移动生产力应用程序

Contents

移动生产力应用程序发布时间表

May 19, 2020

Citrix 移动生产力应用程序两周发布一次。尽管准确的日期可能会发生变化，但是知晓此发布节奏可以帮助您提前制定计划。我们还希望帮助您更加轻松地管理应用程序部署和更新。

关于 **Secure Mail** 和 **Secure Web** 的分阶段发布过程

Secure Mail 和 Secure Web 的新版本可用时，这些版本将以分阶段发布的方式推出，如下所示：

- 对于 iOS 和 Android 用户，Secure Mail 和 Secure Web 更新将在 App Store 和 Google Play 应用商店中提供，以提高每周（7 天）的用户百分比。
- Secure Mail for iOS 和 Secure Web for iOS 的新下载将在本周内获取新版本。Secure Mail for Android 和 Secure Web for Android 的新下载将运行本周的早期版本，直至新版本的推出送达所有用户。
- 对于用户来说，某些功能将逐步发布。

功能标志管理的必备条件

如果生产环境中的 Secure Hub 或 Secure Mail 出现问题，我们可以在应用程序代码内部禁用受影响的功能。为此，我们将使用功能标志以及名为 LaunchDarkly 的第三方服务。不需要做任何配置即可启用传输到 LaunchDarkly 的流量，但当您配置了阻止出站流量的防火墙或代理时除外。在这种情况下，您根据策略要求通过特定 URL 或 IP 地址启用传输到 LaunchDarkly 的流量。有关自移动生产力应用程序 10.6.15 起 MDX 中支持将域从通道中排除的详细信息，请参阅 MDX Toolkit 文档。有关与功能标志和 LaunchDarkly 有关的常见问题解答，请参阅此支持知识中心文章

> 注意：
> 有关正在逐步淘汰的 Citrix Endpoint Management 功能的高级通知，请参阅弃用。

支持移动生产力应用程序

November 16, 2021

启用了自动更新的用户从应用程序商店接收最新版本。最新版本的移动生产力应用程序如下所示：

- 21.11.0（仅限 Android）

Citrix 支持从最后两个版本的移动生产力应用程序进行升级。最后两个版本的移动生产力应用程序如下所示：

- 21.10.5（仅适用于 Secure Mail 和 Secure Web）
- 21.10.0（仅限 Secure Mail for Android 和 Secure Web for Android）

支持的操作系统

最新版本的 Secure Hub、MDX Toolkit 和移动生产力应用程序与最新版本和前两个版本的 Endpoint Management 兼容。有关详细信息，请参阅支持的设备操作系统。

最新版本的移动生产力应用程序要求使用最新版本的 Secure Hub。请确保 Secure Hub 保持最新状态。

> 注意：
>
> 对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持已于 2020 年 6 月结束。

支持进行 **MDX** 加密的设备

Citrix 支持对下列品牌的设备系列进行 MDX 加密。

Android:

- Samsung Note
- Samsung Galaxy
- Google Pixel
- Motorola

iOS:

- 具有前面列表中受支持操作系统版本的所有 iOS 设备都支持进行 MDX 加密。

其他注意事项和限制

有关正在逐步淘汰的 Citrix Endpoint Management 功能的高级通知，请参阅弃用。

Secure Mail

- 由于 Secure Ticket Authority (STA) 和 Secure Mail 存在问题，因此，Endpoint Management 当前不支持 NetScaler 12.0.41.16。此问题在 NetScaler 12.0 Build 41.22 中已修复。有关详细信息和更新，请参阅此支持知识中心文章。
- 适用于 Exchange 2007 和 Lotus Notes 8.5.3 的 Secure Mail 已于 2017 年 9 月 30 日达到生命周期已结束 (EOL) 日期。
- 要在发送 Citrix Files 附件时实现最佳性能，建议使用最新版本的 Citrix Files。Windows 不支持 Citrix Files。
- 在 IBM Notes 环境中，必须配置 IBM Domino Traveler 服务器版本 9.0。有关详细信息，请参阅集成 Exchange Server 或 IBM Notes Traveler 服务器。

Secure Web

在设备上安装最新版本的 Android WebView。用户可以从 Google Play 应用商店下载 Android WebView。

QuickEdit

QuickEdit 仍作为移动生产力应用程序提供。我们将不应用以前公布的 2018 年 9 月 1 日的生命周期已结束 (EOL) 状态。

适用于 **Endpoint Management** 的 **Citrix Content Collaboration**

用户在版本 6.5 之后从公共应用商店访问适用于 Endpoint Management 的 Citrix Content Collaboration。

ShareConnect

ShareConnect 已于 2020 年 6 月 30 日达到生命周期已结束 (EOL) 状态。有关详细信息，请参阅 EOL 和已弃用的应用程序。

Secure Notes 和 **Secure Tasks**

Secure Notes 和 Secure Tasks 已于 2018 年 12 月 31 日达到生命周期结束 (EOL) 状态。有关详细信息，请参阅 EOL 和已弃用的应用程序。

管理员任务和注意事项

June 18, 2021

本文讨论移动生产力应用程序的管理员需要了解的相关任务和注意事项。

功能标志管理

如果生产环境中的移动生产力应用程序出现问题，我们可以在应用程序代码内部禁用受影响的功能。我们可以对适用于 iOS 和 Android 的 Secure Hub、Secure Mail 和 Secure Web 禁用该功能。为此，我们将使用功能标志以及名为 LaunchDarkly 的第三方服务。不需要做任何配置即可启用传输到 LaunchDarkly 的流量，但当您配置了阻止出站流量的防火墙或代理时除外。在这种情况下，您根据策略要求通过特定 URL 或 IP 地址启用传输到 LaunchDarkly 的流量。有关 MDX 中支持将域从通道中排除的详细信息，请参阅 MDX Toolkit 文档。

可以通过以下方式启用传输到 LaunchDarkly 的流量和通信：

启用传输到以下 **URL** 的流量

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

按域创建允许列表

以前，我们在您的内部策略仅要求列出 IP 地址时提供要使用的 IP 地址列表。现在，由于 Citrix 对基础结构做了改进，我们将逐步淘汰自 2018 年 7 月 16 日开始使用的公用 IP 地址。如果可行，我们建议您按域创建允许列表。

在允许列表中列出 **IP** 地址

如果必须在允许列表中列出 IP 地址，可以参阅此 LaunchDarkly 公用 IP 列表，获取当前所有 IP 地址范围的列表。此列表可用于确保您的防火墙配置自动更新，以便与基础结构更新保持一致。有关基础结构变更的当前状态的详细信息，请参阅 LaunchDarkly 状态页面。

> 注意：
>
> 公共应用商店应用程序要求首次部署它们时执行全新安装。不能从应用程序的当前企业打包版本升级到公共应用商店版本。
>
> 通过公共应用商店分发，您不必使用 MDX Toolkit 签名和打包 Citrix 开发的应用程序。可以使用 MDX Toolkit 打包第三方应用程序或企业应用程序。

LaunchDarkly 系统要求

- Endpoint Management 10.7 或更高版本。
- 如果您在 Citrix ADC 上将拆分通道设置为关，请确保应用程序能够与以下服务通信：
  - LaunchDarkly 服务
  - APNs 侦听器服务

支持的应用商店

移动生产力应用程序在 Apple App Store 和 Google Play 中提供。有关在 Windows 设备上确保本机生产力应用程序的安全以及部署这些应用程序的信息，请参阅 Windows 信息保护设备策略。

在不提供 Google Play 的中国，可从以下应用商店中获取 Secure Hub for Android：

- https://shouji.baidu.com
- https://apk.hiapk.com
- https://apk.91.com

启用公共应用商店分发

1. 从 Endpoint Management 下载页面下载适用于 iOS 和 Android 的公共应用商店.mdx 文件。
2. 将.mdx 文件上载到 Endpoint Management 控制台。移动生产力应用程序的公共应用商店版本仍作为 MDX 应用程序上载。请勿在服务器上上载这些应用程序作为公共应用商店应用程序。有关步骤，请参阅添加应用程序。
3. 根据您的安全策略将策略从其默认值更改为其他值（可选）。
4. 将应用程序推送为必需应用程序（可选）。此步骤要求启用您的环境以进行移动设备管理。

5. 将从 App Store、Google Play 或 Endpoint Management 应用商店获取的应用程序安装在设备上。
   - 在 Android 上，用户将被重定向到 Play 应用商店以安装应用程序。在 iOS 中，在包含 MDM 的部署中，不需要将用户定向到应用商店即可安装应用程序。
   - 从 App Store 或 Play 应用商店安装应用程序时，将执行以下操作。只要对应的.mdx 文件已上载到服务器，该应用程序就会转为托管应用程序。转为托管应用程序时，该应用程序会提示输入 Citrix PIN。用户输入 Citrix PIN 时，Secure Mail 将显示帐户配置屏幕。
6. 只有在 Secure Hub 中注册了且对应的.mdx 文件在服务器上时，应用程序才可访问。如果未满足任何一个条件，用户可以安装该应用程序，但其使用将被阻止。

如果您当前使用的应用程序来自 Citrix Ready Marketplace（这些应用程序已在公共应用商店中），则您已熟悉部署过程。移动生产力应用程序采用的方法与多数 ISV 当前使用的方法相同。在应用程序内嵌入 MDX SDK 以使该应用程序可在公共应用商店中提供。

> 注意：
>
> 适用于 iOS 和 Android 的 Citrix Files 应用程序的公共应用商店版本现在通用。手机和平板电脑上使用的 Citrix Files 应用程序相同。

Apple 推送通知

有关配置推送通知的详细信息，请参阅为 Secure Mail 配置推送通知。

公共应用商店常见问题解答

- 我可以为不同的用户组部署多个公共应用商店应用程序的副本吗？例如，我希望为不同的用户组部署不同的策略。

  为每个用户组上载不同的.mdx 文件。但是，在这种情况下，单个用户不能属于多个组。如果用户不属于多个组，则会向该用户分配同一应用程序的多个副本。公共应用商店应用程序的多个副本不能部署到相同设备，因为应用程序 ID 不能更改。

- 是否可以将公共商店应用程序作为必备应用程序推送？

  是。向设备推送应用程序需要 MDM；对于仅 MAM 的部署不支持。

- 我是否需要更新基于用户代理的任何流量策略或 Exchange Server 规则？

  任何基于用户代理的策略和规则的字符串（按平台）都如下所示。

  > 重要：
  >
  > Secure Notes 和 Secure Tasks 已于 2018 年 12 月 31 日达到生命周期结束 (EOL) 状态。有关详细信息，请参阅EOL 和已弃用的应用程序。

Android

应用程序	服务器	用户代理字符串
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

应用程序	服务器	用户代理字符串
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- 是否可以阻止应用程序升级?

  否。公共应用商店中发布更新时，启用了自动更新的任何用户都将接收该更新。

- 是否可以强制执行应用程序升级?

  是，可以通过升级宽限期策略强制执行升级。与更新版本的应用程序对应的新.mdx 文件上载到 Endpoint Management 时，设置此策略。

- 如果无法控制更新时间段，如何在更新到达用户之前测试应用程序?

  与 Secure Hub 的过程类似，在 EAR 期间，可以在 TestFlight for iOS 上测试应用程序。对于 Android，将在 EAR 期间通过 Google Play 测试版程序提供应用程序。可以在此期间测试应用程序更新。

- 如果我没有在自动更新到达用户设备之前更新新.mdx 文件，会发生什么?

  更新后的应用程序保持与较旧的.mdx 文件兼容。依赖于新策略的任何新功能不会被启用。

- 如果安装了 Secure Hub，应用程序是否将转为托管应用程序，或者是否需要注册该应用程序?

  必须在 Secure Hub 中注册用户，公共应用商店应用程序才能激活为托管应用程序（由 MDX 保护）并且可以使用。如果 Secure Hub 已安装但未注册，用户将无法使用公共应用商店应用程序。

- 对于公共商店应用程序，是否需要 Apple 企业开发人员帐户？

  否。由于 Citrix 现在维护移动生产力应用程序的证书和预配配置文件，因此，不需要 Apple 企业开发人员帐户即可为用户部署这些应用程序。

- 企业分发的结束是否适用于部署的任何打包应用程序？

  否，它仅适用于移动生产力应用程序：Secure Mail、Secure Web、适用于 Endpoint Management 的 Citrix Content Collaboration、QuickEdit 和 ShareConnect。已部署的任何企业打包应用程序（内部开发或由第三方开发）可以继续使用企业打包功能。MDX Toolkit 继续面向应用程序开发人员支持企业打包功能。

- 当我安装来自 Google Play 的应用程序时，收到错误代码为 505 的 Android 错误。

  > 注意：
  >
  > 针对 Android 5.x 的支持已于 2018 年 12 月 31 日结束。

  这是 Google Play 和 Android 5.x 版本的已知问题。如果发生此错误，可以按照以下步骤来清理设备上阻止应用程序安装的过期数据：

1. 请重新启动设备。
2. 通过设备设置清除 Google Play 的缓存和数据。
3. 最后，在您的设备上删除并重新添加 Google 帐户。

有关详细信息，请使用以下关键字搜索此 站点：“Fix Google Play Store Error 505 in Android: Unknown Error Code”（修复 Android 中的 Google Play 应用商店错误 505: 未知错误代码）

- 尽管 Google Play 上的应用程序已发布到生产环境，并且没有新的测试版本可用，为什么我在 Google Play 上的应用程序标题后面会看到 Beta 字样？

  如果您已加入我们的早期访问版本 (Early Access Release, EAR) 计划，您始终会在应用程序标题旁边看到 Beta 字样。此名称只是通知用户其对某个特定应用程序的访问级别。Beta 名称指示用户收到最新版本的可用应用程序。最新版本可能是发布到生产跟踪或测试版跟踪的最新版本。

- 安装并打开应用程序后，尽管.mdx 文件已在 Endpoint Management 控制台中，用户仍会看到消息 “未授权的应用程序”。

  如果用户直接从 App Store 或 Google Play 安装应用程序，并且如果 Secure Hub 未刷新，则会出现此问题。不活动计时器过期时必须刷新 Secure Hub。用户打开 Secure Hub 并重新进行身份验证时，策略将刷新。应用程序将在下次用户打开该应用程序时获得授权。

- 是否需要访问代码才能使用应用程序？从 App Store 或 Play 应用商店安装应用程序时，看到提示输入访问代码的屏幕。

  如果看到要求输入访问代码的屏幕，表示您未通过 Secure Hub 在 Endpoint Management 中注册。使用 Secure Hub 注册，并确保应用程序的.mdx 文件部署在服务器上。此外，请确保可以使用该应用程序。访问代码限制为仅供 Citrix 内部使用。应用程序要求激活 Endpoint Management 部署。

- 是否可以通过 VPP 或 DEP 部署 iOS 公共商店应用程序？

Endpoint Management 已针对未启用 MDX 的公共应用商店应用程序的 VPP 分发进行优化。尽管您能够通过 VPP 分发 Endpoint Management 公共应用商店应用程序，但在我们进一步增强 Endpoint Management 和 Secure Hub 应用商店的功能以解决限制问题之前，该部署并非最优部署。有关通过 VPP 部署 Endpoint Management 公共应用商店应用程序的已知问题列表以及可能的解决方法，请参阅 Citrix 知识中心中的这篇文章。

适用于移动生产力应用程序的 **MDX** 策略

通过 MDX 策略，您可以配置 Endpoint Management 强制执行的设置。MDX 策略包括身份验证、设备安全、网络要求和访问、加密、应用程序交互、应用程序限制等。许多 MDX 策略都适用于所有移动生产力应用程序。某些策略是应用程序特定的策略.

策略文件将以.mdx 文件格式向移动生产力应用程序的公共应用商店版本提供。也可以在添加应用程序时，在 Endpoint Management 控制台中配置策略。

有关 MDX 策略的完整说明，请参阅本部分中的以下文章：

- 适用于移动生产力应用程序的 MDX 策略概览
- 适用于 Android 的移动生产力应用程序的 MDX 策略
- 适用于 iOS 的移动生产力应用程序的 MDX 策略

以下各部分内容介绍了与用户连接有关的 MDX 策略。

Secure Mail for Android 中的双模式

移动应用程序管理 (MAM) SDK 可用于替换 iOS 和 Android 平台未涵盖的 MDX 功能区域。MDX 封装技术计划于 2021 年 9 月达到生命周期结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

自 20.8.0 版起，Android 应用程序随 MDX 和 MAM SDK 一起发布，以便为上文提及的 MDX EOL 策略做好准备。MDX 双模式旨在提供一种从旧版 MDX Toolkit 过渡到当前 MAM SDK 的方法。使用双模式将允许您执行以下操作：

- 继续使用 MDX Toolkit 管理应用程序（现在在 Endpoint Management 控制台中命名为旧版 MDX）
- 管理纳入新 MAM SDK 的应用程序。

> 注意：
>
> 使用 MAM SDK 时，不需要封装应用程序。

切换到 MAM SDK 后，不需要执行其他步骤。

有关 MAM SDK 的详细信息，请参阅以下文章：

- MAM SDK 概述
- 设备管理 上的 Citrix Developer 部分
- Citrix 博客文章
- 当您登录到 Citrix 下载 时下载 SDK

必备条件

要成功部署双模式功能，请确保以下各项：

- 将 Citrix Endpoint Management 更新到 10.12 RP2 及更高版本，或 10.11 RP5 及更高版本。
- 将您的移动应用程序更新到 20.8.0 或更高版本。
- 将策略文件更新到版本 20.8.0 或更高版本。
- 如果贵组织使用第三方应用程序，请务必在切换到 Citrix 移动生产力应用程序的 MAM SDK 选项之前将 MAM SDK 合并到第三方应用程序中。您的所有托管应用程序都必须同时移动到 MAM SDK。

