Citrix Workspace

Copyright © 1997–2025. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix Workspace 概述 **3**

新增功能 **5**

Workspace 平台的新增功能 **6**

工作区用户界面 **(UI)** 的新增内容 **14**

Global App Configuration Service 中的新增功能 **44**

开始使用 **Citrix Workspace** **54**

系统要求 **58**

使用 **Citrix Workspace** 交付 **DaaS**、**Virtual Apps and Desktops** **60**

用户访问 **61**

活动管理器 **64**

Citrix Workspace Web 扩展 **73**

安装 **Citrix Workspace Web** 扩展 **76**

工作区离线模式提示 **78**

配置对工作区的访问权限 **79**

配置自定义域 **82**

配置工作区 **URL** **98**

配置身份验证 **107**

自定义你的工作空间体验 **116**

自定义工作区的外观 **117**

自定义工作区互动 **123**

自定义安全和隐私政策 **130**

自定义商店访问 **142**

将服务集成到工作区 **151**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

在 **Citrix Workspace** 中优化 **DaaS** **153**

在工作区中聚合虚拟应用程序和桌面 **154**

直接工作负载连接 **163**

服务连续性 **166**

使用 **Citrix** 联合身份验证服务为工作区启用单点登录 **185**

使用交付组访问策略进行资源过滤 **198**

使用 **Global App Configuration Service** 配置 **Citrix Workspace** 应用程序 **202**

配置云应用商店的设置 **209**

为本地应用商店配置设置 **216**

测试频道配置 **225**

管理 **Citrix Workspace** 应用程序版本 **228**

使用全局应用程序配置服务管理插件 **236**

使用配置文件管理用户组的设置 **245**

跨应用商店、渠道和配置文件克隆设置 **250**

管理混合启动设置（技术预览版） **255**

Citrix Workspace 安全概述 **258**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Workspace 概述

November 7, 2024

Citrix Workspace 是一种服务，可通过 Web 浏览器或 Citrix Workspace 应用程序安全访问您的虚拟应用程序、桌面、Web 和 SaaS 应用程序。

Citrix Workspace 是由 Citrix 管理的云服务。如果您希望在自己的环境中部署此功能，请参阅 StoreFront。

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 的最终用户被称为订阅者，因为您可以让员工“订阅”您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，订阅者将自动向为 Citrix Workspace 购买的每个云托管服务进行身份验证。它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 配置身份验证。

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. 验证您是否已设置在 **Citrix Cloud** 控制台中实施 Citrix Workspace，在其中您可以：
    - 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 将您在 Citrix Cloud 控制台中配置的服务集成到工作区中。
- 自定义工作区的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)。

> 注意：
>
> 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。每个步骤都会指导您完成 Citrix Cloud 控制台中的任务，例如配置身份提供商。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。

最终用户访问权限

最终用户使用 Citrix Workspace 应用程序或其 Web 浏览器从其设备连接到工作区。有关更多信息，请参阅 用户访问

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

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两个因素。第一个因素是您是否要完全迁移到云或采用混合解决方案。第二个因素是您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 为集成到 Workspace 的 Web 和 SaaS 应用程序提供单点登录 (SSO)。该服务还允许您管理访问权限和控制策略。它有助于根据订阅者的凭证批准对企业托管的 Web 应用程序的适当级别的访问。

有关使用 **Citrix Secure Private Access** 服务的更多信息，请访问 技术简介：Secure Private Access。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Gateway 服务

Citrix Gateway 服务根据先进的策略基础设施提供与您的虚拟应用程序和桌面、Web 和 SaaS 应用程序的连接。

按照步骤设置 Citrix Gateway 服务，然后 配置 Workspace 以使用它来提供对您的资源的远程访问。

Citrix Remote Browser Isolation 服务

将 **Citrix** 远程浏览器隔离服务 集成到您的工作区，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。

为了让订阅者访问远程隔离浏览器，请设置 远程浏览器隔离。之后，测试并与您的订阅者分享工作区 URL。

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。产品包括 **Citrix Analytics for Security**、**Citrix Analytics for Performance** 和 **Citrix Analytics (Usage)**。要了解有关这些服务的更多信息，请访问 Citrix Analytics。

新增功能

March 15, 2025

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

不同平台上的 **Citrix Workspace** 应用程序

使用以下链接了解有关您最喜欢的平台的 **Citrix Workspace** 应用程序 中的新功能和增强功能的更多信息。

- 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

May 13, 2025

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。

2025 年 **5** 月

管理员现在可以根据设备的网络连接类型配置不同的不活动超时。有关更多信息，请参阅 工作区会话设置。

2024 年 **11** 月

管理员现在可以根据工作区 URL 配置不同的自定义公告。有关更多信息，请参阅 发送自定义公告。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

July 2024

为您的应用商店 **URL** 配置应用商店名称

管理员现在可以在将商店添加到 Citrix Workspace 应用程序时添加自定义商店名称。商店名称使最终用户更容易识别和区分商店。以前，在多个工作区 URL 设置（cloud.com 的子域）中，所有商店都被称为“Store”，并带有自动生成的数字后缀。例如，商店 1、商店 2、商店 3 等等。这种安排使得管理员和最终用户难以将商店名称与商店 URL 关联起来。

通过此功能，管理员可以为商店起一个最终用户可以识别的简短名称。此外，管理员可以启用或禁用最终用户在其 Citrix Workspace 应用程序上修改商店名称的功能。

有关详细信息，请参阅为您的应用商店 URL 配置应用商店名称。

2024 年 2 月

创建多个 **Workspace URL -** 正式发布 **(GA)**

多工作区 URL 功能现已面向所有用户开放。您现在可以创建多个工作区 URL（cloud.com 的子域）并使用这些 URL 作为策略输入。例如，您可以为组织内的不同子公司或部门配置不同的 URL。每个 URL 可以具有不同的品牌、身份验证方法或桌面和应用程序。

> 注意：
>
> 您最多可以为您的工作区创建 10 个 URL。

每个商店都可以通过唯一的 URL 访问，但在以下方面有所不同：

- 用户界面品牌化（登录后）
- 应用程序和桌面
- 身份验证配置（例如不同的身份提供者）

有关更多信息，请参阅 配置多个工作区 URL。

2023 年 12 月

创建多个工作区 **URL**（技术预览版）

您现在可以创建多个工作区 URL（cloud.com 的子域）并使用这些 URL 作为策略输入。例如，您可以为组织内的不同子公司或部门配置不同的 URL。每个 URL 可以具有不同的品牌、身份验证方法或桌面和应用程序。

> 注意：
>
> 您最多可以为您的工作区创建 10 个 URL。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

每个商店都可以通过唯一的 URL 访问，但在以下方面有所不同：

- 用户界面品牌化（登录后）
- 应用程序和桌面
- 身份验证配置（例如不同的身份提供者）

有关更多信息，请参阅 配置工作区 URL。

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

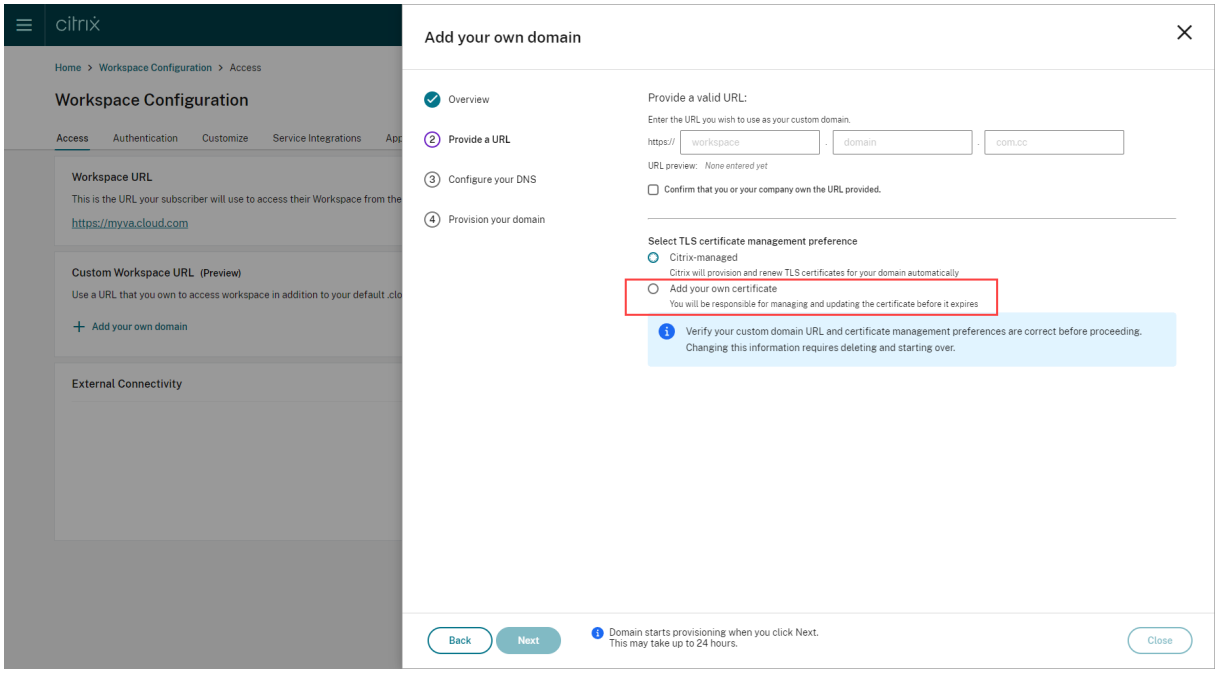
为自定义域添加您自己的 **TLS** 证书（预览版）

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。

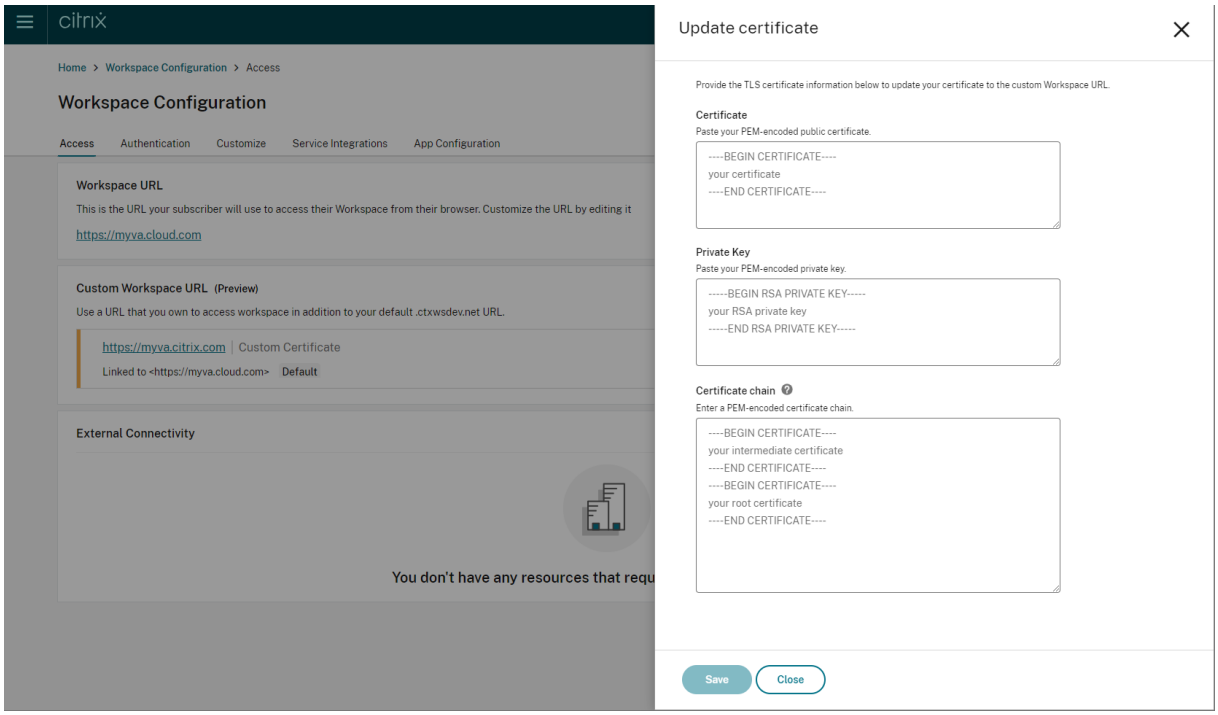
- 它应该采用 PEM 编码。
- 它应至少在接下来的 30 天内保持有效。
- 它应专门用于自定义 Workspace URL，不接受通配符证书。
- 证书的公用名称应与自定义域相匹配。
- 证书上的 SAN 应用于自定义域，不允许使用任何其他 SAN。
- 证书的有效期不应超过 10 年。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2023 年 5 月

配置自定义域（预览）。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全局应用程序配置服务配置适用于 iOS、Android、HTML5、Mac 和 Windows 平台的 Citrix Workspace 应用程序的设置。

2022 年 8 月

改进工作区启动体验。当用户通过网络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

支持与 **Safari** 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获得服务连续性。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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 **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。

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

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。

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。

November 2021

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

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。

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。

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。

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。

服务连续性普遍可用性：服务连续性允许用户即使在 Citrix Cloud 组件或公共云和私有云出现中断期间也能连接到他们的虚拟应用程序和桌面。有关详细信息，请参阅服务连续性。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 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。

2020 年 12 月

服务连续性技术预览：服务连续性允许用户即使在 Citrix Cloud 组件或公共云和私有云出现中断期间也能连接到他们的 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。FedRAMP 是一个旨在促进美国政府机构使用的云服务安全标准的计划。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

** 支持自定义 Citrix Workspace 应用程序设置。本演练将指导您完成 Citrix Cloud 控制台，以便您可以配置身份提供商、添加管理员以及启用工作区身份验证和服务。有关任务概述和快速访问所需说明，请参阅 开始使用 Citrix Workspace。</p>

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

June 10, 2025

Citrix 的目标是及时向客户提供可用的新功能和产品更新。新版本提供了更多价值，因此没有理由延迟更新。

对于您（客户）来说，这个过程是透明的。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程度提高可用性。

本文档中提到的更新可能正在推出，并非所有客户都能同时访问。

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。

25.19

显示专用桌面的电源状态

工作区用户界面 (UI) 现在可以显示专用桌面的电源状态。电源状态指示专用桌面是处于开机、关机还是处于挂起状态（休眠）。这一增强功能使用户能够快速识别其桌面的状态，从而使他们能够做出明智的决策并更有效地管理其资源。

> 笔记：
>
> - 此功能默认启用。
> - 此功能与 Citrix Workspace 应用程序的早期版本向后兼容。

有关更多信息，请参阅 显示专用桌面的电源状态。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

25.11

配置登录后显示的自定义对话框

您可以配置用户登录后显示的自定义对话框。它显示在所有客户端上，包括网络、桌面和移动设备。您可以使用它来显示公司使用政策或即将到来的维护窗口等信息。用户必须接受该对话框才能继续使用其资源。

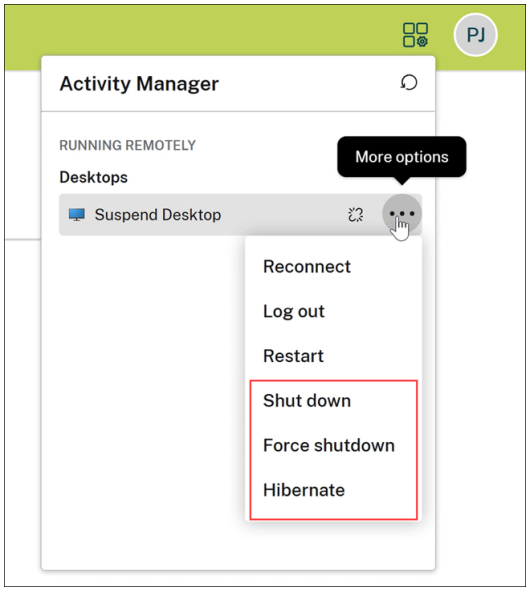
管理员可以决定每个设备显示对话框的频率，即仅显示一次、每天显示一次、每 7 天显示一次或每 30 天显示一次。

有关更多信息，请参阅 配置登录后显示的自定义对话框。

25.10

增强活动管理器体验并引入电源管理控制

活动管理器功能现在默认启用，允许用户断开连接、注销和重新启动他们的虚拟会话。此外，管理员可以使用 Citrix Cloud 管理电源管理控制，例如关机、强制关机和休眠虚拟会话。



有关更多信息，请参阅 电源管理控制。

25.09

颜色自定义适用于工作区 **UI** 元素

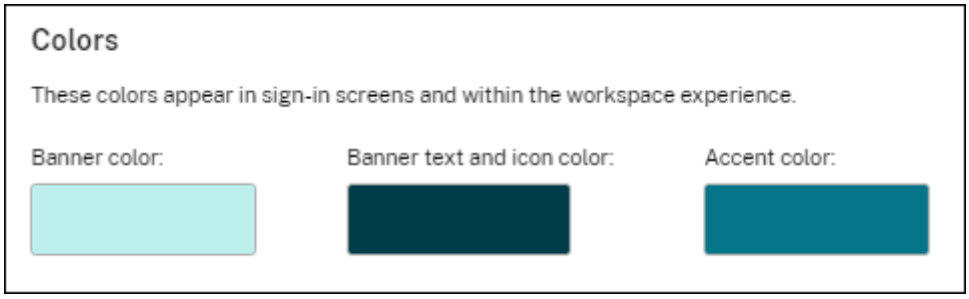
此功能在以下领域进行了增强：

- 完整的 **UI** 颜色自定义：一致的配色方案现在适用于工作区 UI 元素。

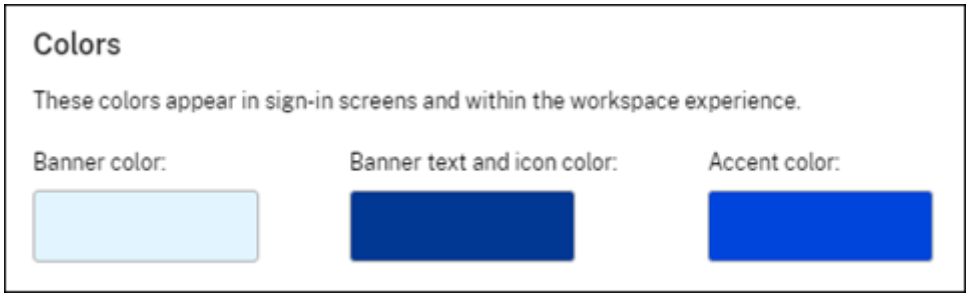
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 统一蓝色主题：已实施新的默认蓝色主题，以与所有 Citrix 应用程序中的通用最终用户主题保持一致。管理员仍然可以使用 Citrix Cloud 根据自己的喜好自定义颜色。

旧的默认颜色：



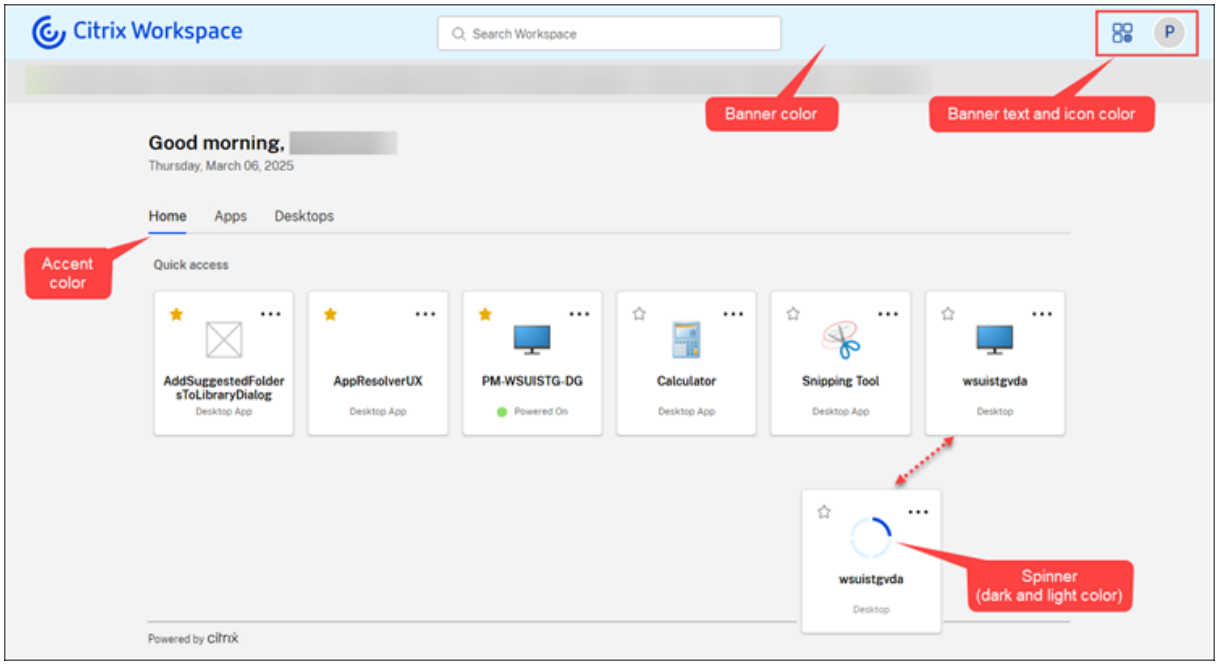
新的默认颜色：

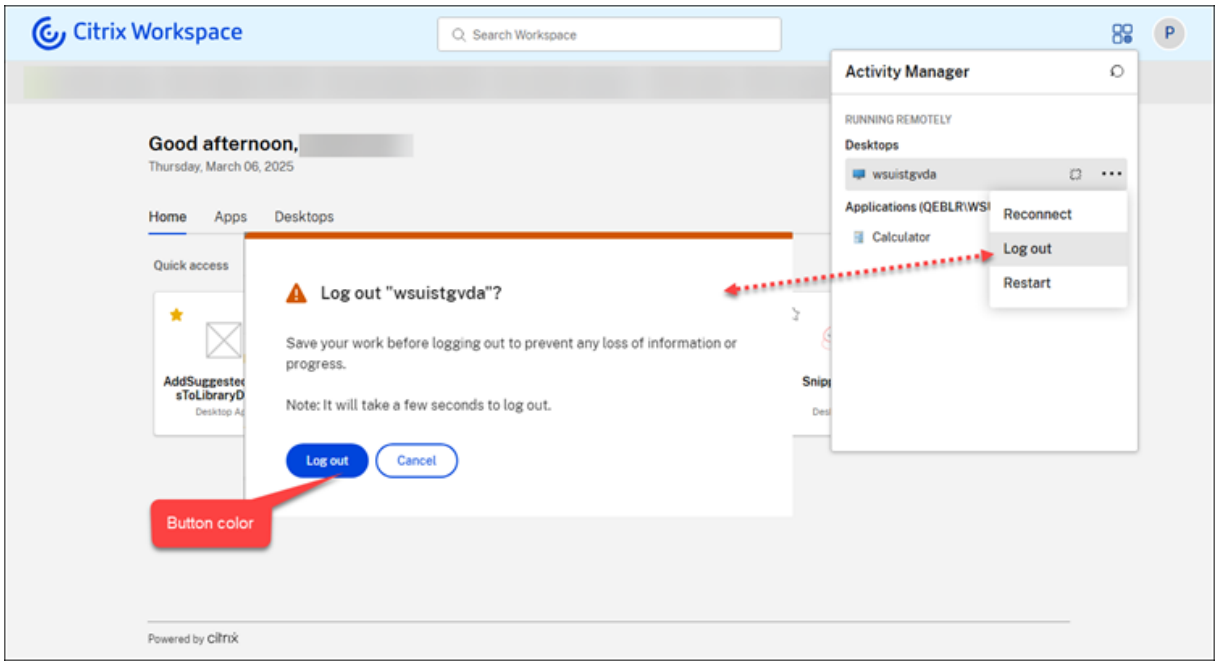


颜色变化会影响 UI 的各个元素，包括：

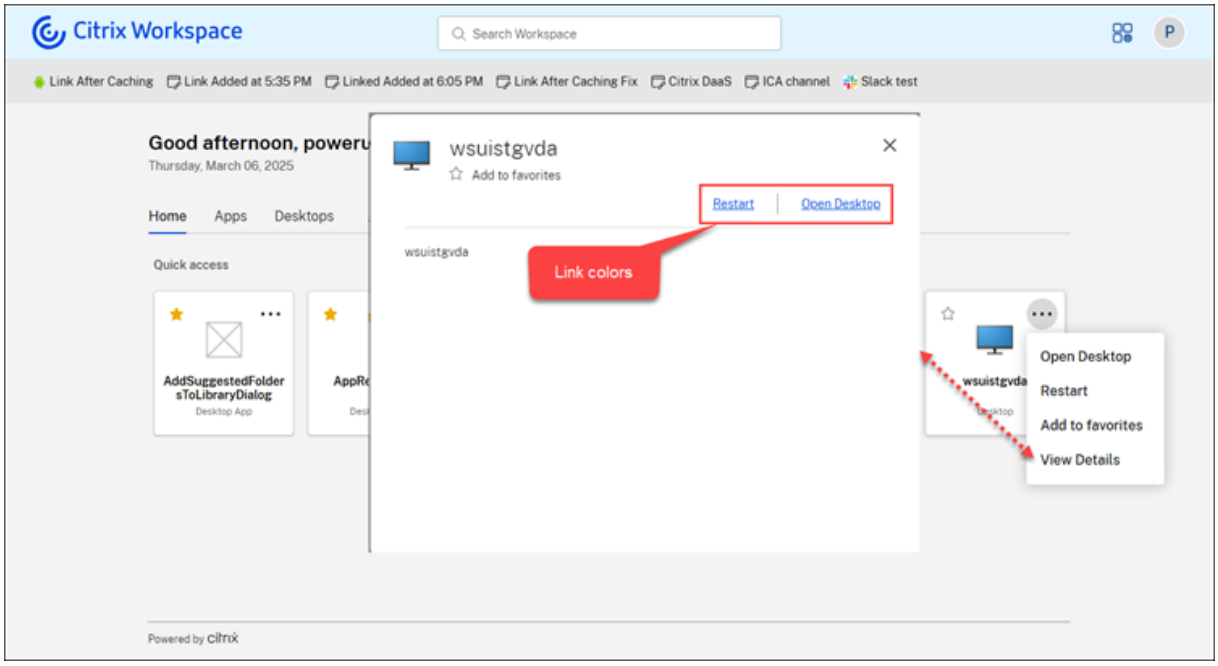
- 横幅文字和图标颜色
- 重音线，即某些元素下方的一条线
- 旋转器（旋转器内的深色和浅色）
- 按钮
- 链接

© 1997–2025 Citrix Systems, Inc. All rights reserved.





© 1997–2025 Citrix Systems, Inc. All rights reserved.



有关自定义主题的更多信息，请参阅 自定义默认主题。

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。

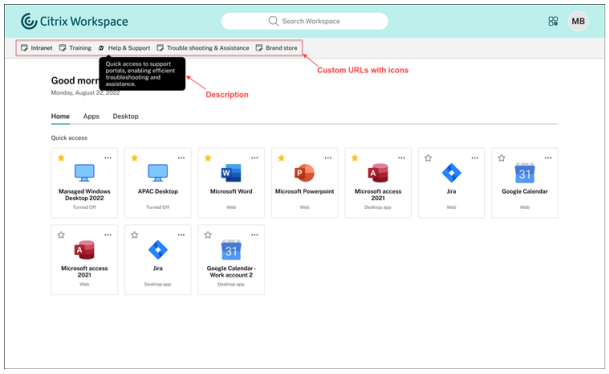
早期版本

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。

25.04

支持固定链接　固定链接是指客户定义的超链接，可以快速访问特定网站。此功能作为快捷方式，帮助用户从 Workspace UI 直接高效地导航到网站。可以向用户提供重要的链接，例如支持网站或公司门户，而无需他们搜索这些链接。它使得导航更加轻松、快捷。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Citrix Workspace Web 客户端和本机 Citrix Workspace 应用程序均支持此功能。

欲了解更多信息，请参阅 固定链接。

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　没有已知问题。

24.49

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.47

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.46

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.45

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.43

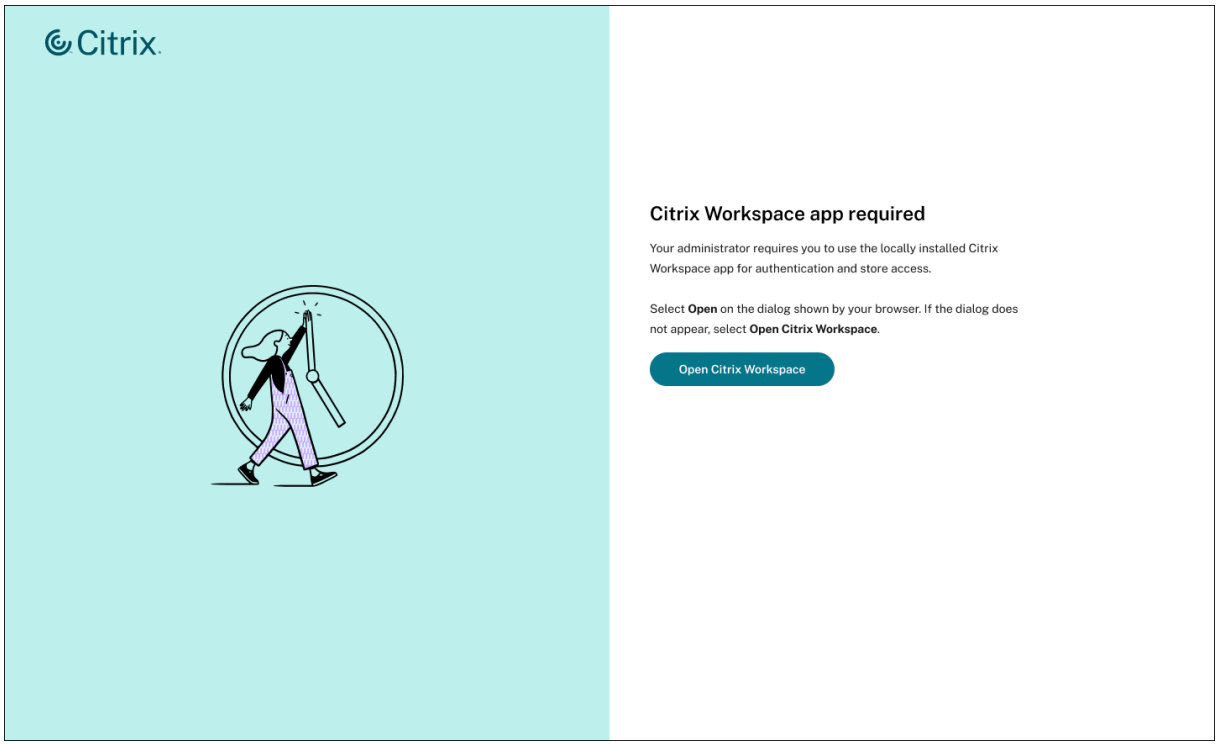
此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.41

要求用户仅通过本机 **Citrix Workspace** 应用程序进行身份验证并打开应用程序和桌面（预览版） 管理员可以强制使用本机 Citrix Workspace 应用程序，从而无需用户通过浏览器访问 Citrix Workspace Web 客户端。此功能专为希望充分利用原生应用优势的客户而设计。原生应用程序具有内置应用程序保护服务、无浏览器版本兼容性问题、增强的安全性以及用于监控和故障排除的遥测等优势。

当管理员启用此功能时，最终用户在浏览器中输入商店 URL 尝试访问 Web 客户端时会看到以下网页。



一旦用户单击 打开 **Citrix Workspace**，商店就会自动添加到本机应用程序中，以便更轻松地从 Web 客户端过渡到本机应用程序。此功能适用于适用于 Windows、Mac、Android 和 iOS 的 Citrix Workspace 应用程序。有关自动商店添加兼容的本机应用程序版本的详细信息，请参阅 Citrix Workspace 应用程序兼容版本。

> 注意：
>
> 该功能适用于所有支持浏览器的云商店。

有关更多信息，请参阅 自定义商店访问。

通过活动管理器重新连接并传输应用程序和桌面 活动管理器引入了重新连接和传输资源功能。重新连接功能让最终用户可以轻松重新连接到 Citrix Workspace 应用程序中断开连接的应用程序和桌面。传输功能允许最终用户将活动会话从其他设备转移到当前设备。

有关更多信息，请参阅 重新连接到已断开的应用程序和桌面 和 传输您的应用程序和桌面。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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　此版本中没有已知问题。

24.40

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.39

工作区离线模式提示：增强的设计、行为和加载时间　工作区离线模式功能在设计、行为和加载时间方面都进行了优化。新的离线模式提示不太具侵入性，因为它不会中断正在进行的用户身份验证。当离线模式选项出现时，用户可以继续其身份验证过程。如果出现身份验证问题，他们可以继续登录或使用离线模式离线工作并访问可用的应用程序。此外，提示是可移动的，允许用户拖动它来查看其隐藏的内容。

此前，用户登录商店网址仅 30 秒就会出现离线模式提示，中断流程。但是，增强提示现在需要等待 60 秒才会出现，并且可以出现在任何网页上，包括登录屏幕和其他重定向页面。新的提示现在作为可选提示出现，允许用户不间断地完成正在进行的身份验证过程。

> 注意：
>
> 该功能默认启用，并且仅适用于云商店。

有关更多信息，请参阅 工作区离线模式提示

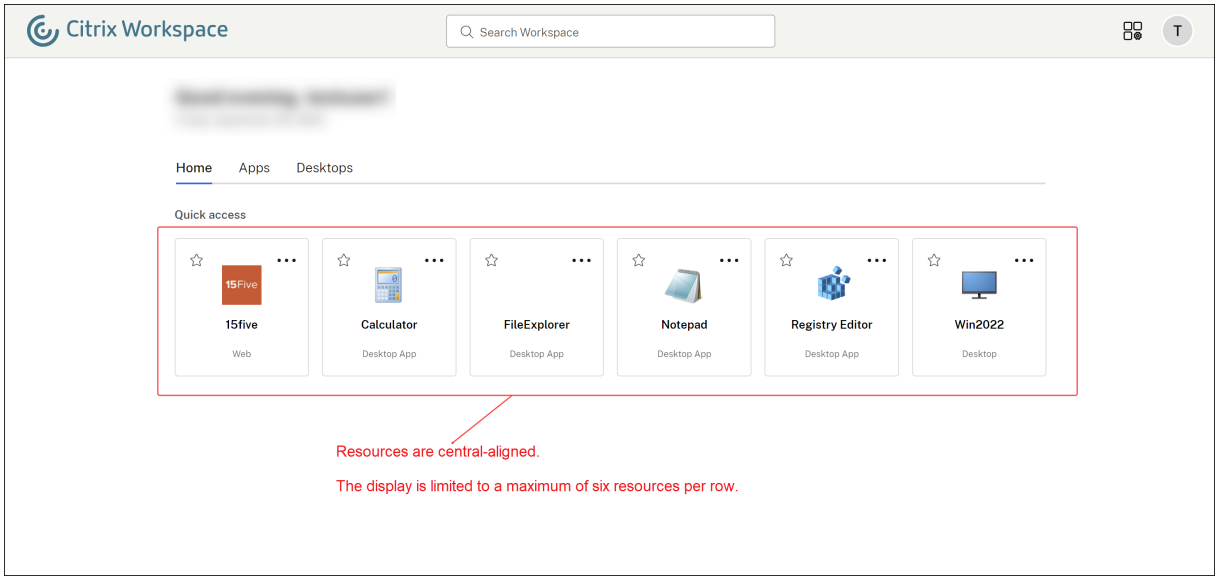
已修复的问题　此版本解决了改进整体性能和稳定性的区域。

已知问题　此版本中没有已知问题。

24.37

增强的用户界面集中式布局　工作区 UI 具有更好的资源对齐，与以前的资源横跨整个屏幕宽度的布局不同，增强的 UI 通过集中对齐资源并将显示限制为每行最多六个资源，提供了更具视觉吸引力的设计。增强的用户界面提供了更好的用户体验，从而提高了工作效率。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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　此版本中没有已知问题。

24.36

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.33

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.32

此版本解决了提高整体性能、稳定性和功能增强的领域。

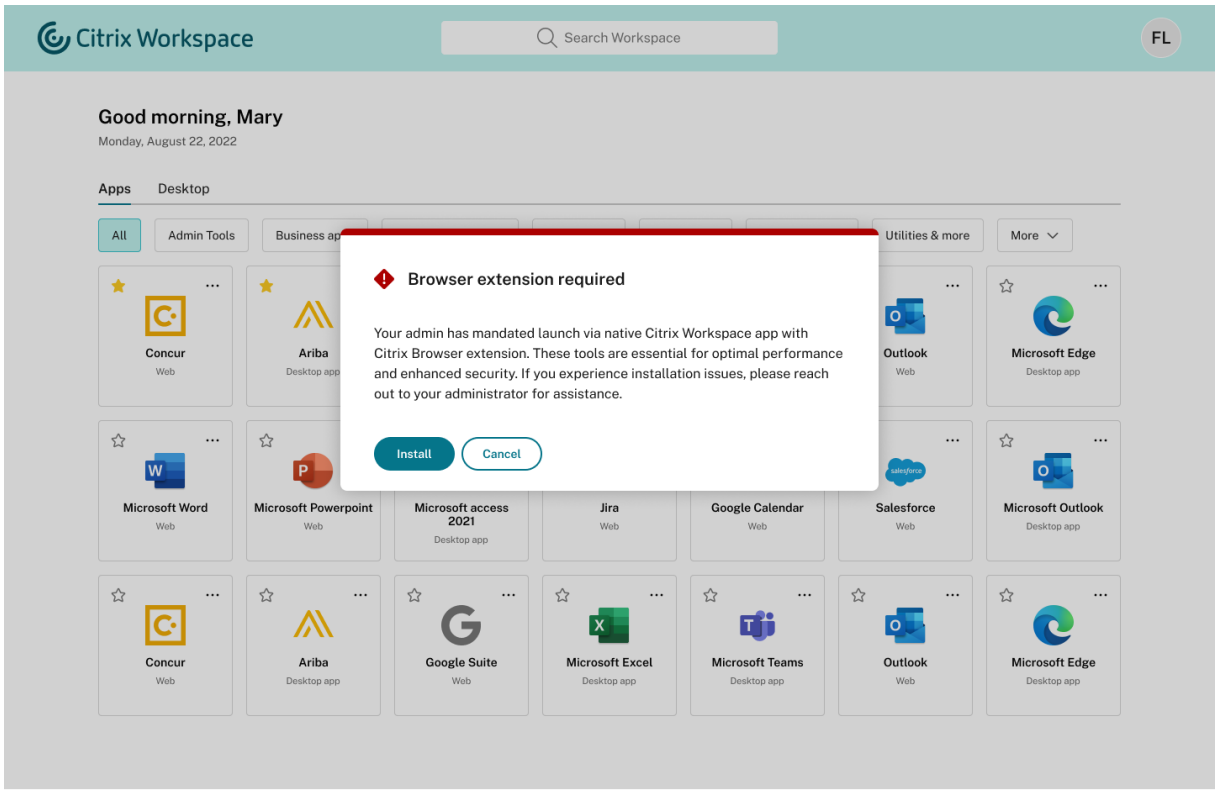
24.31

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.30

管理 **Workspace Web** 扩展程序的安装提示　您现在可以管理 Workspace Web 扩展的安装提示的显示。启用提示可以让 Workspace 检测当用户从浏览器打开 Citrix Workspace 时扩展是否安装在用户的设备上。如果尚未安装该扩展，则会提示用户下载并安装。一旦用户安装了扩展程序，它就会自动打开本机 Citrix Workspace 应用程序中的应用程序和桌面，而无需 Workspace 检测屏幕的干预。根据您的喜好，您可以将提示设置为强制或可选。此提示功能与 Google Chrome 和 Microsoft Edge 浏览器兼容。



当用户点击 安装 按钮时，它会将用户重定向到相应浏览器的 Web 扩展商店，他们可以在那里下载 Workspace Web 扩展。一旦用户下载并安装该扩展程序，下次将不会出现该提示。有关管理提示的更多信息，请参阅 启动应用程序和桌面。

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　此版本中没有已知问题。

24.29

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.28

弃用旧的 **Workspace UI**　旧的 Workspace UI 体验现已弃用。管理员不再有选择为最终用户启用旧 UI。新的 Workspace UI 提供了更好的用户体验并提高了工作效率，并且默认启用。

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。

24.27

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.23

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.22

此版本解决了提高整体性能、稳定性和功能增强的领域。

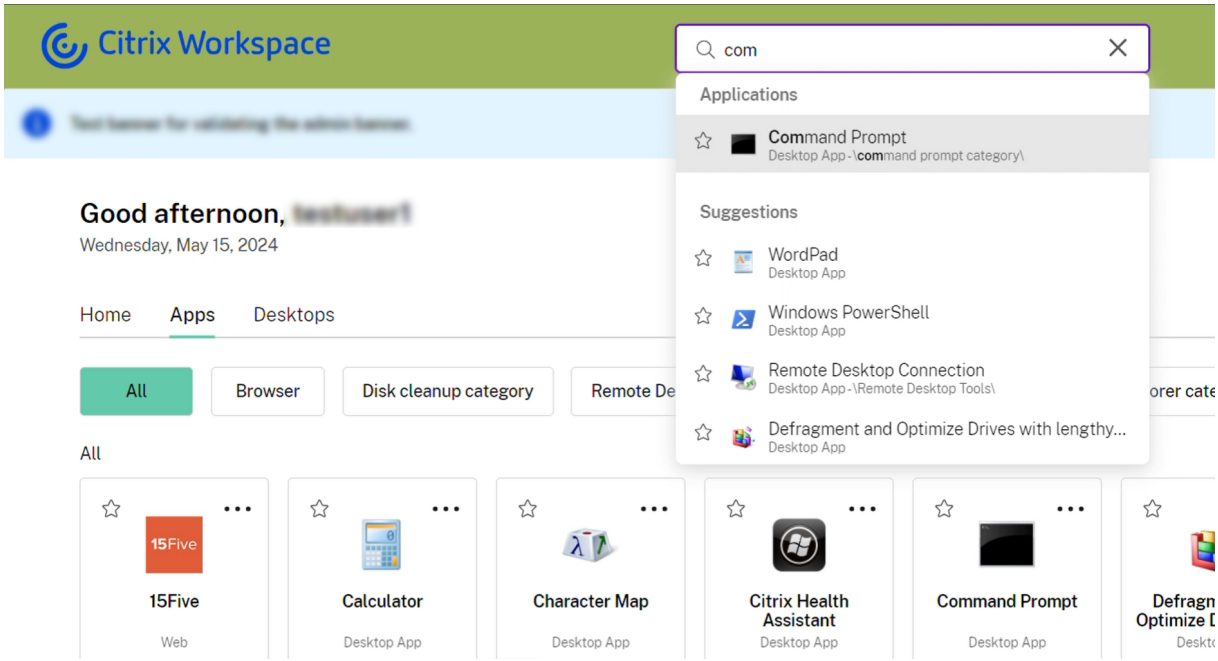
24.21

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.20

增强的搜索体验　Citrix Workspace 应用程序引入了增强的搜索引擎功能，允许最终用户在搜索结果旁边查看应用程序路径。此功能可帮助最终用户快速识别应用程序的位置。较长的应用程序路径会被截断，以保持搜索结果列表干净整洁。将鼠标指针悬停在路径的面包屑上时，您可以看到完整的路径。此外，如果类别名称与搜索输入相匹配，则类别名称将以粗体突出显示，以便于识别。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



性能改进　在以下领域的增强之后，Citrix Workspace UI 现在加载速度比以前更快：

1. 并行化用户身份验证和 **Workspace UI** 加载　Citrix Workspace UI 加载迅速，同时用户身份验证检查在后台运行。与以前的 Citrix Workspace UI 不同，新版本将以前的会话的缓存数据存储在本地，并重新使用它以更快地打开应用程序。因此，该应用程序不再需要用户等待身份验证检查完成。

以前，用户只有完成身份验证检查后才能访问该应用程序。这个大约 1-2 秒的延迟现在已经得到纠正，允许回访用户输入商店网址并开始访问工作区 UI，同时用户身份验证检查在后台运行。如果在后台检查期间发现用户会话未登录，应用程序将提示用户进行身份验证以继续会话。此外，该应用程序会在后台继续刷新应用程序数据，以便这些数据可以在后续会话中使用。

2. 缓存工作区 **UI**　工作区 UI 现在从缓存中加载，从而可以比以前更快地打开应用程序。此外，每当用户最小化 Workspace 应用程序、从 Workspace Web 应用程序选项卡切换到另一个浏览器选项卡或重新加载应用程序时，Workspace UI 都会在后台刷新以获取最新版本的 UI。

> 注意：
>
> 性能改进适用于 Citrix Workspace 应用程序和 Citrix Workspace Web 应用程序。

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　此版本中没有已知问题。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.19

休眠和恢复虚拟桌面会话（预览）

> 注意：
>
> 该功能目前仅在云商店可用。

用户现在可以在不使用时休眠 Citrix Workspace 应用程序上的虚拟桌面会话，并从中断的地方恢复。休眠操作保留桌面会话的整个状态，包括正在运行的应用程序。该功能允许用户在再次登录后无缝恢复他们的会话。与已停止或已解除分配的虚拟桌面相比，恢复后桌面会话启动速度更快。

Citrix Activity Manager 的休眠和恢复功能代表了 VDI 管理的重大进步，为组织提供了优化资源利用率和增强用户体验的强大工具。该功能可有效管理资源、改善用户体验并降低休眠期间的能耗，从而大幅节省成本。

有关在用户设备上配置此功能以及执行休眠和恢复操作的更多信息，请参阅 休眠和恢复虚拟桌面会话（预览版）。

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　此版本中没有已知问题。

Workspace Web 扩展 24.4.0

支持自定义域名　从 24.4.0 版本开始，Workspace Web Extension 现在完全支持在 Microsoft Edge 和 Google Chrome 浏览器上为自定义域开放应用程序和桌面。用户可以通过自定义域名 URL 无缝访问他们的工作区资源，从而提高工作效率并简化工作流程。

24.18

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.17

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.15

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.14

此版本解决了提高整体性能、稳定性和功能增强的领域。

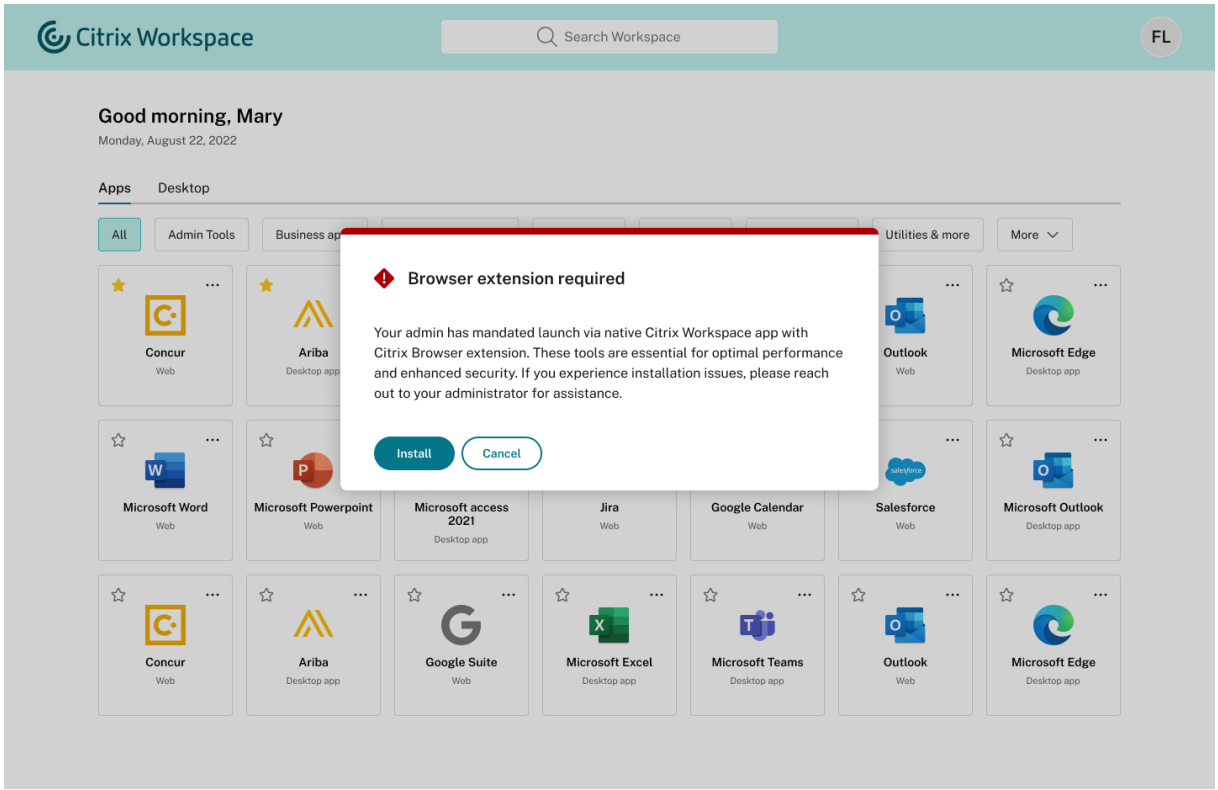
© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.13

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.12

管理 **Workspace Web** 扩展的安装提示（预览）　您现在可以管理 Workspace Web 扩展的安装提示的显示。启用提示可以让 Workspace 检测当用户从浏览器打开 Citrix Workspace 时扩展是否安装在用户的设备上。如果尚未安装该扩展，则会提示用户下载并安装。一旦用户安装了扩展程序，它就会自动打开本机 Citrix Workspace 应用程序中的应用程序和桌面，而无需 Workspace 检测屏幕的干预。根据您的喜好，您可以将提示设置为强制或可选。此提示功能与 Google Chrome 和 Microsoft Edge 浏览器兼容。



当用户单击“安装”按钮时，它会将用户重定向到相应浏览器的 Web 扩展商店，他们可以在那里下载 Workspace Web 扩展。一旦用户下载并安装该扩展程序，下次将不会出现该提示。有关管理提示的更多信息，请参阅 启动应用程序和桌面。

> 注意：
>
> 您可以使用附件 Podio 表格注册此预览功能。

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。

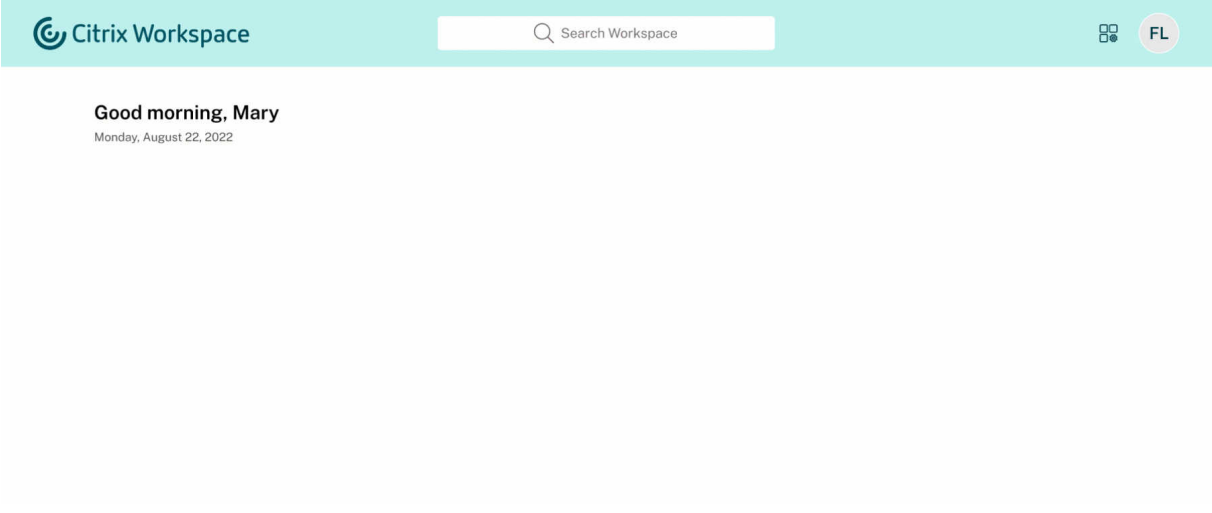
© 1997–2025 Citrix Systems, Inc. All rights reserved.

已知问题　此版本中没有已知问题。

24.11

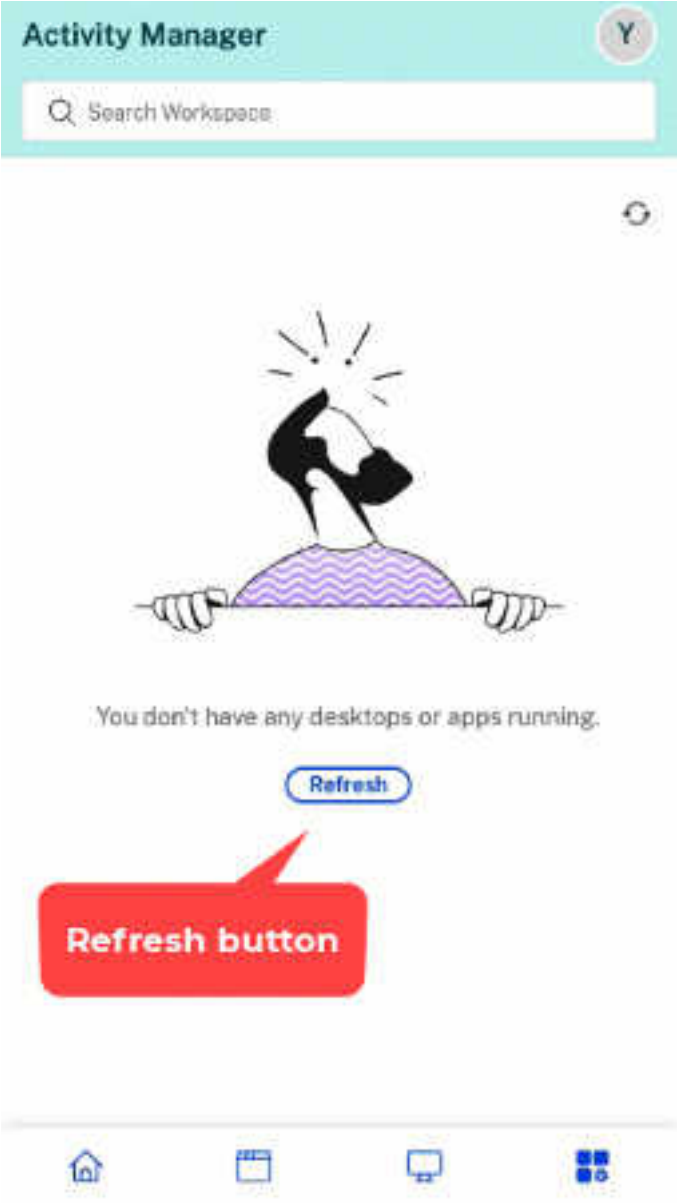
活动管理器有手动刷新选项　通过此版本，最终用户现在可以手动刷新云存储的 活动管理器 内的项目列表，可在桌面和移动设备上访问。他们不再需要重新启动 活动管理器 来查看更新的列表。有两个选项可用于刷新列表：刷新按钮和刷新图标。当 活动管理器 屏幕为空时，最终用户可以 使用 刷新 按钮，并且他们可以使用刷新图标 来更新现有列表。此新功能允许最终用户更高效、更方便地管理 活动管理器 中的会话，从而增强了最终用户体验。

桌面版活动管理器：



移动版活动管理器：

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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　此版本中没有已知问题。

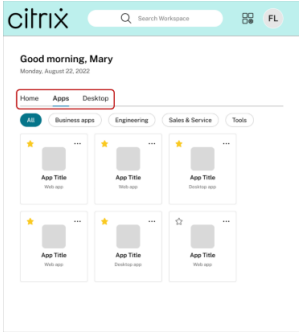
24.10

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.9

禁用工作区 **UI** 的简单视图　当前，当用户启动包含少于 20 个资源的 Citrix Workspace 应用程序时，他们会看到简单视图的屏幕，其中用户看不到导航选项卡，例如主页、应用程序和桌面。所有应用程序和桌面都合并在一个页面上，管理员无法禁用此视图。在此版本中，您可以禁用简单视图并根据您的喜好自定义新的工作区 UI。



即使资源数量少于 20，如果您希望为用户提供一致的视图，您仍然可以使用导航选项卡。有关如何管理简单视图的更多信息，请参阅 工作区视觉和布局改进。

已修复的问题　本版本中没有已修复的问题。

已知问题　此版本中没有已知问题。

24.8

此版本解决了提高整体性能、稳定性和功能增强的领域。

支持芬兰语： Citrix Workspace UI 现已提供芬兰语版本。

24.7

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.6

此版本解决了提高整体性能、稳定性和功能增强的领域。

24.5

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

24.4

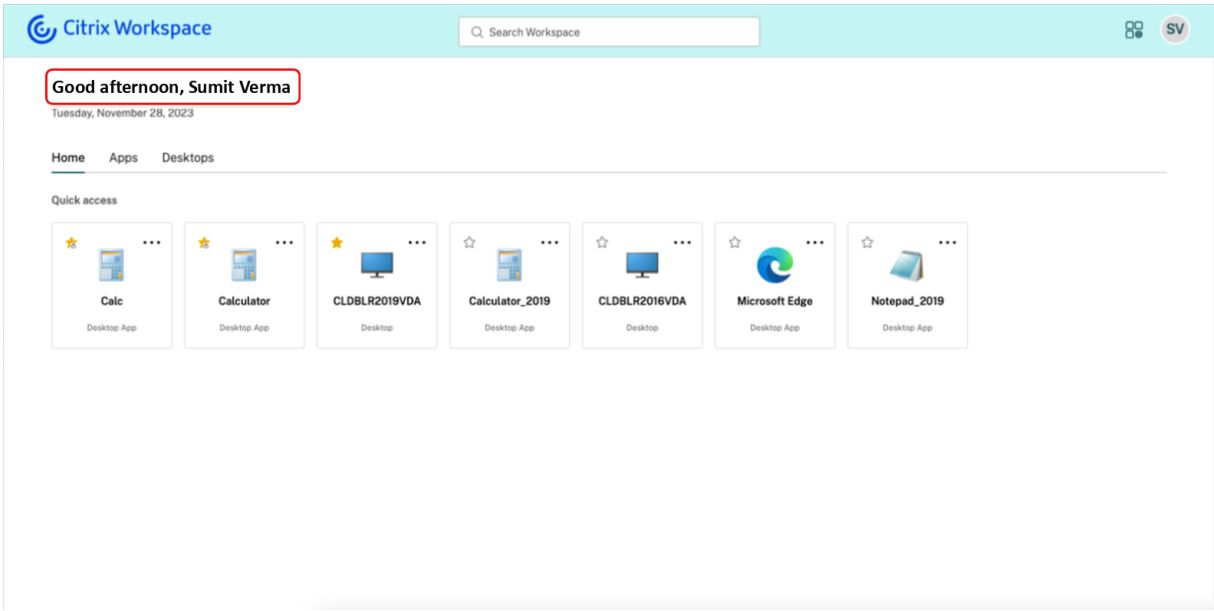
此版本解决了提高整体性能、稳定性和功能增强的领域。

23.49

此版本解决了提高整体性能、稳定性和功能增强的领域。

23.48

在 **Workspace UI** 上查看用户的显示名称和个人资料图片　在此版本中，用户现在可以在 Workspace UI 上查看他们的显示名称和个人资料图片。用户的显示名称与问候语一起显示。个人资料图片、姓名首字母或通用图像会出现在用户菜单的右上角。管理员必须注意，仅当 Active Directory 获取有效数据时，Workspace UI 才会显示此信息。



有关更多信息，请参阅 管理用户的显示名称和个人资料图片

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。

23.46

此版本解决了提高整体性能、稳定性和功能增强的领域。

23.45

此版本解决了改进整体性能和稳定性的区域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

此版本解决了提高整体性能、稳定性和功能增强的领域。

23.43

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

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

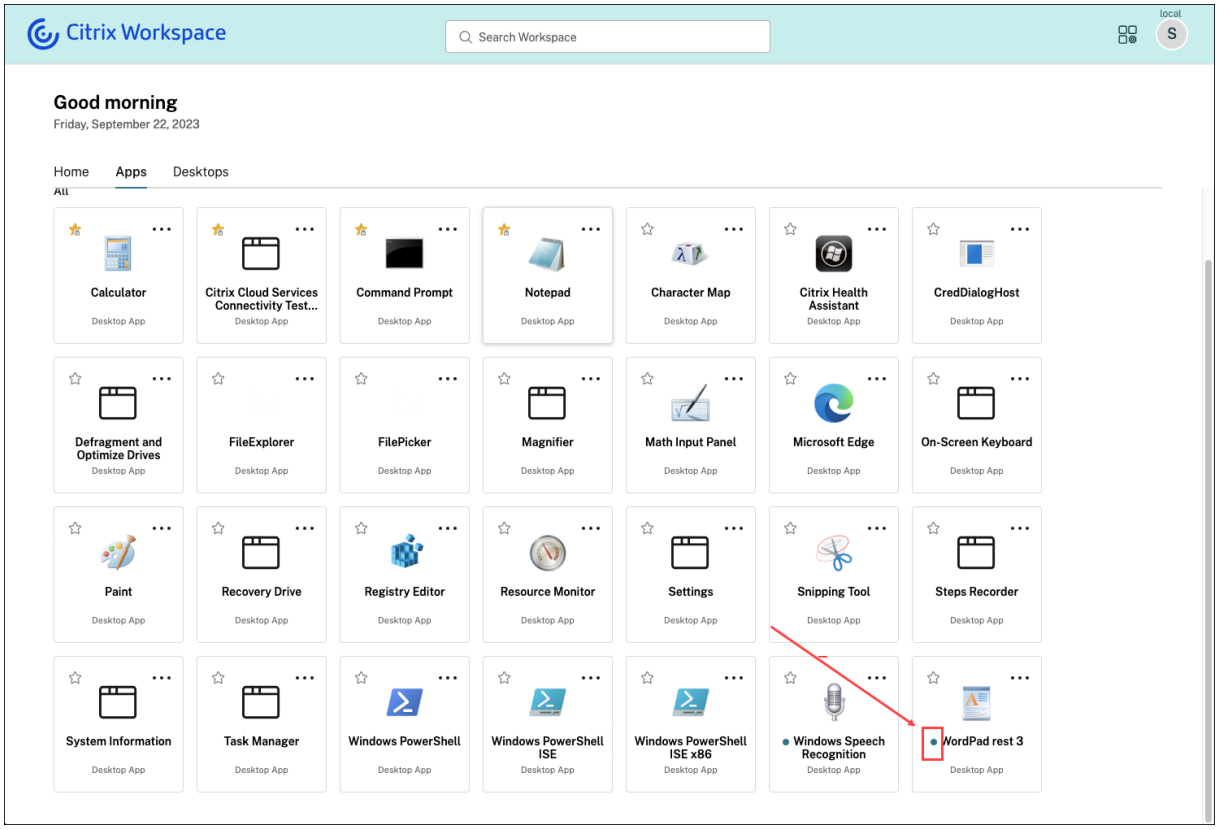
此版本解决了改进整体性能和稳定性的区域。

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

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

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

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

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 - 全面上市　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：从当前会话注销。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。
- 关闭：关闭断开连接的桌面。
- 强制退出：出现技术问题时强制关闭您的桌面电源。
- 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 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。

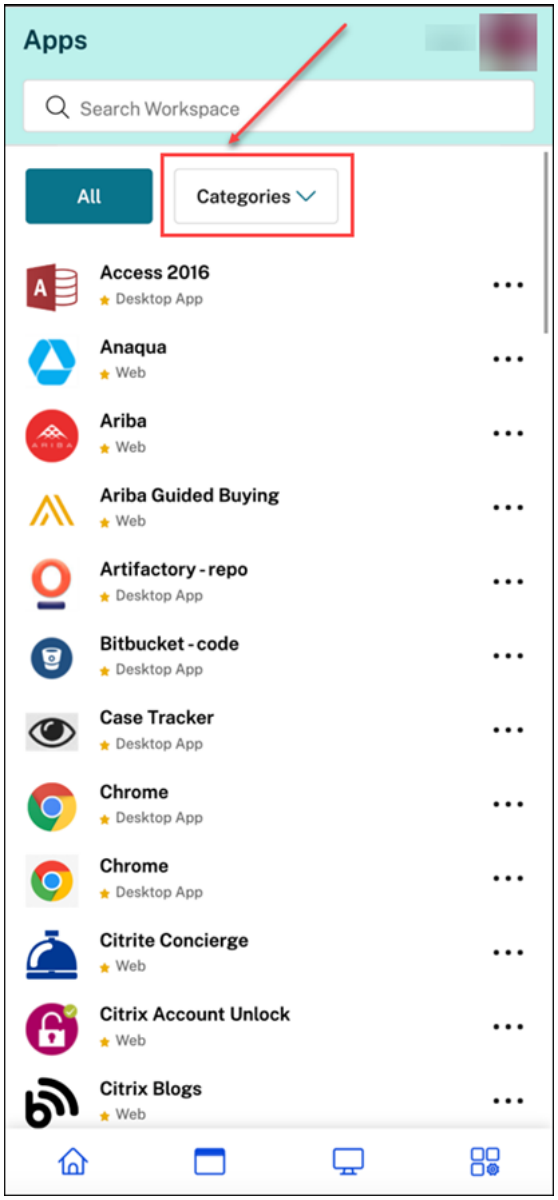
已知问题

- 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。
- 对于启用了 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

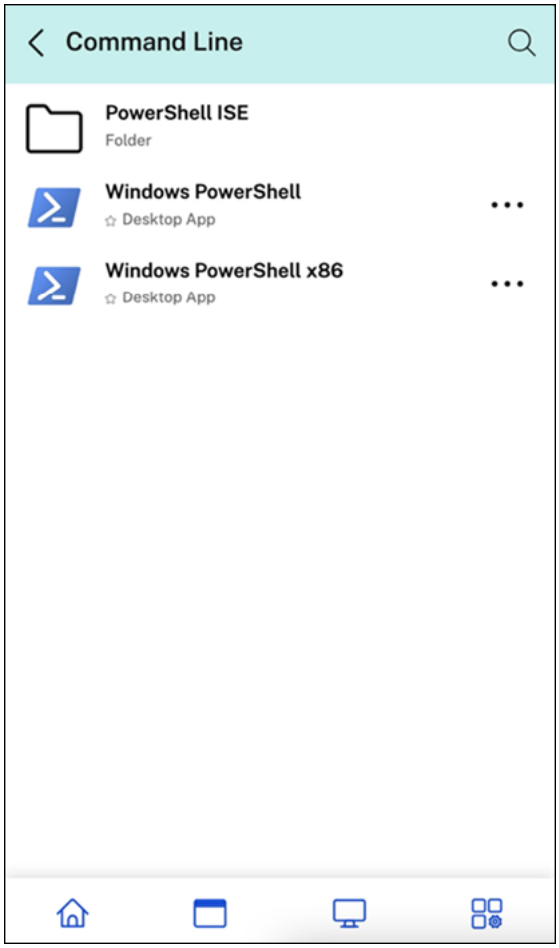
查看移动平台上应用程序的子类别　终端用户现在可以在 Android 和 iOS 设备上查看按类别和子类别整理的应用程序，从而提供便捷的访问和愉快的应用程序浏览体验。要查看类别，请导航至“应用程序”选项卡，然后单击“类别”下拉列表。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

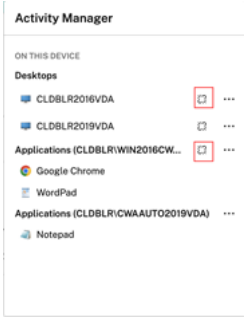


选择相关类别，将根据管理员所做的配置显示可用子类别和应用程序的列表。根据管理员配置，子类别显示为可能包含更多子文件夹或应用程序的文件夹。有关更多信息，请参阅添加文件夹路径

© 1997–2025 Citrix Systems, Inc. All rights reserved.

