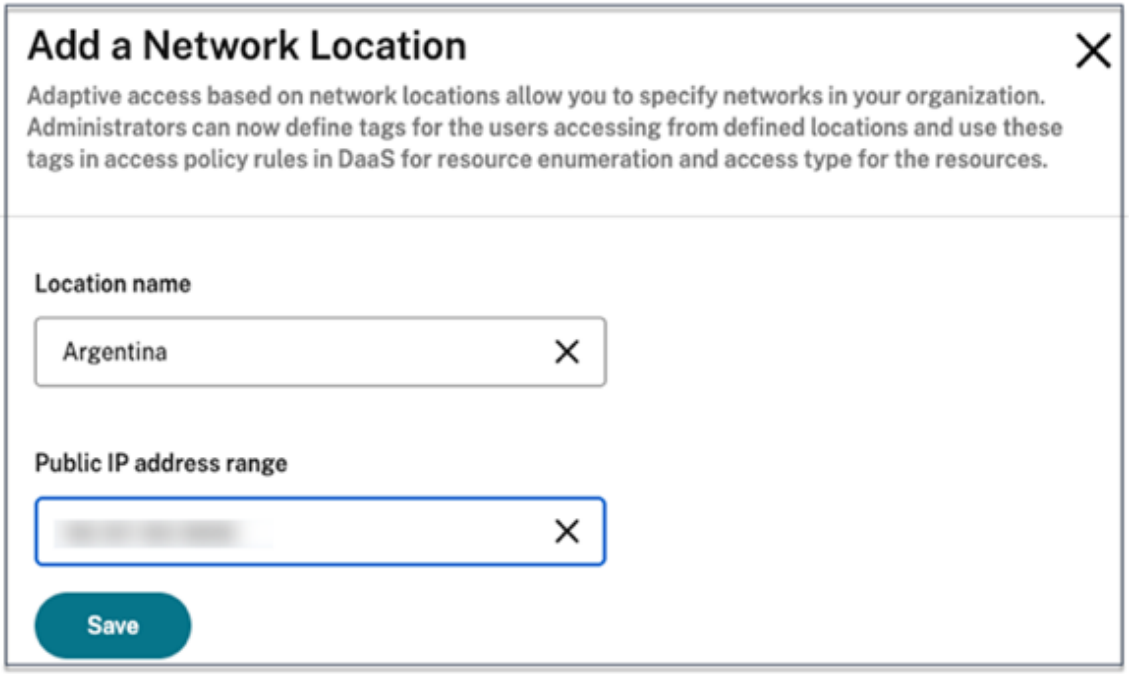
为适用于 **HTML5** 的 **Workspace** 应用程序连接启用 **TLS**

如果您的订阅者使用适用于 HTML5 的 Citrix Workspace 应用程序启动应用程序和桌面，Citrix 建议您在内部网络中的 VDA 上配置 TLS。将 VDA 配置为使用 TLS 连接可确保可以直接启动 VDA。如果 VDA 未启用 TLS，则当订阅者使用适用于 HTML5 的 Citrix Workspace 应用程序时，必须通过网关路由应用程序和桌面启动。使用 Desktop Viewer 启动不会受到影响。有关使用 TLS 保护直接 VDA 连接的更多信息，请参阅 Citrix 支持知识中心中的 CTX134123 。

通过 **GUI** 添加网络位置

通过 Citrix Cloud 进行直接工作负载连接配置涉及使用内部用户连接的每个分支位置的公有 IP 地址范围创建网络位置。

1. 在 Citrix Cloud 控制台中，导航到网络位置。
2. 单击“添加网络位置”。
3. 输入该位置的网络位置名称和公有 IP 地址范围。

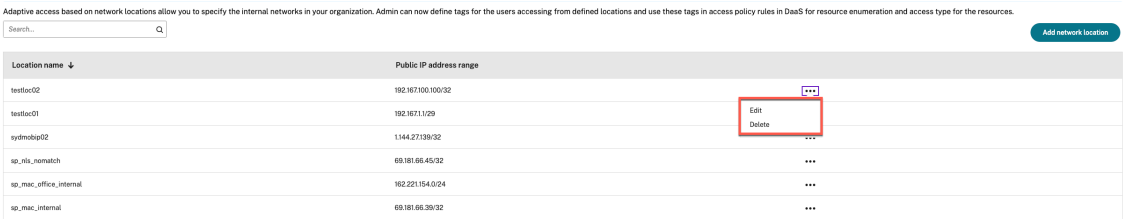


4. 单击保存。
5. 对要添加的每个新网络位置重复这些步骤。

> 注意：
>
> 直接工作负载连接不需要位置标记，因为连接类型始终为内部。只有启用自适应访问功能，添加网络位置页面（**Citrix Cloud >** 网络位置 **>** 添加网络位置 **>** 位置标记）中的位置标记字段才可见。有关详细信息，请参阅 启用自适应访问功能。

修改或移除网络位置

1. 在 Citrix Cloud 控制台中，从主菜单导航到 网络位置。
2. 找到要管理的网络位置，然后单击省略号按钮。



3. 选择以下命令之一：
   - 选择“编辑”以修改网络位置。进行更改后，单击“保存”。
   - 选择“删除”以删除网络位置。选择“是，删除”以确认删除。您无法撤消此操作。

使用 **PowerShell** 添加和修改网络位置

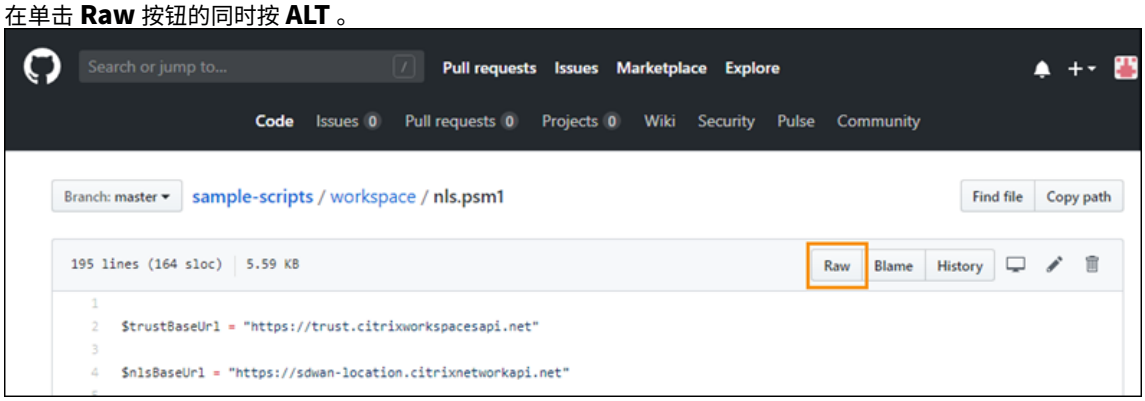
您可以使用 PowerShell 脚本来配置直接工作负载连接，而不是使用 Citrix Cloud 管理控制台界面。使用 PowerShell 进行直接工作负载连接配置涉及以下任务：

1. 确定内部用户连接的每个分支机构的公有 IP 地址范围。
2. 下载 PowerShell 模块。
3. 在 Citrix Cloud 中 @@ 创建安全 API 客户 端，并记下客户端 ID 和密钥。
4. 导入 PowerShell 模块 并使用您的 API 客户端详细信息连接到网络定位服务 (NLS)。
5. 使用您之前确定的公有 IP 地址范围为您的每个分支机构创建 NLS 站点。对于来自您指定的内部网络位置的任何启动，都会自动启用 Direct Workload Connection。
6. 从内部网络上的设备启动应用程序或桌面，并验证该连接是否绕过网关直接连接到 VDA。有关更多信息，请参阅本文中的 ICA 文件日志记录 。

下载 **PowerShell** 模块

在设置网络位置之前，请从 Citrix GitHub 存储库下载 Citrix 提供的 PowerShell 模块 (nls.psm1)。使用此模块，您可以根据需要为 VDA 设置任意数量的网络位置。

1. 在 Web 浏览器中，前往 https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1。
2. 在单击 **Raw** 按钮的同时按 **ALT** 。



3. 在计算机上选择一个位置，然后单击“保存”。

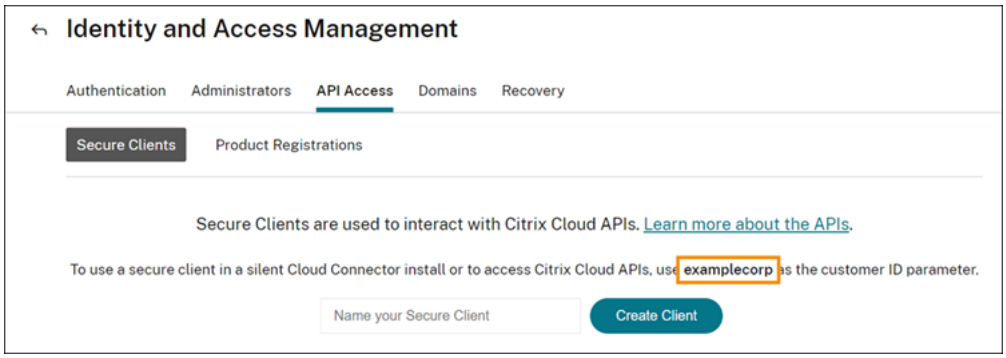
必需的配置详情

要设置网络位置，您需要以下必需信息：

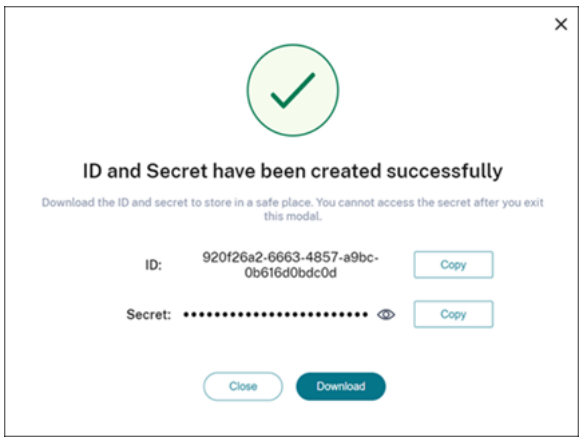
- Citrix Cloud 安全客户端客户 ID、客户端 ID 和客户端密钥。要获取这些值，请参阅本文中的 创建安全客户端 。
- 内部用户连接的网络的公用 IP 地址范围。有关这些公有 IP 地址范围的更多信息，请参阅本文中的 要求 。

创建安全的客户端

1. 登录到 Citrix Cloud，网址为 `https://citrix.cloud.com`。
2. 从 Citrix Cloud 菜单中，选择 身份和访问管理，然后选择 **API** 访问。
3. 在“安全客户端”选项卡上，记下您的客户 ID。



4. 输入客户机的名称，然后选择“创建客户端”。
5. 复制客户端 ID 和客户端密钥。



配置网络位置

1. 打开 PowerShell 命令窗口，然后导航到保存 PowerShell 模块的相同目录。
2. 导入模块：`Import-Module .\nls.psm1 -Force`
3. 使用 创建安全客户端中的安全客户端信息设置所需的变量：
   - `$clientId = "YourSecureClientID"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourSecureClientSecret"`
4. 使用您的安全客户端凭据连接到网络定位服务：

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -
    customer $customer
```

5. 创建网络位置，将参数值替换为与您的内部用户直接连接的内部网络相对应的值：

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

要指定单个 IP 地址而不是范围，请在 IP 地址末尾添加 **/32** 。例如：

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

> 重要：
>
> 使用 `New-NLSSite` 命令时，每个参数至少包含一个值。如果您在没有任何命令行参数的情况下运行此命令，PowerShell 会提示您为每个参数输入相应的值，一次只能输入一个值。`internal` 属性是一

> 个强制性的布尔属性，具有可能的值：通过 PowerShell 映射到用户界面的 $True 或 $False。例如，(UI)Network Internal -> (PowerShell)-internal=$True。

成功创建网络位置后，命令窗口将显示网络位置的详细信息。

6. 对用户连接的所有网络位置重复步骤 5。
7. 运行命令 Get-NLSSite 以返回已使用 NLS 配置的所有站点的列表，并验证其详细信息是否正确。

修改网络位置

要更改现有网络位置，请执行以下操作：

1. 在 PowerShell 命令窗口中，列出所有现有的网络位置：Get-NLSSite
2. 要修改特定网络位置的 IP 范围，请键入

   ```
   (Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
   ```

   其中 [N] 是与列表中的位置（以零开头）对应的数字，"1.2.3.4/32","4.3.2.1/32" 是要使用的逗号分隔的 IP 范围。例如，要修改列出的第一个位置，请键入以下命令：

   ```
   (Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32","141.43.0.0/24")
   ```

移除网络位置

要移除不想再使用的网络位置，请执行以下操作：

1. 在 PowerShell 命令窗口中，列出所有现有的网络位置：Get-NLSSite
2. 要移除所有网络位置，请键入 Get-NLSSite | Remove-NLSSite
3. 要移除特定的网络位置，请键入 (Get-NLSSite)[N] | Remove-NLSSite，其中 [N] 是与列表中的位置相对应的数字。例如，要移除列出的第一个位置，请键入 (Get-NLSSite)[0] | Remove-NLSSite。

检验内部启动路由是否正确

要验证内部启动是否直接访问 VDA，请使用以下方法之一：

- 通过 DaaS 控制台查看 VDA 连接。
- 使用 ICA 文件日志记录来验证客户端连接的地址是否正确。

Citrix DaaS 控制台

选择“管理”**>**“监视”，然后搜索具有活动会话的用户。在控制台的会话详细信息部分中，直接 VDA 连接显示为 UDP 连接，而网关连接显示为 TCP 连接。

如果您在 DaaS 控制台上看不到 UDP，则必须为 VDA 启用 HDX 自适应传输策略。

ICA 文件日志记录

在客户端计算机上启用 ICA 文件日志记录，如 启用 launch.ica 文件日志记录中所述。启动会话后，检查日志文件中的 **Ad** dress 和 **SSLProxyHost** 条目。

直接 **VDA** 连接　对于直接 VDA 连接，地址 属性包含 VDA 的 IP 地址和端口。

以下是客户端使用 NLS 启动应用程序时的 ICA 文件示例：