> 注意：
>
> 支持所有基于云的客户使用 MAM SDK。

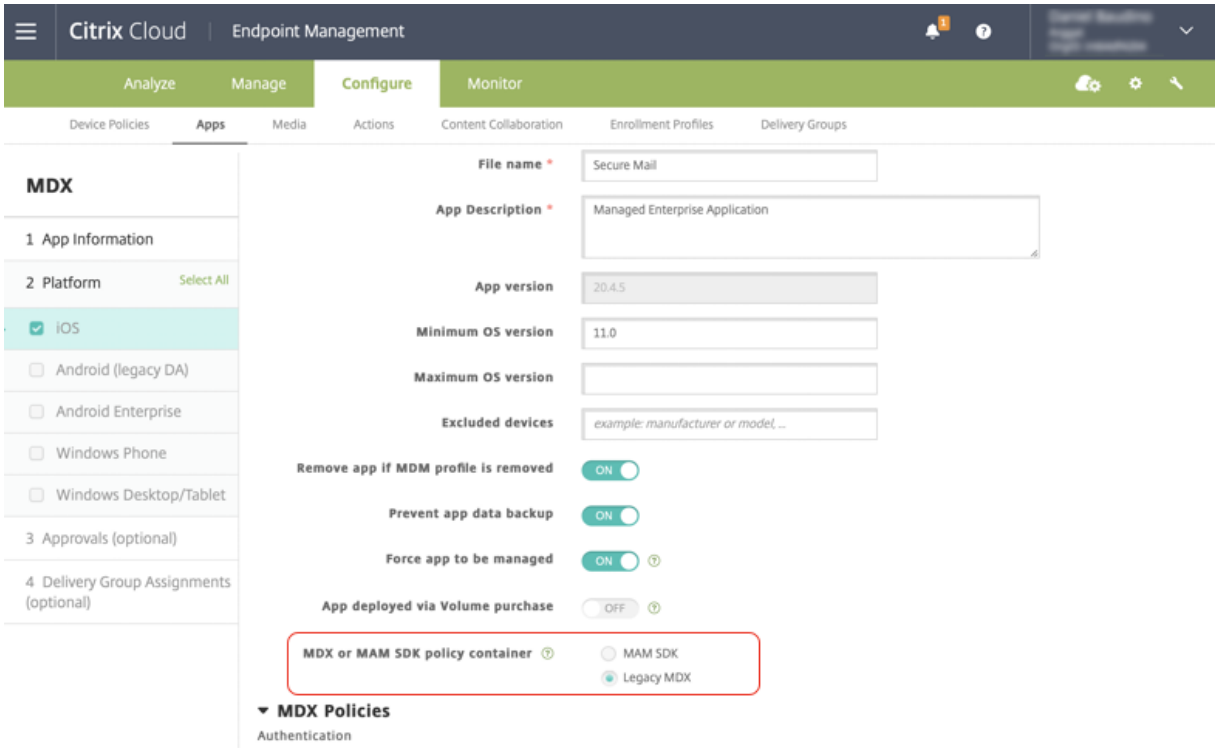
限制

- MAM SDK 仅支持在 Citrix Endpoint Management 部署中在 Android Enterprise 平台下发布的应用程序。对于新发布的应用程序，默认加密是基于平台的加密。
- MAM SDK 仅支持基于平台的加密，不支持 MDX 加密。
- 如果不更新 Citrix Endpoint Management，并且策略文件在版本为 20.8.0 及更高版本的移动应用程序上运行，则会为 Secure Mail 创建网络策略的重复条目。

在 Citrix Endpoint Management 中配置 Secure Mail 时，双模式功能允许您继续使用 MDX Toolkit（现为旧版 MDX）管理应用程序，或者切换到新 MAM SDK 进行应用程序管理。Citrix 建议您切换到 MAM SDK，因为 MAM SDK 的模块化程度更高，仅允许您使用组织使用的一部分 MDX 功能。

可以在 **MDX** 或 **MAM SDK** 策略容器中获取以下策略设置选项：

- **MAM SDK**
- 旧版 **MDX**



在 **MDX** 或 **MAM SDK** 策略容器策略中，您只能将选项从旧版 **MDX** 更改为 **MAM SDK**。不允许使用从 **MAM SDK** 切换到旧版 **MDX** 的选项，您需要重新发布应用程序。默认值为旧版 **MDX**。确保为在同一设备上运行的 Secure Mail 和 Secure Web 设置了相同的策略模式。不能在同一设备上运行两种不同的模式。

与内部网络的用户连接

通过通道连接到内部网络的连接可以使用完整 VPN 通道或无客户端 VPN 的变体（称为“安全浏览”）。“首选 VPN 模式”策略控制该行为。默认情况下，连接使用安全浏览；建议需要进行 SSO 的连接使用该模式。建议对通过客户端证书或端到端 SSL 与内部网络中的资源建立的连接使用完整 VPN 通道设置。该设置通过 TCP 处理任何协议，并且可以在 Windows 和 Mac 计算机以及 iOS 和 Android 设备上使用。

Secure Web for iOS 和 Secure Web for Android 支持对完整 VPN 通道部署使用代理自动配置 (PAC) 文件。如果使用 Citrix ADC 进行代理身份验证，则这种情况确实如此。

允许 VPN 模式切换策略允许用户根据需要在完整 VPN 通道模式与安全浏览模式之间自动切换。默认情况下，此策略设置为“关”。如果此策略设置为“开”，则将在备选模式下尝试重新处理由于无法在首选 VPN 模式下处理身份验证请求而失败的网络请求。例如，服务器对客户端证书的质询可以被完整 VPN 通道模式接受，但不被安全浏览模式接受。同样，使用安全浏览模式时，通过 SSO 向 HTTP 身份验证质询提供服务的可能性更大。

网络访问限制

“网络访问”策略指定是否对网络访问设置限制。默认情况下，Secure Mail 访问不受限制，这表示不对网络访问权限设置任何限制。应用程序对设备连接到的网络具有不受限制的访问权限。默认情况下，Secure Web 访问通过通道连接到

内部网络，这表示将对所有网络访问使用返回到内部网络的 PerApp VPN 通道，并且使用 Citrix ADC 拆分通道设置。您还可以指定阻止的访问，以便应用程序运行时好像设备未建立网络连接。

如果要允许使用 AirPrint、iCloud 以及 Facebook 和 Twitter API 等功能，请勿阻止“网络访问”策略。

“网络访问”策略还与“后台网络服务”策略交互。有关详细信息，请参阅集成 Exchange Server 或 IBM Notes Traveler 服务器。

Endpoint Management 客户端属性

客户端属性包含用户设备上直接提供给 Secure Hub 的信息。客户端属性位于 Endpoint Management 控制台的设置 > 客户端 > 客户端属性中。

客户端属性用于配置诸如以下各项设置：

用户密码缓存

通过用户密码缓存，用户的 Active Directory 密码将本地缓存在移动设备上。如果您启用了用户密码缓存，系统将提示用户设置 Citrix PIN 或通行码。

不活动计时器

不活动计时器定义用户可以让其设备处于不活动状态而不会在用户访问应用程序时提示输入 Citrix PIN 或通行码的时间（单位为分钟）。要为 MDX 应用程序启用此设置，必须将“应用程序通行码”策略设置为开。如果“应用程序通行码”策略设置为关，用户将被重定向到 Secure Hub 以执行完整身份验证。更改此设置时，该值将在系统下次提示用户进行身份验证时生效。

Citrix PIN 身份验证

Citrix PIN 简化了用户身份验证体验。PIN 用于确保客户端证书的安全或在设备本地保存 Active Directory 凭据。如果您配置了 PIN 设置，用户的登录体验将如下所示：

1. 用户首次启动 Secure Hub 时，将收到输入 PIN 的提示，这样将缓存 Active Directory 凭据。
2. 用户下次启动移动生产力应用程序（例如 Secure Mail）时，将输入 PIN 并登录。

使用客户端属性启用 PIN 身份验证、指定 PIN 类型、指定 PIN 的强度、长度以及更改要求。

指纹或 Touch ID 身份验证

适用于 iOS 设备的指纹身份验证（也称为 Touch ID 身份验证）将替代 Citrix PIN。当打包的应用程序（除 Secure Hub 外）需要使用脱机身份验证时（例如不活动计时器过期时），此功能非常有用。可以在下列身份验证方案中启用此功能：

- Citrix PIN + 客户端证书配置

- Citrix PIN + 缓存 AD 密码配置
- Citrix PIN + 客户端证书配置和缓存 AD 密码配置
- Citrix PIN 已关闭

如果指纹身份验证失败，或者用户取消指纹身份验证提示，则封装的应用程序将恢复使用 Citrix PIN 或 AD 密码身份验证。

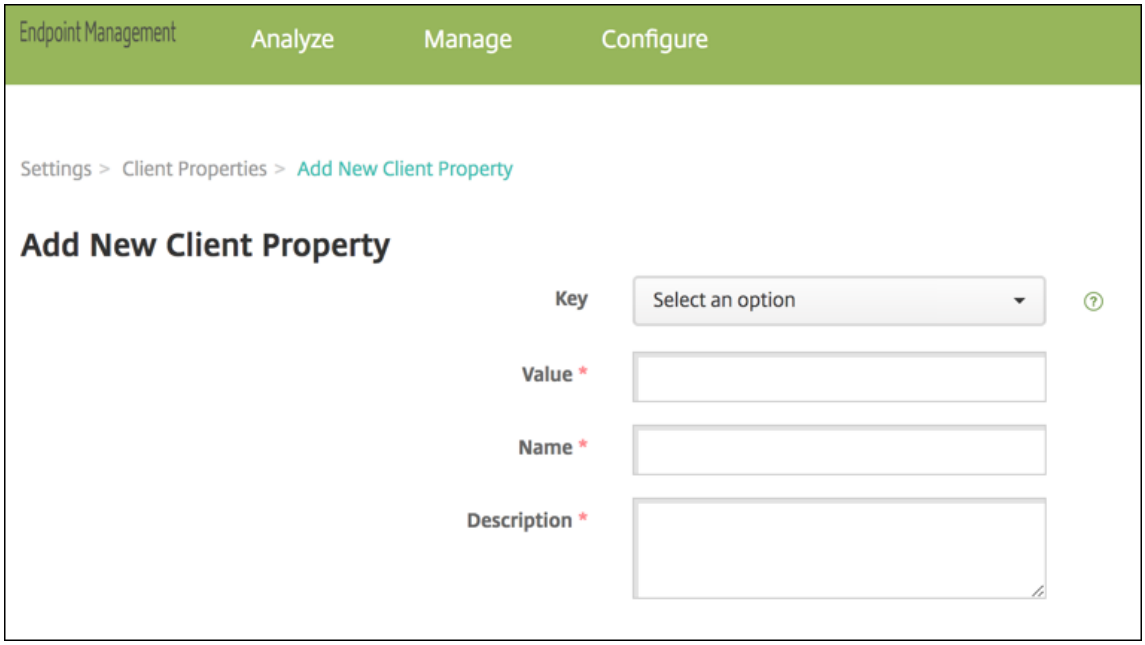
指纹身份验证要求

- 支持指纹身份验证并且至少配置了一个指纹的 iOS 设备（最低版本为 8.1）。
- 必须关闭用户熵功能。

配置指纹身份验证

> 重要：
>
> 如果用户熵已启用，则忽略“启用 Touch ID 身份验证”属性。用户熵通过“Encrypt secrets using Passcode”（使用通行码加密机密）密钥启用。

1. 在 Endpoint Management 控制台中，转到设置 **>** 客户端 **>** 客户端属性。
2. 单击添加。



3. 添加键 **ENABLE_TOUCH_ID_AUTH**，将其值设置为 **True**，然后将策略名称设置为启用指纹身份验证。

配置指纹身份验证后，用户不需要重新注册其设备。

有关“使用通行码加密密钥”密钥和常规客户端属性的详细信息，请参阅有关客户端属性的 Endpoint Management 文章。

功能（按平台）

November 16, 2021

下表汇总了 Citrix 移动生产力应用程序的功能。**X** 指示该平台可用的功能。有关 QuickEdit 中的功能，请参阅 Citrix QuickEdit 文章。

Citrix Secure Hub

功能	iOS	Android
登录进行身份验证	X	X
监视器策略遵守	X	X
访问应用程序和桌面	X	X
HDX 应用程序和桌面	X	X
创建和发送问题日志	X	X
将屏幕截图附加到日志	X	X
在应用程序内部联系技术支持人员	X	X
在应用程序内部联系 Citrix 技术支持	X	X
崩溃收集和分析	X	X
脱机身份验证	X	X
通过 Citrix Secure Mail 发送日志	X	X
Google Analytics	X	X
横向和纵向模式	X	X
适用于信任应用程序的应用内指南	X	X
通过电子邮件注册时，在 Secure Mail（仅 MAM）中自动注册	X	X
Touch ID 脱机身份验证	X	X
通过派生凭据注册	X	
生物特征身份验证		X
使用 Workspace 应用商店	X	X

Citrix Secure Mail

功能	iOS	Android
电子邮件功能		
最小化草稿	X	X
撤消已发送的邮件		X
加密管理	X	X
日历日程的小组件		X
Secure Mail 中的联系人图片	X	X
支持响应式电子邮件	X	X
草稿文件夹自动同步	X	X
草稿文件夹中的附件同步		X
发送、接收、答复、全部答复、转发邮件	X	X
创建、编辑、删除草稿	X	X
为电子邮件添加标志	X	X
标记为“未读”	X	X
查看所有文件夹和子文件夹	X	X
应用程序置于后台时自动保存草稿	X	X
通过 Citrix Secure Notes 实现电子邮件到备忘录。重要：Secure Notes 已于 2018 年 12 月 31 日达到生命周期结束 (EOL) 状态。有关详细信息，请参阅 EOL 和已弃用的应用程序。	X	X
搜索邮件（本地和服务器）	X	X
选择邮件同步期限（最长为 1 个月或所有邮件）	X	X
查看未读邮件	X	X
保证查看附件/播放图片、视频和音频的安全	X	X
多个附件	X	X
答复和转发附件	X	X

功能	iOS	Android
从 Citrix Files 附加文件	X	X
从 Citrix Files 受限区域和连接器附加文件	X	X
附件存储库	X	X
富文本编辑	X	X
带主题的电子邮件通知，在锁屏界面上预览	X	X
从通知界面中答复和删除邮件及邀请	X	
附加或拍摄照片	X	X
选择多封邮件	X	X
下载附件	X	X
加载内联图像	X	X
快速排序	X	X
发送、接收、打开和保存.zip 文件附件	X	X
横向和纵向模式	X；跨邮件列表、邮件阅读、编写、日历和联系人视图	X：仅适用于邮件阅读和编写视图
所粘贴文本的格式保持不变	X	X
从联系人 SMS	X	X
从联系人 FaceTime	X	
消息由于连接问题或发件箱中存储的邮件已满而取消发送	X	X
最近文件夹上浮		X
下拉邮件刷新	X	X
上次刷新时间戳	X	X
向左轻扫显示邮件操作	X	X
Microsoft Exchange 和 IBM Notes Traveler 支持	X	X
轻按刷新邮件、日历和联系人	X	X

功能	iOS	Android
在邮件视图中应用设备辅助功能/字体大小设置	X	X
S/MIME 签名和加密	X	X
通过电子邮件导入 S/MIME 证书	X	X
S/MIME、Intercede 集成	X	
S/MIME、Entrust 集成	X	
针对邮件正文的 Microsoft IRM 保护	X	X
推送通知	X	X
向收件箱推送通知自动更新包括日历在内的所有文件夹	X	
打开 Office 365 文档	X	X
三维触控操作	X	
锁屏界面上的上下文图标	X	X
搜索文件夹	X	X
VIP 邮件文件夹	X	X
支持动态输入	X	X
保持文件夹展开	X	X
邮件分类标记	X	X
拼写检查	X	
附加上次拍摄的照片	X	X
URL 预览	X	X
在 Citrix Files 中打开 Citrix Files 链接	X	X
支持 `.pass` 文件	X	
在搜索模式下选择多封电子邮件	X	X
插入内联图像	X	X
升级到 Exchange ActiveSync (EAS) 16	X	X
限制用户使用未知域或个人域	X	

功能	iOS	Android
支持超宽设备屏幕		X
配置多个 Exchange 帐户	X	X
向左或向右轻扫进行更多操作	X	X
对加密邮件的回复或转发加密	X	
打印电子邮件和内联图像	X	
使用“设置”中的“预览行”功能配置在邮箱视图中作为预览显示的电子邮件正文的行数	X	
支持响应式电子邮件	X	X
附件（MS Office 或图片）的应用内预览。	X	X
私人联系人组	X	X
将用户名迁移到电子邮件地址 (UPN)	X	X
报告网络钓鱼电子邮件	X	X
新式验证 (OAuth)	X	X
打印附件	X	
Android Enterprise (Android for Work)	X	
RTF 签名	X	
丰富的推送通知	X	
源	X	X
照片附件改进功能	X	X
组通知	X	
Slack 集成（预览版）	X	X
管理源	X	
内部域	X	X
管理您的源	X	X
MS Teams 集成	X	X
自助诊断（故障排除）选项		X

功能	iOS	Android
双模式 (MAM SDK)	X	X
自助诊断工具		X
日历		
预览和导入 ICS 文件作为日历事件		X
拖放日历事件	X	X
天、周、月和日程视图	X	X
锁屏界面上显示详细提醒	X	X
同步六个月内的事件	X	X
将事件设为私人事件	X	X
滚动到第一个事件之前的小时	X	
手动刷新选项	X	X
设置提醒	X	X
轻按以在地图上标记地址	X	X
周数	X	X
支持动态输入	X	X
安全性分类标记	X	X
长按地址	X	
设置工作周开始日	X	X
将显示焦点置于选定日期所在周	X	
总是突出显示当前日期	X	X
附件存储库中的日历附件	X	X
个人日历支持	X	X
显示与个人日历事件发生的冲突		X
打印日历事件	X	
轻按日历主题行中的电话号码和 Web 地址	X	
搜索日历	X	
会议		
答复、全部答复、转发会议	X	X

功能	iOS	Android
邀请答复的组织者视图	X	X
被邀请者的可用性（以及推荐的可用性）的组织者视图	X	X
轻按加入在线会议注意：对于 WebEx 和 Lync，必须在 Citrix Endpoint Management 中配置策略以启用这些应用程序。	X	X
轻按加入音频会议	X	X
在新邀请中安排在线会议、音频和会议	X	X
向新邀请中添加 ShareFile 链接	X	X
转发带附件的邀请	X	X
轻按发送“迟到”电子邮件	X	X
轻按答复会议组织者	X	X
轻按答复所有会议邀请	X	X
轻按答复所有会议被邀请者	X	X
轻按答复所有会议邀请并添加附件	X	X
拨入 GoToMeeting	X	X
从锁屏界面或通知界面响应邀请	X	X
拨入 WebEx 或 Lync 会议	X	X
隐藏被拒绝的事件	X	X
显示 3 个以上的同步事件	X	X
快速查看被邀请者的状态	X	X
删除、回复、全部回复以及添加关于已取消事件的注释	X	X
在转发邀请中显示组织者姓名	X	X
共享设备	X	X
加入 Skype for Business 会议	X	X
响应会议通知，例如接受、拒绝和暂定。	X	X

功能	iOS	Android
使用“答复”和“删除”响应邮件通知	X	
通讯录		
在联系人中创建文件夹		X
双向联系人同步	X	X
详细的联系人信息（GAL 搜索）	X	X
将 Secure Mail 联系人导出并同步到本地联系人	X	X
联系人：收藏夹和分类		X
控制导出的联系人字段	X	X
非 Secure Mail 联系人详细信息	X	X
支持动态输入	X	X
将联系人标记为 VIP	X	X
与 `.vcards` 共享联系人	X	X
长按添加联系人		X
即使存在本机邮件帐户也可导出联系人	X	X
查看文件夹和子文件夹	X	
在设备上配置的设置		
iMessage 支持	X	
用于控制通知的高级选项	X	X
锁定屏幕通知控制	X	X
邮件和日历通知声音	X	X
音频刷新文件夹	X	X
设置内部和外部外出通知	X	X
删除前询问	X	X
按线索组织的会话或按时间排列的视图	X	X
在 Wi-Fi 中加载附件	X	X