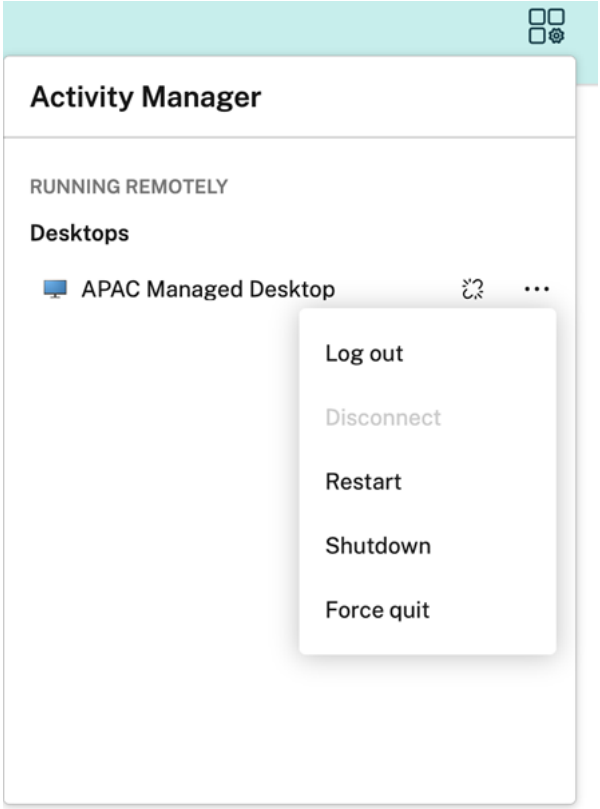


通过任何设备在活动管理器上管理已断开连接的会话　活动管理器现在允许最终用户查看在断开连接模式下运行的本地或远程应用程序和桌面并对其执行操作。可以从移动或桌面设备管理会话，使最终用户能够随时随地执行操作。对断开连接的会话执行操作，例如注销或关闭，可以促进资源的优化使用并降低能耗。



- 断开连接的应用程序和桌面显示在“活动管理器”面板上，并由一个断开连接图标予以指示。
- 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



最终用户可以通过单击省略号按钮对断开连接的桌面执行以下操作：

- 注销：使用此选项可从断开连接的桌面中注销。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。
- 关闭：使用此选项关闭断开连接的桌面。
- 关闭电源：如果出现技术问题，可以使用此选项强制关闭断开连接的桌面电源。
- 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

此版本解决了提高整体性能、稳定性和功能增强的领域。

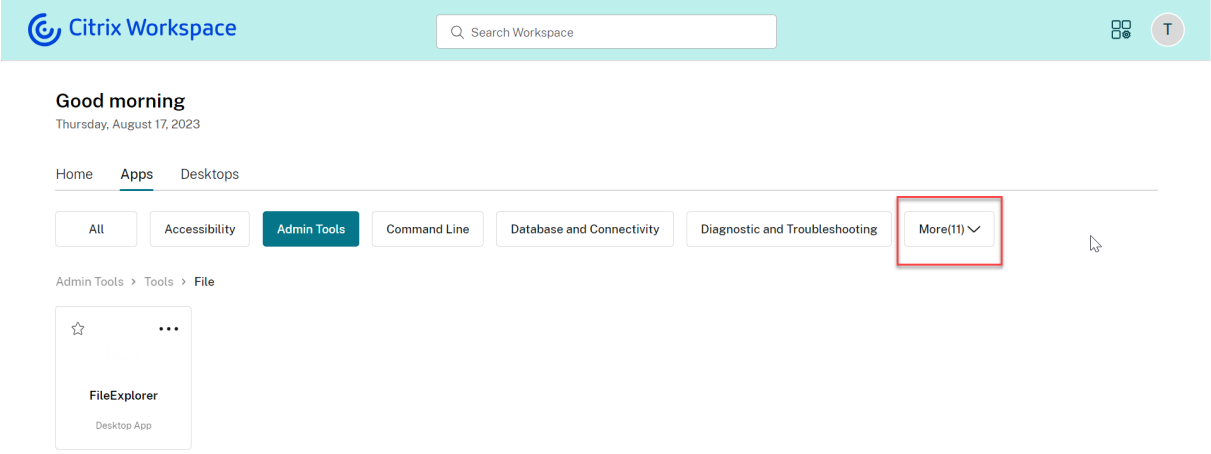
23.34

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

23.33

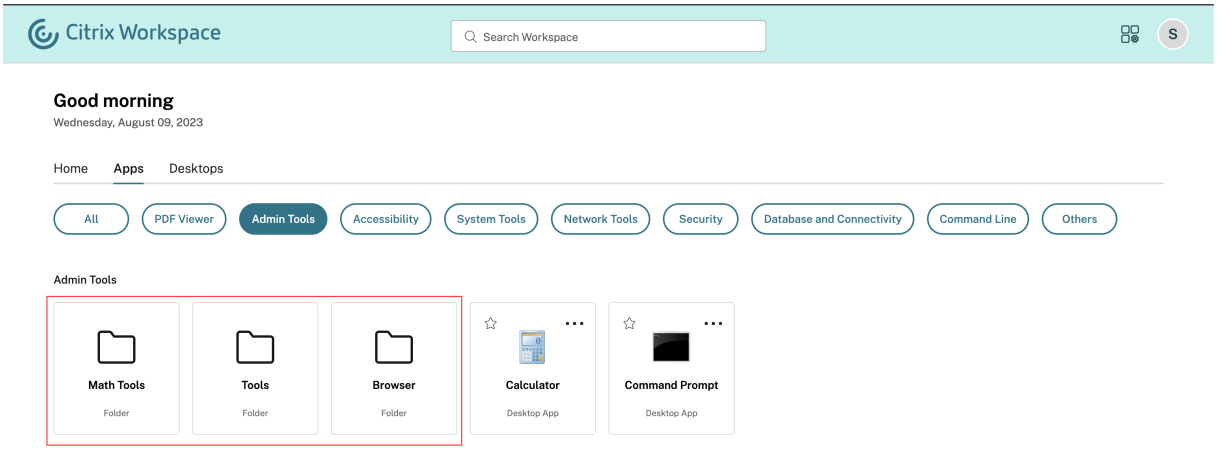
通过应用分类增强用户体验　最终用户可以在 Workspace 用户界面上查看按类别和子类别组织的应用程序。如果分类涉及两个以上的级别，则最终用户将看到他们的应用程序排列在文件夹结构中。用户可以看到导航痕迹。当管理员创建的主要类别的数量超过用户屏幕上的可用空间时，用户界面会根据屏幕大小进行调整，并在“更多”下拉列表中动态移动类别。



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

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。井然有序的多级结构可提供整洁、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。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

此版本解决了提高整体性能、稳定性和功能增强的领域。

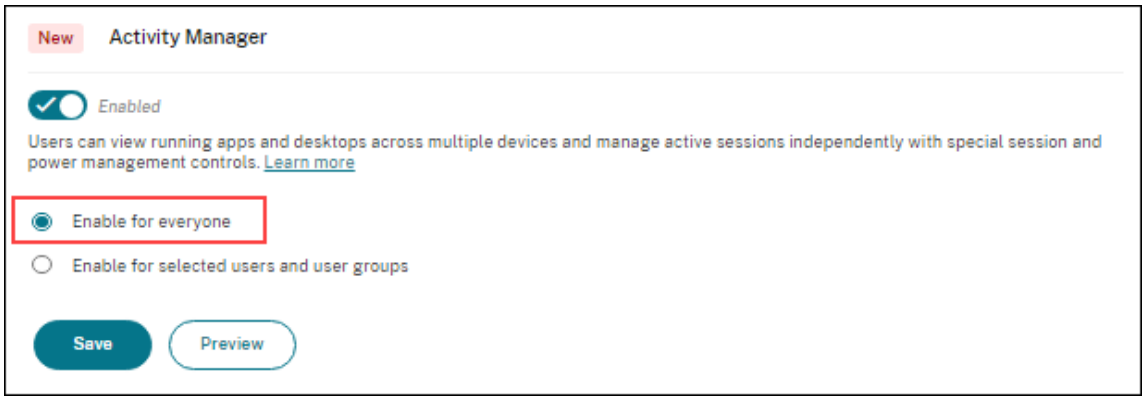
23.30

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。有关详细信息，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。

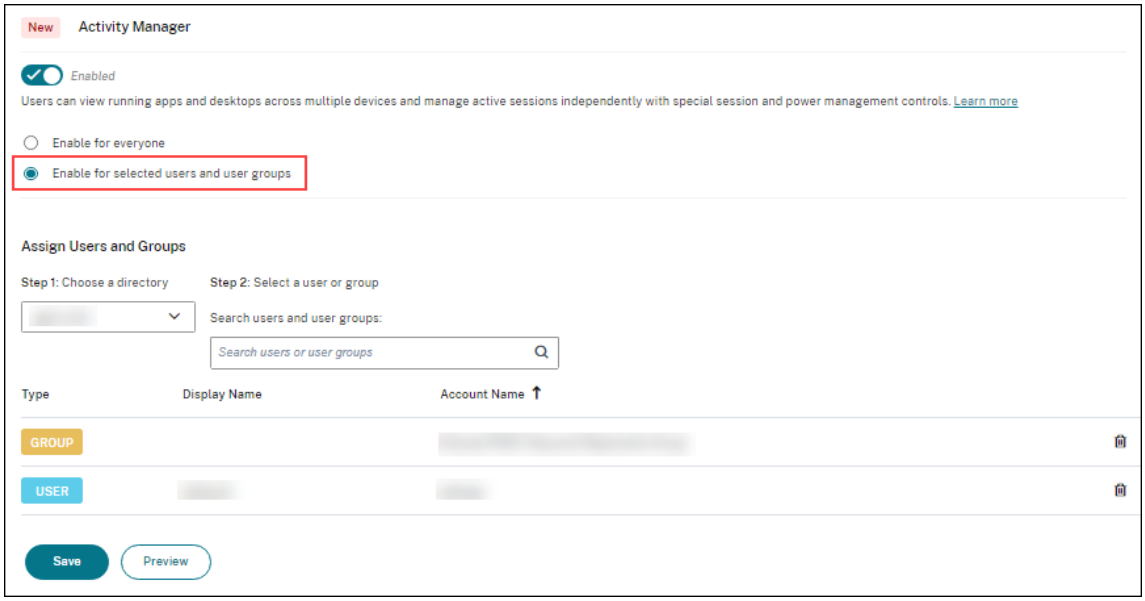
要启用活动管理器，请执行以下操作：

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”。

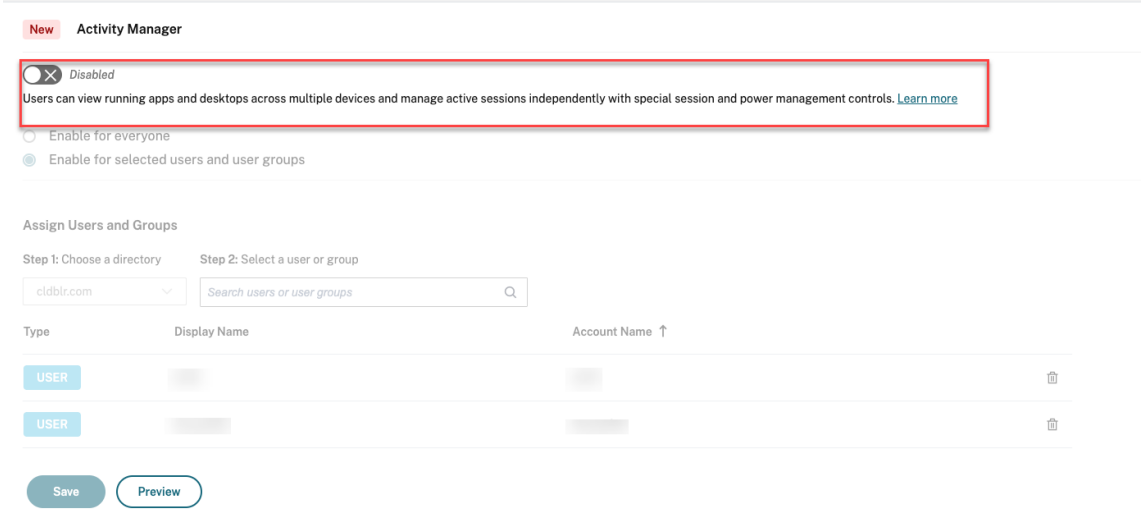


   - 要为选定的用户和用户组启用活动管理器，请选择为选定的用户和用户组启用。然后，您可以选择用户或用户组所属的目录。选择相应的目录后，您可以查看相关的用户和用户组。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 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

此版本解决了提高整体性能、稳定性和功能增强的领域。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

23.28

Internet Explorer 的弃用公告　UI 版本 23.26 可在 Internet Explorer 上使用至 2023 年的最后一周。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

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]

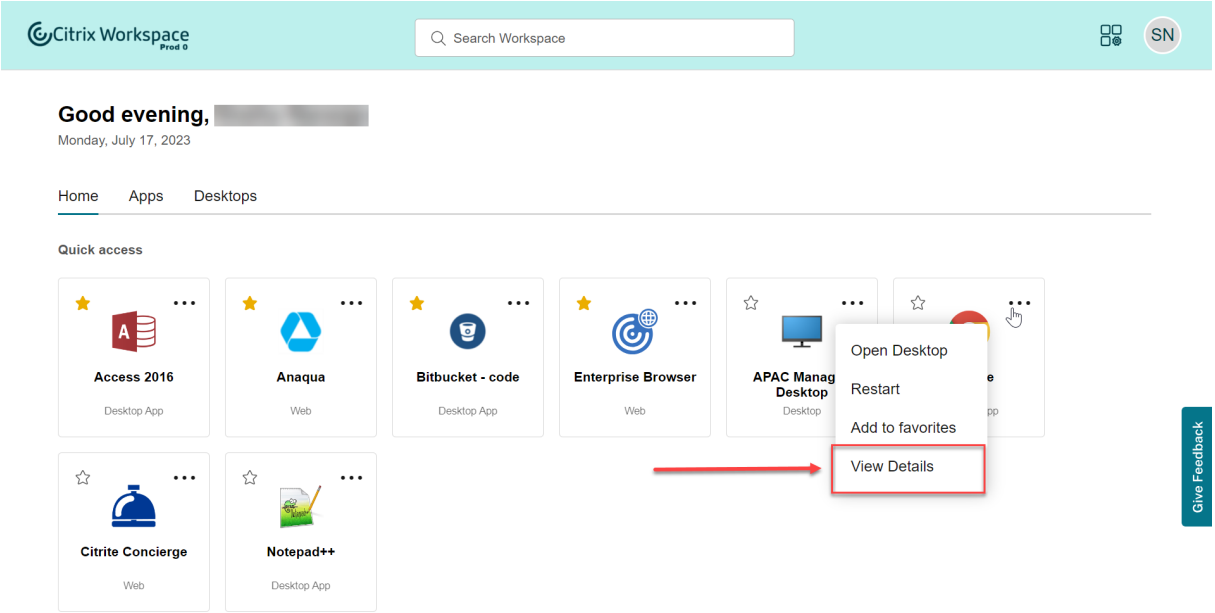
23.26

此版本解决了提高整体性能、稳定性和功能增强的领域。

23.25

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”。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

此版本解决了提高整体性能、稳定性和功能增强的领域。

23.23

此版本解决了提高整体性能、稳定性和功能增强的领域。

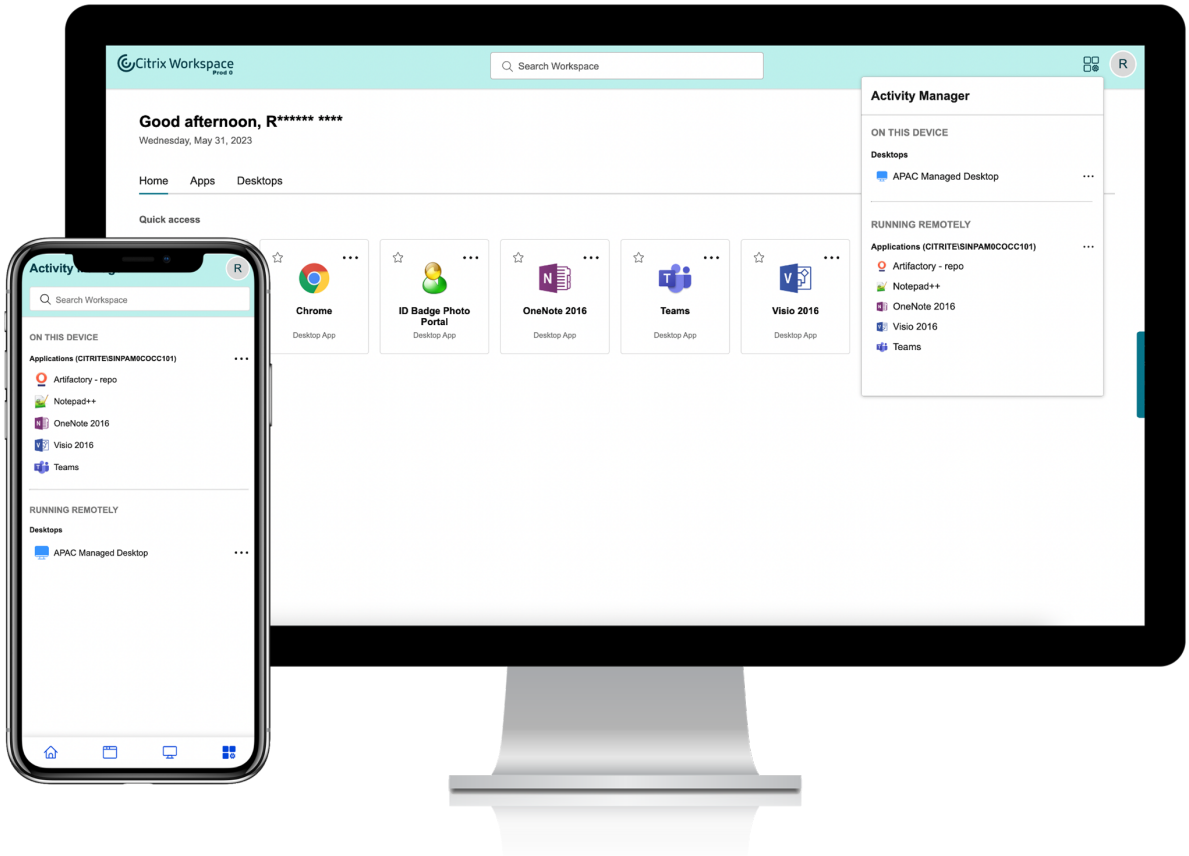
23.22

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



有关详细信息，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 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商店的活动会话。

23.15

新的 **Workspace** 用户界面　引入了新的 UI 功能，具有现代的外观和感觉，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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

增强的首次用户体验　当您第一次从浏览器启动下载的 或 Citrix 时，系统会提示您查看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

May 20, 2025

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

2025 年 5 月 9 日

ControlUp 的 RemoteDX 插件管理

ControlUp 的 RemoteDX 是一种监控和故障排除解决方案，旨在改善远程工作人员的最终用户体验。主要功能包括端点监控、网络洞察、会话可见性和主动警报。通过全局应用程序配置服务，您可以管理 ControlUp 的 RemoteDX 插件管理器。

有关更多信息，请参阅 ControlUp 的 RemoteDX 插件管理。

2025 年 4 月 3 日

GACS 支持混合启动（技术预览版）

从 2503 版本开始，适用于 Windows 和 Mac 的 Citrix Workspace 应用程序支持通过全局应用程序配置服务 (GACS) 进行管理，以实现混合启动。

在混合启动场景中，用户通过 Web 浏览器访问其 Citrix 资源。在浏览器界面中选择应用程序或桌面后，Citrix StoreFront 服务器会生成一个 ICA 文件，其中包含打开该资源的具体说明。本机 Citrix Workspace 应用程序读取

© 1997–2025 Citrix Systems, Inc. All rights reserved.

ICA 文件的内容并启动与远程应用程序或桌面的连接。通过支持混合启动，GACS 现在允许您为用户提供一致的体验，无论他们是通过本机应用程序还是浏览器访问商店。

要了解有关该功能的更多信息，请参阅 管理混合启动设置。

2024 年 12 月 20 日

配置文件功能可供本地商店用户使用

全局应用程序配置服务中的配置文件功能允许管理员为用户组配置设置。此功能现在也可用于本地商店。有关支持此功能的兼容 Citrix Workspace 应用程序版本的详细信息，请参阅 验证 Citrix Workspace 应用程序版本。

有关更多信息，请参阅 使用配置文件管理用户组的设置。

2024 年 12 月 12 日

定义自动更新的时间范围

管理员现在可以在 Mac 设备上随时安排 Citrix 产品的自动更新。在此指定时间内，软件会自动更新，或者用户会收到可用更新的通知。

有关更多信息，请参阅 自动更新时间范围。

管理 **Citrix Workspace** 应用程序的自动更新版本和推出期

管理员可以安排方便的日期范围，在此期间 Citrix Workspace 应用程序的自动更新应推出给最终用户。此功能使他们能够确定推出日期，最大限度地减少对最终用户的干扰并改善用户体验。

有关更多信息，请参阅 Citrix Workspace 应用程序版本。

自动更新管理设置支持配置文件

自动更新管理设置（例如 自动更新时间范围 和 **Citrix Workspace** 应用程序版本）可通过配置文件适用于不同的用户组。

有关更多信息，请参阅 自动更新管理设置支持配置文件。

2024 年 10 月 9 日

云商店用户可在 **Linux** 和 **Android** 上使用配置文件功能

全局应用程序配置服务中的配置文件功能允许管理员为用户组配置设置。从适用于 Linux 的 Citrix Workspace 应用程序版本 2408 和适用于 Android 的版本 24.9.0 发布开始，此功能可在 Linux 和 Android 上供云商店用户使用。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

有关更多信息，请参阅 发行说明：适用于 Linux 的 Citrix Workspace 应用程序 和 发行说明：适用于 Android 的 Citrix Workspace 应用程序

了解有关该功能的更多信息，请参阅 使用配置文件管理用户组的设置。

2024 年 9 月 24 日

iOS 上的云商店用户可使用配置文件功能

全局应用程序配置服务中的配置文件功能允许管理员为用户组配置设置。从适用于 iOS 的 Citrix Workspace 应用程序版本 24.9.0 发布开始，此功能可在 iOS 上供云商店用户使用。

有关更多信息，请参阅 发行说明：适用于 iOS 的 Citrix Workspace 应用程序

了解有关该功能的更多信息，请参阅 使用配置文件管理用户组的设置。

2024 年 7 月 2 日

插件管理器可用于 **Microsoft Teams**

从适用于 Windows 版本 2405 的 Citrix Workspace 应用程序开始，管理员现在可以使用 Microsoft Teams VDI 插件管理器优化通话和会议的音频和视频。这一增强功能提高了虚拟会议期间的性能和用户体验。可以通过 Global App Configuration 服务管理 Microsoft Teams VDI 插件管理器的安装和配置。反过来，该插件管理器会在最终用户的设备上安装并管理 Microsoft Teams 优化插件（VDI 2.0 或 Slimcore 引擎）。

有关更多信息，请参阅 Microsoft Teams VDI 插件管理。

2024 年 6 月 4 日

跨应用商店、渠道和配置文件克隆设置

管理员现在可以使用名为 克隆设置的新功能，通过全局应用程序配置服务跨商店、渠道和配置文件克隆设置。此功能允许您复制现有设置，而不必再次经历整个配置过程。因此，它节省了大量的时间和精力，从而提高了生产力并简化了工作流程。

有关配置此功能的更多信息，请参阅 跨商店、渠道和配置文件克隆设置。

2024 年 5 月 29 日

首次使用 **Citrix Workspace** 应用程序进行 **HTML5** 时应用 **GACS** 设置

从适用于 HTML5 版本 2404.1 及更高版本的 Citrix Workspace 应用程序开始，当最终用户首次启动 Workspace 会话时，将应用全局应用程序配置服务 (GACS) 设置。还可能会提示最终用户重新启动他们的会话以确保合规性。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

有关更多信息，请参阅 Citrix Workspace 应用程序（适用于 HTML5）产品文档。

2024 年 5 月 7 日

使用配置文件管理用户组的设置（预览）

随着适用于 Mac 和 Windows 的 Citrix Workspace 应用程序版本 2402 的发布，您现在可以使用全局应用程序配置服务 (GACS) 中的 配置文件 管理用户组的设置。配置文件用于识别用户组的集合。它允许您管理用户组的设置，而不是将其应用于访问商店的所有用户。为此，您可以创建一个配置文件并向其中添加所需的用户组。然后，您可以选择配置文件，分配设置并发布它们，以将特定的体验应用于不同的用户组。

有关配置配置文件设置的更多信息，请参阅 使用配置文件管理用户组的设置。

> 注意：
>
> 该功能目前适用于 Windows 和 Mac 平台的云商店。对其他平台的支持即将推出。

2024 年 4 月 11 日

全局应用配置服务的改进

随着适用于 Windows 和 Mac 的 Citrix Workspace 应用程序版本 2402 的发布，我们在以下领域增强了全局应用程序配置服务 (GACS)：

通过用户身份验证保护设置　GACS 目前分两个阶段提供服务。Citrix Workspace 应用程序最初会获取在用户身份验证之前需要应用的某些设置，其余设置在身份验证成功后应用。

此功能为即将推出的 GACS 功能铺平了道路，该功能使您能够根据用户所属的用户组为用户配置设置。

> 注意：
>
> 经过身份验证的 GACS 目前仅适用于 Workspace 商店。对 StoreFront 商店的支持即将推出。

发现改进　Citrix Workspace 应用程序现在具有增强的发现和配置各种用户输入设置的能力。用户现在可以开始使用电子邮件地址、域名或商店 URL 使用该应用程序。根据用户输入，GACS 发现相关的商店 URL 并将其全部添加。

以前，当您将多个商店 URL 映射到一个域并为多个商店 URL 配置 GACS 设置时，用户无法将任何商店添加到 Citrix Workspace 应用程序，因为它会发现多个商店。但是，从 2402 版本开始，此限制已被取消。

> 注意：
>
> 从适用于 Windows 2402 和 Mac 2402 的 Citrix 工作区应用程序开始，您可以添加多个启用 GACS 的商店。您首先添加的商店优先为设置分配值，后续商店将继承第一个商店确定的行为。在即将发布的版本中，我们将为管理员引入一项设置，允许您管理是否可以将商店作为单个商店还是作为多个商店的一部分添加到 Citrix Workspace

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 应用程序中。同时，如果您希望启用此设置，请联系 Citrix 支持。

完整的 **StoreFront URL** 支持　GACS 具有额外的灵活性，可以使用通用 FQDN 为 StoreFront URL 配置不同的设置。让我们以商店 `https://mywork.acme.com/Citrix/StoreFTE` 和 `https://mywork.acme.com/Citrix/StorePartner`为例。以前，您只能在 `https://mywork.acme.com` (FQDN) 级别配置设置，这无法为每个商店配置不同的设置：`StoreFTE` 和 `StorePartner`。

2024 年 3 月 18 日

Citrix Enterprise Browser 的其他设置

全局应用程序配置服务 (GACS) 具有新的设置来配置 Citrix Enterprise Browser，允许您管理以下操作：

- 地址自动填充建议
- 信用卡信息的自动填充建议
- 无需提示用户即可启动外部应用程序
- 当使用潜在危险的命令行标志启动浏览器时显示安全警告。
- 管理默认 Cookie 设置
- 管理默认弹出窗口设置
- 将扩展程序、应用程序和主题安装到浏览器
- 禁止浏览器中针对任何可疑相似域名发出警告
- 允许网站检查已保存的付款方式
- 管理浏览器历史记录的保存
- 管理浏览器地址栏中的搜索建议
- 导出书签
- 当用户登录企业浏览器时创建临时配置文件

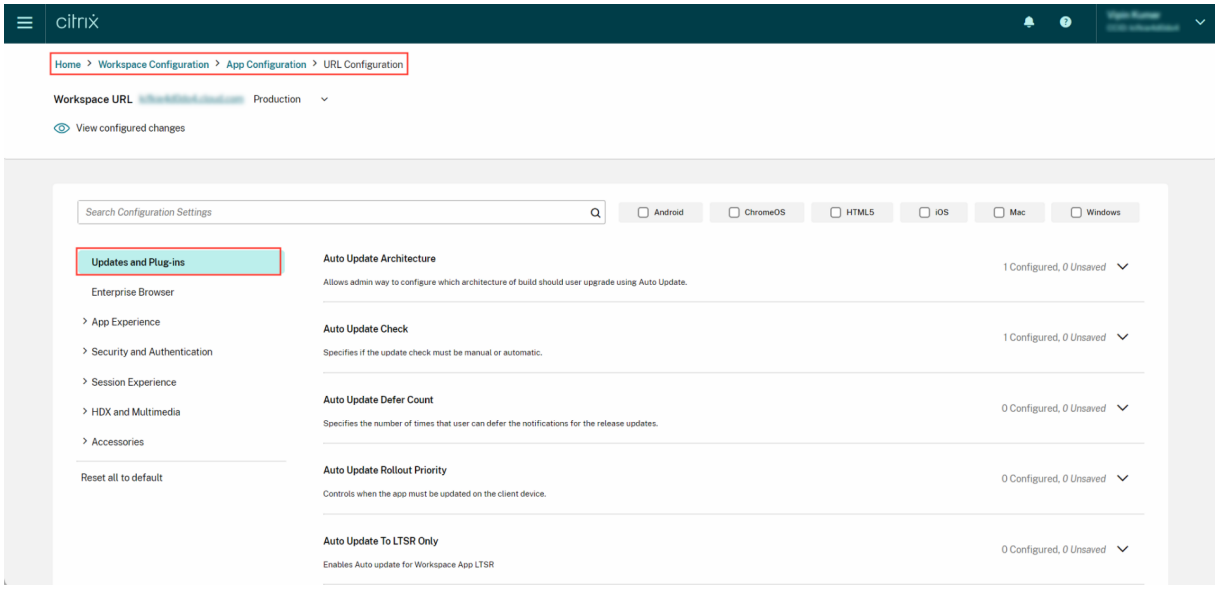
有关设置的更多信息，请参阅 Citrix Enterprise Browser 产品文档中的 通过全局应用程序配置服务管理 Citrix Enterprise Browser 。

2024 年 1 月 18 日

使用全局应用程序配置服务管理插件

全局应用程序配置服务提供了一个集中式平台，帮助您配置插件的安装和更新设置。您可以在托管和非托管设备之间分发插件设置。要配置插件设置，请导航到云门户上 工作区配置 > 应用程序配置 下的 更新和插件 类别。有关详细信息，请参阅 插件管理。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



您可以配置以下插件：

- Citrix 端点分析插件
- Citrix 安全访问代理
- Webex VDI 自动升级插件
- Zoom VDI 插件管理

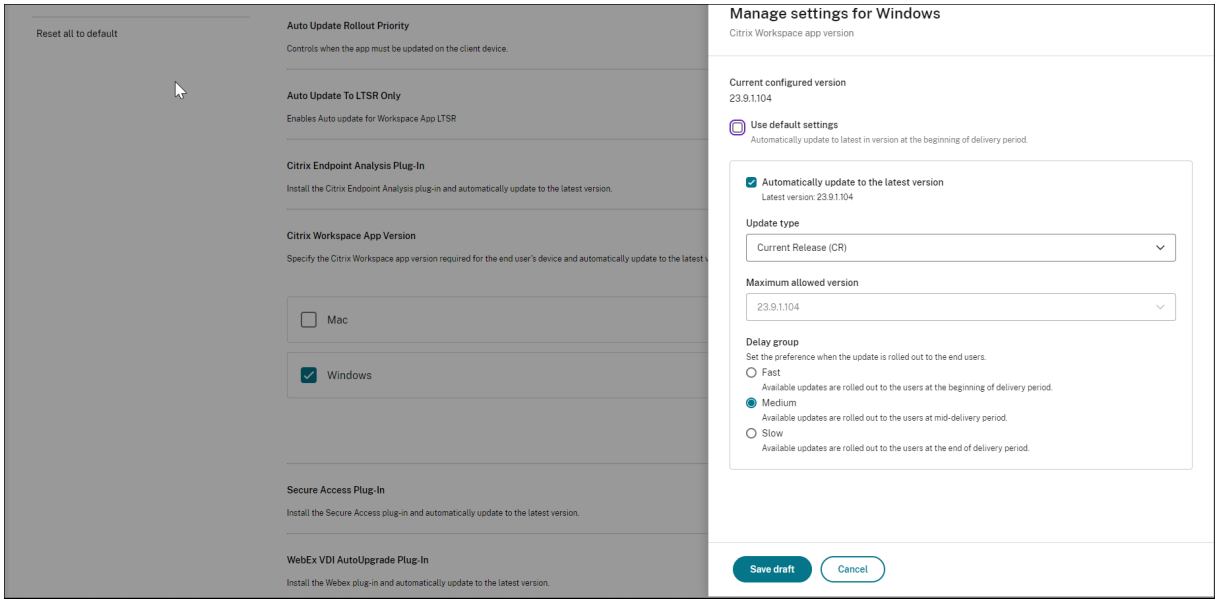
2023 年 11 月 21 日

管理 Citrix Workspace 应用程序版本

作为管理员，您现在可以从集中平台管理 Citrix Workspace 应用程序的自动更新或版本设置。您可以自定义 **CR** （当前版本）和 **LTSR** （长期服务版本）版本的设置。您可以设置一条规则，每当有新版本可用时，自动将最终用户更新到最新版本。如果您不想更新到最新版本，您也可以指定最终用户必须更新到的首选版本才能获得最佳效果。

可以从 更新和插件 部分针对 Windows 和 Mac 平台自定义 **Citrix Workspace** 应用程序版本 设置。有关更多信息，请参阅 管理 Citrix Workspace 应用程序版本。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2023 年 10 月 30 日

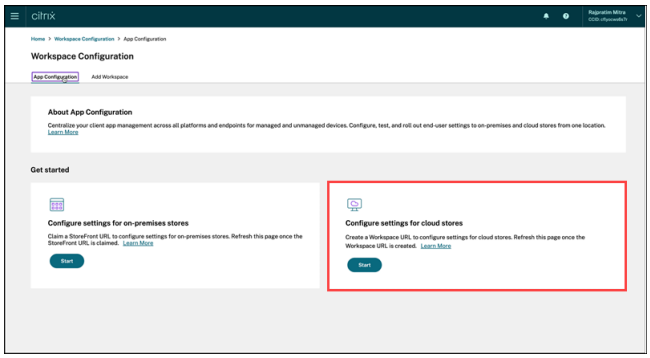
为本地应用商店配置设置

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。如果您已声明您的 StoreFront URL，请参阅 配置设置部分了解更多信息。

如果您尚未认领您的 StoreFront URL，您可以认领它。为此，请单击 **App Configuration** 部分下的 **Claim URL** 来声明您的 URL。有关更多信息，请参阅 开始配置。

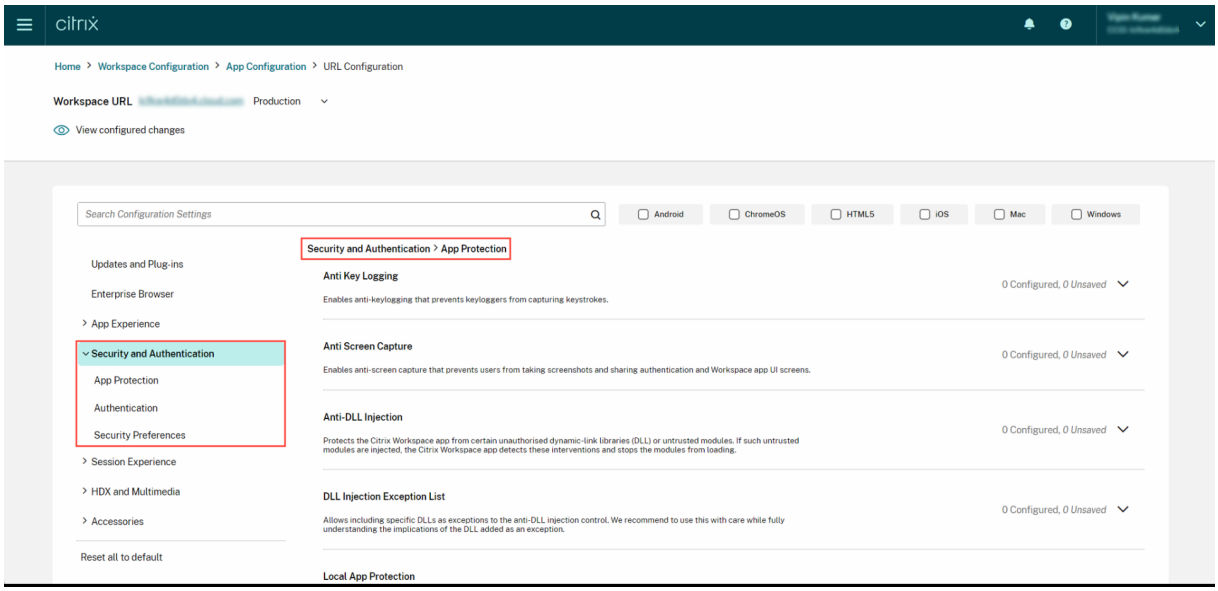


© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

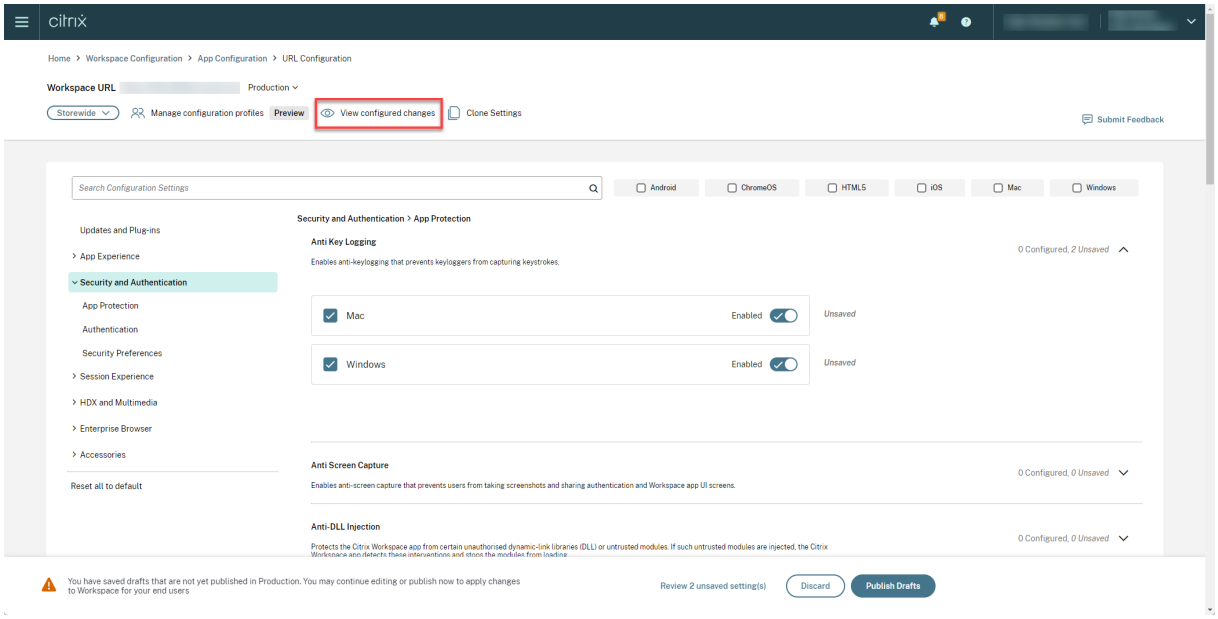


2023 年 7 月 28 日

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。

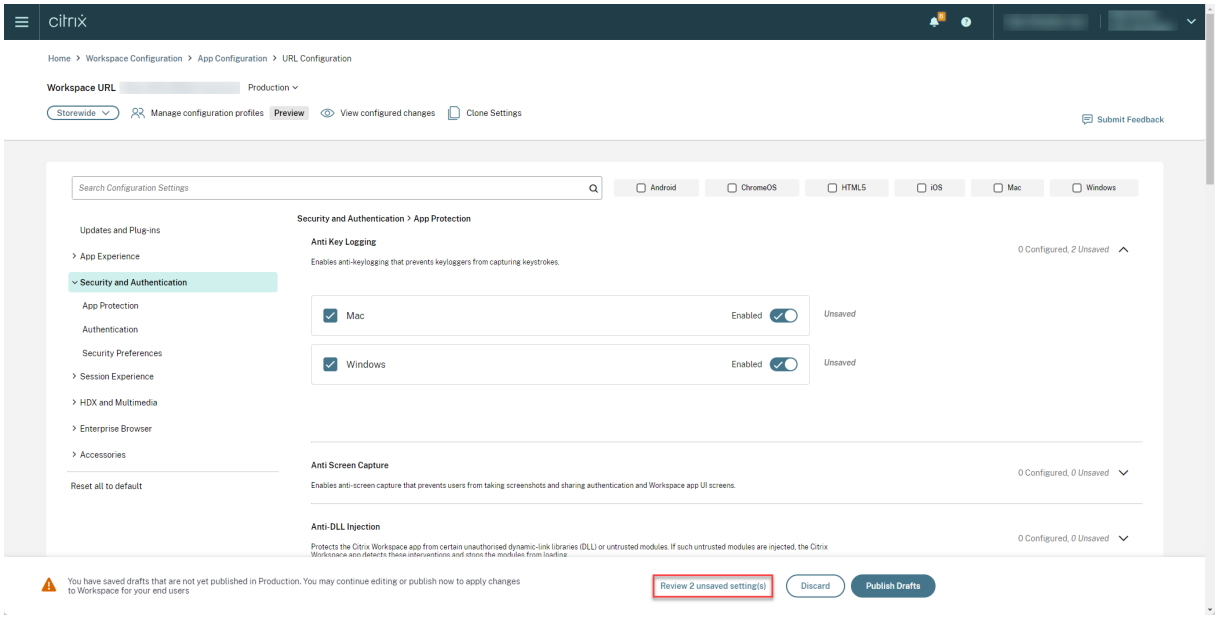
© 1997–2025 Citrix Systems, Inc. All rights reserved.



2023 年 6 月 7 日

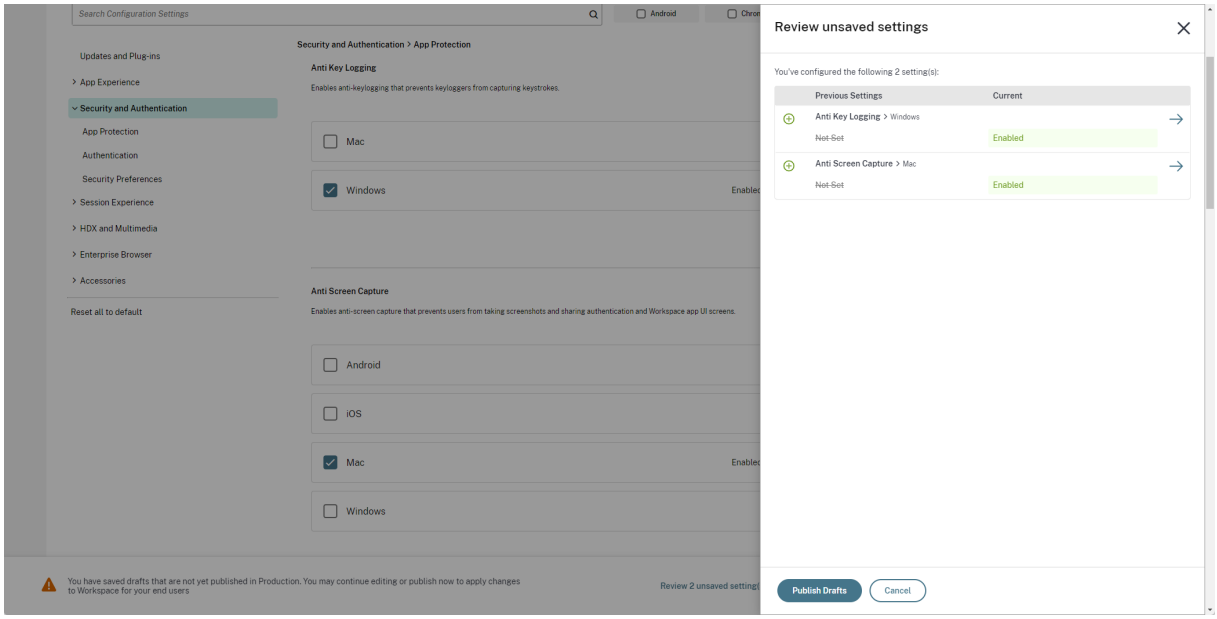
查看未保存的更改

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。

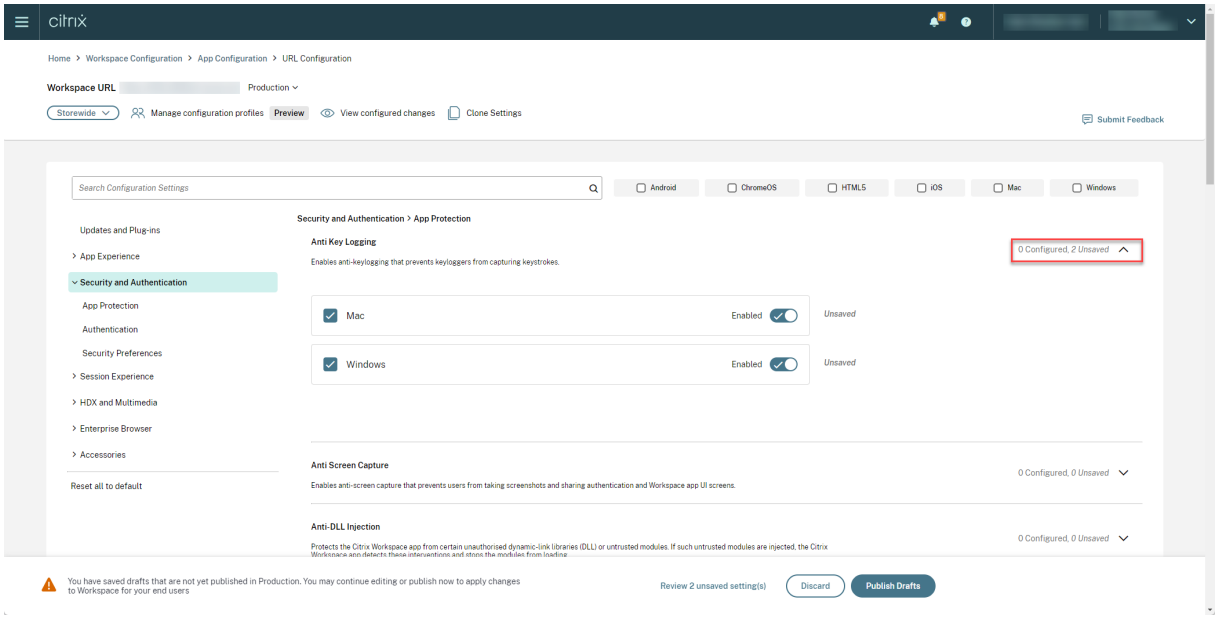
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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



© 1997–2025 Citrix Systems, Inc. All rights reserved.

May 23, 2023

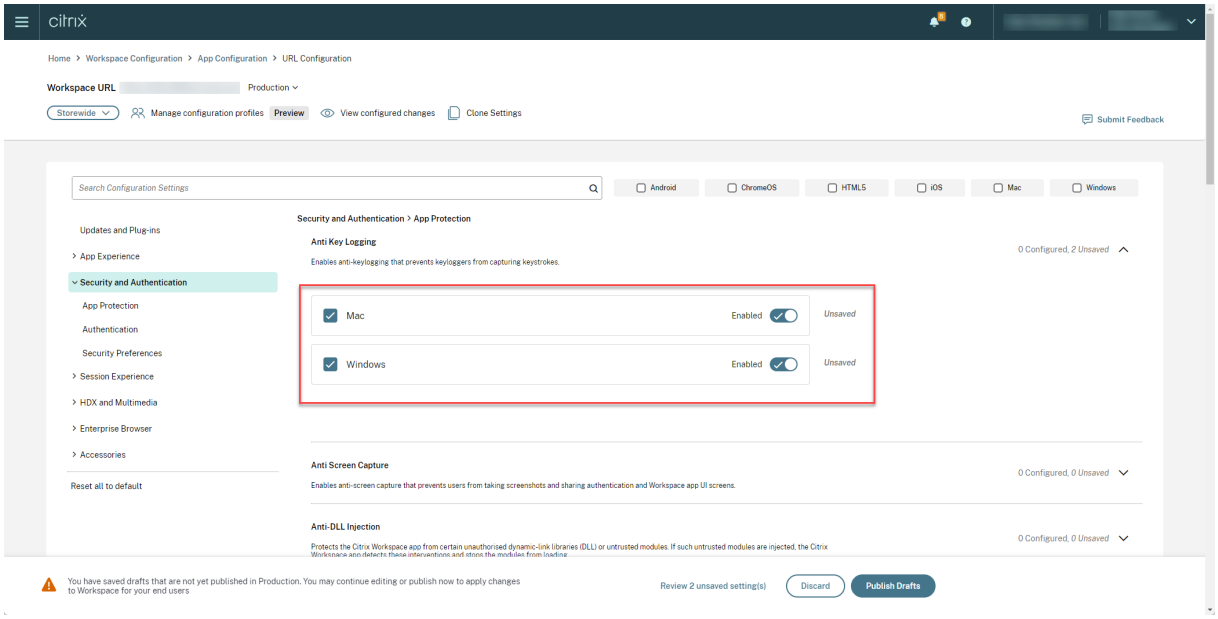
增强的搜索功能

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。

- 使用设置描述搜索 管理员还可以通过输入设置描述中的关键字来定位设置。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** 设置名称搜索 管理员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 7, 2024

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

工作流程概述

在设置 Citrix Workspace 之前，请查看 系统要求。

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

1. 在 Citrix Cloud 中为 Citrix Workspace 做准备。
2. 配置最终用户访问和身份验证。
3. 将服务集成到工作区。
4. 使用您企业特定的偏好（例如徽标和安全策略）自定义工作区 。
5. 向最终用户推出 Citrix Workspace。

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。如果您已经是 Citrix Cloud 客户，并且通过 身份和访问管理添加管理员，则您可以跳至 第 2 阶段：配置订阅者访问和身份验证。

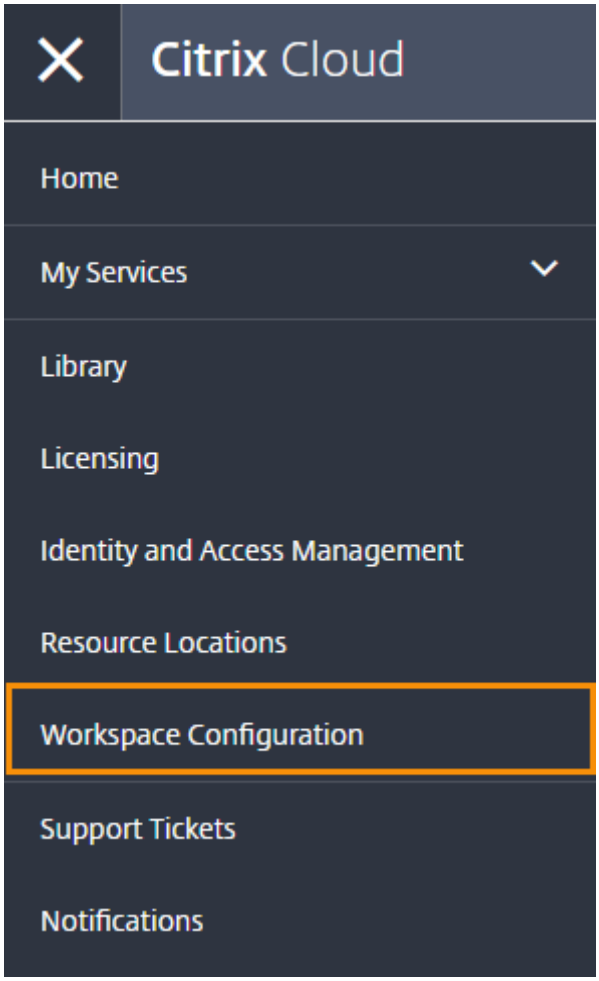
第 1 阶段涉及的步骤包括：

1. 注册 Citrix Cloud。
2. 添加身份提供者 来验证管理员或工作区用户。
3. 添加可以配置工作区的管理员 。如果您已将管理员配置为具有 自定义访问权限，则在 常规 部分下选择 工作区配置。
4. 通过以下方式设置基础架构：
    - 创建资源位置。
    - 部署云连接器。

第 **2** 阶段：配置最终用户访问和身份验证

登录 Citrix Cloud 后，您可以从主菜单访问 工作区配置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



如果您没有看到此选项，请确保您具有 工作区配置 权限，请参阅 修改管理员权限。

第二阶段涉及配置访问控制，包括身份验证方法、工作区 URL 和资源的外部连接。

> 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 简单、安全地访问 Citrix Cloud 服务和工作区。访问 Citrix Workspace 的另一种方式是通过 Web 浏览器。有关更多信息，请参阅 用户访问。

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。它通常涉及以下任务：

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置工作区的身份验证

定义最终用户如何进行身份验证以登录其工作区是一个两步过程：

1. 在 身份和访问管理下，配置 身份和访问管理。
2. 在 工作区配置 **>** 身份验证下，选择您在第一步中配置的身份提供者提供的身份验证方法之一。有关更多信息，请参阅 配置身份验证。

如果您使用联合身份提供程序，您还可以使用 Citrix 联合身份验证服务 (FAS)启用对 VDA 的单点登录 (SSO)。

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

您可以在 工作区配置 中通过以下方式为不同用户定制工作区体验，以满足特定的组织要求：

- 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，例如允许用户创建 收藏夹 并自动启动桌面。有关自定义用户如何与其工作区交互的说明，请访问 自定义工作区交互。
- 自定义隐私和安全设置。这包括设置超时期限、创建登录策略以及允许用户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：向最终用户推出 **Citrix Workspace**

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. 入职用户。
    - 与用户沟通 Citrix Workspace 功能。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 共享 工作区 URL。
- 指导用户安装 Citrix Workspace 应用程序。

系统要求

March 1, 2025

Citrix Cloud

要配置 Citrix Workspace，您必须在 Citrix Cloud 上拥有一个帐户，并且已启用 Citrix Desktops as a Service 或 Secure Private access。

参见 Citrix Cloud 系统和连接要求

DaaS

要访问 DaaS 资源，请参阅 DaaS 系统要求。

最终用户连接

Citrix Workspace 应用程序

最终用户可以使用任何受支持的 Citrix Workspace 应用程序 版本连接到您的工作区。旧版本的 Citrix Workspace 应用程序可能可以运行但不受支持。建议您使用最新版本的 Citrix Workspace 应用程序。并非所有功能在 Citrix Workspace 应用程序的早期版本中都可用。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。

Citrix Receiver 已达到使用寿命终止 (EoL)。它可能会以较少的功能运行但不再受支持。Citrix Workspace 至少需要支持 TLS 1.2 的 Citrix Receiver 版本：

Receiver	最低版本
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0

© 1997–2025 Citrix Systems, Inc. All rights reserved.

如果您需要使用旧版本的 Citrix Receiver，请使用 Citrix StoreFront ，可将其配置为允许旧版本的 TLS（不推荐）。

Web 浏览器

最终用户可以使用以下浏览器的最新版本连接到他们的工作区：

- Citrix Enterprise Browser
- Microsoft Edge
- Google Chrome
- 火狐浏览器
- Apple Safari

管理员可以使用这些网络浏览器来配置工作区。

Citrix Workspace Web 扩展程序　为了获得更好的体验和可靠性，建议用户在其 Web 浏览器中添加 Citrix Workspace Web 扩展。有关更多信息，请参阅 Citrix Workspace Web 扩展 和 安装 Citrix Workspace Web 扩展。

网络连接

有关网络连接的信息，请参阅 Citrix Cloud 文档中的 Citrix Workspace 应用程序连接 。

Citrix Virtual Apps and Desktops 站点聚合

站点聚合可与 Citrix Virtual Apps 和 Desktops 的所有受支持版本一起使用。Citrix Virtual Apps and Desktops 的早期生命周期结束 (EoL) 版本可能可以运行但不受支持。

XenApp 和 XenDesktop 已终止使用 (EoL)。XenApp 和 Desktop 7.0 及更高版本可能可以运行但不受支持。与 Citrix 联合身份验证服务 (FAS) 一起使用需要 XenApp 和 XenDesktop 7.16 或更高版本。

NetScaler Gateway

Citrix Workspace 可以使用任何受支持的 NetScaler Gateway 版本来提供对资源的访问。或者使用 Citrix Gateway 服务实现零部署解决方案。

联合身份验证服务 (FAS)

Citrix Workspace 可以使用 FAS 为资源提供单点登录，有关更多信息，请参阅 。

有关系统要求，请参阅 FAS 系统要求。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

使用 Citrix Workspace 交付 DaaS、Virtual Apps and Desktops

November 7, 2024

Citrix Workspace 是 StoreFront的云服务替代品，它是聚合 Citrix DaaS 应用程序和桌面的本地 Windows 应用程序。Citrix Workspace 是一个云组件，提供远程工作、可扩展性和定制所需的工具、服务和功能。

您可以在单个部署中同时使用本地 StoreFront 和 Citrix Workspace。例如，您可以使用 Citrix Workspace 为外部用户提供访问权限，而内部用户使用本地 StoreFront。

全面迁移至 DaaS

建议您先从本地 CVAD 部署迁移到 DaaS，然后再从本地 StoreFront 迁移到 Citrix Workspace。有关更多信息，请参阅 从本地迁移到云 和 技术区部署指南。

本地 Citrix 虚拟应用程序和桌面站点聚合

您可以使用现有的本地 Virtual Apps and Desktops 部署过渡到 Citrix Workspace。这一过程称为站点聚合。这具有性能和弹性限制，因此仅推荐用于简单部署。

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。

资源连接

以下是如何提供对虚拟应用程序和桌面的访问的选项，这些选项针对不同的业务需求而设计。

连接选项	场景
NetScaler 网关设备	如果您想使用自己的网关与外部资源建立连接，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	如果您想使用 **Citrix Gateway** 服务 与您的资源进行外部连接，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资源 **，请选择此选项。如果您选择此选项，订阅者将无法访问外部资源。

有关更多信息，请参阅 外部连接。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。这包括有关如何执行以下操作的信息：

- 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)。

用户访问

November 7, 2024

用户可以使用两种不同的方法访问工作区。

- Citrix Workspace 应用程序 - 拥有兼容版本的 Citrix Workspace 应用程序的用户可以在 Citrix Workspace 应用程序内访问他们的工作区。这样可以提供最佳的用户体验和最强大的功能。
- 网络浏览器 - 拥有兼容网络浏览器的用户可以通过浏览工作区的 URL 来访问工作区。默认情况下，用户还需要兼容版本的 Citrix Workspace 应用程序才能打开虚拟桌面和应用程序，即 混合启动。但是，您可以配置自己的 Web 站点，使用户无需安装 Citrix Workspace 应用程序即可通过浏览器访问其资源。

Citrix Workspace 应用程序

Citrix Workspace 应用程序是用于访问工作区的本地安装的应用程序。有关更多信息，请参阅 Citrix Workspace 应用程序。

配置 **Citrix Workspace** 应用程序

安装后，必须使用提供用户的桌面和应用程序的应用商店的连接详细信息对 Citrix Workspace 应用程序进行配置。可以通过以下方式之一向用户提供所需的信息，从而简化用户的配置过程。

手动配置　用户可以将 Workspace URL 输入 Citrix Workspace 应用程序中。有关详细信息，请参阅 Citrix Workspace 应用程序文档。

预配文件　用户使用 Web 浏览器登录工作区后，可以前往 帐户设置、高级 并下载工作区配置文件。当用户使用 Citrix Workspace 应用程序打开此文件时，它会将工作区添加到该应用程序中。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Global App Configuration Service 使用全局应用程序配置服务为您的工作区配置 Citrix Workspace 应用程序。请参阅 [配置云存储的设置]/en-us/citrix-workspace/global-app-config-service/configure-gacs-cloud)。

支持的 **Citrix Workspace** 应用程序和 **Citrix Receiver** 版本

有关 Citrix Workspace 应用程序和 Citrix Receiver 支持的版本的详细信息，请参阅 系统要求。

Web 浏览器

作为使用本地安装的 Workspace 应用程序的替代方案，用户可以通过 Web 浏览器访问他们的商店。有关支持的浏览器，请参阅 系统要求。

当用户从 Web 浏览器启动他们的资源时，有两种可能性：

1. 资源在本地安装的 Citrix Workspace 应用程序内打开。这称为“混合启动”。由于它利用了完整的操作系统集成，因此为用户提供了最佳体验。有关更多详细信息，请参阅混合启动
2. 资源在他们的网络浏览器中打开。这使用户无需在本地安装任何软件即可访问资源。

默认配置是资源始终在本地安装的 Citrix Workspace 应用程序中打开。您可以更改配置以始终在浏览器中打开资源或让用户自己选择。有关更多信息，请参阅 启动应用程序和桌面。

如果管理员选择 让最终用户选择，那么当用户第一次在浏览器中打开工作区 URL 时，用户可以选择单击 使用 **Web** 浏览器 在其 Web 浏览器中启动资源。

混合启动

当用户首次在浏览器中打开 Workspace 但配置为在本地安装的 Citrix Workspace 应用程序内启动应用程序时，这称为混合启动。网站可以通过多种方式与本地安装的 Workspace 应用程序通信以打开资源。

Citrix Workspace Web 扩展程序

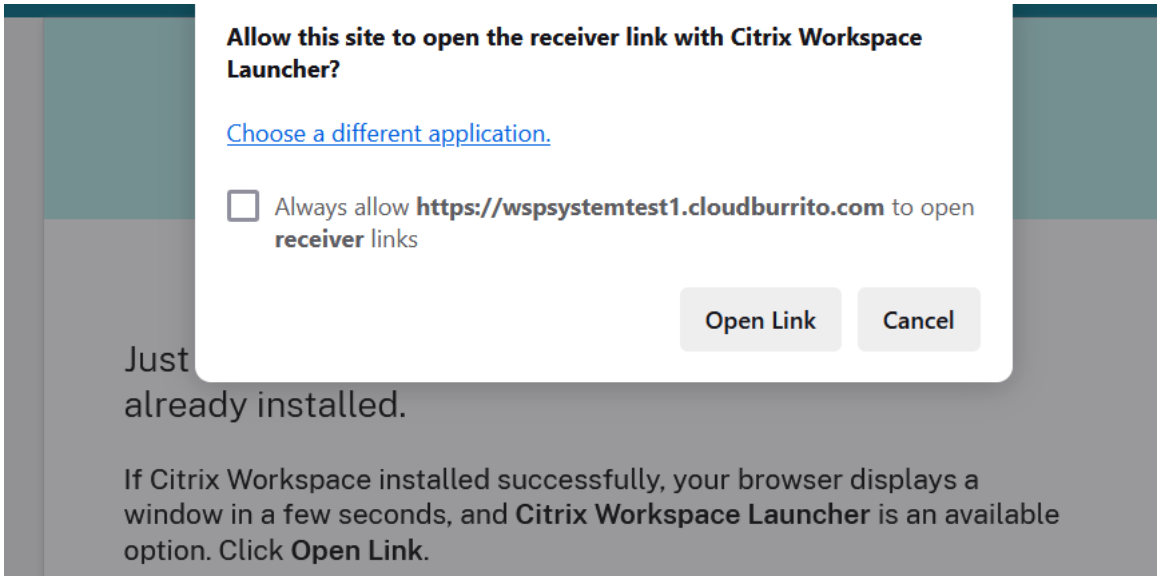
Citrix Workspace Web 扩展程序是适用于常用 Web 浏览器的扩展程序，可以改善用户检测本地安装的 Citrix Workspace 应用程序以及启动虚拟应用程序和桌面的体验。与 Citrix Workspace 启动器相比，这提供了更好的用户体验。

用户第一次访问受支持平台上的 Workspace URL 时，它会提示用户检测本地安装的 Workspace 应用程序。它首先尝试使用 Web 扩展，如果失败，则尝试使用 Citrix Workspace Launcher。已完成 Workspace 应用程序检测的现有用户可以转至帐户设置，单击更改 **Citrix Workspace** 应用程序以重新检测 Workspace 应用程序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Workspace Launcher

当用户首次转到受支持的操作系统和浏览器的工作区 URL，并且未安装 Citrix Web Extensions 时，它会尝试调用 Citrix Workspace Launcher。浏览器可能会提示用户进行确认，例如：



如果安装了受支持版本的 Citrix Workspace 应用程序，则该应用程序会通知 Citrix Workspace，Citrix Workspace 会记住这一点，并且在启动应用程序时使用 Citrix Workspace Launcher。

Citrix Workspace Launcher 需要下列最低版本的 Citrix Receiver 或 Citrix Workspace 应用程序。

- Receiver for Windows 4.3 或更高版本
- Receiver for Mac 12.0 或更高版本

如果 Citrix Workspace 启动器不可用，或者用户不允许其打开，那么它将无法检测本地安装的 Citrix Workspace 应用程序。用户可以选择再试一次，或者单击 已安装，在这种情况下，它会恢复使用.ica 文件启动应用程序。用户可以稍后进入高级设置屏幕并单击 验证连接来重试。

Citrix Workspace 启动器可在 Windows 和 macOS 上使用。

ICA 文件下载

在没有 Citrix Workspace 启动器可用的操作系统上，当用户启动应用程序或桌面时，它会下载一个 ICA 文件，用户可以在本地安装的 Citrix Workspace 应用程序中打开该文件。

在 Windows 和 macOS 上，在客户端检测屏幕上，如果用户单击 已安装，则 Citrix Workspace 启动器不用于启动应用程序和桌面。相反，当用户启动应用程序或桌面时，它会下载一个 ICA 文件，用户可以在本地安装的 Citrix Workspace 应用程序中打开该文件。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

活动管理器

April 30, 2025

活动管理器是 Citrix Workspace 中的一项简单而强大的功能，它可帮助用户高效地管理其资源。它可以方便地从任何设备对处于活动状态的应用程序和桌面进行快速操作，从而提高生产效率。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”面板显示应用程序和桌面的合并列表，其中不但包含当前设备上处于活动状态的应用程序和桌面，而且还包含具有活动会话的任何远程设备上处于活动状态的应用程序和桌面。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。

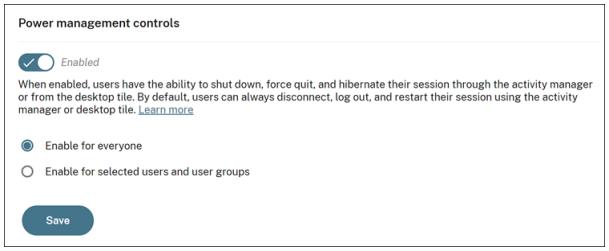
启用活动管理器

活动管理器功能默认启用。

电源管理控制

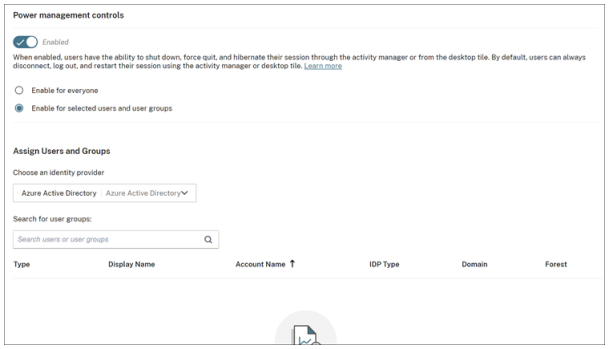
电源管理控制包括 关机、强制关机和 休眠。要使用 Citrix Cloud 启用电源管理控制，请执行以下操作：

1. 导航到 工作区配置 > 自定义 > 功能。
2. 启用切换按钮。
3. 选择 为所有人启用 将设置应用于所有用户。



4. 或者，选择 为选定的用户和用户组启用 将设置应用于选定的用户和用户组。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. 单击向下箭头，然后从下拉列表中选择一个身份提供者。
6. 在 搜索用户组 文本字段中，找到要分配给此功能的用户或组。

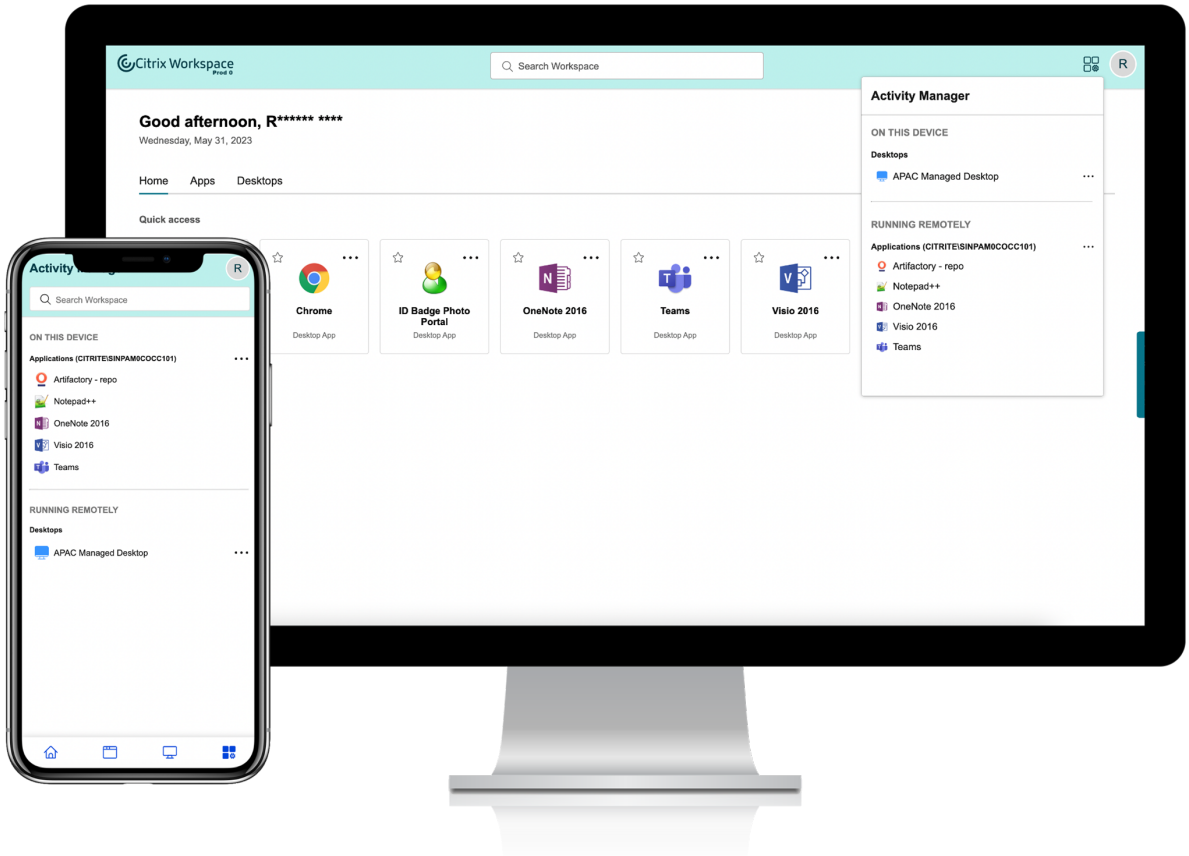
   添加用户或用户组后，您可以在屏幕上看到他们的列表。
7. 单击保存。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



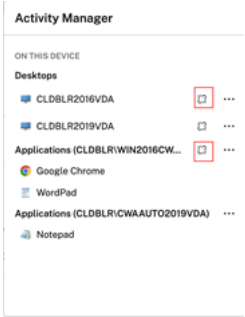
用户可以通过单击相应的省略号 (…) 按钮对应用程序或桌面执行以下操作。

- 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：从当前会话注销。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。
- 关闭：关闭断开连接的桌面。
- 强制退出：出现技术问题时强制关闭您的桌面电源。
- 重新启动：关闭桌面并重新启动。

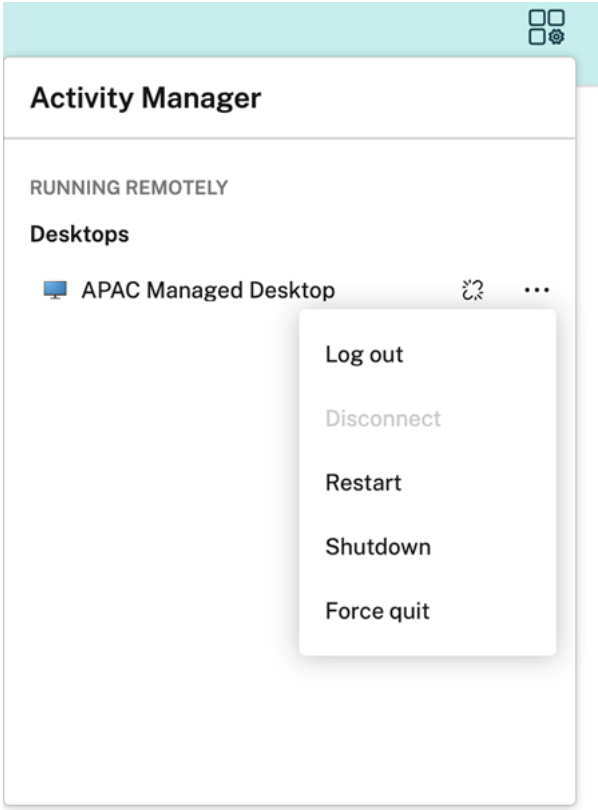
已断开连接的应用程序和桌面

活动管理器现在允许最终用户查看在断开连接模式下运行的本地或远程应用程序和桌面并对其执行操作。可以从移动或桌面设备管理会话，使最终用户能够随时随地执行操作。对断开连接的会话执行操作，例如注销或关闭，可以促进资源的优化使用并降低能耗。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 断开连接的应用程序和桌面显示在“活动管理器”面板上，并由一个断开连接图标予以指示。
- 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。



最终用户可以通过单击省略号按钮对断开连接的桌面执行以下操作：

- 注销：使用此选项可从断开连接的桌面中注销。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。
- 关闭：使用此选项关闭断开连接的桌面。
- 关闭电源：如果出现技术问题，可以使用此选项强制关闭断开连接的桌面电源。
- 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有所不同，如下所述。

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

但是，一旦您关闭并重新打开“活动管理器”，断开连接的会话将被移至正在远程运行下。

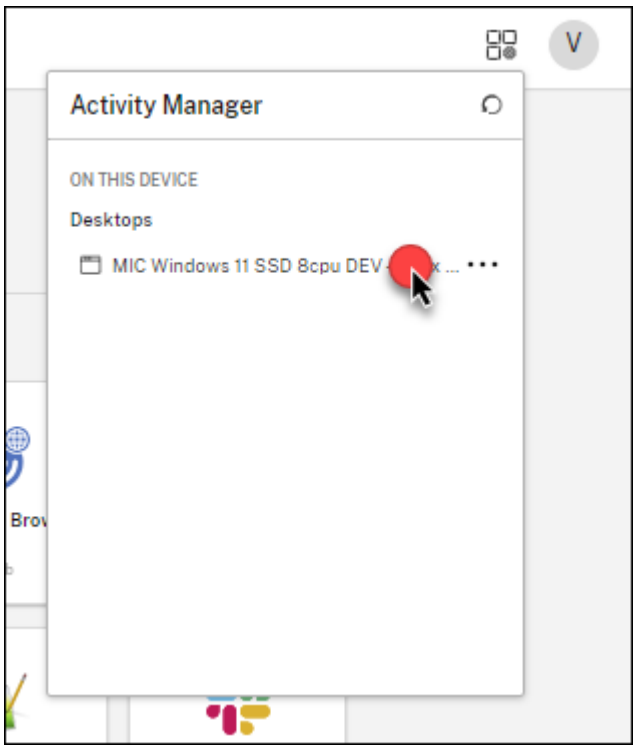
- 如果您通过本机设备登录到 Citrix Workspace 应用程序并断开本地会话的连接，断开连接的会话将从列表中消失。但是，一旦您再次关闭并重新打开“活动管理器”，断开连接的会话将被移至正在远程运行下。

重新连接到断开连接的应用程序和桌面

重新连接功能允许最终用户毫不费力地重新打开已断开连接的应用程序和桌面会话，确保设备之间的平稳过渡而不会丢失进度。此功能可无缝恢复对以前工作环境的访问，无需搜索并重新打开应用程序和桌面。

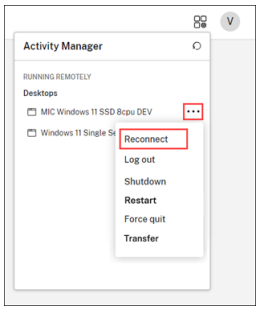
要重新连接到断开连接的应用程序或桌面：

- 打开活动管理器，然后点击资源项。



或

- 单击省略号按钮（…），然后单击 重新连接。



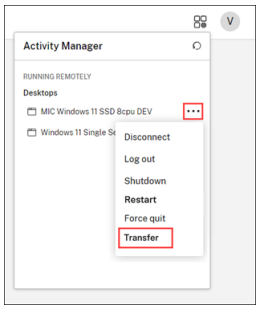
单击 重新连接 可以从您上次中断的地方重新打开断开连接的资源。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

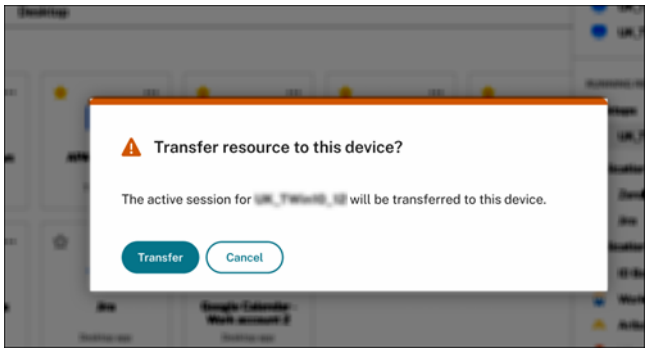
传输您的应用程序和桌面

传输功能允许最终用户将其活动应用程序和桌面从其他设备传输到当前设备。要传输应用程序和桌面，请按照以下步骤操作：

1. 单击省略号按钮（…），然后单击 传输。

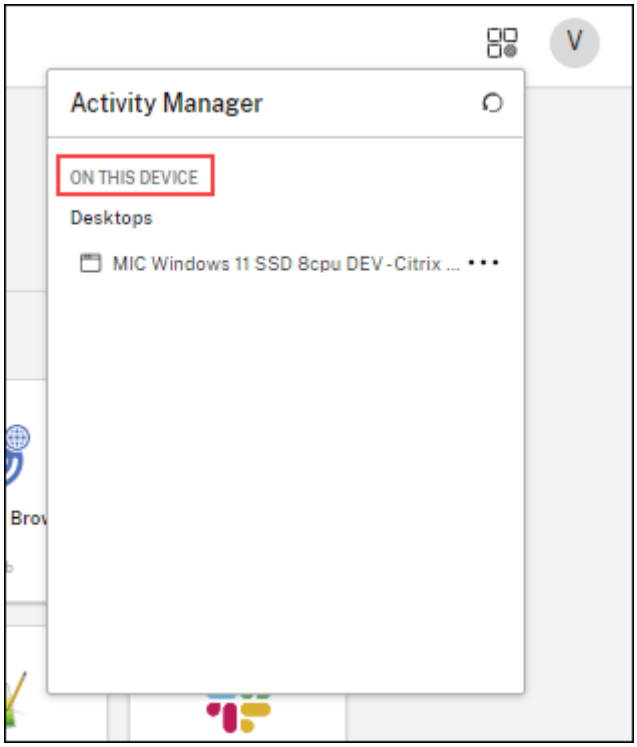


2. 在确认对话框中单击 传输。



一旦资源被转移到当前设备，您就可以在活动管理器的 **ON THIS DEVICE** 部分下看到它们被列出。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



休眠和恢复虚拟桌面会话

休眠和恢复功能允许用户在不使用时休眠虚拟桌面并根据需要无缝恢复，从而优化资源利用率。这不仅节省了成本和能源，而且还通过更快的会话恢复时间增强了用户工作流程。在 Azure 环境中，管理员能够创建完全支持休眠的机器创建服务 (MCS) 机器目录。该功能允许用户暂停虚拟机，并在用户重新连接时无缝恢复到之前的状态，从而优化资源利用率并增强用户体验。

休眠功能对于单会话操作系统机器目录特别有益，无论它们是否持久。启动休眠时，Azure 会与来宾操作系统通信，触发挂起到磁盘的操作。在此过程中，虚拟桌面的内存 (RAM) 内容保留在操作系统磁盘上，而虚拟桌面本身被释放。在后续启动时，虚拟桌面的 RAM 内容将从操作系统磁盘恢复，确保应用程序和进程从上一个状态无缝恢复。

以下部分介绍了管理员如何在用户设备上启用此功能以及用户如何体验它。

> 注意：
>
> 如果用户休眠虚拟桌面超过 60 天，则无法再进行休眠或恢复操作。

配置

仅当管理员启用以下功能时，用户才可以休眠其虚拟桌面会话：

- 用户设备上的 活动管理器，以及
- 虚拟桌面的休眠功能

© 1997–2025 Citrix Systems, Inc. All rights reserved.

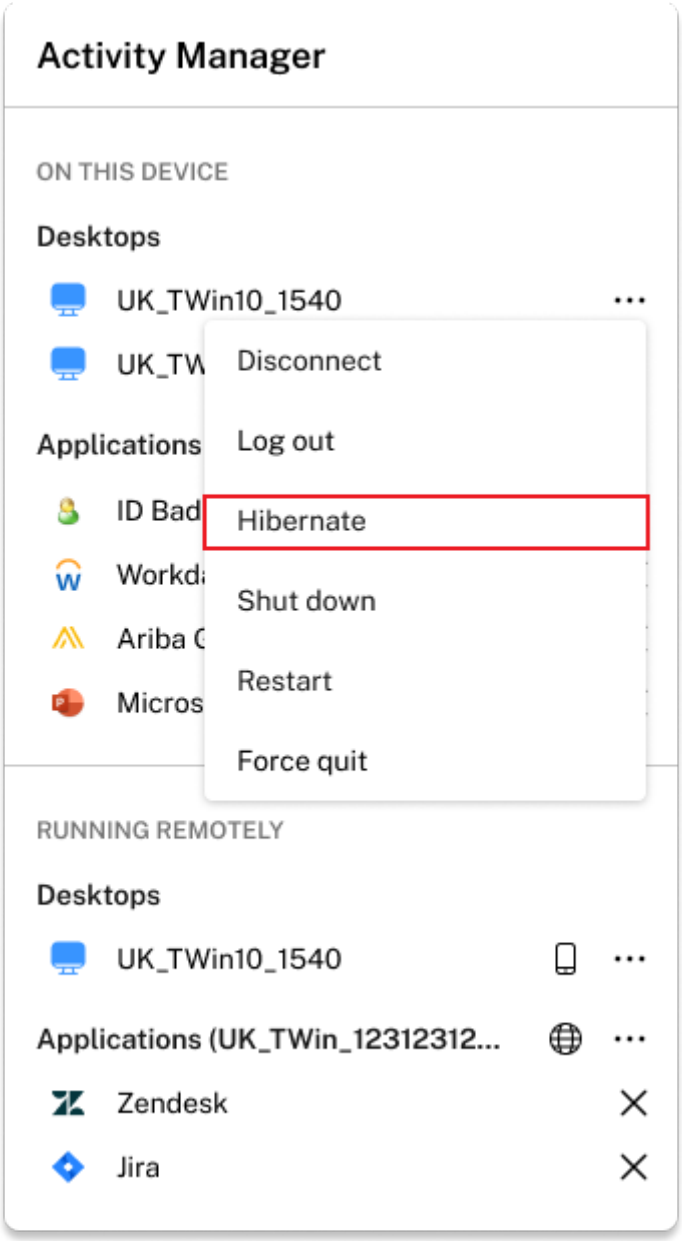
有关启用或禁用活动管理器的更多信息，请参阅 活动管理器。

要启用休眠功能，管理员需要遵循特定的指南并在 Azure 和 Citrix DaaS 中启用预览功能。有关更多信息，请参阅 创建具有休眠功能的虚拟机（预览版）。

用户体验

当管理员启用 活动管理器 和虚拟桌面的休眠功能时，用户可以在 活动管理器 菜单上看到 休眠 选项。

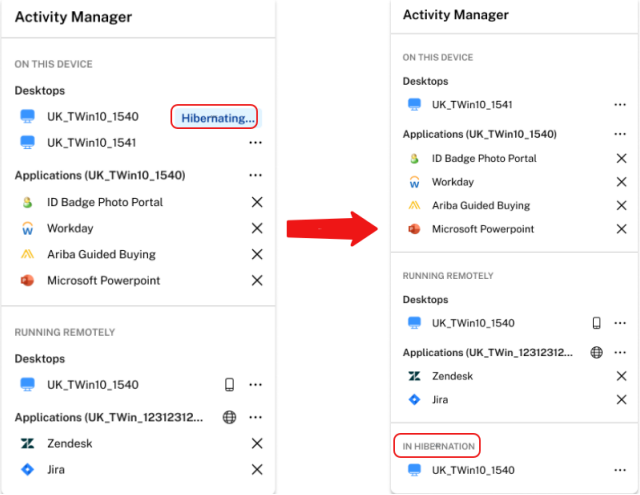
休眠桌面会话：



要休眠桌面会话，用户可以单击三个点按钮（…），然后单击 休眠 选项。一旦用户点击 休眠 选项，桌面就会启动休眠模

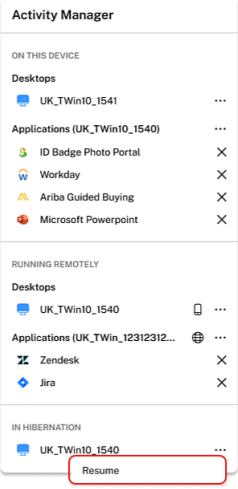
© 1997–2025 Citrix Systems, Inc. All rights reserved.