```
[Notepad++ Cloud]
Address=;10.0.1.54:1494
SSLEnable=Off
<!--NeedCopy-->
```

此文件中不存在 **SSLProxyHost** 属性。只有通过网关启动时才包含此属性。

网关连接　对于网关连接，地址属性包含 Citrix Cloud STA 票证，**SSLEnable** 属性设置为开，**SSLProxyHost** 属性包含网关的 FQDN 和端口

以下是客户端通过 Citrix Gateway 服务建立连接并启动应用程序时的 ICA 文件示例：

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
SSLEnable=On
SSLProxyHost=global.g.nssvcstaging.net:443
<!--NeedCopy-->
```

以下是 ICA 文件的示例，当客户端通过本地网关建立连接并使用在资源位置中配置的本地网关启动应用程序时：

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
SSLEnable=On
SSLProxyHost=onpremgateway.domain.com:443
<!--NeedCopy-->
```

> 注意：
>
> 用于启动虚拟应用程序和桌面的本地网关虚拟服务器必须是 VPN 虚拟服务器，而不是 nFactor 身份验证虚拟服务器。nFactor 身份验证虚拟服务器仅用于用户身份验证，不代理资源 HDX 和 ICA 启动流量。

示例脚本

该示例脚本包含可能需要添加、修改和删除分支机构位置的公有 IP 地址范围的所有命令。但是，您无需运行所有命令即可执行任何单个功能。要运行脚本，请务必包含从 **Import-Module** 到 **Connect-NLS** 的前 10 行。之后，您只能包含要执行的功能的命令。

```
Import-Module .\nls.psm1 -Force

$clientId = "XXXX" #Replace with your clientId
$clientSecret = "YYY"    #Replace with your clientSecret
$customer = "CCCCCC"  #Replace with your customerid

# Connect to Network Location Service
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer $customer

# Create a new Network Location Service Site (Replace with details corresponding to your branch locations)
New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True

# Get the existing Network Location Service Sites (optional)
Get-NLSSite

# Update the IP Address ranges of your first Network Location Service Site (optional)
$s = (Get-NLSSite)[0]
$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
\$s | Set-NLSSite