功能	iOS	Android
将“在 Wi-Fi 中加载附件”标记为默认选项	X	X
设置同步邮件期限	X	X
无限制同步/同步所有邮件		X
设置电子邮件签名	X	X
按名字或姓氏列出联系人	X	X
自动前进	X	X
使用家所在时区		X
快速响应模板		X
推送邮件配置频率		X
导出/导入设置	X	X
轻按设备上的返回按钮消除浮动的操作按钮选项		X

Citrix Secure Web

功能	iOS	Android
将两个应用程序同时与多任务处理结合使用	X	
下载文件	X	X
添加收藏	X	X
清除保存的用户名和密码	X	X
删除缓存/历史记录/cookie	X	X
阻止弹出窗口	X	X
保存脱机页面	X	X
在地址栏中搜索	X	X
打开通知中已下载的项目	X	X
密码自动保存	X	X
代理支持		
企业代理	X	X

功能	iOS	Android
URL 阻止列表和允许列表	X	X
历史记录	X	X
默认主页	X	X
选项卡	X	X
推送书签	X	X
阻止屏幕捕获		X
在当前页面中搜索	X	X
三维触控操作	X	
共享设备	X	X
在共享设备中防止文件篡改	X	
导出/导入设置	X	X
横向和纵向模式	X	X
Android Enterprise (Android for Work)		X
下拉刷新屏幕上的内容	X	X

Citrix Secure Hub

November 16, 2021

Citrix Secure Hub 是移动生产力应用程序的启动板。用户在 Secure Hub 中注册其设备以获得访问应用商店的权限。在应用商店中，用户可以添加 Citrix 开发的移动生产力应用程序以及第三方应用程序。

可以从 Citrix Endpoint Management 下载页面下载 Secure Hub 及其他组件。

有关 Secure Hub 以及移动生产力应用程序的其他系统要求，请参阅系统要求。

有关移动生产力应用程序的最新信息，请参阅文章最新声明。

以下各部分列出了当前版本及早期版本的 Secure Hub 中的新增功能。

> 注意：
>
> 对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持已于 2020 年 6 月结束。

当前版本中的新增功能

Secure Hub 21.11.0

Secure Hub for Android

此版本包括缺陷修复。

早期版本中的新增功能

Secure Hub 21.10.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

支持 **Android 12**。自本版本起，Secure Hub 在运行 Android 12 的设备上受支持。

Secure Hub 21.8.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub 21.7.1

Secure Hub for Android

支持已注册的设备上的 **Android 12**。如果考虑升级到 Android 12，请确保先将 Secure Hub 更新到版本 21.7.1。Secure Hub 21.7.1 是升级到 Android 12 所需的最低版本。此版本可确保已注册的用户从 Android 11 无缝升级到 Android 12。

> 注意：
>
> 如果在升级到 Android 12 之前 Secure Hub 未更新到版本 21.7.1，您的设备可能需要重新注册或恢复出厂设置才能恢复以前的功能。
>
> Citrix 承诺为 Android 12 提供第 1 天支持，并且将进一步向后续版本的 Secure Hub 中添加更新，以完全支持 Android 12。

Secure Hub 21.7.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub 21.6.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub 21.5.1

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub 21.5.0

Secure Hub for iOS

在本版本中，使用 MDX Toolkit 版本 19.8.0 或更早版本封装的应用程序将不再起作用。确保使用最新的 MDX Toolkit 封装应用程序以恢复正确的功能。

Secure Hub 21.4.0

Secure Hub 的颜色改造。Secure Hub 符合 Citrix 品牌颜色更新。

Secure Hub 21.3.2

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub 21.3.0

此版本包括缺陷修复。

Secure Hub 21.2.0

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub 21.1.0

此版本包括缺陷修复。

Secure Hub 20.12.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

Secure Hub for Android 支持直接启动模式。有关直接引导模式的详细信息，请参阅 *Developer.android.com* 上的 Android 文档。

Secure Hub 20.11.0

Secure Hub for Android

Secure Hub 支持 Google Play 对 Android 10 的当前目标 API 要求。

Secure Hub 20.10.5

此版本包括缺陷修复。

Secure Hub 20.9.0

Secure Hub for iOS

Secure Hub for iOS 支持 iOS 14。

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub 20.7.5

Secure Hub for Android

- Secure Hub for Android 支持 Android 11。
- **Secure Hub** 应用程序从 **32** 位转换为 **64** 位。在 Secure Hub 20.7.5 版中，对应用程序的 32 位体系结构的支持已结束，Secure Hub 已更新到 64 位。Citrix 建议客户从 20.6.5 升级到版本 20.7.5。如果用户跳过升级到 Secure Hub 版本 20.6.5 这一步骤，而是直接从 20.1.5 更新到 20.7.5，则必须重新进行身份验证。重新进行身份验证涉及输入凭据和重置 Secure Hub PIN。Secure Hub 版本 20.6.5 在 Google Play 应用商店中提供。
- 从应用商店安装更新。在 Secure Hub for Android 中，如果有可用于应用程序的更新，则会突出显示该应用程序，并在应用商店屏幕中显示可用更新功能。

  轻按可用更新后，您将导航到显示包含待安装的更新的应用程序列表的应用商店。轻按应用程序的详细信息以安装更新。更新应用程序后，详细信息中的向下箭头将更改为复选标记。

Secure Hub 20.6.5

Secure Hub for Android

应用程序从 **32** 位转换为 **64** 位。Secure Hub 20.6.5 版本是支持 Android 移动应用程序的 32 位体系结构的最终版本。在后续版本中，Secure Hub 支持 64 位体系结构。Citrix 建议用户升级到 Secure Hub 版本 20.6.5，以便用户无需重新进行身份验证即可升级到更高版本。如果用户跳过升级到 Secure Hub 版本 20.6.5，而是直接更新到 20.7.5，则需要重新进行身份验证。重新进行身份验证涉及输入凭据和重置 Secure Hub PIN。

> 注意：
>
> 在设备管理员模式下，20.6.5 版本不会阻止注册运行 Android 10 的设备。

Secure Hub for iOS

启用在 **iOS** 设备上配置的代理。如果要允许用户使用其在设置 **> Wi-Fi** 中配置的代理服务器，Secure Hub for iOS 将要求您启用新的客户端属性 `ALLOW_CLIENTSIDE_PROXY`。有关详细信息，请参阅客户端属性参考中的 `ALLOW_CLIENTSIDE_PROXY`。

Secure Hub 20.3.0

> 注意：
>
> 对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持将于 2020 年 6 月结束

Secure Hub for iOS

- 网络扩展已禁用。由于近期更改了 App Store 审查指南，因此，自 20.3.0 版起，Secure Hub 将不支持运行 iOS 的设备上的网络扩展 (NE)。NE 对 Citrix 开发的移动生产力应用程序不产生任何影响。但是，删除 NE 会对部署的企业 MDX 封装的应用程序产生一定的影响。在同步授权令牌、计时器和 PIN 重试次数等组件时，最终用户可能会遇到额外的向 Secure Hub 翻转的情况。有关详细信息，请参阅 https://support.citrix.com/article/CTX270296。

> 注意：
>
> 系统不会提示新用户安装 VPN。

- 支持增强的注册配置文件。Secure Hub 支持注册配置文件支持中针对 Citrix Endpoint Management 宣布的增强的注册配置文件功能。

Secure Hub 20.2.0

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub 20.1.5

此版本包括：

- 用户隐私政策格式和显示的更新。此功能更新改变了 Secure Hub 的注册流程。
- 缺陷修复。

Secure Hub 19.12.5

此版本包括缺陷修复。

Secure Hub 19.11.5

此版本包括缺陷修复。

Secure Hub 19.10.5

Secure Hub for Android

在 **COPE** 模式下注册 **Secure Hub**。在 Android Enterprise 设备中，请在企业拥有但由个人使用 (Corporate Owned Personally Enabled, COPE) 注册配置文件中配置 Citrix Endpoint Management 时，在 COPE 模式下注册 Secure Hub。

Secure Hub 19.10.0

此版本包括缺陷修复。

Secure Hub 19.9.5

Secure Hub for iOS

此版本包括缺陷修复。

Secure Hub for Android

支持管理面向 **Android Enterprise** 工作配置文件和完全托管设备的键盘锁功能。Android 键盘锁管理设备和工作挑战锁定界面。使用 Citrix Endpoint Management 中的“键盘锁管理”设备策略可控制工作配置文件设备上的键盘锁管理以及完全托管和专用设备上的键盘锁管理。通过键盘锁管理，您可以在用户解锁键盘锁屏幕之前指定用户可用的功能，例如信任代理和安全摄像头。或者，可以选择禁用所有键盘锁功能。

有关功能设置以及如何配置设备策略的详细信息，请参阅键盘锁管理设备策略。

Secure Hub 19.9.0

Secure Hub for iOS

Secure Hub for iOS 支持 iOS 13。

Secure Hub for Android

此版本包括缺陷修复。

Secure Hub for Android 19.8.5

此版本包括缺陷修复。

Secure Hub 19.8.0

Secure Hub for iOS

本版本包括性能增强和缺陷修复。

Secure Hub for Android

支持 **Android Q**。此版本包括对 Android Q 的支持。升级到 Android Q 平台之前：有关弃用 Google Device 管理 API 如何影响运行 Android Q 的设备的信息，请参阅从设备管理迁移到 Android Enterprise。另请参阅博客 Citrix Endpoint Management and Android Enterprise - a Season of Change（Citrix Endpoint Management 和 Android Enterprise - 变革季节）。

Secure Hub 19.7.5

Secure Hub for iOS

本版本包括性能增强和缺陷修复。

Secure Hub for Android

支持 **Samsung Knox SDK 3.x**。Secure Hub for Android 支持 Samsung Knox SDK 3.x。有关迁移到 Samsung Knox 3.x 的详细信息，请参阅 Samsung Knox 开发人员文档。此版本还包括对新 Samsung Knox 命名空间的支持。有关对旧 Samsung Knox 命名空间所做的更改的详细信息，请参阅对旧 Samsung Knox 命名空间的更改。

> 注意：
>
> Secure Hub for Android 在运行 Android 5 的设备上不支持 Samsung Knox 3.x。

Secure Hub 19.3.5 到 19.6.6

这些版本包括性能增强和缺陷修复。

Secure Hub 19.3.0

支持 **Samsung Knox Platform for Enterprise**。Secure Hub for Android 支持在 Android Enterprise 设备上使用 Knox Platform for Enterprise (KPE)。

Secure Hub 19.2.0

本版本包括性能增强和缺陷修复。

Secure Hub 19.1.5

适用于 Android Enterprise 的 Secure Hub 现在支持以下策略：

- **WiFi** 设备策略。Wi-Fi 设备策略现在支持 Android Enterprise。有关此策略的详细信息，请参阅 Wi-Fi 设备策略。
- 自定义 **XML** 设备策略。自定义 XML 设备策略现在支持 Android Enterprise。有关此策略的详细信息，请参阅自定义 XML 设备策略。
- 文件设备策略。您可以在 Citrix Endpoint Management 中添加脚本文件以在 Android Enterprise 设备上执行各种功能。有关此策略的详细信息，请参阅文件设备策略。

Secure Hub 19.1.0

Secure Hub 已改进了字体、颜色并增加了其他 **UI** 改进功能。此修改丰富了您的用户体验，同时与纵贯我们全套移动生产力应用程序的 Citrix 品牌美学非常一致。

Secure Hub 18.12.0

本版本包括性能增强和缺陷修复。

Secure Hub 18.11.5

- 适用于 **Android Enterprise** 的限制设备策略设置。“限制”设备策略的新设置允许用户在 Android Enterprise 设备上访问以下功能：状态栏、锁定屏幕键盘、帐户管理、位置共享，以及将 Android Enterprise 设备的设备屏幕保持打开状态。有关信息，请参阅限制设备策略。

Secure Hub 18.10.5 到 18.11.0 包括性能增强和缺陷修复。

Secure Hub 18.10.0

- 支持 **Samsung DeX** 模式：借助 Samsung DeX，用户能够将支持 KNOX 的设备连接到外部显示器，以在与 PC 类似的界面上使用应用程序、查看文档以及观看视频。有关 Samsung DeX 设备要求和设置 Samsung DeX 的信息，请参阅 How Samsung DeX works（Samsung DeX 工作原理）。

  要在 Citrix Endpoint Management 中配置 Samsung DeX 模式功能，请更新针对 Samsung Knox 的限制设备策略。有关信息，请参阅限制设备策略中的 Samsung KNOX 设置。

- 支持 **Android SafetyNet**：您可以配置 Endpoint Management 以使用 **Android SafetyNet** 功能来评估安装了 Secure Hub 的 Android 设备的兼容性和安全性。结果可以用于在设备上触发自动化操作。有关信息，请参阅 Android SafetyNet。

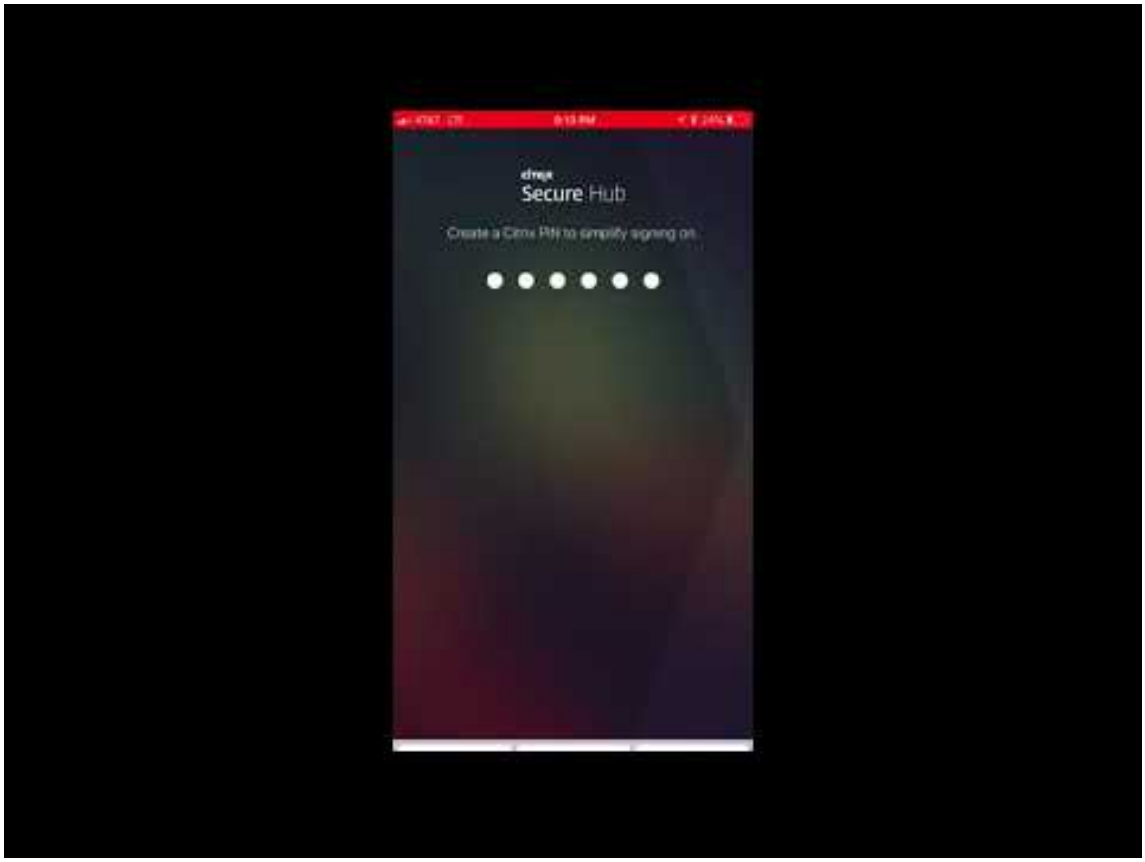
- 禁止在 **Android Enterprise** 设备上使用相机：您可以通过限制设备策略的新设置允许使用相机来阻止用户在其 Android Enterprise 设备上使用相机。有关信息，请参阅限制设备策略。

Secure Hub 10.8.60 到 18.9.0

这些版本包括性能增强和缺陷修复。

Secure Hub 10.8.60

- 支持波兰语。
- 支持 Android P。
- 支持使用 Workspace 应用商店。
  打开 Secure Hub 时，用户不再看到 Secure Hub 应用商店。用户单击添加应用程序按钮后将转到 Workspace 应用商店。以下视频演示了 iOS 设备如何使用 Citrix Workspace 应用程序注册 Citrix Endpoint Management。



> 重要：
>
> 此功能仅适用于新客户。我们当前不支持迁移现有客户。

要使用此功能，请配置以下各项：

- 启用密码缓存和密码身份验证策略。有关配置策略的详细信息，请参阅适用于移动生产力应用程序的 MDX 策略概览。
- 将 Active Directory 身份验证配置为 AD 或 AD+ 证书我们支持这两种模式。有关配置身份验证的详细信息，请参阅域或域加安全令牌身份验证。
- 为 Endpoint Management 启用 Workspace 集成。有关 Workspace 集成的详细信息，请参阅配置 Workspace。

> 重要：
>
> 启用此功能后，将通过 Workspace 而不是通过 Endpoint Management（以前称为 XenMobile）进行 Citrix Files SSO。我们建议您先在 Endpoint Management 控制台中禁用 Citrix Files 集成，然后再启用 Workspace 集成。

Secure Hub 10.8.55

- 能够使用配置 JSON 为 Google 零接触和 Samsung Knox 移动环境 (KME) 门户传递用户名和密码。有关详细信息，请参阅 Samsung Knox 批量注册。

- 启用了证书固定时，用户无法使用自签名证书在 Endpoint Management 中注册。如果用户尝试使用自签名证书向 Endpoint Management 注册，系统会警告其证书不可信。

Secure Hub 10.8.25： Secure Hub for Android 包括对 Android P 设备的支持。

> 注意：
>
> 升级到 Android P 平台之前，请确保您的服务器基础结构符合 subjectAltName (SAN) 扩展中包含匹配的主机名的安全证书的要求。要验证主机名，服务器必须提供一个具有匹配 SAN 的证书。不包含与主机名匹配的 SAN 的证书不再可信。有关详细信息，请参阅 Android 开发人员文档。