式。一旦桌面进入休眠状态，桌面资源就会移动到 活动管理器上的 休眠 部分。



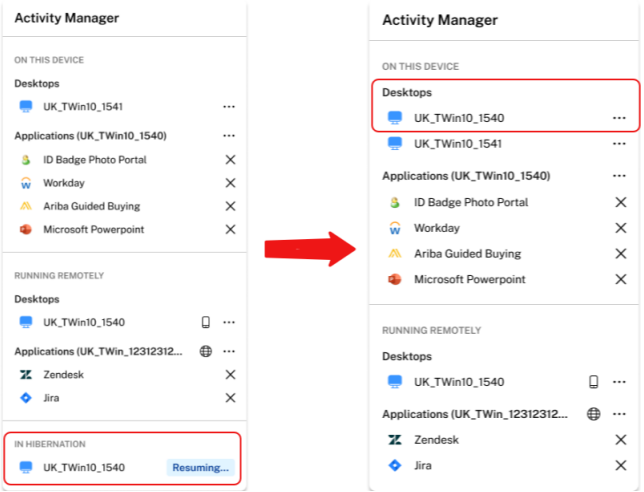
恢复休眠的桌面会话：

休眠桌面会话可在 休眠 部分下的 活动管理器中找到。要恢复休眠的桌面会话，用户可以单击三个点按钮（…），然后单击 恢复 选项。



一旦用户点击 恢复 选项，桌面就会恢复。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Citrix Workspace Web 扩展

May 13, 2025

Citrix Workspace Web 扩展在 Citrix Workspace Web 客户端和本地安装的 Citrix Workspace 应用程序之间建立安全可靠的连接。它简化了从 Web 客户端到使用 HDX 协议的本机应用程序和桌面的打开。在浏览器上安装此扩展程序后，当您访问 Web 客户端并打开任何应用程序或桌面时，此扩展程序会从您的本机 Citrix Workspace 应用程序打开应用程序或桌面。

网络扩展提供了各种好处，例如无缝打开桌面和应用程序、服务连续性、支持应用程序保护服务等。有关 Web 扩展的优势的更多信息，请参阅 Citrix Workspace Web 扩展的优势。

> 注意：
>
> 用户需要在其设备上本地安装 Citrix Workspace 应用程序客户端才能使此扩展程序正常运行。要下载 Citrix Workspace 应用程序，请访问 Citrix 下载 页面。

Citrix Workspace Web 扩展在 Google Chrome、Microsoft Edge 和 Apple Safari 浏览器上受支持。该扩展程序同时适用于云应用商店和本地应用商店。

有关安装 Web 扩展的更多信息，请参阅 StoreFront 上的 Citrix Workspace Web 扩展。

支持的浏览器

浏览器名称	操作系统	浏览器版本
Google Chrome	Windows、macOS、Linux	最新的

© 1997–2025 Citrix Systems, Inc. All rights reserved.

浏览器名称	操作系统	浏览器版本
Microsoft Edge	Windows、macOS、Linux	最新的

支持的 **Citrix Workspace** 和 **StoreFront** 版本

Citrix Workspace Web 扩展始终可与 Citrix Workspace 一起使用，无需任何额外配置。

要将 Citrix Workspace Web 扩展与 StoreFront 一起使用，需要 StoreFront 2203 CU2 或更高版本。

- 对于 2402 之前的 StoreFront 版本，Citrix Workspace Web 扩展默认处于禁用状态，您必须手动启用它。
- 对于 StoreFront 版本 2402，Citrix Workspace Web 扩展在新部署中默认启用，但从以前的版本升级时必须手动启用它。
- 对于 StoreFront 2407 及更高版本，Citrix Workspace Web 扩展默认启用，因此您无需进行任何配置。

有关在 StoreFront 中启用 Citrix Workspace Web 扩展的详细信息，请参阅 StoreFront 上的 Citrix Workspace Web 扩展。

Citrix Workspace Web 扩展的优势

Web 扩展程序增强了混合部署的可靠性和安全性。它附带以下内置功能。

无缝打开桌面和应用程序

通常情况下，Citrix Workspace Web 客户端使用 Citrix Workspace Launcher 来检测本地安装的 Citrix Workspace 应用程序并在内存中打开应用程序。但是，根据浏览器的不同，用户可能需要在每次启动时单击弹出窗口。Workspace Web 扩展允许 Web 客户端无缝打开桌面和应用程序，而不会弹出浏览器窗口。Citrix Workspace Web 客户端可以利用扩展的功能在本机 Citrix Workspace 应用程序中打开应用程序和桌面，而无需通过客户端检测验证 Citrix Workspace 应用程序是否在本地安装。这为用户在绕过客户端检测步骤时打开应用程序或桌面提供了更顺畅的体验。

更可靠地启动 **StoreFront GSLB** 部署

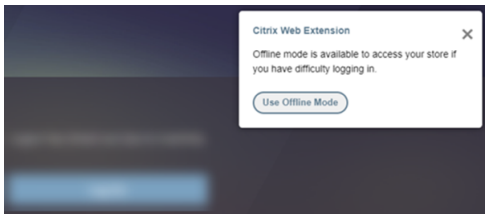
在全局服务器负载均衡器 (GSLB) 后面使用多个 StoreFront 部署时，响应可能会被定向到错误的服务器，导致无法打开应用程序和桌面。这可以通过 GSLB 配置来缓解，但是配置起来很复杂。Citrix Workspace Web 扩展允许可靠的客户端检测和应用程序和桌面的打开，而无需针对 GSLB 部署进行特殊配置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Workspace 的服务连续性

如果用户无法登录其 Workspace，服务连续性将使其能够在脱机模式下打开资源。有关详细信息，请参阅服务连续性。

访问 Workspace Web 客户端时，用户必须安装 Citrix Workspace Web 扩展才能实现服务连续性。在初始登录期间，该扩展程序将存储连接租约。随后，如果 60 秒后登录失败，Web 扩展程序将显示使用离线模式的提示。



用户可以在不丢失数据的情况下继续工作，从而提高工作效率。一旦连接恢复，用户可以单击 重新连接到工作区 切换到在线模式。

> 注意：
>
> 此功能仅在使用 Workspace 时适用，而不是 StoreFront 时。
>
> 此新的离线模式提示仅适用于 Chrome 和 Edge 浏览器。对于 Safari 浏览器，旧提示保持不变。

面向 **Workspace** 的 **App Protection**

使用 Workspace 时，Web 扩展程序允许用户查看和打开启用了 App Protection 的应用程序。此功能通过保护用户免受键盘记录、屏幕捕获和其他安全威胁的侵害，防止未经授权访问应用程序中的敏感信息。

有关详细信息，请参阅 App Protection。

> 注意：
>
> 与 Workspace 不同，StoreFront 不需要 Workspace Web 扩展来进行应用程序保护。有关详细信息，请参阅 StoreFront 文档。

安装 **Citrix Workspace Web** 扩展

有关安装 Web 扩展的更多信息，请参阅 Citrix Workspace Web 扩展。

参考文章

- StoreFront 上的 Citrix Workspace Web 扩展程序
- Citrix Workspace 产品文档
- Citrix Workspace 应用程序产品文档
- 支持 Citrix Enterprise Browser 上的浏览器扩展程序

© 1997–2025 Citrix Systems, Inc. All rights reserved.

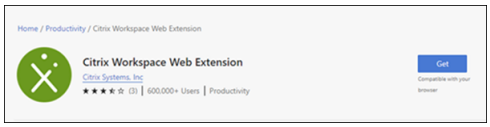
- 通过 Citrix Workspace 浏览器扩展程序安全、可靠地访问 Citrix Workspace
- 服务连续性 - 采用 DaaS 部署的 Citrix Workspace

安装 Citrix Workspace Web 扩展

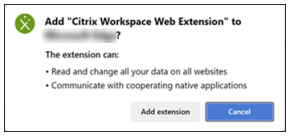
November 7, 2024

管理员和最终用户可以根据以下说明将扩展程序添加到用户设备中。

1. 从首选浏览器的 Web 应用商店下载 Citrix Workspace Web 扩展程序。
   - Chrome 网上应用店
   - Microsoft Edge 加载项
   - Mac 应用商店
2. 从您喜欢的浏览器应用商店添加扩展程序。

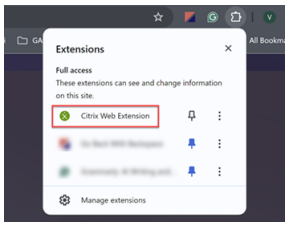


3. 确认弹出消息以将扩展程序添加到浏览器。

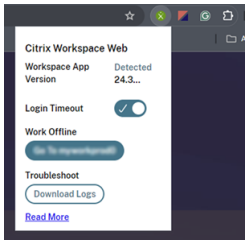


一旦添加扩展，您就可以看到工具栏上的 扩展 按钮下显示的扩展图标。仅当用户访问 Web 客户端时，该扩展程序才会被激活。否则，它将保持非活动状态。

（推荐）为了便于访问，您甚至可以根据浏览器设置固定扩展程序。



该扩展程序会自动检测 Citrix Workspace 应用程序是否已本地安装在您的设备上，并显示应用程序版本。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

登录超时：通过浏览器中的 Citrix Workspace Web 扩展管理离线模式提示。要关闭离线模式提示，请单击扩展图标并禁用切换按钮。

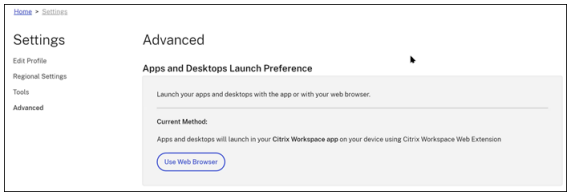
离线工作：手动切换到离线模式，无需等待 60 秒的离线模式提示。当 登录超时 被禁用时，此选项也很有用。

故障排除：当出现任何问题时，您可以使用 下载日志 选项收集错误日志。

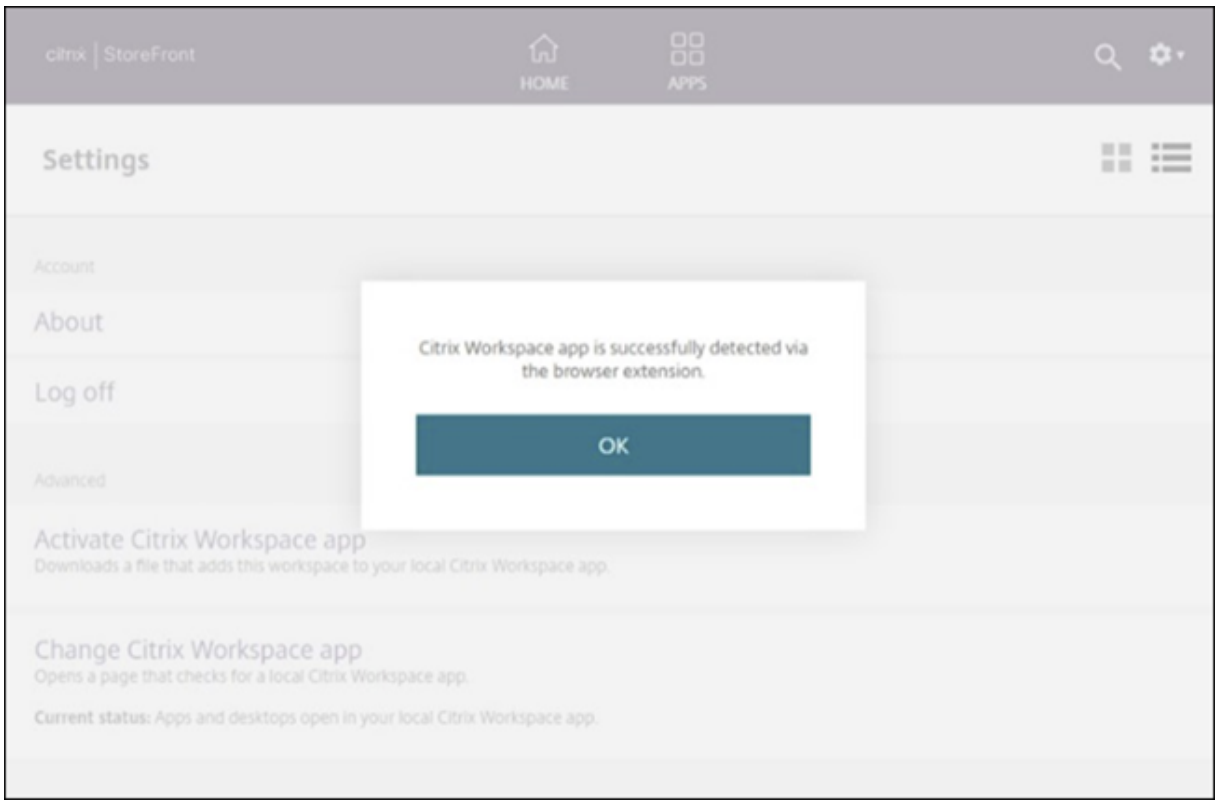
阅读更多：单击此链接了解有关服务连续性功能的更多信息。

添加 Web 扩展后，您可以验证它是否已激活并在本机应用程序上打开应用程序和桌面。您可以通过导航至 设置 > 高级来验证。

如果您使用的是下一代 UI，设置 屏幕会显示消息 应用程序和桌面将使用 **Citrix Workspace Web** 扩展在您设备上的 Citrix Workspace 应用程序中启动。



如果您正在使用具有统一 UI 的本地 StoreFront，请单击 更改 **Citrix Workspace** 应用程序。如果检测到 Web 扩展，则会显示消息 **Citrix Workspace** 应用程序已通过浏览器扩展成功检测到。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

在托管设备上部署 **Web** 扩展程序

如果设备由组织管理，管理员必须使用组策略对象 (GPO) 将扩展程序安装在用户的设备上。

根据浏览器和操作系统的不同，您可以自动将 Citrix Workspace Web 扩展程序部署到您管理的设备上。

- 要部署 Microsoft Edge 扩展，请参阅 使用组策略管理 Microsoft Edge 扩展。
- 要使用组策略部署 Google Chrome 扩展程序，请参阅 Set Chrome app and extension policies (Windows)（设置 Chrome 应用程序和扩展程序策略 (Windows)）。
- 要使用 Google 管理控制台部署 Chrome 扩展程序，请参阅 Automatically install apps and extensions（自动安装应用程序和扩展程序）。

> 注意：
>
> - 要在 Citrix Enterprise Browser 上添加扩展，管理员需要将该扩展添加到允许列表中。有关详细信息，请参阅 Citrix Enterprise Browser 文档中的支持浏览器扩展程序。
> - 默认情况下，Citrix Workspace Web 扩展会在每次新版本发布时自动更新。

工作区离线模式提示

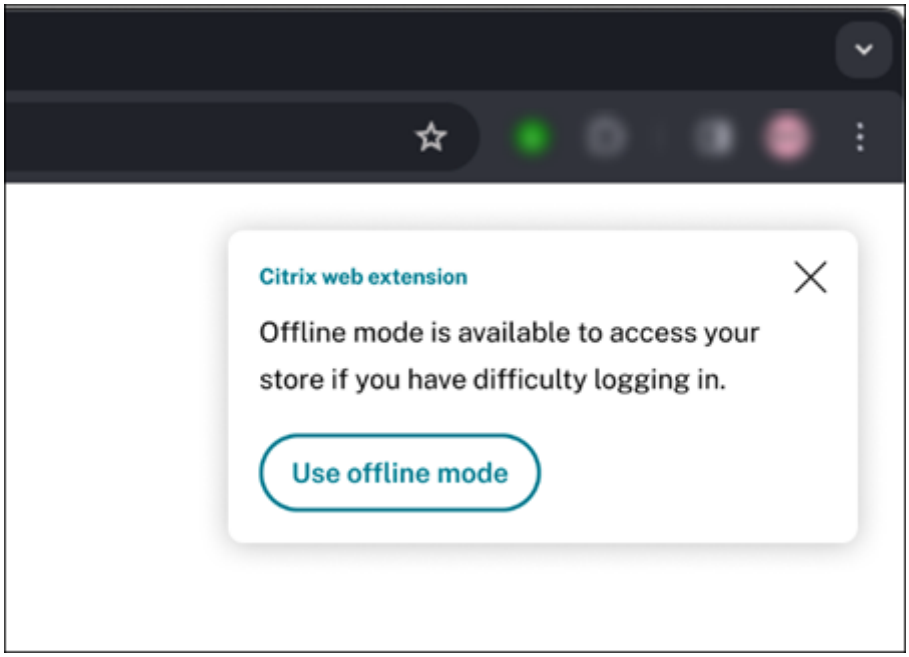
November 7, 2024

新的提示在以下方面带来了增强：改进的设计、增强的行为和加载时间。

设计

新的提示现在以弹出窗口的形式出现在屏幕上。以前，提示会以新页面的形式出现，要求用户重新启动身份验证或离线工作。但是，新的弹出窗口设计不需要用户强制响应。如果用户遇到任何连接问题，它为用户提供了选择离线模式的选项。新的提示不那么具有侵扰性，并允许用户继续正在进行的身份验证过程。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



此外，新的提示是可移动的，允许用户将其拖动到屏幕上的任何位置以查看其后面的内容。

行为和加载时间

离线模式提示的行为和加载时间得到了显著增强。

旧行为：以前，提示会在用户在浏览器中输入商店 URL 后 30 秒内出现。有时，用户可能需要一些额外的时间才能登录 Workspace 商店，例如等待推送通知、输入双因素身份验证码、网页加载时间等。如果由于这些原因，用户身份验证超过了 30 秒的阈值，则会出现提示，中断身份验证过程。

用户对提示的响应是强制性的，并且只留下两个选项：切换到离线模式或重试身份验证过程。选择重试选项需要用户重新启动整个过程，并且一旦提示窗口出现，他们就无法继续正在进行的身份验证过程。

新行为：增强的离线提示干扰性较小，因为它不会中断正在进行的用户身份验证。如果用户遇到任何连接问题，则可以选择继续身份验证过程或使用离线模式。

离线模式提示现在仅在 60 秒后出现在网页上，而不会中断正在进行的用户身份验证过程。由于某些原因，如果 IdP 域未能响应，浏览器将不会加载任何页面。在这种情况下，会出现一个离线模式对话框，而不是通常的弹出提示。

配置对工作区的访问权限

January 7, 2025

首次启用 Workspace 时，会创建一个默认的 cloud.com Workspace URL，以允许用户从其本地安装的 Citrix Workspace 应用程序或 Web 浏览器访问 Workspace。您可以自定义此 URL 或添加其他 URL。有关更多信息，请

© 1997–2025 Citrix Systems, Inc. All rights reserved.

参阅本文中的 工作区 URL 。

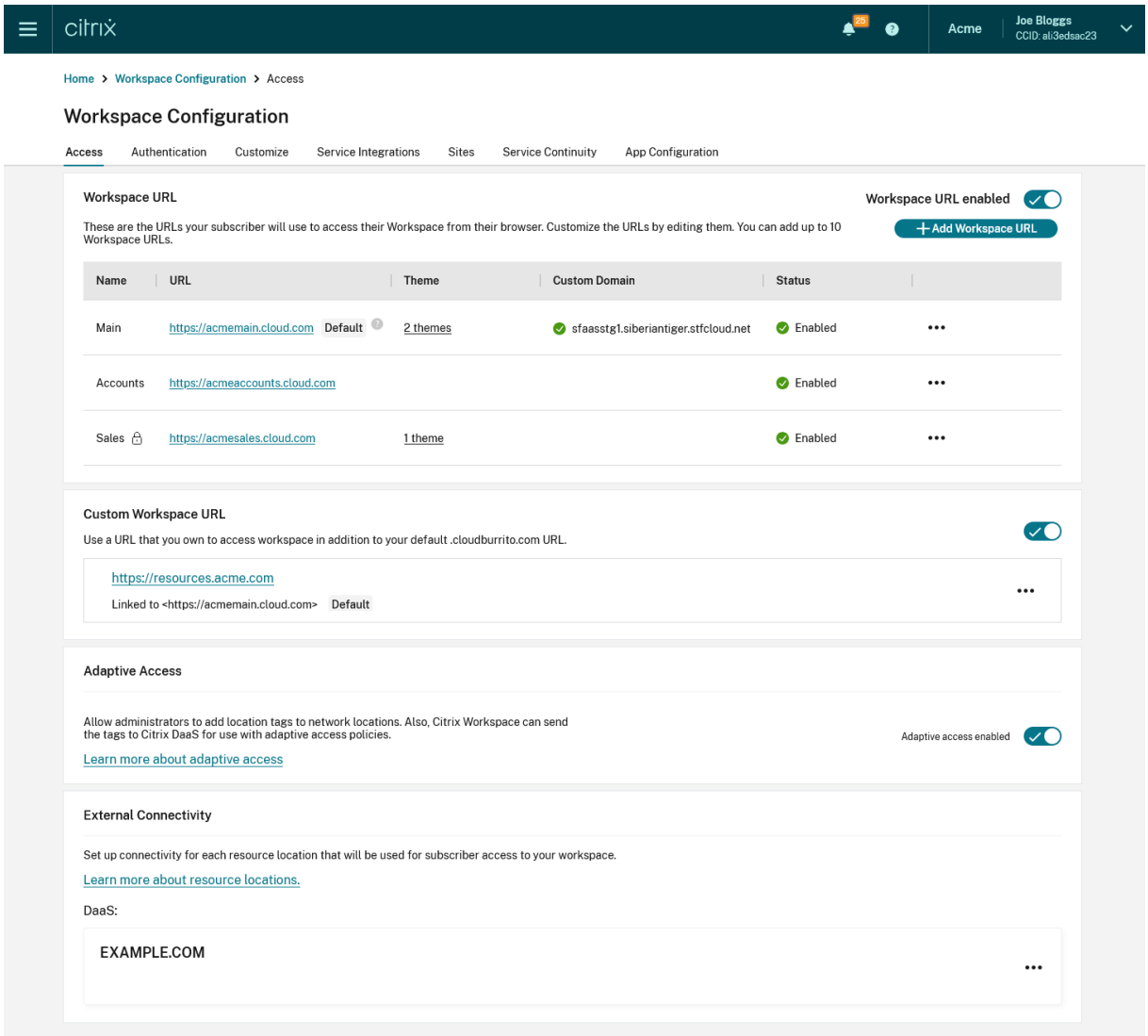
有关用户如何连接到 Citrix Workspace 的信息，请参阅 用户访问选项。

要配置用户如何向 Workspace 进行身份验证，请参阅 配置身份验证。

当用户启动资源时，用户的设备必须能够到达虚拟交付代理 (VDA)。对于内部用户，端点必须直接连接到虚拟交付代理 (VDA) 的 IP 地址。如果您配置与 Citrix Gateway 或 Citrix Gateway 服务的外部连接，远程用户就可以获得对其资源的外部访问权限。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 。

要配置访问设置：

1. 转到 Citrix Cloud 并使用您的凭据登录。
2. 导航到 工作区配置 > 访问。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

Workspace URL

要配置最终用户用于访问其工作区的 cloud.com URL，请参阅 配置工作区 URL。

自定义域

除了 cloud.com 工作区 URL 之外，您还可以使用自己的自定义域代替默认工作区 URL。有关更多信息，请参阅 配置自定义域。

自适应访问

自适应访问功能使管理员能够根据上下文为用户提供可访问的应用程序的细粒度访问权限。有关更多信息，请参阅 自适应访问。

启用自适应访问

1. 转到 访问 选项卡
2. 转到部分 自适应访问 并单击切换按钮。此时将显示确认屏幕。
3. 按 启用。

要禁用自适应访问：

1. 转到 访问 选项卡
2. 转到部分 自适应访问 并单击切换按钮。此时将显示确认屏幕。
3. 按 禁用。

外部连接

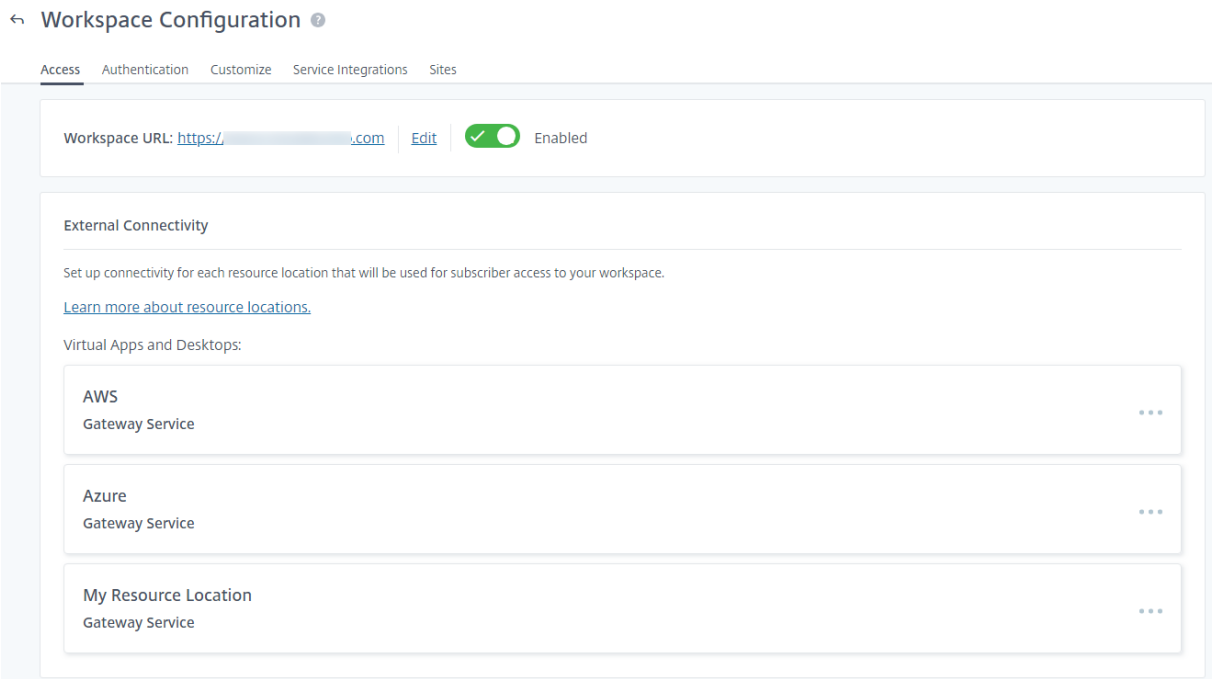
通过将 Citrix Gateway 或 Citrix Gateway 服务添加到资源位置，为远程订阅者提供安全访问。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> 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。

配置自定义域

May 13, 2025

您可以允许用户使用自定义域名或 `cloud.com` 域名访问他们的商店。您必须拥有该域名，并且每个域名只能用于访问单个商店。

每个帐户可以有一个链接到主商店的自定义域。如果您有其他商店，则只能使用其“cloud.com”URL 进行访问。

支持的场景

方案	受支持	不支持
身份提供商	AD (+Token)、Microsoft Entra ID、Citrix Gateway、Okta 和 SAML	Google

© 1997–2025 Citrix Systems, Inc. All rights reserved.

方案	受支持	不支持
资源类型	Virtual Apps and Desktops	Web 应用程序、SaaS 应用程序和已发布内容
访问方法	浏览器、Citrix Workspace 应用程序	-

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)。
- 建议您使用专用域作为 Citrix Workspace 访问的自定义域。如果有必要，它可以帮助您轻松更改域名。
- 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共 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。

- 域名长度不得超过 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。

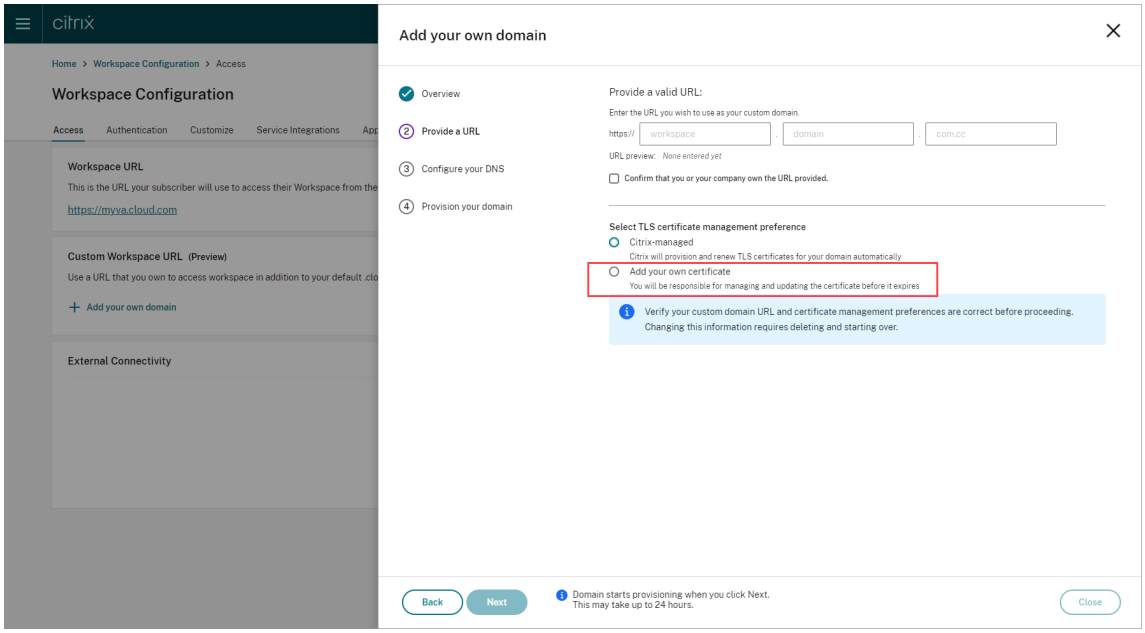
如果您使用 SAML 连接到身份提供商，则需要执行额外的步骤才能完成 SAML 配置。有关更多信息，请参阅 SAML。

> 注意：
>
> 添加自定义 URL 和配置 SAML 时，Citrix Cloud 需要 24 小时进行配置。

添加自定义域

1. 登录 Citrix Cloud。
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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



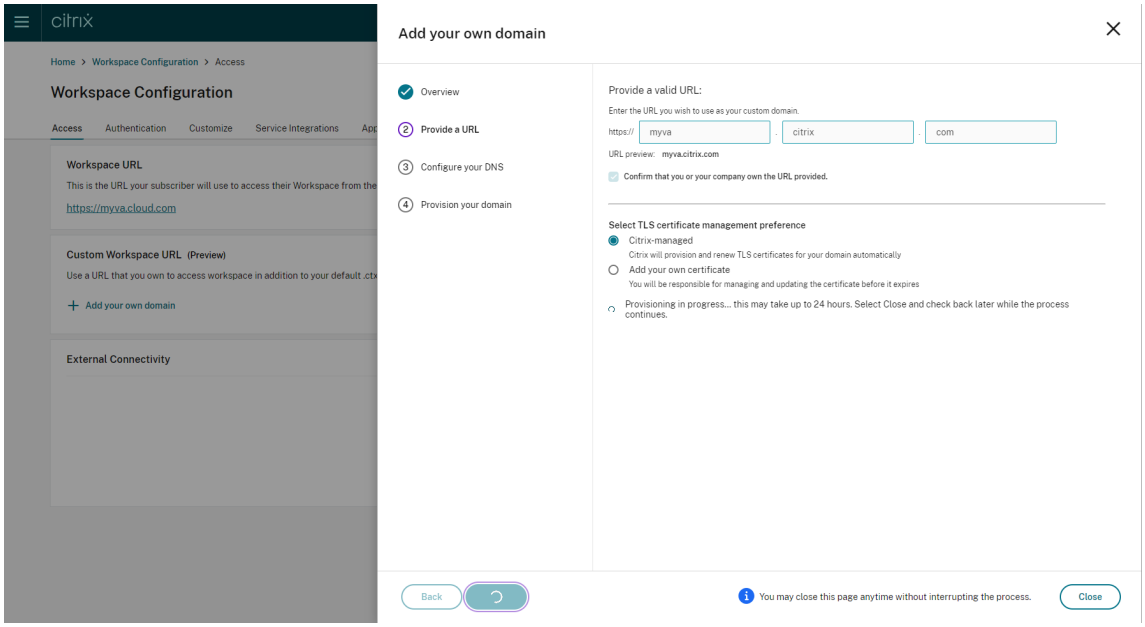
4. 阅读 概述 页面上显示的信息，然后选择 下一步。

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。建议选择 管理，因为证书更新由系统为您处理。有关更多信息，请参阅提供续订证书。在“等效 **CLI** 命令”中，查看命令并单击“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。

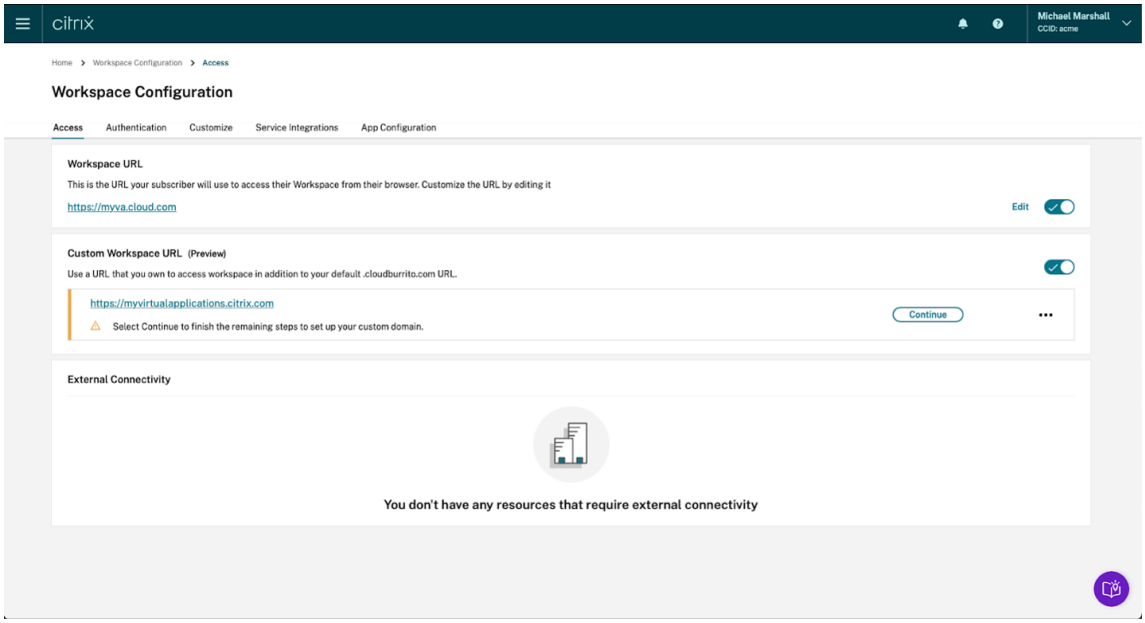
   预配您选择的域需要一些时间。您可以等待页面处于打开状态，也可以在配置进行时将其关闭。



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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

问”选项卡中为您的自定义域选择“继续”按钮。

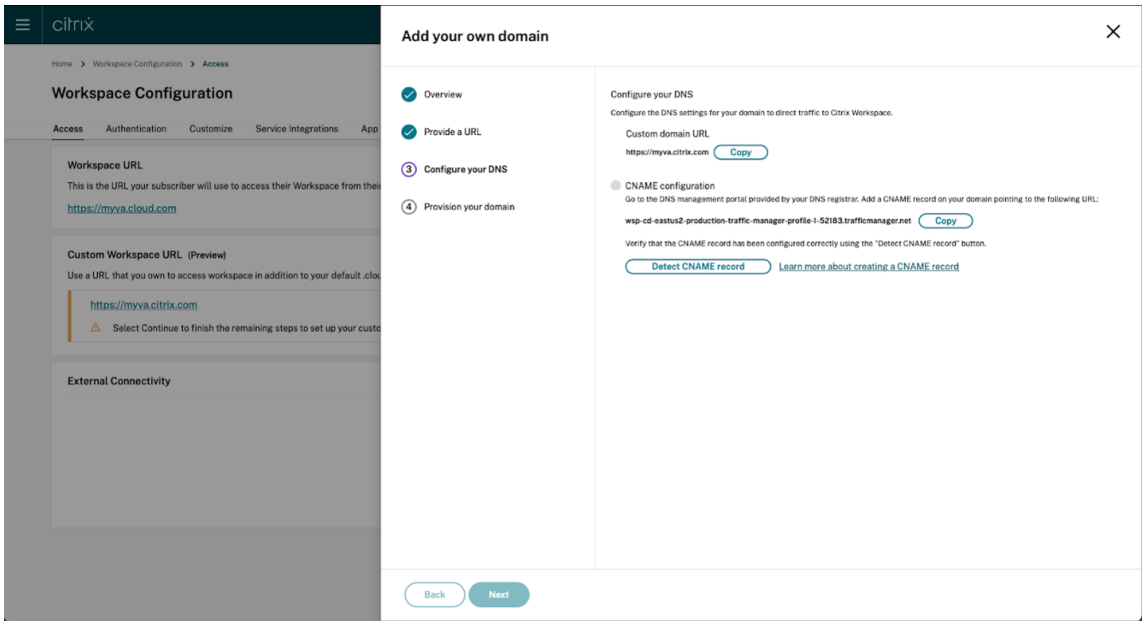


7. 在您的 DNS 注册商提供的管理门户中执行此步骤。为您选择的自定义域添加一个 **CNAME** 记录，该记录指向分配给您的 Azure 流量管理器。

   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”*



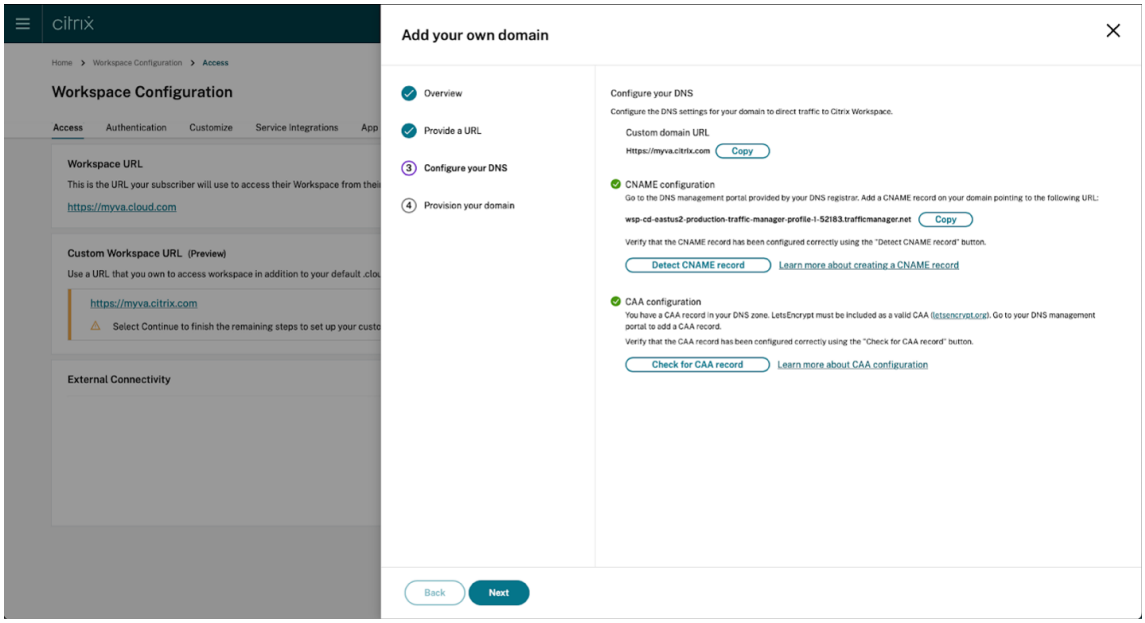
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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”。



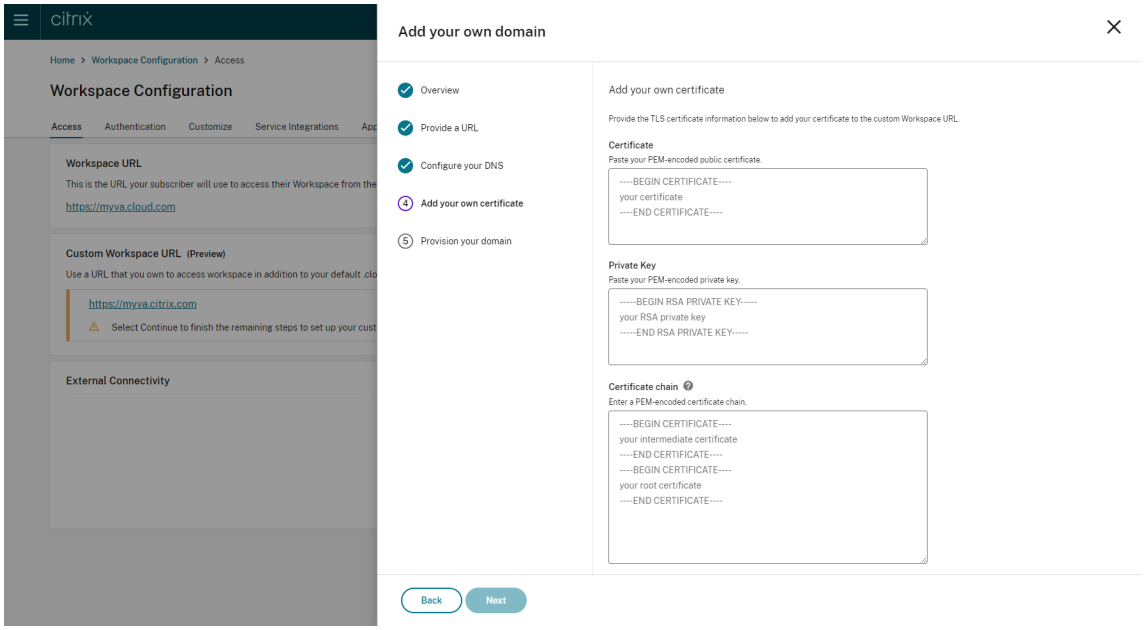
9. 这是一个可选步骤。如果您选择添加自己的证书，请在添加自己的证书页面上填写所需信息。

   > 注意：
   >
   > 不支持受密码保护的证书。

   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。

   - 它必须是 PEM 编码的。
   - 它必须至少在接下来的 30 天内保持有效。
   - 它必须专门用于自定义工作区 URL。不接受通配符证书。
   - 证书的通用名称必须与自定义域相匹配。
   - 证书上的 SAN 必须用于自定义域。不允许使用额外的 SAN。
   - 该证书的有效期不得超过 10 年。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> 注意：
>
> 建议您使用采用安全加密哈希函数（SHA 256 或 > 更高）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 提供更新的证书 部分。

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

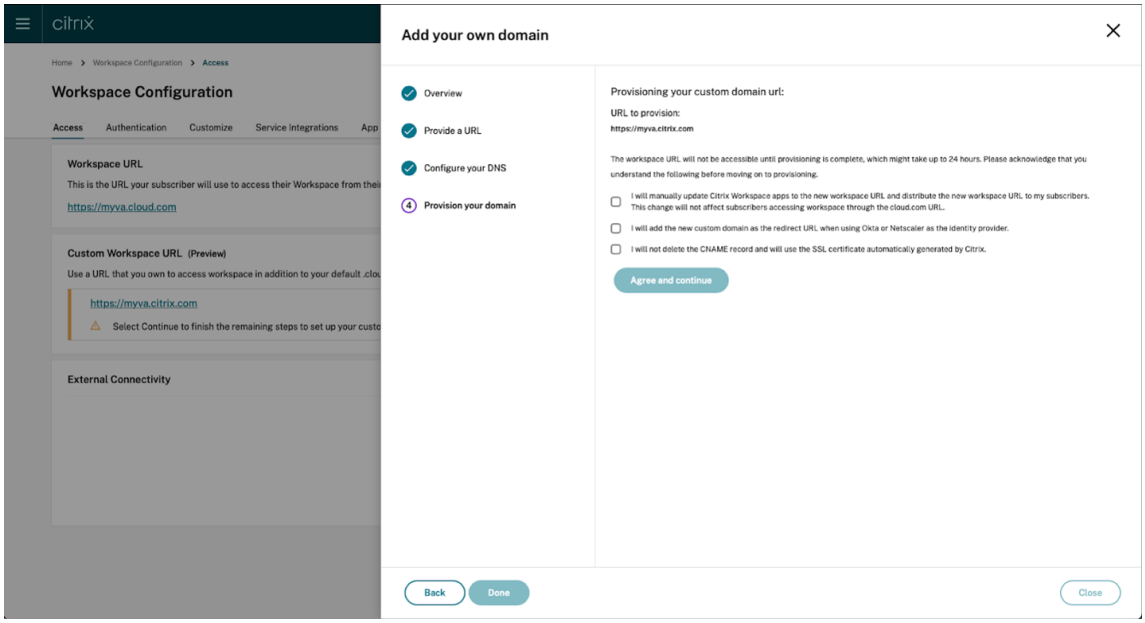
    在身份提供商中配置应用程序时，请使用以下详细信息：

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`
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 **Provision your domain** 页面上显示的信息并确认给出的说明。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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



删除自定义域

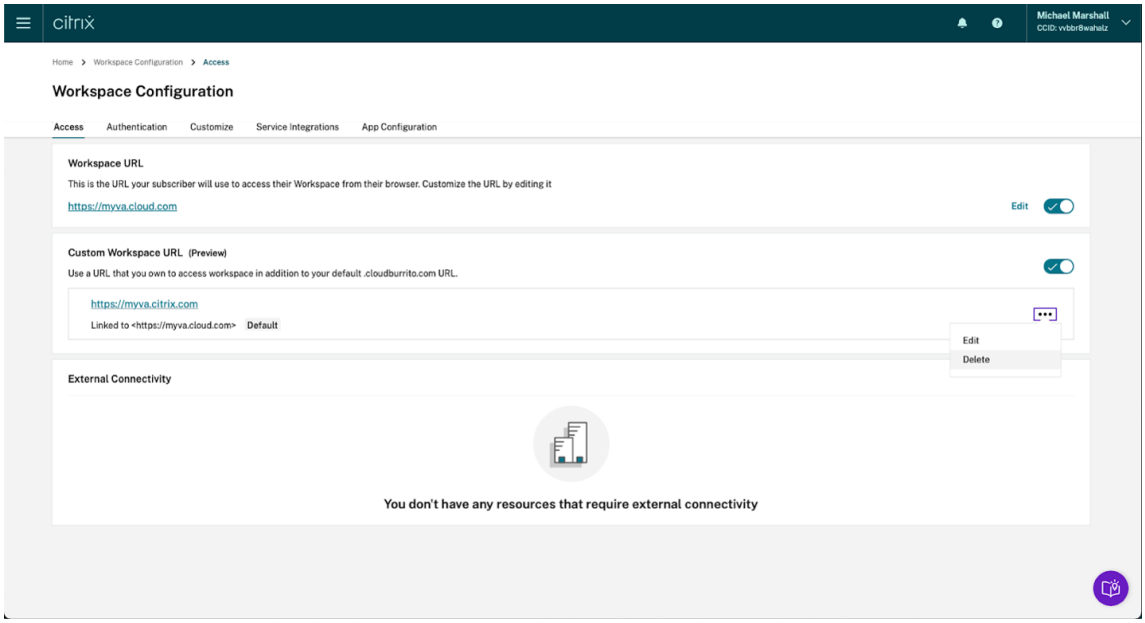
从客户那里删除自定义域将无法使用自定义域访问 Citrix Workspace。删除自定义域后，您只能使用 cloud.com 地址访问 Citrix Workspace。

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，

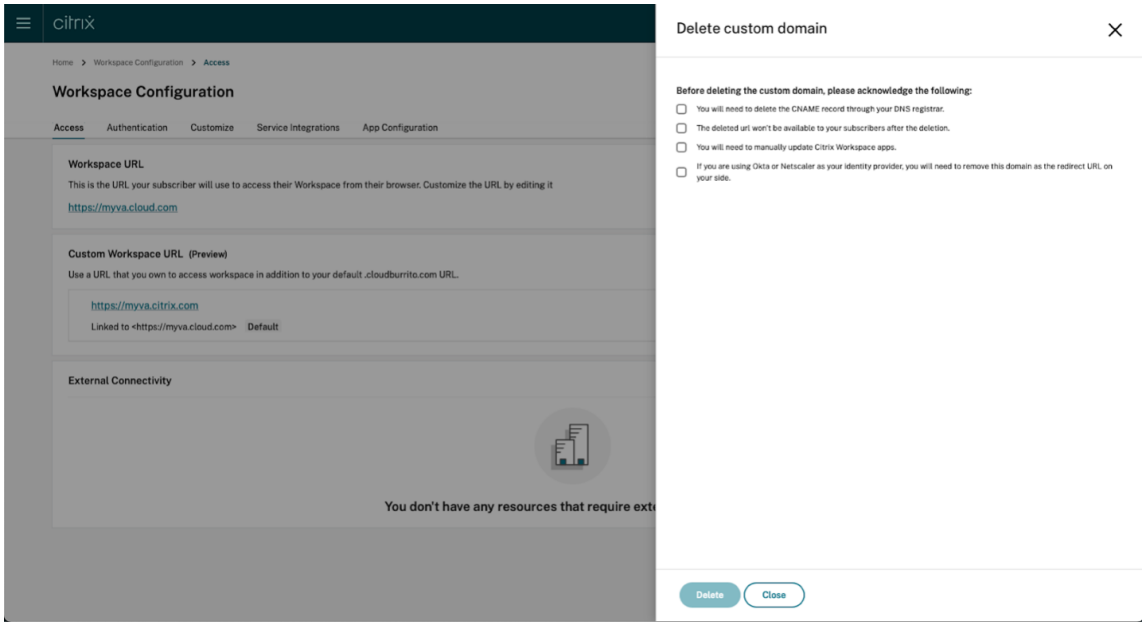
1. 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **Workspace** 配置 **>** 访问权限。
3. 展开上下文菜单 **(…)** 在“访问”选项卡上为自定义域，然后选择“删除”。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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

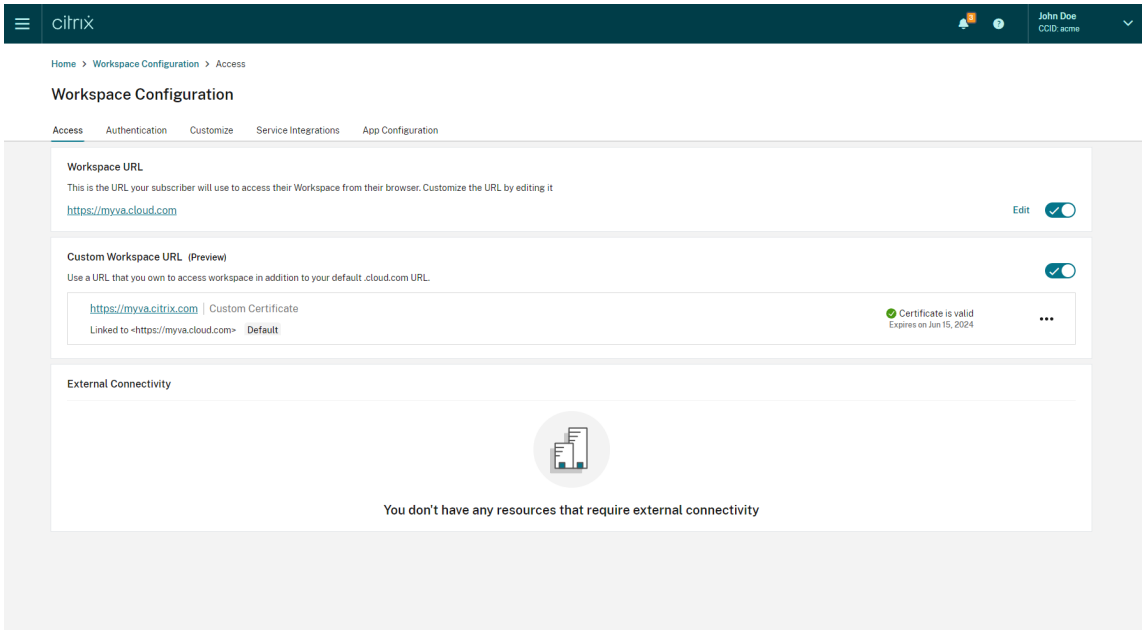
   删除自定义域需要一些时间才能完成。您可以在操作完成时等待页面处于打开状态，也可以关闭页面。



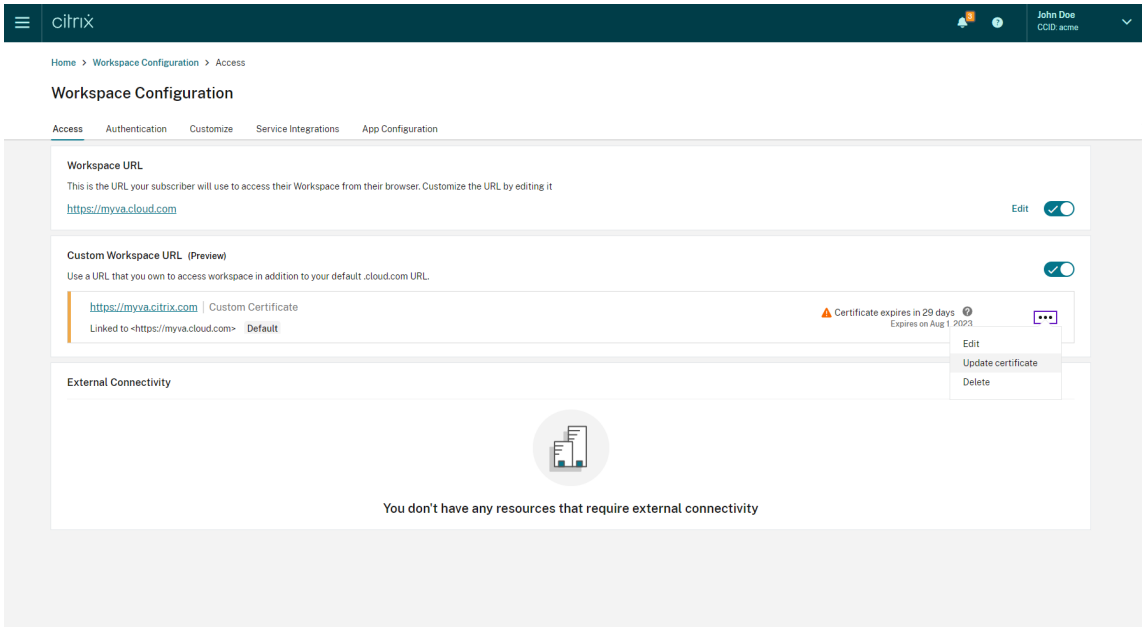
提供续订证书

1. 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **Workspace** 配置 > 访问权限。
3. 证书的到期日期与其分配到的自定义域一起显示。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

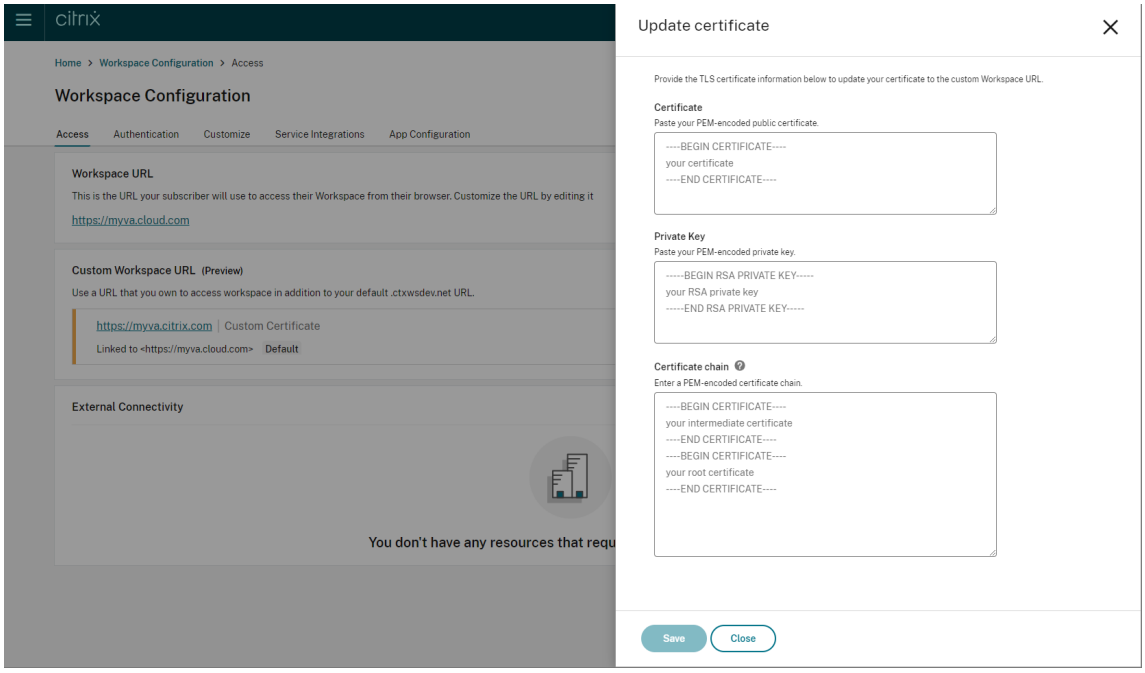


当您的证书即将在 30 天或更短时间内到期时，您的自定义域会显示警告。



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”。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。有关更多信息，请参阅 添加自定义域。

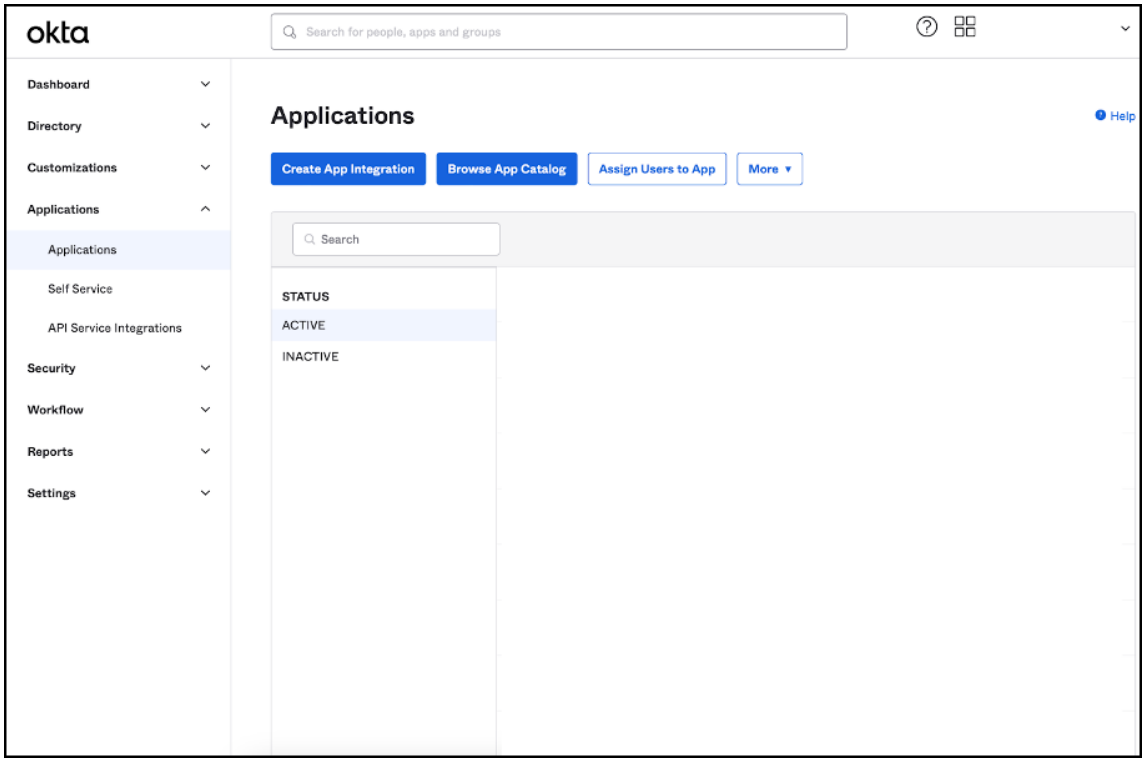
配置您的身份提供商

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。

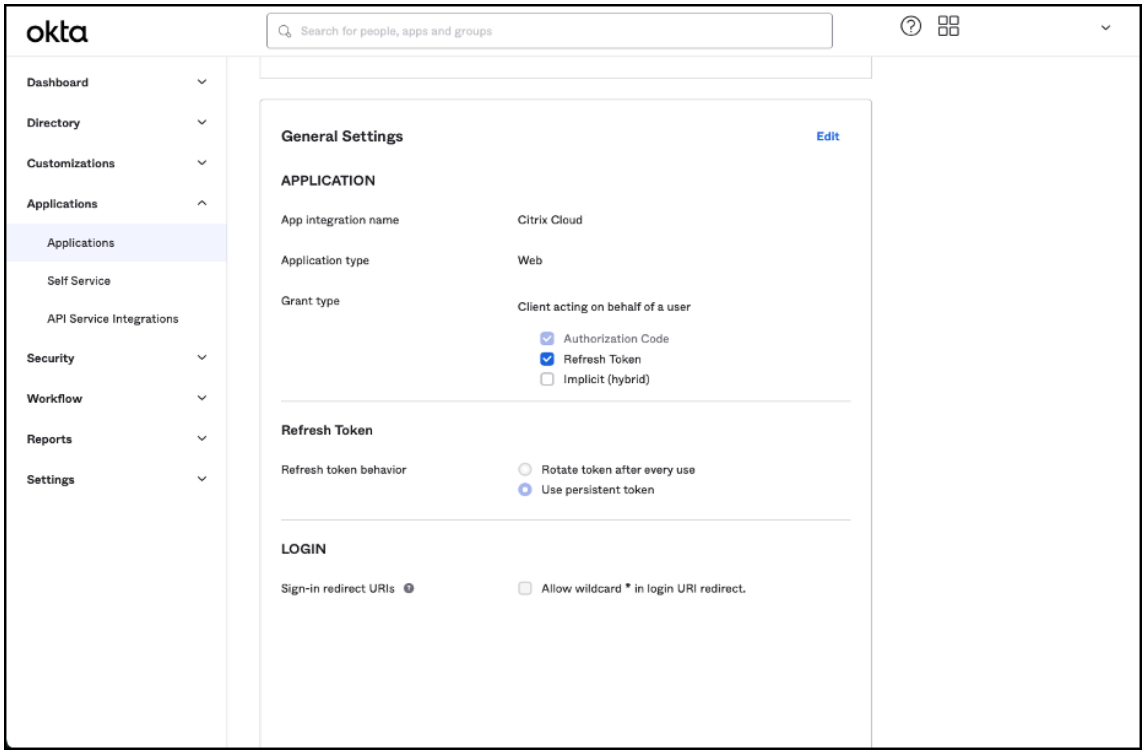
1. 登录您的 Okta 实例的管理员门户。此实例包含 Citrix Cloud 使用的应用程序。
2. 展开 应用程序，然后在菜单中选择 应用程序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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”。

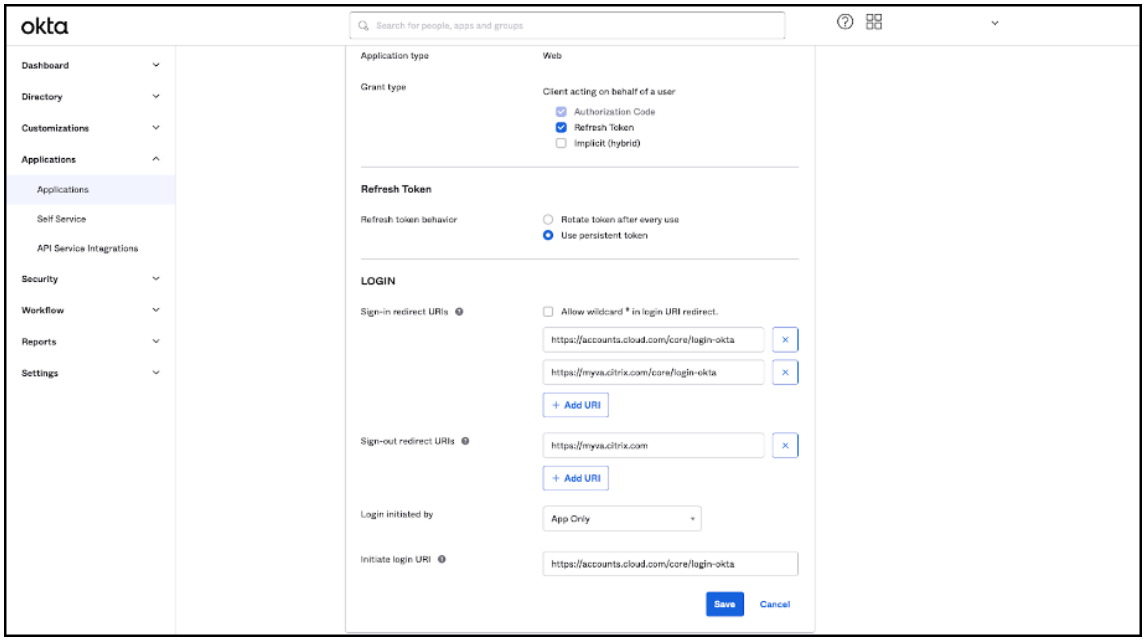


5. 在 常规设置的 **LOGIN** 部分中，为 登录重定向 **URI** 添加一个值。添加新值而不替换任何现有值。新值必须采用

© 1997–2025 Citrix Systems, Inc. All rights reserved.

以下格式：<https://your.company.com/core/login-okta>

6. 在同一节中为 注销重定向 **URI** 添加另一个值。添加新值而不替换任何现有值。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。

> 注意：
>
> 要使用自定义域配置 SAML，请按照 SAML 配置中提到的步骤进行操作。

配置 **OAuth** 策略和配置文件

> 重要
>
> 仅当 OAuth 凭据丢失时，才必须更新将 Citrix Cloud 和 Citrix Gateway 或自适应身份验证 HA 对链接在一起的现有 OAuth 策略和配置文件。更改此策略可能会破坏 Citrix Cloud 与 Workspaces 之间的链接，并影响您登录 Workspaces 的能力。

配置 **Citrix Gateway**

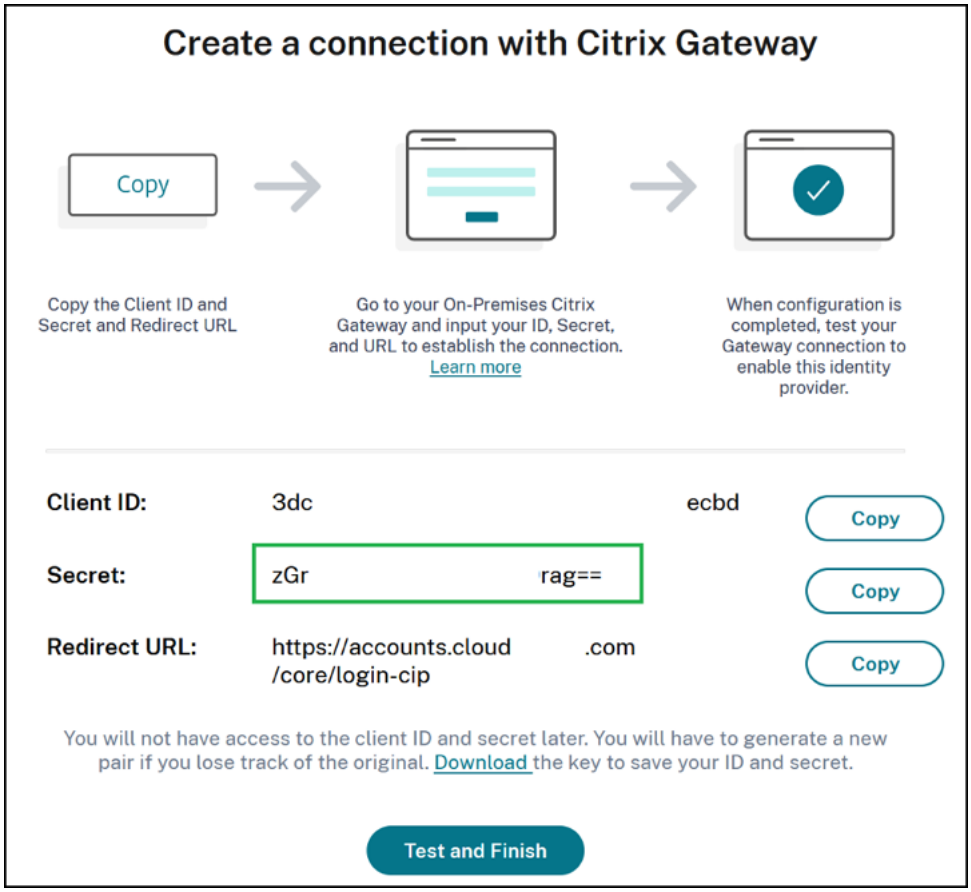
Citrix Cloud 管理员有权访问未加密的客户端密钥。这些凭证由 Citrix Cloud 在 Citrix Gateway 链接过程中在“身份和访问管理” **>** “身份验证”中提供。OAuth 配置文件和策略由 Citrix 管理员创建。它是在连接过程中在 Citrix Gateway 上手动创建的。

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 界面或命令行界面 (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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

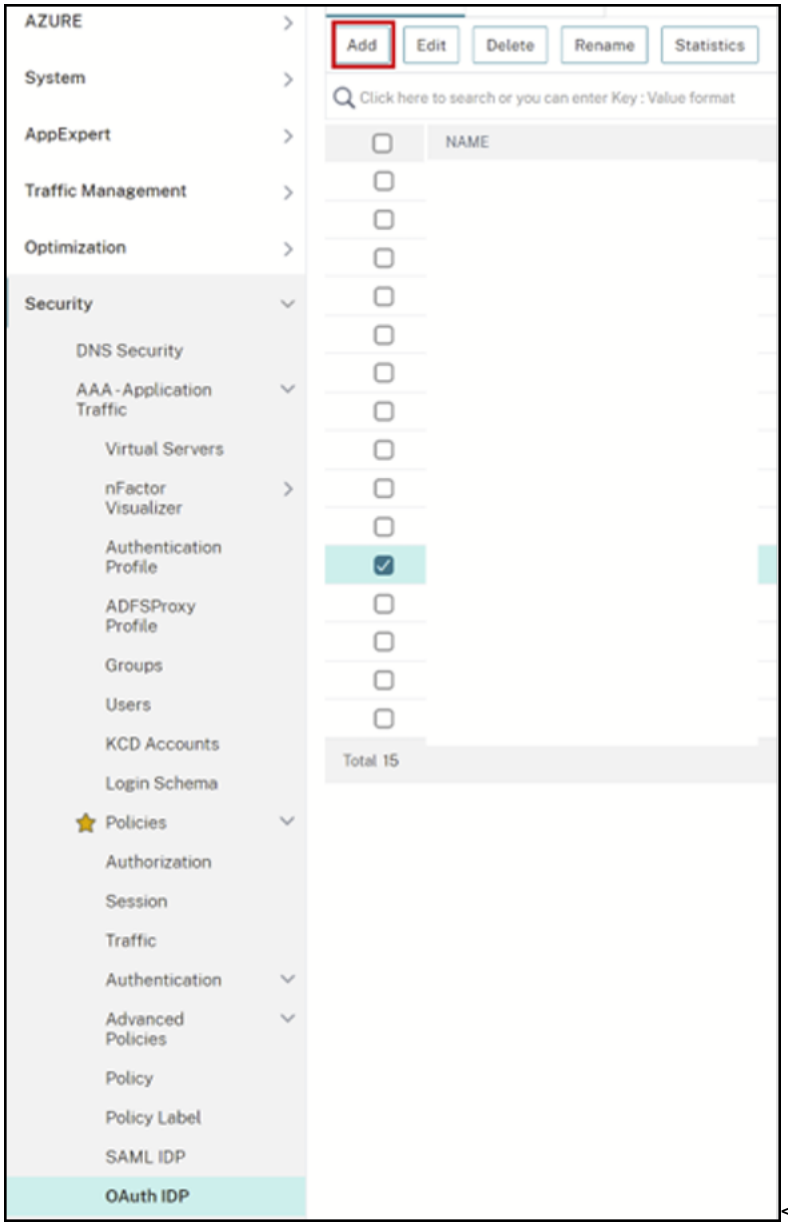
> 注意：
>
> 连接 Citrix Gateway 后，管理员无法获取未加密机密的副本。他们必须在连接过程中保存凭证。



使用 **Citrix Cloud**　执行以下步骤使用 Citrix Gateway 界面添加另一个 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”。</p>

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1

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* 。

```
![修改 OAuth 策略名称](/en-us/citrix-workspace/media/using-citrix-cloud-2.png)
```

1

在 Citrix Gateway GUI 上，创建您现有的 OAuth 配置文件

1

在同一个 GUI 菜单上单击 添加。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
![添加策略](/en-us/citrix-workspace/media/using-citrix-cloud-3.png)
```

1

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。

1

导航到“安全” > “虚拟服务器” > “编辑”。

```
![创建策略](/en-us/citrix-workspace/media/using-citrix-cloud-4.png)</ol
>
```

使用命令行界面 **(CLI)**

> 重要
>
> 如果您没有安全保存的 OAuth 凭据副本，则需要断开并重新连接 Citrix Gateway。使用 Citrix Cloud Identity and Access Management 提供的新 OAuth 凭据更新您现有的 OAuth 配置文件。不建议使用此过程，并且仅当旧凭证无法恢复时才可使用。

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
>
> 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

OAuthPolicy 绑定到您现有的身份验证、授权和审计虚拟服务器。首先评估较低优先级的数字。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。

   ```
   > sh runn | grep oauth
   add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf -clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret cd20[redacted]
   [redacted]614a222303d -encrypted -encryptmethod ENCMTHD_3 -kek -suffix 2023_04_[redacted]
   [redacted]_09_12_25 -redirectURL "https://accounts.cloudburrito.com/core/login-cip" -audience b1656835-20d1-4f6b-addd-1a531fd253f6 -sendPassword ON
   ```

4. 修改从上一步复制的行。使用它来构建一个新的 CLI 命令，允许您使用客户端 ID 的加密版本创建 OAuth 配置文件。必须包含所有加密参数。

   - 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

以下示例涵盖了这两项更新。

```
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

- 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。
- 如果您在以前的解决方案上配置了自定义域，并使用 SAML 或 Microsoft Entra ID 来验证 Citrix Workspace 访问权限，则 无法 在新解决方案上配置自定义域，除非先 删除现有的 自定义域。
- 当您使用 Citrix Workspace Web Extension 并访问自定义域帐户时，服务连续性功能不起作用。[WSP-23564]

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。

配置工作区 **URL**

May 13, 2025

© 1997–2025 Citrix Systems, Inc. All rights reserved.