# Remove all Network Location Service Sites (optional)
Get-NLSSite | Remove-NLSSite

# Remove your third site (optional)
\(Get-NLSSite)\[2] | Remove-NLSSite
```

故障排除

VDA 启动失败

如果 VDA 会话无法启动，请验证您使用的是来自正确网络的公有 IP 地址范围。配置网络位置时，必须使用内部用户连接的网络的公有 IP 地址范围来访问 Internet。有关更多信息，请参阅本文中的 要求 。

内部 **VDA** 启动仍通过网关路由

如果内部启动的 VDA 会话仍像外部会话一样通过网关进行路由，请验证您使用的是内部用户连接的正确公有 IP 地址来访问他们的工作区。NLS 站点中列出的公用 IP 地址必须与启动资源的客户端用于访问 Internet 的地址相对应。要为客

户端获取正确的公有 IP 地址，请登录客户端计算机，访问搜索引擎，然后在搜索栏中输入“我的 IP 是什么”。

在同一办公地点启动资源的所有客户端通常都使用相同的网络出口公有 IP 地址访问 Internet。这些客户端必须具有通往 VDA 所在子网的互联网网络路由，该路径不受防火墙阻止。有关更多信息，请参阅本文中的 要求 。

在非 **Windows** 平台上运行 **PowerShell** 命令时出错

如果在 PowerShell Core 上使用正确的参数运行 cmdlet 时遇到错误，请验证该操作是否已成功执行。例如，如果在运行 New-NLSSite cmdlet 时遇到错误，请运行 `Get-NLSSite` 以验证站点是否已创建。即使操作成功运行，使用 PowerShell Core 在 macOS 或 Linux 平台上运行这些 cmdlet 也可能会导致错误。

如果您在使用 PowerShell 的 Windows 平台上使用正确的参数运行 cmdlet 时遇到此问题，请确保您使用的是最新版本的 PowerShell 模块。对于最新版本的 PowerShell 模块，Windows 平台上不会出现此问题。

其他帮助和支持

有关疑难解答帮助或疑问，请联系您的 Citrix 销售代表或 Citrix 支持人员。

服务连续性

November 26, 2023

服务连续性消除了或最大限度地减少了对连接过程中所涉及组件可用性的依赖。无论云服务的运行状况如何，用户都可以启动其 Citrix DaaS 应用程序和桌面。

服务连续性允许用户在中断期间连接到其 DaaS 应用程序和桌面，只要用户设备保持与资源位置的网络连接。在 Citrix Cloud 组件或公共和私有云中断期间，用户可以连接到 DaaS 应用程序和桌面。用户可以直接连接到资源位置或通过 Citrix Gateway 服务进行连接。

通过使用 Progressive Web Apps 服务工作线程技术在用户界面中缓存资源，服务连续性改善了停机期间已发布资源的可视化表示。

服务连续性使用 Workspace 连接租约来允许用户在停机期间访问应用程序和桌面。Workspace 连接租约是长期存在的授权令牌。Workspace 连接租用文件安全地缓存在用户设备上。当用户登录 Citrix Workspace 时，Workspace 连接租用文件将保存到发布给用户的每个资源的用户配置文件中。服务连续性允许用户在中断期间访问应用程序和桌面，即使用户以前从未启动过应用程序或桌面。Workspace 连接租用文件经过签名和加密，并与用户和用户设备相关联。启用服务连续性后，默认情况下，Workspace 连接租约允许用户在七天内访问应用程序和桌面。您可以将 Workspace 连接租约配置为允许访问长达 30 天。

用户退出 Citrix Workspace 应用程序时，Citrix Workspace 应用程序将关闭，但保留 Workspace 连接租约。用户通过右键单击系统任务栏中的 Citrix Workspace 应用程序图标或重新启动用户设备来退出 Citrix Workspace 应用

程序。您可以配置服务连续性，以便在用户在中断期间注销 Citrix Workspace 时删除或保留 Workspace 连接租约。默认情况下，当用户在中断期间注销时，会从用户设备中删除 Workspace 连接租约。

在虚拟桌面上安装 Citrix Workspace 应用程序时，双跃点方案支持服务连续性。

有关 Citrix Cloud 恢复功能（包括服务连续性）的深入技术文章，请参阅 Citrix Cloud 弹性。

> 注意：
>
> 已弃用的名为“连接租用”的 Citrix DaaS 功能与 Workspace 连接租用类似，因为它提高了中断期间的连接弹性。否则，该弃用的功能与服务连续性无关。

用户设备设置

要在中断期间访问资源，用户必须在中断发生之前登录 Citrix Workspace。启用服务连续性时，用户必须在其设备上执行以下步骤：

1. 下载并安装受支持版本的 Citrix Workspace 应用程序。
2. 将组织的 Workspace URL 添加到 Citrix Workspace 应用程序（例如 `https://example.cloud.com`）。
3. 登录 Citrix Workspace。

当用户首次登录 Citrix Workspace 时，服务连续性会将 Workspace 连接租约下载到用户设备。

下载 Workspace 连接租约可能需要长达 15 分钟才能首次登录。用户可以在下载期间继续启动已发布的资源。

中断期间的用户体验

启用服务连续性后，停机期间的用户体验会因以下因素而异：

- 中断的类型
- Citrix Workspace 应用程序是否配置了域直通身份验证
- 是否为用户连接的应用程序或桌面启用了会话共享

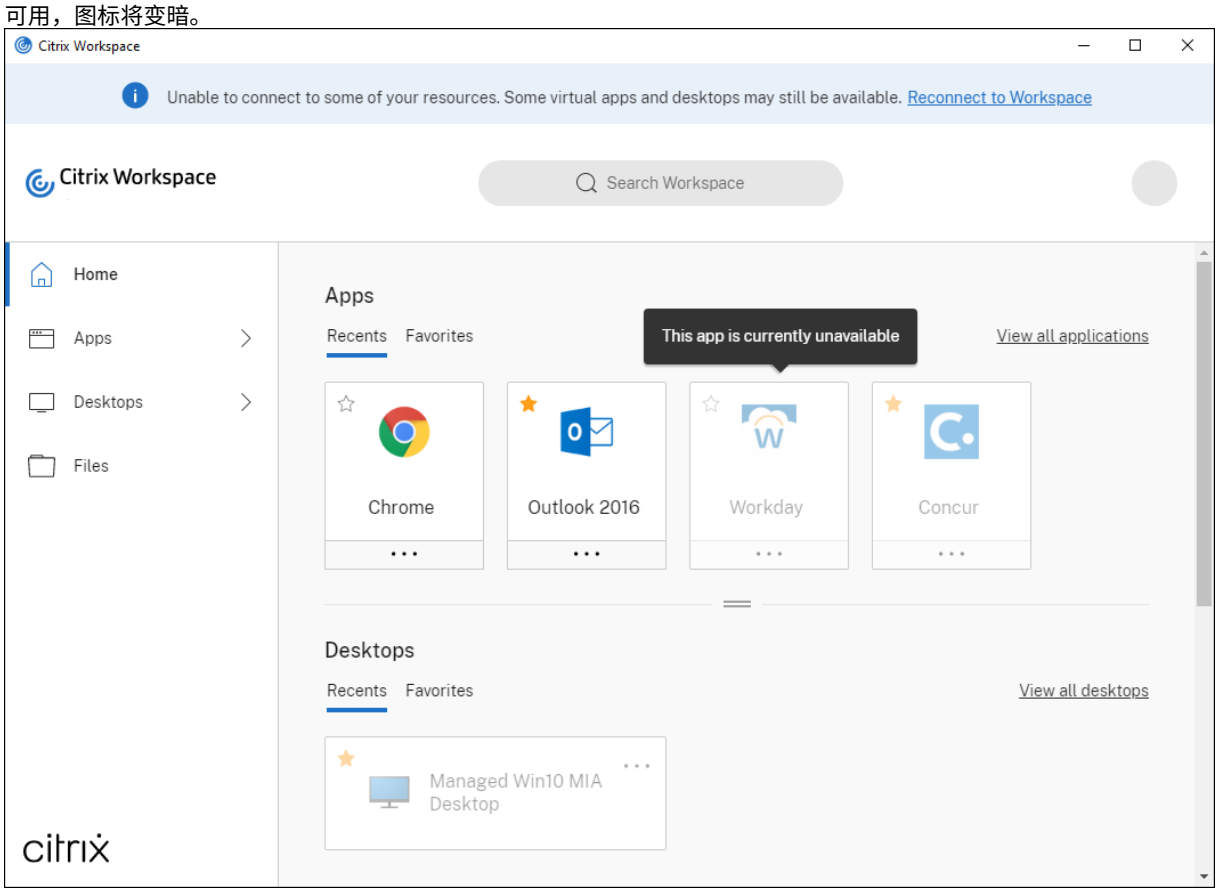
对于某些中断，用户可以继续访问其 DaaS，而不会改变其用户体验。对于其他中断，用户可能会看到 Workspace 的显示方式发生了变化，或者系统会提示用户采取一些措施。

此表总结了服务连续性如何帮助用户在不同类型的中断期间访问应用程序和桌面。

中断发生的地方	服务连续性如何维护用户访问权限	中断期间的用户体验
Citrix Workspace 服务	Citrix Workspace 应用程序根据用户设备上的本地缓存枚举应用程序和桌面。	不可用的应用程序和桌面的图标显示为灰色。用户仍然可以访问图标未变暗的应用程序和桌面。单击未变暗的图标后，系统可能会提示用户在 VDA 中重新输入其凭据。要重新获得对所有应用程序和桌面的访问权限，用户可以尝试通过单击“重新连接到 Workspace”链接来建立与 Workspace 的连接。
身份提供商	Citrix Workspace 应用程序，并根据用户设备上的本地缓存枚举应用程序和桌面。	用户可能无法登录到 Workspace。用户单击“脱机使用 Workspace”链接访问某些应用程序和桌面，体验与 Workspace 服务中断完全相同。
Citrix Cloud 代理服务	Cloud Connector 中的高可用性服务会接管代理。在 Cloud Broker 服务中注册的所有 VDA 都会在高可用性服务中注册。	在 VDA 向高可用性服务注册时，某些用户可能无法访问虚拟资源。现有会话不受影响。无需用户操作。
Secure Ticket Authority	当 ICA 文件无法访问虚拟资源时，Workspace 连接租约提供对虚拟资源的访问权限。	会话启动可能需要几秒钟的时间。无需用户操作。
Citrix Gateway 服务	网络流量故障转移到最近的运行状况良好的 Citrix Gateway 服务接入点 (POP)。	现有会话可能需要几秒钟才能重新连接。无需用户操作。
局域网上的互联网连接	Citrix Workspace 应用程序根据用户设备上的本地缓存枚举应用程序和桌面。如果用户与资源位置有直接的网络连接，则当用户单击未变暗的图标时，Citrix Workspace 应用程序将绕过 Citrix Gateway 服务。 Citrix Workspace 应用程序通过 TCP 2598 联系 Cloud Connector，通过 TCP 2598 或 UDP 2598 联系 VDA。	不可用的应用程序和桌面的图标显示为灰色。用户仍然可以访问图标未变暗的应用程序和桌面。单击未变暗的图标后，系统可能会提示用户在 VDA 中重新输入其凭据。要重新获得对所有应用程序和桌面的访问权限，用户可以尝试通过单击“重新连接到 Workspace”链接来建立与 Workspace 的连接。

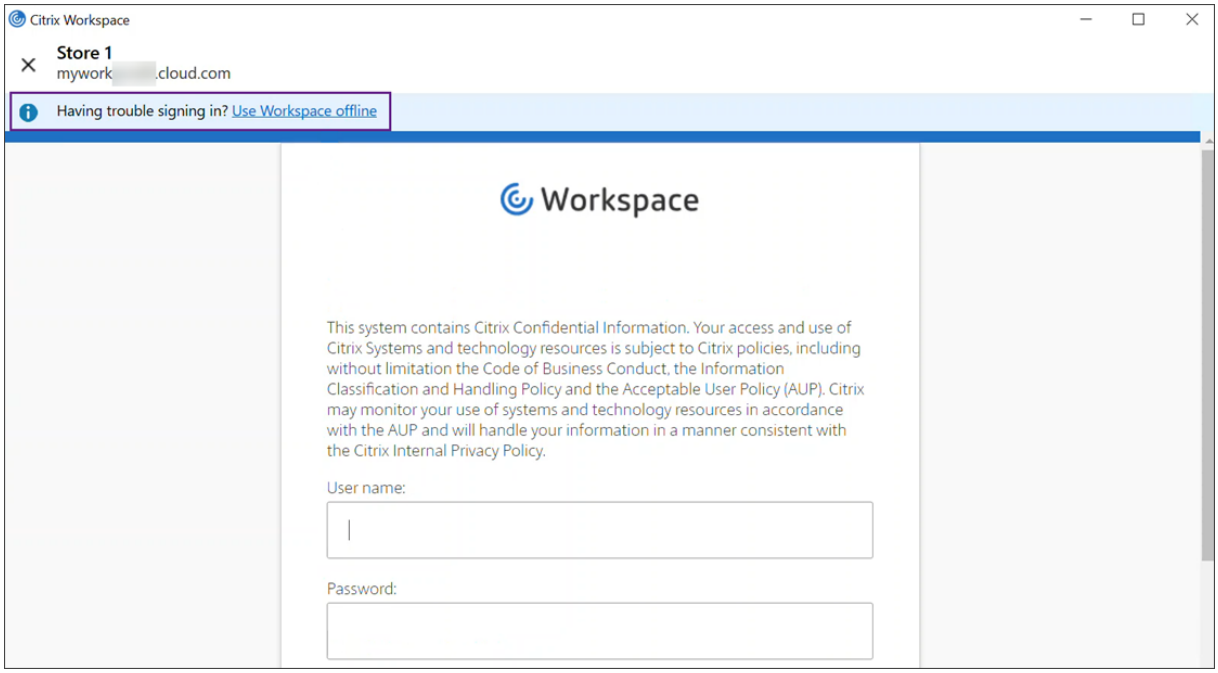
> 注意：
>
> 有关在非生产环境中验证停机情况的信息，请参阅服务连续性配套指南。

在 Citrix Workspace 中断期间，用户会在 Citrix Workspace 主页顶部看到以下消息：“无法连接到您的某些资源。一些虚拟应用程序和桌面可能仍然可用。”用户可以看到在中断期间可以连接的应用程序和桌面。如果应用程序或桌面不可用，图标将变暗。



要在中断期间访问可用资源，用户可以选择不变灰的资源图标。如果出现提示，用户将在访问资源之前在 VDA 重新输入其 AD 凭据。

在工作区身份验证的身份提供程序中断期间，用户可能无法通过工作区登录页面登录 Citrix Workspace。40 秒后，此消息将显示在 Citrix Workspace 主页的顶部。



之后，将显示 Citrix Workspace 主页。然后，用户可以像在 Citrix Workspace 中断期间一样访问资源。

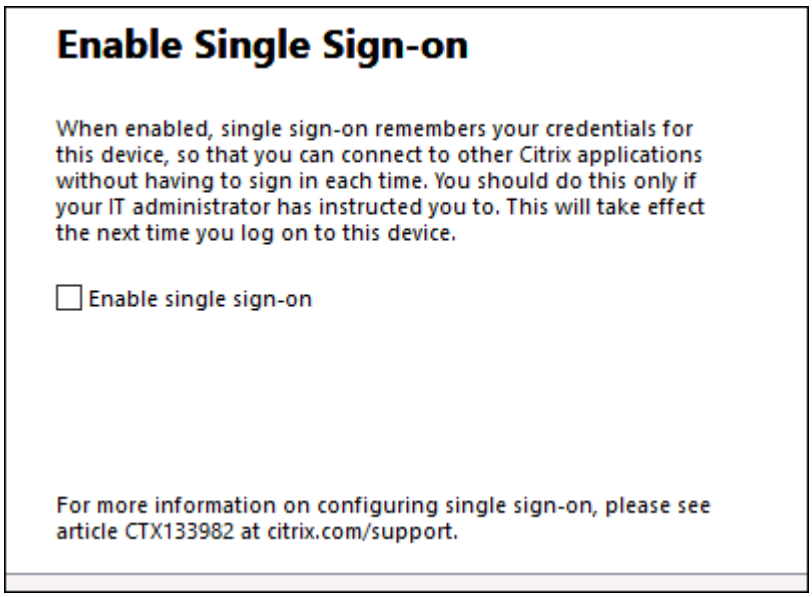
无论中断的类型如何，如果用户退出并重新启动 Citrix Workspace 应用程序，他们都可以继续访问资源。用户可以在不失去资源访问权限的情况下重启其用户设备。

在服务连续性的默认配置中，如果用户注销 Citrix Workspace，则无法访问其资源。如果希望用户在注销后保留对其资源的访问权限，请指定在用户注销时保留 Workspace 连接租约。请参见 配置服务连续性。

根据 Citrix Workspace 应用程序和 VDA 的配置方式，在中断期间，VDA 可能会提示用户在 Windows 登录用户界面中输入其凭据。如果出现此提示，则用户输入其 Active Directory (AD) 凭据或智能卡 PIN 以访问应用程序或桌面。如果在中断期间未传递用户凭据，则需要执行此步骤。在访问应用程序或桌面之前，用户必须重新向 VDA 进行身份验证。

在以下情况下，用户无需输入 AD 凭据即可访问资源：

- 通过选中单点登录框，Citrix Workspace 可在安装期间配置为单点登录。



- Citrix Workspace 应用程序配置了域直通身份验证。在 Citrix Workspace 中断期间，用户无需输入凭据即可访问任何可用资源。有关为适用于 Windows 的 Citrix Workspace 应用程序配置域直通身份验证的信息，请参阅身份验证文档中的使用图形用户界面配置单点登录。

  > 注意
  >
  > 在中断期间，不需要 StoreFront 来允许单点登录您的 VDA。

- 会话共享已启用。用户在为同一 VDA 上的一个资源提供凭据后，即可访问托管在同一 VDA 上的应用程序或桌面。会话共享是为包含 VDA 上资源的应用程序组配置的。有关配置应用程序组的信息，请参阅 创建应用程序组。

在所有其他配置中，系统会提示用户在访问资源之前在 VDA 重新输入其 AD 凭据。

要求和限制

现场要求

- 使用 Workspace 体验时，所有版本的 Citrix DaaS 和 Citrix DaaS Standard for Azure 均受支持。
- 不支持将站点聚合到本地 Virtual Apps and Desktops 的 Citrix Workspace。
- 将本地 Citrix Gateway 用作 ICA 代理时不受支持。（支持使用 Citrix Gateway 作为工作区身份验证方法。）

用户设备要求

支持的最低 Citrix Workspace 应用程序版本：

- 适用于 Windows 的 Citrix Workspace 应用程序 2106
- 适用于 Linux 的 Citrix Workspace 应用程序 2106

- 适用于 Mac 的 Citrix Workspace 应用程序 2106
- 适用于 Android 22.2.0 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 22.4.5
- 适用于 ChromeOS 的 Citrix Workspace 应用程序 2301

> 注意：
>
> 有关安装适用于 Linux 的 Citrix Workspace 应用程序的信息，包括有关安装应用程序以实现服务连续性的信息，请参阅适用于 Linux 的 Citrix Workspace 应用程序。

- 对于使用浏览器访问其应用程序和桌面的用户：
  - Google Chrome 或 Microsoft Edge。
  - 至少适用于 Windows 的 Citrix Workspace 应用程序 2109。支持 Google Chrome 和 Microsoft Edge。
  - 适用于 Mac 的 Citrix Workspace 应用程序最低版本 2112 适用于 Google Chrome。
  - 适用于 Mac 的 Citrix Workspace 应用程序至少 2206 版可与 Safari 浏览器配合使用

  请参阅 浏览器中的服务连续性。
- 每台设备仅支持一个用户。不支持网亭或“移动办公桌”用户设备。

支持的 **Workspace** 身份验证方法

- Active Directory
- Active Directory 加令牌
- Azure Active Directory
- Okta
- Citrix Gateway（主用户声明必须来自 AD）
- SAML 2.0

身份验证限制

- 不支持使用 Citrix 联合身份验证服务 (FAS) 进行单点登录。用户在 VDA 上的 Windows 登录用户界面中输入其 AD 凭据。
- 不支持单点登录到 VDA。
- 不支持本地映射帐户。
- 不支持加入到 Azure AD 的 VDA。所有 VDA 都必须加入到 AD 域。

Citrix Cloud Connector 规模和大小

- 4 个 vCPU 或更多
- 4 GB 或更大内存

Citrix Cloud Connector Powershell 安全性

通过将执行策略设置为适合您的环境的 **remotedSigned** 值，确保启用脚本执行。
其他脚本执行权限也可以起作用，例如 **Default** 或 **AllSigned**。

Citrix Cloud Connector 连接

Citrix Cloud Connector 必须能够访问 `https://rootoftrust.apps.cloud.com`。配置防火墙以允许此连接。有关 Cloud Connector 防火墙的信息，请参阅 Cloud Connector 代理和防火墙配置。

Workspace 应用程序网络连接

如果配置从局域网外部到资源位置的连接，则用户设备上的 Workspace 应用程序必须能够访问 Citrix Gateway 服务 FQDN `https://*.g.nssvc.net`。确保将防火墙配置为允许传出流量 `https://global-s.g.nssvc.net:433`，以便用户设备可以随时连接到 Citrix Gateway 服务。

连接优化限制

不支持高级端点分析 (EPA)。

中断期间不支持 Enlightened Data Transport (EDT)。

VDA 要求和限制

- 支持 VDA 7.15 LTSR 或任何尚未到期的最新版本。
- 不支持加入到 Azure AD 的 VDA。所有 VDA 都必须加入到 AD 域。
- VDA 必须处于联机状态，以便用户在中断期间访问 VDA 资源。当 VDA 受到中断影响时，VDA 资源不可用：
  - AWS
  - Azure
  - 云 Delivery Controller，除非为交付资源的交付组启用了 AutoScale
- 中断期间支持的 VDA 工作负载：
  - 托管共享应用程序和桌面
  - 具有电源管理功能的随机非持久桌面（池 VDI 桌面）
  - 静态非持久桌面
  - 静态永久桌面，包括 Remote PC Access

> 注意：
>
> 中断期间不支持首次使用时分配。如果 Cloud Connector 与 Citrix Cloud 断开连接，则默认情况下，具有电源管理功能的随机非永久桌面不可用，除非为交付组配置了 `ReuseMachinesWithoutShutdownInOutage`。有关更多详细信息，请查看应用程序和桌面支持。

有关中断期间可用 VDA 功能的详细信息，请参阅 中断期间的 VDA 管理。

本地键盘映射要求和限制

提示用户在 VDA 上重新进行身份验证的 Windows 登录用户界面不支持本地键盘语言映射。要允许用户在设备上具有本地键盘语言映射的情况下在中断期间重新进行身份验证，请预加载这些用户所需的键盘布局。

> 警告：
>
> 注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。在编辑注册表之前，请务必进行备份。

在 VDA 映像中编辑以下注册表项：

`HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`

必须安装虚拟桌面映像中的相应语言包。

有关与键盘语言关联的键盘标识符的列表，请参阅 适用于 Windows 的键盘标识符和输入法编辑器。

配置资源位置网络连接以实现服务连续性

您可以将资源位置配置为接受来自 LAN 内部、局域网外部或两者的连接。

配置 **LAN** 内部的连接

1. 从 Citrix Cloud 菜单中，转到 **Workspace** 配置 **>** 访问权限。
2. 选择 配置连通性。
3. 选择“仅限内部”作为您的连接类型。
4. 单击保存。

将 Citrix Cloud Connector 和 VDA 防火墙配置为接受通过通用网关协议 (CGP) TCP 端口 2598 进行的连接。此配置是默认设置。

配置来自 **LAN** 外部的连接

1. 从 Citrix Cloud 菜单中，转到 **Workspace** 配置 **>** 访问权限。
2. 选择 配置连通性。
3. 选择 网关服务 作为您的连接类型。
4. 单击保存。

配置来自 **LAN** 外部和内部的连接

运行这个 PowerShell 命令：

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocationE
)-EnableHybridConnectivityForResourceLeases $true
```

将 `YourResourceLocationExternalUid` 替换为资源位置的外部 UID。

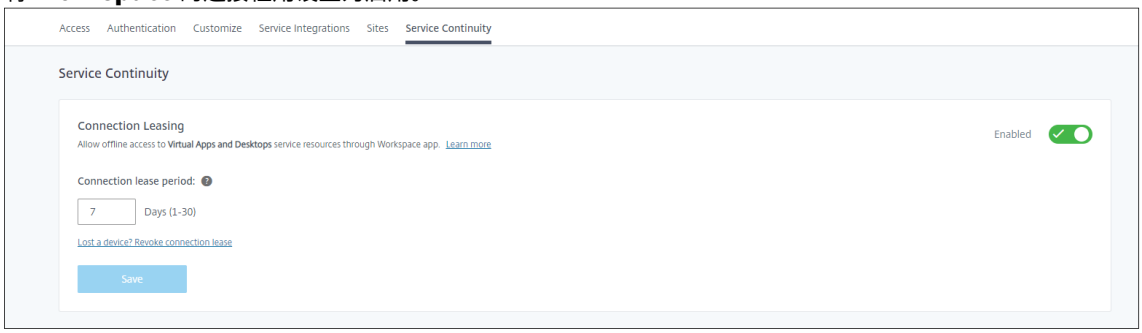
此命令允许在中断期间通过 TCP 2598 直接连接到 Citrix Cloud Connector FQDN。如果该连接失败，则使用网关服务作为后备。允许内部用户绕过网关直接连接到资源位置可减少内部网络流量的延迟。