2018 年 **3** 月 **19** 日发布的 **Secure Hub for iOS** 更新：适用于 iOS 的 Secure Hub 10.8.6 可用于修复 VPP 应用程序策略存在的问题。有关详细信息，请参阅此 Citrix 知识中心文章。

Secure Hub 10.8.5：在 Secure Hub for Android 中支持 Android Work (Android for Work) 的 COSU 模式。有关详细信息，请参阅 Citrix Endpoint Management 文档。

管理 Secure Hub

可在对 Endpoint Management 进行初始配置过程中执行与 Secure Hub 有关的大多数管理任务。对于 iOS 和 Android，要使 Secure Hub 对用户可用，请将 Secure Hub 上载到 iOS App Store 和 Google Play 应用商店。

当用户的 Citrix Gateway 会话在使用 Citrix Gateway 进行身份验证后恢复时，Secure Hub 还会刷新 Endpoint Management 中存储的适用于已安装应用程序的大多数 MDX 策略。

> 重要：
>
> 更改以下任何策略后都需要用户删除并重新安装应用程序，以应用更新后的策略：安全组、启用加密和 Secure Mail Exchange Server。

Citrix PIN

可以将 Secure Hub 配置为使用 Citrix PIN，这是在 Endpoint Management 控制台的设置 > 客户端属性中启用的一项安全功能。该设置要求已注册的移动设备用户登录 Secure Hub 并使用个人识别码 (PIN) 激活所有 MDX 打包的应用程序。

Citrix PIN 功能简化了登录到受保护的打包应用程序时的用户身份验证体验。用户不需要重复输入其他凭据，例如 Active Directory 用户名和密码。

首次登录 Secure Hub 的用户必须输入其 Active Directory 用户名和密码。登录过程中，Secure Hub 在用户设备上保存 Active Directory 凭据或客户端证书，然后提示用户输入 PIN。用户再次登录时，只需输入 PIN 即可安全地访问其 Citrix 应用程序和 Store，直至活动用户会话的下一个空闲超时期限结束。相关客户端属性允许您使用 PIN 加密机密信息、指定 PIN 的通行码类型以及指定 PIN 的强度和长度要求。有关详细信息，请参阅客户端属性。

启用了指纹 (Touch ID) 身份验证时，用户可以在由于应用程序不活动而需要进行脱机身份验证时进行登录。当用户首次登录 Secure Hub 和重新启动设备时，以及在不活动计时器过期后，用户仍必须输入 PIN。有关启用指纹身份验证的信息，请参阅指纹或 Touch ID 身份验证。

证书固定

Secure Hub for iOS 和 Secure Hub for Android 支持 SSL 证书固定。此功能可确保 Citrix 客户端与 Endpoint Management 通信时使用贵企业签署的证书，因此，可防止在设备上安装根证书时从客户端到 Endpoint Management 的连接危及 SSL 会话的安全。Secure Hub 检测到对服务器公钥所做的任何更改时，Secure Hub 都会拒绝连接。

自 Android N 起，操作系统不再允许使用用户添加的证书颁发机构 (CA)。Citrix 建议使用公共根 CA 代替用户添加的 CA。

如果升级到 Android N 的用户使用私有或自签名 CA，他们可能会遇到问题。在下列情况下，Android N 设备上的连接会断开：

- 使用专用/自签名 CA，并且 “Required Trusted CA for Endpoint Management”（Endpoint Management 所需的可信 CA）选项设置为 **ON**（开）。有关详细信息，请参阅设备管理。
- 使用专用/自签名 CA，且 Endpoint Management 自动发现服务 (ADS) 不可访问。出于安全考虑，ADS 不可访问时，“Required Trusted CA”（所需的可信 CA）即使最初设置为 **OFF**（关）也会变为 **ON**（开）。

注册设备或升级 Secure Hub 之前，请考虑启用证书固定功能。该选项默认设置为关，并通过 ADS 进行管理。启用了证书固定时，用户无法使用自签名证书在 Endpoint Management 中注册。如果用户尝试使用自签名证书进行注册，系统会警告其证书不可信。如果用户不接受证书，注册将失败。

要使用证书固定，应请求 Citrix 向 Citrix ADS 服务器上载证书。使用 Citrix 技术支持门户打开一个技术支持案例。请务必不要将私钥发送到 Citrix。然后，提供以下信息：

- 包含用户注册所用帐户的域。
- Endpoint Management 的完全限定域名 (FQDN)。
- Endpoint Management 实例名称。默认情况下，实例名称为 zdm 并区分大小写。
- 用户 ID 类型，可以是 UPN 或电子邮件。默认情况下，类型为 UPN。
- 用于 iOS 注册的端口（如果更改了默认端口号 8443）。
- Endpoint Management 通过其接受连接的端口（如果更改了默认端口号 443）。
- Citrix Gateway 的完整 URL。
- （可选）管理员的电子邮件地址。
- 您希望添加到域且采用 PEM 格式的证书，该证书必须是公用证书，而非私钥。
- 如何处理现有服务器证书：立即删除旧服务器证书（因为此证书已失效）还是继续支持旧非服务器证书直至其过期。

当您的详细信息和证书添加到 Citrix 服务器时，您的技术支持案例将更新。

证书 **+** 一次性密码身份验证

您可以配置 Citrix ADC，以便 Secure Hub 使用证书及安全令牌（作为一次性密码）执行身份验证。此配置提供了强大的安全选项，可在设备中消除 Active Directory 所占用的空间。

为使 Secure Hub 能够使用证书 + 一次性密码类型的身份验证，请执行以下操作：在 Citrix ADC 中添加一个重写

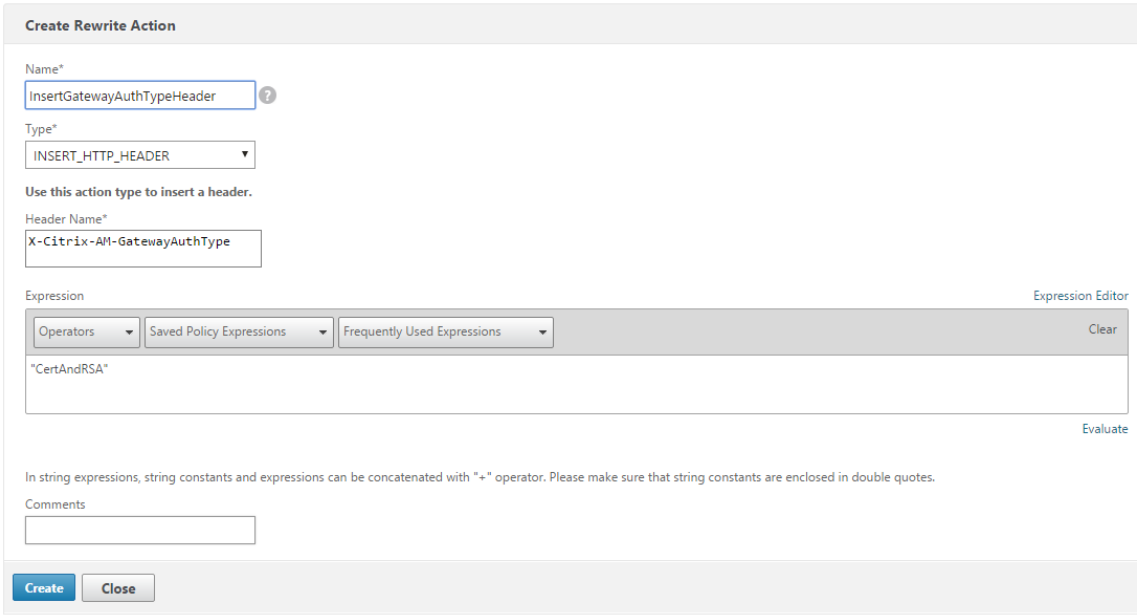
操作和一个重写策略，用于插入格式为 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 的自定义响应头以指示 Citrix Gateway 登录类型。

通常，Secure Hub 使用在 Endpoint Management 控制台中配置的 Citrix Gateway 登录类型。但是，在 Secure Hub 首次完成登录之前此信息不可用。因此，需要自定义头。

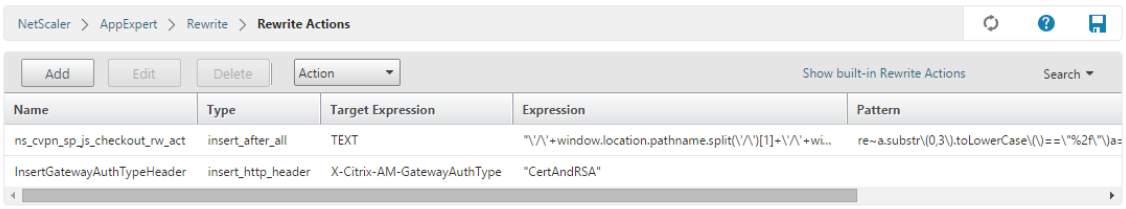
> 注意：
>
> 如果为 Endpoint Management 和 Citrix ADC 设置不同的登录类型，将会使用 Citrix ADC 配置。有关详细信息，请参阅 Citrix Gateway 和 Endpoint Management。

1. 在 Citrix ADC 中，导航到 **Configuration**（配置）**> AppExpert > Rewrite**（重写）**> Actions**（操作）。
2. 单击添加。

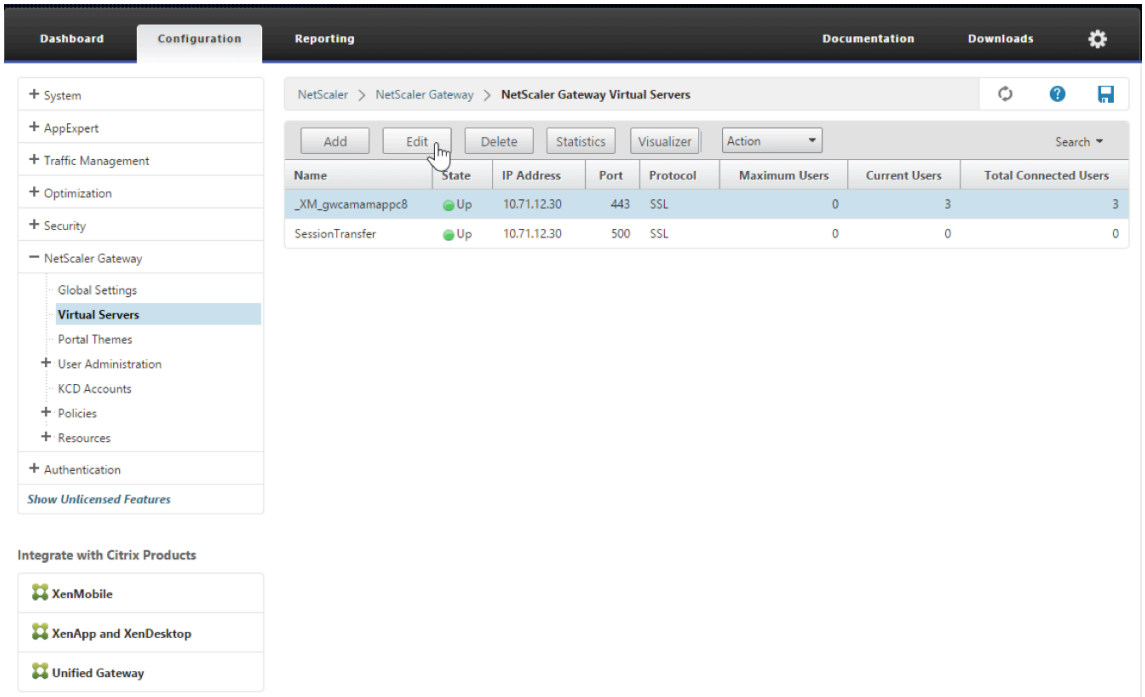
   此时将显示 **Create Rewrite Action**（创建重写操作）屏幕。
3. 填写每个字段（如下图所示），然后单击 **Create**（创建）。



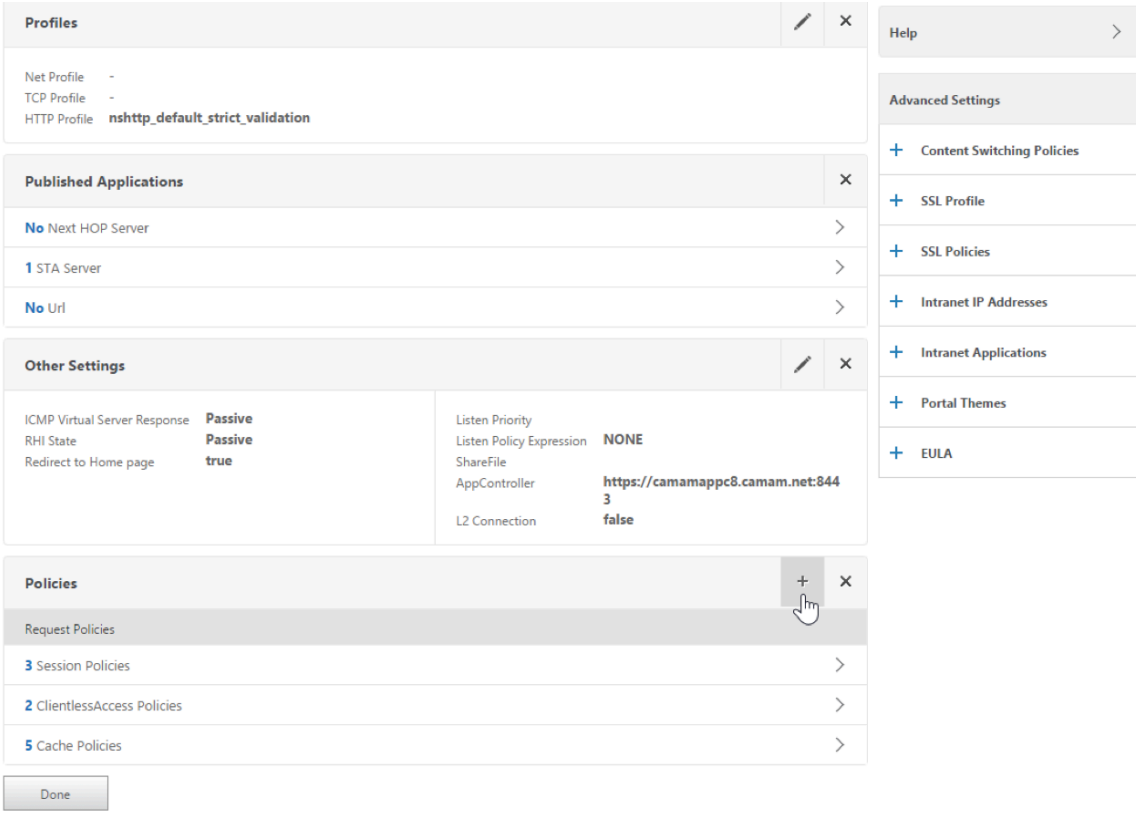
以下结果将显示在主 **Rewrite Actions**（重写操作）屏幕上。



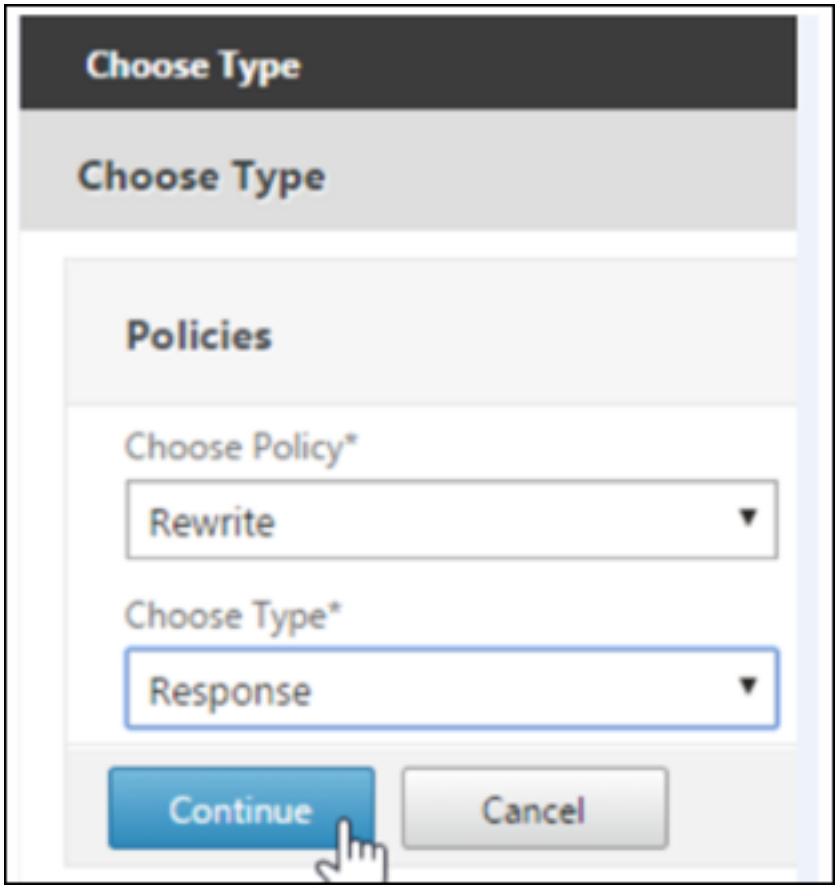
4. 然后您需要将重写操作作为重写策略绑定到虚拟服务器。转到 **Configuration**（配置）**> NetScaler Gateway > Virtual Servers**（虚拟服务器），然后选择您的虚拟服务器。



5. 单击编辑。
6. 在 **Virtual Servers configuration**（虚拟服务器配置）屏幕上，向下滚动到 **Policies**（策略）。
7. 单击 **+** 添加新策略。