概述

首次启用 Workspace 时，系统会创建一个形式为 `customername.cloud.com` 的 Workspace URL，可用于从 Web 浏览器或本地安装的 Citrix Workspace 应用程序访问 Workspace。

您可以添加其他 cloud.com URL。如果您定义了多个工作区 URL，则可以使用这些 URL 作为策略输入。例如，您可能希望为组织内的不同部门提供不同的品牌、身份验证方法和资源。

您还可以使用自己的自定义域作为默认 cloud.com 域的别名。有关更多信息，请参阅 配置自定义域。

存储名称

每个工作区 URL 都有一个商店名称。此名称显示在 Citrix Workspace 应用程序内的帐户列表中。

您可以配置用户是否可以在 Citrix Workspace 应用程序中修改商店名称。要允许用户从 Citrix Workspace 应用程序编辑其应用商店名称，用户必须使用以下版本的 Citrix Workspace 应用程序客户端：

- 适用于 Windows 的 Citrix Workspace 应用程序 2405 或更高版本
- 适用于 iOS 的 Citrix Workspace 应用程序 24.2.0 或更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 2402

启用或禁用工作区 **URL**

您可以禁用对 cloud.com URL 的工作区的所有访问。这会影响本地安装的 Citrix Workspace 应用程序和浏览器。用户可以继续使用自定义工作区 URL 访问默认工作区。如果您没有自定义工作区 URL，那么这会阻止所有访问。

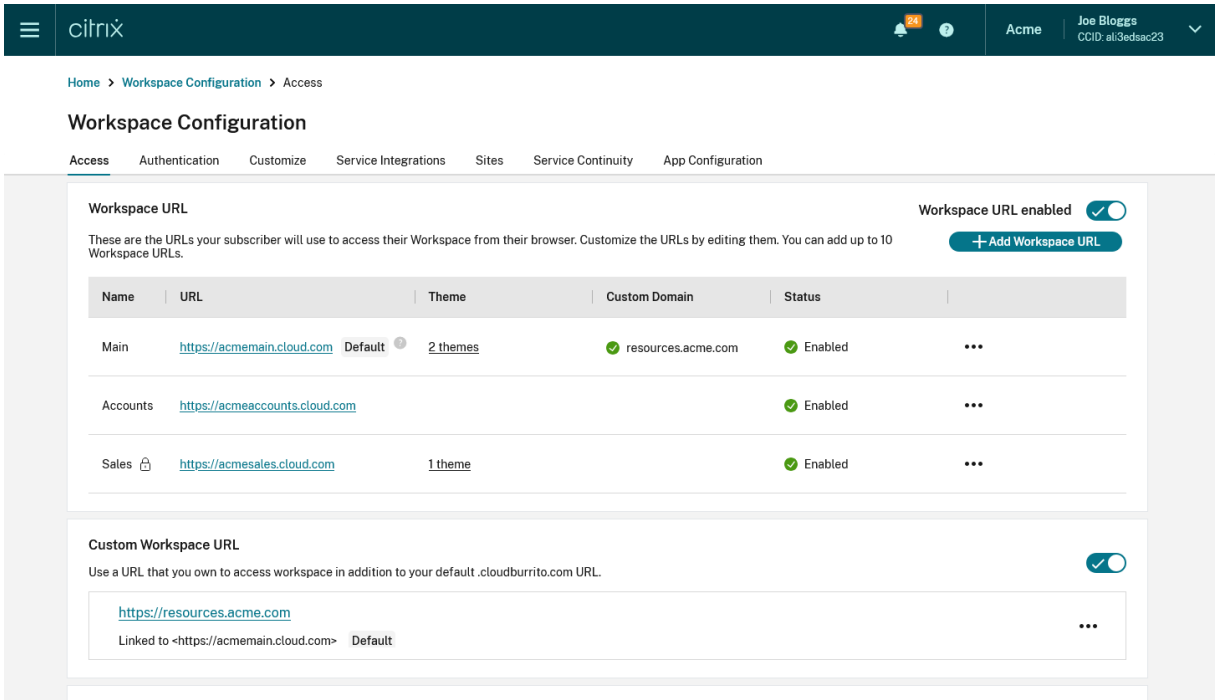
要禁用通过 cloud.com 的访问：

1. 取消勾选 工作区 **URL** 已启用。这将弹出一个确认屏幕。
2. 选中复选框以确认您理解。
3. 按 禁用。

查看 **URL**

1. 转到 Citrix Cloud 并使用您的凭据登录。
2. 导航到 工作区配置 > 访问。在 工作区 **URL** 下，您可以找到现有 URL 的列表。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



添加工作区 **URL**

您最多可以创建 10 个 URL。您选择的工作区 URL 必须是唯一的。Citrix Cloud 拒绝其他客户已在使用的工作区 URL。建议使用包含您的组织独有的字符串的命名约定。

> 注意：
>
> 避免使用通用 URL，例如 `workspace.cloud.com`或 `mystore.cloud.com`。

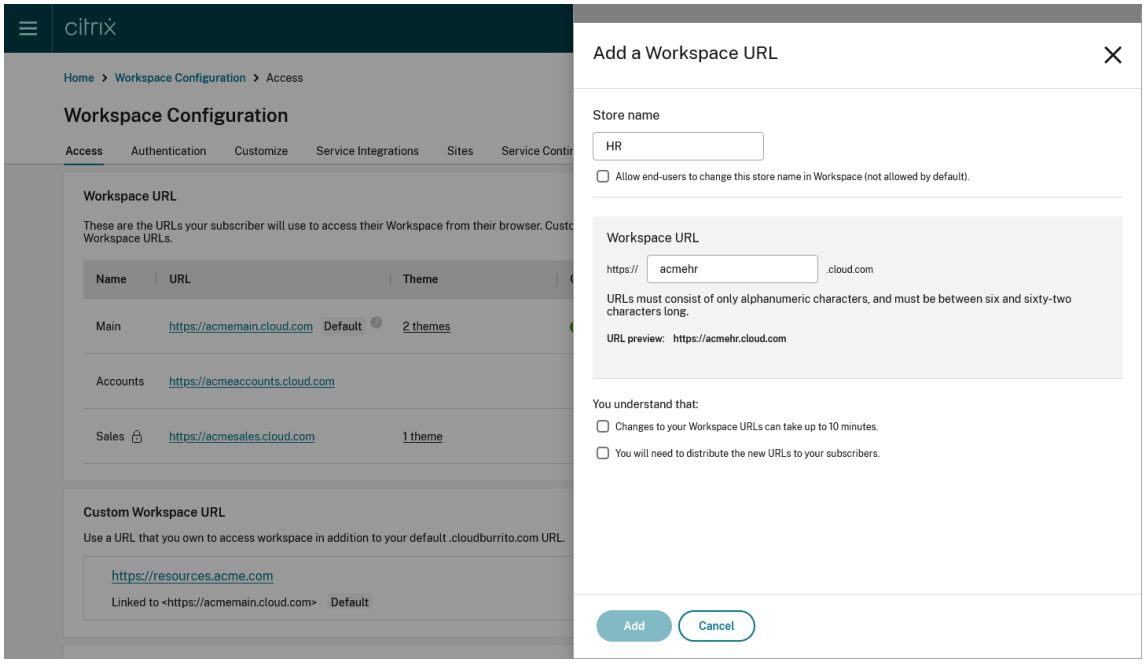
例如，您可以使用以下格式创建 URL：

- `YourOrgsales.cloud.com`
- `YourOrgengineering.cloud.com`
- `YourOrgmarketing.cloud.com`

从“访问”选项卡添加 URL：

1. 点击 **+** 添加工作区 **URL**
2. 输入应用商店名称.
3. 选择是否希望用户能够在 Citrix Workspace 应用程序中修改商店名称。
4. 输入子域名。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



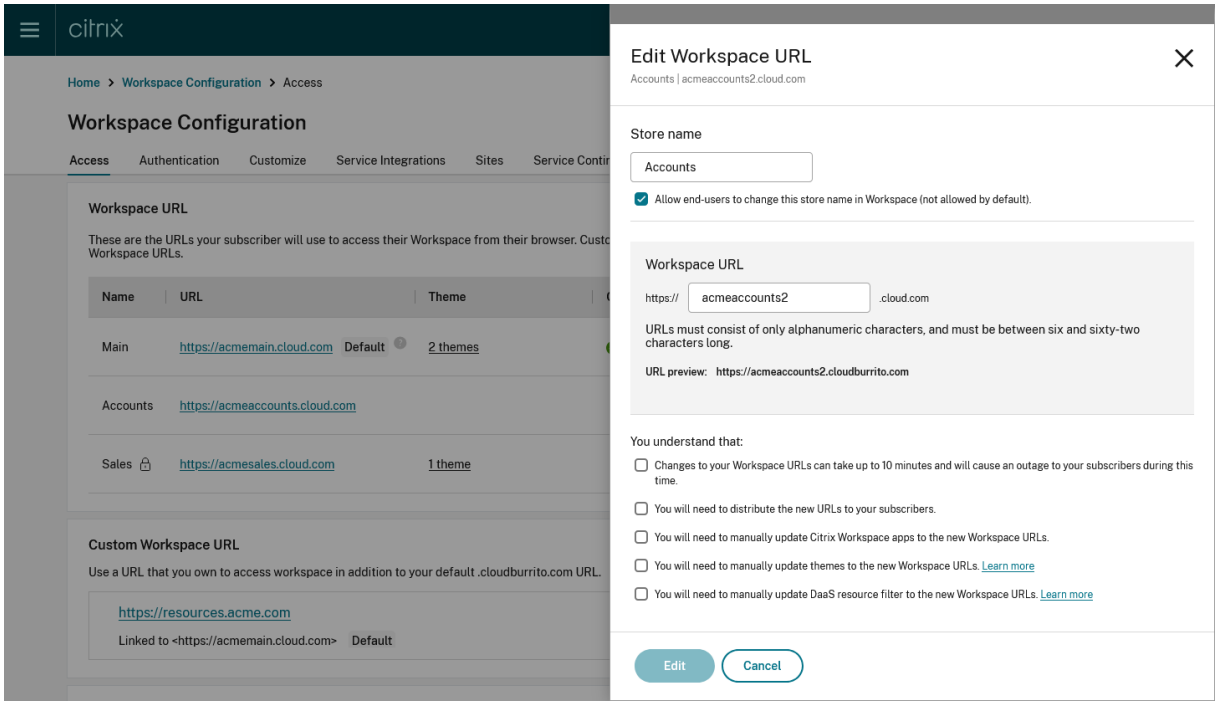
5. 选中复选框作为确认您必须在配置后向最终用户提供新的 URL。
6. 单击 添加 保存 URL。

修改工作区 **URL**

> 警告：
>
> 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。新的 URL 最多 10 分钟内不可用。如果任何策略中使用该 URL，则必须手动更新该策略。

1. 单击 …在您想要编辑的工作区 URL 行上。
2. 根据需要修改商店名称和工作区 URL。
3. 如果您修改了 URL，那么您必须勾选几个复选框以确认您了解其后果。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. 按“编辑”保存更改

使用 **PowerShell** 配置工作区 **URL**

您还可以使用 PowerShell API 来添加或更改工作区 URL。

运行 cmdlet `Set-WorkspaceCustomConfigurations` 并将 `$WorkspaceHosts` 列表作为 `-WorkspaceHosts` 参数的参数，以更新工作区的 URL 列表。将现有的 URL 作为 `-WorkspaceUrl` 参数的参数。例如：

```
#  Set a variable to the value of existing URL for the workspace.
$WSPURL = "wspmultiurlmain.cloud.com"

# Specify the new URLs that you want to create in a list, including any existing URLs.
$WorkspaceHosts = @($WSPURL,"wspmultiurl2.cloud.com","wspmultiurl3.cloud.com")

# Update the configuration
Set-WorkspaceCustomConfigurations -WorkspaceUrl $WSPURL `
                                  -WorkspaceHosts $WorkspaceHosts `
                                  -ClientId $APIClientID `
                                  -ClientSecret $APIClientSecret `
                                  -Verbose
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
Name                                Value
----                                -----
windowsShareIdpSessions
disallowICADownload                 False
macShareIdpSessions
androidWebviewtype
iosWebviewtype
inactivityTimeoutInMinutesM...
linuxShareIdpSessions
idpdomains
inactivityTimeoutInMinutes
workspaceHosts                      {wspmultiurlmain.cloud.com, wspmultiurl2.cloud.com, wspmultiurl3.cloud.com}
```

配置身份验证方法

为每个 URL 配置不同的身份验证方法：

1. 创建一个 条件身份验证配置文件。
2. 添加类型为 工作区 **URL** 的 策略条件，然后选择该条件应适用的工作区 URL。
3. 选择该工作区 URL 的身份验证方法。
4. 对每个工作区 URL 重复此操作。
5. 在工作区配置 身份验证中，选择您创建的条件身份验证配置文件。

或者，如果您正在使用自适应身份验证，请参阅 配置自适应身份验证策略。

配置主题和徽标

您可以为每个工作区创建并分配单独的主题和徽标。有关更多信息，请参阅 外观。

使用安全私有访问进行资源过滤

在使用安全私有访问配置 Citrix DaaS 时，您可以控制最终用户对资源的访问。您可以通过配置基于工作区 URL 的访问策略来实现此功能。可以使用工作区 URL 过滤器为交付组配置访问策略。

有关更多信息，请参阅 Citrix Secure Private Access

发送自定义公告

您可以根据用户的工作区 URL 向他们显示不同的自定义公告。有关更多信息，请参阅 发送自定义公告。

资源 从 **DaaS** 中过滤资源

您可以根据工作区 URL 为交付组配置访问策略。有关更多信息，请参阅 使用交付组访问策略进行资源过滤。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置自适应身份验证策略

如果您使用自适应身份验证，则可以将身份验证策略与工作区 URL 关联。这使您能够根据最终用户使用的工作区 URL 为他们配置不同的身份验证策略。

步骤 **1**：配置一系列您想要用于工作区 URL 的身份验证操作和策略。策略配置取决于您想要使用的身份验证类型和身份验证因素。可以使用任何受支持的 nFactor 身份验证流程。

有关更多信息，请参阅 自适应身份验证

例如，考虑以下场景：

- 第一个 URL <https://wspmultiurlmain.cloud.com> 必须映射到 LDAP 身份验证和 OTP。
- 第二个 URL <https://wspmultiurl2.cloud.com> 必须映射到 LDAP 身份验证。
- 第三个 URL <https://wspmultiurl3.cloud.com> 必须具有最终用户证书身份验证

例子：

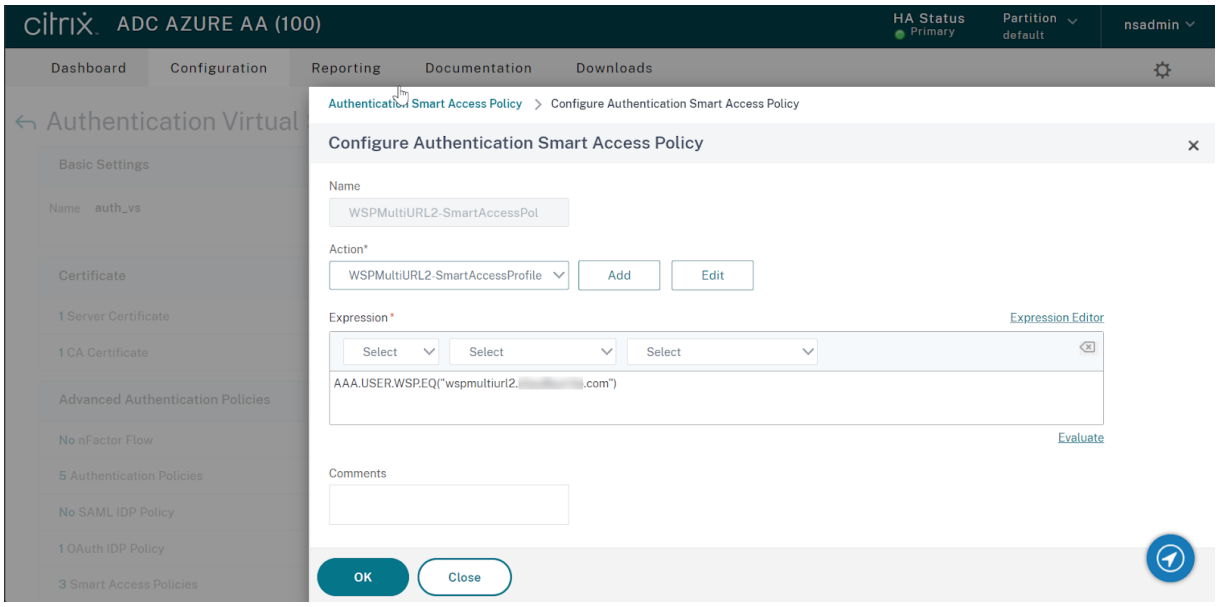
使用精确的字符串匹配来检查特定的工作区 URL。

```
AAA.USER.WSP.EQ("wspmultiurlmain.cloud.com")
```

使用子字符串匹配检查特定字符串是否包含在工作区 URL 中。

```
AAA.USER.WSP.CONTAINS("wspmultiurlmain")
```

第 **2** 步：配置身份验证策略并添加您的工作区 URL 作为表达式。然后，身份验证策略对于您在 表达式 文本字段中输入的工作区 URL 有效。



步骤 **3**：一旦您根据您的 URL 配置了身份验证策略，您就需要将它们绑定到您的身份验证虚拟服务器。有关更多信息，请参阅 身份验证策略。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

电子邮件发现将工作区 **URL** 添加到 **Citrix Workspace** 应用程序

电子邮件发现将服务 URL 列表中配置的所有工作区 URL 添加为存储。如果您想通过电子邮件发现添加两个或更多商店，请将每个工作区 URL 配置为服务 URL。它确保在电子邮件发现过程中将 URL 添加为存储。您可以使用以下任意一种方式添加店铺：

- 全局应用程序配置服务 UI：有关更多信息，请参阅 配置云存储设置
- 全局应用程序配置 API：您可以使用上述门户，使用您注册的域对 POST /aca/discovery/app/workspace/-domain 进行 API 调用。有关更多信息，请参阅全局应用程序配置服务 API。

如果在 Citrix Workspace 应用程序中输入 `<user@yourdomain.com>` ，则电子邮件发现服务会添加服务 URL 中列出的所有存储。当 UPN 或电子邮件地址包含正确的域后缀 `mydomain.com`时，您可以使用它。

已知限制

以下是影响多个 URL 功能的一些限制。

工作区配置

- 工作区仅限于单个自定义域。它始终链接到管理控制台中标记为默认的工作区 URL。
- 您不能禁用单个 URL。如果您在 Citrix Cloud 管理控制台中禁用工作区 URL，它将禁用所有配置的 URL。

Citrix Virtual Apps and Desktops

- 不支持使用 Citrix Virtual Apps 和 Desktops（本地聚合）的工作区 URL 进行资源过滤。

Citrix Workspace 应用程序　要将来自同一客户的多个 URL 添加为商店，用户必须使用以下版本的 Citrix Workspace 应用程序客户端：

- 适用于 Windows 的 Citrix Workspace 应用程序 2302 或更高版本
- 适用于 iOS 的 Citrix Workspace 应用程序 2303 或更高版本
- 适用于 Android 的 Citrix Workspace 应用程序 2303 或更高版本
- 适用于 Linux 的 Citrix Workspace 应用程序 2303 或更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 2305
- 适用于 iOS 的 Citrix Workspace 应用程序版本 2303
- 旧版本的 Citrix Workspace 应用程序显示 Workspace 域选择器菜单。在这种情况下，最终用户必须选择添加商店时输入的相同 URL。选择不同的 URL 需要用户再次登录。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Global App Configuration Service

- 如果为多个工作区 URL 配置了全局应用程序配置服务设置，则一次只能将一个工作区 URL 添加到 Citrix Workspace 应用程序。向 Citrix Workspace 应用程序添加第二个 URL 失败。例如，如果为 <https://wspmultiurlmain.yourdomain.com:443> 和 <https://wspmultiurl2.yourdomain.com:443> 同时配置了 GACS 设置，则用户只能向 Citrix Workspace 应用程序添加一个 URL。
- 如果在全局应用程序配置服务发现期间发现多个 GACS 配置的 URL，则帐户添加失败。例如，考虑用户在 Citrix Workspace 应用程序中输入 <user@yourdomain.com> 的情况。基于域的发现找到两个结果，并且为它们都配置了 GACS 设置。返回的响应是：<https://wspmultiurlmain.yourdomain.com:443> 和 <https://wspmultiurl2.yourdomain.com:443>。在这种情况下，Citrix Workspace 应用程序添加帐户会失败，因为它仅支持添加一个具有 GACS 设置配置的帐户。

```
 {

   "items": [
  {

    "domain": {

      "name": "yourdomain.com"
     }
,
    "app": {

      "workspace": {

        "serviceURLs": [
          {

            "url": "https://wspmultiurlmain.yourdomain.com:443"
           }
,
          {

            "url": "https://wspmultiurl2.yourdomain.com:443"
           }
,
          {

            "url": "https://wspmultiurl3.yourdomain.com:443"
           }

        ]
       }

     }

   }

```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

```
    ],
    "nextToken": "None",
    "count": 1
  }
```

配置身份验证

November 7, 2024

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：

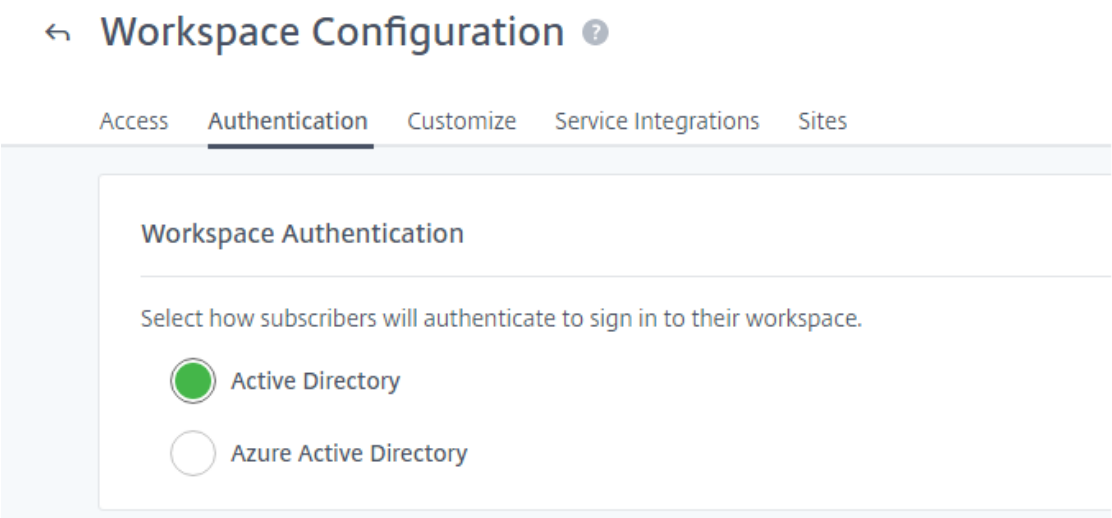
- Active Directory (AD)
- Active Directory 加令牌
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

Citrix Workspace 还支持单点登录您的虚拟应用程序和桌面。当用户输入其 Active Directory 凭据时，Workspace 可以使用这些凭据为资源提供 SSO。当使用其他 IdP 时，Workspace 可以使用 Citrix 联合身份验证服务 (FAS) 为资源提供单点登录 (SSO)。

选择或更改身份验证方法

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 工作区配置 **>** 身份验证 **>** 工作区身份验证中选择或更改订阅者如何对其工作区进行身份验证。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> 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。

使用 AD 单点登录 VDA

使用 AD 身份验证时，Workspace 在启动加入 AD 的虚拟应用程序和桌面时提供 SSO 功能。

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”。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

使用 **AD plus** 令牌单点登录 **VDA**

当使用 AD 加令牌身份验证时，Workspace 在启动加入 AD 的虚拟应用程序和桌面时提供 SSO 功能。

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。

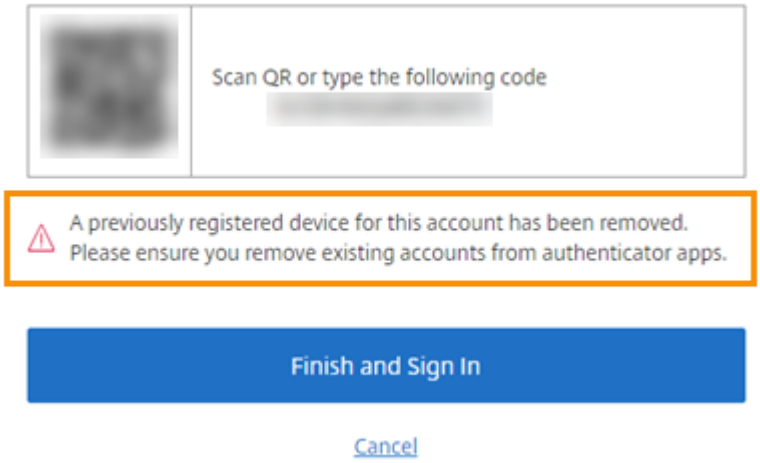
> 重要：
>
> 在设备注册过程中，订阅者会收到一封包含临时验证码的电子邮件。此临时代码仅用于注册订阅者的设备。不支持使用此临时代码作为通过双重身份验证登录 Citrix Workspace 的令牌。只有从已注册设备上的身份验证应用程序生成的验证码才是支持双重身份验证的令牌。

重新注册设备

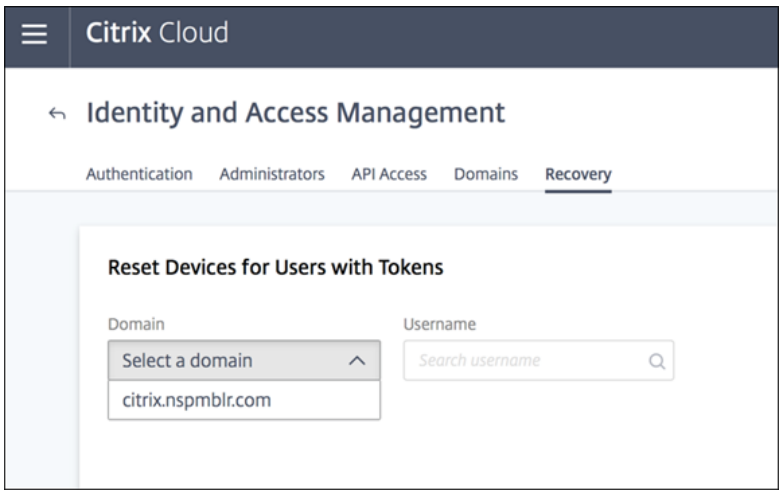
如果订阅者不再拥有已注册的设备或需要重新注册该设备（例如，从设备中擦除内容后），Workspace 将提供以下选项：

- 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 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 Microsoft Entra ID（以前称为 Microsoft Azure AD）。有关 Citrix Cloud 使用的 Microsoft Entra ID 应用程序和权限的详细信息，请参阅 Citrix Cloud 的 Azure Active Directory 权限。
- 在本地 AD 域中安装的 Citrix Cloud Connector。该机器还必须加入与 Microsoft Entra ID 同步的域。
- VDA 版本 7.15.2000 LTSR CU VDA 或 7.18 当前版本的 VDA 或更高版本。
- Microsoft Entra ID 和 Citrix Cloud 之间的连接。有关信息，请参阅 将 Azure Active Directory 连接到 Citrix Cloud。
- 任何版本的 Citrix Workspace 应用程序。如果使用旧版 Citrix Receiver，则必须使用以下最低版本：
  - Citrix Receiver for Windows 4.11 CR 或 4.9 LTSR CU2 或更高版本

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - Citrix Receiver for Linux 13.8
  - Citrix Receiver for Android 3.13 及更高版本

将您的 Active Directory 同步到 Microsoft Entra ID 时，UPN 和 SID 条目必须包含在同步中。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 Microsoft Entra ID，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 Microsoft Entra ID 用户会话启动失败。
> - 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 Microsoft Entra ID 身份验证后：

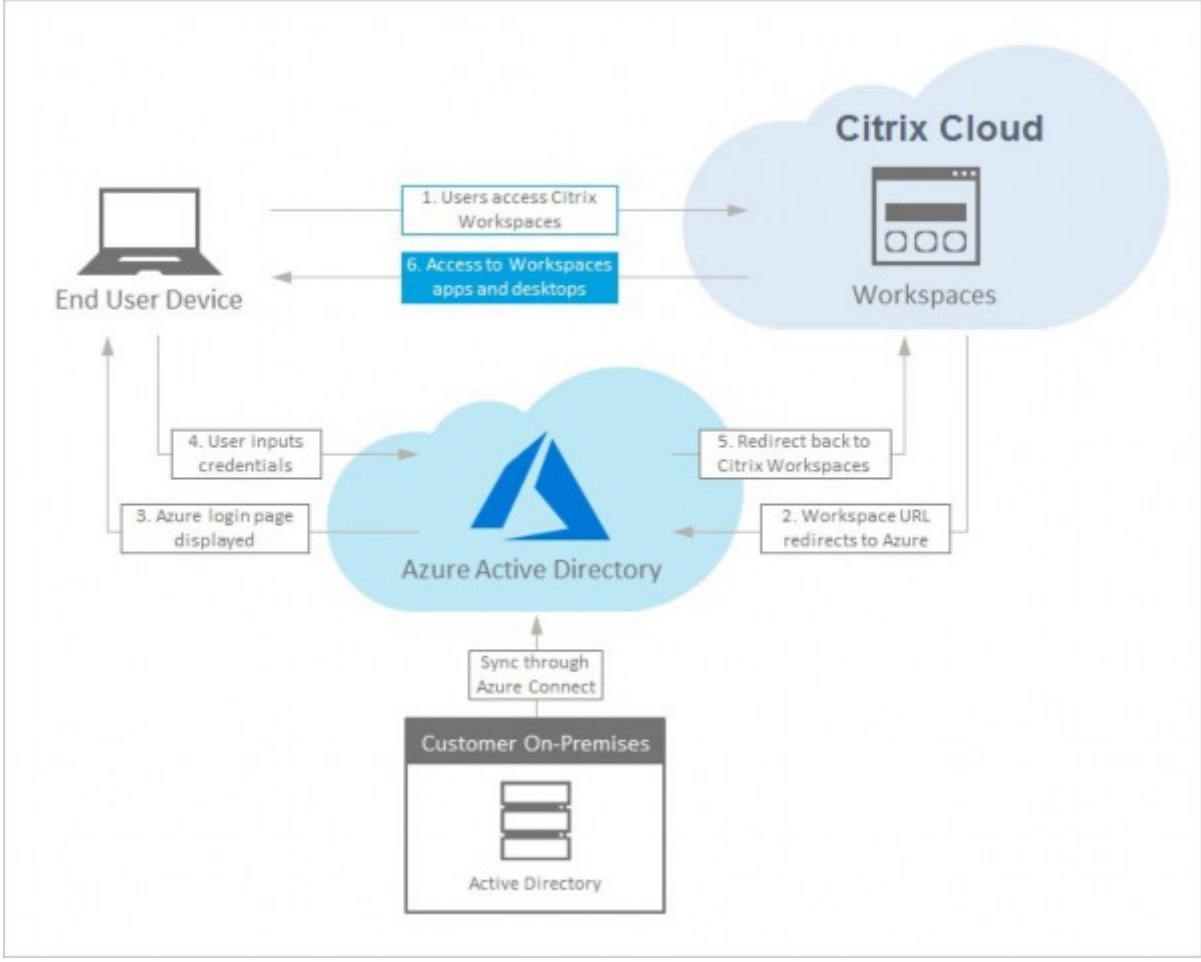
- 增强安全性：出于安全考虑，启动应用程序或桌面时，系统会提示用户重新登录。密码信息直接从用户的设备流向托管会话的 VDA。
- 登录体验： Microsoft Entra ID 身份验证提供联合登录，而不是单点登录 (SSO)。订阅者从 Azure 登录页面登录，并且在打开 Citrix DaaS 时可能需要再次进行身份验证。

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 Microsoft Entra ID 的登录体验。有关信息，请参阅 Microsoft 文档。在工作区配置中进行的任何登录自定义（徽标）都不会影响 Microsoft Entra ID 登录体验。

下图显示了 Microsoft Entra ID 身份验证的顺序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



退出体验

使用 设置 **>** 注销 完成从工作区和 Microsoft Entra ID 的退出过程。如果订阅者关闭浏览器而不是使用 注销 选项，他们可能仍然登录到 Microsoft Entra ID。

> 重要：
>
> 如果 Citrix Workspace 因不活动而在浏览器中超时，订阅者仍会保持登录 Microsoft Entra ID 的状态。这可以防止 Citrix Workspace 超时强制关闭其他 Microsoft Entra ID 应用程序。

使用 **EntraId** 单点登录 **VDA**

使用 EntraId 身份验证时，要启用 VDA 的单点登录，您必须使用 FAS。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

使用网关进行单点登录

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

使用 **Google** 单点登录 **VDA**

使用 Google 身份验证时，要启用 VDA 单点登录，您必须使用 FAS。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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. 订阅者被重定向到 Okta 登录页面，并使用 Okta 中配置的方法进行身份验证（例如，多重身份验证、条件访问策略等）。
3. 成功进行身份验证后，将显示订阅者的工作区。

使用 **Okta** 单点登录 **VDA**

使用 Okta 身份验证时，要启用 VDA 的单点登录，您必须使用 FAS。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

使用 **SAML 2.0** 单点登录 **VDA**

使用 SAML 身份验证时，要启用 VDA 单点登录，必须使用 FAS。

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虚拟应用程序和桌面。

有关更多信息，请参阅 Citrix 联合身份验证服务 (FAS)。

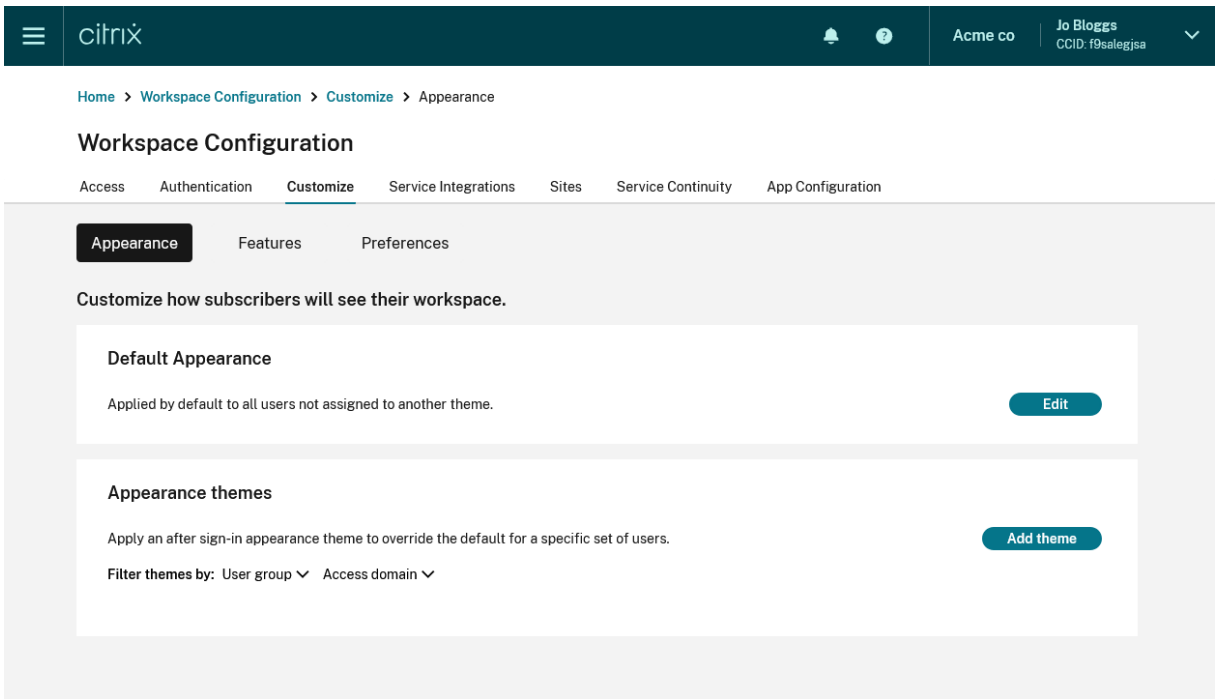
更多信息

- 技术简报：工作区单点登录
- 技术见解 - Citrix Workspace

自定义你的工作空间体验

November 7, 2024

要自定义工作区，请从菜单中打开 工作区配置，然后打开 自定义 选项卡。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

外观

要使用您自己的徽标和颜色定制您的工作区，请转到 外观 选项卡。有关详细信息，请参阅自定义工作区的外观。

功能

要自定义用户可以访问的功能，请转到 功能 选项卡。有关更多信息，请参阅 启用和禁用功能。

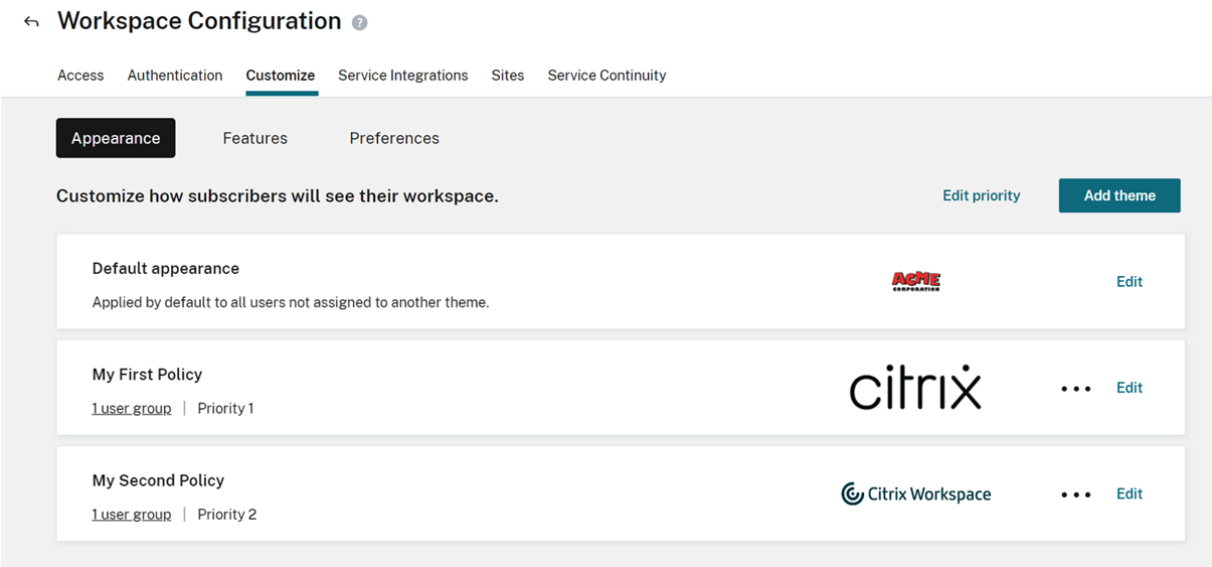
首选项

要修改行为、外观的其他方面，并配置商店、应用程序和桌面的访问方法，请转到 首选项 选项卡。有关更多信息，请参阅 自定义安全和隐私政策、自定义工作区交互和 自定义存储访问。

自定义工作区的外观

May 13, 2025

您可以创建主题来自定义工作区的徽标和颜色，以符合您的企业品牌指南。您可以配置默认主题以及适用于特定工作区或用户组的其他主题覆盖。要查看和修改外观，请从 工作区配置 选择 自定义，然后选择 外观。



支持的自定义

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 注意：
>
> 登录徽标的更改不会影响使用第三方身份提供商（例如 Microsoft Entra ID 和 Okta）对其工作区进行身份验证的用户。
>
> 有关如何自定义 Microsoft Entra ID 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 开发人员文档。

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。

登录后的外观

您可以自定义以下元素

物品	说明
徽标	屏幕顶部横幅中显示的徽标
横幅颜色	屏幕顶部横幅的颜色
横幅文字和图标颜色	横幅中的活动管理器和个人资料图标的颜色
强调色	用于突出显示选定项目和按钮的颜色

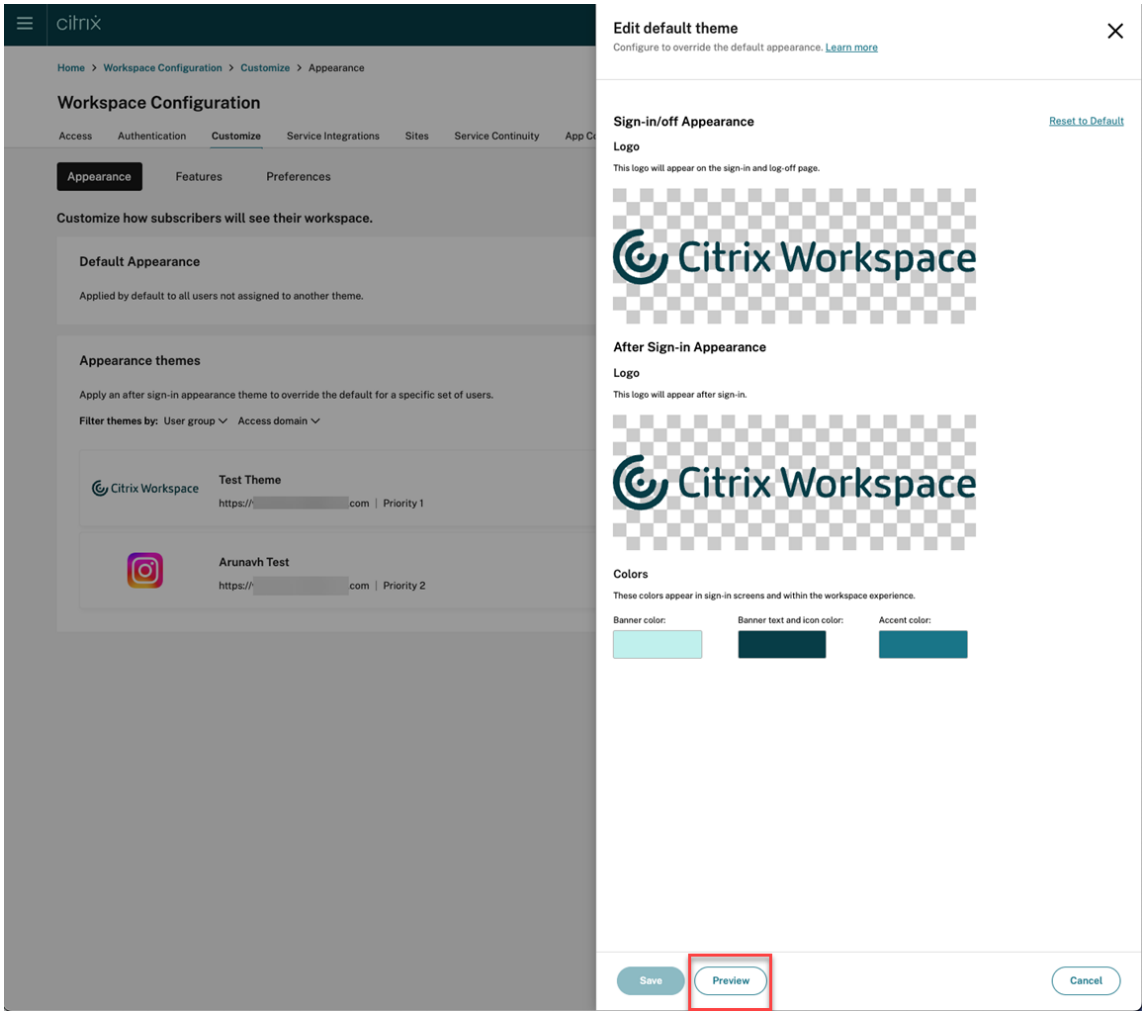
编辑默认主题

当没有其他主题适用时，将使用默认主题。它还包括无法覆盖的登录屏幕徽标。

修改默认主题：

1. 在 默认外观 卡中，选择 编辑。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



2. 在登录/注销外观部分，可选择拖放图像文件作为徽标使用。徽标应为 480 x 120 像素，最大大小为 2 MB，文件扩展名为 JPEG、JPG 或 PNG。
3. 在登录后外观部分，可选择拖放一个图像文件作为徽标。徽标应为 340 x 80 像素，最大 2 MB，文件扩展名为 JPEG、JPG 或 PNG。
4. 单击颜色即可更改颜色。从颜色选择器中选择或输入颜色值。您可以在十六进制、HSL 和 RGB 值之间切换。
5. 要预览最终用户将看到的主题，请选择 **Preview**。
6. 选择 保存。

对于使用 Web 浏览器的用户，更改将在用户下次登录或刷新页面时应用。对于使用 Citrix Workspace 应用程序的用户，更改大约需要五分钟才能生效。

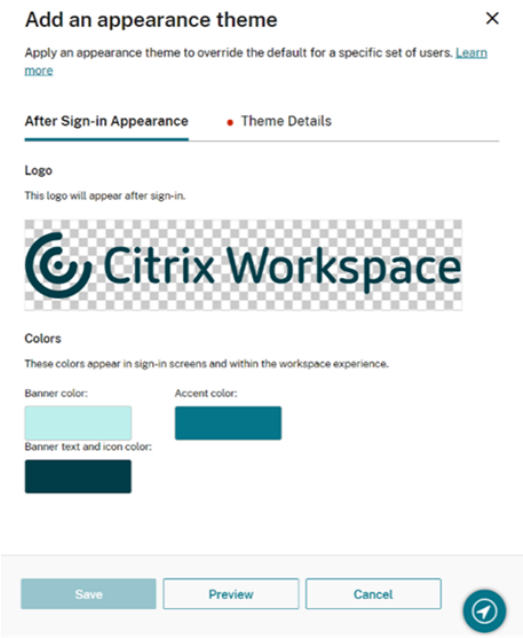
自定义主题

您可以配置并优先考虑适用于特定工作区和用户组的其他主题。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

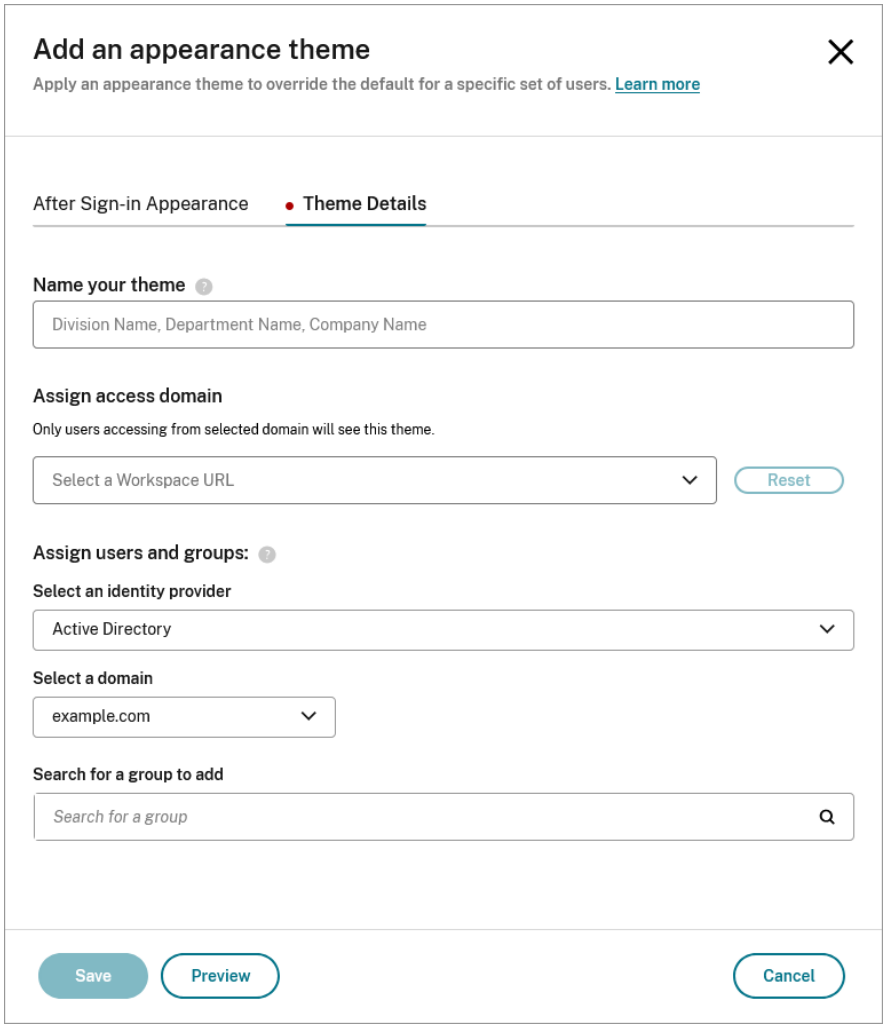
添加自定义主题

1. 按 添加主题。



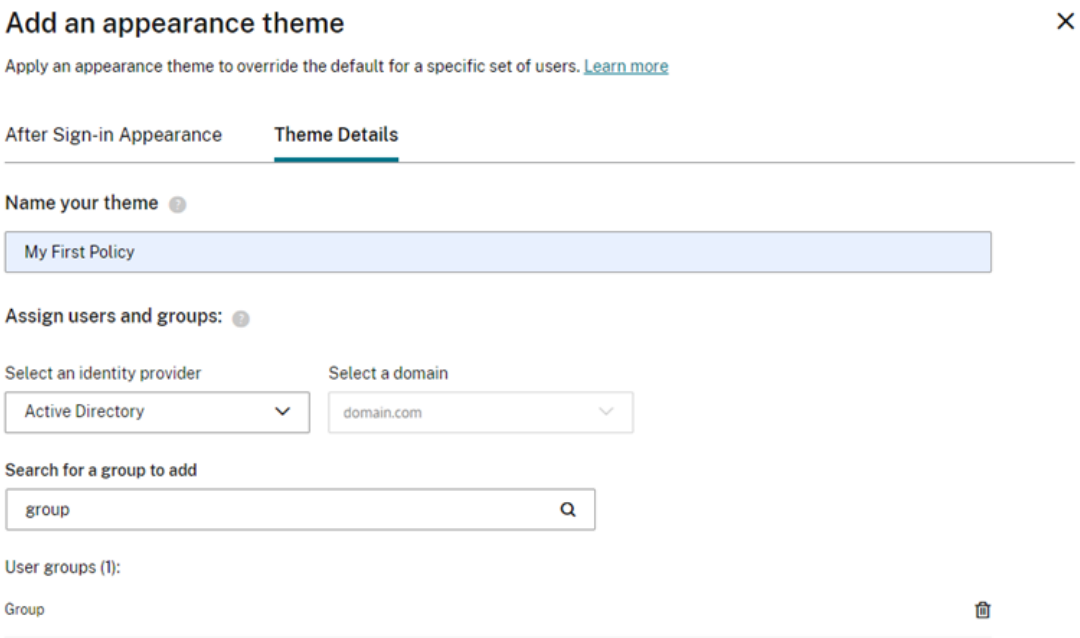
2. 配置您的自定义主题，方式与 默认主题相同。
3. 选择 主题详情 选项卡。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. 输入主题的名称。
5. 可选择指定主题适用于哪个工作区。
6. 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) 对您想要使用主题的每个组重复此过程。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



7. 或者选择 预览 来查看您的工作区在最终用户眼中的样子。
8. 按 保存。

编辑自定义主题

1. 在主题卡上，选择 编辑。
2. 根据需要进行更改。
3. 选择 保存。

删除自定义主题

1. 在主题卡上，选择 …打开菜单。
2. 选择 删除。
3. 在确认窗口中，选择 删除。

优先考虑自定义主题

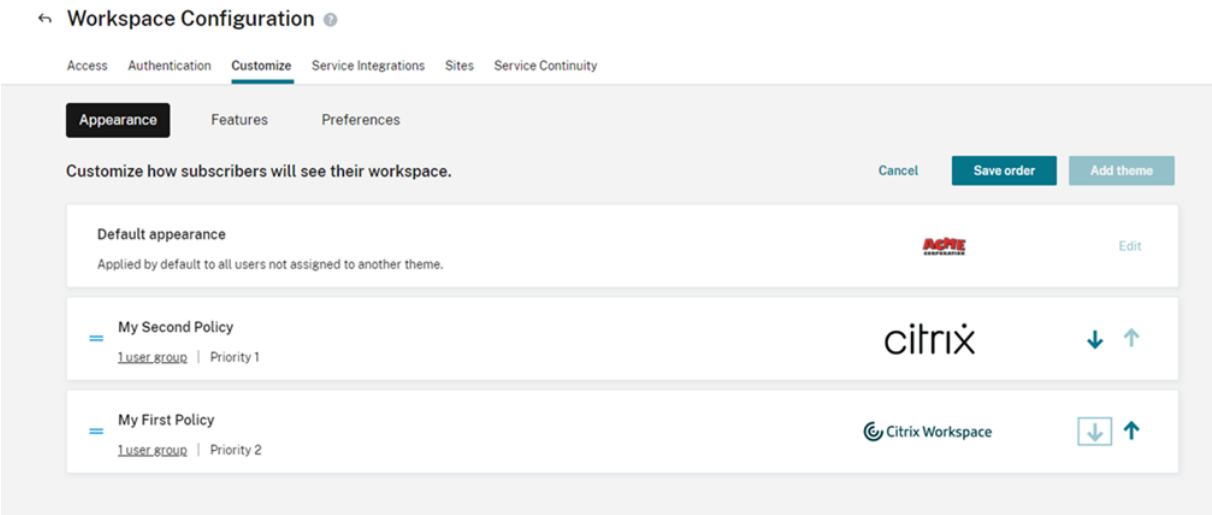
一个用户可能属于多个用户组，每个用户组可能与不同的主题匹配。您可以定义主题的优先顺序。应用与用户的工作区和组匹配的第一个主题。如果没有其他主题适用，则用户会看到默认主题。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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

March 1, 2025

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 设置可增强订阅者通过 Web 浏览器访问 Citrix Workspace 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

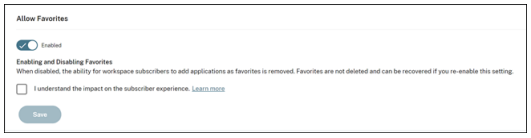
有权访问 **Workspace** 配置 和新 Workspace 体验的客户可以让用户在 Citrix Workspace 应用程序上添加或删除他们最喜欢的应用程序和桌面。用户可以通过 主页 选项卡快速访问自己喜欢的应用程序和桌面。默认情况下，“允许收藏

© 1997–2025 Citrix Systems, Inc. All rights reserved.

夹”功能处于启用状态。

要配置 允许收藏夹 功能，请按照以下说明操作：

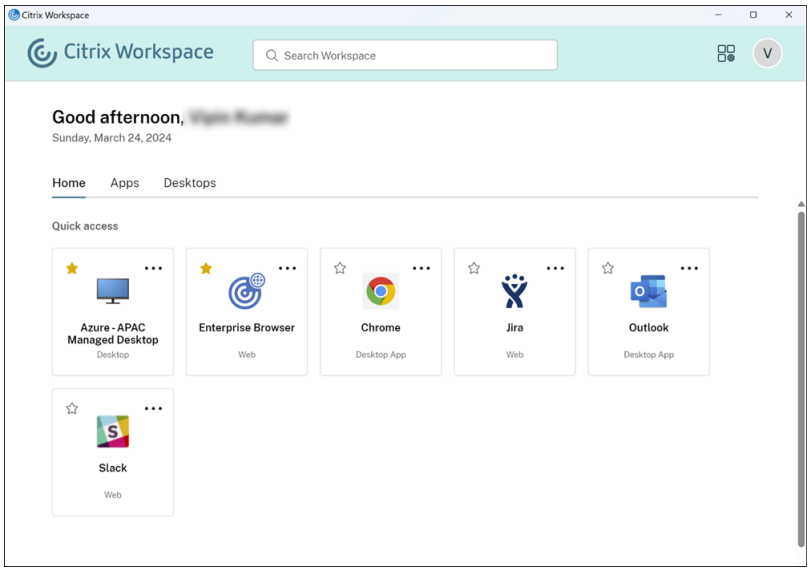
1. 导航到 工作区配置 > 自定义 > 首选项。
2. 单击切换按钮可启用或禁用该功能。
3. 选中声明复选框，然后单击 保存。



> 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”。您可以决定何时为您的用户启用此功能。

用户体验

当您启用 允许收藏夹 功能时，用户可以通过单击应用程序和桌面卡左上角的星形图标添加最多 250 个收藏夹。当用户将其标记为收藏时，星形图标会变成金色。再次单击星形图标可将其从收藏列表中删除。



当用户添加超过 250 个收藏资源时，将删除最旧（或尽可能接近）的收藏资源，以保留最近收藏的资源。

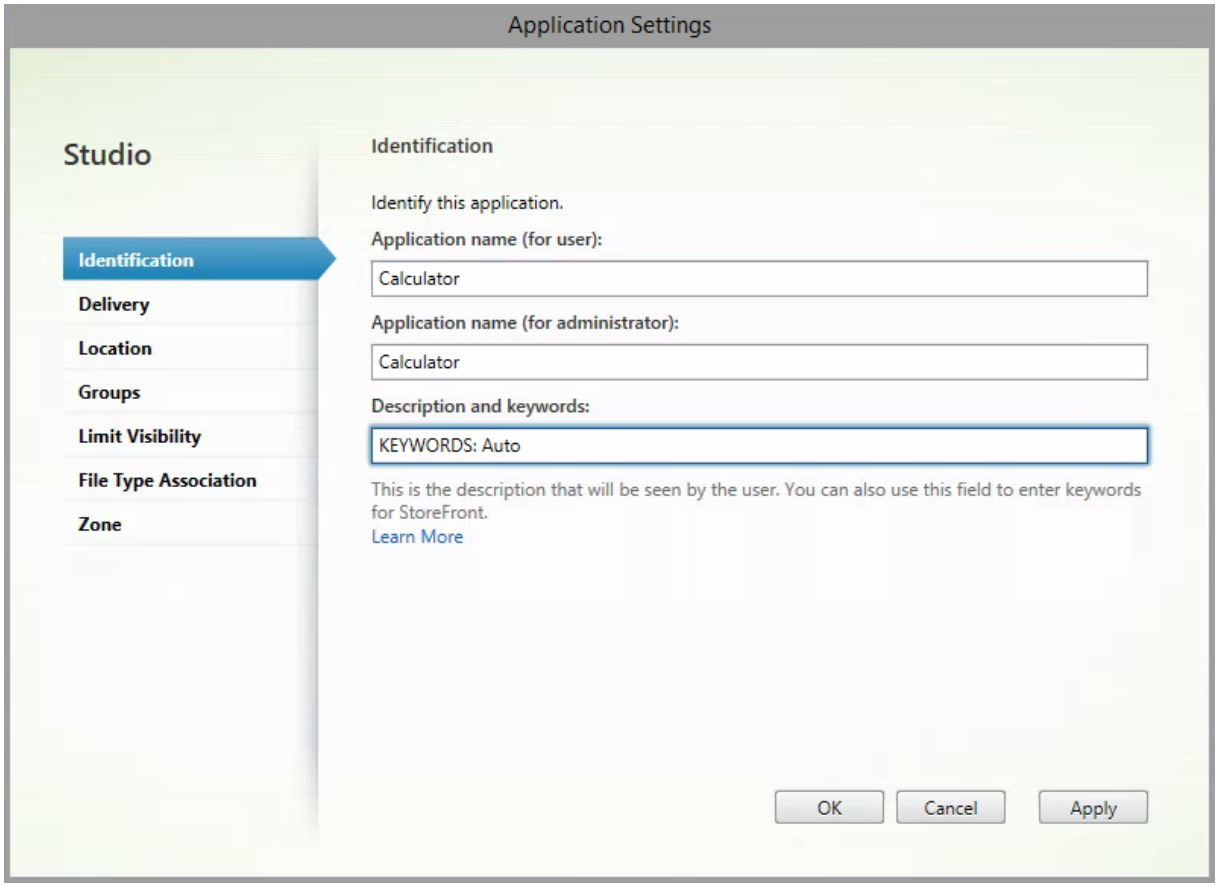
当您禁用 允许收藏夹 功能时，收藏夹资源将从 Citrix Workspace 应用程序的 主页 选项卡中删除。并且，它无法快速访问。用户仍然可以从 应用程序 选项卡和 桌面 选项卡访问这些资源。

> 注意：
>
> - 允许收藏 功能默认启用。
> - 如果您的用户无权访问已配置的桌面，则导航栏上不会出现 桌面 选项卡。

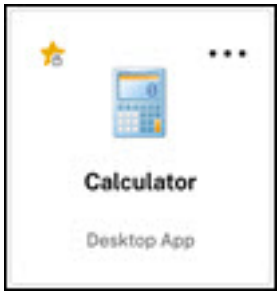
© 1997–2025 Citrix Systems, Inc. All rights reserved.

应用程序和桌面关键字

您可以使用 Citrix DaaS 中的 `KEYWORDS:Auto` 和 `KEYWORDS:Mandatory` 设置自动为用户添加喜爱的应用程序或桌面（管理 > 完整配置 > 应用程序）。



- 关键词：自动 - 应用程序或桌面被添加为收藏夹，用户可以根据自己的喜好将其从收藏夹列表中删除。
- 关键词：强制 - 该应用程序或桌面已添加为收藏夹，用户无法撤消此操作。强制应用程序和桌面显示带有挂锁的星形图标，表示不能将其从收藏夹列表中删除。



> 注意：
>
> 如果您对某个应用同时使用 **Mandatory** 和 **Auto** 关键字，则 **Mandatory** 关键字将覆盖 **Auto** 关键字，并且添加为收藏夹的应用或桌面无法被删除。

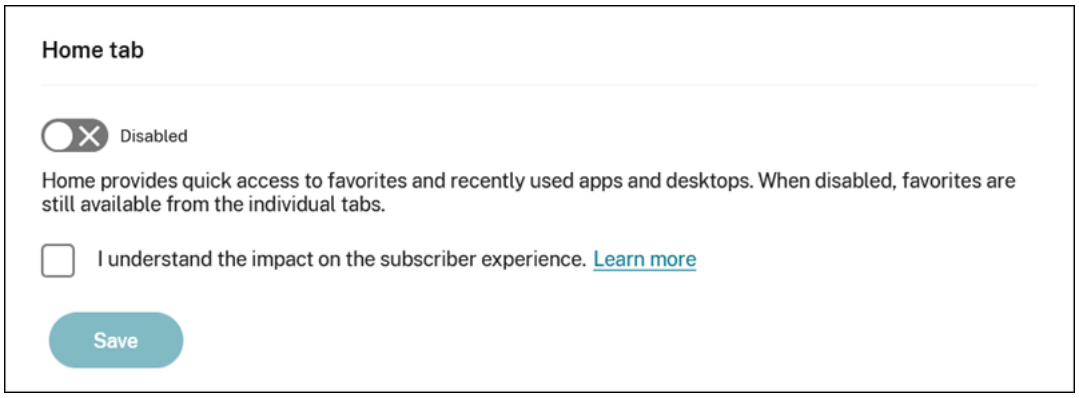
© 1997–2025 Citrix Systems, Inc. All rights reserved.

主页选项卡

您可以为您的用户启用或禁用 主页 选项卡。

要配置设置：

1. 登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 自定义 > 首选项。
2. 在 主页选项卡下，将切换开关设置为 已启用 或 已禁用。
3. 选中声明复选框。
4. 单击保存。
5. 开启切换后，用户将被导航到 主页。如果您禁用切换，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。



启用时（默认），将显示 **Home** 选项卡。禁用时，没有 主页 选项卡，用户将进入 应用程序 选项卡。

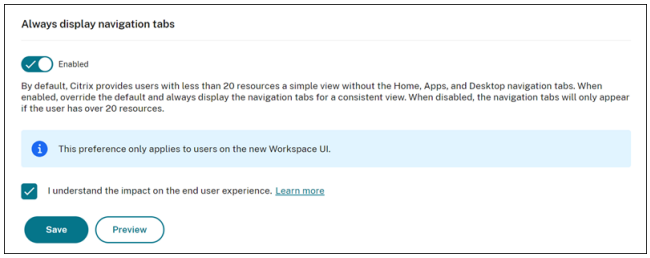
当“始终显示导航选项卡 ”被禁用且用户拥有超过 20 个应用程序或桌面时，此功能不适用。在这种情况下，选项卡被隐藏。

始终显示导航标签

默认情况下，如果用户拥有的资源少于 20 个，则 UI 将显示没有任何选项卡或类别的简单视图。要禁用简单视图并启用导航选项卡以获得一致的体验，即使资源少于 20 个，也请执行以下操作：

1. 登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 自定义 > 首选项。
2. 转到部分 始终显示导航选项卡。
3. 单击切换按钮可启用或禁用该功能。
4. 选中声明复选框。
5. 单击保存。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



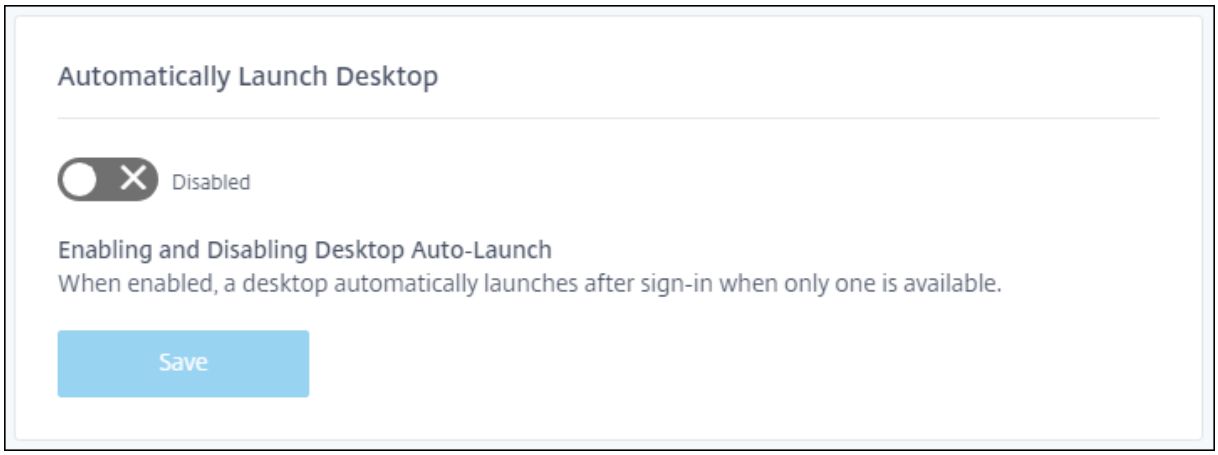
自动启动桌面

您可以配置 Workspace 以自动启动用户的桌面。启用后，如果用户只有一个可用桌面，则当用户登录其工作区时，该桌面会自动启动。禁用时（默认），用户必须在登录后手动启动其桌面。

此功能仅适用于使用 Web 浏览器，而不适用于 Citrix Workspace 应用程序。

要更改配置：

1. 导航到 工作区配置 > 自定义 > 首选项。
2. 在 自动启动桌面下，将开关设置为 启用 或 禁用。
3. 按 保存。

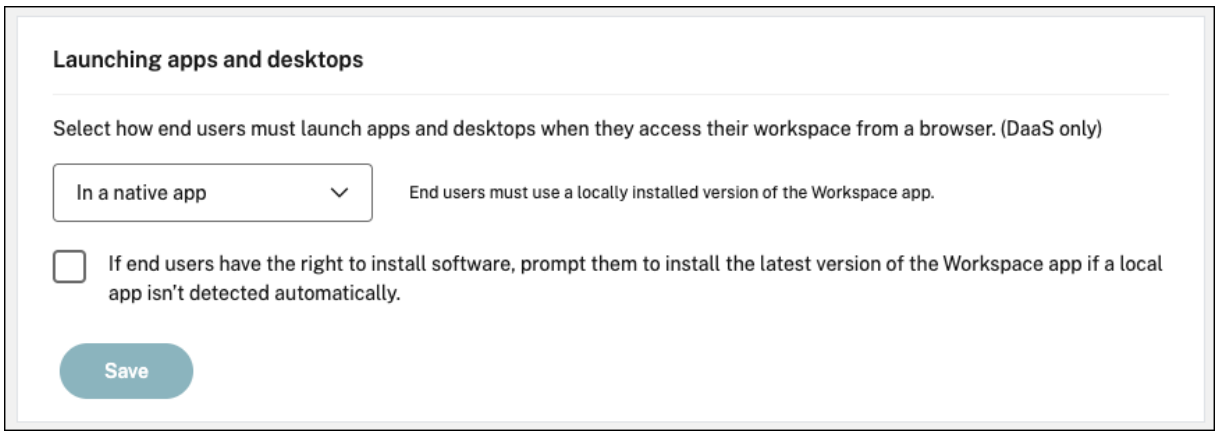


启动应用程序和桌面

有权访问 工作区配置 和新工作区体验的客户可以使用 启动应用程序和桌面 设置。新老客户均可享受此优惠。但是，此功能的引入不会改变现有客户的任何设置。

该偏好仅适用于用户打开由 **Citrix DaaS** 提供的应用程序和桌面的方式。这可以是 **Citrix DaaS** 服务，也可以是来自 站点聚合 功能的内部部署。启动应用程序和桌面 例如不适用于 Citrix Gateway 服务提供的 SaaS 应用程序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



选择下列设置之一：

- 在本机应用程序中（默认）：最终用户需要使用本地安装的 Workspace 应用程序版本。
- 在浏览器中：最终用户需要使用适用于 HTML5 的 Workspace 应用程序的浏览器版本。
- 让最终用户选择：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，或者在浏览器中启动应用程序和桌面。

的附加选项在本机应用程序 和 中让最终用户选择 会在未自动检测到本地应用程序时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，请删除此选项。

管理 **Workspace Web Extension** 的安装提示

Workspace 可以检测用户是否在其设备上安装了 Workspace Web Extension。如果没有，Workspace 会提示用户下载并安装该扩展。如果用户安装扩展程序，则不会显示工作区检测步骤。

要管理 Workspace Web Extension 的安装提示，请导航至 **Workspace Configuration** > **Customize** > **Preferences** > **Launching apps and desking**，然后选择以下设置之一：

- 提示最终用户下载 **Workspace Web Extension**，但如果未检测到则允许访问 **Workspace** （默认）：即使最终用户决定稍后安装 Workspace Web Extension，他们也可以使用 Workspace。
- 要求最终用户下载 **Workspace Web Extension** 并阻止对 **Workspace** 的访问，直到检测到：最终用户在安装 Workspace Web Extension 之前不得使用 Workspace。
- 不提示最终用户下载 **Workspace Web Extension**： Workspace 不提示最终用户安装 Workspace Web Extension。

固定链接

固定链接是客户定义的链接到特定网站的超链接。管理员可以根据自己的喜好在 Workspace UI 上设置固定链接。此功能可帮助用户只需单击管理员定义的固定链接即可轻松访问特定网站。固定链接需要显示名称和网站 URL。它还可以通过图标和描述进行个性化，其中描述提供有关链接的简要信息。

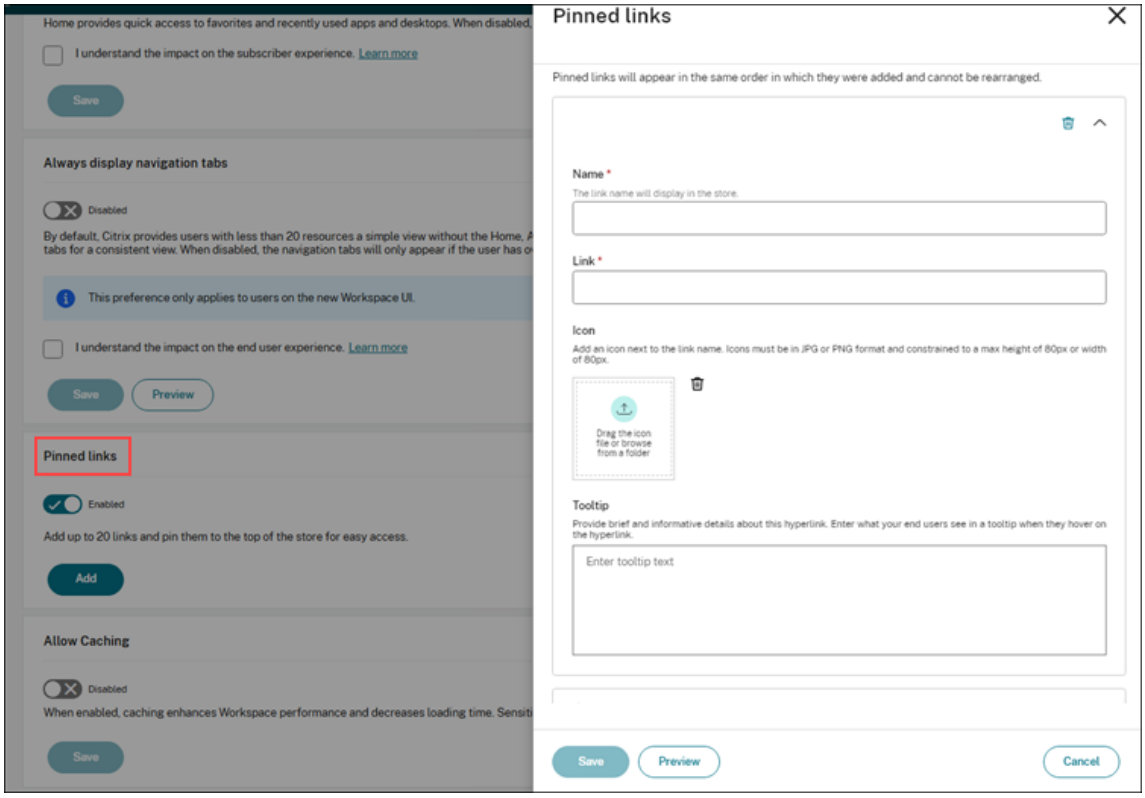
© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置

管理员可以使用他们的 Citrix Cloud 帐户在用户设备上管理此功能。

要启用此功能，请按照以下步骤进行操作：

1. 在 Citrix Cloud 帐户中导航到 工作区配置 > 自定义 > 首选项。
2. 在 固定链接下，切换按钮以启用该功能。此时将显示一个新窗口。



3. 在 名称 文本字段中，输入您想要固定在工作区 UI 上的链接的名称。
4. 在 链接 文本字段中，输入网站的 URL。
5. 在 图标下，如果您想在固定链接旁边显示一个图标，请附加一个图标。
6. 在 工具提示下，提供有关该网站的简短描述，当用户将鼠标悬停在固定链接上时会出现该描述。
7. 如果您想预览更改，请单击 预览。此操作是可选的。
8. 单击 保存 保存您的更改。

> 注意：
>
> 标有星号的字段是必填项。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

自定义安全和隐私政策

June 1, 2025

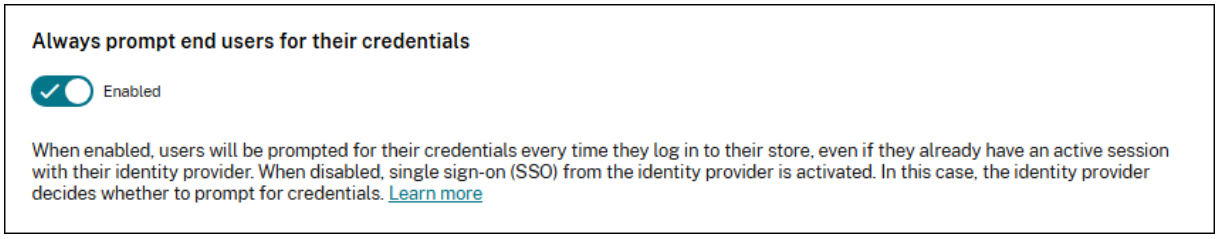
本文提供有关如何在配置完 Workspace 访问和身份验证后自定义登录体验的指导。

有关配置工作区访问和身份验证的概述，请访问 配置访问。有关如何配置工作区订阅者身份验证的信息，请访问 配置身份验证。

工作区会话

使用 工作区配置 **>** 自定义 **>** 首选项 中的 工作区会话设置 来选择用户何时需要输入其凭据以及用户保持登录状态的时间。更新设置后，按 保存 应用设置或按 恢复 取消设置。

始终提示最终用户输入其凭证

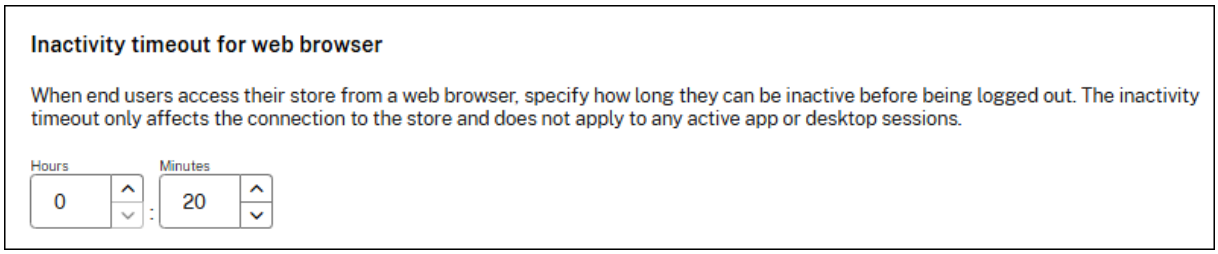


启用（默认）后，当需要新的 Workspace 会话时，Workspace 会强制向身份提供者发出登录提示。对于 OIDC 身份验证，Workspace 在身份验证请求中包含 `prompt=login` 。对于 SAML 身份验证，Workspace 在身份验证请求中发送 `ForceAuthn=true` 。

禁用时，如果身份提供者已经具有有效会话，则可能不会提示用户向身份提供者进行身份验证。

Web 浏览器不活动超时

使用 **Web** 浏览器不活动超时 设置来指定用户自动退出 Citrix Workspace 之前允许的空闲时间量（最多 8 小时）。只有与 Workspace 的交互（例如刷新页面或启动应用程序）才算活动。