> 注意：
>
> 此 PowerShell 命令与直接工作负载连接类似，因为它通过允许内部用户绕过网关直接连接到 VDA 来优化与工作区的连接。启用服务连续性后，直接工作负载连接在中断期间不可用。

配置服务连续性

要为您的站点启用服务连续性，请执行以下操作：

1. 从 Citrix Cloud 菜单中，转到 **Workspace** 配置 **>** 服务连续性。
2. 将 **Workspace** 的连接租用设置为启用。



3. 将 连接租用期限 设置为 Workspace 连接租用可用于维护连接的天数。Workspace 连接租用期限适用于通过您的站点进行的所有 Workspace 连接租用。Workspace 连接租用期从用户首次登录 Citrix Cloud Workspace 应用商店时开始。用户每次登录时都会刷新 Workspace 连接租约，最多每天刷新一次。Workspace 连接租用期可以是 1 天到 30 天。默认值为七天。
4. 单击保存。

启用服务连续性后，将为站点中的所有交付组启用该功能。要禁用交付组的服务连续性，请使用以下 PowerShell 命令：

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

`deliverygroup` 替换为交付组的名称。

默认情况下，如果用户在中断期间退出 Citrix Workspace，则会从用户设备中删除 Workspace 连接租约。如果希望在用户注销后仍保留用户设备上的 Workspace 连接租约，请使用以下 PowerShell 命令：

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

> 注意：
>
> 在用户注销与适用于 Mac 的 Citrix Workspace 应用程序连接的用户后，无法将 Workspace 连接租约设置为保留在用户设备上。适用于 Mac 的 Citrix Workspace 无法读取 `DeleteResourceLeaseOnLogOff` 属性的值。

服务连续性如何运作

如果没有中断，用户将使用 ICA 文件访问虚拟应用程序和桌面。每当用户选择虚拟应用程序或桌面图标时，Citrix Workspace 都会生成一个唯一的 ICA 文件。每个 ICA 文件都包含一个 Secure Ticket Authority (STA) 票证和一个登录票证，只能兑换一次以获得对虚拟资源的授权访问权限。每个 ICA 文件中的票证将在大约 90 秒后过期。使用 ICA 文件中的票证或到期后，用户需要从 Citrix Workspace 获得另一个 ICA 文件才能访问资源。如果未启用服务连续性，如果 Citrix Workspace 无法生成 ICA 文件，中断可能会阻止用户访问资源。

无论是否启用了服务连续性，Citrix Workspace 都会在用户启动虚拟应用程序和桌面时生成 ICA 文件。启用服务连续性后，Citrix Workspace 还会生成构成 Workspace 连接租约的唯一文件集。与 ICA 文件不同，Workspace 连接租用文件是在用户登录 Citrix Workspace 时生成的，而不是在用户启动资源时生成的。当用户登录 Citrix Workspace 时，将为发布给该用户的每个资源生成连接租用文件。Workspace 连接租约包含允许用户访问虚拟资源的信息。如果中断导致用户无法登录 Citrix Workspace 或使用 ICA 文件访问资源，则连接租约将提供对资源的授权访问权限。

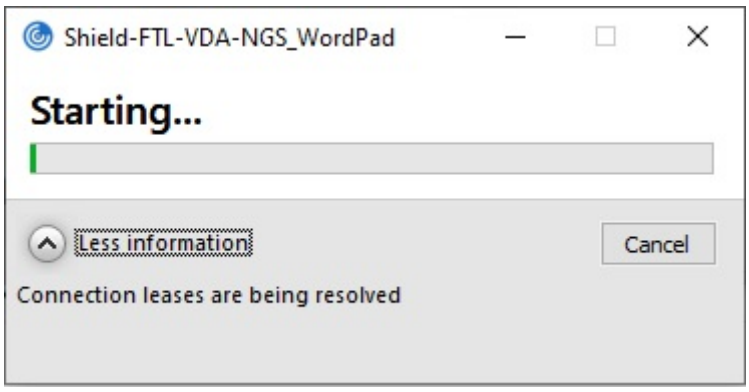
会话在中断期间如何启动

当用户在中断期间单击应用程序或桌面的图标时，Citrix Workspace 应用程序会在用户设备上找到相应的 Workspace 连接租约。然后，Citrix Workspace 应用程序会打开一个连接。如果将与托管应用程序或桌面的资源位置的连接配置为接受来自局域网外部的连接，则会打开与 Citrix Gateway 服务的连接。如果您将与托管应用程序或桌面的资源位置的连接配置为仅接受来自局域网内部的连接，则会打开与 Cloud Connector 的连接。

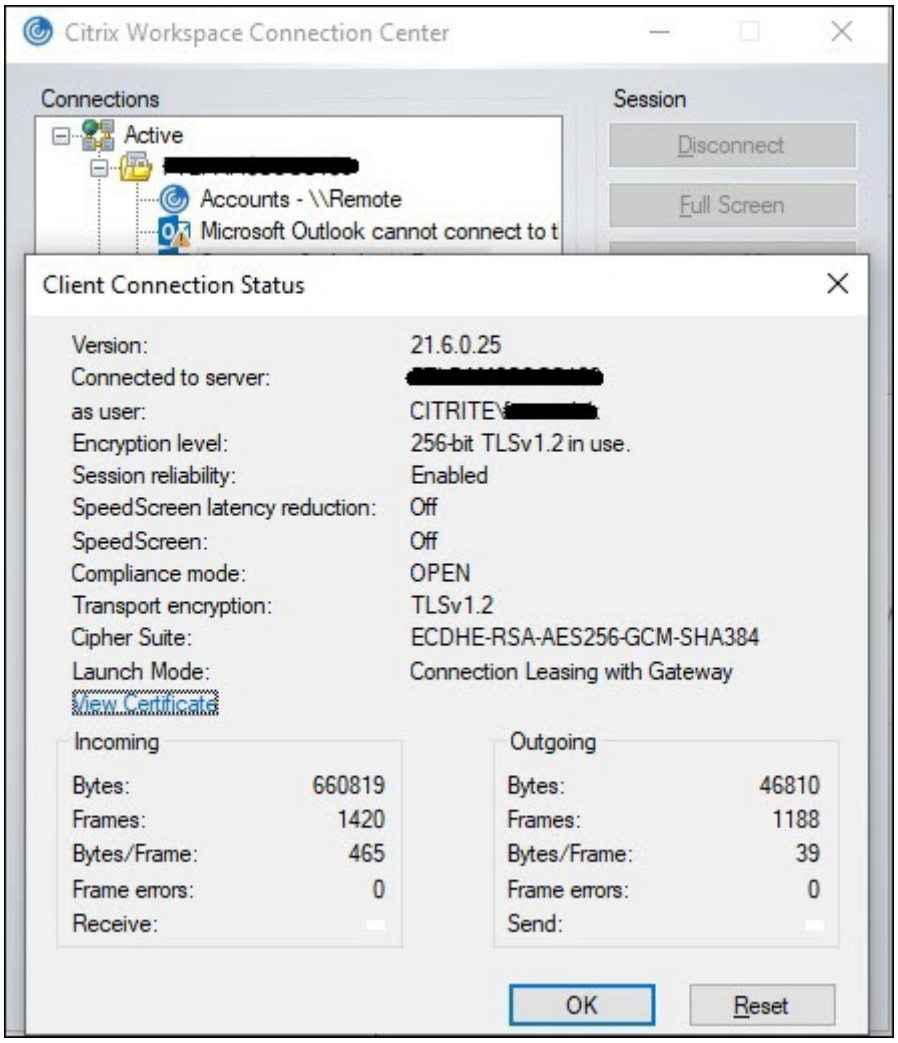
当 Citrix Cloud 代理处于联机状态时，Cloud Connector 将使用 Citrix Cloud 代理来解析哪个 VDA 可用。当 Citrix Cloud 代理处于脱机状态时，Cloud Connector（也称为高可用性服务）的辅助代理将侦听并处理连接请求。

发生中断时连接的用户可以继续不间断地工作。重新连接和新连接会遇到最短连接延迟。此功能类似于本地主机缓存，但不需要本地 StoreFront。

当用户在中断期间启动会话时，会出现此窗口，指示会话启动使用了 Workspace 连接租约：



用户登录完会话后，这些属性将显示在 Workspace 连接中心中：



启动模式属性提供有关用于启动会话的 Workspace 连接租约的信息。

在运行适用于 Mac 的 Citrix Workspace 应用程序的设备上，Citrix Viewer 显示的信息表明 Workspace 连接租约用于会话启动：

是什么让它安全

Workspace 连接租用文件中的所有敏感信息均使用 AES-256 密码进行加密。Workspace 连接租约绑定到与特定客户端设备唯一关联的公钥/私钥对，不能在其他设备上使用。内置的加密机制强制在每台设备上使用唯一的密钥对。

Workspace 连接租约存储在 AppData\Local\Citrix\SelfService\ConnectionLeases 中的用户设备上。

服务连续性的安全架构建立在公钥密码学之上，类似于公钥基础设施 (PKI)，但没有证书链和证书颁发机构。相反，所有组件都依靠名为信任根的新 Citrix Cloud 服务（其行为类似于证书颁发机构）来建立传递信任。

区块连接租约

如果用户设备丢失或被盗，或者用户帐户被关闭或泄露，则可以阻止 Workspace 连接租用。当您阻止与用户关联的 Workspace 连接租约时，该用户无法连接到资源。Citrix Cloud 不再为用户生成或同步工作区连接租约。

当您阻止与某个用户帐户关联的 Workspace 连接租用时，会阻止与该帐户关联的所有设备上的连接。您可以阻止用户或用户组中的所有用户的 Workspace 连接租约。

要撤消单个用户或用户组的 Workspace 连接租约，请使用以下 PowerShell 命令：

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays
 Days
```

替换为 `username` 与要阻止连接的帐户关联的用户。`username` 替换为用户组以阻止用户组中所有帐户的连接。`Days` 替换为连接被阻止的天数。

例如，要在接下来的 7 天内阻止 xd.local/user1 的连接，请键入以下内容：

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
    LeaseRevocationDays 7
```

要查看撤销 Workspace 连接租约的时间段，请使用以下 PowerShell 命令：


```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

`username` 替换为要查看其时间段的用户或用户组。

例如，要查看撤销 xd.local/user1 的 Workspace 连接租约的时间段，请键入：

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

此信息将显示：

```
1 FullName                          :
2 Name                              : XD\user2
3 UPN                               :
4 Sid                               : S-1-5-21-nnnnnn
5 LeaseRevocationDays               : 2
6 LeaseRevocationDateTimeInUtc      : 2020-12-17T17:34:25Z
7 LastUpdateDateTimeInUtc           : 2020-12-19T17:34:25Z
```

从此输出中，您可以看到，用户 xd.local/user2 在 UTC 每天 17:34:25 撤销了 2020 年 12 月 17 日至 2020 年 12 月 19 日两天的 Workspace 连接租约。

要允许撤销了 Workspace 连接租约的用户帐户再次接收连接，请使用以下 PowerShell 命令移除该块：

```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

`username` 替换为要接收连接的被阻止的用户或用户组。要允许所有被封禁的用户帐户接收连接，请省略 `Name` 选项。

双跃点场景

如果用户在中断之前登录 Citrix Workspace，则服务连续性可以允许用户在双跃点场景中断期间访问虚拟资源。在双跃点方案中，物理用户设备连接到安装了 Citrix Workspace 应用程序的虚拟桌面。然后，虚拟桌面连接到另一个虚拟资源。

在双跃点方案中，服务连续性允许用户在停机期间访问虚拟资源，而不管虚拟桌面的类型如何。如果虚拟桌面保留用户更改，则服务连续性还可以在用户未登录时发生的停机期间提供对虚拟资源的访问权限。

服务连续性将双跃点场景中的物理用户设备和虚拟设备视为单独的客户端端点。每台设备都有自己的 Workspace 连接租约集。当用户在物理设备上登录 Citrix Workspace 时，Workspace 连接租用文件将下载并保存到物理设备上的用户配置文件中。然后，用户访问虚拟桌面并登录到该虚拟桌面上的 Citrix Workspace。此时，将下载另一组 Workspace 连接租约，并将用户配置文件保存在虚拟桌面上。Workspace 连接租用文件与下载到的设备相关联。Workspace 连接租用文件不能复制到其他设备并重复使用，即使是同一个用户也是如此。因此，如果虚拟桌面放弃用户会话期间所做的更改，则在会话结束后发生的中断期间，服务连续性将无法提供对资源的访问。对于此类虚拟桌面，Workspace 连接租用属于已放弃的更改之一。

以下是每种受支持的虚拟桌面的双跃点方案中服务连续性的工作方式。

对于包括…的双跃点	服务连续性可以在停机期间提供对虚拟资源的访问…
托管共享桌面	如果在用户登录虚拟桌面时发生中断。
随机非持久桌面（池 VDI 桌面）	如果在用户登录虚拟桌面时发生中断。
静态非持久桌面	如果自用户上次登录以来虚拟桌面尚未重新启动。
静态持久桌面	任何时候发生中断。

停机期间的 **VDA** 管理

服务连续性使用 Citrix Cloud Connector 中的 本地主机缓存 功能。当云 Delivery Controller 与 Cloud Connector 之间的连接失败时，本地主机缓存允许在站点上继续进行连接代理。由于服务连续性依赖于本地主机缓存，因此它与本地主机缓存有一些共同的限制。