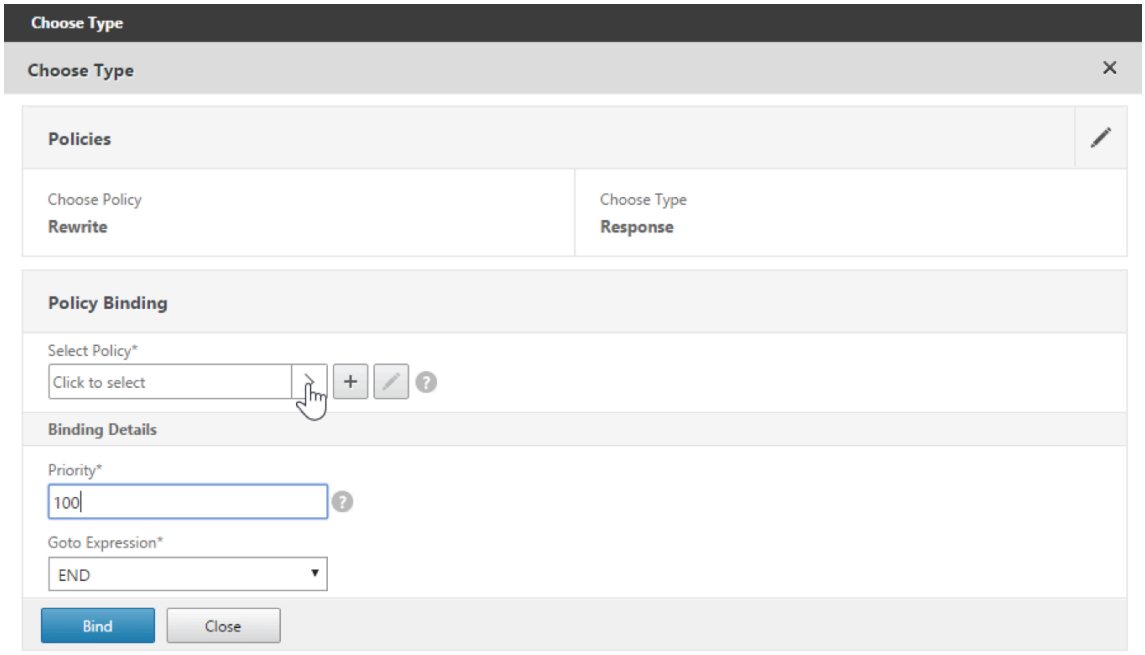


8. 在 **Choose Policy**（选择策略）字段中输入 **Rewrite**（重写）。
9. 在 **Choose Type**（选择类型）字段中输入 **Response**（响应）。



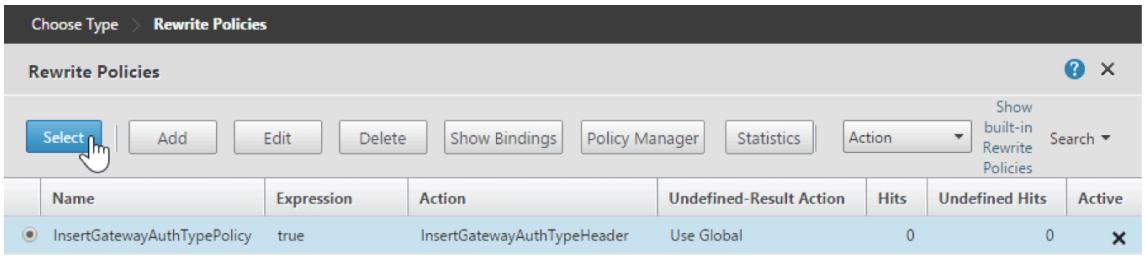
10. 单击继续。

    Policy Binding（策略绑定）部分将展开。

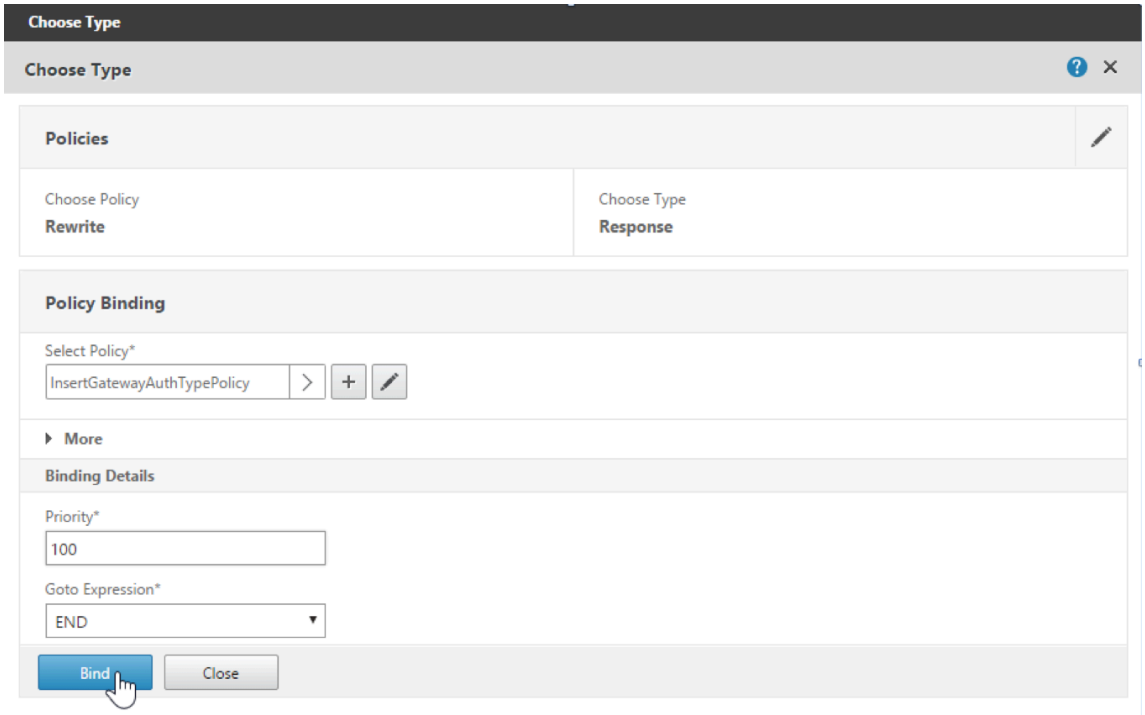


11. 单击 **Select Policy**（选择策略）。

    将出现一个包含现有策略的屏幕

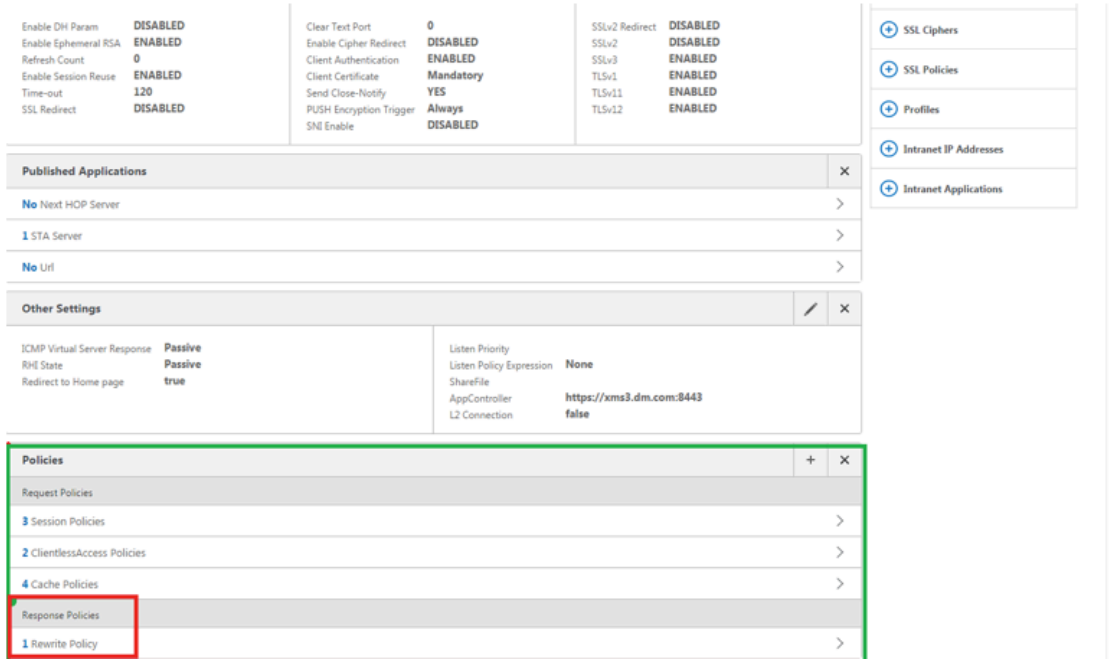


12. 单击刚创建的策略所在行，然后单击 **Select**（选择）。将再次显示 **Policy Binding**（策略绑定）屏幕，其中包含您已填入的选定策略。

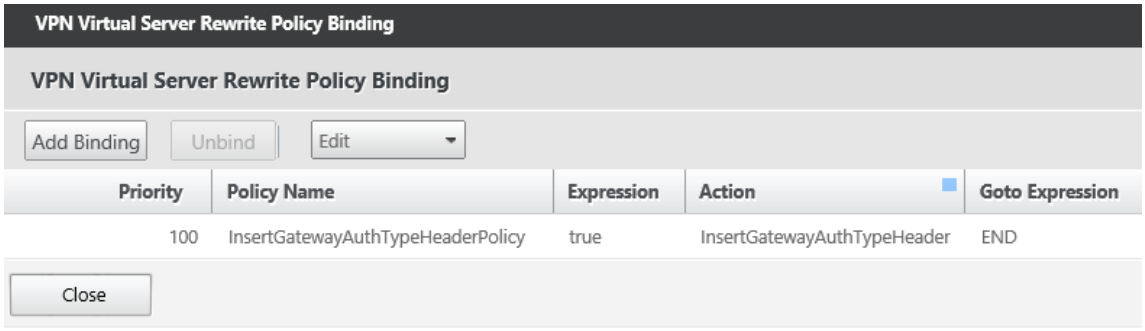


13. 单击 **Bind**（绑定）。

    如果绑定成功，将出现主配置屏幕，其中显示了已完成的重写策略。



14. 要查看策略详细信息，请单击 **Rewrite Policy**（重写策略）。



Android 设备进行 **ADS** 连接的端口要求

端口配置确保从 Secure Hub 连接的 Android 设备可以通过企业网络访问 Citrix ADS。下载通过 ADS 提供的安全更新时，具有访问 ADS 的能力至关重要。ADS 连接可能与您的代理服务器不兼容。在这种情况下，允许 ADS 连接跳过代理服务器。

> 重要：
>
> Secure Hub for Android 和 Secure Hub for iOS 要求您允许 Android 设备访问 ADS。有关详细信息，请参阅 Citrix Endpoint Management 文档中的端口要求。此通信采用出站端口 443。您的现有环境很可能允许此访问。对于无法保证此通信的客户，建议不要升级到 Secure Hub 10.2。如有任何疑问，请联系 Citrix 技术支持。

必备条件：

- 收集 Endpoint Management 和 Citrix ADC 证书。证书必须采用 PEM 格式，并且必须是公用证书，而非私钥。
- 联系 Citrix 技术支持并请求启用证书固定功能。在此过程中，系统会要求您提供证书。

新的证书固定改进功能要求设备先连接到 ADS，然后再注册。此必备条件可确保最新的安全信息对正在其中注册设备的环境中的 Secure Hub 可用。如果设备无法访问 ADS，Secure Hub 不允许设备注册。因此，在内部网络内开启 ADS 访问对于允许设备注册至关重要。

要允许 Secure Hub for Android 访问 ADS，请为以下 IP 地址和 FQDN 打开端口 443：

FQDN	IP 地址	端口	IP 和端口用法
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS 通信
`discovery.mdm.zenprise.com`	52.1.30.122	443	Secure Hub - ADS 通信
`ads.xm.cloud.com`：请注意，Secure Hub 10.6.15 及更高版本使用 `ads.xm.cloud.com`。	34.194.83.188	443	Secure Hub - ADS 通信

FQDN	IP 地址	端口	IP 和端口用法
ads.xm.cloud.com：请注意，Secure Hub 10.6.15 及更高版本使用 ads.xm.cloud.com。	34.193.202.23	443	Secure Hub - ADS 通信

如果启用了证书固定：

- Secure Hub 在设备注册过程中固定您的企业证书。
- 升级过程中，Secure Hub 将丢弃当前固定的所有证书，然后在已注册用户首次连接时固定服务器证书。

  > 注意：
  >
  > 如果您在升级后启用证书固定，用户必须重新注册。

- 如果证书公钥未更改，证书续订不需要重新注册。

证书固定支持分支证书，不支持中间证书或颁发者证书。证书固定适用于 Citrix 服务器（例如 Endpoint Management 和 Citrix Gateway），不适用于第三方服务器。

禁用“删除帐户”选项

在启用了自动发现服务 (ADS) 的环境中，可以在 Secure Hub 中禁用删除帐户选项。

要禁用删除帐户选项，请执行以下步骤：

1. 为域配置 ADS。
2. 在 Citrix Endpoint Management 中打开自动发现服务信息，并将 `displayReenrollLink` 的值设置为 **False**。
   默认情况下，此值为 **True**。
3. 如果您的设备是在 MDM+MAM (ENT) 模式下注册的，请注销并重新登录，更改才能生效。
   如果您的设备是在其他模式下注册的，则必须重新注册设备。

使用 **Secure Hub**

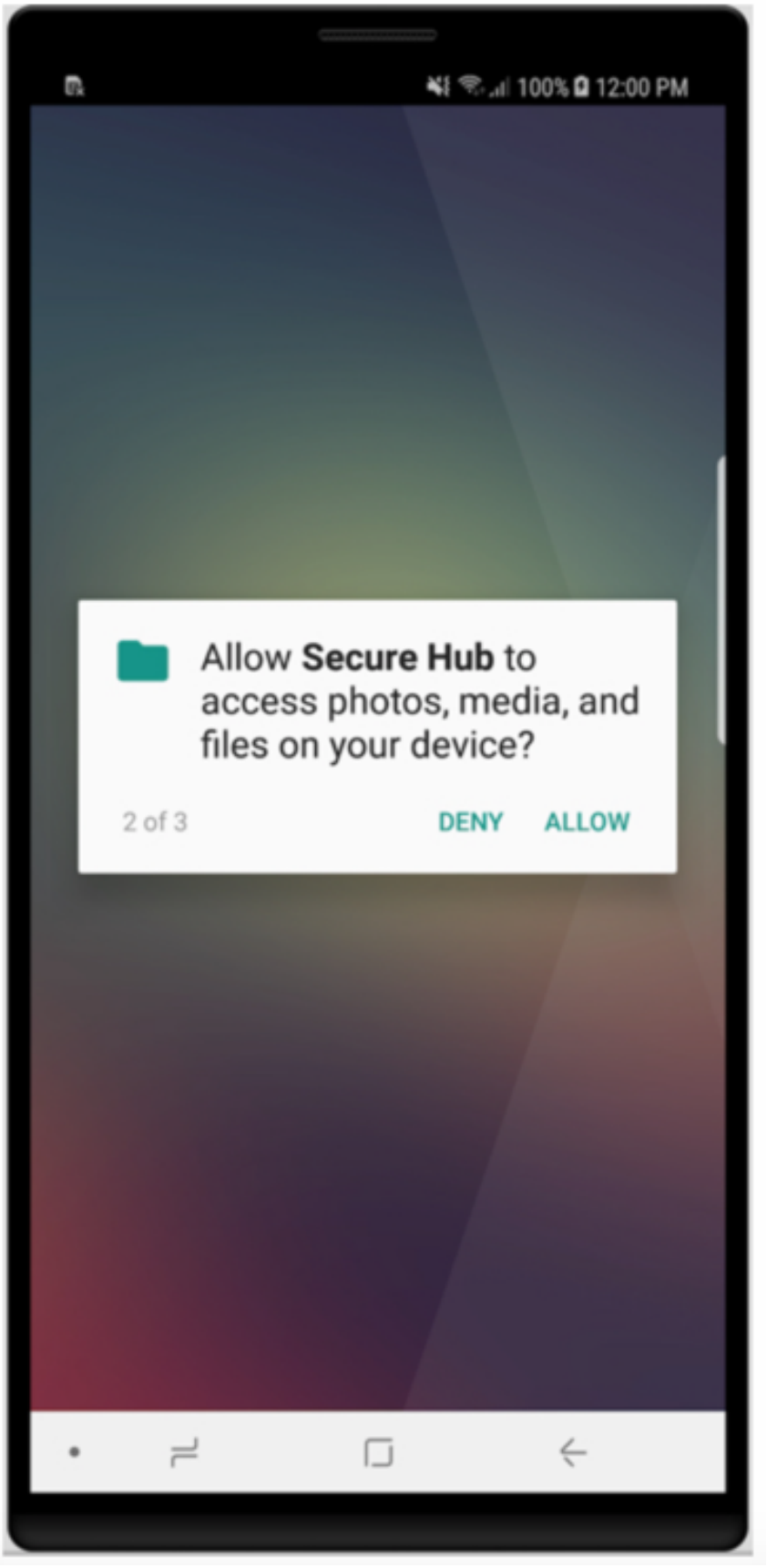
用户首先将 Secure Hub 从 Apple 或 Android 应用商店下载到其设备。

Secure Hub 打开时，用户输入其公司提供的凭据以在 Secure Hub 中注册其设备。有关设备注册的更多详细信息，请参阅用户帐户、角色和注册。

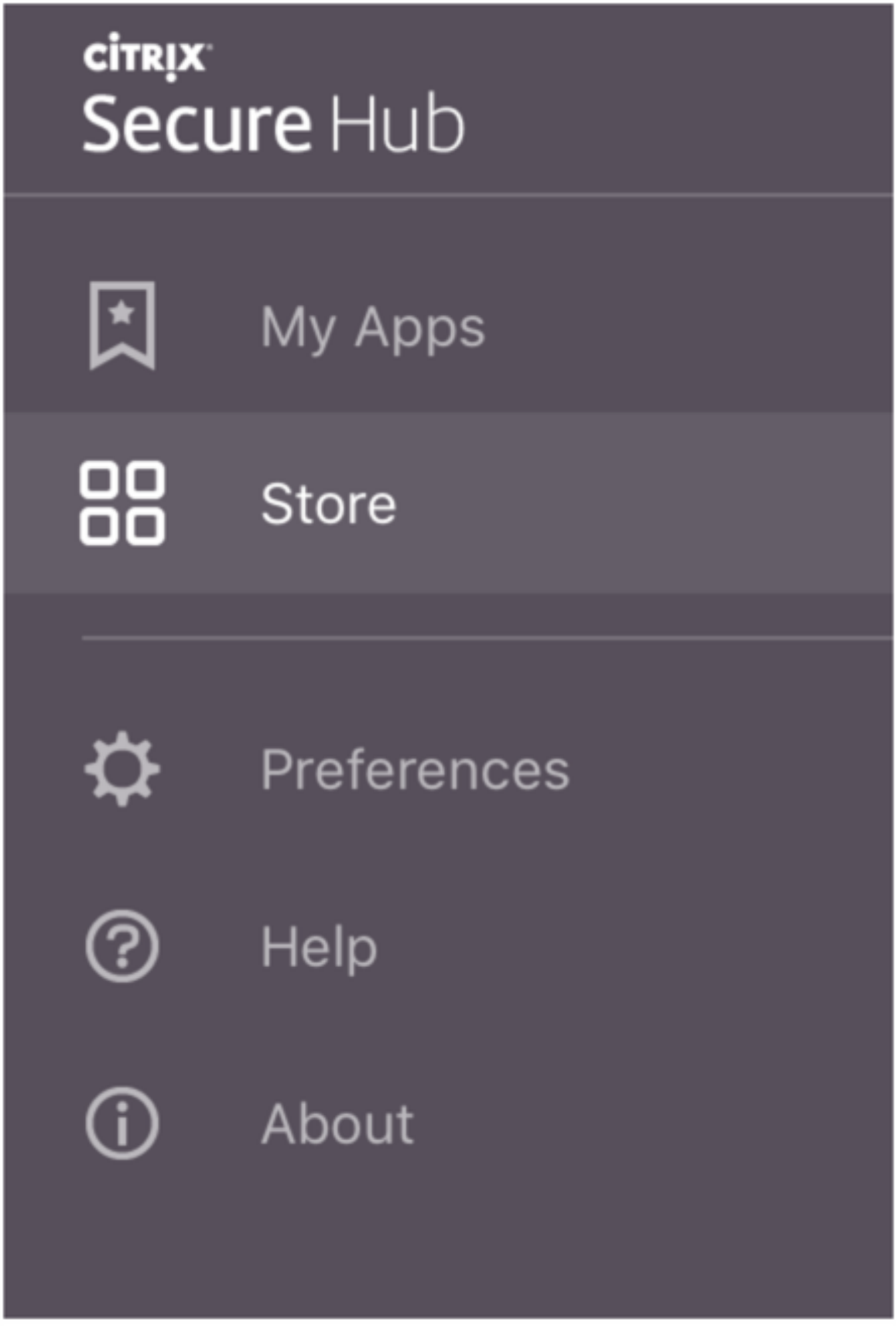
在 Secure Hub for Android 上执行初始安装和注册过程中，将显示以下消息：Allow Secure Hub to access photos, media, and files on your device?（是否允许 Secure Hub 访问您的设备上的照片、媒体和文件?）