与断开 DaaS 会话的手动注销不同，即使因不活动而超时，用户仍能保持与其 DaaS 会话的连接。用户未从其身份提供者中注销。因此，如果“始终提示最终用户输入其凭据”处于关闭状态，则用户可能无需输入其凭据即可重新登录。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

另请参阅 配置每个网络连接类型的超时。

Workspace 应用程序不活动超时

桌面　使用 **Workspace** 应用程序不活动超时 设置的 桌面 选项来指定在用户自动退出适用于 Windows、Mac 和 Linux 的 Citrix Workspace 应用程序之前允许的空闲时间量（最多 24 小时）。任何与鼠标或键盘的交互都算作活动并延长超时。

与手动注销（断开 DaaS 会话）不同，即使因不活动而超时，订阅者仍然保持与其 DaaS 会话的连接。

您可以使用 PowerShell 模块修改设置。使用 `Set-WorkspaceCustomConfiguration` cmdlet 和参数 `InactivityTimeoutInMinutes`。

另请参阅 配置每个网络连接类型的超时。

移动　使用 **Workspace** 应用程序不活动超时 设置的 移动 选项来指定 Citrix Workspace 应用程序锁定之前允许的空闲时间量（最多 24 小时）。这适用于适用于 iOS 和 Android 的 Citrix Workspace 应用程序。一旦锁定，用户必须使用生物识别技术或其设备 PIN 来解锁 Citrix Workspace 应用程序。如果设备上未启用生物识别技术，则用户将被注销。

您可以使用 PowerShell 模块修改设置。使用 `Set-WorkspaceCustomConfiguration` cmdlet 和参数 `InactivityTimeoutInMinutesMobile`。

另请参阅 配置每个网络连接类型的超时。

为每个网络连接类型配置超时

您可以根据用户是在您的内部网络、已知的外部网络还是其他任何地方，以不同的方式配置 Web、桌面和移动超时。例如，您可以为连接到内部网络的设备配置更短的超时时间。

要配置网络连接类型的超时：

1. 确保 Adaptive Access 已启用。
2. 根据用户的公共 IP 地址，定义 网络位置 代表您的内部位置和外部已知位置。如果用户的 IP 地址与网络位置不匹配，则其网络连接类型被视为未定义。
3. 从 Citrix Workspace PowerShell 模块，使用 `Internal`、`External` 或 `Undefined` 参数调用 `Set-StoreClientLocationConfiguration` cmdlet。参数值必须是一个哈希表，其键为 `inactivityTimeoutInMinutesWeb`、`inactivityTimeoutInMinutesDesktop` 或 `inactivityTimeoutInMinutesMobile`，值以分钟为单位给出时间。

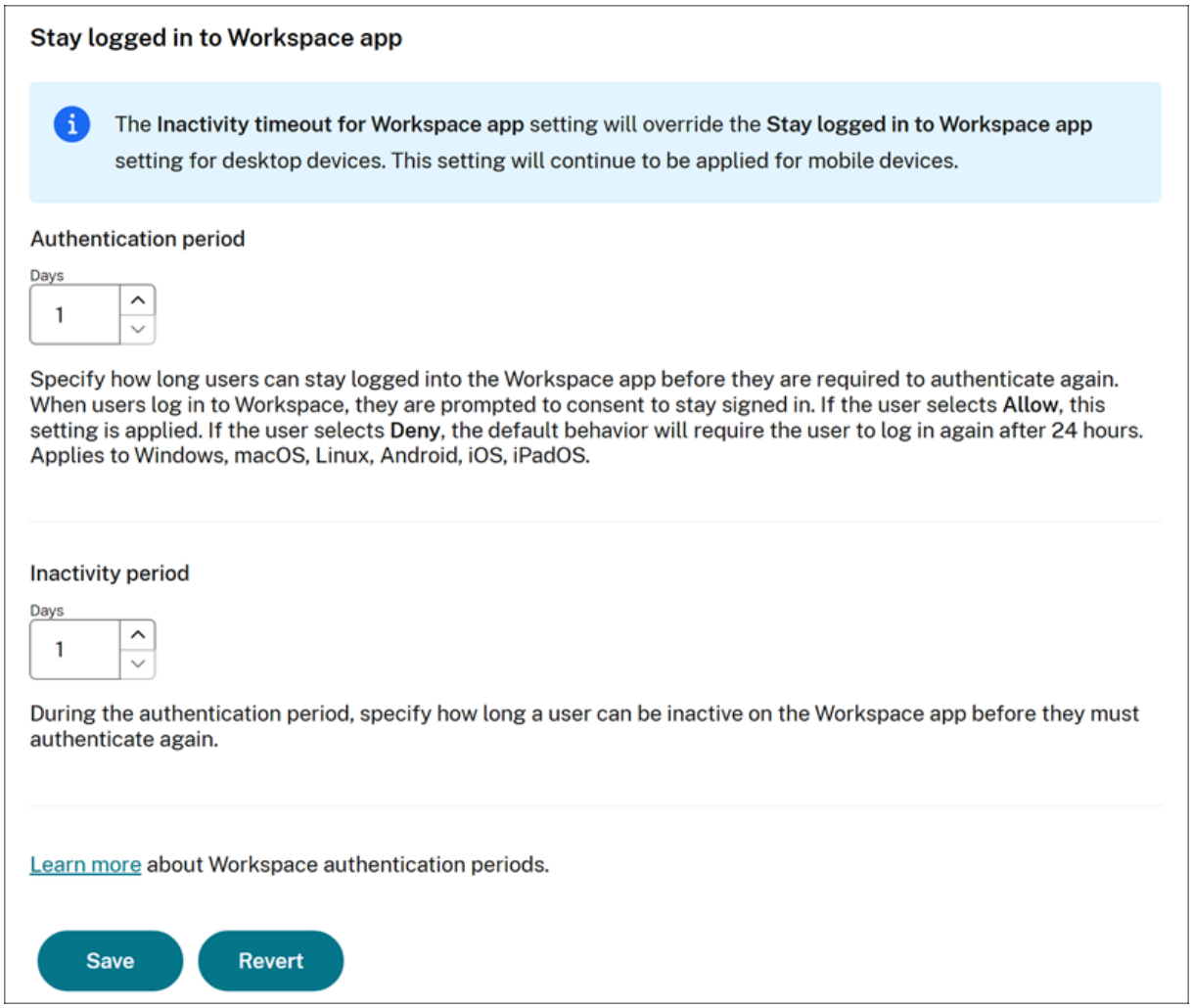
如果您没有为网络连接类型配置特定的超时，则将使用非位置特定的超时。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 重要：
>
> 如果用户设备移动到具有不同连接类型的网络，则新的超时不会立即应用。Citrix Workspace 应用程序每 90 分钟更新一次超时。如果使用网络浏览器，则超时会在用户下次刷新网页时更新。

保持登录到 **Workspace** 应用程序

使用 保持登录到 **Workspace** 应用程序 设置来指定用户在需要再次登录之前可以保持登录到 Citrix Workspace 应用程序的时间长度。这些设置不适用于网络浏览器。



认证期限 定义了用户必须重新认证之前的最长时间。默认情况下，该值设置为 30 天，但您可以配置 1 到 365 天之间的值。如果期限超过 1 天，则用户在进行身份验证时必须同意保持登录状态。

不活动期 定义了用户在必须重新认证之前可以处于不活动状态的时间。默认情况下为 4 天，但您可以将其配置为 1 天到重新认证期之间的值。如果用户处于不活动状态的时间超过此值，则下次尝试访问其工作区时，系统将提示他们重新进行身份验证。要在桌面上设置少于 24 小时的不活动时间，请使用 工作区应用程序不活动超时 设置的 桌面 选项。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

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：

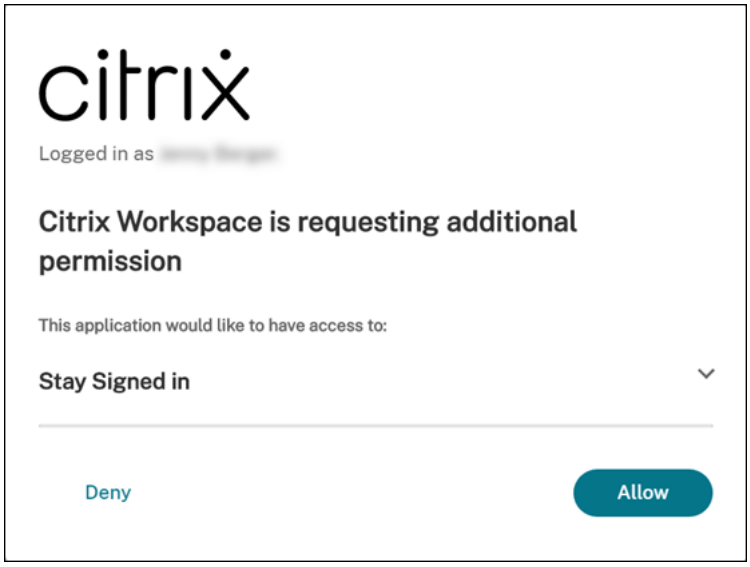
- 适用于 Windows 的 Workspace 应用程序 2106 或更高版本
- 适用于 Mac 的 Workspace 应用程序 2106 或更高版本
- 适用于 iOS 的 Workspace 应用程序 21.6.5 或更高版本
- 适用于 Android 的 Workspace 应用程序 21.6.0 或更高版本

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
- 恩特拉身份证
- 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 选项时，他们会在重新认证期间保持登录状态。如果在配置的天数内未在订阅者的设备上检测到任何活动，则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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

和桌面，重新身份验证期限就会一直有效。

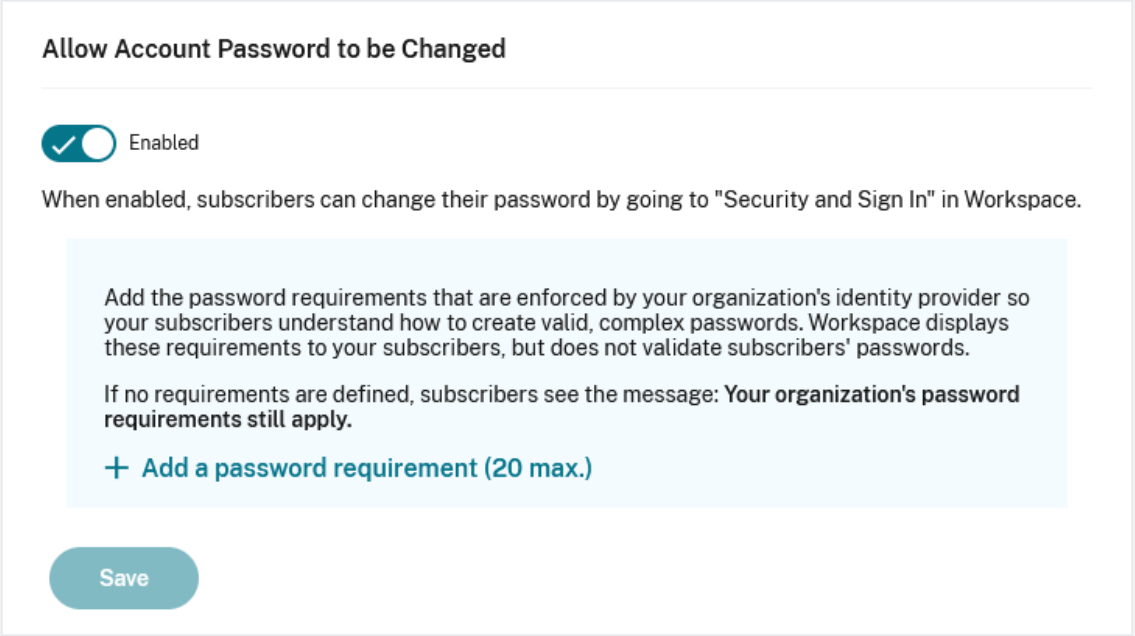
如果订阅者选择 拒绝，系统可能会提示用户再次登录。之后，Workspace 会提示订阅者在 24 小时后再次登录。

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。

允许最终用户更改其帐户密码

如果您使用 Active Directory 或 Active Directory (AD) 加令牌身份验证，那么您可以选择用户是否可以更改其密码。启用后（默认），用户可以根据组织的 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 Citrix Workspace 内更改未过期的密码。要配置此项：

1. 导航到 **Workspace** 配置 **>** 自定义 **>** 首选项。
2. 转到部分 允许更改帐户密码。
3. 切换 启用。



4. 按 保存 保存任何更改。

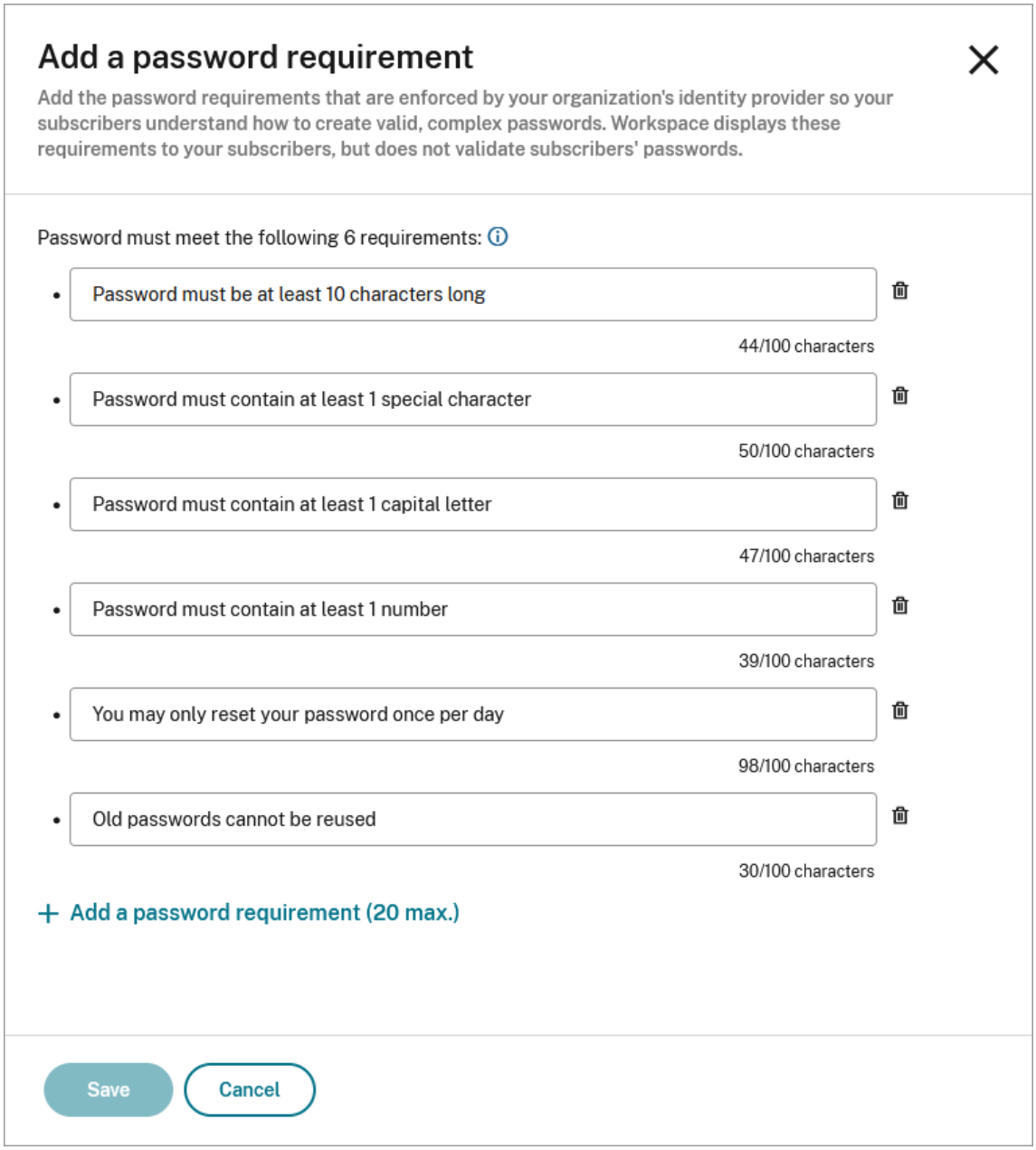
您最多可以添加 20 个密码要求，以满足贵组织的安全策略并由身份提供商强制执行。当订阅者从 Workspace 的“帐户设置”页面更改密码时，Workspace 会将这些要求显示为指南。如果您未添加任何密码要求，Workspace 会显示消息“您所在组织的密码要求仍然适用。”

要添加密码要求，请执行以下操作：

1. 如果当前没有密码要求，请选择 添加密码要求。如果已经至少有一个密码要求，则选择 编辑。

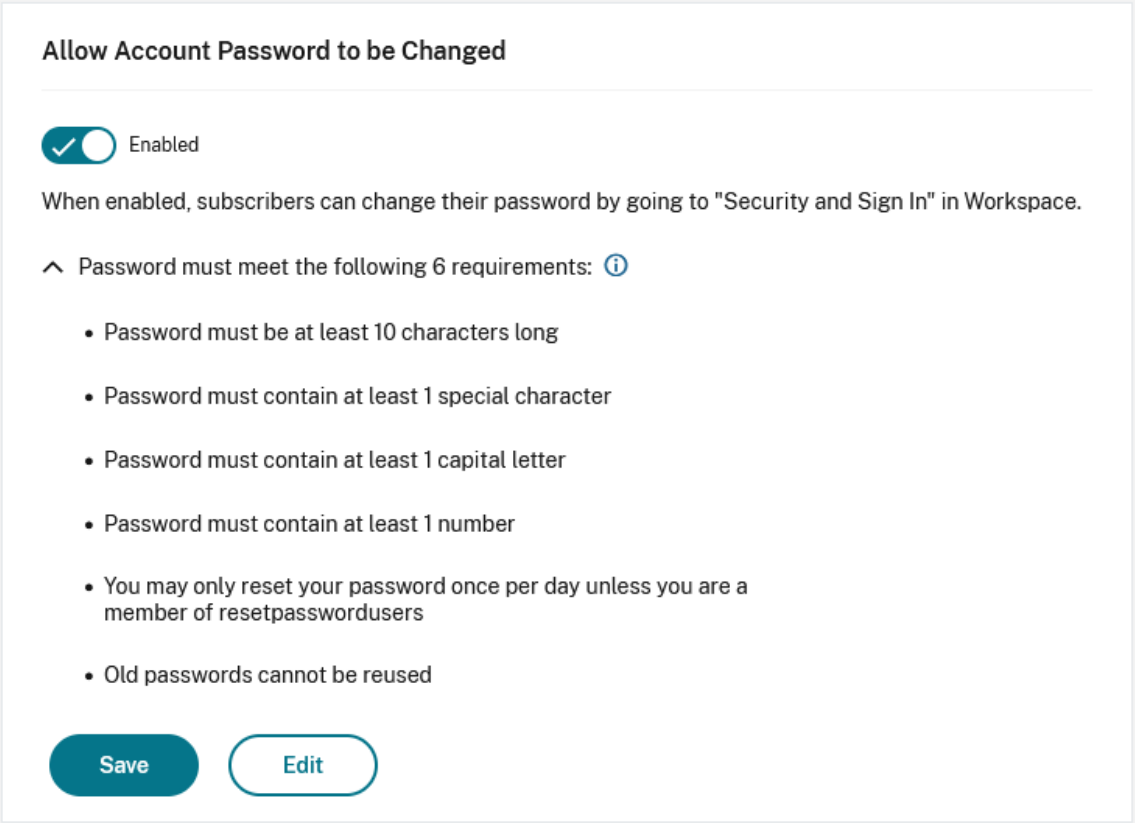
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. 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。



3. 添加完需求后，选择 保存。您可以扩展需求列表：

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. 再次选择“保存”以保存所有设置更改。

支持的 **Citrix 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 2101 或更高版本的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序 2012 或更高版本
- 适用于 Chrome 2010 或更高版本的 Citrix Workspace 应用程序
- 适用于 HTML5 2101 或更高版本的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序 21.1.0 或更高版本

订阅者从 Web 浏览器访问工作区时也可以使用此功能。

以下设备不支持此功能：

- 旧版本的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序

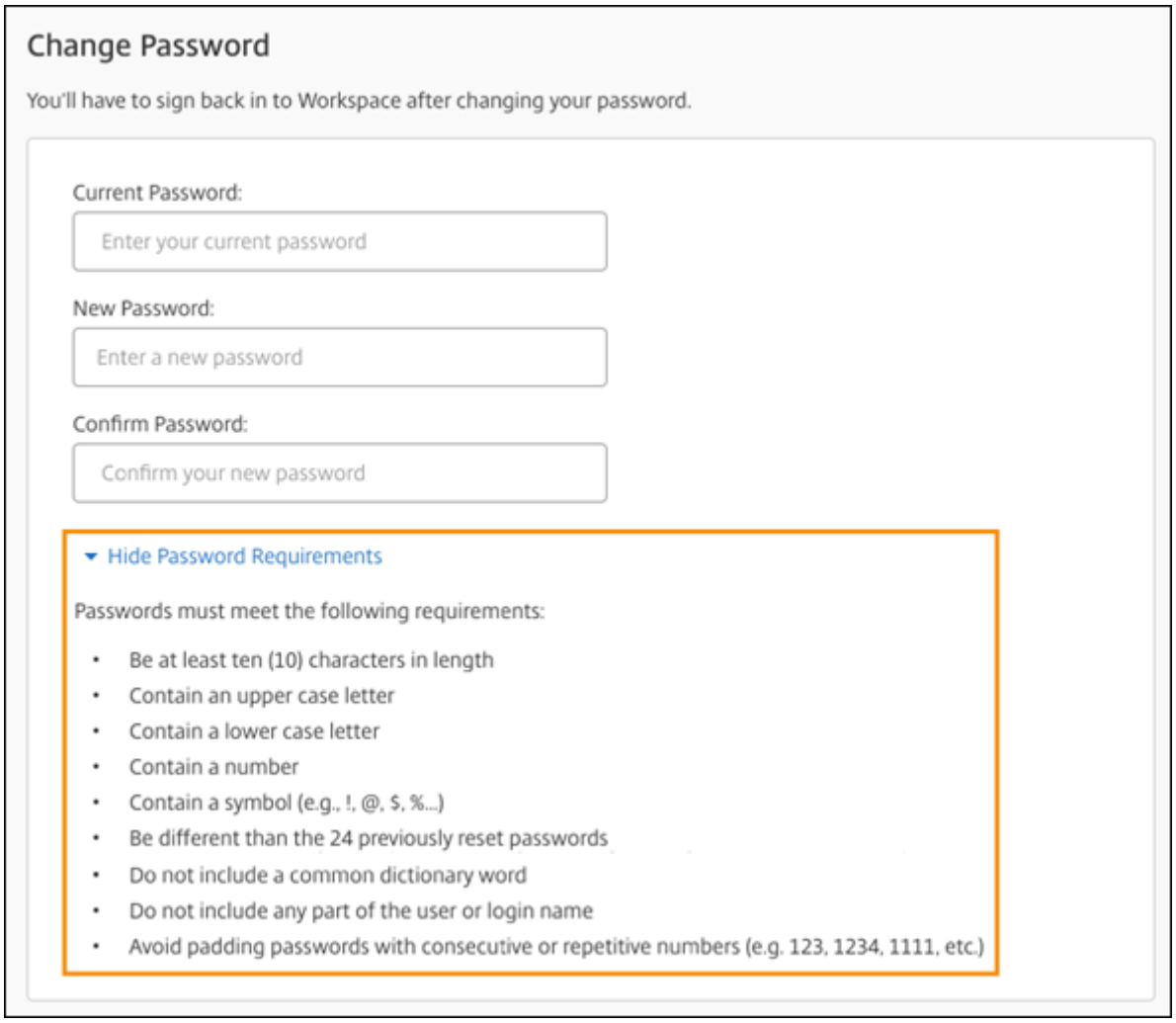
更改密码时的最终用户体验

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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 pdf 文件 获取可包含在您自己的通信和知识库文章中的说明。

当启用 允许更改帐户密码 时，最终用户可以通过转到 帐户设置 **>** 安全 **&** 登录在工作区中更改他们的密码。

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



用户更改密码后会自动注销，必须使用新密码重新登录。

发送自定义公告

您可以在给定的时间段内向用户发送自定义公告，例如通知他们即将进行的维护。您可以为每个工作区配置默认公告以及覆盖。每个工作区只能配置一个公告。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

添加公告

1. 导航到 工作区配置 **>** 自定义 **>** 首选项 **>** 发送自定义公告。
2. 要添加适用于没有活动覆盖的工作区的公告，请选择 添加默认通知。要为特定工作区添加公告，请选择 添加覆盖通知。
3. 如果您添加了覆盖公告，请选择适用该公告的工作区。这不适用于默认公告。
4. 输入 公告标题。
5. 输入 描述文本。
6. 输入公告出现的时间段。
7. 选择将公告放在顶部还是底部。
8. 要查看您的消息如何显示给用户，请选择 预览。
9. 完成后，选择“保存”。

删除公告

1. 在包含公告的行中，选择 …打开菜单，然后选择 删除。
2. 在确认窗口中，选择 删除。

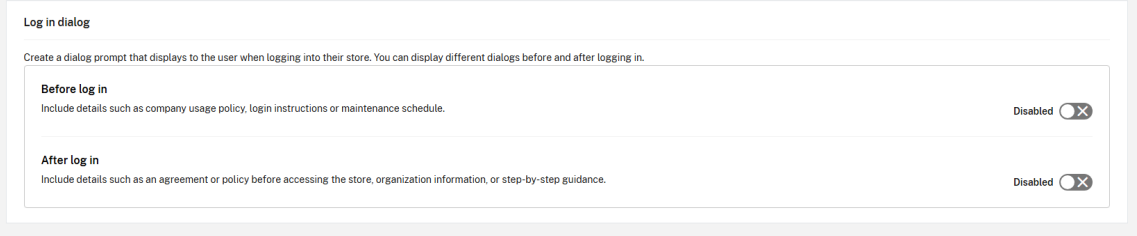
编辑公告

1. 在包含公告的行中，选择 …打开菜单，然后选择 编辑。
2. 根据需要进行更改。
3. 选择 保存。

配置登录前显示的自定义对话框

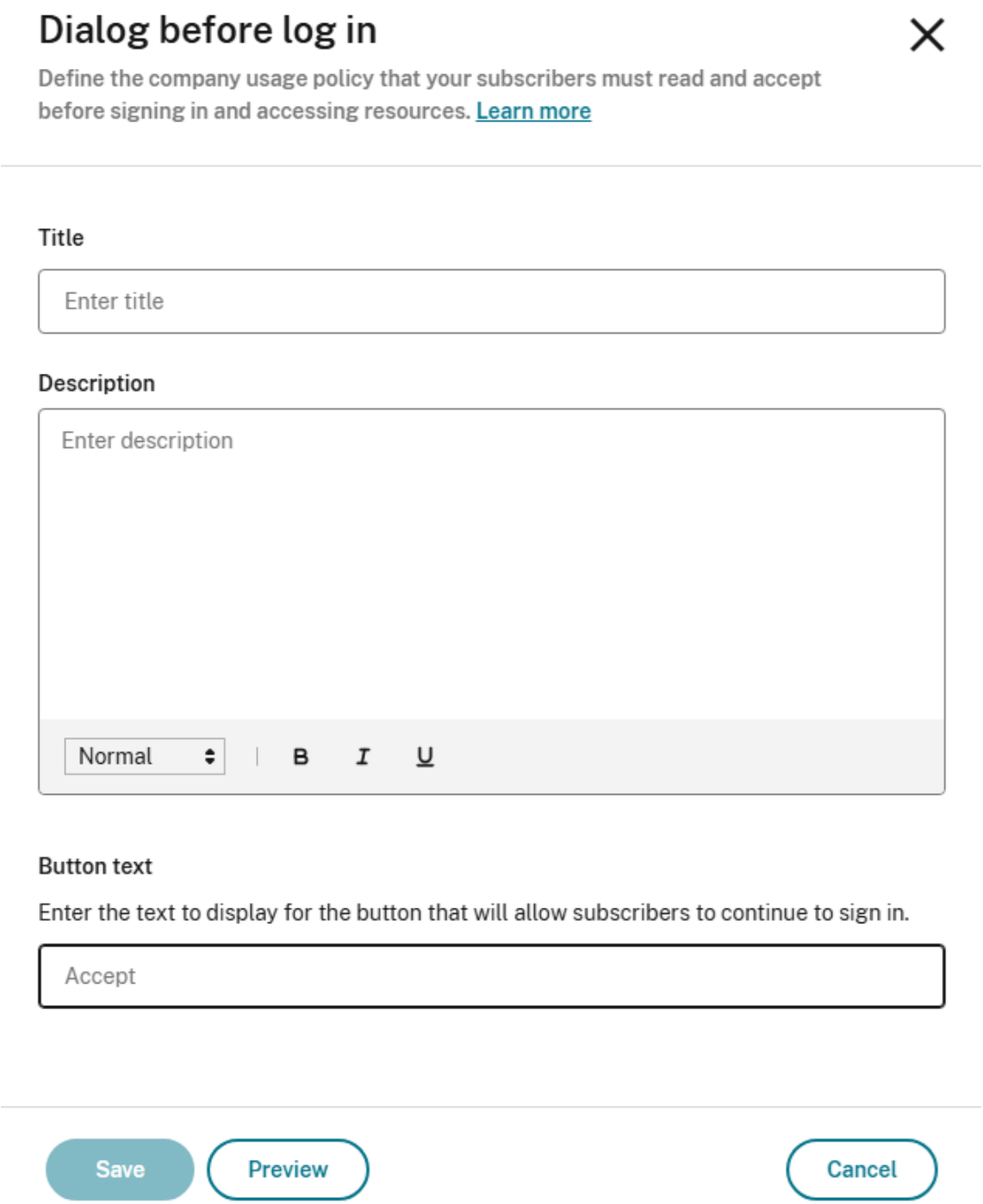
创建在用户登录前显示的自定义对话框。它显示在所有客户端上，包括网络、桌面和移动设备。您可以使用它来显示公司使用政策或即将到来的维护窗口等信息。用户必须接受该对话框才能进入登录屏幕。

1. 从 **Citrix Cloud** 菜单中，选择 **Workspace** 配置 **>** 自定义 **>** 首选项。
2. 导航到 登录对话框 部分。
3. 如果未启用，请选择标有 的切换按钮，登录前。如果已经启用，请单击 编辑 按钮。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

4. 将出现一个配置对话框。
5. 输入对话框的 标题。
6. 输入要在对话框中显示的 描述。无法本地化文本，但是您可以在描述中添加多种不同的语言。
7. 输入 按钮文本。用户必须按下此按钮才能继续。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. 选择 预览 查看对话框对于最终用户的外观。
9. 完成后，选择“保存”。

> 注意：
>
> 如果您已将 Citrix Gateway 配置为您的 Workspace 身份提供程序，则您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，可以作为现有 nFactor 身份验证流程的一部分，也可以使用 Citrix Cloud 管理控制台在流程之外配置。

配置登录后显示的自定义对话框

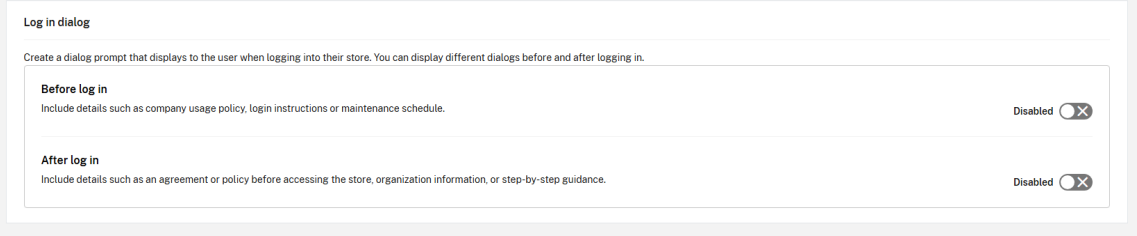
您可以配置用户登录后显示的自定义对话框。它显示在所有客户端上，包括网络、桌面和移动设备。您可以使用它来显示公司使用政策或即将到来的维护窗口等信息。用户必须接受该对话框才能继续使用其资源。

管理员可以决定每个设备显示对话框的频率，即仅显示一次、每天显示一次、每 7 天显示一次或每 30 天显示一次。

> 注意：
>
> 当用户清除缓存和 cookie 时，对话框会再次出现。

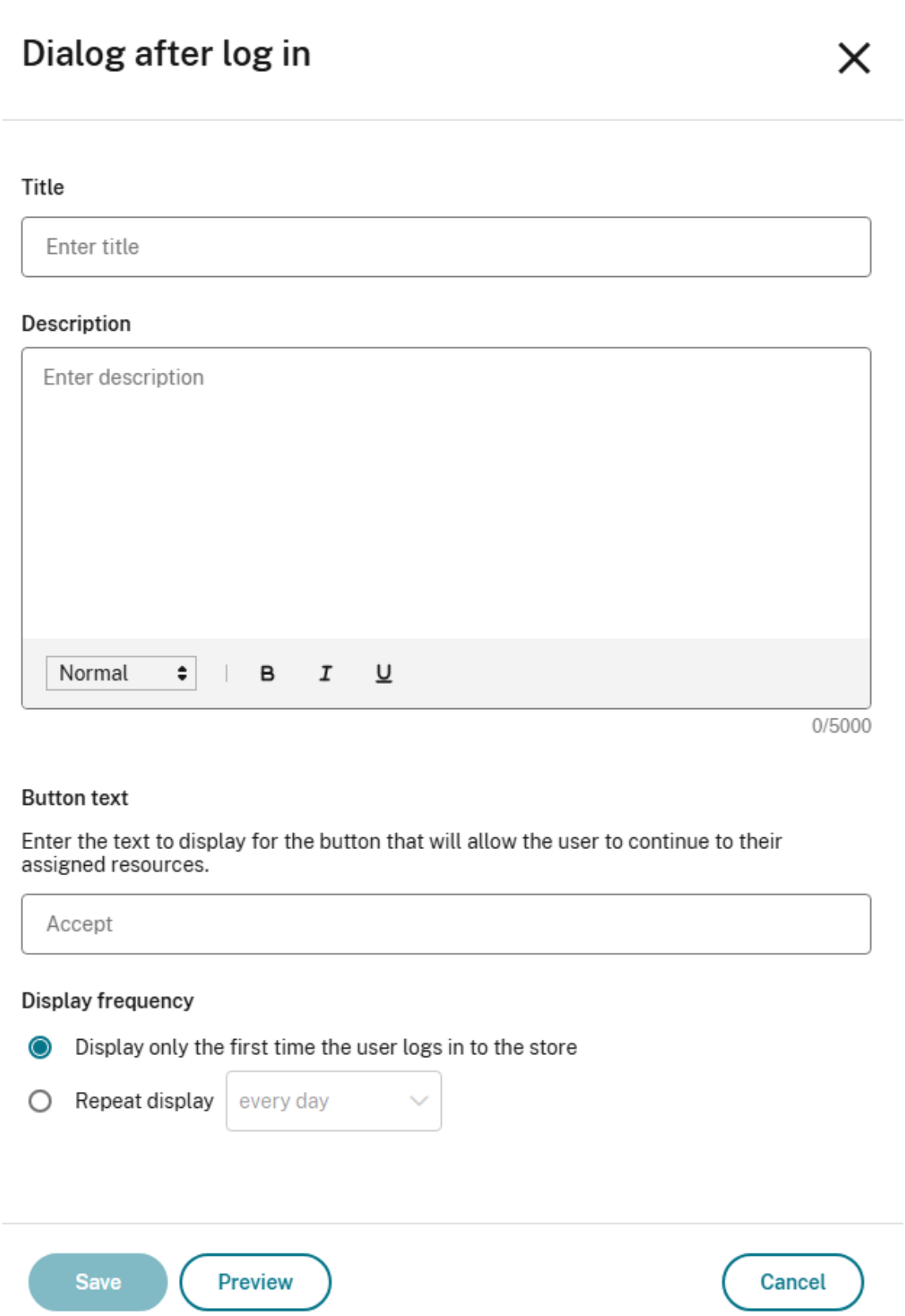
1. 从 **Citrix Cloud** 菜单中，选择 **Workspace Configuration** > **Custom** > **Preferences**。
2. 导航到 登录对话框 部分。
3. 如果未启用，请选择标有 的切换按钮，登录后 即可启用。如果已经启用，请单击 编辑 按钮。

   出现配置对话框。



4. 输入对话框的 标题。
5. 输入要在对话框中显示的 描述。无法本地化文本。但是，您可以在描述中附加多种不同的语言。
6. 输入 按钮文本。用户必须按下此按钮才能继续。
7. 输入显示频率选项，以确定每个用户看到对话框的频率。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



© 1997–2025 Citrix Systems, Inc. All rights reserved.

8. 选择 预览 查看对话框对于最终用户的外观。
9. 自我审查后，选择 保存。

自定义商店访问

November 7, 2024

管理员可以选择是否要求最终用户通过 Citrix Workspace 应用程序或第三方 Web 浏览器 (HTML5)（例如 Chrome、Safari、Firefox 和 Edge）进行身份验证和访问其商店。

如果最终用户通过第三方浏览器访问应用程序和桌面，您还可以决定虚拟 Web 和 SaaS 应用程序和桌面的打开位置。管理员可以定义应用程序和桌面是否始终在浏览器（HTML5）或本机应用程序中打开。在这种情况下，如果您希望用户使用本机应用程序，请确保他们已安装 Citrix Workspace Web 扩展。

要求最终用户通过本机应用程序进行身份验证并访问应用程序和桌面

> 注意：
>
> 默认情况下，此功能处于禁用状态。要启用此功能，管理员必须通过 Citrix Cloud 配置此功能。有关更多信息，请参阅 配置。

在用户设备上强制使用本机 Citrix Workspace 应用程序意味着限制最终用户只能登录并使用本地安装的 Citrix Workspace 应用程序。这样一来，最终用户就无法通过浏览器访问 Citrix Workspace Web 客户端，除非通过 Citrix Enterprise Browser。此功能专为想要充分利用原生应用优势的客户而设计。

本机 Citrix Workspace 应用程序具有以下优势：

- 增强安全性 因为它不需要下载 `.ica` 文件。
- 增强了打开应用程序和桌面的可靠性，因为它不依赖于客户端检测。
- 内置应用程序保护服务 提供了额外的安全层，以防止键盘记录和屏幕捕获恶意软件。
- **Citrix Workspace Web** 扩展上没有依赖。
- 没有浏览器兼容性检查。由于本机应用程序不依赖于浏览器，因此需要进行浏览器兼容性检查，这与 Workspace Web 客户端不同。
- 更好的遥测 因为本机应用程序提供了用于监控目的的大量信息。
- 增强的 **HDX** 功能 具有优化编解码器压缩和高效音频视频压缩等增强功能。这些改进为涉及高清内容或图形密集型应用的任务提供了高质量和性能。

支持的平台

支持所有平台，例如 Windows、Mac、Linux、ChromeOS、Android 和 iOS。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 注意：
>
> Linux 和 ChromeOS 平台不支持自动商店添加，而 Windows 和 Mac 平台则有版本要求。在这种情况下，用户需要在原生应用中手动添加商店网址。有关更多信息，请参阅 手动存储添加。

配置

管理员可以使用他们的 Citrix Cloud 帐户强制用户设备上使用本机 Citrix Workspace 应用程序。要管理此功能，请按照以下步骤操作：

1. 在 Citrix Cloud 中导航到 工作区配置 > 自定义 > 首选项。
2. 在 商店访问下，选择 要求最终用户从 **Citrix** 客户端应用程序访问他们的商店。

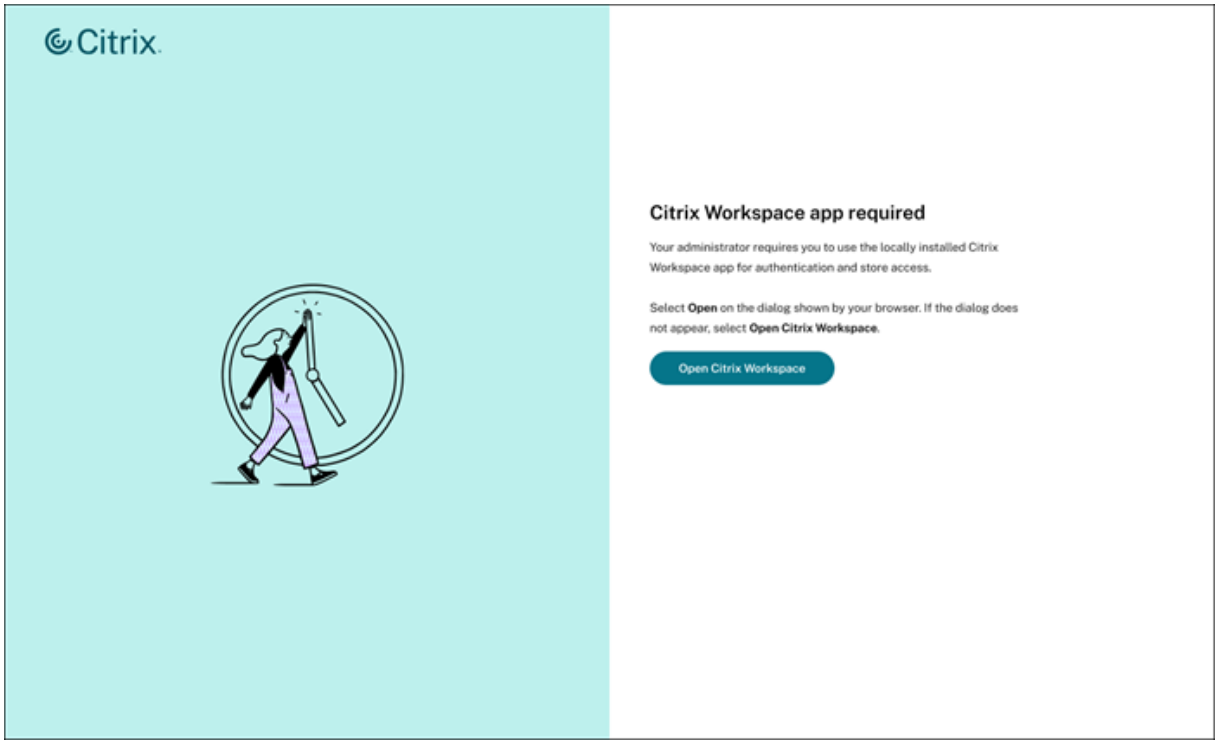
   [可选] 选择 提示最终用户下载 **Citrix Workspace** 应用程序，以提示用户下载 Citrix Workspace 应用程序（如果用户尚未在其设备上安装该应用程序）。有关更多信息，请参阅 为最终用户配置原生应用下载链接。

3. 单击 保存 保存更改，或单击 恢复 放弃更改。

最终用户体验

第一阶段。本机应用程序授权　一旦管理员强制执行本机应用程序，最终用户就无法在浏览器中使用 Citrix Workspace Web 客户端。当用户尝试通过在浏览器中输入商店 URL 来访问 Web 客户端时，他们会看到以下网页，提示打开原生应用程序。

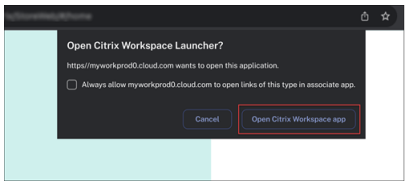
© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. 单击 打开 **Citrix Workspace**。

   客户端检测过程启动，检查 Citrix Workspace 应用程序是否在用户设备本地安装。

   出现 打开 **Citrix Workspace Launcher** 提示，要求用户打开本机应用程序。

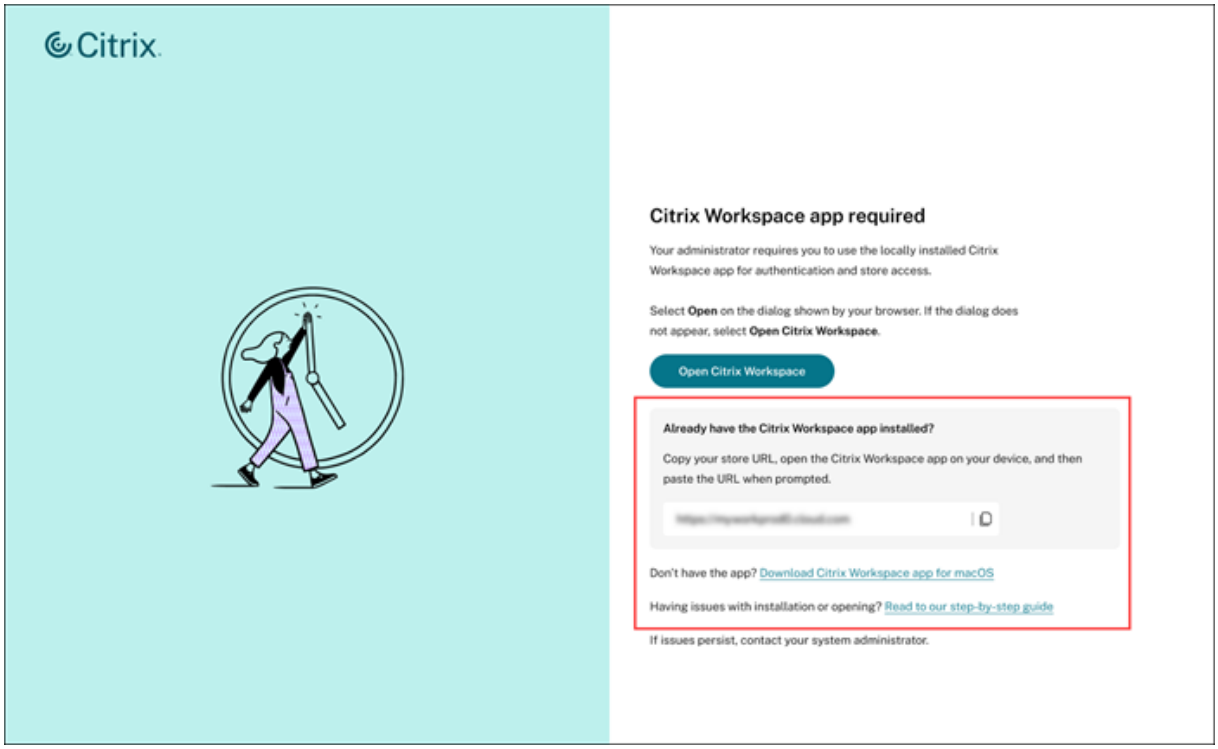
   

2. 单击 打开 **Citrix Workspace** 应用程序。

如果用户没有看到提示或没有在 5 秒内单击提示上的“打开 **Citrix Workspace** 应用程序”，则网页会提供以下额外选项以继续：

- 在本机 Citrix Workspace 应用程序中手动复制和添加的商店 URL。
- 用于安装 Citrix Workspace 应用程序的下载链接。此链接的行为取决于管理员如何配置它。有关更多信息，请参阅 配置。
- 最终用户指南的链接，其中提供了安装和打开 Citrix Workspace 应用程序的分步说明。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



> 注意：
>
> 如果用户在 iPad 上使用 Safari 浏览器，则浏览器无法将其与 Mac 桌面区分。因此，用户必须单击 我在 **iPad** 上 链接才能继续自动添加商店。
>
> Linux 和 ChromeOS 不支持自动商店添加。因此，这些设备上不会出现 打开 **Citrix Workspace Launcher** 提示。在这种情况下，用户需要在原生应用中手动添加商店网址。有关更多信息，请参阅 手动存储添加。

第二阶段：增加商店

自动添加商店　Citrix Workspace 应用程序的兼容版本

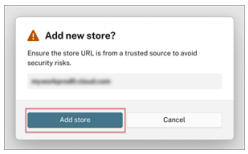
以下是支持自动存储添加的兼容 Citrix Workspace 应用程序版本：

操作系统	兼容版本
Windows	24.9.0 或更高版本
Mac	24.5.0 或更高版本
Android 和 iOS	24.9.0 或更高版本

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序 24.5.0 版支持在预览模式下自动添加存储，默认情况下此功能处于禁用状态。要启用该实用程序：
>
> 1. 启动注册表编辑器。
> 2. 导航到 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ Citrix\Dazzle` 注册表路径。
> 3. 创建具有以下属性的注册表值：
> - 注册表项名称：`GoNativeForCloudEnabled`
> - 类型：字符串值
> - 值：`True`
> 4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

一旦用户单击 打开 **Citrix Workspace** 应用程序，就会出现以下对话框，请求用户确认将商店 URL 添加到本机应用程序。

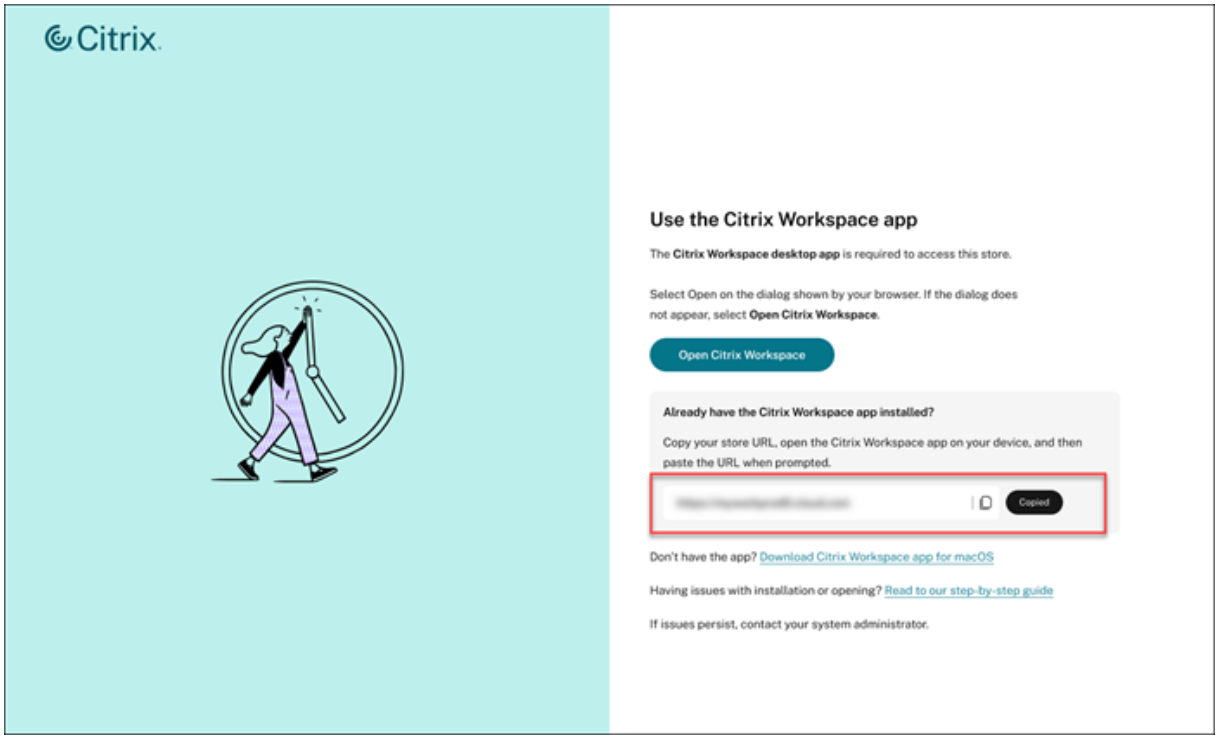


点击 添加商店。

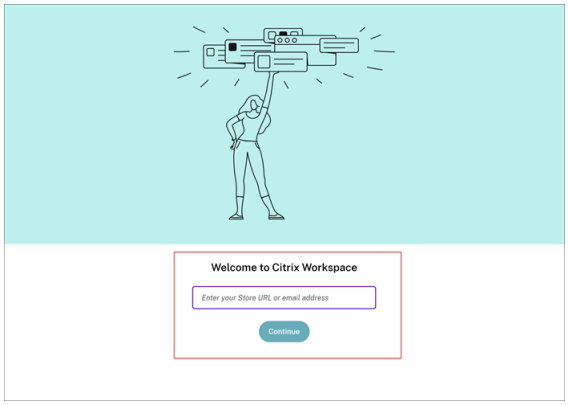
一旦点击，原生应用会自动捕获浏览器中输入的商店 URL，并显示用户登录的身份验证页面。身份验证成功后，用户可以看到本机 Citrix Workspace 应用程序的主页。

手动添加商店　如果用户单击 添加商店 选项时本机应用程序没有自动捕获商店 URL，则可以手动将商店添加到 Citrix Workspace 应用程序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



1. 从本机授权网页复制商店 URL，然后将其粘贴到 欢迎使用 **Citrix Workspace** 页面中。



2. 单击继续。

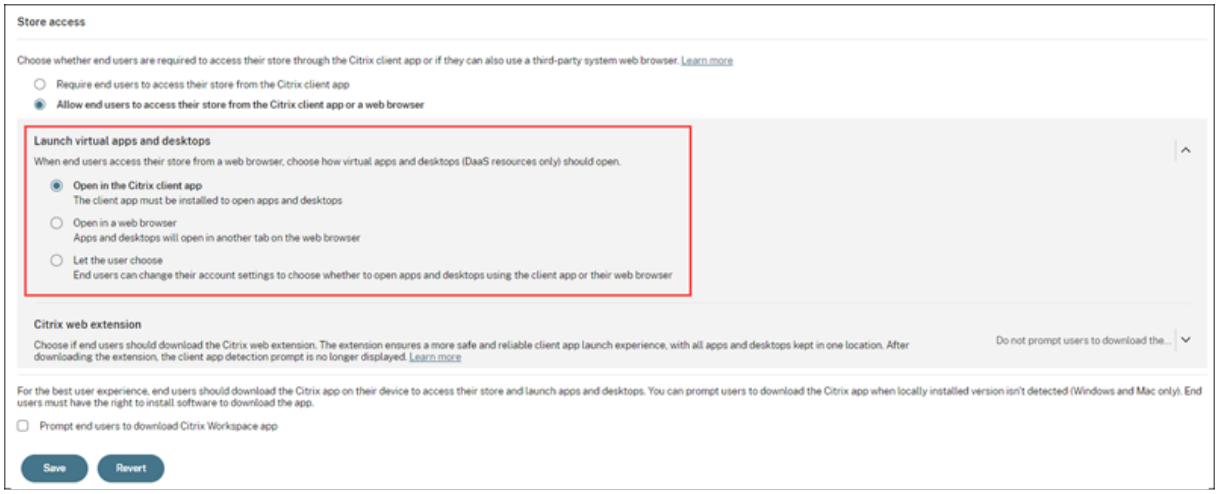
提交有效的商店 URL 后，Citrix Workspace 应用程序将显示供用户登录的身份验证页面。身份验证成功后，用户可以看到本机 Citrix Workspace 应用程序的主页。

启动虚拟应用程序和桌面

如果管理员不愿意强制使用本机应用程序进行身份验证和访问应用程序和桌面，您可以允许最终用户通过第三方 Web 浏览器进行身份验证和访问其商店，并使用 Web 浏览器（HTML5）或本机应用程序打开应用程序和桌面。

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，也可以是来自站点聚合 功能的内部部署。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



要管理此功能，请按照以下步骤操作：

1. 在 Citrix Cloud 中导航到 工作区配置 > 自定义 > 首选项。
2. 在 商店访问下，选择 允许最终用户从 **Citrix** 客户端应用程序或 **Web** 浏览器访问他们的商店 并选择适当的设置：
   - 在 **Citrix** 客户端应用程序中打开：有关更多信息，请参阅 在浏览器中进行身份验证并在本机应用程序中访问应用程序和桌面。
   - 在网络浏览器中打开：有关更多信息，请参阅 在浏览器中验证和访问应用程序和桌面（HTML5）。
   - 让用户选择：有关更多信息，请参阅 最终用户可以选择本机应用程序或浏览器。

在浏览器中进行身份验证并在本机应用程序中访问应用程序和桌面

管理员可以允许最终用户从 Web 浏览器进行身份验证并访问他们的商店，并且仅使用本机应用程序打开应用程序和桌面。要管理此功能，请按照以下步骤操作：

1. 导航到 存储访问。
2. 在 启动虚拟应用程序和桌面下，单击 在 **Citrix** 客户端应用程序中打开。

   [可选] 选择 提示最终用户下载 **Citrix Workspace** 应用程序，以提示用户下载 Citrix Workspace 应用程序（如果用户尚未在其设备上安装该应用程序）。有关更多信息，请参阅 为最终用户配置原生应用下载链接。
3. 单击 保存 保存更改。

在浏览器中验证并访问应用程序和桌面 (HTML5)

管理员可以允许最终用户从 Web 浏览器进行身份验证和访问他们的商店，并使用 Web 浏览器 (HTML5) 打开应用程序和桌面。

1. 导航到 存储访问。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. 在 启动虚拟应用程序和桌面下，单击 在 **Web** 浏览器中打开。

   [可选] 选择 提示最终用户下载 **Citrix Workspace** 应用程序，以提示用户下载 Citrix Workspace 应用程序（如果用户尚未在其设备上安装该应用程序）。有关更多信息，请参阅 为最终用户配置原生应用下载链接。

3. 单击 保存 保存更改。

Citrix Virtual Apps 和 Desktops 提供的资源聚集在商店中，并通过 Citrix Workspace 应用程序在网站上提供。在网站上启用适用于 HTML5 的 Citrix Workspace 应用程序后，用户可以在其 Web 浏览器中访问应用程序和桌面。有关更多信息，请参阅 适用于 ChromeOS 的 Citrix Workspace 应用程序 产品文档。

> 注意：
>
> **Citrix Web** 扩展 设置不适用于 在 **Citrix** 客户端应用程序中打开 选项。

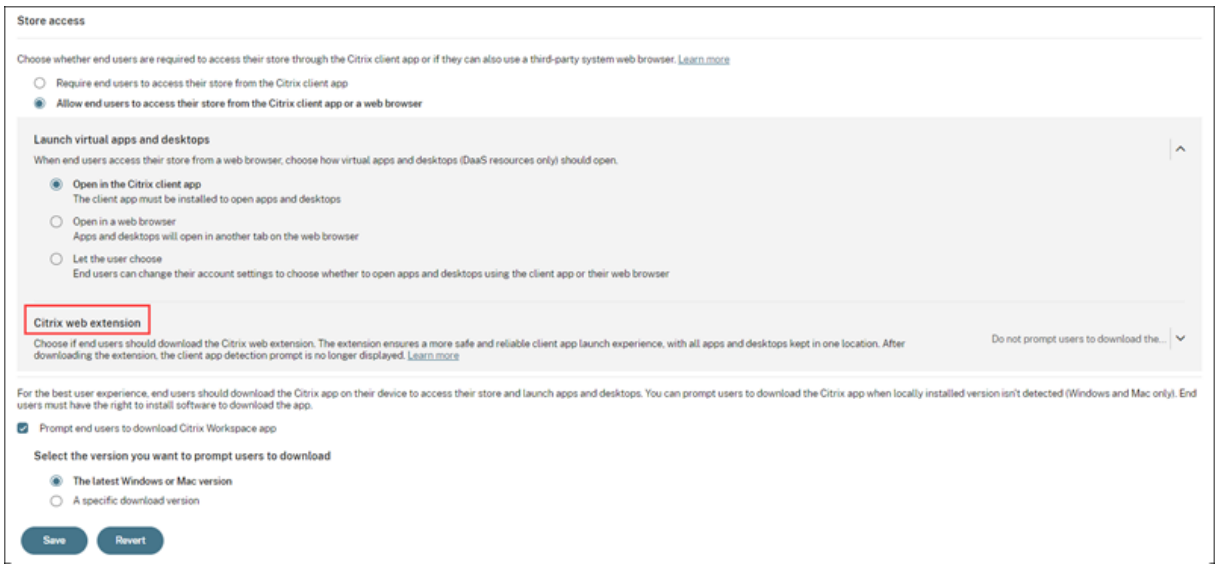
最终用户可以选择本机应用程序或浏览器

管理员可以允许用户从 Web 浏览器（HTML5）进行身份验证和访问商店，并使用浏览器或本机应用程序打开应用程序和桌面。

1. 导航到 存储访问。
2. 在 启动虚拟应用程序和桌面下，单击 让用户选择。[可选] 选择 提示最终用户下载 **Citrix Workspace** 应用程序，以提示用户下载 Citrix Workspace 应用程序（如果用户尚未在其设备上安装该应用程序）。有关更多信息，请参阅 为最终用户配置原生应用下载链接。
3. 单击 保存 保存更改。

管理 **Citrix Workspace Web** 扩展的安装提示

Workspace 可以检测用户是否在其设备上安装了 Workspace Web Extension。如果没有，Workspace 会提示用户下载并安装该扩展。如果用户安装扩展程序，则不会显示工作区检测步骤。



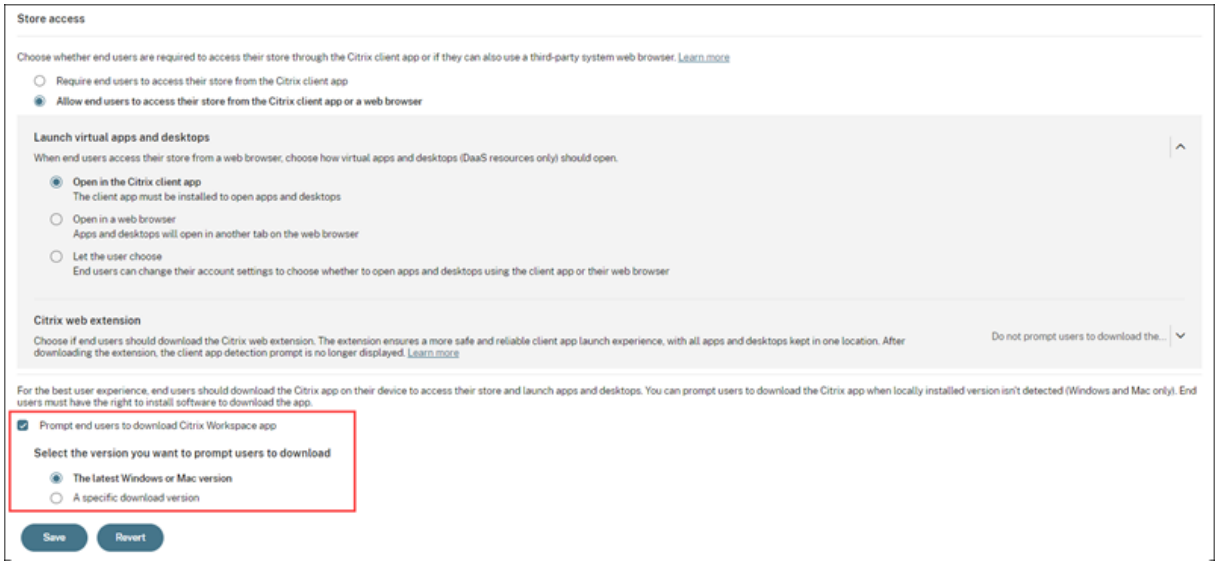
© 1997–2025 Citrix Systems, Inc. All rights reserved.

要管理 Workspace Web Extension 的安装提示，请导航至 **Workspace Configuration** > **Customize** > **Preferences** > **Launching apps and desking**，然后选择以下设置之一：

- 提示最终用户下载 **Workspace Web Extension**，但如果未检测到则允许访问 **Workspace** （默认）：即使最终用户决定稍后安装 Workspace Web Extension，他们也可以使用 Workspace。
- 要求最终用户下载 **Workspace Web Extension** 并阻止对 **Workspace** 的访问，直到检测到：最终用户在安装 Workspace Web Extension 之前不得使用 Workspace。
- 不提示最终用户下载 **Workspace Web Extension**： Workspace 不提示最终用户安装 Workspace Web Extension。

为最终用户配置本机应用下载链接

如果最终用户的设备上尚未安装 Citrix Workspace 应用程序，管理员可以提示最终用户下载该应用程序。



选择以下任一选项：

- 最新的 **Windows** 或 **Mac** 版本：提示用户在其设备上下载最新版本的 Citrix Workspace 应用程序。当用户点击下载链接时，他们会被重定向到相应的下载页面。

> 注意：
>
> 对于运行 Linux 的设备，当用户单击下载链接时，它会打开 Citrix 下载页面，用户可以在其中手动下载可执行文件。对于 ChromeOS、Android 和 iOS 设备，下载链接会分别将用户重定向到 Chrome 网上应用店、Play Store 和 App Store。

- 特定下载版本：在 下载 **URL** 文本字段中，提供您希望用户下载的 Citrix Workspace 应用程序版本的 URL。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 注意：
>
> 管理员需要根据用户设备的操作系统提供特定版本的 Citrix Workspace 应用程序的下载 URL。如果有用户同时拥有 Windows 和 Mac 设备，管理员可以提供一个指向 Citrix Workspace 应用程序下载页面的通用链接，而不是仅提供一个操作系统的 URL。

将服务集成到工作区

November 7, 2024

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。

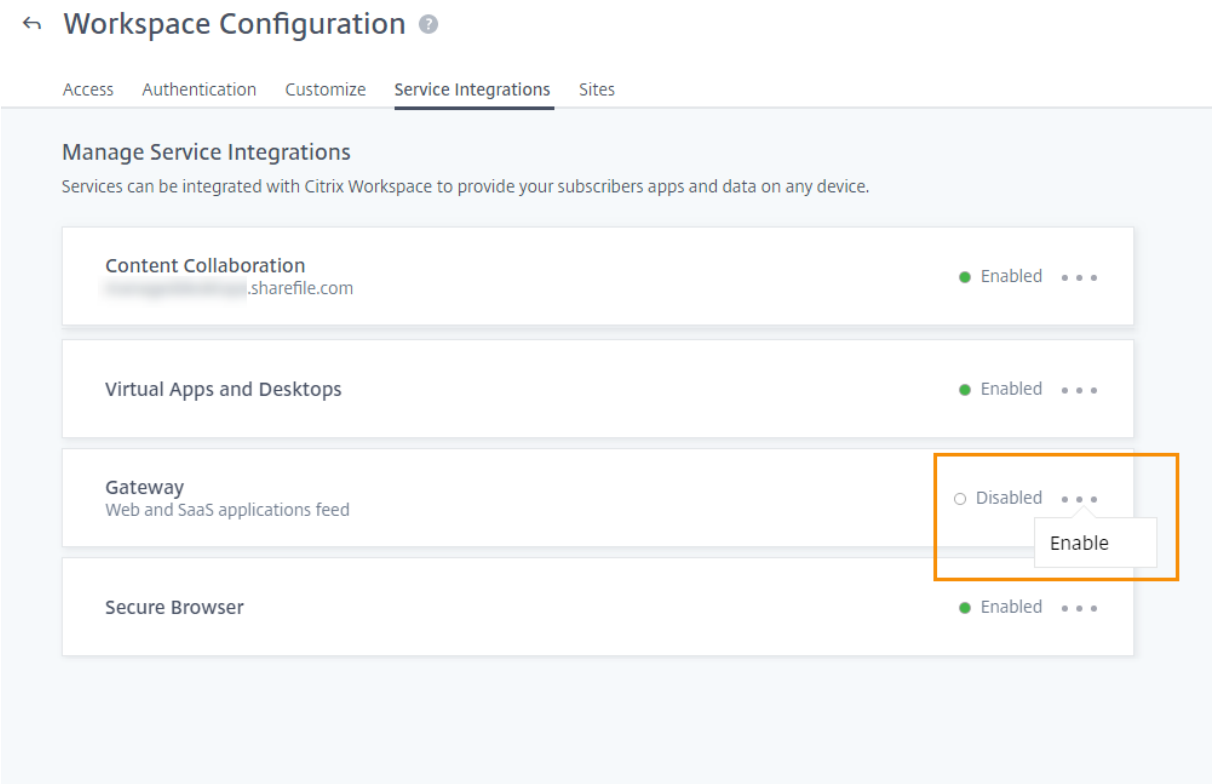
默认情况下，订阅 **DaaS** 和 **Remote Browser Isolation** 服务会将其启用。默认情况下，您的组织订阅的所有其他新服务都处于禁用状态。

> 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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。



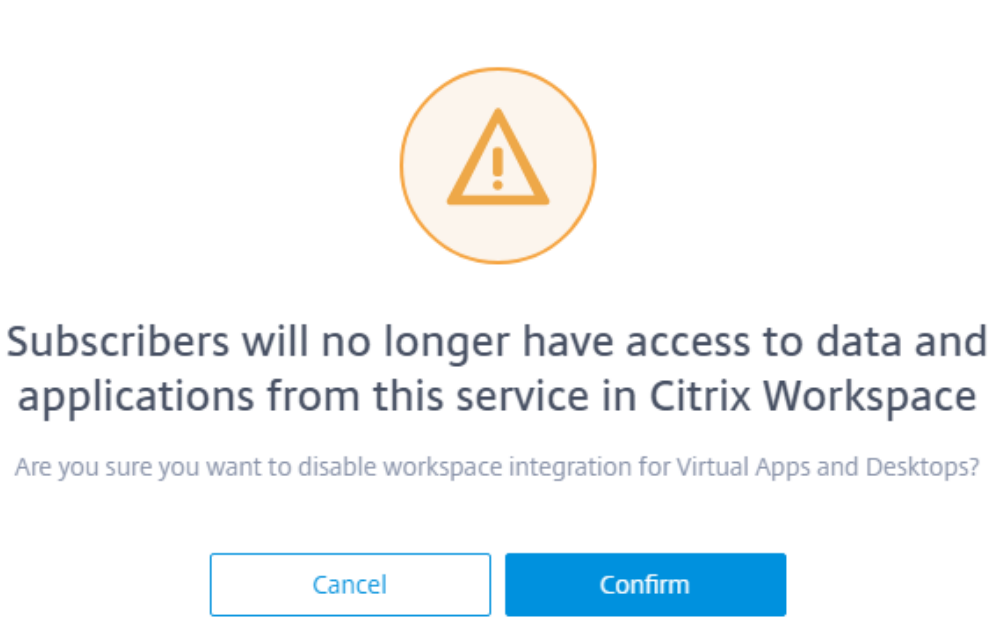
禁用服务

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



在 **Citrix Workspace** 中优化 **DaaS**

May 13, 2025

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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商（例如 Microsoft Entra ID（以前称为 Microsoft Azure AD）或 Okta）的订阅者在登录其工作区时仅输入一次其凭据。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。

资源过滤

Citrix Workspace 将用于存储的信息传递给 DaaS，您可以使用这些信息来过滤资源。有关更多信息，请参阅 使用交付组访问策略进行资源过滤

在工作区中聚合虚拟应用程序和桌面

November 7, 2024

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

> 注意：
>
> 有关聚合 DaaS 站点的信息，请参阅 集中站点管理（技术预览）。

聚合本地虚拟应用程序和桌面

以下部分提供有关聚合本地虚拟应用程序和桌面的详细信息。

支持的环境

有关 Citrix Virtual Apps 和 Desktops 的最低支持版本，请参阅 系统要求。

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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 。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- **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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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”。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

直接工作负载连接

May 13, 2025

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，以加快 HDX 会话速度。通常，内部和外部网络上的用户都通过外部网关连接到 VDA。此网关可能位于您的组织内部，或作为 Citrix 的服务提供并添加到 Citrix Cloud 内的资源位置。直接工作负载连接允许内部用户绕过网关并直接连接到 VDA，从而减少内部网络流量的延迟。

> 注意：
>
> HDX direct 功能允许客户端在可能的情况下自动直接连接到 VDA。这样就无需手动配置内部网络位置。

要设置直接工作负载连接，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 Citrix Cloud 中的 网络位置 页面为这些客户端所在的每个办公位置添加一个公共地址。

网络位置对应于您的内部用户所连接的网络的公共 IP 范围，例如您的办公室或分支机构。Citrix Cloud 使用公共 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内部还是外部。如果订阅者从内部网络连接，Citrix Cloud 会将连接直接路由到 VDA，绕过 NetScaler Gateway。如果订阅者从外部连接，Citrix Cloud 会通过 NetScaler Gateway 对其进行路由，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 服务并且启用了 Rendezvous 协议 ，Citrix Cloud 会通过 Gateway 服务将外部用户路由到内部网络中的 VDA。笔记本电脑等漫游客户端可能会使用其中任一网络路由，具体取决于启动时客户端是在公司网络内部还是外部。

远程浏览器隔离启动始终通过网关路由。这些启动不会通过配置直接工作负载连接获得性能改进。

要求

网络要求

- 公司网络和访客 Wi-Fi 网络必须具有单独的公共 IP 地址。如果您的公司网络和来宾网络共享公共 IP 地址，则来宾网络上的用户将无法启动 DaaS 会话。
- 使用内部用户所连接网络的公共 IP 地址范围。这些网络上的内部用户必须与 VDA 直接连接。否则，虚拟资源的启动将失败，因为 Workspace 会尝试将内部用户直接路由到 VDA，而这是不可能的。
- 虽然 VDA 通常位于您的本地网络内，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才能联系 VDA，而不会被防火墙阻止。这需要从您的本地网络到 VDA 所在的虚拟网络的 VPN 隧道。

在 **Web** 浏览器中打开资源时的 **TLS** 要求

如果您的最终用户使用 Web 浏览器打开应用程序和桌面，Citrix 建议您在内部网络中的 VDA 上配置 TLS。将您的 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 Citrix Workspace 应用程

© 1997–2025 Citrix Systems, Inc. All rights reserved.