> 注意：
>
> 尽管服务连续性在 Cloud Connector 中使用本地主机缓存，但与本地主机缓存不同，本地 StoreFront 不支持服务连续性。

停机期间的 **VDA** 电源管理

如果 Cloud Connector 断开了与 Citrix Cloud 的连接，连接器将无法从 Citrix Cloud 接收虚拟机管理程序凭据。这意味着：

- 在停机期间，所有计算机都处于未知电源状态，无法启动任何电源操作。但是，已打开电源的主机上的 VM 可以用于连接请求。

默认情况下，如果 Cloud Connector 与 Citrix Cloud 断开连接，则启用了 **ShutdownDesktopsAfterUse** 属性的池化交付组中由电源管理的桌面 VDA 不可用于新连接。您可以通过在交付组上配置 `ReuseMachinesWithoutShutdownInOutage` 标记来更改此设置，以便在 Cloud Connector 断开与 Citrix Cloud 的连接时允许使用这些桌面。将 `ReuseMachinesWithoutShutdownInOutage` 参数更改为 $true 可能会导致先前用户会话中的数据一直存在于 VDA 中，直到 VDA 重新启动为止。

停电后恢复正常运行时，电源管理将恢复。

计算机分配和自动注册

仅当在正常操作过程中发生了分配时，才可以使用分配的计算机。在中断期间不能执行新分配。

无法自动注册和配置 Remote PC Access 计算机。但是，正常操作过程中注册和配置的计算机可以使用。

不同区域中的 **VDA** 资源

如果资源在不同的区域中，服务器托管的应用程序和桌面用户使用的会话可能超过其配置的会话限制。

与本地主机缓存不同，服务连续性可以从不同区域中的已注册 VDA 启动应用程序和桌面，前提是资源发布在多个区域中。Citrix Workspace 应用程序可能需要更长的时间才能找到正常运行的区域，因为它会按顺序循环浏览工作区连接租约中的所有区域。

监视和故障排除

服务连续性主要执行两个操作：

- 将 Workspace 连接租约下载到用户设备。Workspace 连接租约是生成的，并与 Citrix Workspace 应用程序同步。
- 使用 Workspace 连接租约启动虚拟桌面和应用程序。

下载 **Workspace** 连接租约故障排除

您可以在用户设备上的此位置查看 Workspace 连接租约。

在 Windows 设备上：

`C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\Store GUID\User GUID\leases`

`Username` 是用户名。

`Store GUID` 是 Workspace 应用商店的全局唯一标识符。

`User GUID` 是用户的全局唯一标识符。

在 Mac 设备上：

`$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot`

例如，打开 `/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot`

在 Linux 上：

`$HOME/.ICAClient/cache/ConnectionLease`

例如，打开 `/home/user1/.ICAClient/cache/ConnectionLease`

Workspace 连接租约是在 Citrix Workspace 应用程序连接到 Workspace 应用商店时生成的。查看用户设备上的注册表项值，以确定 Citrix Workspace 应用程序是否已成功联系 Citrix Cloud 中的 Workspace 连接租赁服务。

在用户设备上打开注册表编辑器并查看以下密钥：

`HKCU\Software\Citrix\Dazzle\Sites\store-xxxx`

如果这些值出现在注册表项中，则 Citrix Workspace 应用程序已联系或尝试联系 Workspace 连接租赁服务：

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

如果 Citrix Workspace 应用程序尝试联系 Workspace 连接租用服务未成功，则会 `leaseLastCallHomeTime` 显示带有无效时间戳的错误：

```
leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM
```

如果 `leaseLastCallHomeTime` 未初始化，Citrix Workspace 应用程序将永远不会尝试联系工作区连接租赁服务。要解决此问题，请从 Citrix Workspace 应用程序中删除该帐户，然后重新添加。

工作区连接租用的 **Citrix Workspace** 应用程序错误代码

当用户设备上出现服务连续性错误时，错误消息中将显示错误代码。常见错误包括：

错误代码：	说明
3000	不存在连接租用文件
3002	无法读取或找到连接租约
3003	未找到资源位置
3004	租约中缺少连接详情
3005	ICA 文件为空
3006	连接租约已过期。重新登录到 Workspace。
3007	连接租约无效
3008	连接租用验证结果：空
3009	连接租用验证结果：无效
3010	缺少参数
3020	连接租用验证失败
3021	未找到发布应用程序的资源位置
3022	连接租用验证结果：拒绝
3023	Citrix Workspace 应用程序已超时
3024	用户取消了基于租约的启动
3025	超过启动重试次数的次数

错误代码：	说明
3026	协商的资源（应用程序或桌面）无法启动

访问 **selfservice.txt**

要访问 `selfservice.txt` 文件以进行自助故障排除，请执行以下步骤：

1. 创建一个空白文本文件并命名它 `enableshieldandlogging.reg`。
2. 将以下文本复制到文件中并保存：

   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle]
   “Tracing” =” True”
   “AuxTracing” =” True”
   “DefaultTracingConfiguration” =” global all -detail”
   “ConnectionLeasingEnabled” =” True”

   [HKEY_CURRENT_USER\Software\Citrix\Dazzle]
   “RemoteDebuggingPort” =” 8088”
3. 将保存的文件放入客户端终端节点。
4. `selfservice.txt` 文件现在可以在以下路径中找到：`%LocalAppData%\Citrix\SelfService`。

浏览器中的服务连续性

Google Chrome 和 Microsoft Edge 的扩展程序为使用这些浏览器访问应用程序和桌面的 Windows 用户提供了服务连续性。这些扩展程序被称为 Citrix Workspace Web 扩展程序，可在 Chrome 网上应用店和 Microsoft Edge 附加组件网站上找到。

这些浏览器扩展需要在用户设备上安装本机 Citrix Workspace 应用程序才能支持服务连续性。支持以下版本：

- 至少适用于 Windows 的 Citrix Workspace 应用程序 2109。支持 Google Chrome 和 Microsoft Edge。
- 适用于 Mac 的 Citrix Workspace 应用程序至少为 2112 版。支持 Google Chrome。
- 适用于 Mac 的 Citrix Workspace 应用程序至少 2206 版可与 Safari 浏览器配合使用

不支持适用于 Windows 的 Citrix Workspace 应用程序（应用商店）。

本机 Workspace 应用程序使用浏览器扩展程序的本机消息传递主机协议与 Citrix Workspace Web 扩展进行通信。本机 Workspace 应用程序和 Workspace Web 扩展一起使用 Workspace 连接租约，允许浏览器用户在停机期间访问其应用程序和桌面。

此视频展示了如何在浏览器中安装和使用服务连续性。

这是一个嵌入式视频。单击链接观看视频

浏览器用户的用户设备设置

要在浏览器中使用服务连续性，用户必须在其设备上执行以下步骤：

1. 下载并安装浏览器用户支持的 Citrix Workspace 应用程序版本。
2. 下载并安装适用于 Chrome 或 Edge 的 Citrix Workspace 网络扩展程序。

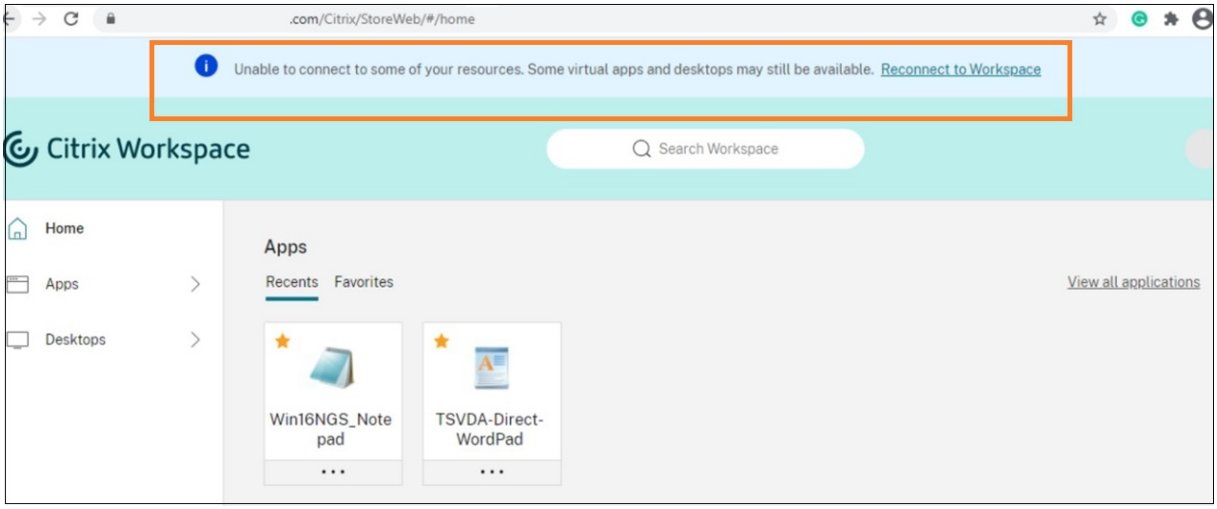
浏览器用户体验

当用户单击其应用程序或桌面时，应用程序或桌面将打开，而不会提示用户打开 **Citrix Workspace** 启动器。

停机期间的浏览器用户体验

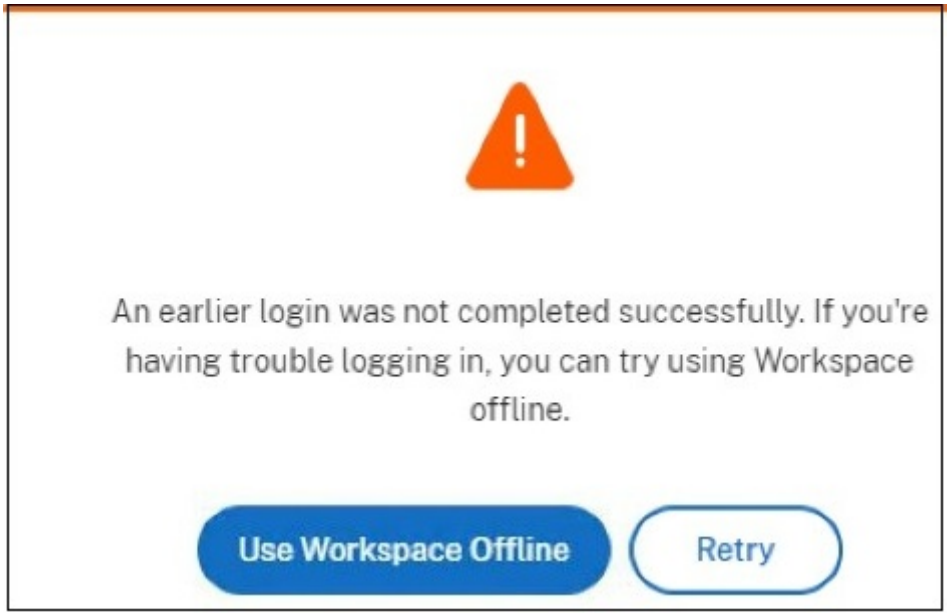
用户可以在中断期间通过浏览器访问其应用程序和桌面，只要用户设备保持与资源位置的网络连接。

如果用户通过浏览器登录 Workspace 时发生中断，则会在浏览器窗口顶部附近显示以下消息：



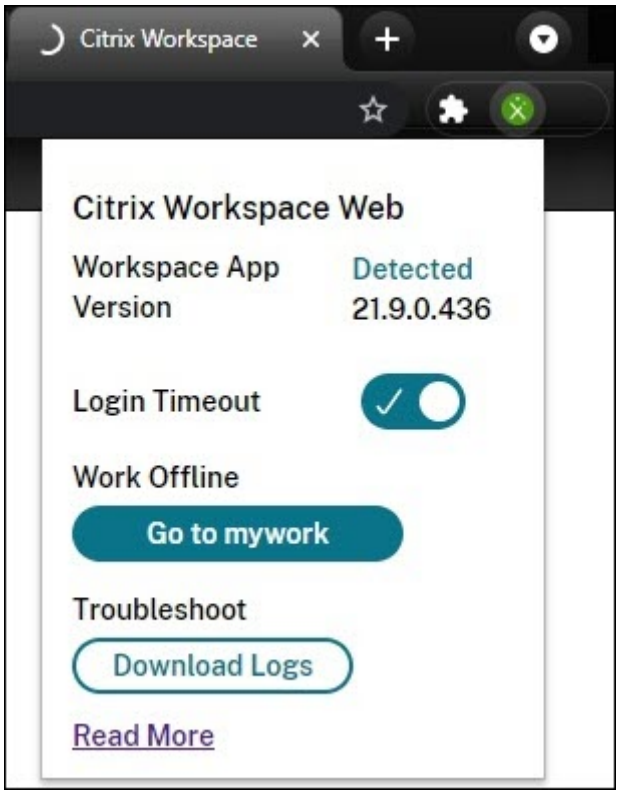
用户可以通过单击任何未变灰的图标来访问离线可用的应用程序和桌面。用户也可以尝试通过单击“重新连接到 **Workspace**”来恢复联机。

当中断导致用户无法通过浏览器登录 Workspace 时，系统会提示用户脱机工作或尝试重新登录。要脱机访问可用的应用程序和桌面，用户可单击离线 使用 **Workspace**。



如果中断阻止用户在导航到 Workspace URL 后登录到 Workspace，则窗口将在指定的超时间隔后显示。默认情况下，该窗口会在用户导航到 Workspace URL 30 秒后显示。您可以将此值设置为 15、30、45 或 60 秒。您也可以禁用登录超时。如果禁用登录超时，则当用户导航到 Workspace URL 时，将显示提示用户脱机工作的窗口。