此消息来自 Android 操作系统，而非来自 Citrix。轻按允许时，Citrix 以及管理 Secure Hub 的管理员在任何时候都不会查看您的个人数据。但是，如果您与管理员进行远程支持会话，则管理员可以在会话中查看您的个人文件。

注册后，用户将看到您已在其我的应用程序选项卡中推送的所有应用程序和桌面。用户可以从 Store 中添加更多应用程序。在手机上，应用商店链接位于左上角的设置汉堡型图标下方。



在平板电脑上，Store 是一个单独的选项卡。



使用运行 iOS 9 或更高版本的 iPhone 的用户从应用商店安装移动生产力应用程序时，他们会看到一条消息。该消息指出在该 iPhone 上企业开发者 Citrix 不受信任，消息指明在信任该开发者之前，该应用程序将不可用。此消息显示时，Secure Hub 提示用户查看一个指南，指导他们完成为其 iPhone 信任 Citrix 企业应用程序的过程。

自动在 **Secure Mail** 中注册

对于仅 MAM 部署，可以配置 Endpoint Management，以便使用电子邮件凭据在 Secure Hub 中注册的 Android 或 iOS 设备用户能够自动在 Secure Mail 中注册。用户无需输入更多信息或执行额外的步骤即可注册 Secure Mail。

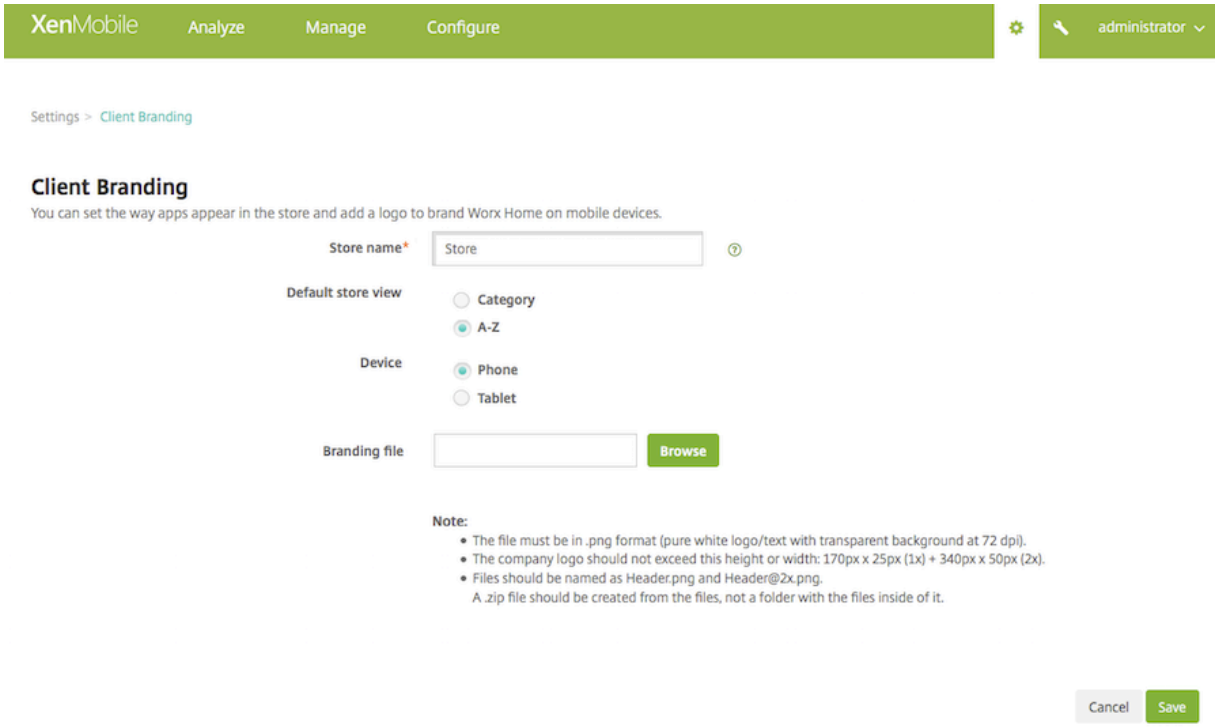
首次使用 Secure Mail 时，Secure Mail 会从 Secure Hub 获取用户的电子邮件地址、域名和用户 ID。Secure Mail 使用电子邮件地址进行自动发现。Exchange Server 使用域和用户 ID 进行标识，这让 Secure Mail 可以自动对用户进行身份验证。如果策略设置为不传递密码，系统会提示用户输入密码。但是，用户不需要输入更多信息。

要启用此功能，请创建三个属性：

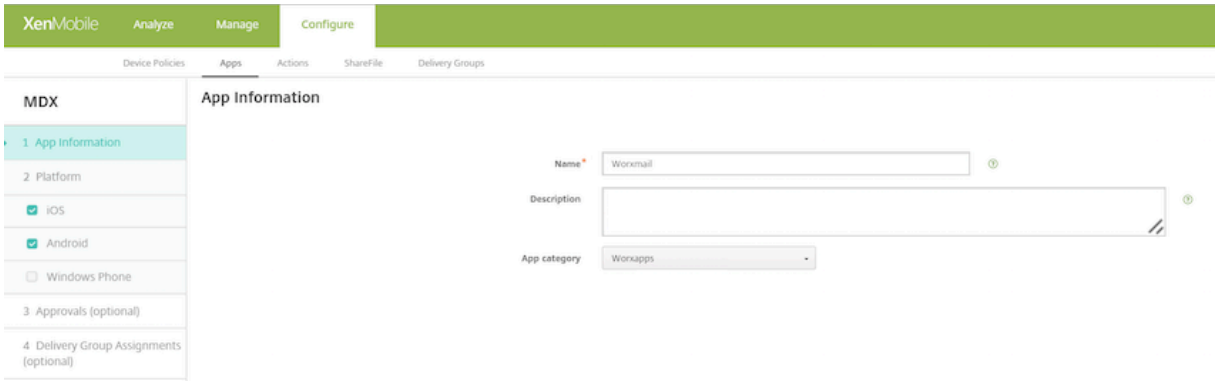
- 服务器属性 MAM_MACRO_SUPPORT。有关说明，请参阅服务器属性。
- 客户端属性 ENABLE_CREDENTIAL_STORE 和 SEND_LDAP_ATTRIBUTES。有关说明，请参阅客户端属性。

自定义的应用商店

如果您需要自定义应用商店，请转到设置 **>** 客户端外观方案，以更改名称、添加徽章及指定应用程序显示方式。



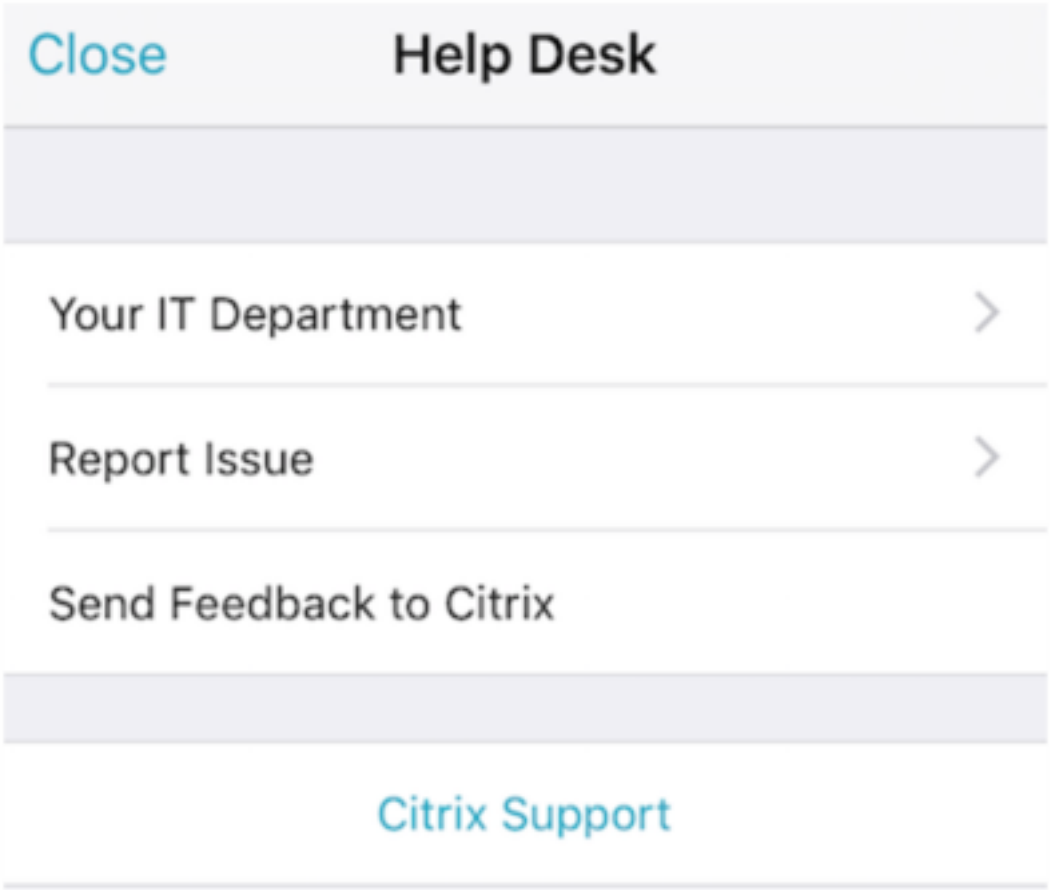
可以在 Endpoint Management 控制台中编辑应用程序说明。单击配置，然后单击应用程序。从表格中选择应用程序，然后单击编辑。选择正在编辑其说明的应用程序的平台，然后在说明框中键入文本。



在 Store 中，用户只能浏览已在 Endpoint Management 中配置且受保护的那些应用程序和桌面。要添加应用程序，用户可以轻按详细信息，然后轻按添加。

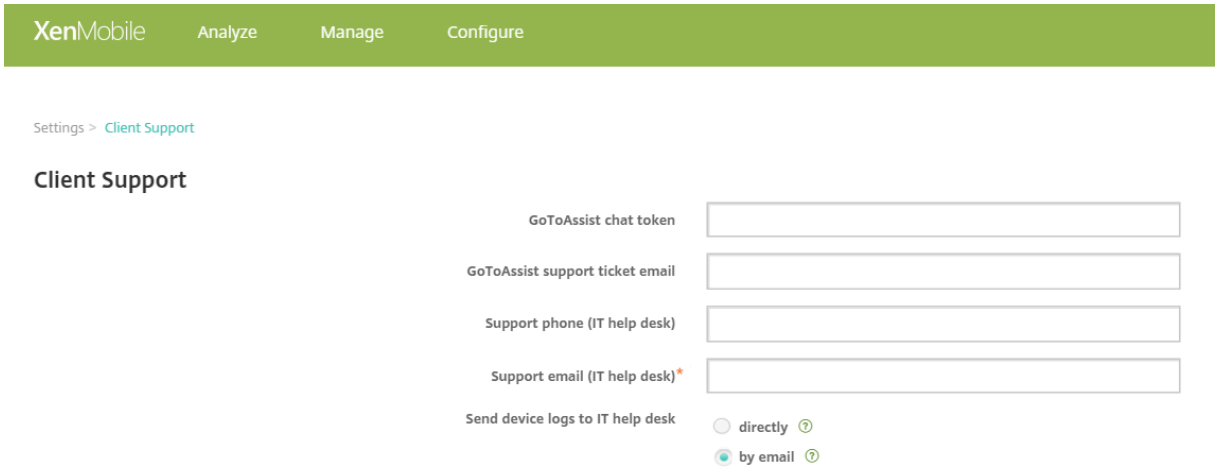
配置的帮助选项

Secure Hub 还向用户提供各种获得帮助的方法。在平板电脑上，轻按右上角的问号将打开帮助选项。在手机上，用户可以轻按右上角的汉堡型菜单图标，然后轻按帮助。



您的 **IT** 部门显示贵公司的技术支持人员的电话和电子邮件，用户可以直接从该应用程序中进行访问。您需要在 Endpoint Management 控制台中输入电话号码和电子邮件地址。单击右上角的齿轮型图标。此时将显示设置页面。

单击更多，然后单击客户端支持。将显示用于输入信息的屏幕。



Report Issue（报告问题）将显示应用程序的列表。用户选择有问题的应用程序。Secure Hub 会自动生成日志，然后在 Secure Mail 中打开一封邮件并将日志附加为 zip 文件。用户添加主题行和问题描述信息。他们还可以附加屏幕截图。

向 **Citrix** 发送反馈在 Secure Mail 中打开一封填写了 Citrix 技术支持地址的邮件。在邮件正文中，用户可以输入关于如何改进 Secure Mail 的建议。如果设备上未安装 Secure Mail，则将打开本机邮件程序。

用户还可以轻按 **Citrix** 支持，之后将打开 Citrix 知识中心。用户可以从中搜索所有 Citrix 产品的支持文章。

在首选项中，用户可以找到关于其帐户和设备的信息。

位置策略

Secure Hub 还提供地理定位和地理跟踪策略，例如，可用于确保公司拥有的设备不会超出特定地理边界。有关详细信息，请参阅定位设备策略。

崩溃收集和分析

Secure Hub 自动收集并分析失败消息，让您能够了解导致特定失败的原因。软件 Crashlytics 支持此功能。

有关适用于 iOS 和 Android 的更多功能，请参阅 Citrix Secure Hub 的“功能（按平台）列表”。

Secure Mail 概述

November 16, 2021

通过 Citrix Secure Mail，用户可以在其移动电话和平板电脑上管理其电子邮件、日历和联系人。为了维护 Microsoft Outlook 或 IBM Notes 帐户的持续性，Secure Mail 会与 Microsoft Exchange Server 和 IBM Notes Traveler 服务器同步。

作为 Citrix 应用程序套件的一部分，由于与 Citrix Secure Hub 的单点登录 (SSO) 兼容性，Secure Mail 从中受益。用户登录 Secure Hub 后，可以无缝移至 Secure Mail，而不需要重新输入其用户名和密码。您可以将 Secure Mail 配置为在 Secure Hub 中注册用户设备时自动推送到用户设备，或者用户可以从 Store 添加该应用程序。

> 注意：
>
> 对 Exchange Server 2010 的支持已于 2020 年 10 月 13 日结束。

Secure Mail 与以下各项兼容：

- Exchange Server 2019 累积更新 11
- Exchange Server 2019 累积更新 10
- Exchange Server 2019 累积更新 9
- Exchange Server 2019 累积更新 8
- Exchange Server 2019 累积更新 7
- Exchange Server 2019 累积更新 6
- Exchange Server 2016 累积更新 22
- Exchange Server 2016 累积更新 21
- Exchange Server 2016 累积更新 20
- Exchange Server 2016 累积更新 19
- Exchange Server 2016 累积更新 18
- Exchange Server 2016 累积更新 17
- Exchange Server 2013 累积更新 23
- Exchange Server 2013 累积更新 22
- Exchange Server 2013 累积更新 21
- IBM Domino Mail Server 10.0.1
- IBM Domino 邮件服务器 9.0.1 FP10 HF197
- IBM Lotus Notes Traveler 10.0.1.0 Build 201811191126_20
- IBM Lotus Notes Traveler 9.0.1.21
- Microsoft Office 365 (Exchange Online)

要开始使用，请从 Citrix Endpoint Management 下载页面下载 Secure Mail 及其他 Endpoint Management 组件。

有关 Secure Mail 及其他移动应用程序的系统要求，请参阅系统要求。

有关应用程序在后台运行或关闭时 Secure Mail for iOS 和 Secure Mail for Android 中的通知信息，请参阅 Secure Mail 的推送通知。

有关 Secure Mail 支持的 iOS 功能，请参阅适用于 Secure Mail 的 iOS 功能。

有关 Secure Mail 支持的 Android 功能，请参阅适用于 Secure Mail 的 Android 功能。

有关 Secure Mail 支持的 iOS 和 Android 功能，请参阅适用于 Secure Mail 的 iOS 和 Android 功能。

有关用户帮助文档，请参阅 Citrix 用户帮助中心中的 Citrix Secure Mail 页面。

Citrix Secure Web

March 26, 2021

Citrix Secure Web 是一款 HTML5 兼容的 Web 浏览器，用于提供对内部和外部站点的安全访问。您可以将 Secure Web 配置为在 Secure Hub 中注册用户设备时自动推送到用户设备。或者，您也可以从 Endpoint Management 应用商店添加应用程序。

有关 Secure Web 以及其他移动生产力应用程序系统要求，请参阅系统要求。

集成并交付 **Secure Web**

> 注意：
>
> MDX Toolkit 10.7.10 是支持打包移动生产力应用程序的最后一个版本。用户从公共应用商店访问移动生产力应用程序 10.7.5 及更高版本。

要集成并交付 Secure Web，请按照以下常规步骤进行操作：

1. 要对内部网络启用单点登录 (SSO)，请配置 Citrix Gateway。

   对于 HTTP 流量，Citrix ADC 可以向 Citrix ADC 支持的所有代理身份验证类型提供 SSO。对于 HTTPS 流量，“Web 密码缓存” 策略允许 Secure Web 进行身份验证并通过 MDX 提供对代理服务器的 SSO。MDX 仅支持基本身份验证、摘要式身份验证和 NTLM 代理身份验证。密码使用 MDX 缓存并存储在 Endpoint Management 共享保管库（用于存储敏感应用程序数据的安全存储区域）中。有关 Citrix Gateway 配置的详细信息，请参阅 Citrix Gateway。