序进行 HTML5 时，应用程序和桌面启动必须通过网关进行路由。使用 Desktop Viewer 启动不会受到影响。有关使用 TLS 保护直接 VDA 连接的详细信息，请参阅 Citrix 支持知识中心内的 CTX134123 。

配置网络位置

您可以在 Citrix Cloud 内配置网络位置。有关更多信息，请参阅 网络位置。

如果启用了自适应访问，则必须将位置配置为 内部。如果禁用自适应访问，则您无法选择网络位置类型，并且所有配置的网络位置都被视为内部。

验证内部启动是否正确路由

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正确寻址。

Citrix DaaS 控制台

选择 管理 **>** 监控 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，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

按照 Citrix Workspace app for Windows 文档中的说明在客户端计算机上启用 ICA 文件日志记录。启动会话后，检查记录的 ICA 文件中的 **Address** 和 **SSLProxyHost** 条目。

直接 **VDA** 连接　对于直接 VDA 连接，**Address** 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
```

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

网关连接　对于网关连接，**Address** 属性包含 Citrix Cloud STA 票证，**SSLEnable** 属性设置为 **On**，**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
```

以下是客户端通过本地网关建立连接并使用在资源位置内配置的本地网关启动应用程序时的 ICA 文件示例：

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

> 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。

故障排除

VDA 启动失败

如果 VDA 会话无法启动，请验证您使用的是正确的网络的公共 IP 地址范围。配置网络位置时，您必须使用内部用户所连接的网络的公共 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路由，请验证您使用的是正确的公共 IP 地址，内部用户可以通过该地址连接以到达他们的工作区。NLS 站点中列出的公共 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。要获取客户端的正确公共 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”。

在同一办公地点内启动资源的所有客户端通常使用相同的网络出口公共 IP 地址访问互联网。这些客户端必须具有到 VDA 所在子网的 Internet 网络路由，并且该路由不会被防火墙阻止。有关更多信息，请参阅本文中的 要求 。

额外的帮助和支持

如需故障排除帮助或有任何疑问，请联系您的 Citrix 销售代表或 Citrix 支持。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

服务连续性

May 20, 2025

服务连续性消除或最大限度地减少了对连接过程中涉及的组件可用性的依赖。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，前提是用户设备维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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

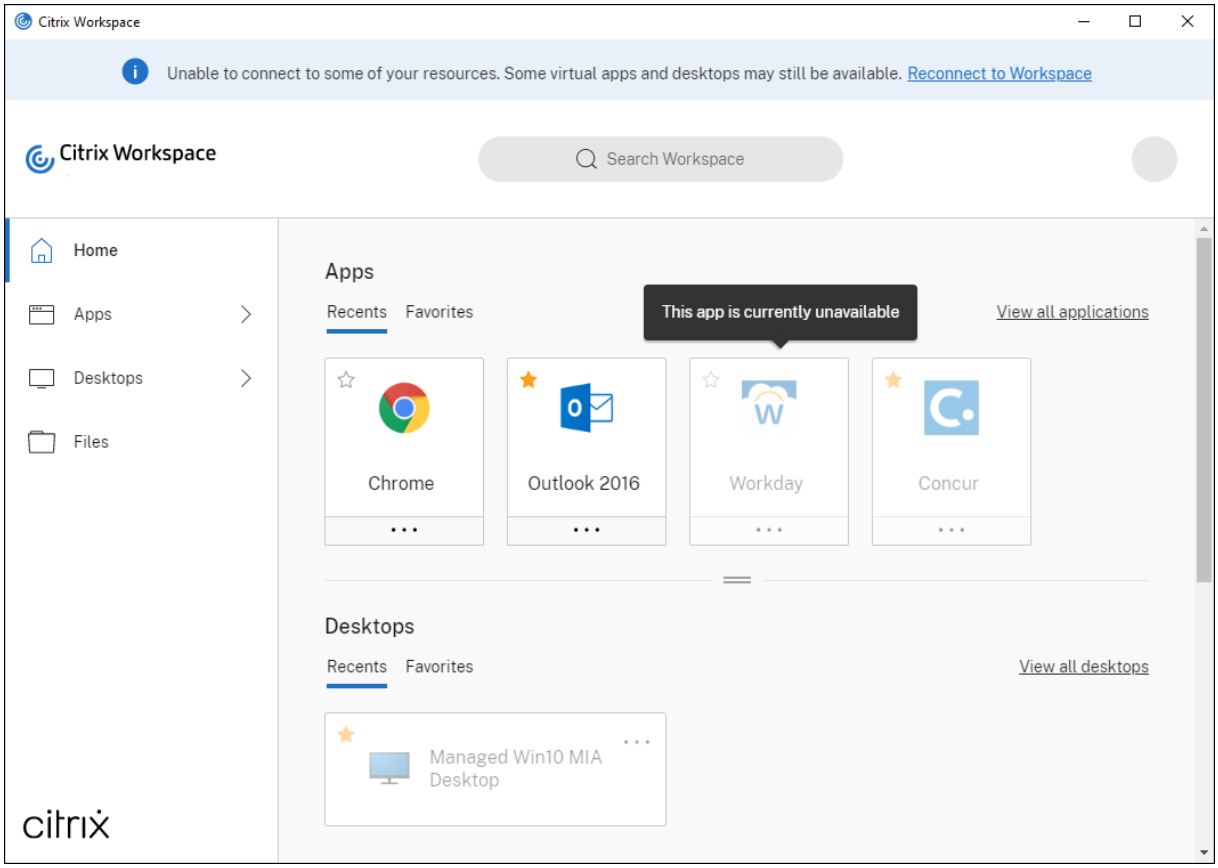
中断发生的地方	服务连续性如何维护用户访问权限	中断期间的用户体验
Citrix Workspace 服务	Citrix Workspace 应用程序根据用户设备上的本地缓存枚举应用程序和桌面。	不可用的应用程序和桌面的图标显示为灰色。用户仍然可以访问图标未变暗的应用程序和桌面。单击未变暗的图标后，系统可能会提示用户在 VDA 中重新输入其凭据。要重新获得对所有应用程序和桌面的访问权限，用户可以尝试通过单击“重新连接到 Workspace”链接来建立与 Workspace 的连接。
身份提供商	Citrix Workspace 应用程序，并根据用户设备上的本地缓存枚举应用程序和桌面。	用户可能无法登录到 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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。

有关在非生产环境中验证中断场景的信息，请参阅 服务连续性伴侣指南。

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。”用户会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。

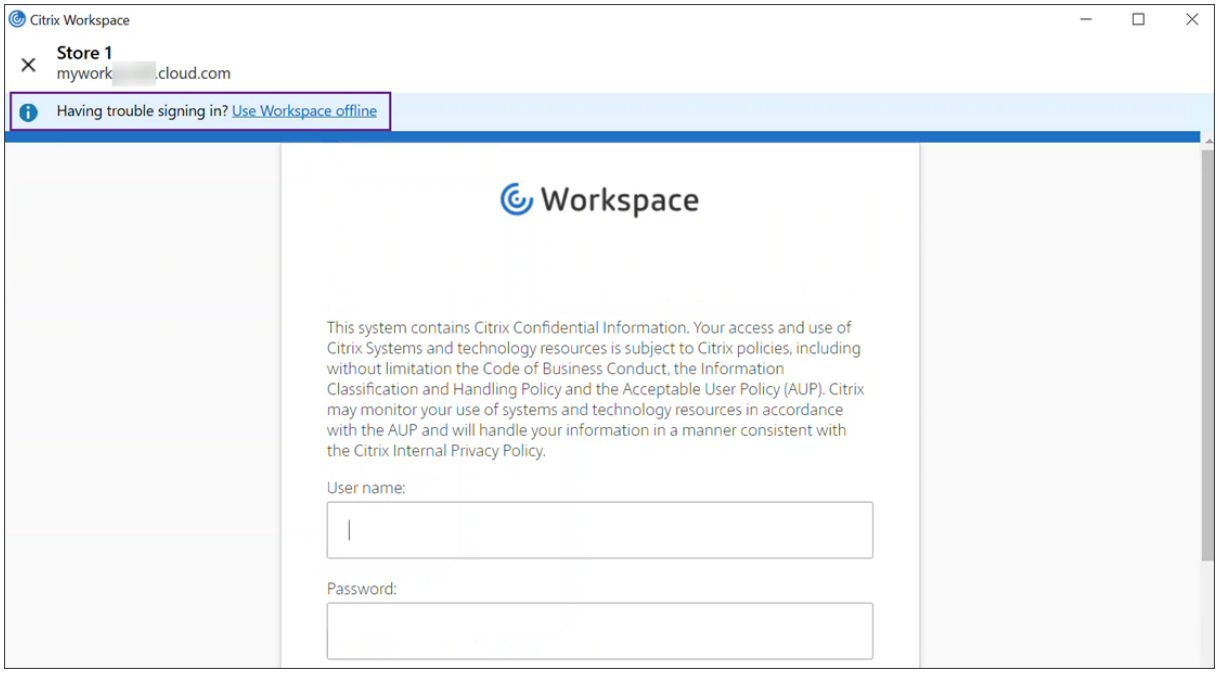


要在中断期间访问可用资源，用户可以选择不变灰的资源图标。如果出现提示，用户将在访问资源之前在 VDA 重新输入

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

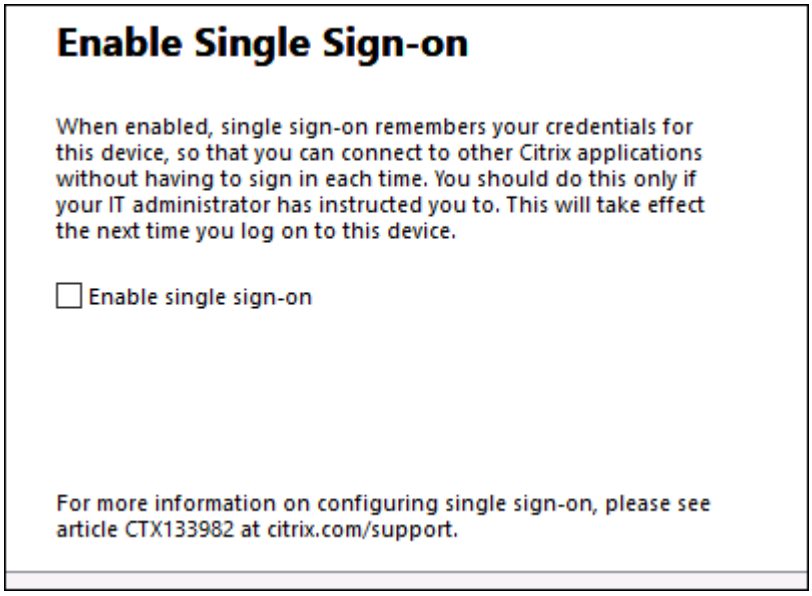
在服务连续性的默认配置中，如果用户注销 Citrix Workspace，则无法访问其资源。如果希望用户在注销后保留对其资源的访问权限，请指定在用户注销时保留 Workspace 连接租约。请参见 配置服务连续性。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 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。）
- 不支持 Citrix Cloud Government 环境。

用户设备要求

支持的最低 Citrix Workspace 应用程序版本：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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
- 条件认证

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。
- 有关无连接器资源位置（例如 Entra ID 连接的 VDA）中的 VDA 服务连续性的更多信息，请参阅 无连接器工作负载的服务连续性 。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 如果使用自适应身份验证或设备状态服务，则自适应身份验证或设备状态服务必须保持可达以确保服务连续性。
  - 为了保持安全性，服务连续性会在启动会话之前验证设备姿态的最新扫描结果。如果扫描结果不可用或过期，服务连续性将阻止会话启动，确保符合安全策略。

Citrix Cloud Connector 规模和大小

- 4 个 vCPU 或更多
- 6 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:443`，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 Microsoft Entra ID 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

  - 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要您自担风险。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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

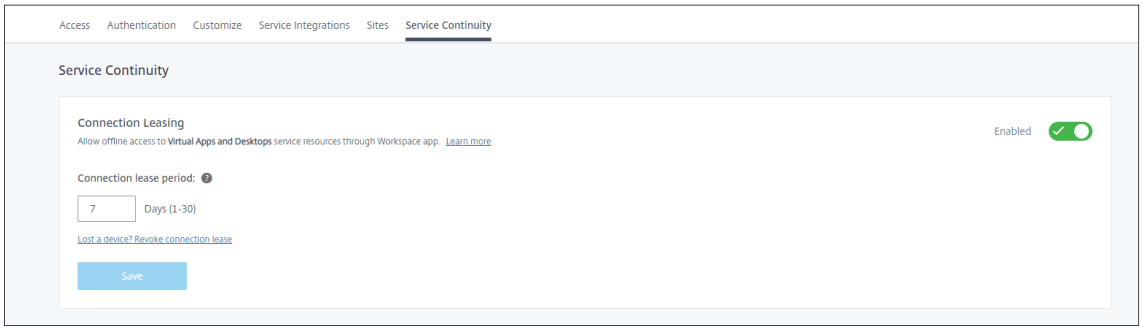
> 注意：
>
> 此 PowerShell 命令与直接工作负载连接类似，因为它通过允许内部用户绕过网关直接连接到 VDA 来优化与工作区的连接。启用服务连续性后，直接工作负载连接在中断期间不可用。

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 工作区配置 **>** 服务连续性。
2. 将 **Workspace** 的连接租用设置为启用。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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
```

> 笔记：
>
> - 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。
> - 配置设置后，Workspace 应用程序客户端可能需要最多 12 小时才能更新。

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

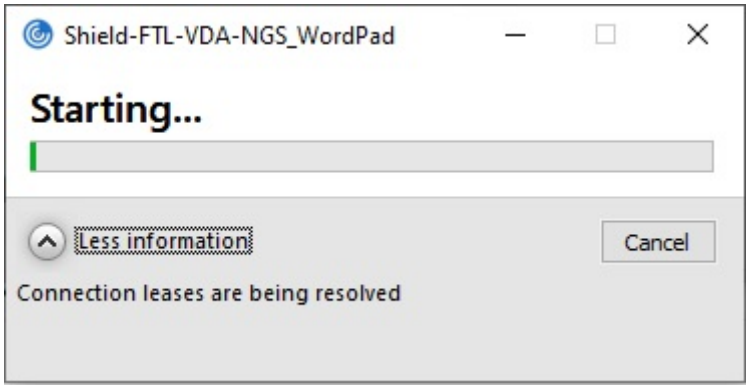
会话在中断期间如何启动

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。

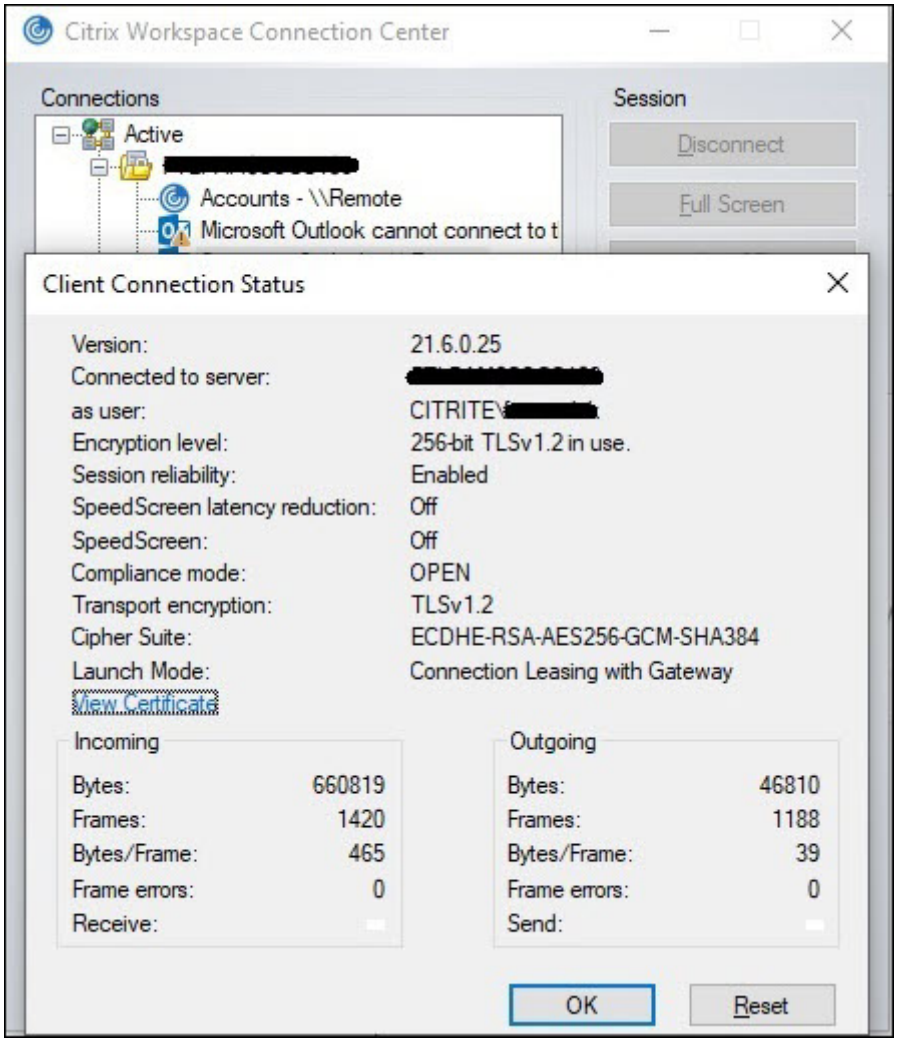
发生中断时连接的用户可以继续不间断地工作。重新连接和新连接会遇到最短连接延迟。此功能类似于本地主机缓存，但不需要本地 StoreFront。

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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：

```
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：

```
Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

此信息将显示：

```
FullName                        :
Name                            : XD\user2
UPN                             :
Sid                             : S-1-5-21-nnnnnn
LeaseRevocationDays             : 2
LeaseRevocationDateTimeInUtc    : 2020-12-17T17:34:25Z
LastUpdateDateTimeInUtc         : 2020-12-19T17:34:25Z
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
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] “追踪” = “真” “辅助追踪” = “真” “DefaultTracingConfiguration” = “全局全部-详细信息” “ConnectionLeasingEnabled” = “真”

   [HKEY_CURRENT_USER\Software\Citrix\Dazzle] “远程调试端口” = “8088”
3. 将保存的文件放入客户端终端节点。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

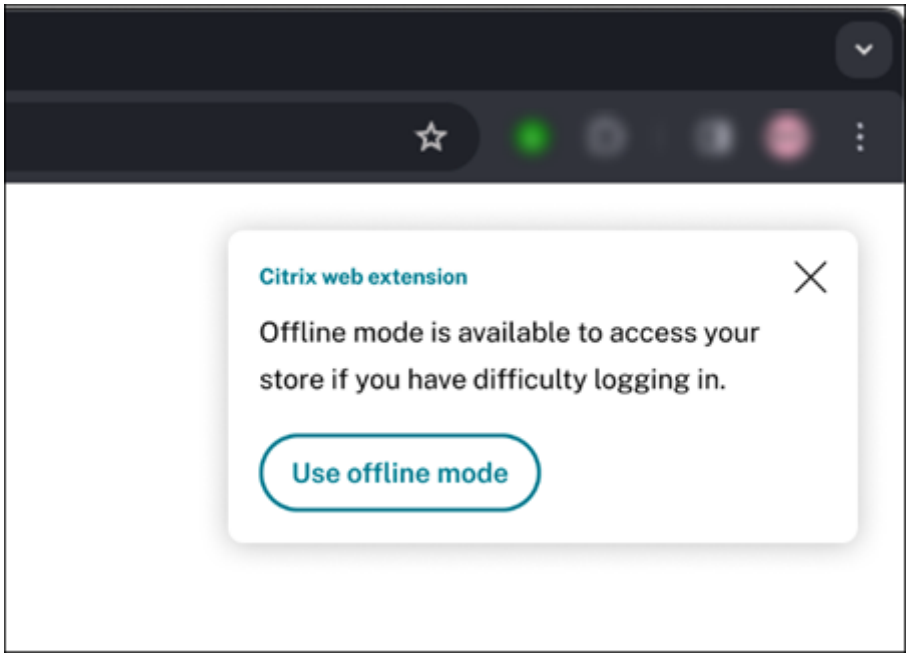
浏览器用户体验

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

尽管网络中断，用户仍可以通过浏览器从 Workspace Web 客户端访问他们的应用程序和桌面。如果用户因网络中断而遇到身份验证问题，60 秒后网页上会弹出以下提示。

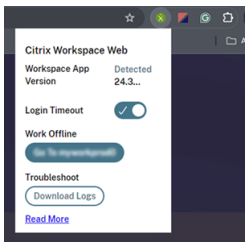
© 1997–2025 Citrix Systems, Inc. All rights reserved.



此提示是可选的，允许用户根据自己的喜好选择是否使用离线模式。此外，提示是可移动的，允许用户将其拖动到网页上的任何位置。

要离线访问可用的应用程序和桌面，用户可以单击 使用离线模式。

要管理离线模式提示，请单击用户设备上的浏览器中的 Citrix Workspace Web 扩展。出现以下屏幕：



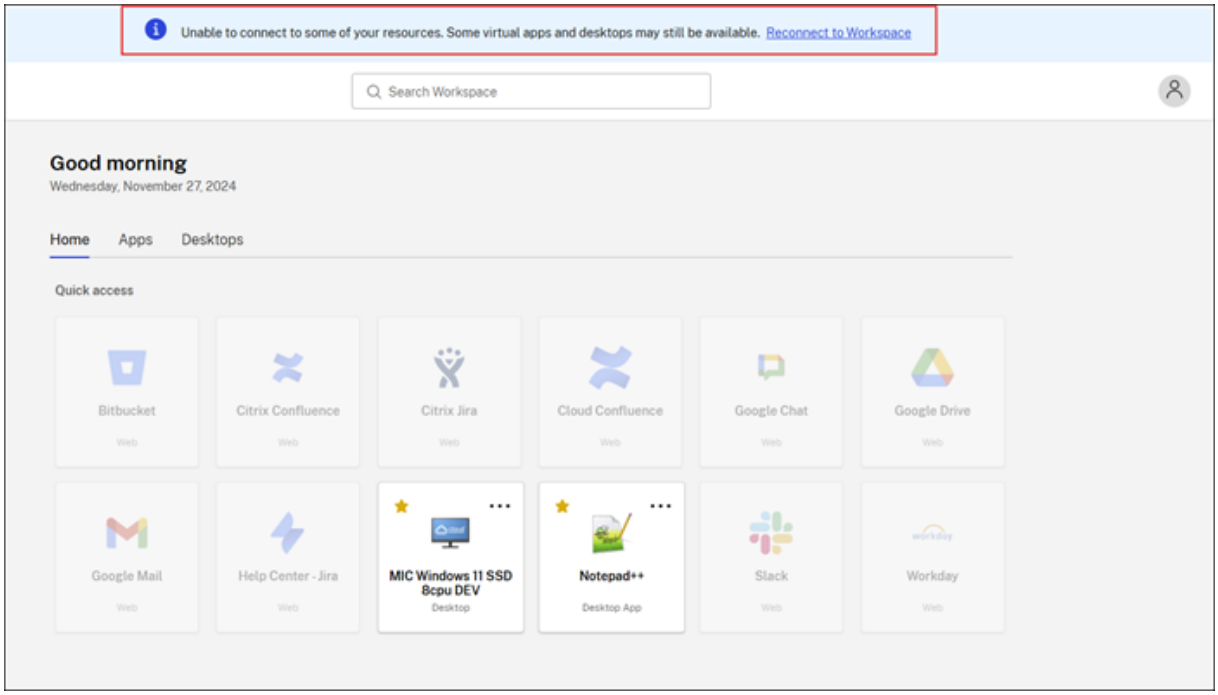
通过单击 登录超时 切换按钮来启用或禁用离线模式提示。

用户可以使用 离线工作 选项手动切换到离线模式，而无需等待 60 秒的离线模式提示。当用户禁用 登录超时时，此选项也很有用。要管理 离线工作 功能，请单击标有 的按钮，转到 [工作区存储名称]。

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。用户无需采取任何操作或等待登录超时间隔。

中断后，一旦网络恢复在线，用户可以单击 重新连接到工作区 将工作区重新连接到在线。当用户离线访问应用程序和桌面或在线访问应用程序和桌面时发生中断时，Workspace Web 客户端上会出现以下消息。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。

浏览器扩展不支持隐身模式。

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 7, 2024

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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。

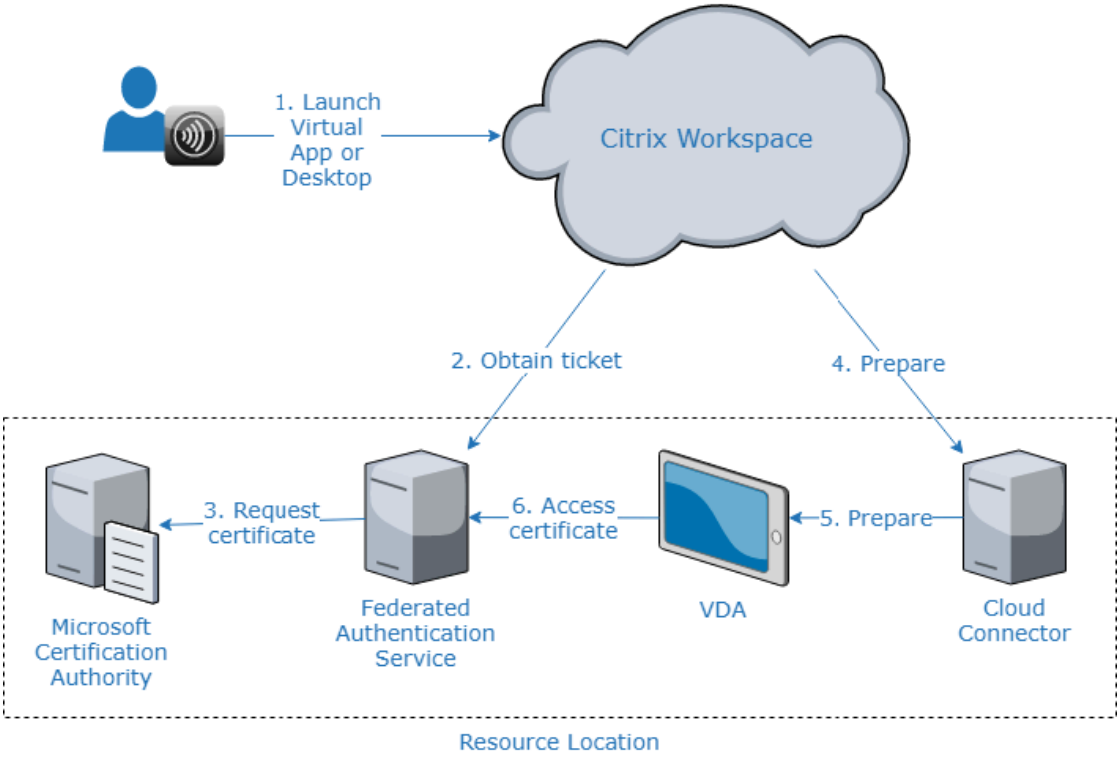
FAS 服务器与多个资源位置相连

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

安装和配置 **FAS**

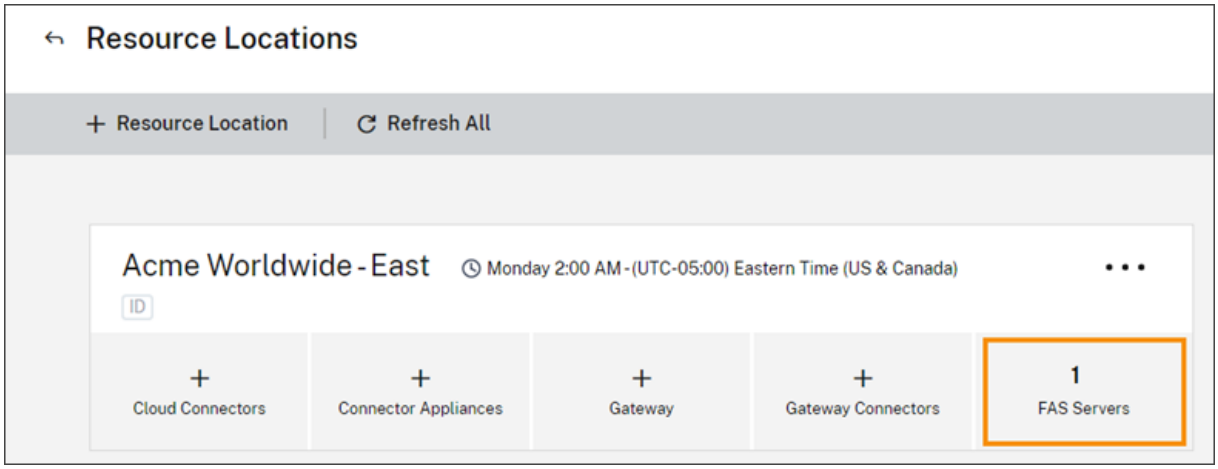
按照 FAS 产品文档中描述的 FAS安装和配置过程进行操作。StoreFront 和 Delivery Controller 配置步骤不是必需的。

> 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

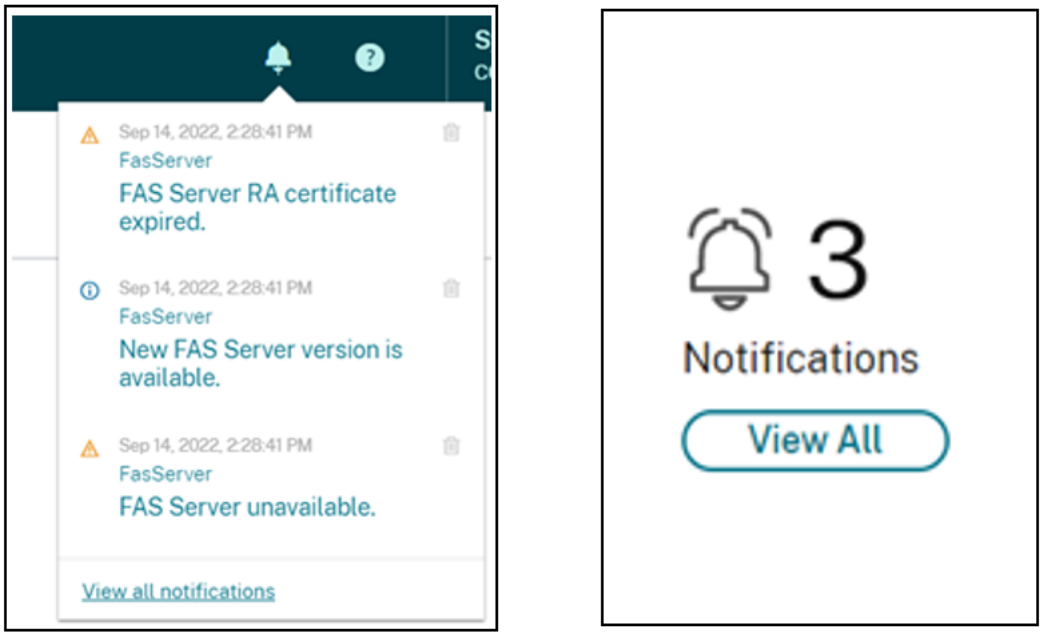
FAS 现在支持云通知。使用适用于 FAS 服务器的新 Cloud 通知，您将在以下情况下收到通知：

- 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。



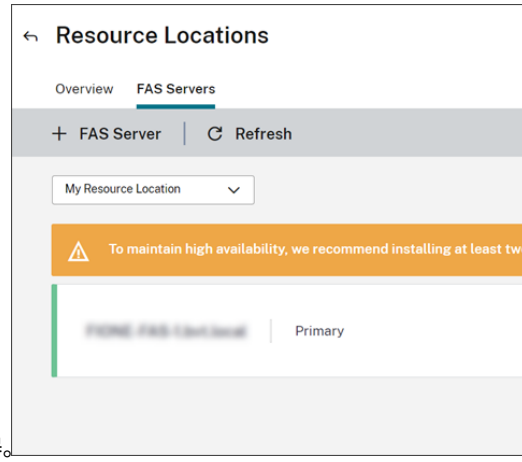
> 注意：
>
> 发出通知后，只有在问题未得到解决的情况下，才会定期再次发出通知。

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。

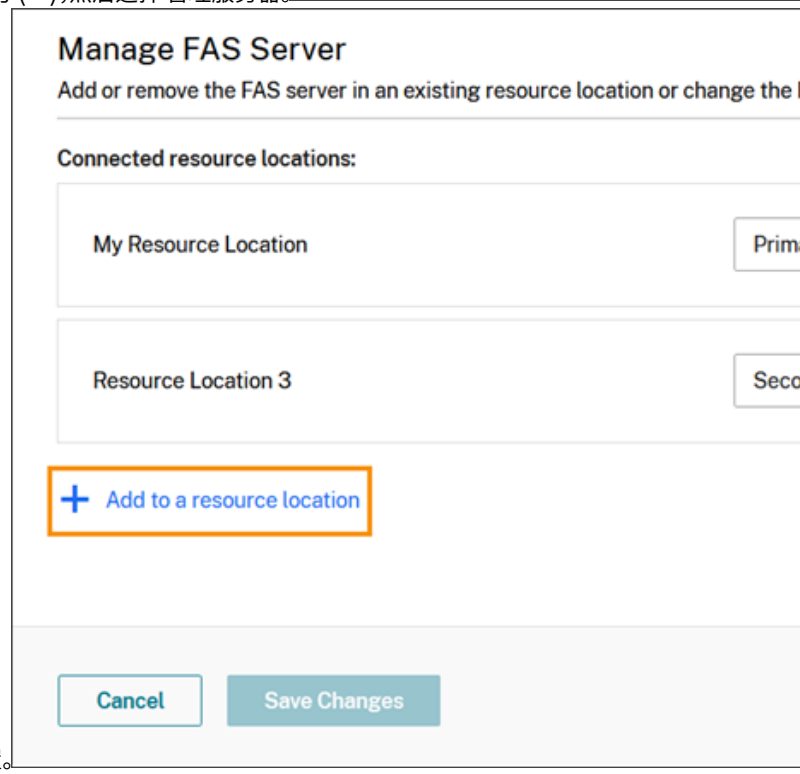
将 **FAS** 服务器添加到多个资源位置

1. 从 Citrix Cloud 菜单中，选择 资源位置，然后选择 **FAS** 服务器 选项卡。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。



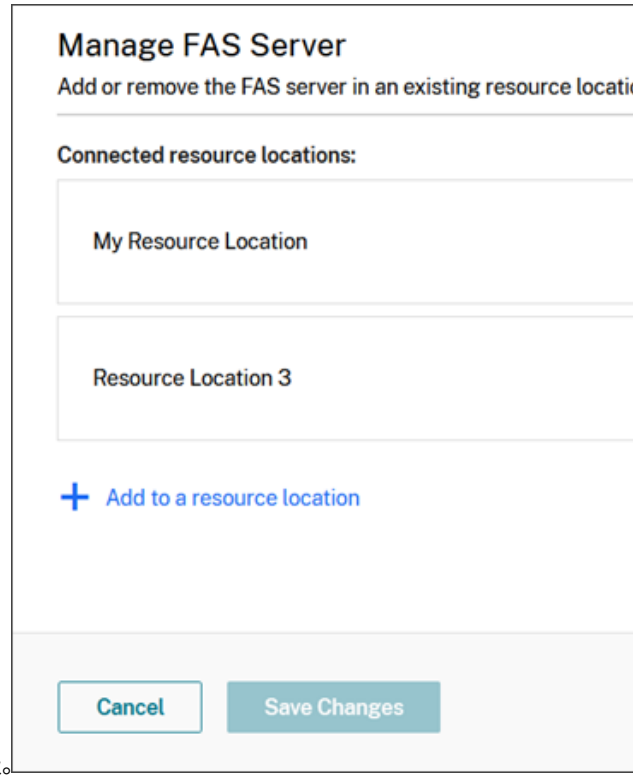
3. 选择“添加到资源位置”，然后选择所需的资源位置。
4. 选择 “主” 或 “辅助” 作为 FAS 服务器在每个选定资源位置的故障转移优先级。
5. 选择 保存更改。

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

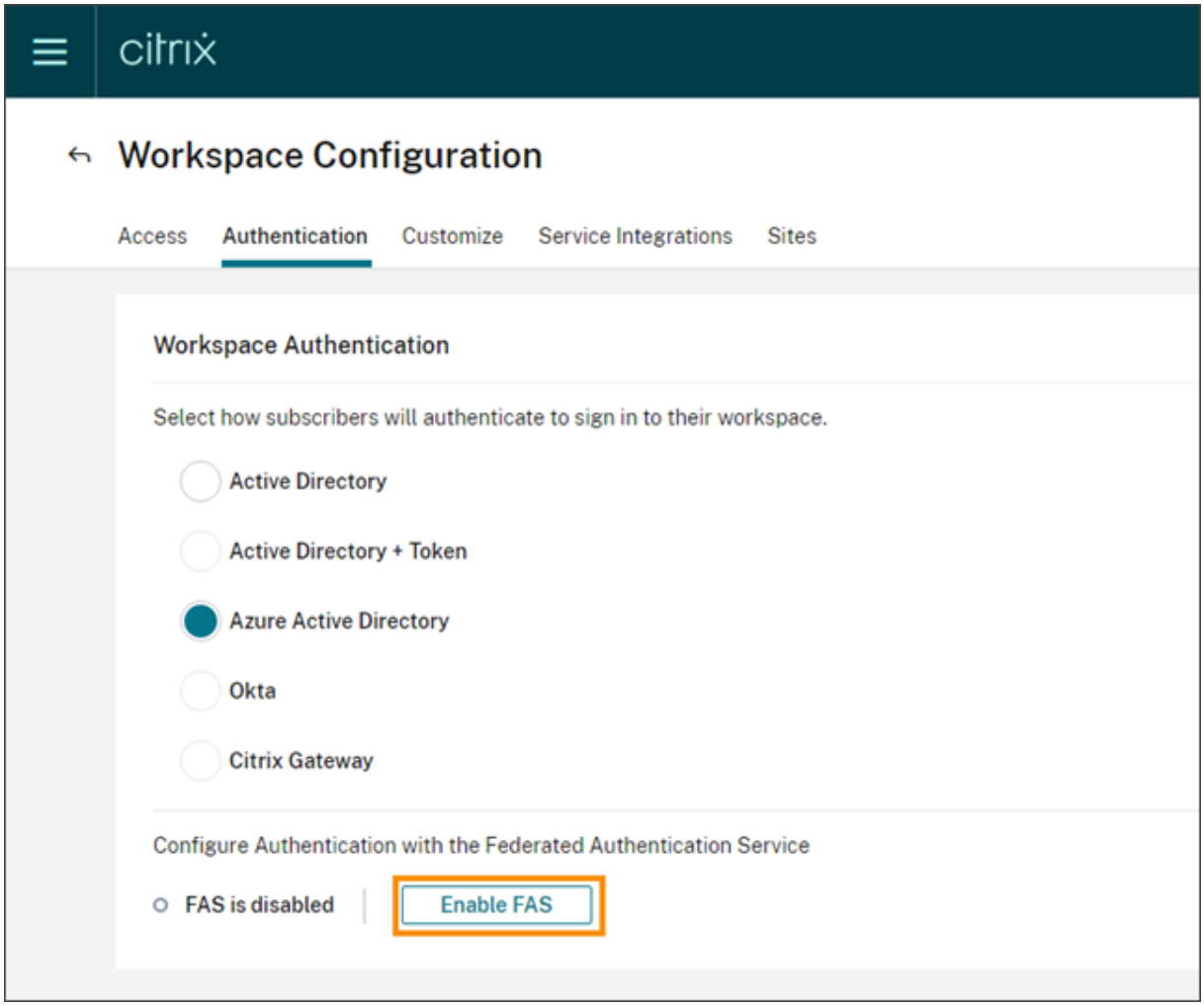


4. 找到要更改优先级的资源位置，然后从下拉列表中选择新的优先级。
5. 选择 保存更改。

为工作区启用联合身份验证

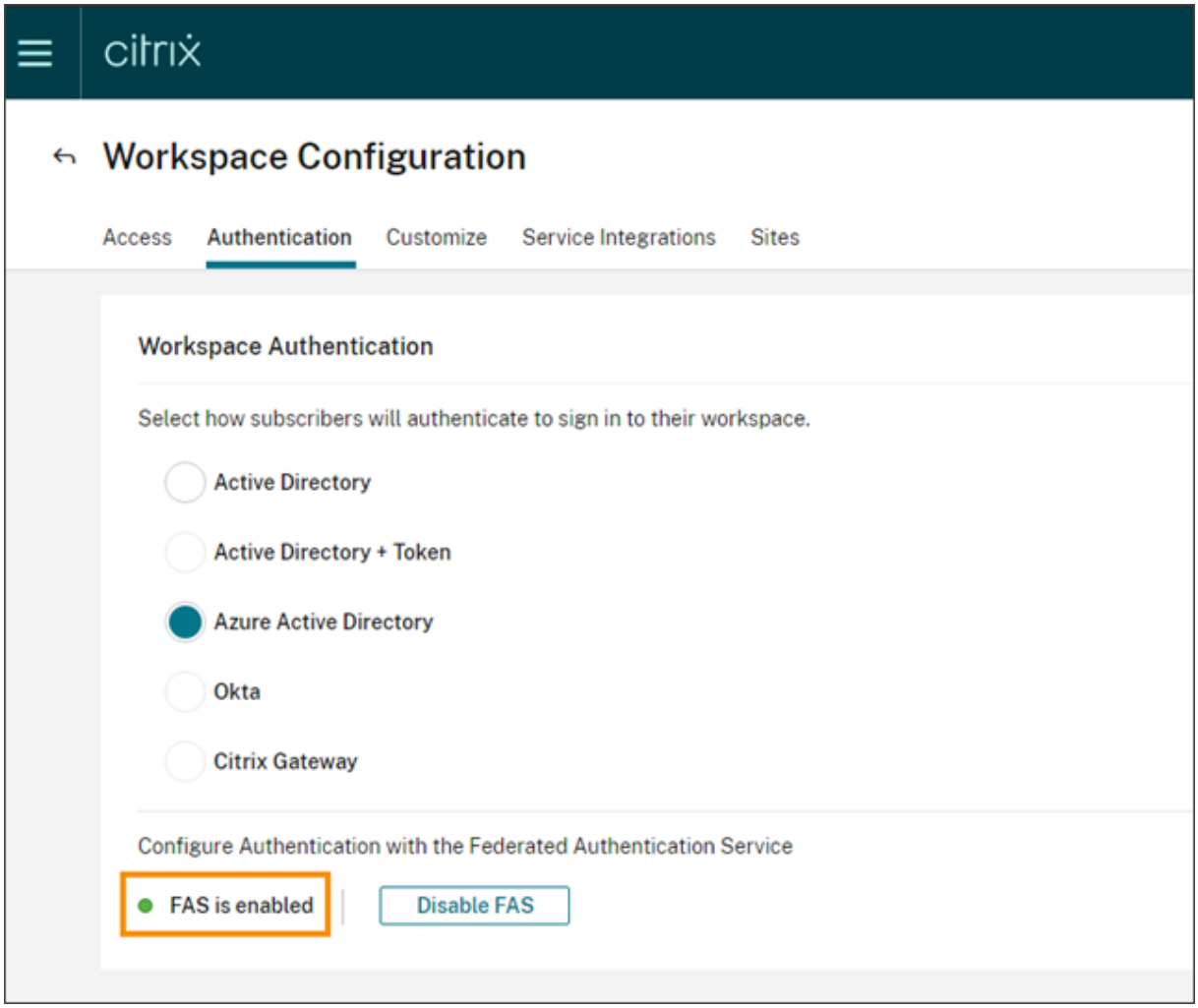
1. 在 Citrix Cloud 菜单中，选择 **Workspace Configuration**（Workspace 配置），然后选择 **Authentication**（身份验证）。
2. 单击 **Enable FAS**（启用 FAS）。此更改最多可能需要五分钟才能应用到订阅者会话。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



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。

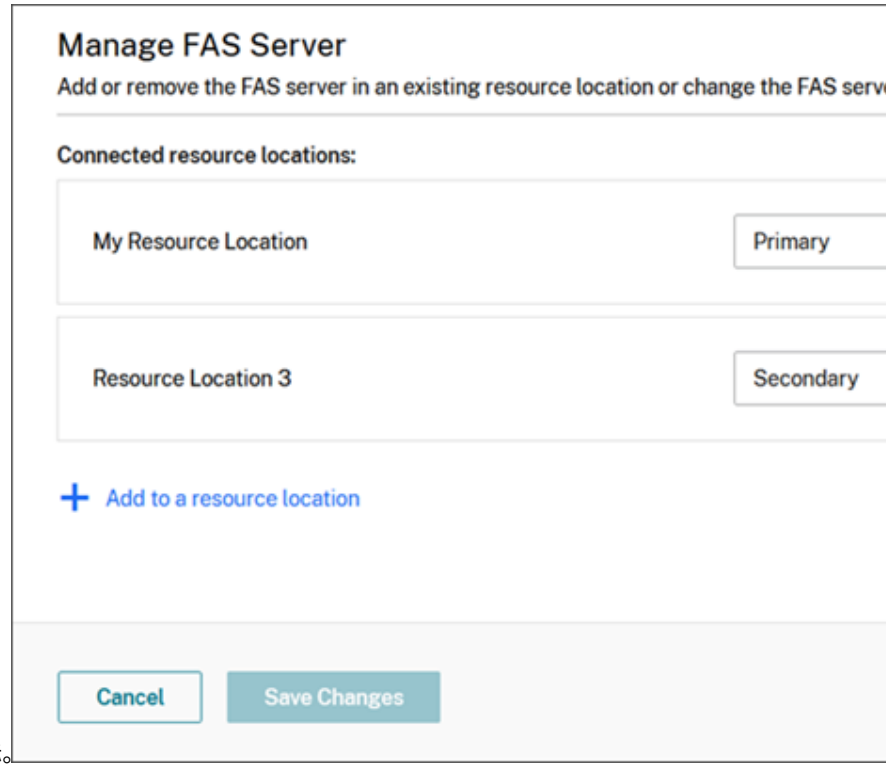
> 注意：
>
> 如果资源位置中的所有 FAS 服务器都已关闭或处于维护模式，应用程序启动将成功，但单点登录未激活。系统会提示订阅者输入其 AD 凭据以访问每个应用程序或桌面。

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。

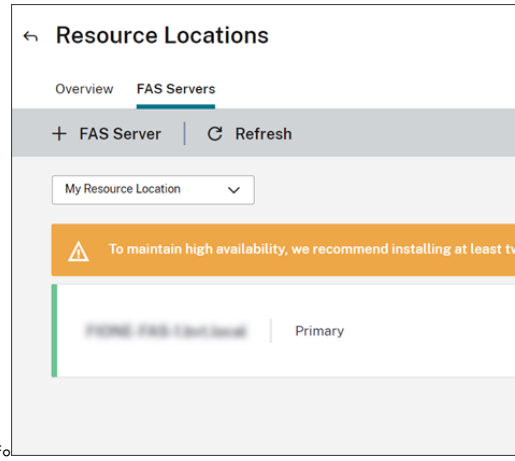
© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. 找到要移除的资源位置，然后单击 **X** 图标。

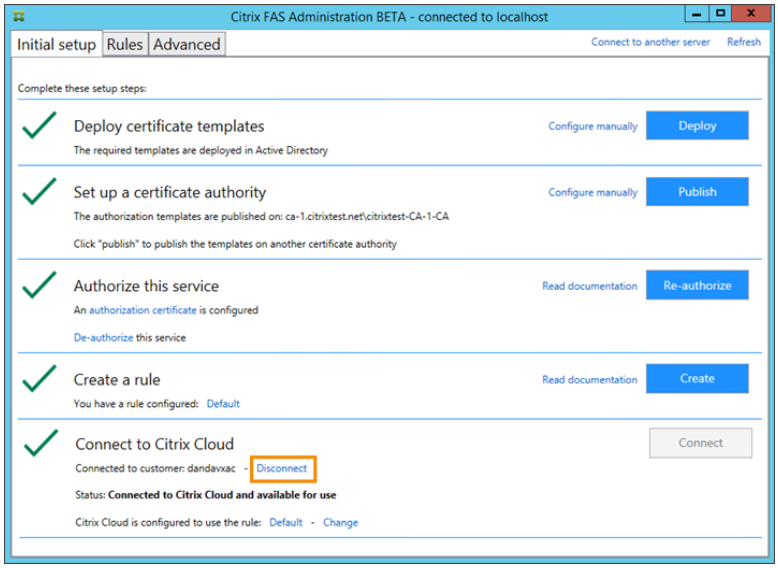
要从所有连接的资源位置删除 FAS 服务器，请执行以下操作：

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。



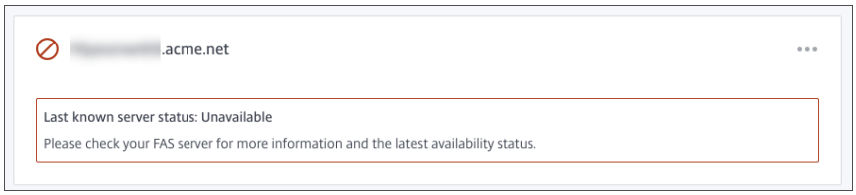
3. 找到要删除的 FAS 服务器，单击条目右侧的省略号，然后选择删除 **FAS** 服务器。
4. 在 FAS 管理控制台（在您的本地 FAS 服务器上）的 连接到 **Citrix Cloud** 中，选择 断开连接。或者，您可以卸

© 1997–2025 Citrix Systems, Inc. All rights reserved.

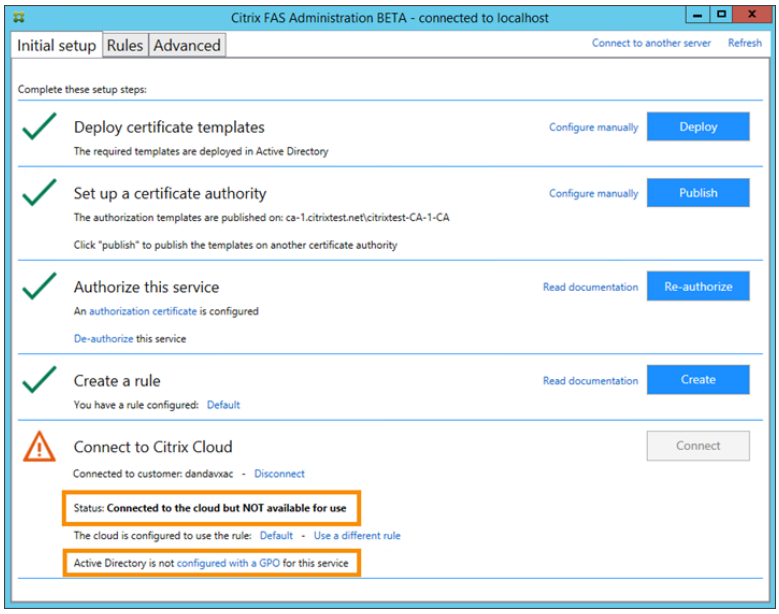
载 FAS。 

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：



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

使用交付组访问策略进行资源过滤

May 13, 2025

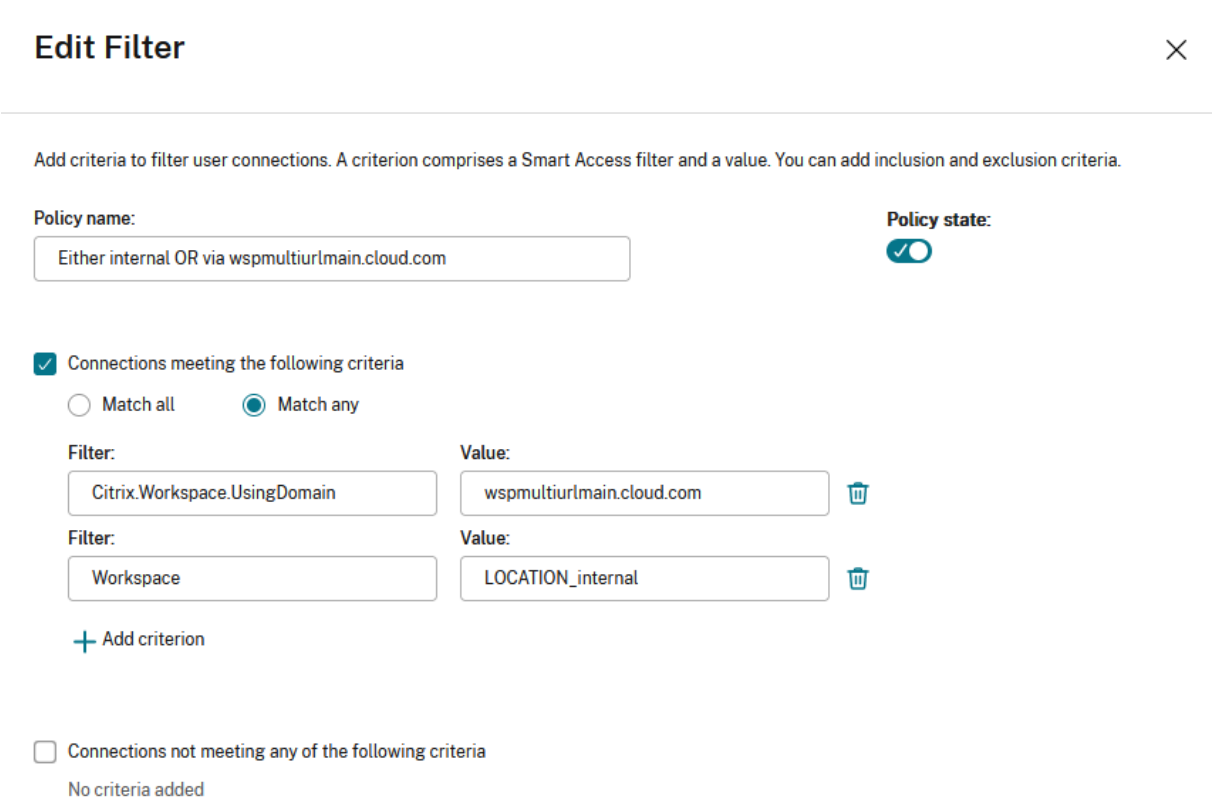
您可以根据工作区 URL 为交付组配置访问策略。您可以根据最终用户正在使用的工作区 URL 来控制他们对资源的访问。要根据工作区 URL 为交付组配置访问策略，您需要应用以下 SmartAccess 过滤器。过滤器值也作为 SmartAccess 标签发送到 DaaS 服务。它适用于以下两种场景：

- 同时列出 DaaS 发布的应用程序和桌面
- 启动应用程序或桌面时

过滤	值	说明
Citrix.Workspace. 使用域	示例.cloud.com	允许通过工作区 URL 过滤交付组资源。该值是工作区 URL 的完全限定域名。
Citrix Via Workspace	True	表示最终用户正在使用 Citrix Workspace，而不是本地 StoreFront 部署。

> 注意：
>
> SmartAccess 标签会自动发送。如果启用了 自适应访问 ，则 DaaS 会将来自 Workspace 的请求视为通过 Citrix Gateway，因此您必须向 **Citrix Gateway** 连接 规则添加条件。如果自适应访问被禁用，则必须向 非 **Citrix** 网关连接 规则添加条件。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



这允许根据以下标准对交付组内的应用程序和桌面进行过滤：

- 最终用户正在使用的工作区 URL
- 用户是否已登录 Workspace 或 StoreFront

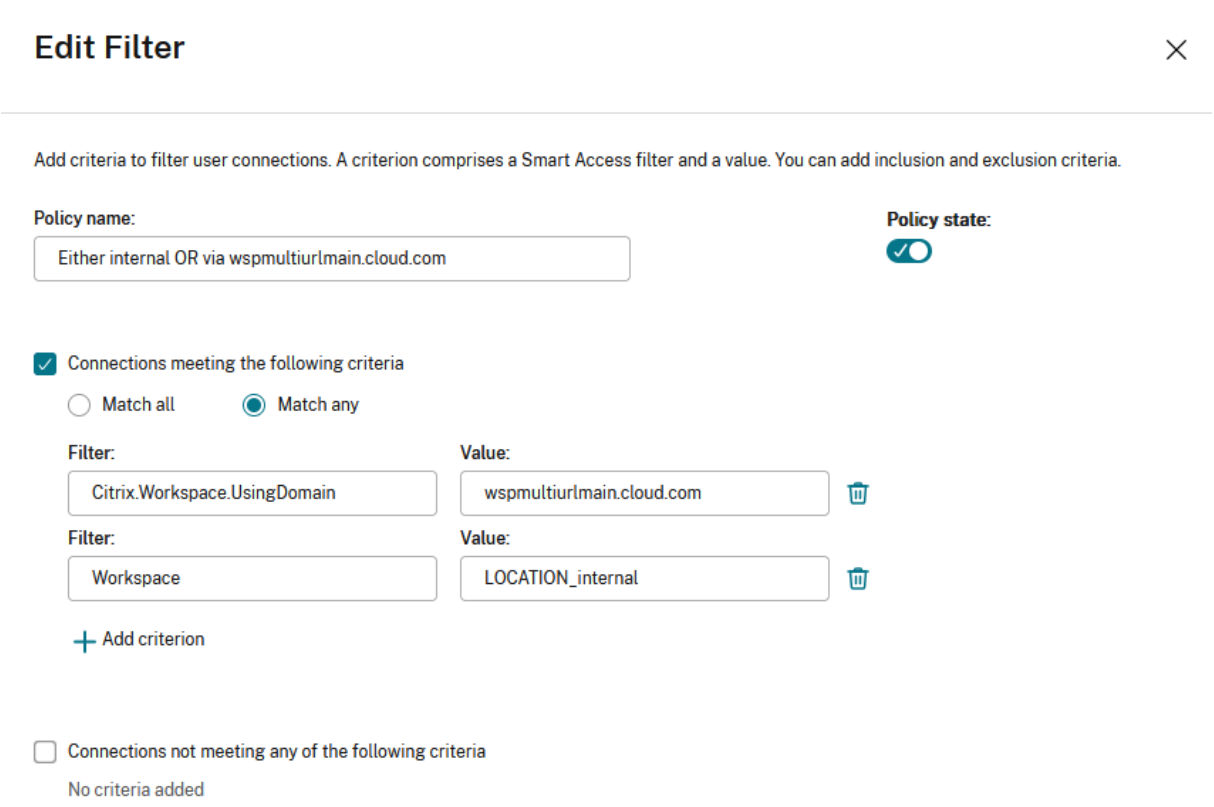
有关配置交付组的访问策略的更多信息，请参阅 管理交付组。

为多个 **URL** 工作流创建访问策略规则

1. 要创建访问策略规则，请转到 编辑交付组 **>** 访问策略，然后单击添加。仅当创建交付组后才可以更改访问策略。
2. 添加描述性策略名称。
3. 选择以下其中一个条件作为您的过滤器：
   - 匹配任何：如果任何给定的过滤条件与传入请求匹配，则访问策略允许访问。
   - 匹配全部：仅当所有给定的过滤条件与传入请求匹配时，访问策略才允许访问。
4. 为 `**Citrix.Workspace.UsingDomain**` 和 `**Citrix-Via-Workspace**` 过滤器添加值。

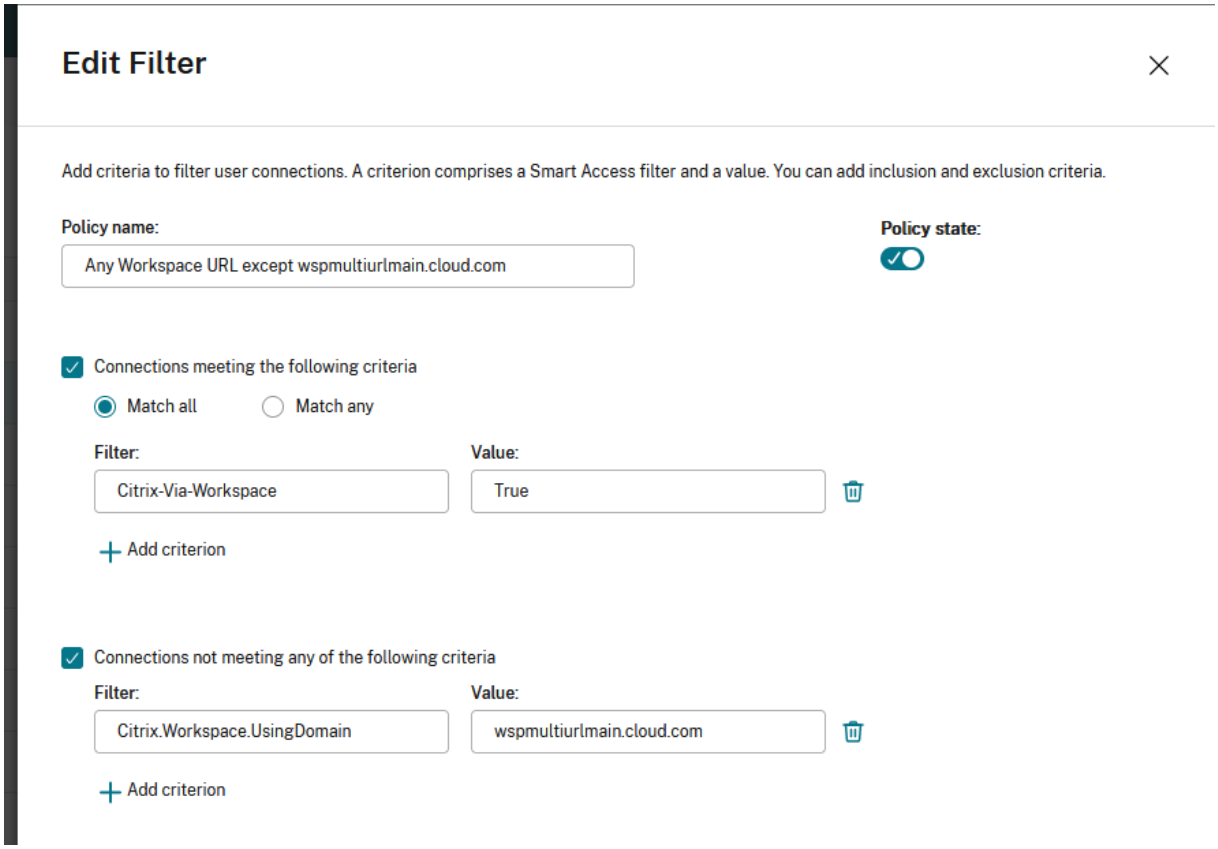
例如，在以下场景中，使用 匹配任何 过滤器意味着该规则允许使用 的用户或从内部网络连接的用户进行访问（根据网络位置配置）。有关更多信息，请参阅 [根据用户网络位置的自适应访问](/zh-cn/citrix-daas/manage-deployment/adaptive-access/adaptive-access-based-on-users-network-location.html)。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



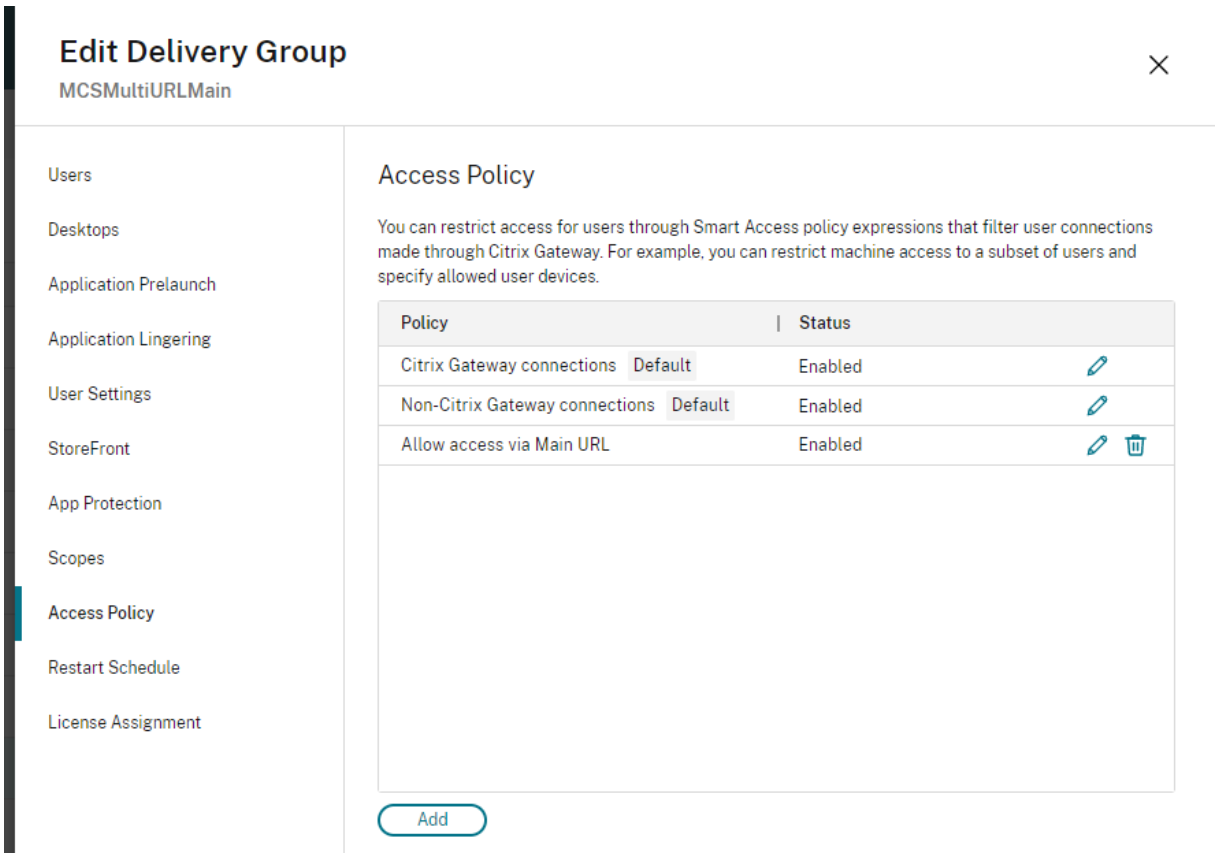
将过滤器更改为 匹配所有 意味着该规则只允许使用 <wspmultiurlmain.cloud.com> 从内部网络访问的用户。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



确认更改后，新策略就会出现在“访问策略”页面上。有关更多信息，请参阅 管理交付组

© 1997–2025 Citrix Systems, Inc. All rights reserved.



使用 **Global App Configuration Service** 配置 **Citrix Workspace** 应用程序

December 31, 2024

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。

该服务支持 Windows、Mac、Linux（仅限云存储）、Android、iOS、HTML5 和 ChromeOS 平台。

主要好处

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

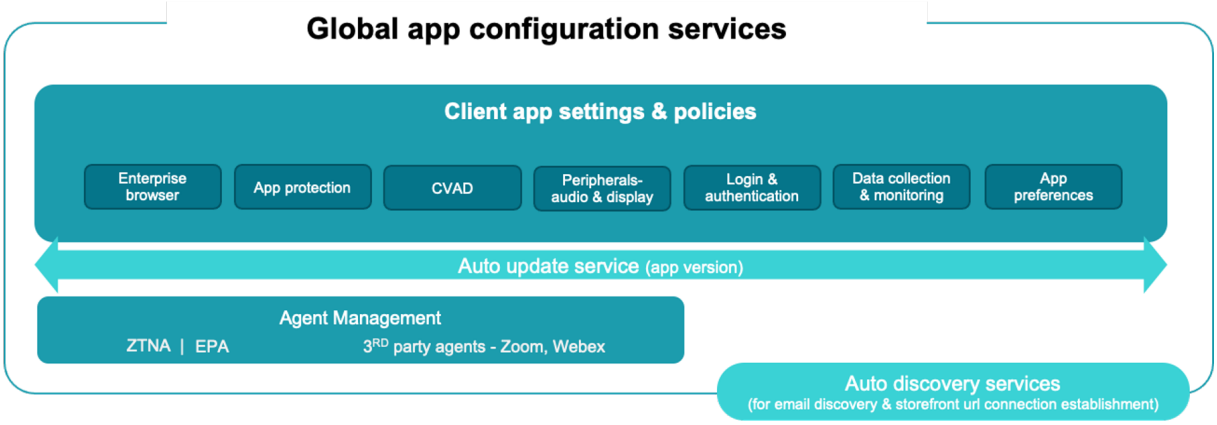
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 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。



> 注意：
>
> 随着适用于 Windows 和 Mac 的 Citrix Workspace 应用程序版本 2402 的发布，GACS 分两个阶段提供设置。Citrix Workspace 应用程序最初会获取在用户身份验证之前需要应用的某些设置，其余设置在身份验证成功后应用。

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。

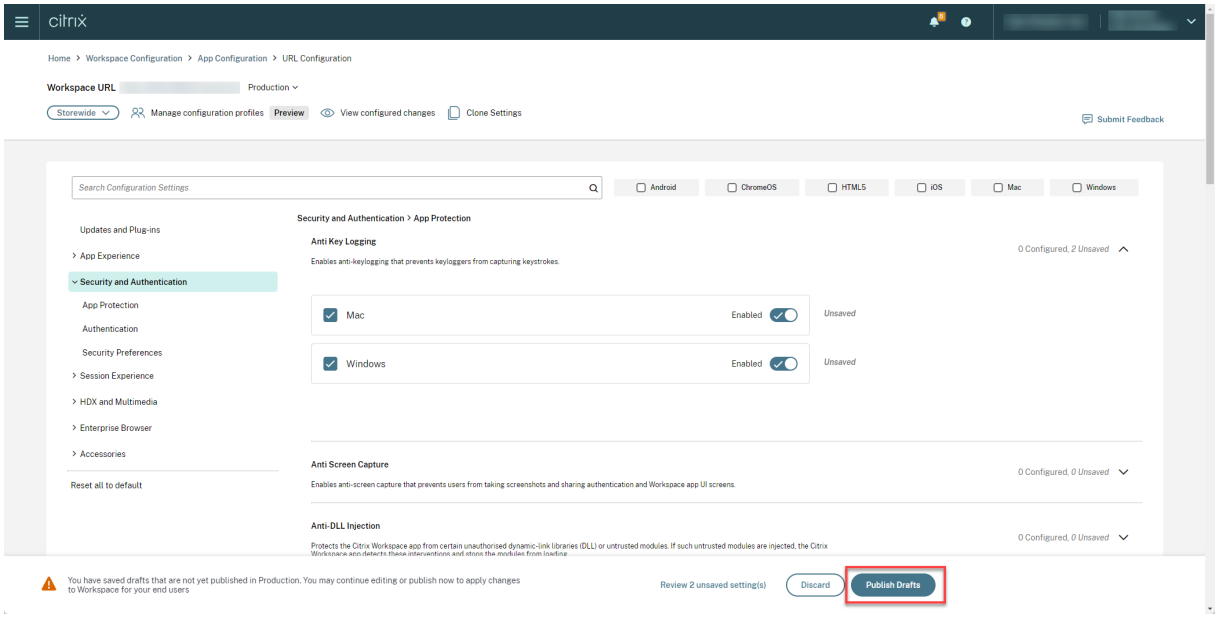
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
Linux	2408
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

如何使用 **Global App Configuration Service**

要配置设置：

1. 登录 Citrix Cloud 门户并导航到 工作区配置 > 应用程序配置。
2. 从已配置的商店 URL 列表中，选择您要映射设置的商店，然后单击 配置。
3. 根据您组织的政策修改应用程序设置。
4. 单击 发布草稿 保存并发布您的设置。

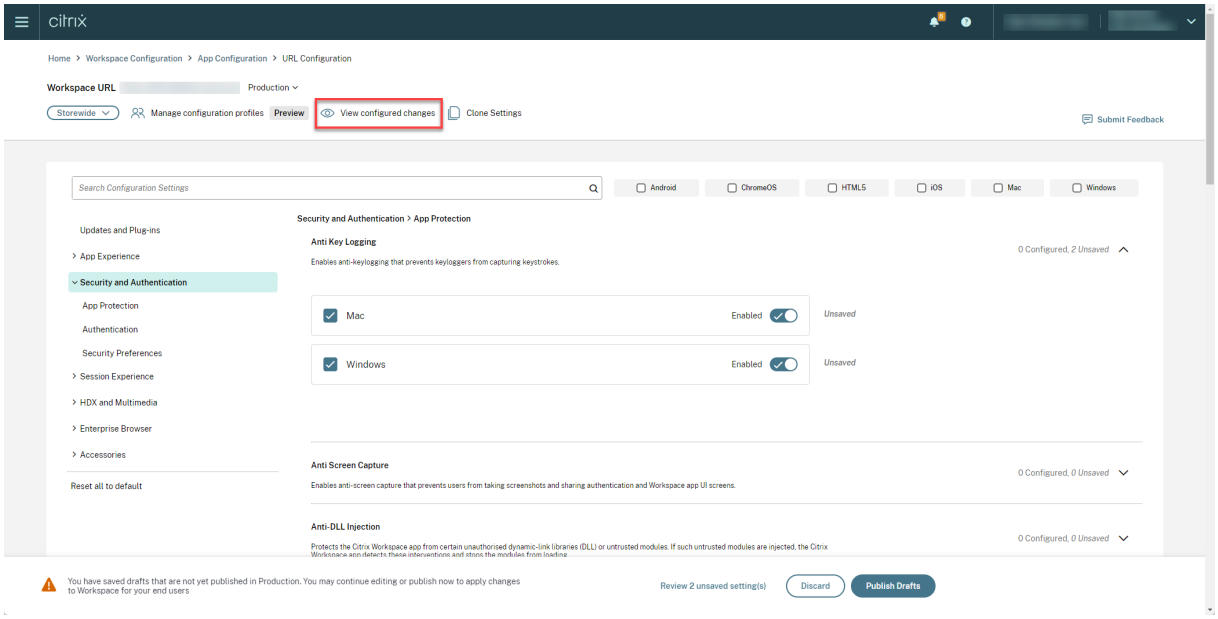


用户界面还提供以下选项，以简化用户体验。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

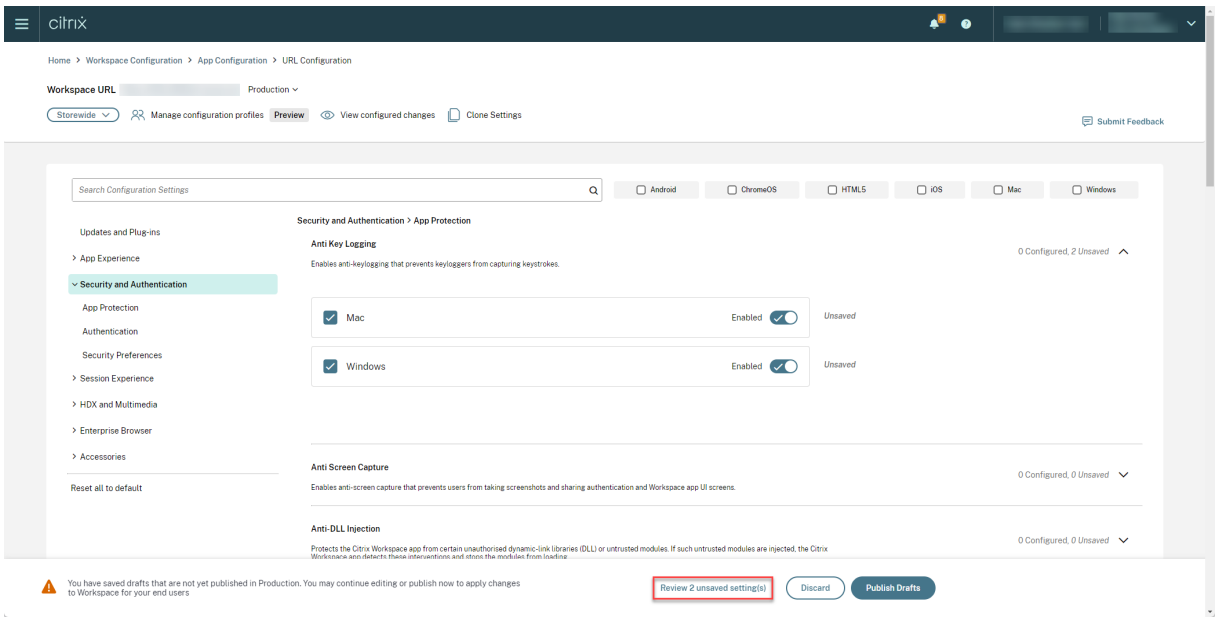
查看已配置设置的摘要

您可以通过单击 查看配置的更改 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。



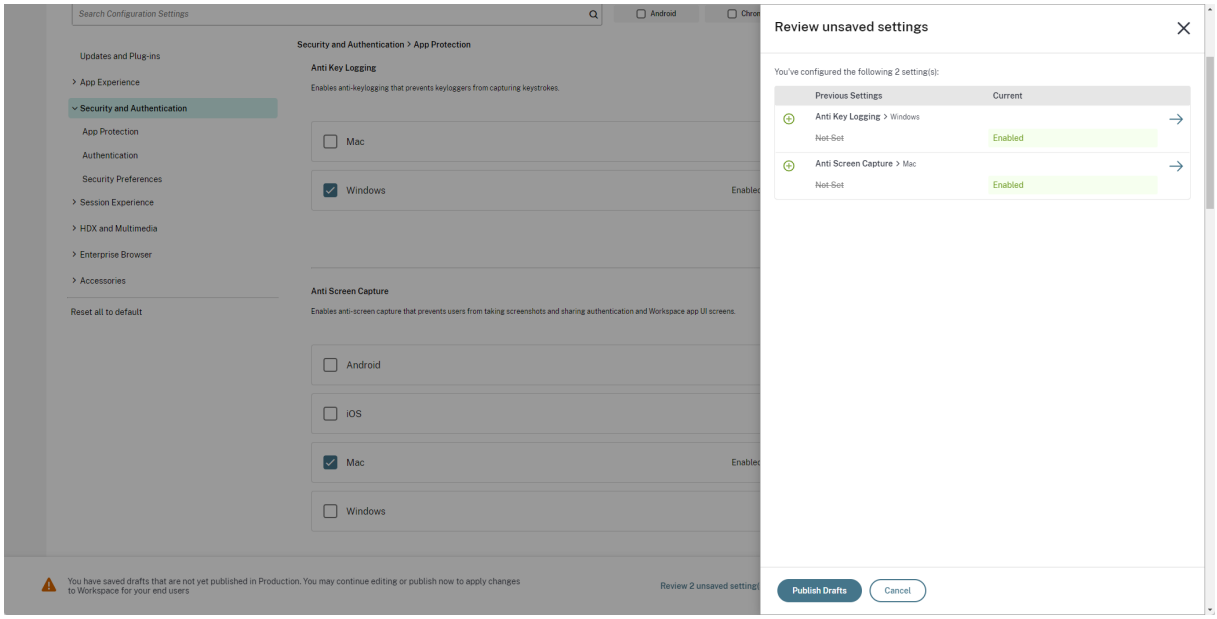
查看未保存的更改

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。

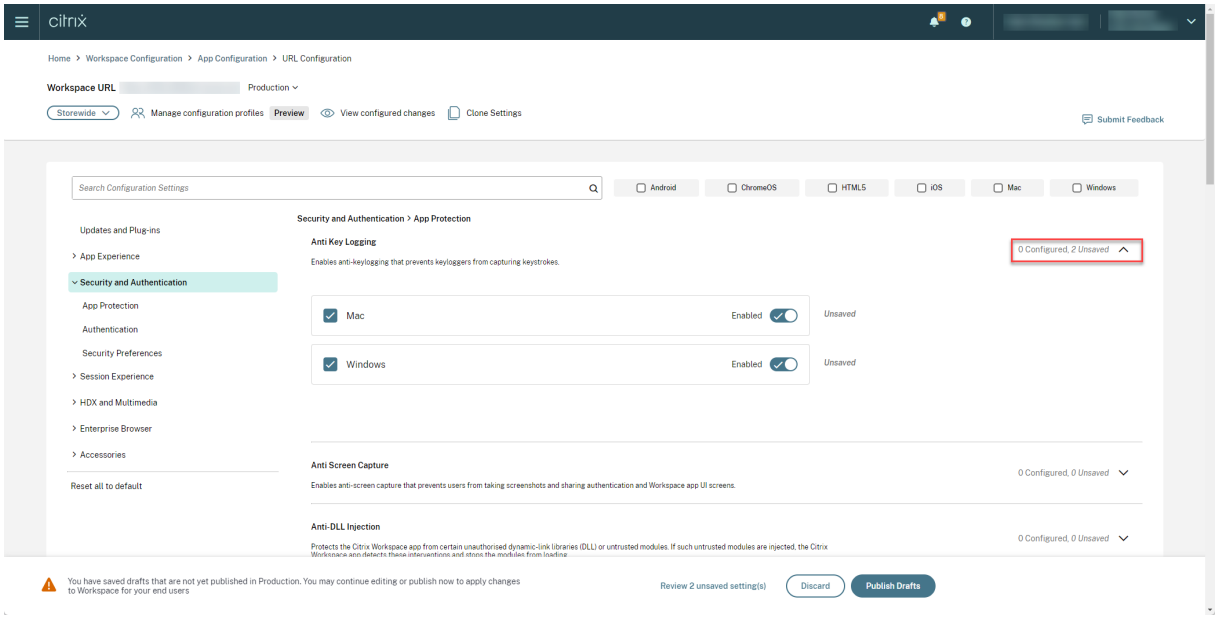
© 1997–2025 Citrix Systems, Inc. All rights reserved.