要配置登录超时设置，请单击用户设备浏览器中的扩展程序图标。使用显示的窗口启用或禁用登录超时并设置超时持续时间：



如果浏览器已重定向到第三方身份提供商身份验证站点，中断可能会阻止用户登录。在这种情况下，用户可以在浏览器

中键入 Workspace URL，这会显示提示用户脱机工作的窗口。用户不必等到登录超时间隔后才会显示窗口。

用户还可以通过以下方式访问停机期间可用的应用程序和桌面：

1. 在浏览器中单击扩展程序图标。
2. 在出现的窗口中，单击“脱机工作”下的按钮。此按钮显示转至，然后显示您的 Workspace 应用商店的名称。
3. 在出现的窗口中，单击“脱机使用 **Workspace**”。

在某些中断期间，当扩展程序检测到 Workspace 端问题时，会自动显示提示用户脱机工作的警告窗口。用户无需在登录超时间隔内执行任何操作或等待。

浏览器限制

如果用户在中断期间清除浏览器中的 Cookie 和其他网站数据，则在他们再次向 Workspace 进行身份验证之前，服务连续性将无法正常工作。

除非用户允许扩展程序在隐身模式下工作，否则在隐身模式下不支持服务连续性。

浏览器用户疑难解答

在 Citrix Workspace 浏览器应用程序帐户设置的 高级 菜单中，确保应用程序和桌面启动的当前方法首选项设置为 使用 **Citix Workspace** 应用程序。如果将此选项设置为 使用 **Web** 浏览器，则浏览器不支持服务连续性。

确保浏览器加载 Workspace URL 后，浏览器中的扩展图标显示为绿色。

要下载日志，请单击浏览器中的扩展程序图标。然后单击“下载日志”。

使用 **Citrix** 联合身份验证服务为工作区启用单点登录

November 26, 2023

Citrix 联合身份验证服务 (FAS) 支持在 Citrix Workspace 中对 DaaS 进行单点登录 (SSO)。如果您使用以下身份提供商之一进行 Citrix Workspace 身份验证，通常会采用 FAS：

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

使用 FAS，订阅者只需输入一次凭据即可访问其 DaaS 应用程序和桌面。

如果您使用的是 Active Directory (AD)、AD plus 令牌或 Citrix Gateway 的特定配置，则对 DaaS 的 SSO 不需要 FAS。有关配置 Citrix Gateway 的更多信息，请访问 在本地 Citrix Gateway 上创建 OAuth IdP 策略。

FAS 服务器

在每个资源位置中，可以将多个 FAS 服务器连接到 Citrix Cloud，以便进行负载平衡和故障转移。

Citrix Cloud 支持在以下情况下使用 FAS 服务器。

在这两种情况下，通过联合身份提供商登录其工作区的订阅者只需输入一次凭据即可访问应用程序和桌面。

通过单个资源位置连接的 **FAS** 服务器

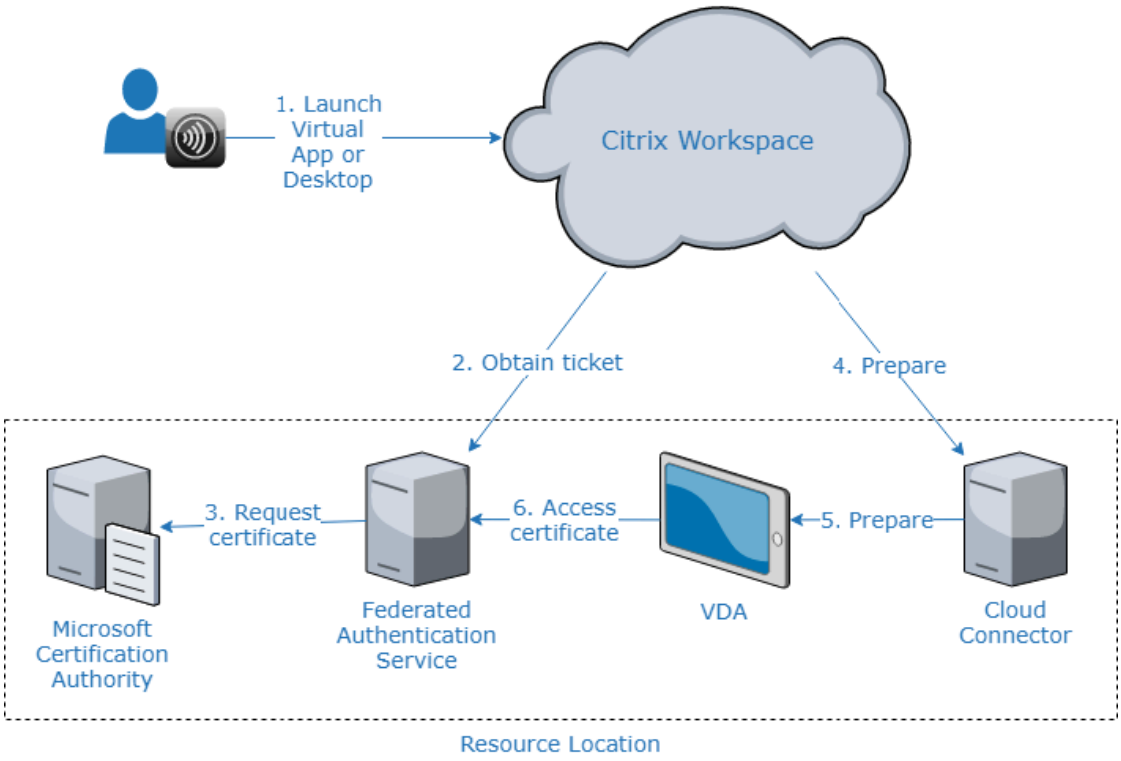
如果您的资源位置包含不同的基础架构（例如，不同的资源位置包含不同的 AD 林），请将 FAS 服务器部署到 VDA 所在的资源位置。SSO 仅在连接了一个或多个 FAS 服务器的资源位置处于活动状态。

FAS 服务器与多个资源位置相连

如果您的资源位置之间有网络连接，并且它们包含相似的基础架构，则可以将 FAS 服务器与多个资源位置连接。SSO 适用于连接到这些资源位置中的应用程序和桌面的 Workspace 订阅者。在这种情况下，无需将单独的 FAS 服务器连接到每个资源位置。

订阅者启动虚拟应用程序或桌面时，Citrix Cloud 会选择与正在启动的应用程序或桌面位于同一资源位置的 FAS 服务器。Citrix Cloud 联系选定的 FAS 服务器以获取票证，该票证授予对 FAS 服务器上存储的用户证书的访问权限。要对订阅者进行身份验证，VDA 将连接到 FAS 服务器并出示票证。

您可以对本地和 Citrix Cloud 使用相同的 FAS 服务器，并配置正确的规则。



多个资源位置的故障切换优先级

使用具有多个资源位置的 FAS 服务器时，位于一个资源位置的 FAS 服务器可以提供到其他资源位置的 FAS 服务器的故障转移。将 FAS 服务器添加到其他资源位置时，将每台服务器指定为主服务器或辅助服务器。订阅者启动虚拟应用程序或桌面时，Citrix Cloud 将按以下方式使用此名称来选择 FAS 服务器：

- 首先考虑在给定资源位置中被指定为主服务器的 FAS 服务器。
- 如果没有主服务器可用，则考虑指定为辅助服务器的 FAS 服务器。
- 如果没有辅助服务器可用，则启动会继续，但不会进行单点登录。

视频概览

有关 Citrix Workspace 的联合身份验证服务的概述，请观看以下技术洞察视频：

要求

连接要求

使用 FAS 管理控制台将 FAS 服务器连接到 Citrix Cloud。您可以使用此控制台配置本地或远程 FAS 服务器。要使用 FAS 为工作区启用 SSO，FAS 管理控制台和 FAS 服务分别使用控制台用户的帐户和网络服务帐户访问以下地址。

- FAS 管理控制台，使用控制台用户的帐户：
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - 第三方身份提供程序所需的地址（如果您的环境中使用了第三方身份提供程序）
- FAS 服务，使用“网络服务”帐户：
  - `*.citrixworkspacesapi.net`
  - `https://*.citrixnetworkapi.net/`

如果您的环境包含代理服务器，请使用 FAS 管理控制台的地址配置用户代理。此外，请确保将网络服务帐户的地址配置为适合您的环境。

FAS 系统要求

本节中的要求适用于计划与 Citrix Cloud 连接的所有 FAS 服务器。

FAS 产品文档的 系统要求部分描述了 FAS 服务器的完整系统要求 。

本地 Citrix Virtual Apps and Desktops 环境中的 FAS 服务器必须安装联合身份验证服务 2003（版本 10.1）或更高版本。

如果现有 FAS 服务器的版本早于版本 10，则可以在创建此连接之前从 Citrix 下载最新的 FAS 软件并就地升级服务器。创建连接时，请选择 FAS 服务器的资源位置。SSO 仅在存在 FAS 服务器的资源位置对订阅者有效。

有关升级现有 FAS 服务器的更多信息，请参阅 FAS 产品文档中的 安装和配置 。同一 FAS 服务器可用于 Workspace 和本地部署。

Citrix Workspace

必须在 Workspace 中配置并启用 Citrix DaaS。默认情况下，订阅服务后，将在“Workspace 配置”中启用 DaaS。但是，该服务要求您部署 Citrix Cloud Connector 才能允许 Citrix Cloud 与您的本地环境通信。

Cloud Connector

Citrix Cloud 连接器支持您的资源位置（VDA 所在的位置）与 Citrix Cloud 之间的通信。部署至少两个 Cloud Connector 以确保高可用性。安装 Cloud Connector 软件的服务器必须满足以下要求：

- Cloud Connector 技术详情中所述的系统要求
- 未安装其他 Citrix 组件，服务器不是 Active Directory 域控制器，也不是对您的资源位置基础架构至关重要的计算机。
- 已加入您的 VDA 所在的域。

有关部署 Cloud Connector 的更多信息，请参阅以下文章：

- Cloud Connector 代理和防火墙配置
- Cloud Connector 安装

设置概述

1. 如果要部署新的 FAS 服务器，请查看 要求 并按照本文中 安装和配置 FAS 中的说明进行操作。
2. 按照本文将 FAS 服务器连接到 Citrix Cloud 中所述，将 FAS 服务器连接到 Citrix Cloud。完成此任务后，您的 FAS 服务器连接到单个资源位置。
3. 如果您计划将 FAS 服务器连接到多个资源位置，请按照本文中 将 FAS 服务器添加到多个资源位置 中的说明进行操作。

安装和配置 **FAS**

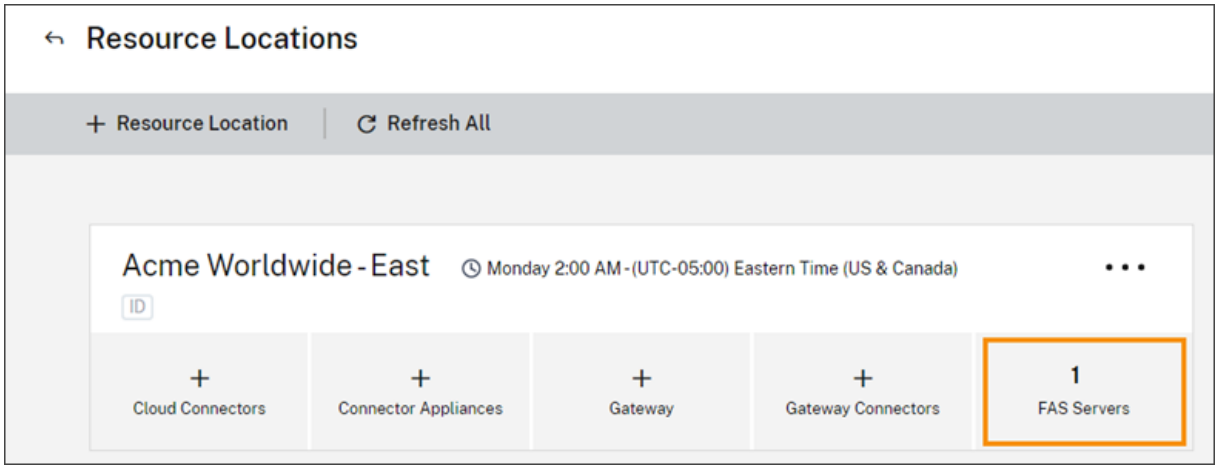
按照 FAS 产品文档中描述的 FAS安装和配置过程进行操作。StoreFront 和 Delivery Controller 配置步骤不是必需的。

> 提示：
>
> 您也可以从 Citrix Cloud 控制台下载联合身份验证服务安装程序：
>
> 1. 从 Citrix Cloud 菜单中，选择资源位置。
> 2. 选择 **FAS** 服务器 磁贴，然后单击 下载。

将 **FAS** 服务器连接到 **Citrix Cloud**

按照 FAS 产品文档中的 安装和配置 中所述，使用 FAS 管理控制台将 FAS 服务器连接到 Citrix Cloud。

完成“连接到 **Citrix Cloud**”配置步骤后，Citrix Cloud 会注册 FAS 服务器并将其显示在您的 Citrix Cloud 帐户的“资源位置”页面上。