2. 下载 Secure Web。
3. 确定如何配置与内部网络之间的用户连接。
4. 将 Secure Web 添加到 Endpoint Management 中（操作步骤与其他 MDX 应用程序相同），然后配置 MDX 策略。有关 Secure Web 特定策略的详细信息，请参阅本文后面的 “关于 Secure Web 策略”。

配置用户连接

Secure Web 支持以下用户连接配置：

- 安全浏览：通过通道连接到内部网络的连接可以使用无客户端 VPN 的变体（称为 “安全浏览”）。这是为首选 **VPN** 模式策略指定的默认配置。建议对需要单点登录 (SSO) 的连接使用安全浏览。

- 完整 **VPN** 通道：通过通道连接到内部网络的连接可以使用首选 **VPN** 模式策略配置的完整 VPN 通道。建议对通过客户端证书或端到端 SSL 与内部网络中的资源建立的连接使用完整 VPN 通道。但是，Secure Web 不是可以读取存储在移动设备上的客户端证书的应用程序。可能会安装一些可提供此功能的第三方封装企业应用程序。完整 VPN 通道通过 TCP 处理任何协议，并且可以在 Windows 和 Mac 计算机以及 iOS 和 Android 设备上使用。
- 允许 **VPN** 模式切换策略允许用户根据需要在完整 VPN 通道模式与安全浏览模式之间自动切换。默认情况下，此策略设置为 “关”。如果此策略设置为 “开”，则将在备选模式下尝试重新处理由于无法在首选 VPN 模式下处理身份验证请求而失败的网络请求。例如，完整 VPN 通道模式接受服务器对客户端证书的质询，但安全浏览模式不接受。同样，使用安全浏览模式时，通过 SSO 向 HTTP 身份验证质询提供服务的可能性更大。
- 使用 **PAC** 的完整 **VPN** 通道：可以对 iOS 和 Android 设备的完整 VPN 通道部署使用代理自动配置 (PAC) 文件。PAC 文件中包含的规则用于定义 Web 浏览器如何选择代理以访问指定 URL。PAC 文件规则可以指定对外部和内部站点的处理方式。Secure Web 解析 PAC 文件规则并将代理服务器信息发送到 Citrix Gateway。
- 使用 PAC 文件时，完整 VPN 通道的性能可以与安全浏览模式相媲美。有关 PAC 配置的详细信息，请参阅使用 PAC 的完整 VPN 通道。

下表说明了 Secure Web 是否会根据配置和站点类型提示用户输入凭据：

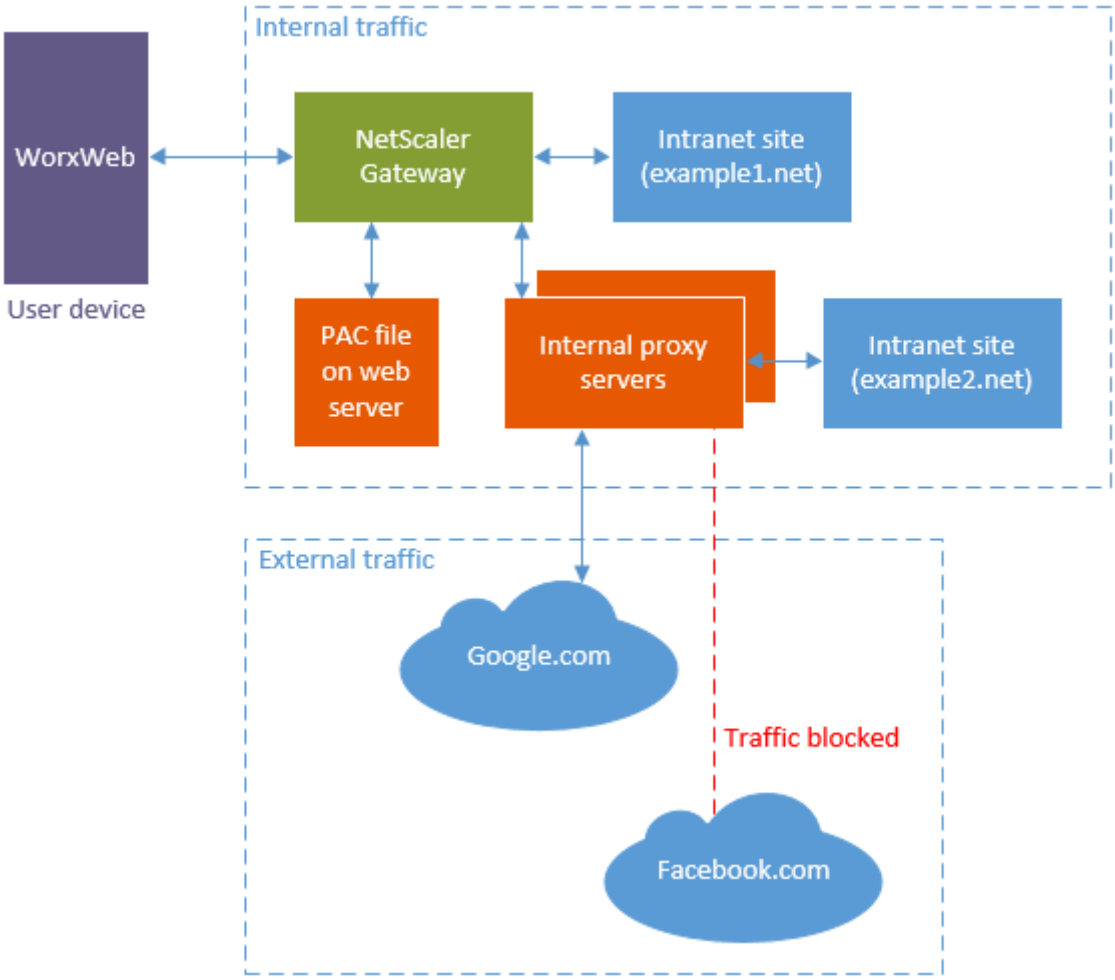
连接模式	站点类型	密码缓存	为 Citrix Gateway 配置的 SSO	在首次访问 Web 站点时，Secure Web 提示输入凭据	在之后访问 Web 站点时，Secure Web 提示输入凭据	在更改密码后，Secure Web 提示输入凭据
安全浏览	HTTP	否	是	否	否	否
安全浏览	HTTPS	否	是	否	否	否
完整 VPN	HTTP	否	是	否	否	否
完整 VPN	HTTPS	是；如果 Secure Web MDX 策略 “启用 Web 密码缓存” 设置为 “开”。	否	是；在 Secure Web 中缓存凭据时需要。	否	是

使用 **PAC** 的完整 **VPN** 通道

> 重要：
>
> 如果为 Secure Web 配置了 PAC 文件，并且为代理操作配置了 Citrix ADC，Secure Web 将超时。请务必在使用 “使用 PAC 的完整 VPN 通道” 之前删除为代理配置的 Citrix Gateway 流量策略。

为 Secure Web 配置使用 PAC 文件或代理服务器的完整 VPN 通道时，Secure Web 通过 Citrix Gateway 将所有流量发送到代理。Citrix Gateway 随后根据代理配置规则路由流量。在此配置中，Citrix Gateway 无法识别 PAC 文件或代理服务器。该通信流与不使用 PAC 文件的完整 VPN 通道的通信流相同。

下图显示了 Secure Web 用户导航到某个 Web 站点时的通信流：



在该示例中，流量规则指定以下内容：

- Citrix Gateway 直接连接到 Intranet 站点 `example1.net`。
- 流向 Intranet 站点 `example2.net` 的流量通过内部代理服务器代理。
- 外部流量通过内部代理服务器代理。代理规则阻止流向以下站点的外部流量 `Facebook.com`.

配置使用 **PAC** 的完整 **VPN** 通道

1. 验证并测试 PAC 文件。

   > 注意：
   >
   > 有关创建和使用 PAC 文件的详细信息，请参阅 https://findproxyforurl.com/。

   使用 PAC 验证工具（例如 Pacparser）验证 PAC 文件。读取 PAC 文件时，请确保 Pacparser 结果与您的预期相同。如果 PAC 文件包含语法错误，移动设备将忽略 PAC 文件。（PAC 文件仅存储在移动设备上的内存中。）

   PAC 文件按照从上到下的顺序处理，有规则与当前查询匹配时停止处理。

请在将 PAC 文件 URL 输入 Endpoint Management 的 PAC/代理字段之前，在 Web 浏览器中测试此 URL。确保计算机可以访问 PAC 文件所在的网络。

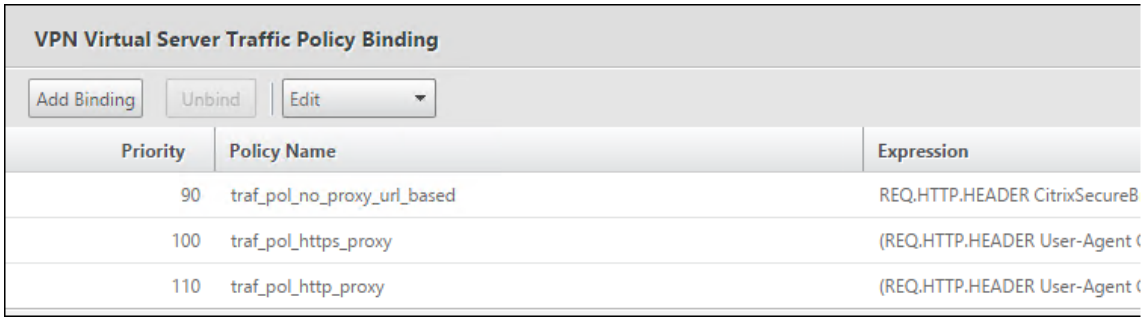
```
https://webserver.local/GenericPAC.pac
https://webserver.local/GenericPAC.pac
```

经过测试的 PAC 扩展名为.txt 或.pac。

PAC 文件在 Web 浏览器中显示其内容。

> 重要：
>
> 每次更新用于 Secure Web 的 PAC 文件时，都会通知用户必须关闭并重新打开 Secure Web。

2. 配置 Citrix Gateway：
   - 禁用 Citrix Gateway 拆分通道。如果启用了拆分通道并且配置了 PAC 文件，PAC 文件规则将覆盖 Citrix ADC 拆分通道规则。代理不会覆盖 Citrix ADC 拆分通道规则。
   - 删除为代理配置的 Citrix Gateway 流量策略。这是 Secure Web 正常运行必需的。下图显示了要删除的策略规则示例。



3. 配置 Secure Web 策略：
   - 将“首选 VPN 模式”策略设置为完整 **VPN** 通道。
   - 将“允许 VPN 模式切换”策略设置为关。
   - 配置 PAC 文件 URL 或代理服务器策略。Secure Web 支持 HTTP 和 HTTPS 以及默认端口和非默认端口。对于 HTTPS，如果证书为自签名证书或者不受信任，则必须在设备上安装根证书颁发机构。

     请务必在配置策略之前，先在 Web 浏览器中测试 URL 或代理服务器地址。

     PAC 文件 URL 示例：

     ```
     http[s]://example.com/proxy.pac
     http[s]://10.10.0.100/proxy.txt
     ```

     示例代理服务器（需要配置端口）：

     ```
     myhost.example.com:port
     ```

     ```
     10.10.0.100:port
     ```


> 注意：
>
> 如果配置了 PAC 文件或代理服务器，请不要在 Wi-Fi 的系统代理设置中配置 PAC。

- 将“启用 Web 密码缓存”策略设置为开。Web 密码缓存处理 HTTPS 站点的 SSO。

  如果代理支持相同的身份验证基础结构，Citrix ADC 可以对内部代理执行 SSO。

PAC 文件支持的限制

Secure Web 不支持：

- 从一台代理服务器故障转移到另一台代理服务器。PAC 文件评估可以返回某个主机名对应的多台代理服务器。Secure Web 仅使用返回的第一个代理服务器。
- PAC 文件中的协议（例如 FTP 和 gopher）。
- PAC 文件中的 SOCKS 代理服务器。
- Web 代理自动发现协议 (Web Proxy AutoDiscovery Protocol, WPAD)。

Secure Web 忽略 PAC 文件功能警报，以使 Secure Web 能够解析不包括这些调用的 PAC 文件。

Secure Web 策略

添加 Secure Web 时，请注意 Secure Web 特定的这些 MDX 策略。对于所有受支持的移动设备：

允许或阻止的 **Web** 站点

Secure Web 通常不过滤 Web 链接。您可以使用此策略配置特定的允许或阻止站点的列表。可以对 URL 模式进行配置，以限制浏览器可以打开的 Web 站点，其格式为逗号分隔的列表。加号 (+) 或减号 (-) 作为前缀添加到列表中的每种模式前面。浏览器按列出顺序将 URL 与模式进行比较，直至找到一个匹配项。找到匹配项后，前缀将决定要执行的操作，如下所示：

- 减号 (-) 前缀指示浏览器阻止打开 URL。在这种情况下，该 URL 被视为 Web 服务器地址无法解析。
- 加号 (+) 前缀允许按常规处理 URL。
- 如果随模式提供 + 或 -，则会假定提供 +（允许）。
- 如果 URL 与列表中的任何模式都不匹配，则允许打开该 URL。

要阻止所有其他 URL，请在列表结尾添加减号后跟星号 (-*)。例如：

- 策略值 +`http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` 允许在 `mycorp.com` 域中使用 HTTP URL，但在其他位置阻止这些 URL，允许在任何位置使用 HTTPS 和 FTP URL，但阻止所有其他 URL。
- 策略值 +`http://*.training.lab/*,+https://*.training.lab/*,-*` 允许用户通过 HTTP 或 HTTPS 打开 Training.lab 域 (Intranet) 中的任何站点。但是，无论协议如何，您都无法打开公用 URL，例如 Facebook、Google 和 Hotmail。

默认值为空（允许打开所有 URL）。

阻止弹出窗口

弹出窗口是在未经您允许的情况下 Web 站点打开的新选项卡。此策略确定 Secure Web 是否允许弹出窗口。如果设为“开”，Secure Web 将阻止 Web 站点打开弹出窗口。默认值为关。

预加载的书签

为 Secure Web 浏览器定义一组预加载的书签。此策略是一组用逗号分隔的元组列表，包括文件夹名称、友好名称和 Web 地址。每个元组必须采用 folder, name, url 格式，其中 folder 和 name 可能会有选择地用双引号 (“) 引起。

例如，策略值 `,"Mycorp, Inc. home page",https://www.mycorp.com, "MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx` 定义了三个书签。第一个为主链接（无文件夹名称），标题为 “Mycorp, Inc. home page”。第二个链接放置在标题为 “MyCorp Links”、标签为 “Account logon” 的文件夹中。第三个链接放置在 “MyCorp Links” 文件夹的 “Investor Relations” 子文件夹中，显示为 “Contact us”。

默认值为空。

主页 **URL**

定义 Secure Web 在启动时加载的 Web 站点。默认值为空（默认启动页面）。

仅限受支持的 Android 和 iOS 设备：

浏览器用户界面

规定 Secure Web 的浏览器用户界面控件的行为和可见性。通常情况下，所有浏览控件都可用。这些控件包括前进、后退、地址栏和刷新/停止控件。可以配置此策略以限制这些控件的使用和可见性。默认值为所有控件都可见。

选项

- 所有控件都可见。所有控件都可见，并且不限制用户使用。
- 只读地址栏。所有控件都可见，但用户无法编辑浏览器地址字段。
- 隐藏地址栏。隐藏地址栏，但不隐藏其他控件。
- 隐藏所有控件。禁止显示整个工具栏以提供无框浏览体验。

启用 **Web** 密码缓存

当 Secure Web 用户为访问或请求 Web 资源输入凭据时，此策略确定 Secure Web 是否以无提示方式在设备上缓存密码。此策略适用于在身份验证对话框中输入的密码，不适用于在 Web 表单中输入的密码。

如果设置为开，Secure Web 将缓存用户在请求 Web 资源时输入的所有密码。如果设置为关，Secure Web 将不缓存密码并删除已缓存的现有密码。默认值为关。

仅当您同时将“首选 VPN”策略设置为此应用程序的完整 VPN 通道时才能启用此策略。

代理服务器

在安全浏览模式下使用时，还可以为 Secure Web 配置代理服务器。有关详细信息，请参阅此 博客文章。

DNS 后缀

在 Android 上，如果未配置 DNS 后缀，VPN 可能会失败。有关配置 DNS 后缀的详细信息，请参阅支持使用面向 Android 设备的 DNS 后缀进行 DNS 查询。

准备用于 **Secure Web** 的 **Intranet** 站点

此部分面向 Web 站点开发人员，他们需要准备用于 Secure Web for Android 和 Secure Web for iOS 的 Intranet 站点。旨在用于桌面浏览器的 Intranet 站点需要更改才能在 Android 和 iOS 设备上正常使用。

Secure Web 依靠 Android WebView 和 iOS WkWebView 来提供 Web 技术支持。Secure Web 支持的一些 Web 技术包括：

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL

Secure Web 不支持的一些 Web 技术包括：

- Flash
- Java

下表显示了 Secure Web 支持的 HTML 呈现功能和技术。X 表示相应功能适用于某个平台、浏览器和组件组合。

技术	iOS Secure Web	Android 6.x/7.x Secure Web
JavaScript 引擎	JavaScriptCore	V8
本地存储	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X

技术	iOS Secure Web	Android 6.x/7.x Secure Web
WebGL		X
requestAnimationFrame API		X
导航计时 API		X
资源计时 API		X

技术在不同设备上作用方式相同；但 Secure Web 对不同的设备返回不同的用户代理字符串。要确定用于 Secure Web 的浏览器版本，可以查看其用户代理字符串。从 Secure Web 导航到 https://whatsmyuseragent.com/。

Intranet 站点故障排除

要解决在 Secure Web 中查看 Intranet 站点时遇到的呈现问题，请将 Web 站点在 Secure Web 上的呈现情况与在兼容的第三方浏览器中的呈现情况进行比较。

对于 iOS，用于测试的兼容第三方浏览器为 Chrome 和 Dolphin。

对于 Android，用于测试的兼容第三方浏览器为 Dolphin。

> 注意：
>
> Chrome 是 Android 上的本机浏览器。请勿将其用于比较。

在 iOS 中，请确保浏览器支持设备级 VPN。可以通过在设备上导航到设置 **> VPN >** 添加 **VPN** 配置来配置 VPN。

还可以使用应用商店中提供的 VPN 客户端应用程序，例如 Citrix VPN、Cisco AnyConnect 或 Pulse Secure。

- 如果 Web 页面在两个浏览器上的呈现情况相同，则问题源于您的 Web 站点。请更新此站点，并确保它可以很好地适用于操作系统。
- 如果 Web 页面上的问题仅出现在 Secure Web 中，请联系 Citrix 技术支持，以打开一个支持票证。请提供您的故障排除步骤，包括测试过的浏览器和操作系统类型。如果 Secure Web for iOS 存在呈现问题，请按以下步骤所述将页面的 Web 存档包括在内。这样可帮助 Citrix 更加快速地解决该问题。