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



© 1997–2025 Citrix Systems, Inc. All rights reserved.

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

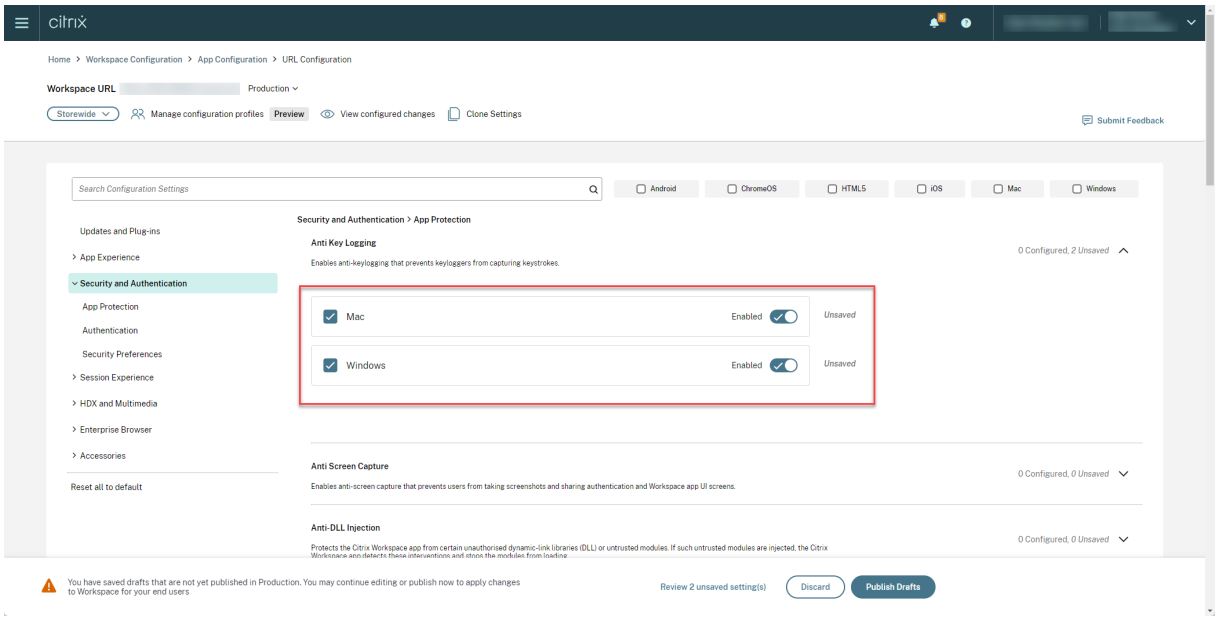
您可以通过输入在设置描述中找到的关键字来查找设置。它允许使用与所需设置相关的术语进行更灵活的搜索方法。

- 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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

平台	更新设置所需的最长时间
适用于 macOS 的 Citrix Workspace 应用程序	最长 6 小时
适用于 Linux 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
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)** 或 **MDM >** 全局应用程序配置服务
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 Linux 的 Citrix Workspace 应用程序	云	**MDM >** 全局应用配置服务
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**

© 1997–2025 Citrix Systems, Inc. All rights reserved.

平台	应用商店类型	优先顺序
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

只有第一个启用全局应用程序配置服务的存储可以获取该设置。

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

March 15, 2025

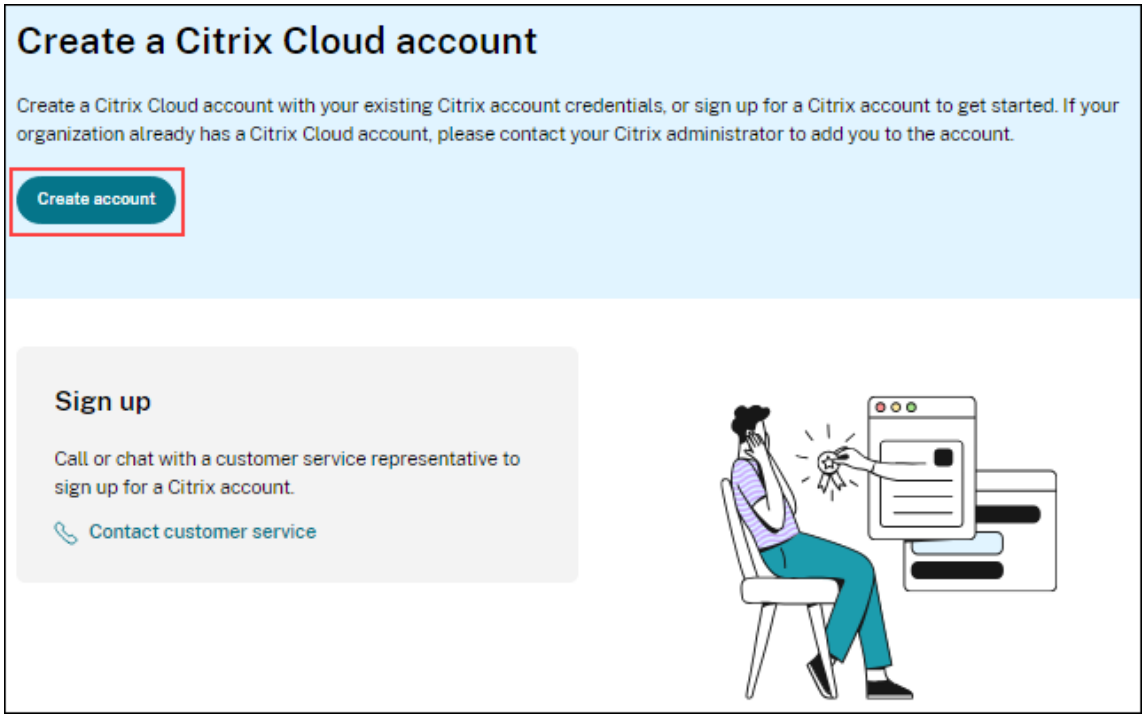
概述

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>、<https://gacs-discovery.cloud.com>和 <https://gacs-config.cloud.com> 必须是可联系的。它是基于电子邮件的发现和全局应用程序配置服务运行所必需的。
- 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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

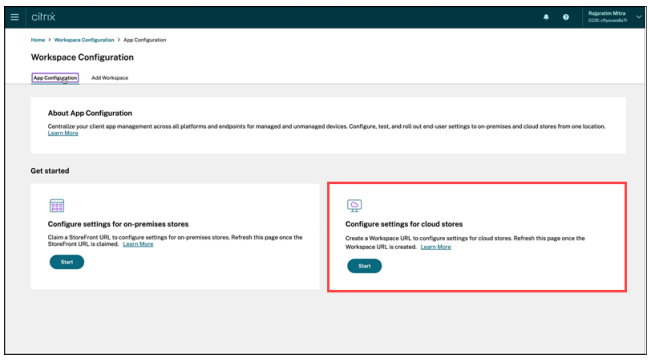


- 验证您是否订阅了 Workspace。

开始配置

您可以登录您的 Citrix Cloud 帐户并从 工作区配置 > 应用程序配置配置设置。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存储。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。

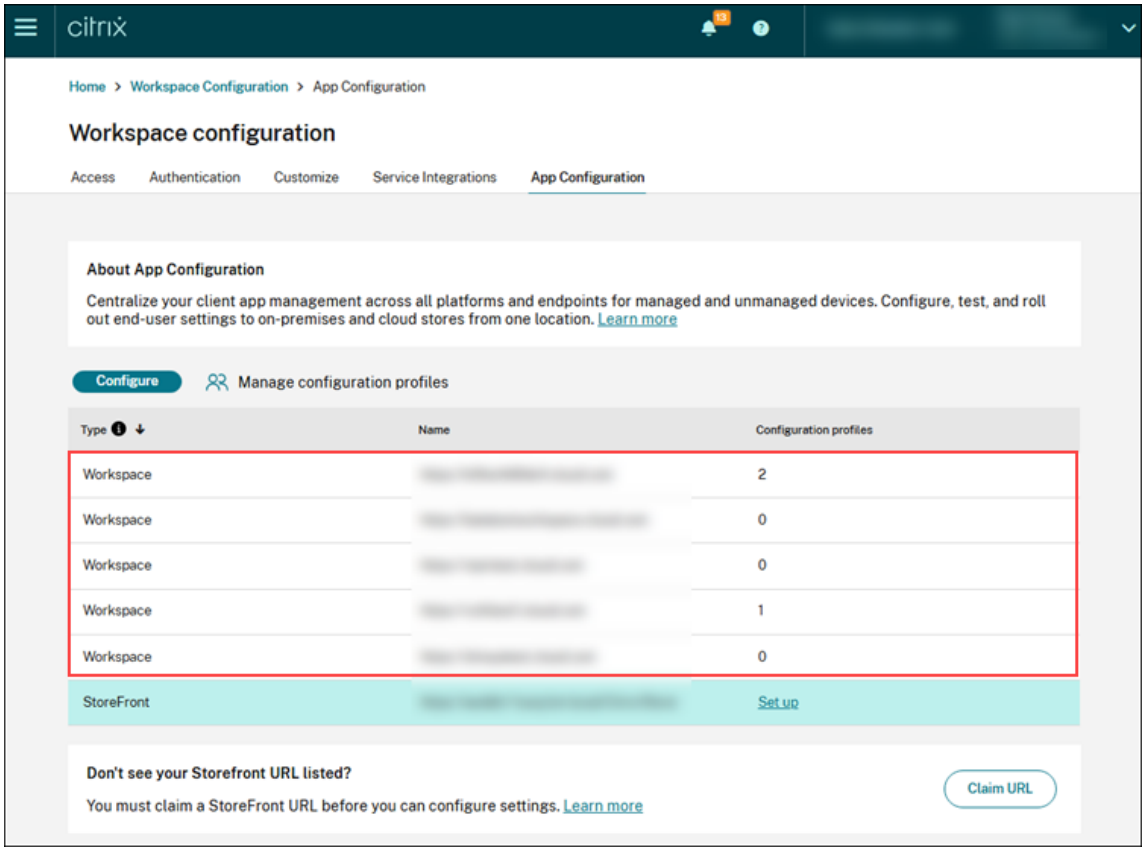


© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置设置

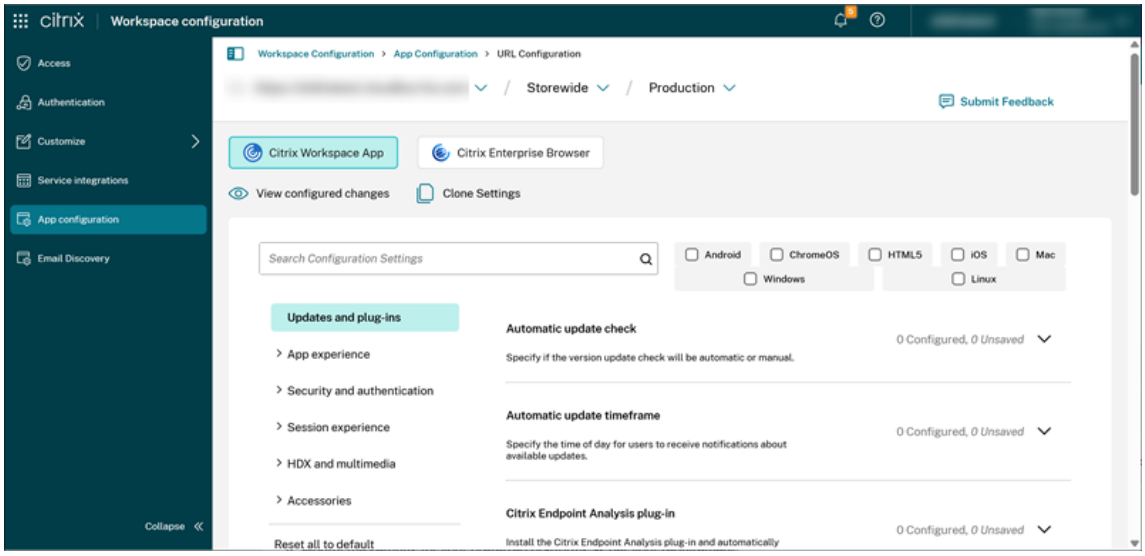
您可以从 Citrix Cloud 门户配置 Citrix Workspace 应用程序的设置。如果已为您的组织配置了多个应用商店，则可以单独配置每个应用商店。

1. 登录 Citrix Cloud。
2. 导航到 工作区配置 > 应用程序配置。
3. 从已配置的商店 URL 列表中，选择您要映射设置的商店，然后单击 配置。



4. 根据您的要求修改首选平台的设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



5. 单击 **Publish Drafts**（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。

使用配置文件管理用户组的设置

本节介绍管理员如何使用全局应用程序配置服务 (GACS) 中的配置文件功能为使用 Citrix Workspace 应用程序云存储的用户组配置设置。

要开始使用此功能，管理员需要验证其 Citrix Workspace 应用程序版本是否兼容，如下表所示：

Citrix Workspace 应用程序平台	支持的最低版本
Windows	2405
Mac	2405.11

配置

有关利用配置文件将设置分配给用户组的说明，请参阅 使用配置文件管理用户组的设置。

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。要为云存储启用此服务，请执行以下步骤：

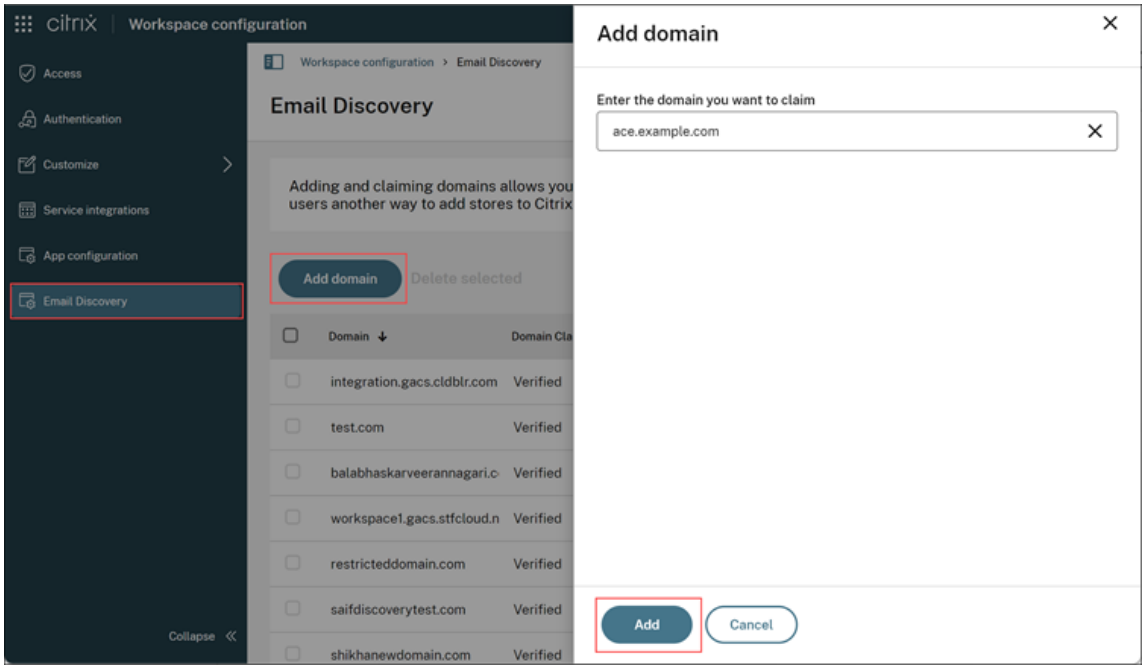
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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. 登录 Citrix Cloud。
2. 导航到 工作区配置 > 电子邮件发现。
3. 单击 添加域。
4. 输入您想要声明的域名（例如，`ace.example.com`）。

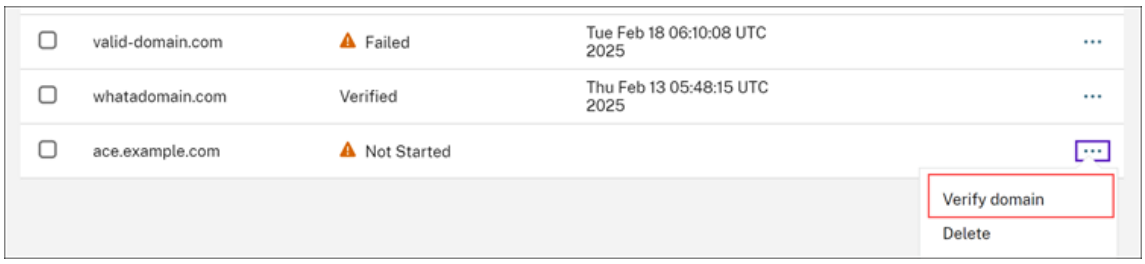


5. 单击添加。

   您可以看到域名已添加到 电子邮件发现 页面上。

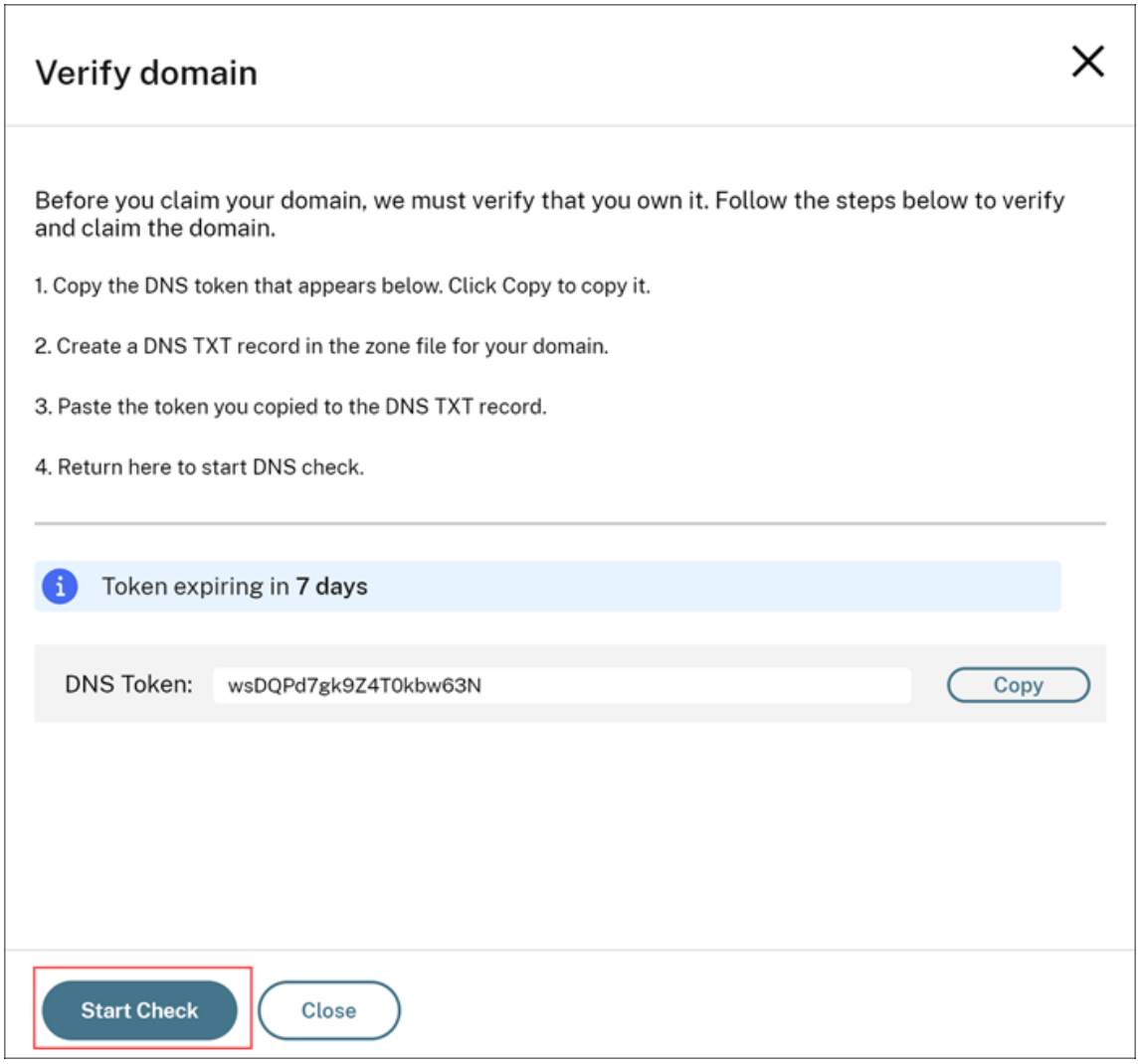
   域名声明状态显示为 未开始。您需要按照以下步骤验证域名：

6. 单击省略号菜单（…），然后选择 验证域。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

7. 复制屏幕上显示的 DNS 令牌，然后单击 开始检查。



您的域名状态更改为 待定。

验证完成后，您的域名状态将从 待处理 更改为 已验证。

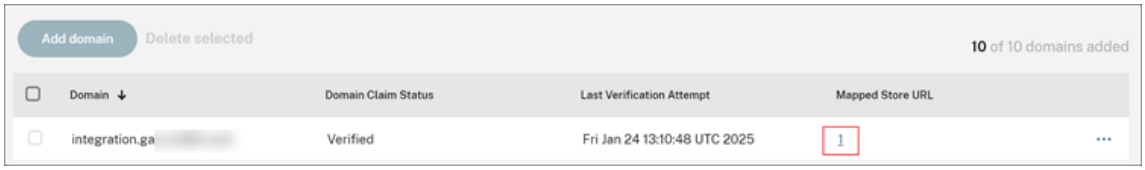
> 注意：
>
> 您最多可以声明 10 个域名。如果您想要申请超过 10 个域，请联系 Citrix 支持 并提供您的客户 ID。

创建域到 **URL** 的映射

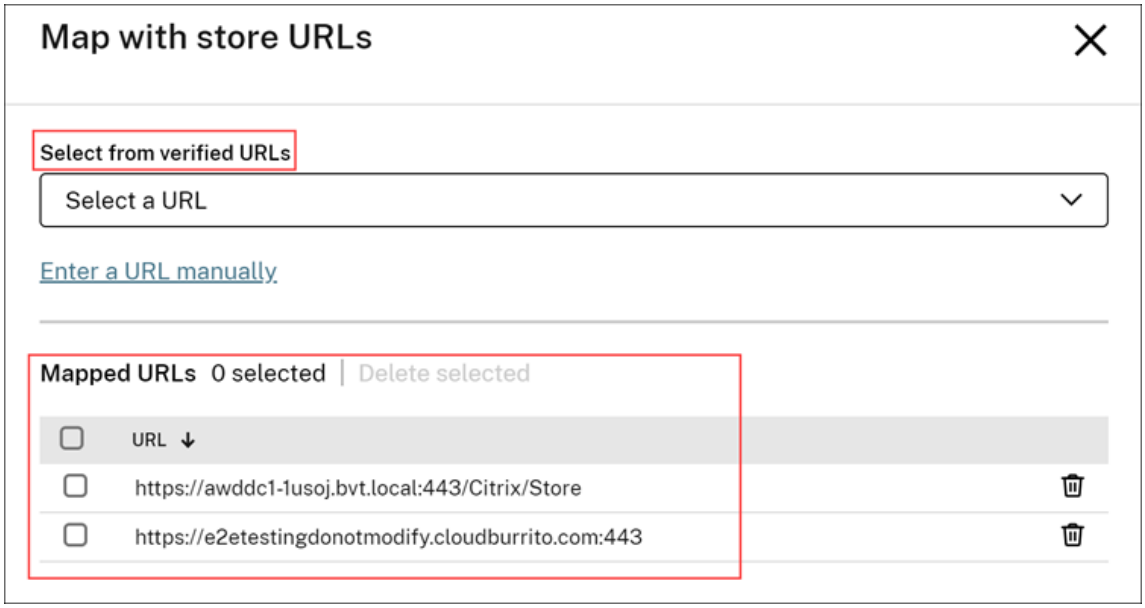
域名验证完成后，您可以按照以下步骤映射 URL：

1. 导航到 工作区配置 > 电子邮件发现。
2. 转到您已添加的域并单击映射的商店 URL。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



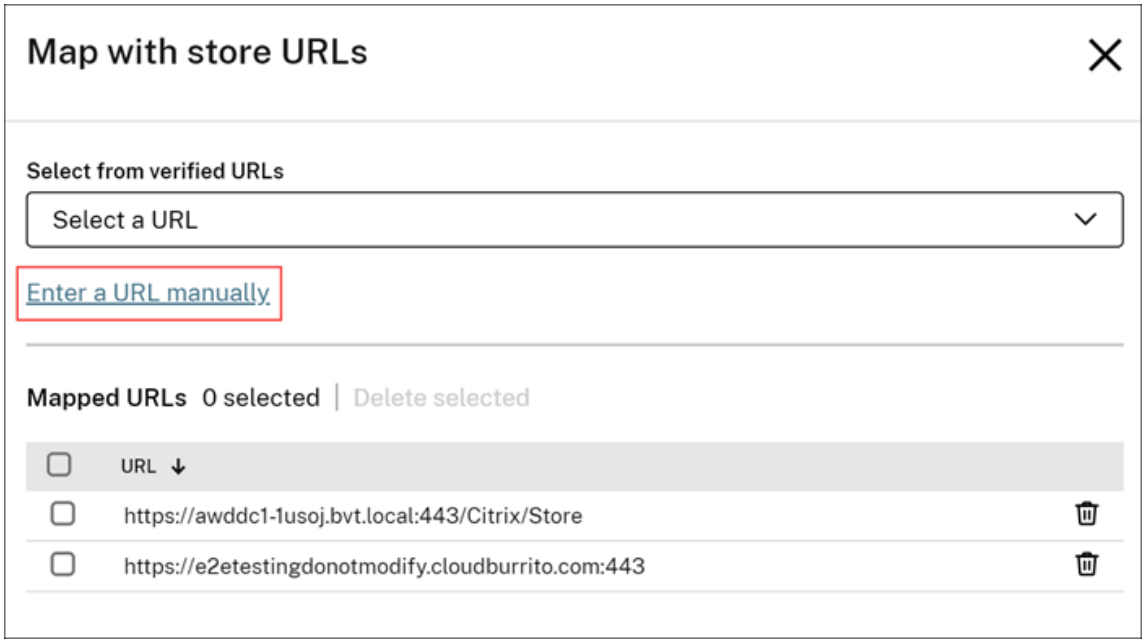
3. 从下拉菜单中选择已声明的 URL。



4. 单击保存。

或者，您可以使用 手动输入 **URL** 选项手动映射 URL。为此：

1. 单击 手动输入 **URL** 选项。



© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. 输入您要映射到此域的应用商店 URL。
3. 单击添加。

> 注意：
>
> 商店 URL 中必须包含端口号 443。例如，`https://example.cloud.com:443`。

为本地应用商店配置设置

March 15, 2025

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`>、<`https://gacs-discovery.cloud.com`>和 <`https://gacs-config.cloud.com`> 必须是可联系的。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。

开始配置

要配置本地商店的设置，请登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 应用程序配置。如果您已声明对 StoreFront URL 的所有权，请参阅 配置设置 部分了解更多信息。

如果您尚未认领您的 StoreFront URL，您可以认领它。为此，请单击 **App configuration** 部分下的 **Claim StoreFront URL** 来声明您的 URL。有关更多信息，请参阅 为本地存储声明 URL 部分。

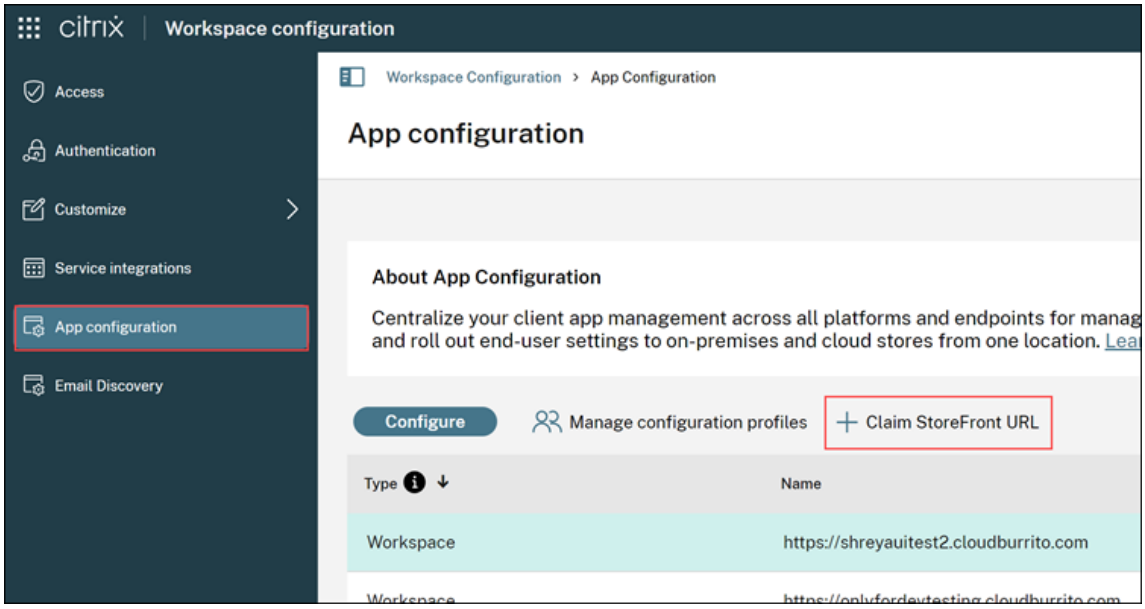
© 1997–2025 Citrix Systems, Inc. All rights reserved.

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：

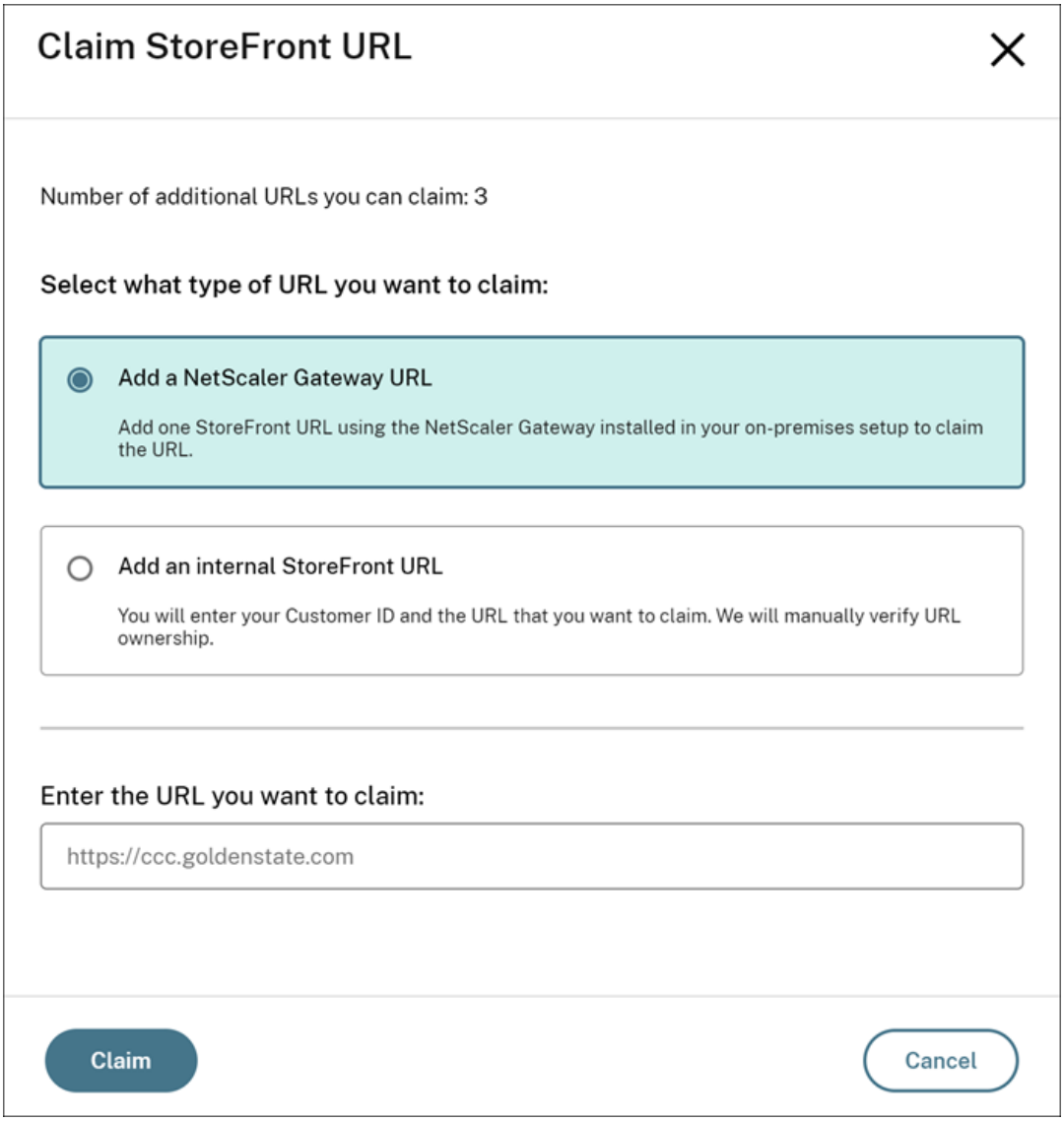
1. 登录 Citrix Cloud。
2. 导航到 工作区配置 > 应用程序配置。
3. 单击 声明 **StoreFront URL**。



4. 根据您的组织设置，选择 添加 **NetScaler Gateway URL** 或 添加内部 **StoreFront URL** 。
   - 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。选择 添加 **NetScaler** 网关 **URL**。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



b. 键入。在给定的文本字段中输入 URL。

c. 点击 领取。

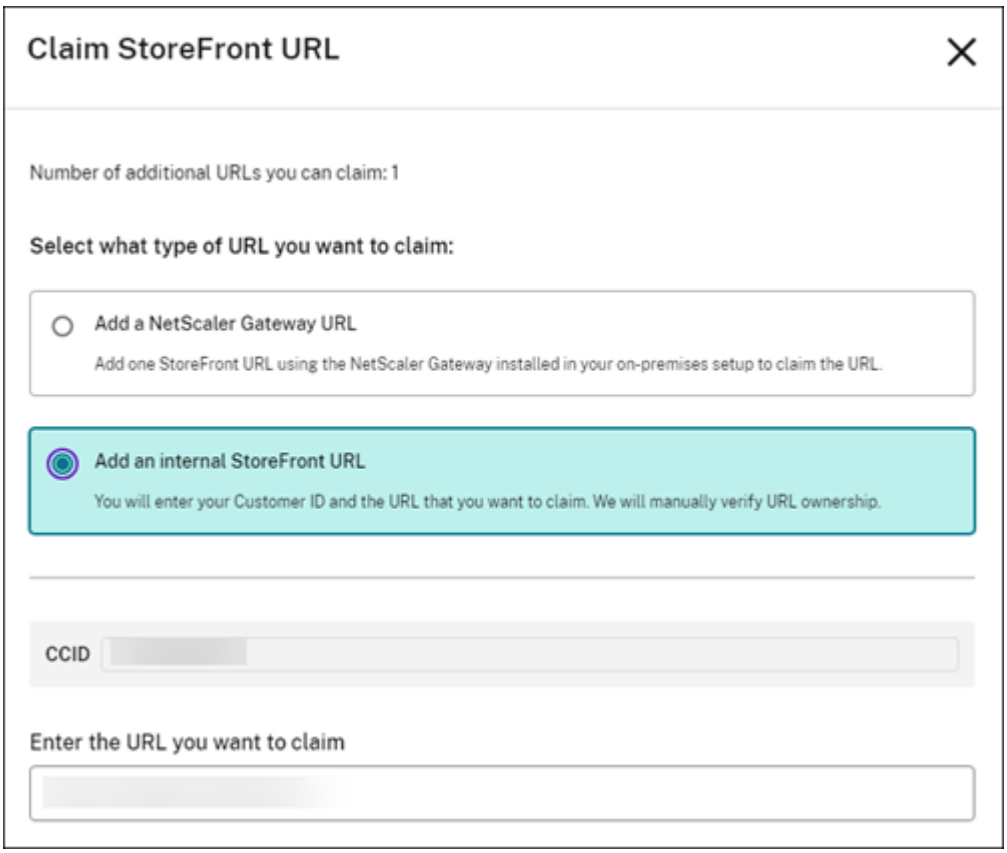
URL 已添加，处于‘未开始验证’状态。

- 如果要声明非基于 NetScaler 的 URL，请执行以下操作：

  a。选择 添加内部 **StoreFront URL**。

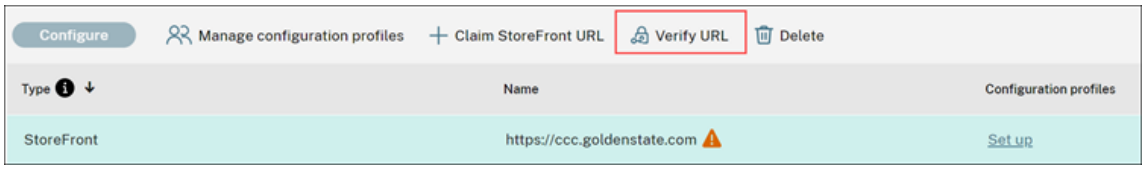
  b. 键入。输入您的客户 ID（CCID）和您想要认领的 URL。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



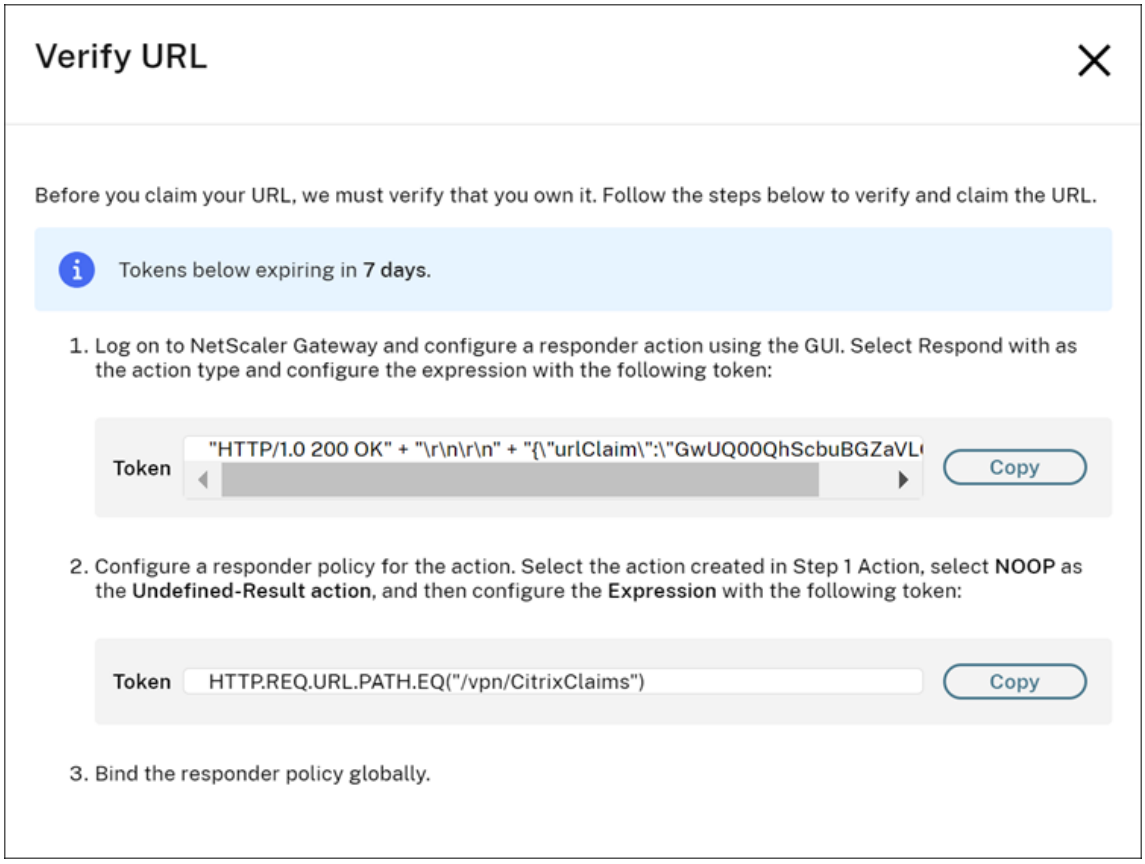
c. 点击 领取。

5. 要验证 URL，请选择 URL 并单击 验证 **URL**。



6. 验证 **URL** 屏幕包含指导您在 NetScaler 中创建和配置响应程序操作和响应程序策略的步骤。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



a。在全球范围内绑定您的响应者政策。

b. 键入。转到 `https://<customergatewayurl>/vpn/CitrixClaims` 验证您的响应策略是否配置正确。

c. 导航回 工作区配置 > 应用程序配置，并找到您添加的 URL。

d. 选择 URL 并单击 验证 **URL**。

e. 单击 验证 **URL** 开始验证过程。

> 注意：
>
> 一旦您单击 验证 **URL** ，URL 验证过程就会启动，大约需要 15 分钟才能完成。

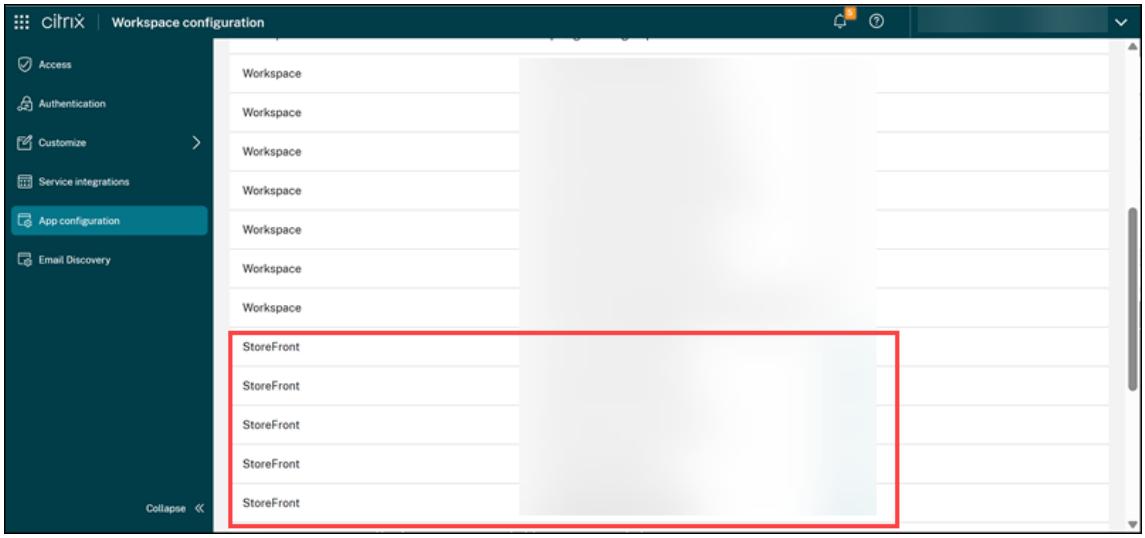
配置设置

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。

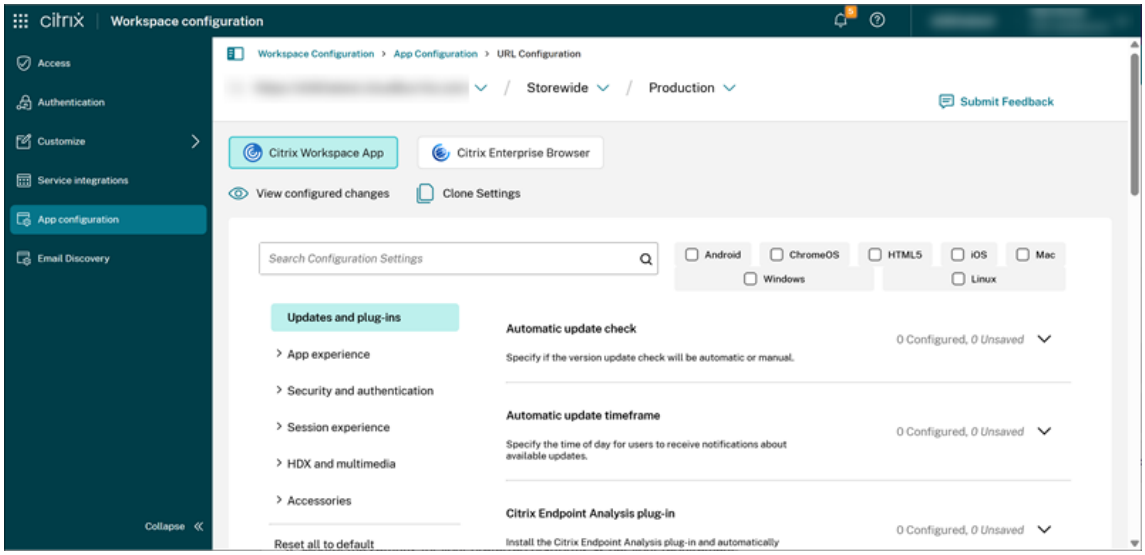
1. 前往 Citrix Cloud 门户并使用您的证书登录。
2. 导航到 工作区配置 > 应用程序配置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

3. 从已配置的 StoreFront URL 列表中，选择要映射设置的 URL，然后单击 配置。



4. 根据您的要求修改首选平台的设置。



5. 单击 **Publish Drafts**（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。

使用配置文件管理用户组的设置

本节介绍管理员如何使用全局应用程序配置服务 (GACS) 中的配置文件功能为使用 Citrix Workspace 应用程序本地存储的用户组配置设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

必备条件

要开始使用此功能，管理员需要满足以下先决条件：

- 验证 Citrix Workspace 应用程序版本
- StoreFront 服务器要求
- 为 Active Directory 管理配置 Cloud Connector 或 Connector Appliance
- 配置注册工具

验证 **Citrix Workspace** 应用程序版本　验证您的 Citrix Workspace 应用程序版本是否等于或高于下表中指定的版本。

Citrix Workspace 应用程序平台	支持的最低版本
Windows	2405
Mac	2405.11

StoreFront 服务器要求　StoreFront 服务器要求的最低版本是 2203.0.3000.14。

为 **Active Directory** 管理配置 **Cloud Connector** 或 **Connector Appliance**　Citrix Cloud Connector 和 Connector Appliance 是 Citrix 组件，用作 Citrix Cloud 和您的资源位置之间的通信渠道。它支持在资源位置内使用 Active Directory 林和域，从而允许管理员访问用于管理配置文件的 AD 组信息。

要了解有关 Citrix Cloud Connector 的更多信息，请参阅 Citrix Cloud 产品文档中的 Citrix Cloud Connector 。

要了解有关 Connector Appliance 的更多信息，请参阅 Citrix Cloud 产品文档中的 Connector Appliance for Cloud Services 。

配置注册工具　管理员需要在 StoreFront 服务器上下载并运行注册工具。注册工具会安装一个证书，以在 StoreFront 服务器和 GACS 之间建立信任。因此，GACS 可以收集有关他们所属的 AD 组的信息，以管理配置文件。

该过程涉及以下步骤：

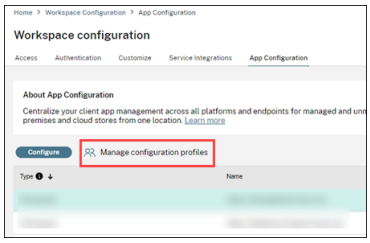
1. 生成注册工具。
2. 下载并运行注册工具。
3. 验证注册工具。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

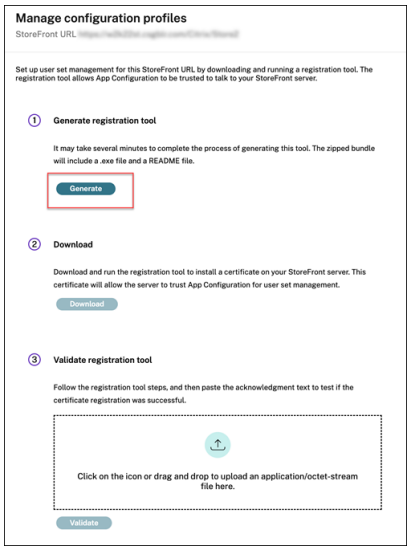
生成注册工具　注册工具是一个可执行文件，需要在组织内托管的 StoreFront 服务器上运行。这会将 GACS 注册为访问 AD 组信息的受信任服务。

要生成注册工具，请执行以下操作：

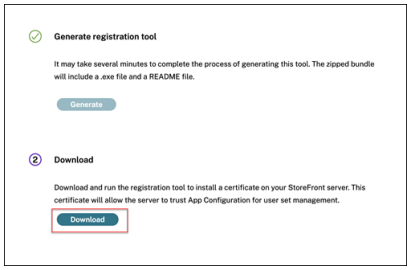
1. 导航到 工作区配置 > 应用程序配置。
2. 选择您的 StoreFront URL，然后单击 管理配置文件。



3. 在 管理配置文件 屏幕上，单击 生成 以生成注册工具。



下载并运行注册工具　下载注册工具：生成注册工具后，下载 选项将启用，允许管理员下载该工具。当管理员点击 下载 选项时，注册工具将以可执行格式下载。



> 注意：
>
> 注册工具以.zip 文件形式下载，并与 README 文件捆绑在一起。README 文件提供了下载和运行注册工具的详

© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 细说明。

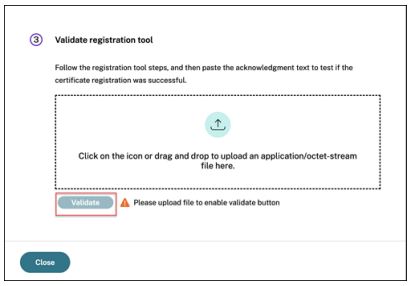
运行可执行文件：下载注册工具后，管理员可以运行注册工具在组织内托管的 StoreFront 服务器上安装证书。此证书允许服务器信任 GACS 进行配置文件管理。

运行注册工具时，您可以决定是在 StoreFront 服务器的单个商店还是所有商店上运行该工具。一旦运行该工具，它就会修改 StoreFront 商店的身份验证服务的 web.config 文件，该文件将 GACS 注册为受信任的服务。

> 注意：
>
> 由于注册工具执行成功，`web.config` 文件被修改后，IIS 重新启动。

验证注册工具　成功执行注册工具后，将下载一个包含确认文件和文本文件的.zip 文件。该文本文件提供从 StoreFront 服务器提取的以下信息：

- 公共证书：公共证书使 GACS 能够处理 StoreFront 服务器颁发的传入辅助令牌，以便向运行 Citrix Workspace 应用程序的客户端端点设备提供经过身份验证的基于组的设置。
- 配置值：提取与商店相关的各种配置值以保持一致性并确保商店在任何更改或恢复步骤后正常运行。



管理员必须按照以下步骤验证证书注册是否成功：

1. 上传确认文件。
2. 点击 验证。

证书注册验证成功后，将出现“注册已验证”消息。

1. 单击 关闭 按钮，您就可以看到 管理配置文件 屏幕。

配置　有关利用配置文件将设置分配给用户组的说明，请参阅 使用配置文件管理用户组的设置。

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。要为本地商店启用此服务，您需要执行以下步骤。

1. 声明域
2. 创建域到 URL 的映射

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。

> 注意：
>
> 商店 URL 中必须包含端口号 443。例如，`https://storefront.example.com:443`。

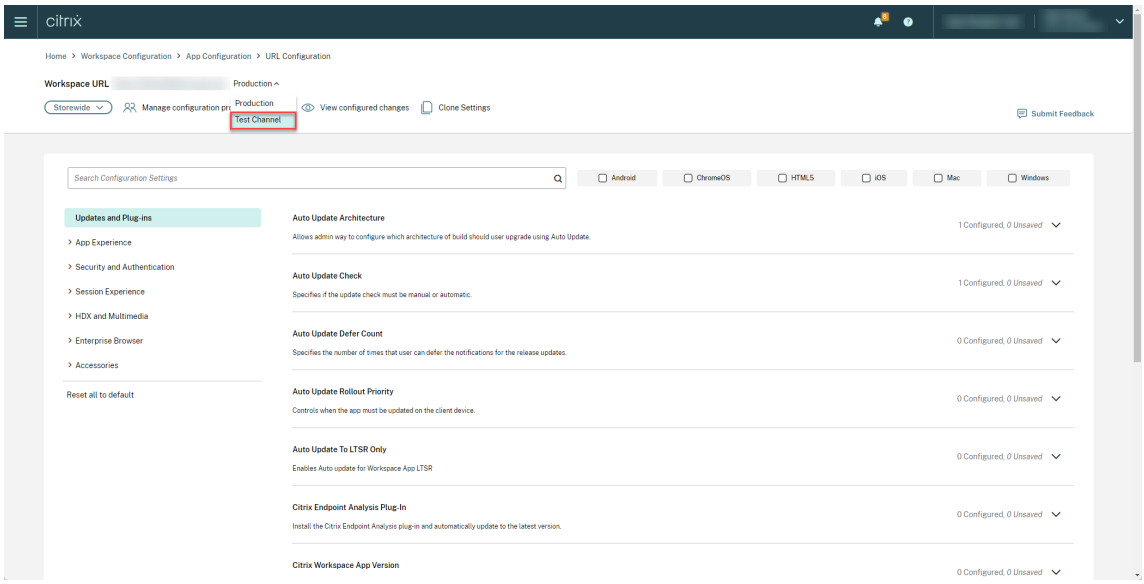
测试频道配置

November 7, 2024

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：

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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. 从已配置的商店 URL 列表中，选择您要映射设置的商店，然后单击 配置。
4. 单击下拉选项并选择 测试频道。默认情况下，它设置为“生产”。



5. 根据您的要求修改首选平台的设置。
6. 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
```

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。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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
```