如果您的浏览器中已经加载了“资源位置”页面，请刷新该页面以显示已注册的 FAS 服务器。

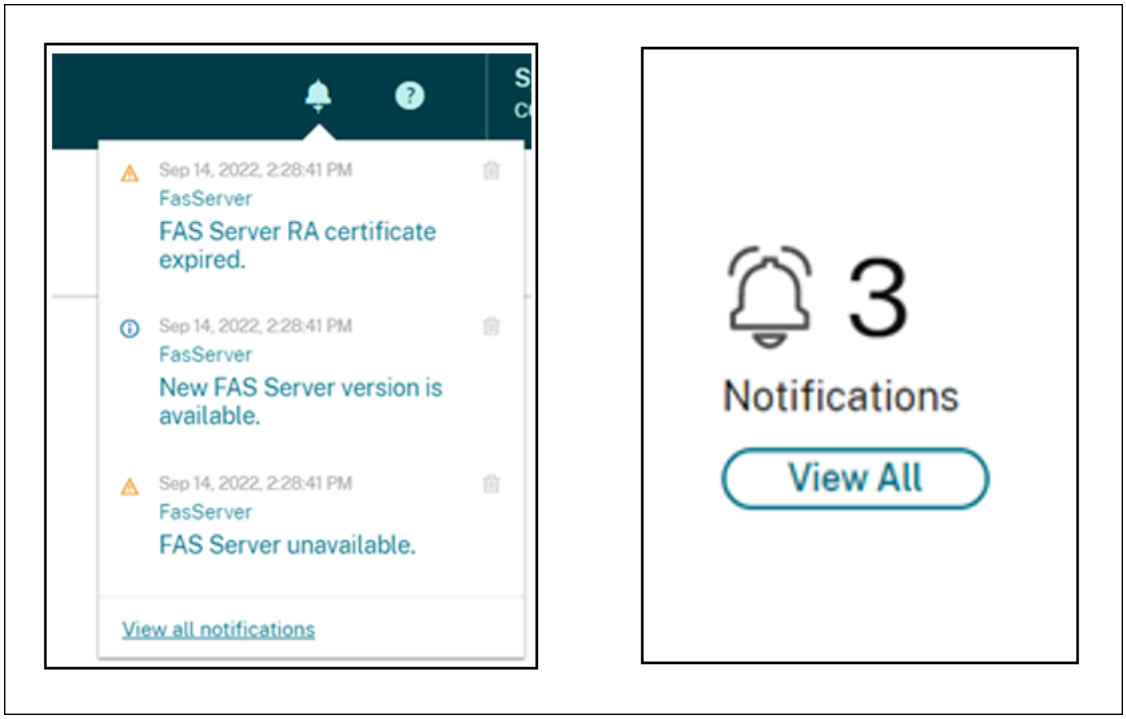
支持云端通知

FAS 现在支持云通知。使用适用于 FAS 服务器的新 Cloud 通知，您将在以下情况下收到通知：

- FAS 服务器已关闭或不可用。
- FAS 服务器的注册管理机构 (RA) 证书已过期或即将过期。
- FAS 的新版本可供下载。

引发通知

在 Citrix Cloud 管理控制台中对新通知进行定期检查并提出。通知显示在 Citrix Cloud 管理控制台右上角的钟形图标下方。选择通知图标上的“查看全部”以查看所有通知。有关更多信息，请参阅 通知。

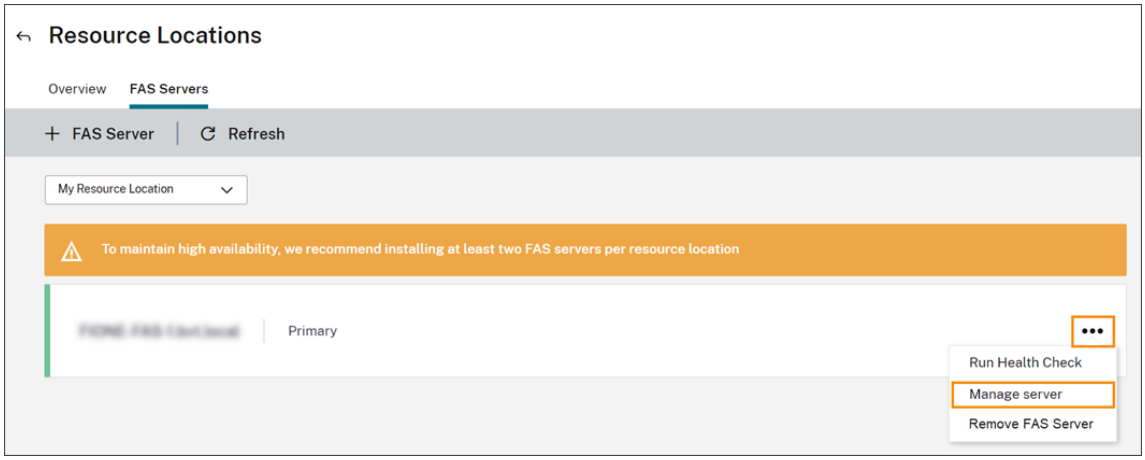


> 注意：
>
> 发出通知后，只有在问题未得到解决的情况下，才会定期再次发出通知。

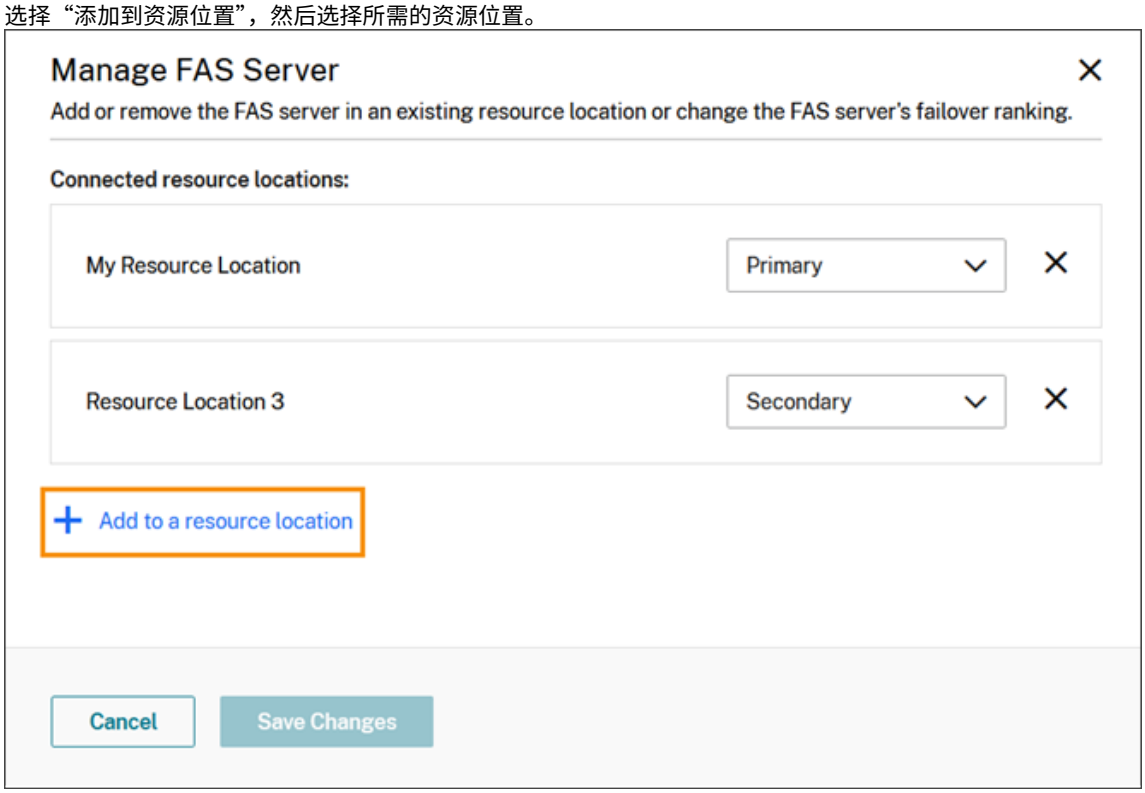
所有通知都包含受影响的 FAS 服务器的 FQDN。RA 证书到期通知仅对版本为 10.10.0.14 及更高版本的 FAS 服务器显示。

将 **FAS** 服务器添加到多个资源位置

1. 从 Citrix Cloud 菜单中，选择 资源位置，然后选择 **FAS** 服务器 选项卡。
2. 找到要管理的 FAS 服务器，单击条目右侧的省略号 (…)，然后选择 管理服务器。



3. 选择“添加到资源位置”，然后选择所需的资源位置。



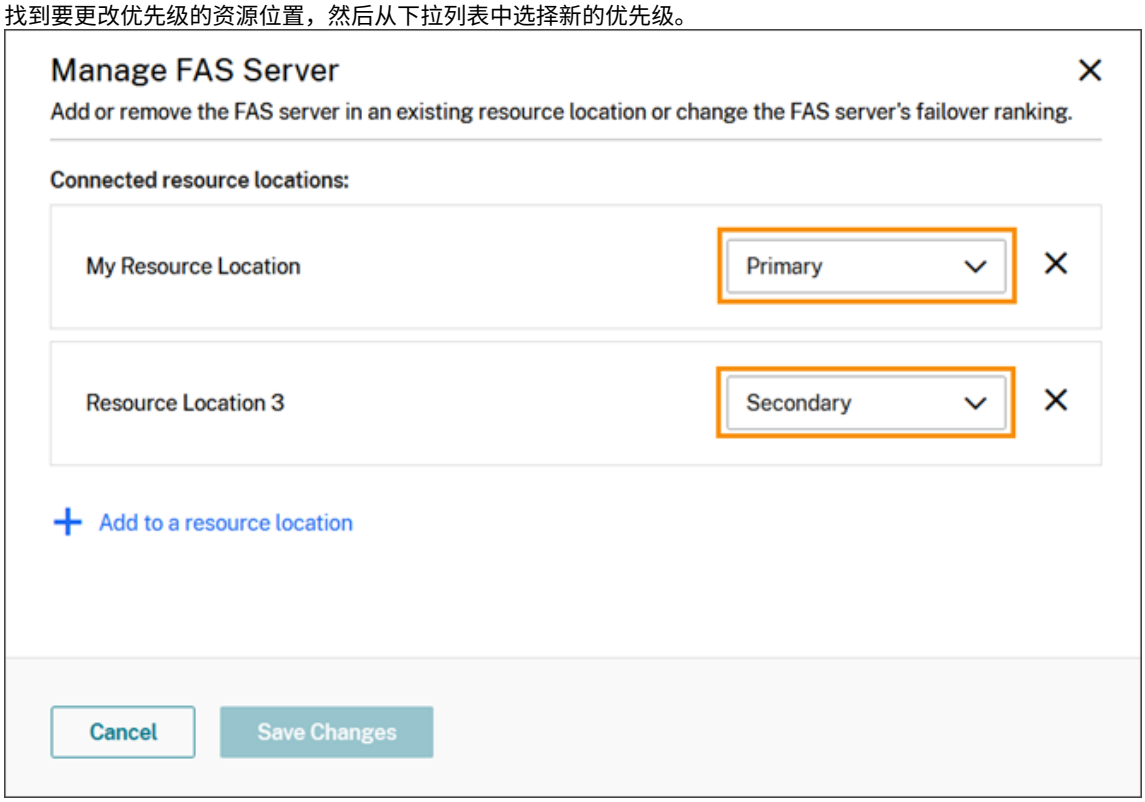
4. 选择“主”或“辅助”作为 FAS 服务器在每个选定资源位置的故障转移优先级。
5. 选择 保存更改。

要查看添加的 FAS 服务器，请从 **Citrix Cloud** 菜单中选择“资源位置”，然后选择“**FAS** 服务器”选项卡。此时将显示所有已连接资源位置的所有 FAS 服务器的列表。要显示特定资源位置的 FAS 服务器，请从下拉列表中选择资源位置。

更改 **FAS** 服务器的故障切换优先级

1. 在“资源位置”页面中，选择要管理的资源位置的 **FAS** 服务器磁贴。
2. 选择 **FAS** 服务器 选项卡。

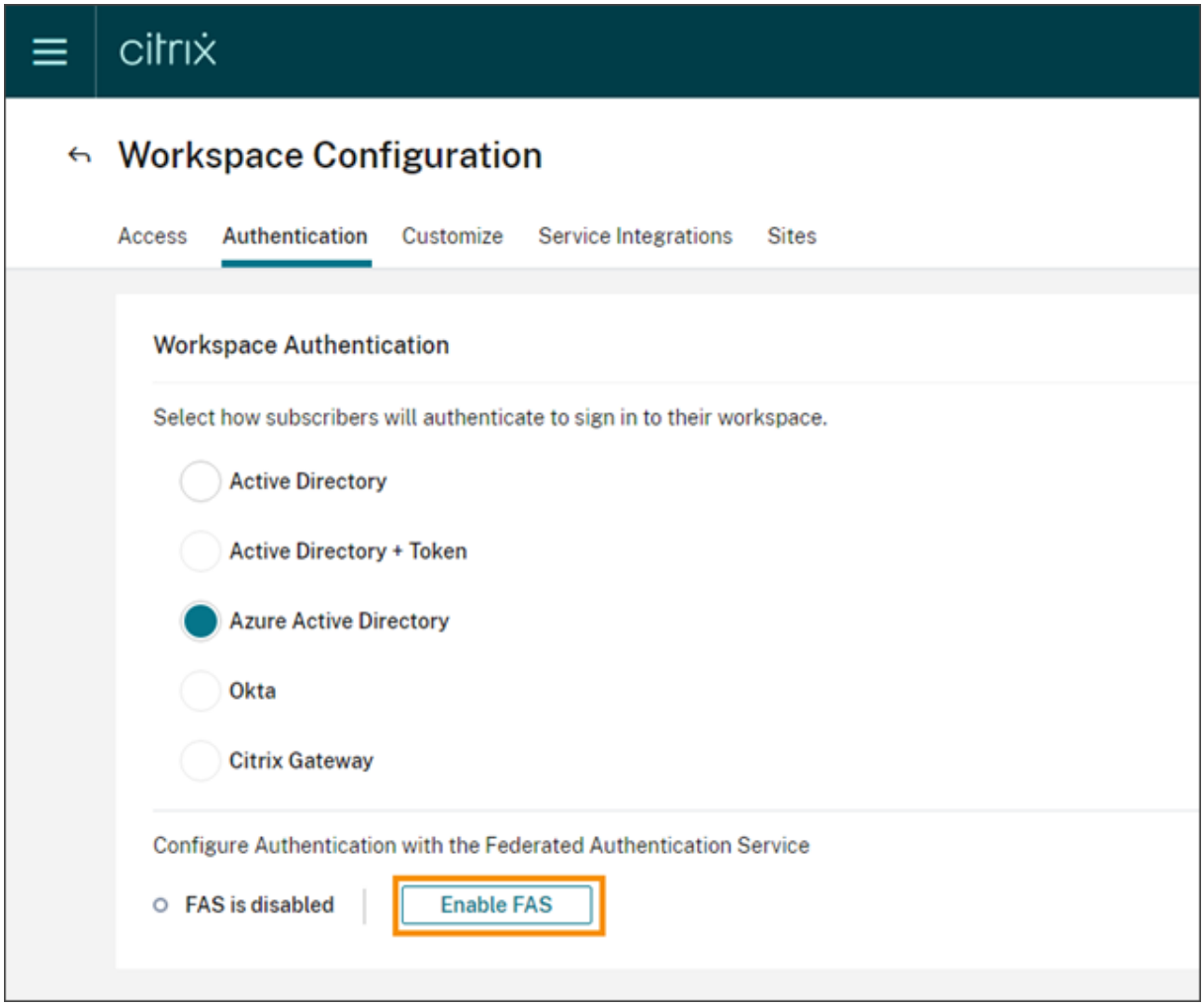
3. 找到要管理的 FAS 服务器，单击条目右侧的省略号，然后选择 管理服务器。
4. 找到要更改优先级的资源位置，然后从下拉列表中选择新的优先级。