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
```

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。

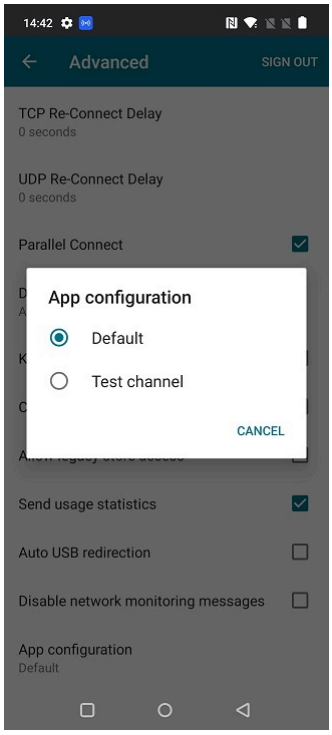
1. 登录 Citrix Workspace 应用程序。
2. 前往“设置”>“高级”>“应用程序配置”。
3. 选择测试频道。
4. 现在，您可以测试管理员定义的配置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

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。



管理 **Citrix Workspace** 应用程序版本

January 7, 2025

概述

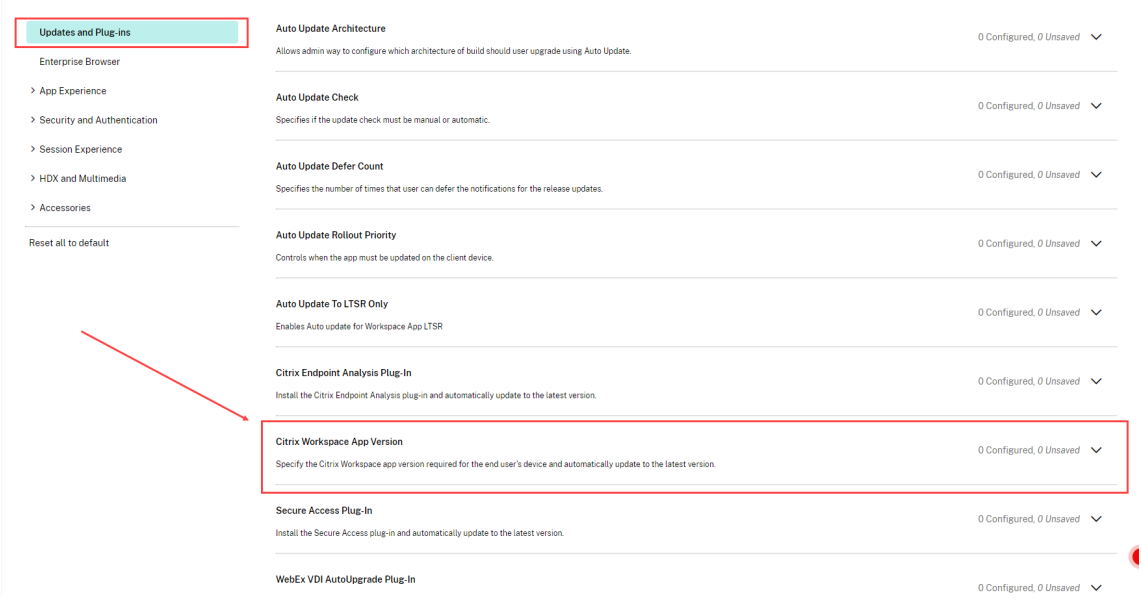
您可以使用 **Citrix Workspace** 应用程序版本 设置来指定最终用户必须使用哪个 Citrix Workspace 应用程序版本才能获得最佳效果。您可以设置一条规则，将应用程序更新到最新的 CR（当前版本）或 LTSR（长期服务版本）。您还可以指定是否必须自动升级或者最终用户是否可以手动更新应用程序。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

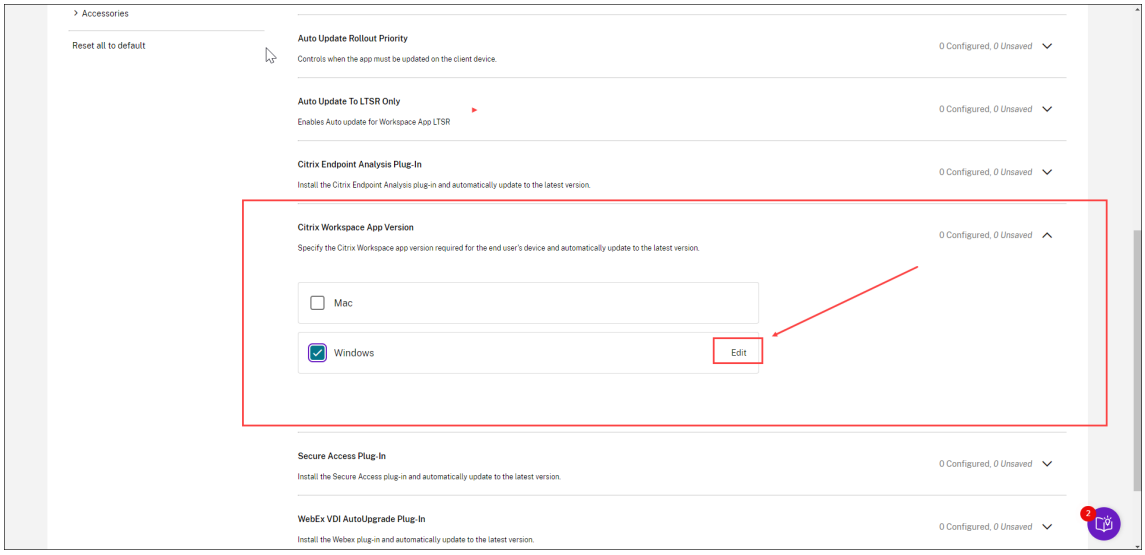
> 注意：
>
> 此设置仅可针对 macOS 和 Windows OS 配置。

要管理应用程序版本设置，请登录您的 Citrix Cloud 控制台。

1. 导航到 工作区配置 > 应用程序配置。
2. 转到 更新和插件 类别。
3. 展开 **Citrix Workspace** 应用程序版本 设置。



4. 选择 Windows 或 Mac 复选框，然后单击 编辑。



5. 您现在可以按照 管理版本设置 部分中的说明自定义设置。
6. 保存您的设置。

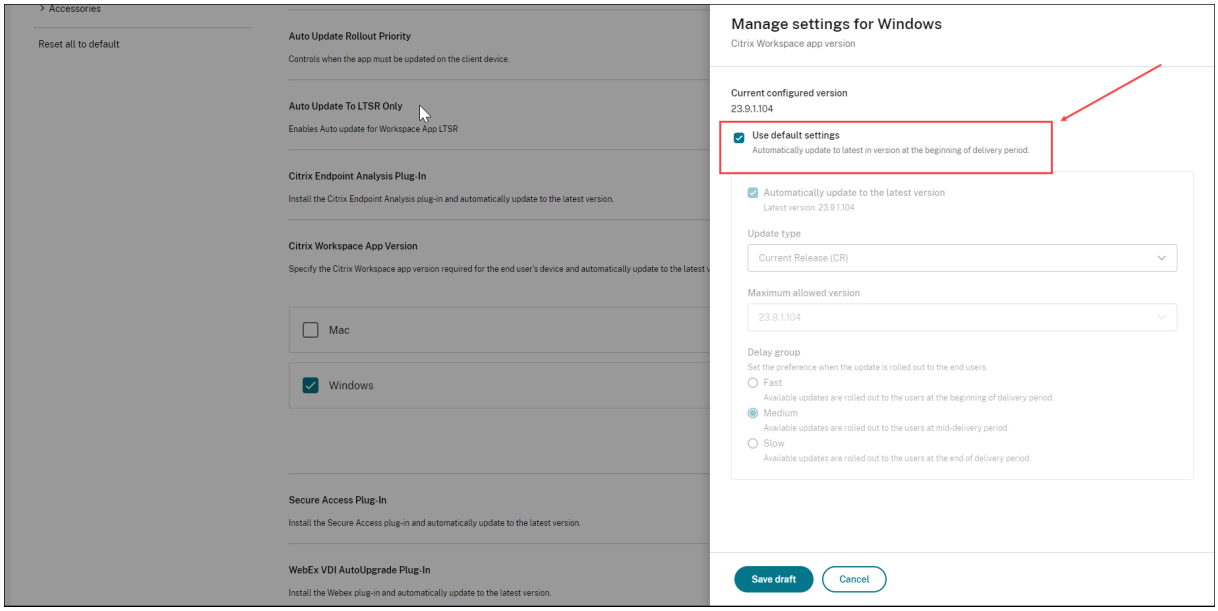
© 1997–2025 Citrix Systems, Inc. All rights reserved.

管理版本设置

您可以自定义 Citrix Workspace 应用程序版本设置以涵盖以下用例之一。

自动将您的最终用户升级到最新的 **CR** 版本

如果您选中 使用默认设置 复选框，您的最终用户将更新到最新的 CR 版本。升级将在交付期开始时自动进行，即新 CR 版本推出后立即自动进行。有关交货期的更多信息，请参阅 延迟组。



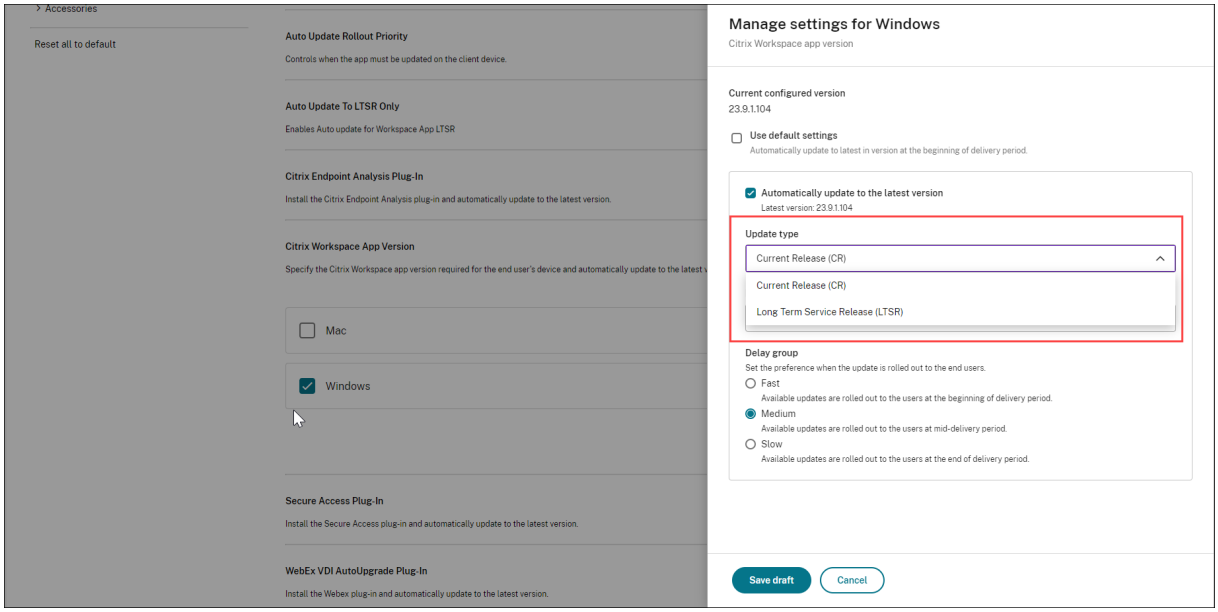
自动将您的最终用户升级到最新的 **LTSR** 或 **CR** 版本

自动更新到最新版本 设置使您能够将最终用户升级到最新版本。但是，您必须在 延迟组 设置下选择升级的交付期。

要使用此选项，您必须首先清除 使用默认设置 复选框。只有这样，您才能够选择 自动更新到最新版本 设置。在 更新类型 字段中，选择 LTSR 或 CR。

升级将按照您的延迟组设置进行。例如，如果您在“延迟”组下选择了“快速”，则应用程序会在新版本推出后立即自动更新。有关交货期的更多信息，请参阅 延迟组。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

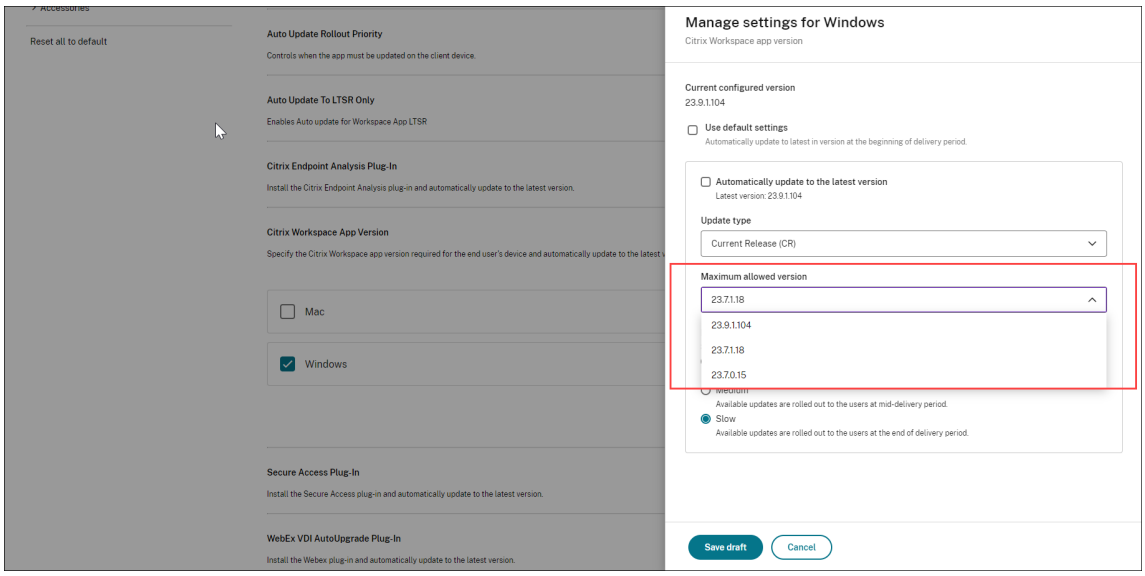


当应用程序自动更新到最新版本时，允许的最高版本 字段会自动禁用。

将最终用户升级到指定的 **CR** 或 **LTSR** 版本

如果您要选择最终用户必须更新到的特定版本，请按以下步骤操作。

1. 清除（禁用）使用默认设置 复选框。
2. 清除（禁用）自动更新到最新版本 复选框。
3. 在 更新类型 字段中，选择您喜欢的发布类型。
4. 在 允许的最高版本中，选择您想要将最终用户升级到的版本。您可以从 3 个先前版本的列表中选择适当的版本。



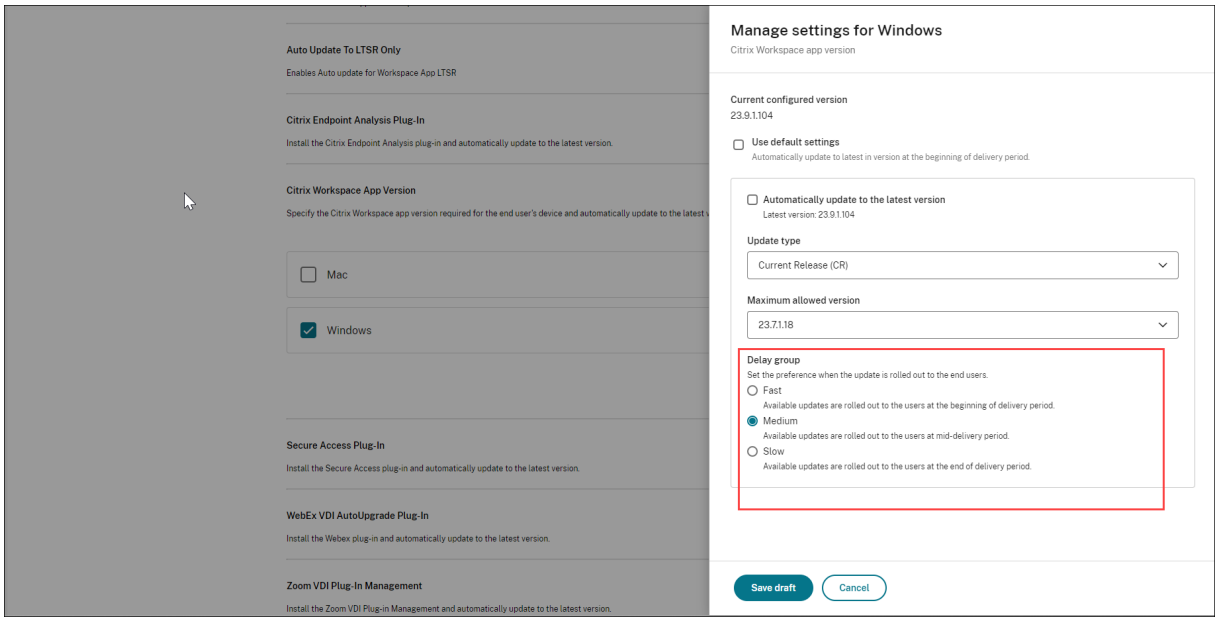
5. 在“延迟组”部分下，选择首选的交付期。有关交付期的更多信息，请参阅 延迟组。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

延时组

新版本的 Citrix Workspace 应用程序可用时，Citrix 会在特定交付期间推出更新。通过此选项，您可以控制在交付期间的哪个阶段可以接收更新。

- 快速：更新推出发生在交付期的开始。
- 中：更新推出发生在交付中期。
- 慢：更新推出发生在交付期结束时。



自动更新时间范围

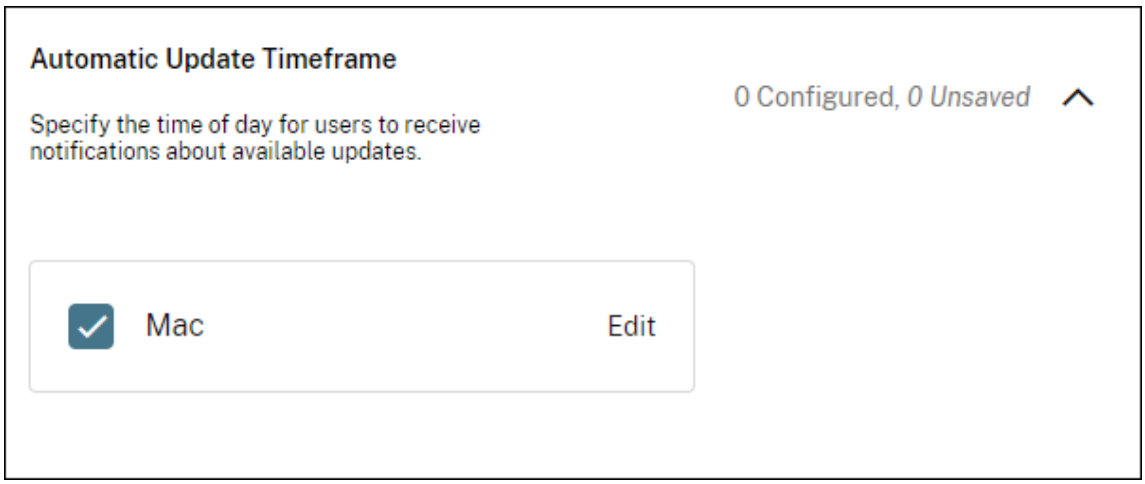
管理员现在可以在 Mac 设备上随时安排 Citrix 产品的自动更新。在此指定时间内，软件会自动更新，或者用户会收到可用更新的通知。此功能适用于 Mac 平台上的所有 Citrix 更新。目的是尽量减少对最终用户工作时间的干扰，从而提供增强的用户体验。

要启用此功能，请执行以下操作：

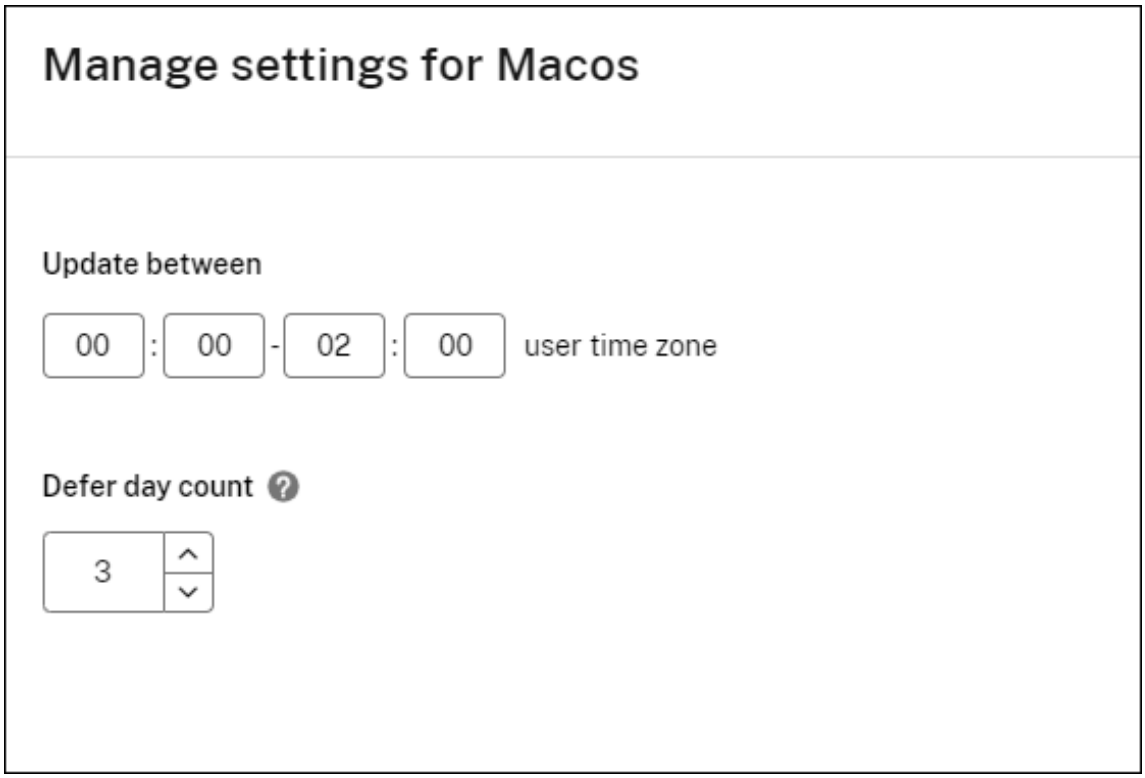
> 注意：
>
> 该功能目前仅在 Mac 平台上可用。

1. 在 Citrix Cloud 中导航到 工作区配置 > 应用程序配置。
2. 从列表中选择所需的商店网址。
3. 导航到 配置 > 更新和插件，然后单击 自动更新时间范围 设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



4. 选择适当的操作系统，然后单击 编辑 来定义自动更新发生的时间窗口。



在之间更新：在此字段中，添加您希望执行自动更新的开始时间和结束时间。

> 注意：
>
> 开始和结束时间应至少相差 1 小时，并且应在同一天。

推迟天数：在此字段中，提及用户可以推迟自动更新的次数。当用户用完了分配的延期计数时，自动更新将在 在 字段之间更新中定义的时间范围内发生。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Citrix Workspace 应用程序版本

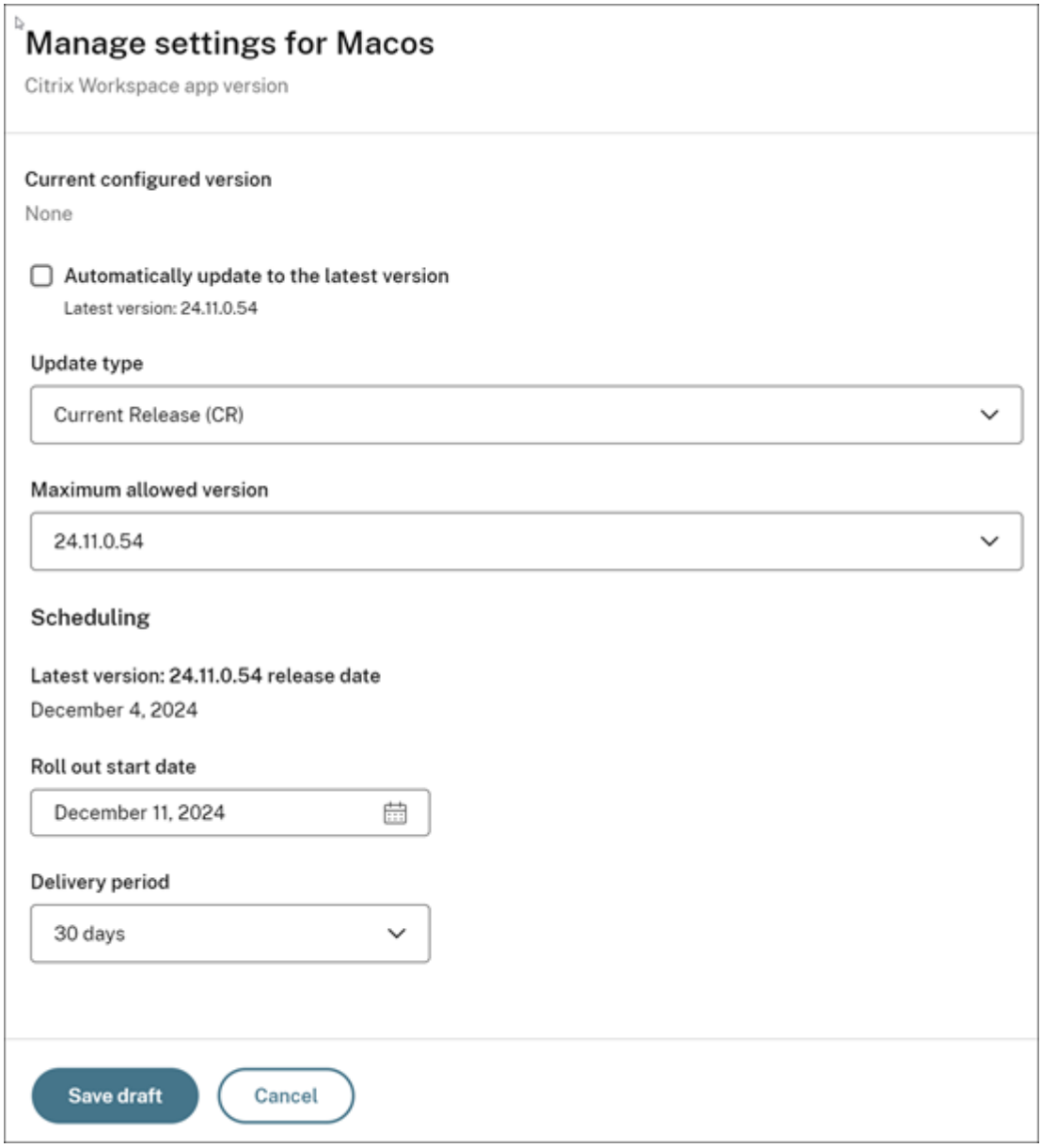
管理员可以安排方便的日期范围，在此期间 Citrix Workspace 应用程序的自动更新应推出给最终用户。此功能使他们能够确定推出日期，最大限度地减少对最终用户的干扰并改善用户体验。

要启用此功能，请执行以下操作：

注意：该功能目前仅适用于 Mac 平台上的 Citrix Workspace 应用程序。

1. 在 Citrix Cloud 中导航到 工作区配置 > 应用程序配置。
2. 从列表中选择所需的商店网址。
3. 导航到 配置 > 更新和插件，然后单击 **Citrix Workspace** 应用程序版本 设置。
4. 选择适当的操作系统，然后单击 编辑 来配置设置

© 1997–2025 Citrix Systems, Inc. All rights reserved.



允许的最高版本：定义您想要允许自动更新的最高软件版本。

推出开始日期：定义您希望开始 Citrix Workspace 应用程序自动更新的开始日期。一旦设定了日期，即使有更新版本的应用程序可用，它也不会更新。

交付期：输入自动更新推出的天数。自动更新过程将在指定的交付期内完成。交货期以 15 为增量。

> 注意：
>
> 仅当用户登录 Citrix Workspace 应用程序后才会发生自动更新。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

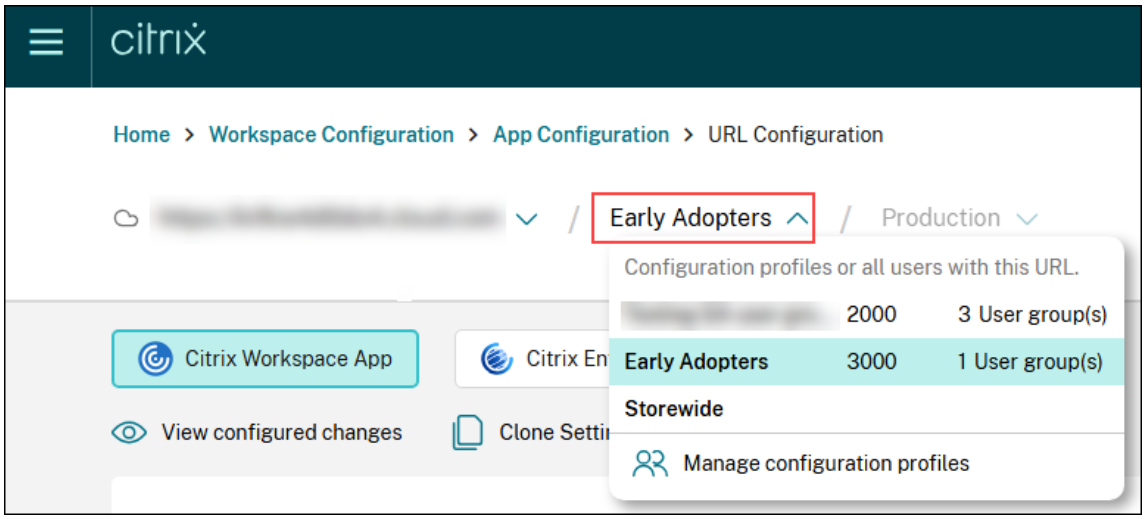
自动更新管理设置支持配置文件

自动更新管理设置（例如 自动更新时间范围 和 **Citrix Workspace** 应用程序版本）可通过配置文件适用于不同的用户组。

要启用此功能，请执行以下操作：

> 注意：
>
> 该功能目前仅在 Mac 平台上可用。

1. 在 Citrix Cloud 中导航到 工作区配置 > 应用程序配置。
2. 从列表中选择所需的商店网址。
3. 导航到 配置。
4. 从列表中选择一个配置文件。



5. 配置设置 自动更新时间范围 或 **Citrix Workspace** 应用程序版本，如 自动更新时间范围 和 Citrix Workspace 应用程序版本中所述。

使用全局应用程序配置服务管理插件

May 13, 2025

概述

通过全局应用程序配置服务，您可以从集中平台配置插件的安装和更新设置。这些插件必须由 Citrix 或其合作伙伴构建。全局应用程序配置服务 UI 为管理员提供了一个集中平台，用于在托管设备和个人设备之间分发插件。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

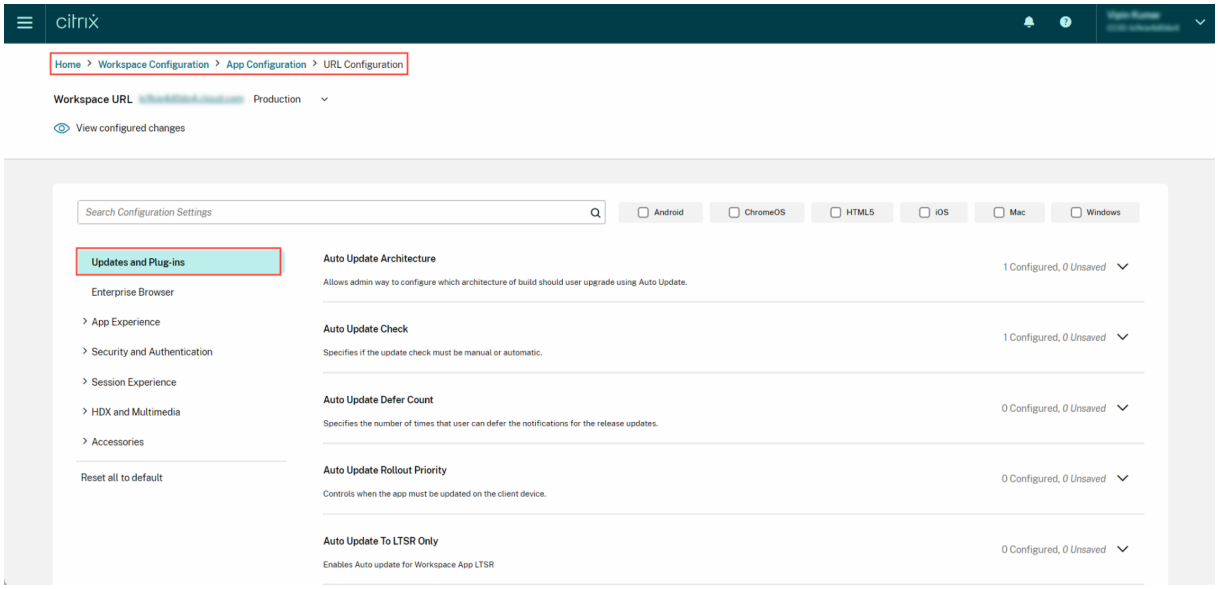
> 注意：
>
> 以下 Citrix Workspace 应用程序版本支持插件安装或升级：
>
> - 适用于 Windows 2212（当前版本）或更高版本的 Citrix Workspace 应用程序
> - 适用于 Windows 2402 (LTSR) 的 Citrix Workspace 应用程序
> - 适用于 Mac 的 Citrix Workspace 应用程序 2409 或更高版本

如果您的商店配置了 GACS，并且最终用户已将其添加到他们的 Citrix Workspace 应用程序中，则插件设置中的任何更改都会按照指定的持续时间 此处反映。这意味着您发布更改后，可能需要几个小时才能在客户端更新设置，具体取决于平台。

在客户端获取配置后，Citrix 自动更新服务将根据您的 延迟组 设置或在 24 小时内（以较早者为准）安装插件。

> 注意：
>
> 最终用户可以使用系统托盘中的 检查更新 选项手动更新到最新版本的插件。这将覆盖任何延迟组设置。但是，此选项还会将 Citrix Workspace 应用程序更新为最新版本或管理员指定的版本。

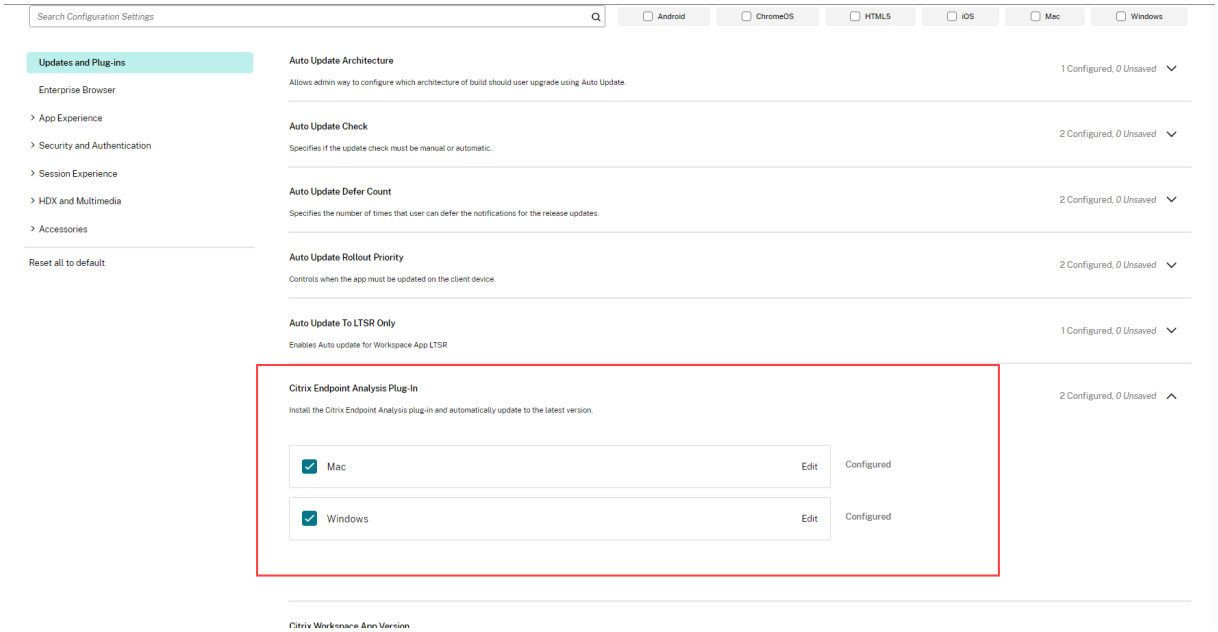
可以在 GACS UI 的 更新和插件 部分下找到支持的插件。



Citrix 端点分析插件

此设置可帮助您为最终用户安装 Citrix Endpoint Analysis 插件并将其更新为最新版本。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Citrix Endpoint Analysis 插件使您能够在最终用户设备上运行设备态势检查。Citrix Device Posture 服务是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求才能访问 Citrix DaaS（虚拟应用程序和桌面）或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）。

您可以按照 部署模式设置 部分中所述配置您的插件设置。

> 注意：
>
> 该插件仅适用于 Windows 和 Mac 平台。

有关更多信息，请参阅 管理设备姿态服务的 Citrix Endpoint Analysis 客户端。

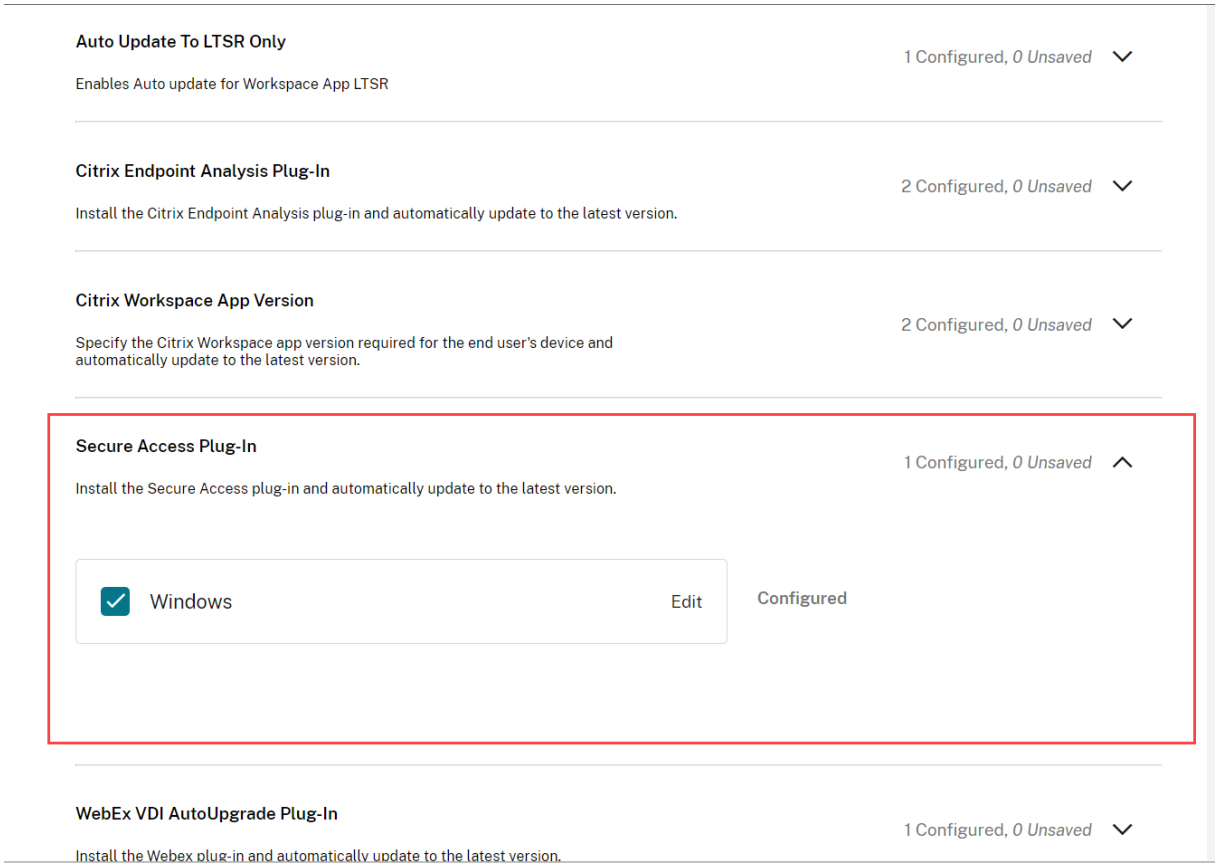
Citrix 安全访问代理

最终用户可以通过在客户端设备上安装 Citrix Secure Access 代理轻松访问所有经批准的私人应用程序。

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

您可以按照 部署模式设置 部分中所述配置您的插件设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Webex VDI 自动升级插件

Webex App VDI 解决方案优化了通话和会议的音频和视频。使用 GACS，您可以管理 Webex VDI 插件管理器。反过来，Webex VDI 插件管理器会安装并管理最终用户设备上安装的 Webex 插件。

> 注意：
>
> 该插件仅适用于 Windows 平台。

Webex VDI 插件安装程序引擎在 Citrix Workspace 应用程序的定期自动更新期间或手动检查更新时安装。

> 重要：
>
> Citrix 仅管理 Webex VDI 插件管理器的安装和更新。安装在最终用户设备上的 Webex 插件由 Webex 本身管理。

配置插件设置

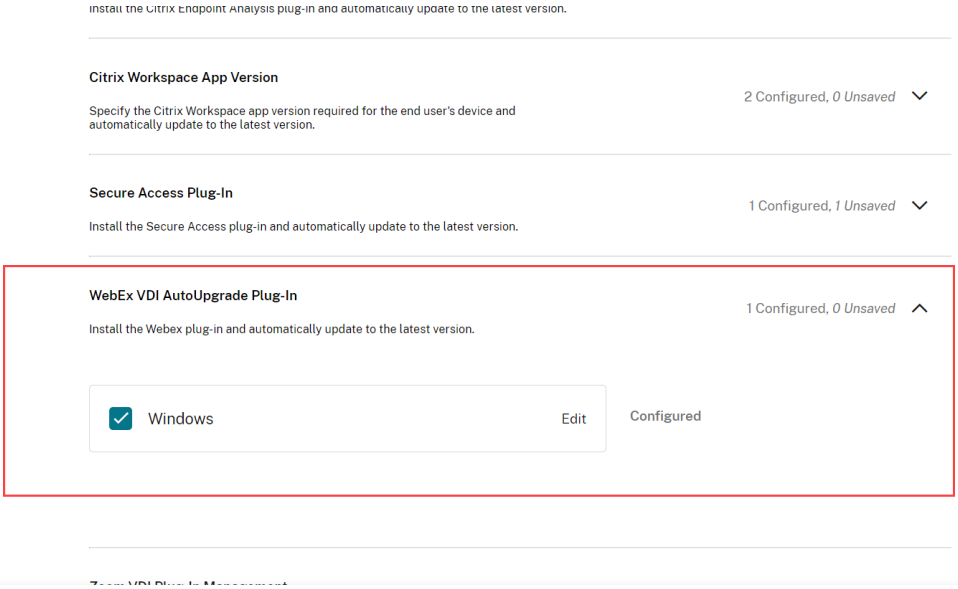
在继续之前，您必须确保已完成下面 先决条件 部分中列出的步骤。然后，您可以按照 部署模式 部分中所述配置插件设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

必备条件　配置虚拟通道必须遵循以下步骤：

1. 禁用或配置 Broker 上的虚拟通道列表策略，以允许 Webex 使用 VC，如 此处所述。
2. 使用以下注册表项在安装了 Webex App for VDI 的虚拟桌面上启用 VDI 插件的自动升级 `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Spark Native`，设置 `AutoUpgradeVDIPluginEna` `=1`

您现在可以登录您的 Citrix Cloud 帐户并按照 部署模式设置 部分中的说明配置您的插件设置。



Webex VDI 插件与 **Webex** 应用程序的兼容性

配置完成后，在 VDI 中运行的 Webex 应用程序的菜单中会出现一个刷新选项。单击刷新选项，Webex 应用程序将关闭，并且 Webex VDI 插件将安装在用户的端点上。

即使安装后，Webex VDI 插件也不会出现在 Windows 上的程序列表中。要检查插件是否已安装，您可以在 VDI 中运行的 Webex 应用程序上运行 健康检查。检查 **VDI** 部分以验证插件是否已安装。您还可以验证插件版本是否与 Webex 应用程序版本兼容。

Webex VDI 插件管理器会自动安装与最终用户的 Webex 应用程序兼容的最新 Webex 插件版本。有关兼容版本的更多信息，请参阅 Webex 版本支持。

如果版本不匹配，请使用以下步骤检查是否已禁用 VDI 上的兼容性检查：

1. 转到 “HKEY_LOCAL_MACHINE\Software\Cisco Spark Native\”。
2. 创建一个名为 `VDIDisableCompatibilityVersionCheck` 的 DWORD（32 位）注册表项，并为其赋予以下值之一：

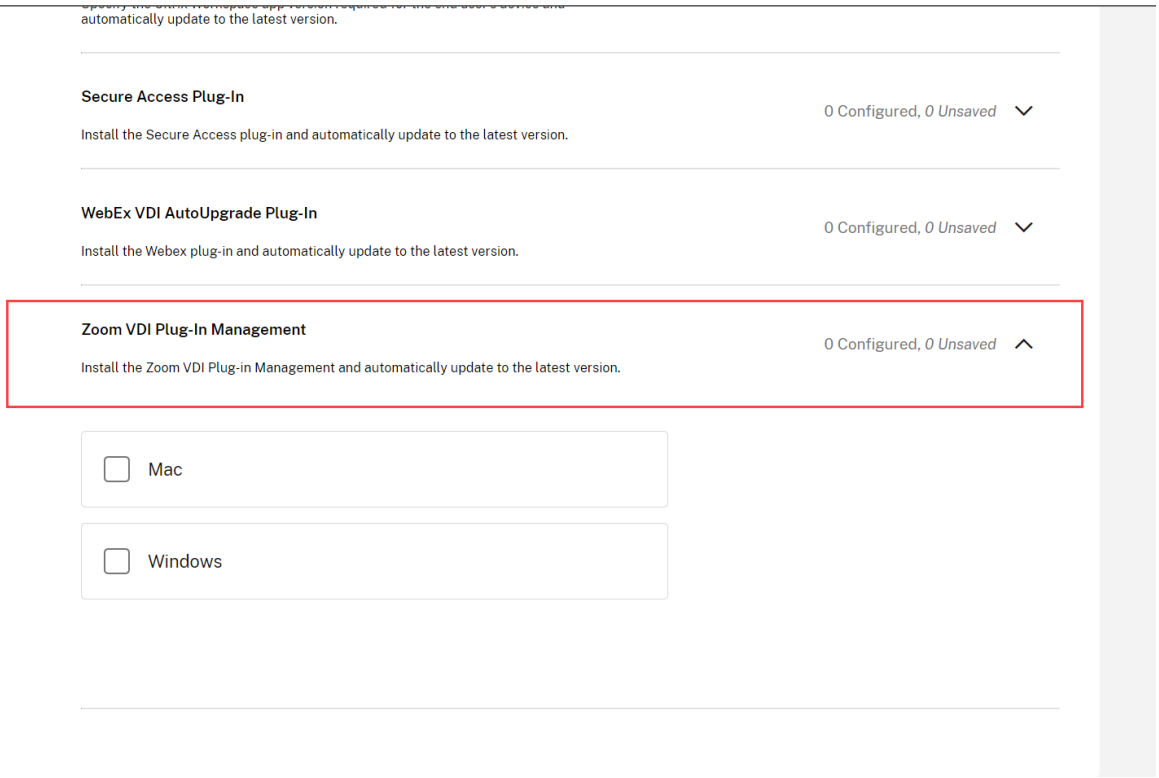
```
- 0 – enables the version compatibility check (default)
- 1 – disables the version compatibility check
```

© 1997–2025 Citrix Systems, Inc. All rights reserved.

Zoom VDI 插件管理

使用 GACS，您可以管理 Zoom VDI 插件管理器。反过来，Zoom VDI 插件管理器会安装并管理最终用户设备上安装的 Zoom 插件。

> 重要：
>
> Citrix 仅管理 Zoom VDI 插件管理器的安装和更新。安装在最终用户设备上的 Zoom 插件由 Zoom 本身管理。



配置插件设置

在继续之前，您必须确保已完成下面 先决条件 部分中列出的步骤。然后，您可以按照 部署模式设置 部分中的说明配置插件设置。

必备条件

配置虚拟通道必须遵循以下步骤：

1. 禁用或配置 Broker 上的虚拟通道列表策略，以允许 Zoom 使用虚拟通道，如 此处所述。
2. 使用注册表项启用 Zoom VDI 插件管理的虚拟桌面，如 此处所述。

您可以按照 部署模式设置 部分中所述配置您的插件设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置完成后，打开 Zoom 应用程序并使其在 VDI 上运行。一段时间后（在用户的端点上下载 Zoom VDI 插件安装程序后），用户应该会看到一个弹出窗口（提示），通知他们会话将断开以在端点上安装 VDI 插件。单击 **OK** 后，Zoom 将关闭 Citrix 会话并继续在用户的端点上安装插件。

Microsoft Teams VDI 插件管理

Microsoft Teams VDI 插件管理器可优化通话和会议的音频和视频。通过全局应用程序配置服务，您可以管理 Microsoft Teams 插件管理器的安装。反过来，该插件管理器会在最终用户的设备上安装并管理 Microsoft Teams 优化插件（VDI 2.0 或 Slimcore 引擎）。

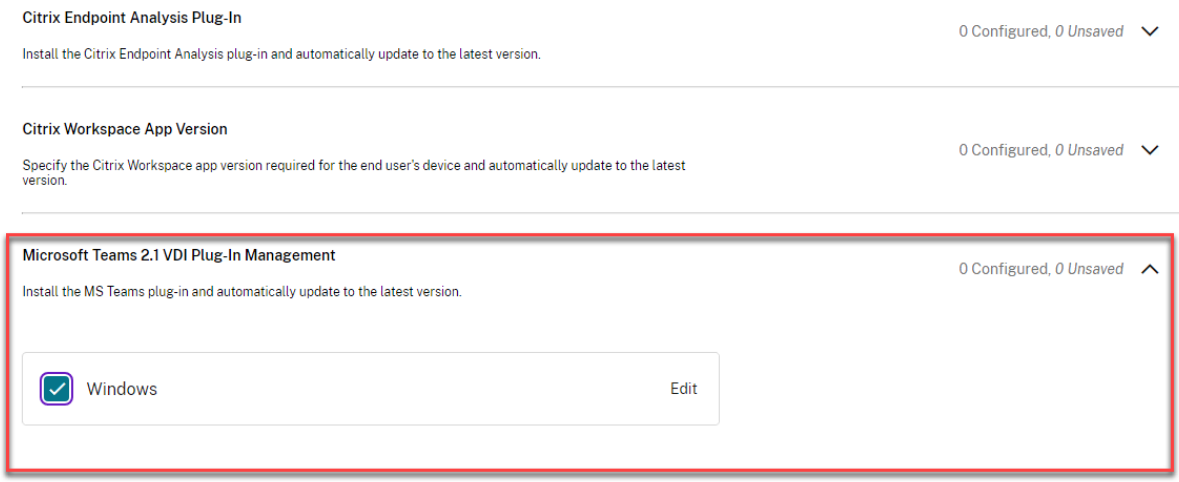
配置插件设置

在继续之前，您必须确保已完成以下 先决条件 部分中列出的步骤。

必备条件

管理员需要在 VDA 中配置新的注册表设置，以使新的 Microsoft Teams 能够访问 Citrix 虚拟通道。有关更多信息，请参阅 Microsoft Teams 优化中给出的 注释。如果您使用的是 CVAD 2402 LTSR 及以上版本（或）2203 LTSR CU5 及以上版本，则不需要此注册表设置。

您现在可以登录您的 Citrix Cloud 帐户并按照 部署模式设置 部分中的说明配置您的插件设置。



有关更多信息，请参阅 Teams 的新 VDI 解决方案。

> 注意：
>
> - 在最终用户设备上成功安装插件后重新连接会话。之后，需要重启两次 Microsoft Teams VDI 应用程序才能进入 VDI 2.0 模式。
> - 该插件仅在 Windows 平台上可用，从适用于 Windows 版本 2405 的 Citrix Workspace 应用程序开始

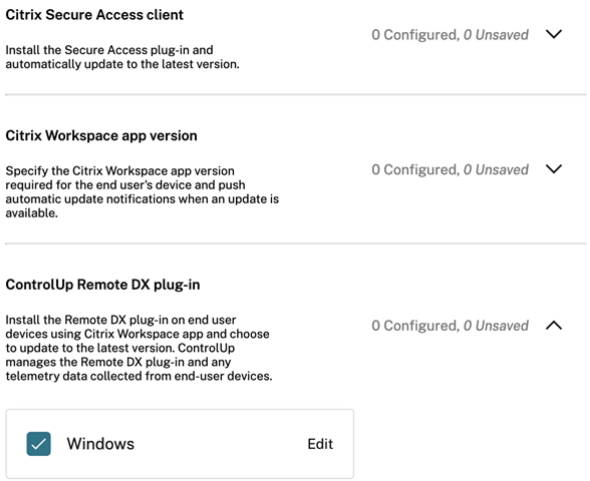
© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 适用。
> - 此插件仅适用于新团队（Teams 2.x），而不适用于经典团队。

ControlUp 的 **RemoteDX** 插件管理

ControlUp 的 RemoteDX 是一种监控和故障排除解决方案，旨在改善远程工作人员的最终用户体验。主要功能包括端点监控、网络洞察、会话可见性和主动警报。通过全局应用程序配置服务，您可以管理 ControlUp 的 RemoteDX 插件管理器。

> 重要：
>
> Citrix 仅管理 RemoteDX 插件管理器的安装和更新。ControlUp 直接管理安装在最终用户设备上的 RemoteDx 插件。RemoteDX 插件从最终用户设备收集的遥测数据（如果有）也由 ControlUp 管理。

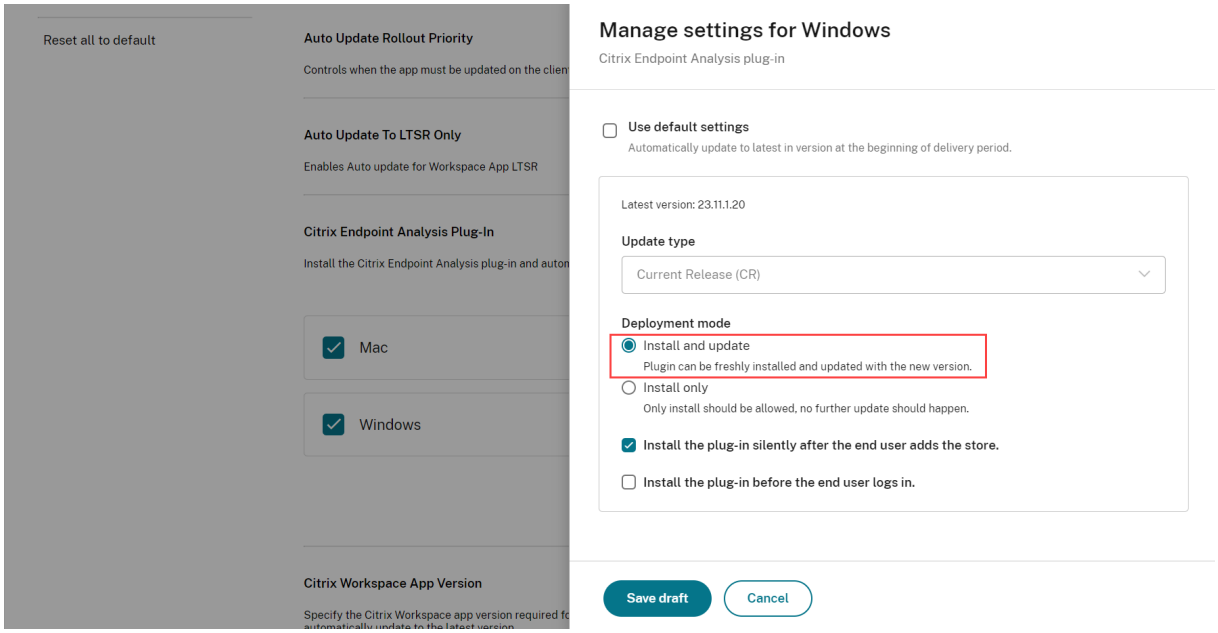


部署模式设置

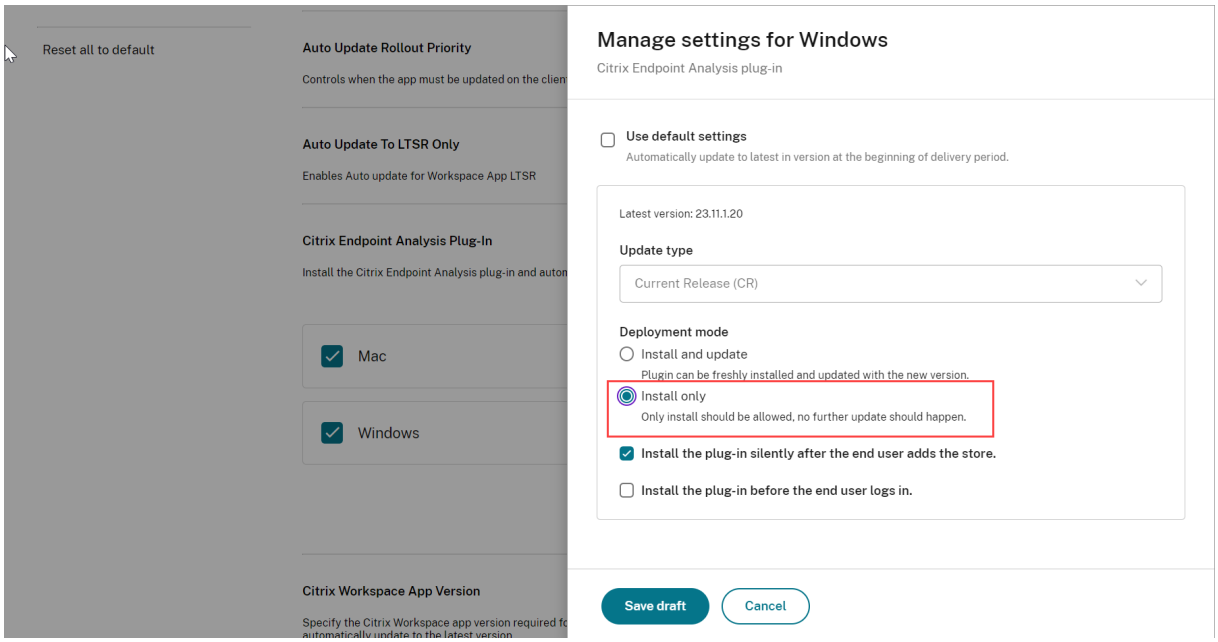
登录您的 Citrix Cloud 帐户并导航到 工作区配置 **>** 应用程序配置。从已配置的 URL 列表中，选择您想要映射设置的 URL，然后单击 配置。在 更新和插件 部分下，导航到所需的插件并单击展开图标以查看适用的平台。选择您要配置设置的平台，然后单击 编辑。

- 安装和更新：在最终用户的设备上安装最新版本的插件。它会自动将插件更新到最新版本。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

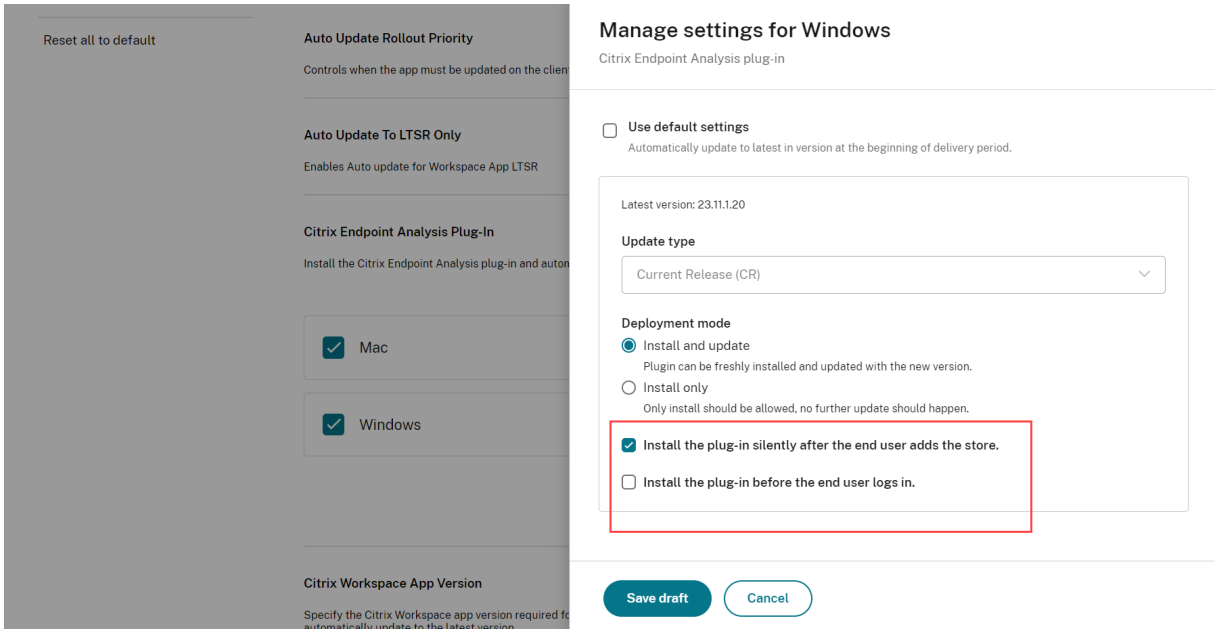


- 仅安装：在最终用户的设备上安装最新版本的插件。它不会自动更新。



选择部署模式后，您必须指定插件安装或更新是否需要最终用户的干预。您可以选择下列选项之一。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



- 最终用户添加商店后静默安装插件：最终用户添加商店后，安装插件或更新到最新版本。安装在后台完成，安装或更新完成后最终用户会收到通知。他们可以照常登录并访问他们的商店。
- 在最终用户登录之前安装插件：在安装完成之前，最终用户将无法登录到他们的 Citrix 商店。安装完成后，最终用户会收到通知。然后，最终用户将被重定向以进行身份验证并访问商店。升级发生在定期的自动更新周期中。

延时组

- 快速：更新推出发生在交付期的开始。
- 中：更新推出发生在交付中期。
- 慢：更新推出发生在交付期结束时。

使用配置文件管理用户组的设置

May 13, 2025

本节介绍如何使用全局应用程序配置服务 (GACS) 中的配置文件功能为用户组配置设置。

> 注意：
>
> 该功能目前适用于 Windows、Mac、Linux、Android 和 iOS 平台上的云商店。

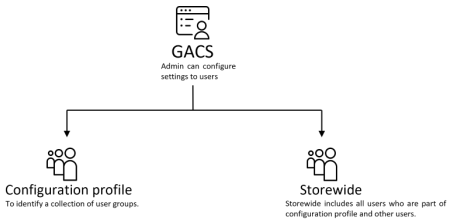
© 1997–2025 Citrix Systems, Inc. All rights reserved.

用户组和配置文件介绍

用户组是由管理员创建和管理的用户集合。为用户组配置设置可确保用户组内的所有用户同时拥有相同的体验。您可以利用存储在组织身份提供商 (IdP) 中的 AD 组信息，通过该 IdP 创建用户组。有关受支持的身份提供者列表的更多信息，请参阅 配置身份验证。

配置文件用于标识用户组的集合，它代表用户组的更高级别的抽象，每个配置文件可以包含多个用户组。如果您需要为特定用户组配置某些设置，您可以创建一个配置文件并将这些用户组添加到其中。您可以选择任何配置文件并为其分配设置，以便将体验应用于配置文件内的所有用户组。

> 注意：
>
> - 您最多可以创建 20 个配置文件。
> - 您最多可以在配置文件中添加 10 个用户组。



商店范围和配置文件的工作流程

管理员可以通过 Storewide 或配置文件为用户配置设置。本节介绍配置过程在 Storewide 和配置文件中的工作方式。

全店

当您为 Storewide 配置设置时，它将通过以下两种方式生效，具体取决于该设置的上下文：

- 仅适用于 **Storewide** 的设置：某些设置仅适用于 Storewide。例如，“使用 Web 浏览器进行身份验证”设置。当您配置此类设置时，它们适用于所有用户，包括配置文件中的用户。
- 对于 **Storewide** 和 **Configuration** 配置文件可用的设置：某些设置可用于 Storewide 和 Configuration 配置文件。例如，“重新连接应用程序和桌面”设置。当您为 Storewide 配置此类设置时，它们默认不会应用于分配到配置文件的用户。还必须在单独的配置文件中配置此类设置才能使这些设置生效。

有关配置 Storewide 设置的更多信息，请参阅 配置 Storewide 设置。

配置文件

当您为配置文件配置设置时，它将应用于该配置文件内的所有用户。

有关配置配置文件设置的更多信息，请参阅 配置配置文件的设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

设置优先级

当一个用户组属于多个配置文件时，优先级最高的配置文件的设置将应用于该用户或用户组。值越小，优先级越高。有关设置优先级的更多信息，请参阅 创建配置文件 和 编辑优先级。

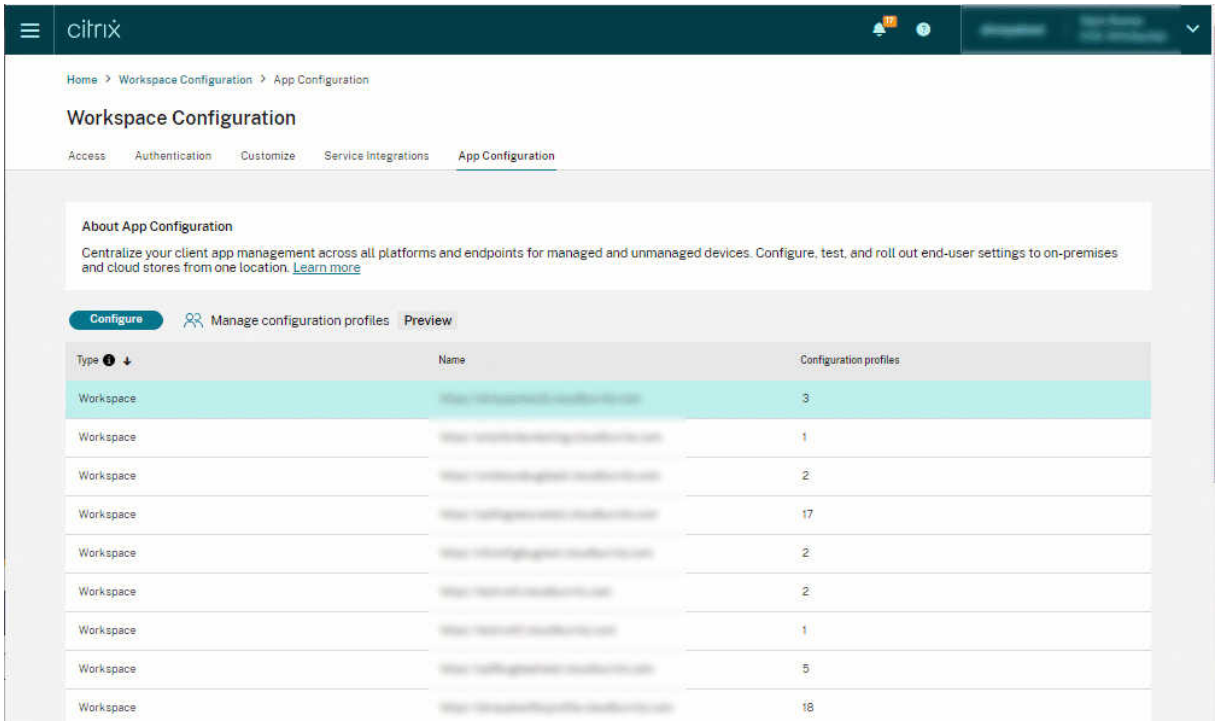
> 注意：
>
> 我们建议配置文件的优先级之间留出足够的间隙，例如 1000、2000、3000 等。这使得稍后创建其他配置文件时插入新的优先级值变得更加容易，而无需编辑现有值。

创建配置文件

您可以通过两种不同的方式创建配置文件。可以从 应用程序配置 页面或者 应用程序配置 > **URL** 配置 页面获取。

从“工作区配置”页面创建配置文件

1. 登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 应用程序配置。
2. 单击 管理配置文件。
3. 单击 创建 创建配置文件。
4. 分别在 名称、描述和 优先级 字段中输入配置文件的名称、描述和优先级。
5. 在 搜索用户组 字段中，输入关键字并搜索您想要添加到此配置文件中的用户组。您可以通过单击搜索列表中的用户组来添加所需的用户组。
6. 单击保存。

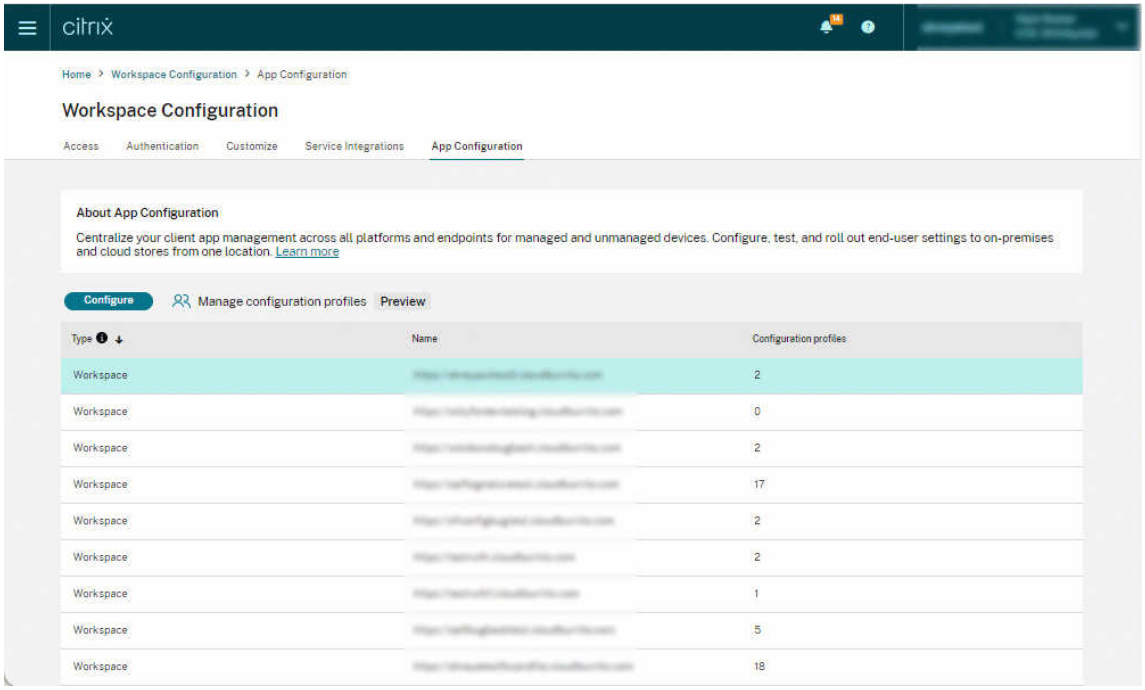


© 1997–2025 Citrix Systems, Inc. All rights reserved.

> 注意：
>
> 名称 和 优先级 是必填字段。

从 **URL** 配置页面创建配置文件

1. 登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 应用程序配置 > **URL** 配置。您可以通过单击 配置 按钮导航到 URL 配置页面。



2. 单击 管理配置文件，然后单击 创建。

有关更多说明，请参阅 从工作区配置页面创建配置文件中给出的步骤 3 –7。

编辑配置文件

1. 导航到 **Workspace** 配置 > 应用程序配置。
2. 单击 管理配置文件。
3. 从给定的列表中选择要删除的配置文件。
4. 单击编辑。
5. 更新相关字段，然后单击 保存。

编辑配置文件的优先级

1. 导航到 **Workspace** 配置 > 应用程序配置。

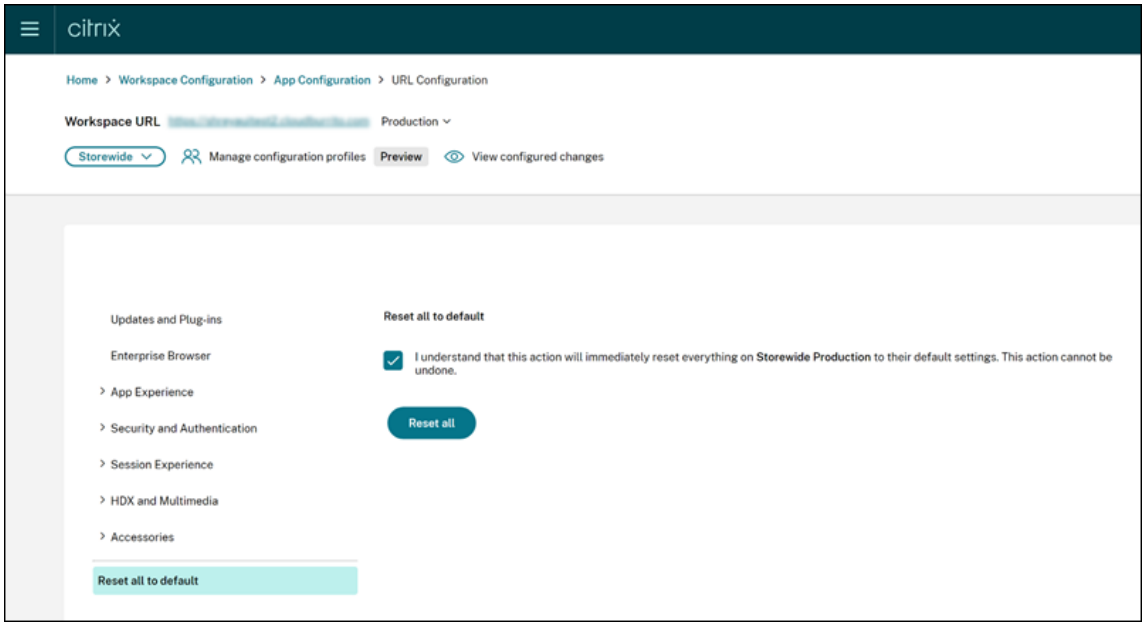
© 1997–2025 Citrix Systems, Inc. All rights reserved.

2. 单击 管理配置文件。
3. 从给定的列表中选择要删除的配置文件。
4. 点击 编辑优先级。
5. 更新优先级值，然后单击 ☒ 更新值或单击 ☒ 取消更改。
6. 单击关闭。

删除配置文件

要删除配置文件，您必须重置配置文件内的所有配置设置。详细步骤如下所示：

1. 导航到 **Workspace** 配置 > 应用程序配置。
2. 单击 配置 按钮，然后从下拉列表中选择适当的配置文件。
3. 点击 全部重置为默认。
4. 检查声明，然后单击“全部重置”。



> 注意：
>
> 如果您尚未为配置文件配置任何设置，则无需重置设置。因此，在这种情况下，您可以跳过步骤 2 至 4。

1. 单击 管理配置文件。
2. 从给定的列表中选择要删除的配置文件。
3. 单击删除。

> 注意：
>
> 您可以在 工作区配置 页面和 **URL** 配置 页面中使用 编辑、删除和 编辑优先级 选项。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

配置配置文件的设置

1. 登录您的 Citrix Cloud 帐户并导航到 工作区配置 > 应用程序配置 > **URL** 配置。
2. 从下拉列表中选择适当的配置文件。
3. 配置配置文件的相关设置。

配置全店设置

本节介绍您只需针对全店配置设置的两种场景。

用例 **1**：仅可针对全店配置的设置

某些设置不能具有针对用户组的自定义值。这些设置属于 Storewide 的一部分，在配置文件中访问时显示为非活动状态。您可以看到一条警告消息，其中有一个选项可以切换到 **Storewide** 配置页面。

或者，您可以按照以下说明配置整个商店的设置。

1. 导航到 工作区配置 > 应用程序配置 > **URL** 配置。
2. 从下拉列表中选择 **Storewide** 。
3. 配置相关设置。

用例 **2**：为其余用户配置设置

如果您尚未将任何用户分组到配置文件下，则剩余用户将受到 Storewide 的覆盖。要为此类用户配置设置，请参阅 中给出的步骤 1 –3 用例 1：只能为全店配置的设置。

> 注意：
>
> 当您为 Storewide 和配置文件配置设置时，配置文件在应用设置时具有最高优先级。

跨应用商店、渠道和配置文件克隆设置

November 7, 2024

克隆设置是指复制已通过全局应用程序配置服务配置的设置的能力。管理员无需再次经历整个配置过程，只需克隆现有设置即可，以节省时间和精力。此功能简化了工作流程，提高了生产力并保持一致性。

GACS 允许在以下场景中克隆设置：

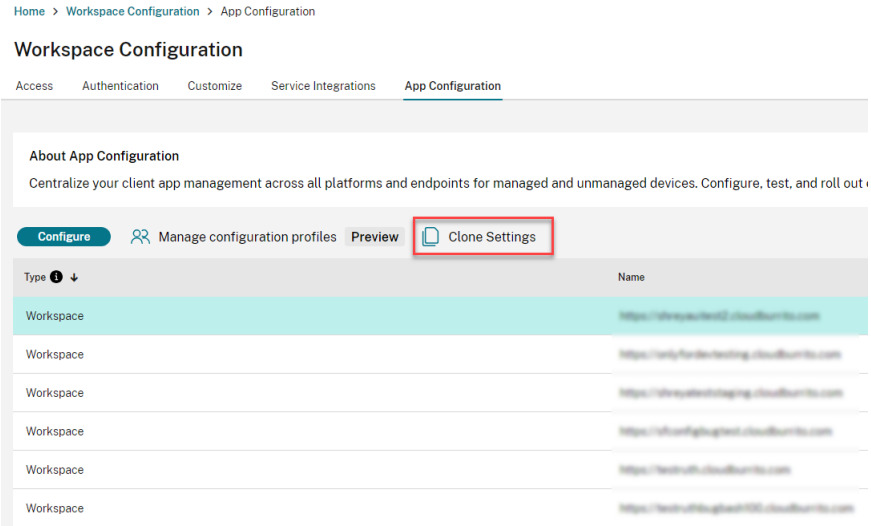
© 1997–2025 Citrix Systems, Inc. All rights reserved.

- 通道之间：将配置的设置从一个通道克隆到另一个通道。
- 配置文件之间：在商店内创建的配置文件之间克隆配置的设置。
- 从商店到配置文件：将商店范围内配置的设置克隆到配置文件。
- 商店之间：将配置的设置从当前商店克隆到另一个商店。

> 注意：
>
> - 克隆的设置将覆盖目标处的现有设置。
> - 某些仅限商店范围的设置无法通过“从商店到配置文件”选项克隆到配置文件中。
> - 仅同一类型的商店之间才可以进行商店之间的克隆。源商店和目标商店都需要是 Workspace 商店或 StoreFront 商店。

要使用此功能，您需要：

1. 在您的 Citrix Cloud 帐户中导航到 工作区配置 > 应用程序配置。
2. 从给定的商店列表中选择所需的商店，然后单击 克隆设置 选项。



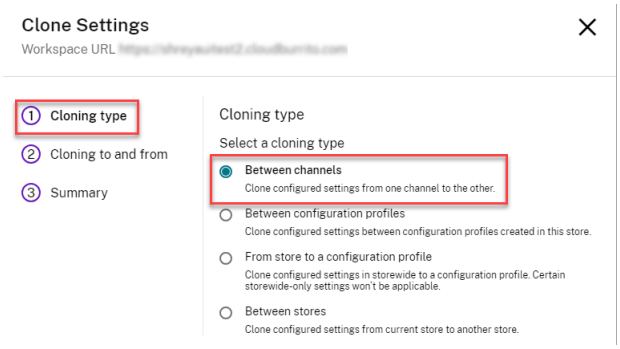
3. 从 克隆设置 窗口中选择一种克隆类型，然后单击 下一步。
4. 从下拉列表中选择适当的详细信息，选择 克隆到和从 克隆信息。

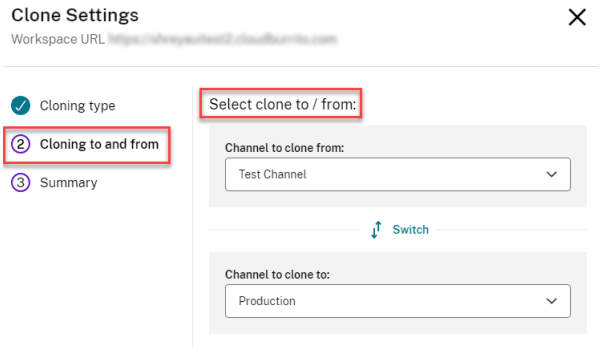
   有关步骤 3 和步骤 4 的更多信息，请参阅以下部分。

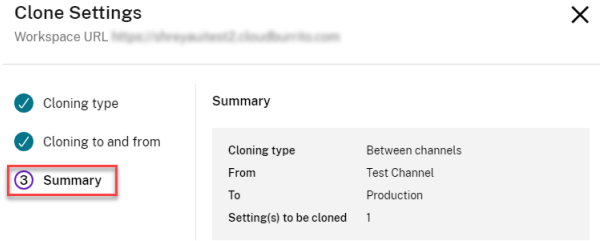
   通道间克隆设置：

   您可以在 Storewide 中克隆生产渠道和测试渠道之间的设置。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

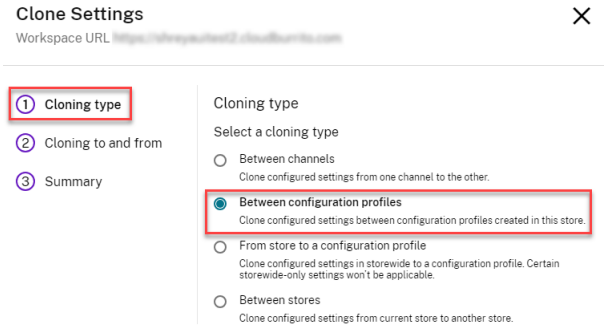




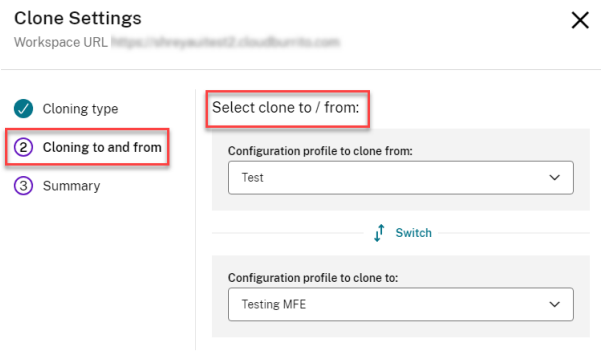


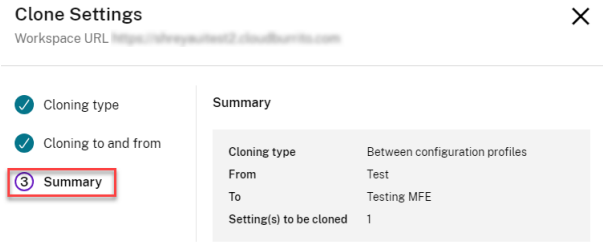
配置文件之间的克隆设置：

您可以在两个配置文件之间克隆设置。



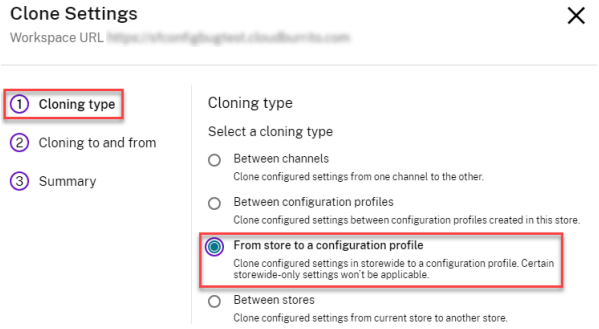
© 1997–2025 Citrix Systems, Inc. All rights reserved.

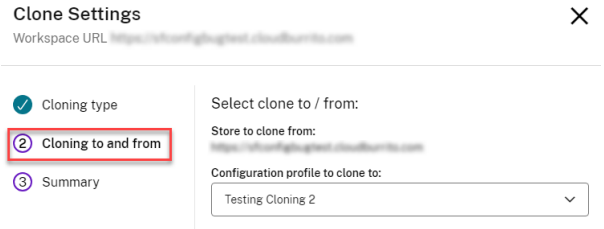




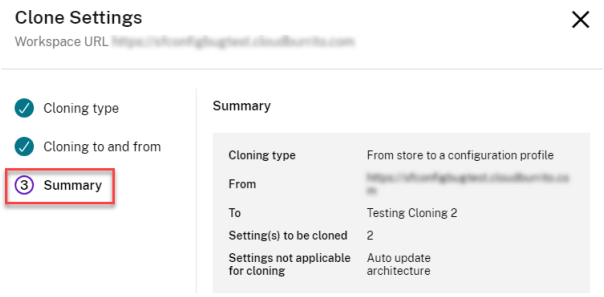
将设置从商店克隆到配置文件：

您可以将设置从商店克隆到配置文件。



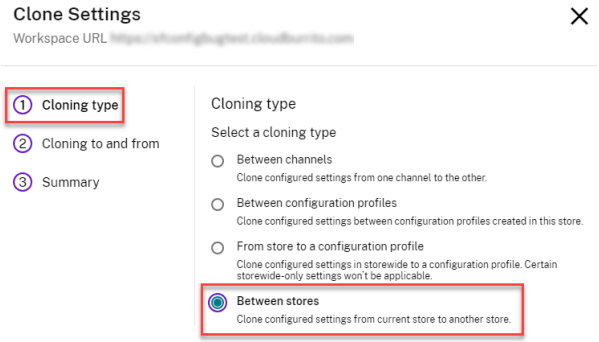


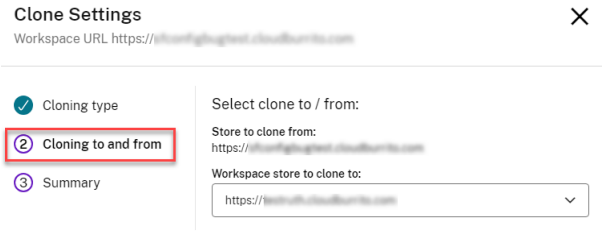
© 1997–2025 Citrix Systems, Inc. All rights reserved.

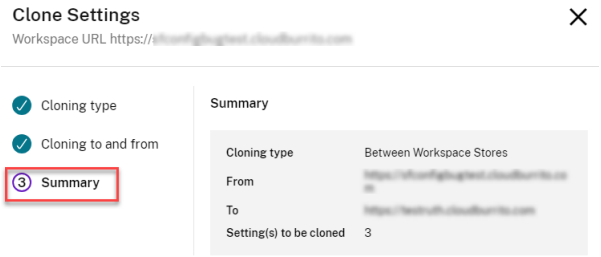


商店之间的克隆设置：

您可以在商店之间克隆设置。

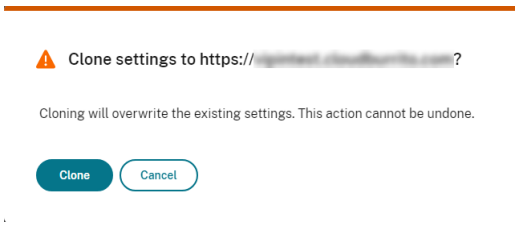




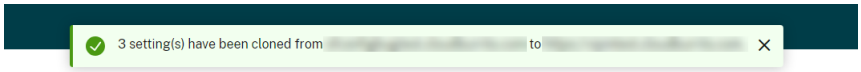


5. 在“等效 **CLI** 命令”中，查看命令并单击“下一步”。
6. 在 摘要 页面上验证配置的克隆设置，然后单击 克隆。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



克隆成功后您将看到通知。



管理混合启动设置（技术预览版）

May 13, 2025

Citrix Workspace 应用程序通过全局应用程序配置服务 (GACS) 实现混合启动场景的管理。

在混合启动场景中，用户通过 Web 浏览器访问其 Citrix 资源。在浏览器界面中选择应用程序或桌面后，Citrix StoreFront 服务器会生成一个 ICA 文件，其中包含启动该资源的具体说明。本机 Citrix Workspace 应用程序读取 ICA 文件的内容并启动与远程应用程序或桌面的连接。

通过支持混合启动，GACS 现在允许您为用户提供一致的体验，无论他们是通过本机应用程序还是浏览器访问商店。

Citrix Workspace 应用程序支持的版本

Citrix Workspace 应用程序平台	支持的最低版本
Windows	2503
Mac	2503

验证 **Citrix Workspace** 应用程序行为

本节介绍 Citrix Workspace 应用程序在混合模式下的各种用例中的行为。

场景	行为
用户通过 Web 浏览器访问商店并使用客户端重定向启动会话。	会话内设置仅从后续启动开始应用，而其余设置可供使用。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

场景	行为
用户在应用程序中添加商店，然后通过网络浏览器访问同一家商店。	通过本机添加的商店检索和应用设置。
用户通过 Web 浏览器从商店 1 打开一个会话，然后从商店 2 打开另一个会话。	从最近访问的商店启动的会话应用其设置。
用户打开会话，并且 GACS 设置在活动会话期间发生变化。	GACS 设置将在下次会话启动时应用。

> 注意：
>
> 会话启动完成后，将在 6 小时时间窗口后获取 GACS 设置。如果之前需要设置，用户必须转到“重置工作区”并再次启动会话。

云存储支持（技术预览）

首先，管理员需要启用内存混合启动。这意味着您必须禁用 ICA 文件下载才能在混合启动的情况下管理 Citrix Workspace 应用程序。要禁用 Workspace 的 ICA 文件下载，请参阅 Workspace PowerShell 文档。

> 注意：
>
> 目前不支持通过 Citrix Workspace 浏览器扩展进行混合启动。

要启用此功能，请使用此 启用表单提交请求。

本地支持

要开始使用此功能，管理员需要满足以下先决条件：

- 列入白名单 GACS 端点
- 配置注册工具
- 启用内存混合启动
- StoreFront 的最低支持版本为 2503。

> 注意：
>
> 目前不支持通过 Citrix Workspace 浏览器扩展进行混合启动。

列入白名单 **GACS** 端点

有关更多信息，请参阅 先决条件。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

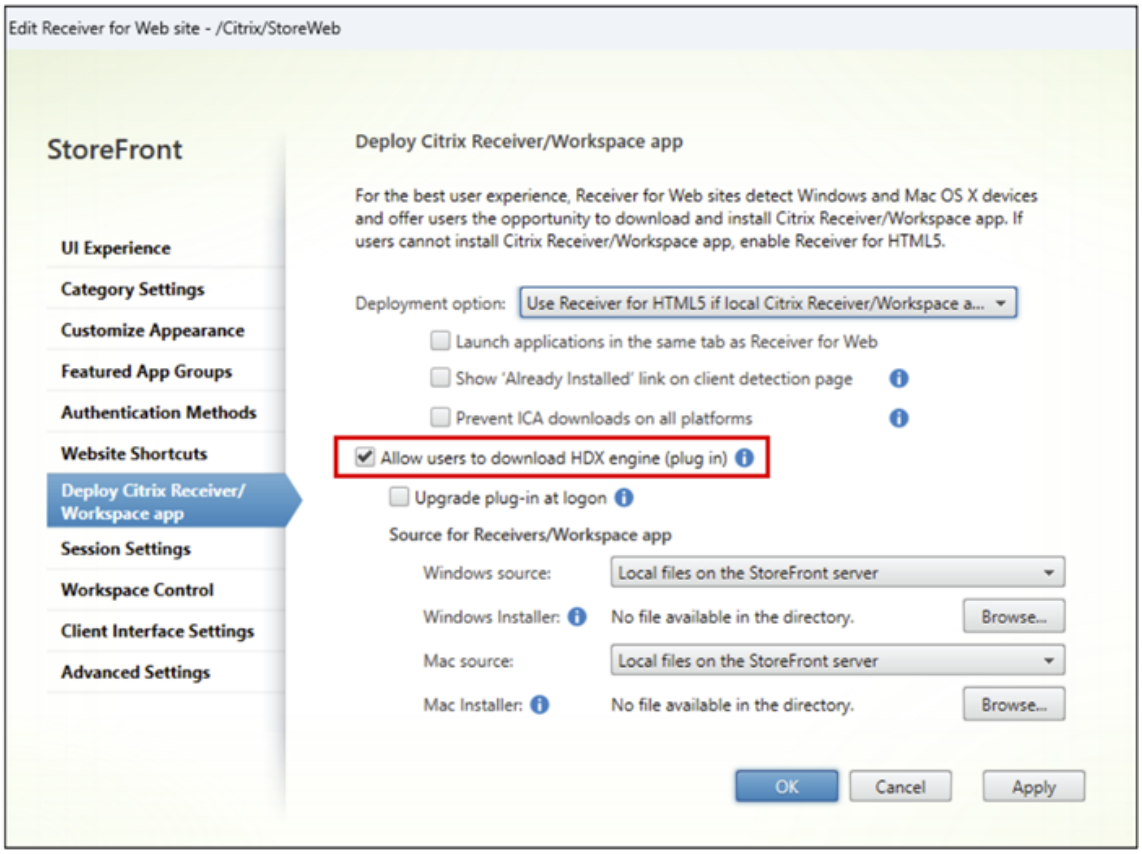
配置注册工具

有关详细信息，请参阅 配置注册工具。

启用内存混合启动

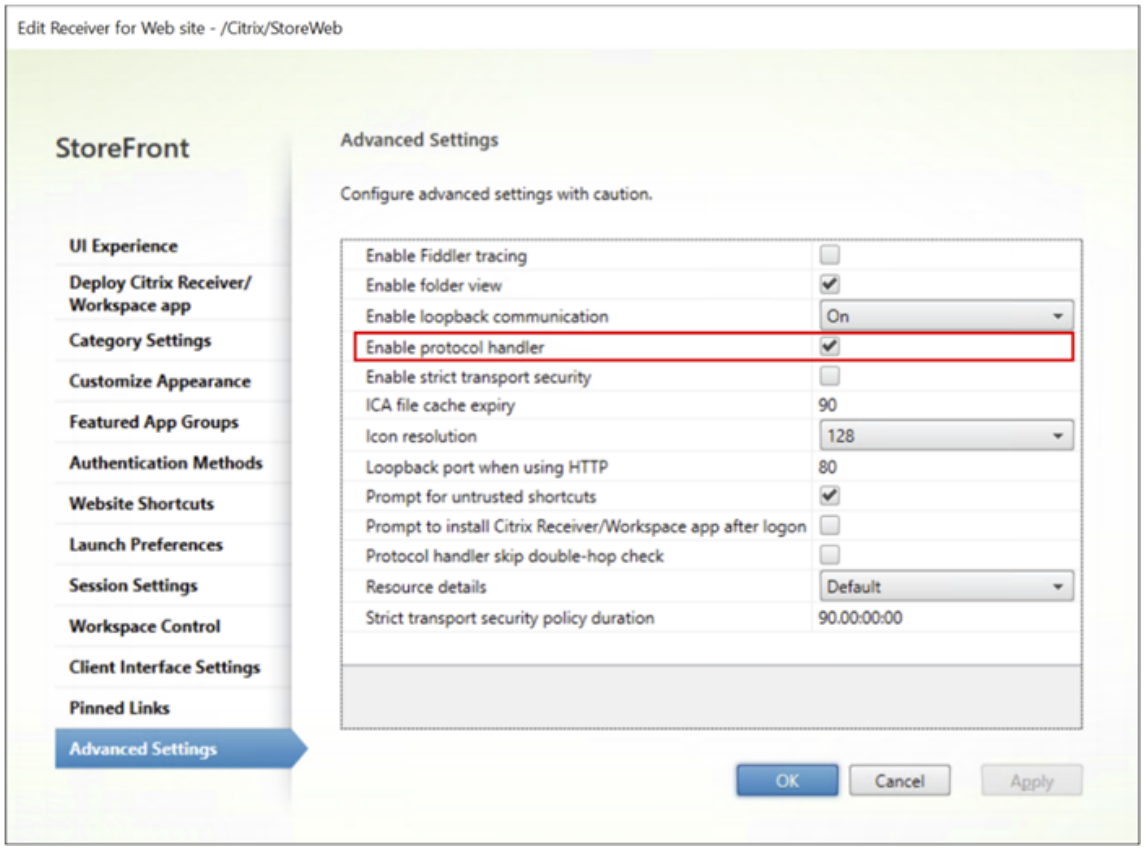
要启用内存混合启动，请执行以下步骤：

1. 要允许使用 Citrix Workspace 启动器进行混合启动，请选中 允许用户下载 **HDX** 引擎（插件）复选框。



2. 在 高级设置下，选中 启用协议处理程序 复选框。

© 1997–2025 Citrix Systems, Inc. All rights reserved.



Citrix Workspace 安全概述

November 7, 2024

用户身份验证

Citrix Workspace 可以配置为使用多种身份验证方法。有关更多详细信息，请参阅 配置身份验证。

要配置会话超时，请参阅 自定义安全和隐私政策。

客户端连接

客户端必须使用带有 TLS 1.2 或更高版本的 HTTPS 连接到 Citrix Workspace。有关最低客户端版本和网络连接要求，请参阅 系统要求。

Citrix Workspace 启用 HTTP 严格传输安全 以要求 Web 浏览器仅使用 HTTPS。

© 1997–2025 Citrix Systems, Inc. All rights reserved.

App Protection

您可以使用 应用程序保护 来防止屏幕捕获和屏幕记录器。当使用 Web 浏览器时，这需要 Citrix Web 扩展。

更多信息

- 《适用于 Citrix Cloud 平台的安全部署指南》：本指南概述了使用 Citrix Cloud 时的安全性最佳做法并介绍了 Citrix Cloud 收集和管理的信息。本指南还包含指向有关 Citrix Cloud Connector 的综合性信息的链接。
- Citrix DaaS 的技术安全概述 。
- Citrix 信任中心：提供有关我们的安全性、隐私性和合规性方法的最新信息。

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG' s Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.