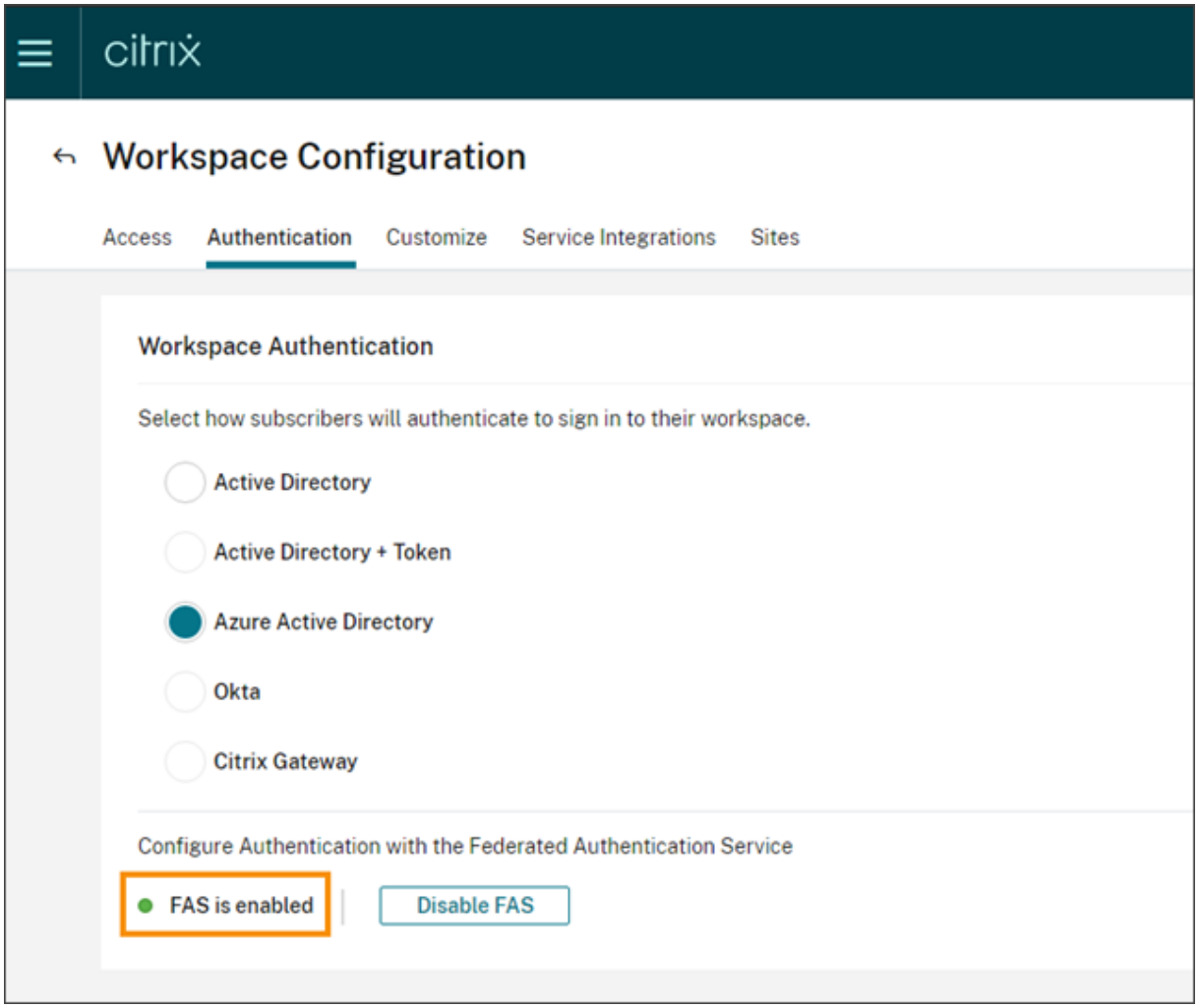
5. 选择 保存更改。

为工作区启用联合身份验证

1. 在 Citrix Cloud 菜单中，选择 **Workspace Configuration**（Workspace 配置），然后选择 **Authentication**（身份验证）。
2. 单击 **Enable FAS**（启用 FAS）。此更改最多可能需要五分钟才能应用到订阅者会话。



之后，联合身份验证服务将对从 Citrix Workspace 启动的所有虚拟应用程序和桌面启用。



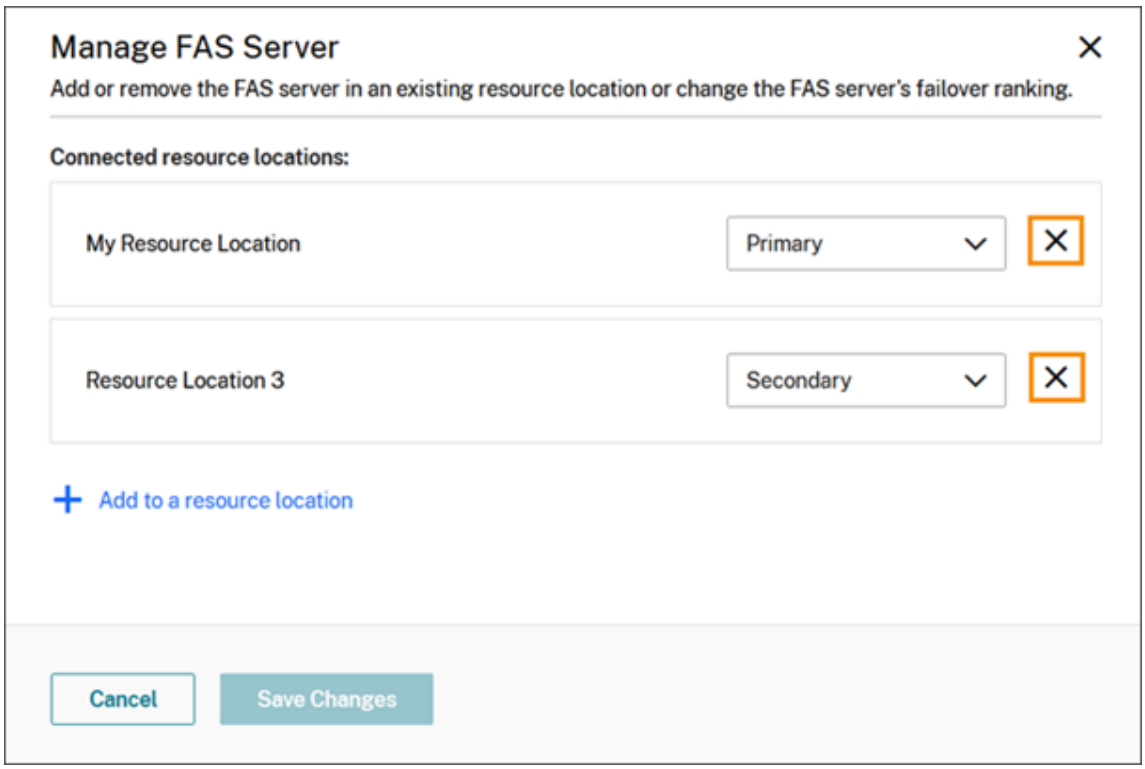
当订阅者登录其工作区并在与 FAS 服务器相同的资源位置启动虚拟应用程序或桌面时，应用程序或桌面将在不提示输入凭据的情况下启动。

> 注意：
>
> 如果资源位置中的所有 FAS 服务器都已关闭或处于维护模式，应用程序启动将成功，但单点登录未激活。系统会提示订阅者输入其 AD 凭据以访问每个应用程序或桌面。

移除 **FAS** 服务器

要从单个资源位置删除 FAS 服务器，请执行以下操作：

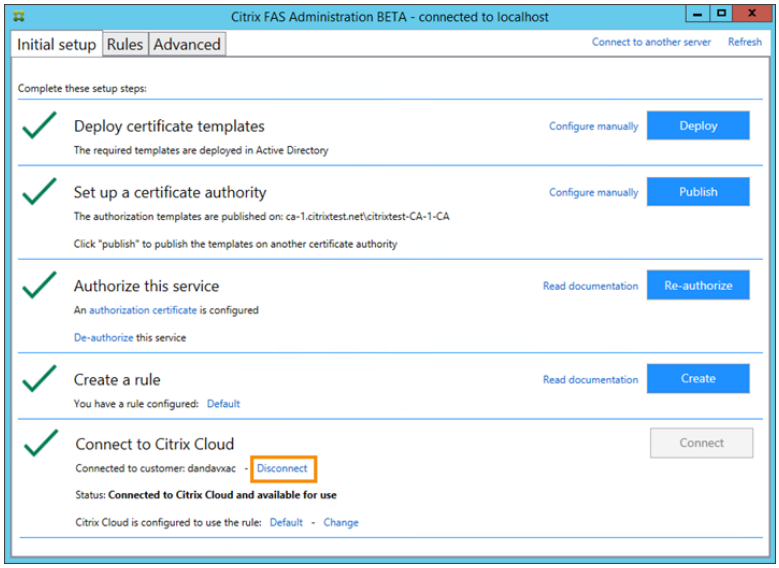
1. 在“资源位置”页面中，选择要管理的资源位置的 **FAS** 服务器磁贴。
2. 选择 **FAS** 服务器 选项卡。
3. 找到要管理的 FAS 服务器，单击条目右侧的省略号，然后选择 管理服务器。
4. 找到要移除的资源位置，然后单击 **X** 图标。



要从所有连接的资源位置删除 FAS 服务器，请执行以下操作：

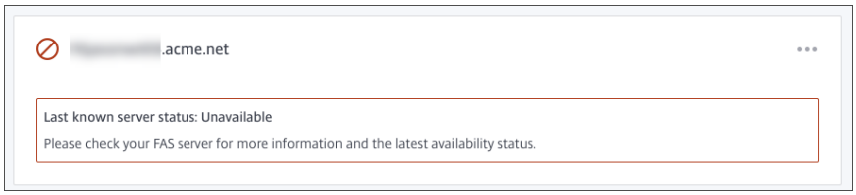
1. 从 Citrix Cloud 菜单中，选择资源位置。
2. 找到要管理的资源位置，然后选择 **FAS** 服务器 磁贴。
3. 找到要删除的 FAS 服务器，单击条目右侧的省略号，然后选择删除 **FAS** 服务器。

4. 在 FAS 管理控制台（在您的本地 FAS 服务器上）的 连接到 **Citrix Cloud** 中，选择 断开连接。或者，您可以卸载 FAS。

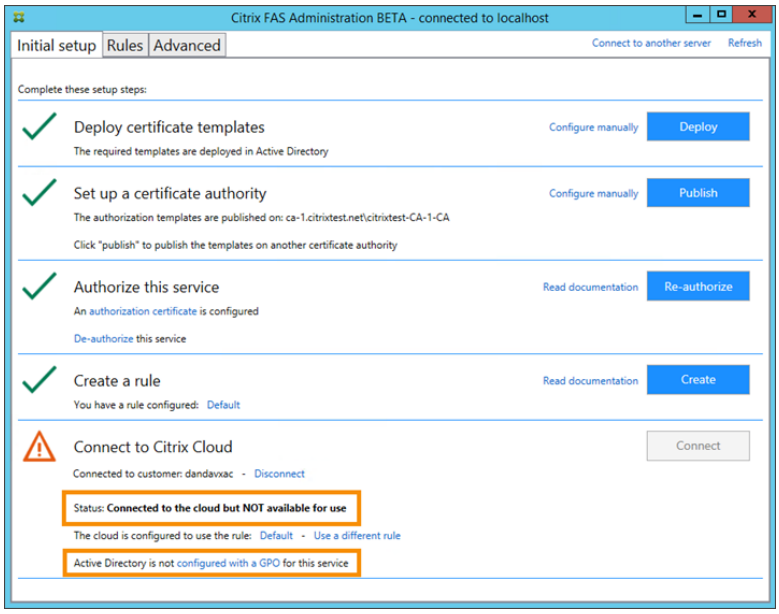


故障排除

如果 FAS 服务器不可用，则 FAS 服务器页面上会显示一条警告消息。



要诊断问题，请打开本地 FAS 服务器上的 FAS 管理控制台并检查状态。例如，FAS 服务器在 FAS 服务器 GPO 中不存在：



如果 FAS 管理控制台指示服务器运行正常，但仍存在 VDA 登录问题，请参阅 FAS 故障排除指南。

更多信息

配置到 Workspace 应用程序的单点登录