创建 Web 存档文件

在 macOS 10.9 或更高版本上使用 Safari，可以将 Web 页面另存为 Web 存档文件（又称为“阅读列表”）。Web 存档文件包括所有链接的文件，例如图像、CSS 和 JavaScript。

1. 在 Safari 中，清空“阅读列表”文件夹：在 **Finder** 中，单击菜单栏中的前往菜单，选择前往文件夹，键入路径名称 ~/Library/Safari/ReadingListArchives/，然后删除该位置下的所有文件夹。
2. 在菜单栏中，转到 **Safari >** 偏好设置 **>** 高级并启用“在菜单栏中显示 **“开发”** 菜单”。

3. 在菜单栏中，转到开发 **>** 用户代理并输入 Secure Web 用户代理：（Mozilla/5.0（iPad，CPU OS 8_3，例如 macOS）AppleWebKit/600.1.4（KHTML，例如 Gecko）Mobile/12F69 Secure Web/10.1.0 （内部版本 1.4.0）Safari/8536.25）。
4. 在 Safari 中，打开要另存为阅读列表（Web 存档文件）的 Web 站点。
5. 在菜单栏中，转到书签 **>** 添加到阅读列表。存档在后台进行，可能需要几分钟时间。
6. 找到存档的阅读列表：在菜单栏中，转到查看 **>** 显示阅读列表边栏。
7. 验证存档文件：
   - 关闭与 Mac 之间的网络连接。
   - 打开阅读列表中的 Web 站点。

     该 Web 站点完全呈现。
8. 压缩存档文件：在 **Finder** 中，单击菜单栏中的前往菜单，选择前往文件夹，键入路径名称 ~/Library/Safari/ReadingListArchives/。现在将压缩使用随机十六进制字符串作为文件名的文件夹。打开支持票证时，可以将此文件发送给 Citrix 技术支持。

Secure Web 功能

Secure Web 利用移动数据交换技术创建专用 VPN 通道，以便用户能够访问内部和外部 Web 站点以及所有其他 Web 站点。这包括受贵公司的策略保护的环境中包含敏感信息的站点。

Secure Web 与 Secure Mail 和 Citrix Files 的集成在安全的 Endpoint Management 容器中提供无缝的用户体验。下面是集成功能的几个示例：

- 用户轻按 **Mailto** 链接时，将在 Citrix Secure Mail 中打开一封新电子邮件，不需要进一步进行身份验证。
- 在 iOS 中，用户可以在 Secure Web 中从本机邮件应用程序打开链接，方法是在 URL 前插入 **ctxmobilebrowser://**。例如，从本机邮件应用程序中打开 `example.com`，使用 URL ctxmobilebrowser://example.com。
- 当用户单击电子邮件中的 Intranet 链接时，Secure Web 会转到该站点而无需进行额外的身份验证。
- 用户可以将其在 Secure Web 中从 Web 下载的文件上载到 Citrix Files。

Secure Web 用户还可以执行以下操作：

- 阻止弹出窗口。

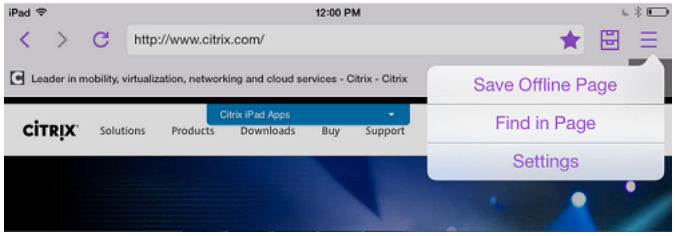
  > 注意：
  >
  > Secure Web 的大多数内存用于呈现弹出窗口，因此，通常可通过在“设置”中阻止弹出窗口来提高性能。

- 为收藏的站点添加书签。
- 下载文件。
- 脱机保存页面。

- 自动保存密码。
- 清除缓存/历史记录/cookie。
- 禁用 Cookie 和 HTML5 本地存储。
- 与其他用户安全地共享设备。
- 在地址栏中搜索。
- 允许他们在 Secure Web 中运行的 Web 应用程序访问其位置。
- 导出和导入设置。
- 直接在 Citrix Files 中打开文件，而不必下载文件。要启用此功能，请在 Endpoint Management 中将 **ctx-sf:** 添加到“允许的 URL ”策略。
- 在 iOS 中，请使用三维触控操作来打开新选项卡，并直接从主屏幕访问脱机页面、收藏的站点和下载内容。
- 在 iOS 中，下载任意大小的文件并在 Citrix Files 或其他应用程序中打开。

  > 注意：
  >
  > 将 Secure Web 置于后台将导致下载停止。

- 使用在网页中查找在当前页面视图中搜索词语。



Secure Web 还具有动态文本支持功能。此应用程序显示用户在其设备上设置的字体。

适用于移动生产力应用程序的 **Citrix QuickEdit**

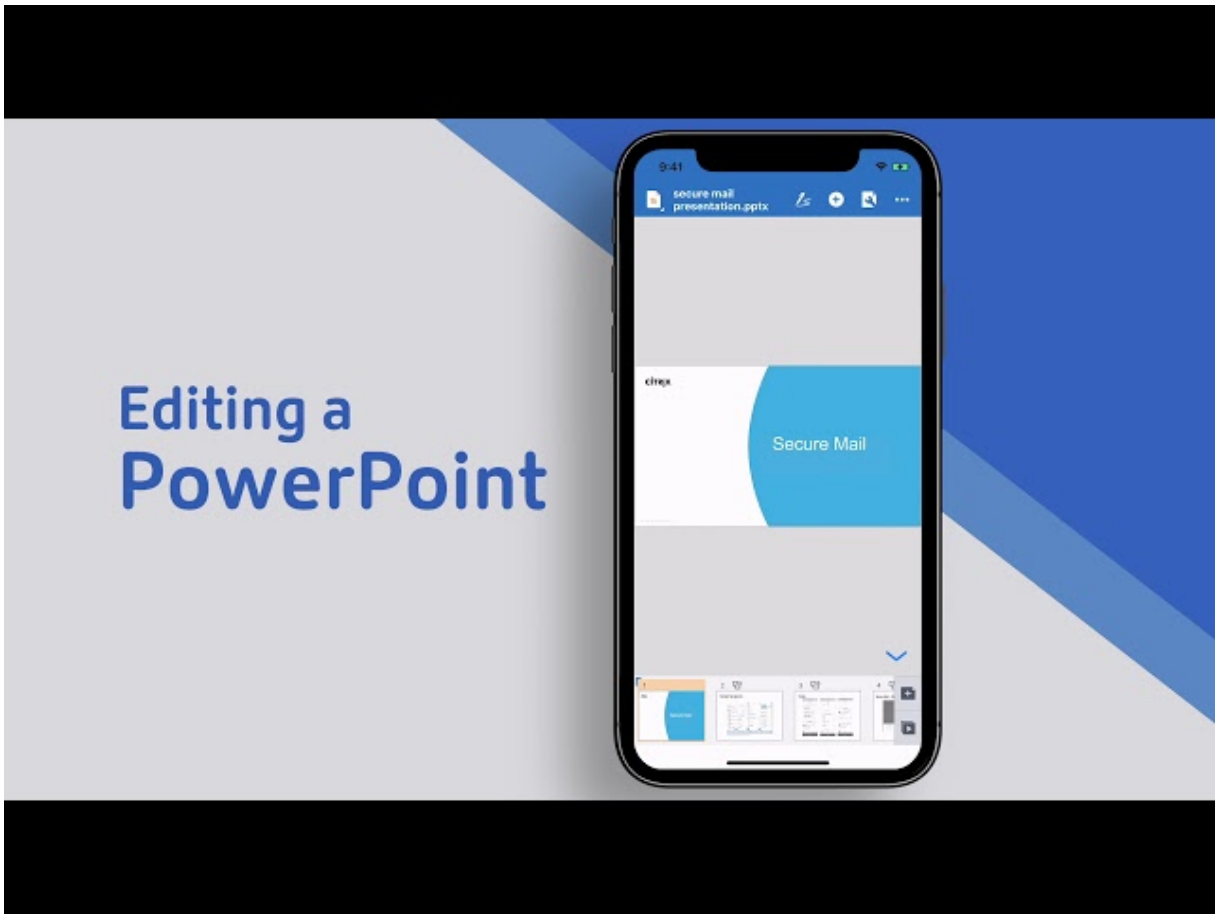
May 20, 2021

Citrix QuickEdit 是用于移动生产力应用程序的编辑工具。它与 Citrix Secure Mail 和适用于 Endpoint Management 的 Citrix Content Collaboration 兼容，允许在安全的 Endpoint Management 环境中无缝执行工作流。

> 更新：
>
> - **2020** 年 **6** 月 **19** 日更新： MDX 加密将于 2020 年 9 月 1 日达到生命周期已结束 (EOL) 状态。您必须在 2020 年 7 月之前测试并计划从 MDX 加密迁移。
> - **2018** 年 **7** 月 **2** 日更新： QuickEdit 仍作为移动生产力应用程序提供。我们将不应用以前公布的 2018 年

> 9 月 1 日的生命周期已结束 (EOL) 状态。相反，我们计划推出 QuickEdit 的内容管理组件的更新。

有关介绍 Citrix QuickEdit 功能的视频，请观看 Citrix YouTube 频道中的此视频：



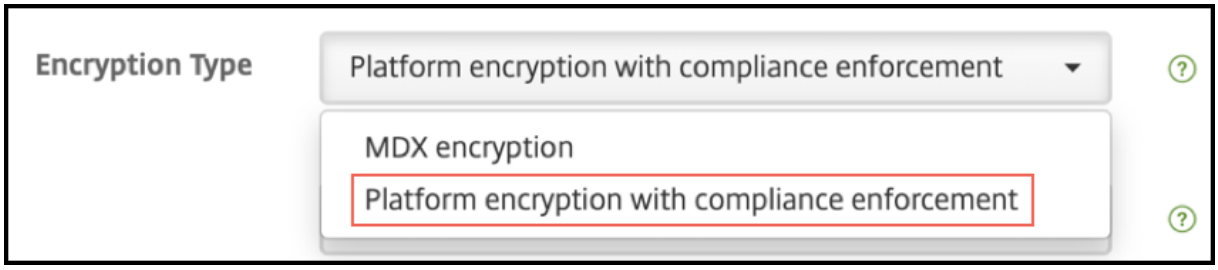
有关 QuickEdit 及其他移动生产力应用程序的系统要求，请参阅系统要求。

您可以将 QuickEdit 配置为在 Secure Hub 中注册用户设备时自动推送到用户设备。此外，用户还可以从应用商店中添加该应用程序。

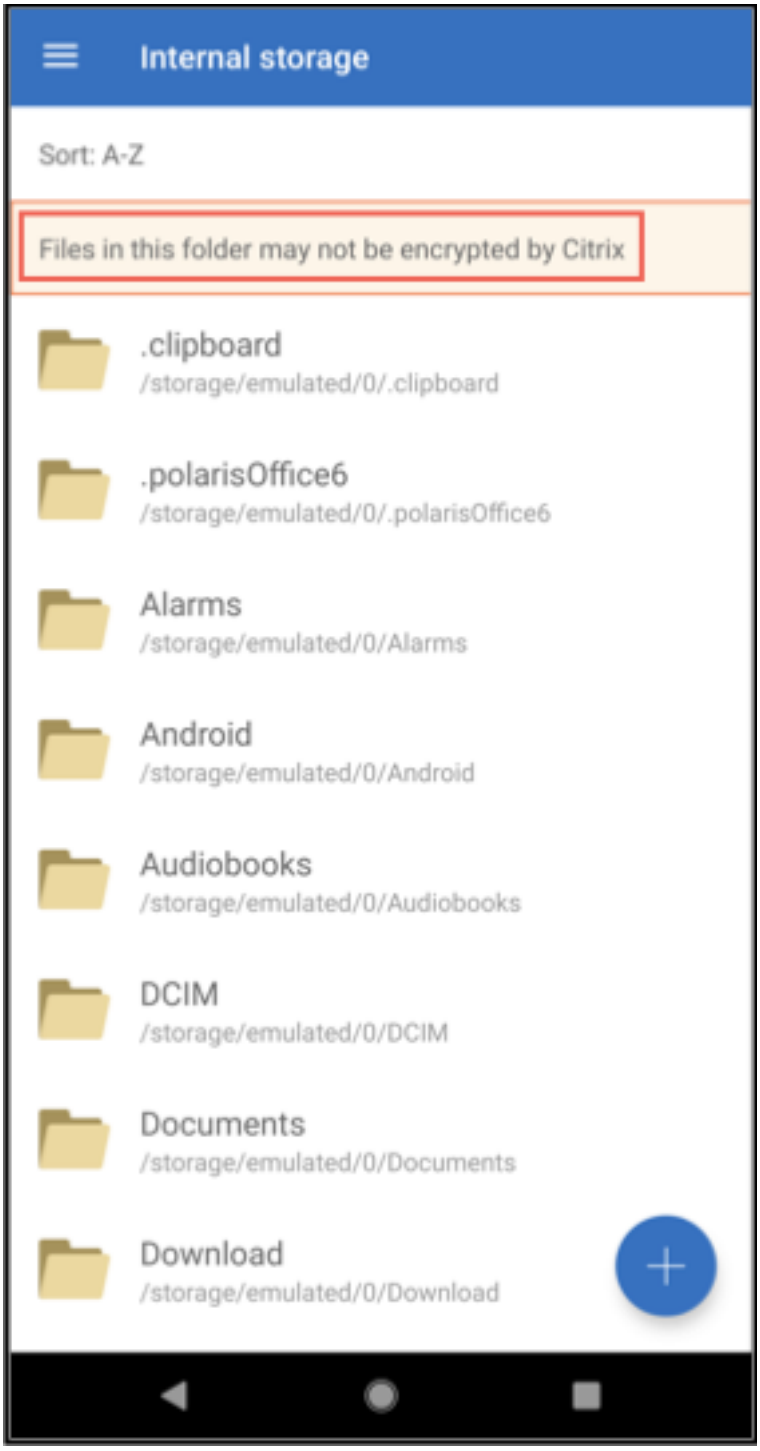
QuickEdit 还与本机邮件程序兼容，以通过附件或 Citrix Files 链接的形式轻松共享或传输文件。

加密

使用 QuickEdit 20.5.0 及更高版本，您可以选择数据加密的类型。为设备平台选择强制合规的平台加密以对数据进行加密。



选择强制合规的平台加密加密类型时，数据将保留在您的设备的 SD 卡上，但不会加密 SD 卡中存在的文件。您会在设备上收到以下警告：



对存储在云存储库中的文件的唯一影响是数据加密类型发生变化。

受支持的文件类型

- Microsoft Word - .doc 和.docx
- Microsoft Excel - .xls 和.xlsx
- Microsoft PowerPoint - .ppt 和.pptx
- .csv、.txt
- .jpeg、.png、.png、.svg、.bmp

截至最新版本已弃用以下文件类型：.docm、.xlsm、.pptm 和.rft。

集成并交付 **QuickEdit**

要将 QuickEdit 与 Endpoint Management 进行集成并交付，请按照以下常规步骤进行操作：

1. 可以选择启用从 Secure Hub 进行 SSO。为此，请在 Endpoint Management 中配置 Citrix Files 帐户信息，以将 Endpoint Management 用作 Citrix Files 的 SAML 身份提供程序。

   在 Endpoint Management 中配置 Citrix Files 帐户信息是用于所有 Endpoint Management 客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端的一次性设置。有关详细信息，请参阅集成并交付 Citrix Files 客户端。

2. 下载 QuickEdit。

   - 可以从 Endpoint Management 下载页面下载 QuickEdit。
   - 对于新用户，也可以在 Citrix Workspace 平台上使用 QuickEdit。有关详细信息，请参阅Citrix Workspace 平台。

3. 使用与针对其他 MDX 应用程序相同的步骤将 QuickEdit 添加到 Endpoint Management。有关详细信息，请参阅添加应用程序。

上载文件

可以将文件从您的设备上载到云存储库（例如 ShareFile），并在其他设备上对其进行访问。目前我们仅支持适用于 iOS 和 Android 的 QuickeEdit。但是，如果将文件迁移到云存储库，您可以使用设备上的任何其他工具对其进行编辑。

当前版本中已修复的问题和已知问题

下面是最新版本中的已知问题或已修复的问题。

已修复的问题

- 尝试从 QuickEdit for iOS 或 ScanDirect 向 Secure Mail 发送文件时，传输失败。解决方法：在这些应用程序的策略设置中添加以下文件加密排除项：“/tmp/.com.apple.Pasteboard”。（位于版本 6.14 中）

已知问题

- 如果页面大小超过 10000 点（宽度或高度），文档将不会打开，以防止出现潜在的内存错误。
- QuickEdit 不支持数字签名和内联图像。
- 在 iOS 12 设备上的 QuickEdit 中，用户创建文件时，出现“由于内存不足”问题。
- 仅当文件在“编辑”模式下打开并且选择了“批注”选项时，用户才能查看 PDF 文件的批注。
- 如果用户打开的 PDF 文件超过 150 MB，将显示“不支持的文件”错误消息。
- 在适用于 iPad 的 QuickEdit 中，在编辑模式下，键盘不按预期显示。
- 用户无法创建包含多个照片的 PowerPoint (.ppt) 文件。

限制

- 共享设备不支持 QuickEdit。
- 如果您运行的是支持共享设备的旧版 QuicKEdit，并且升级到 QuickEdit for iOS 7.4.0 或更高版本，所有本地托管的文件和文件夹都将丢失。但是，Citrix Files 数据仍不受影响且可访问。

ShareConnect

August 21, 2020

> 重要：
>
> ShareConnect 已于 2020 年 6 月 30 日达到生命周期已结束 (EOL) 状态。有关详细信息，请参阅EOL 和已弃用的应用程序。

借助 ShareConnect，用户可以通过 iPad、Android 平板电脑和 Android 手机安全地连接到其计算机，以访问文件和应用程序。用户可以执行以下操作：

- 处理同时位于其计算机上以及位于已连接并联网的驱动器上的文件。
- 从 ShareConnect 中的目标计算机运行应用程序。
- 进行移动应用程序访问，无需打包其他移动生产力应用程序。
- 在 Citrix Virtual Desktops 上运行 ShareConnect 以实现移动优化的访问。

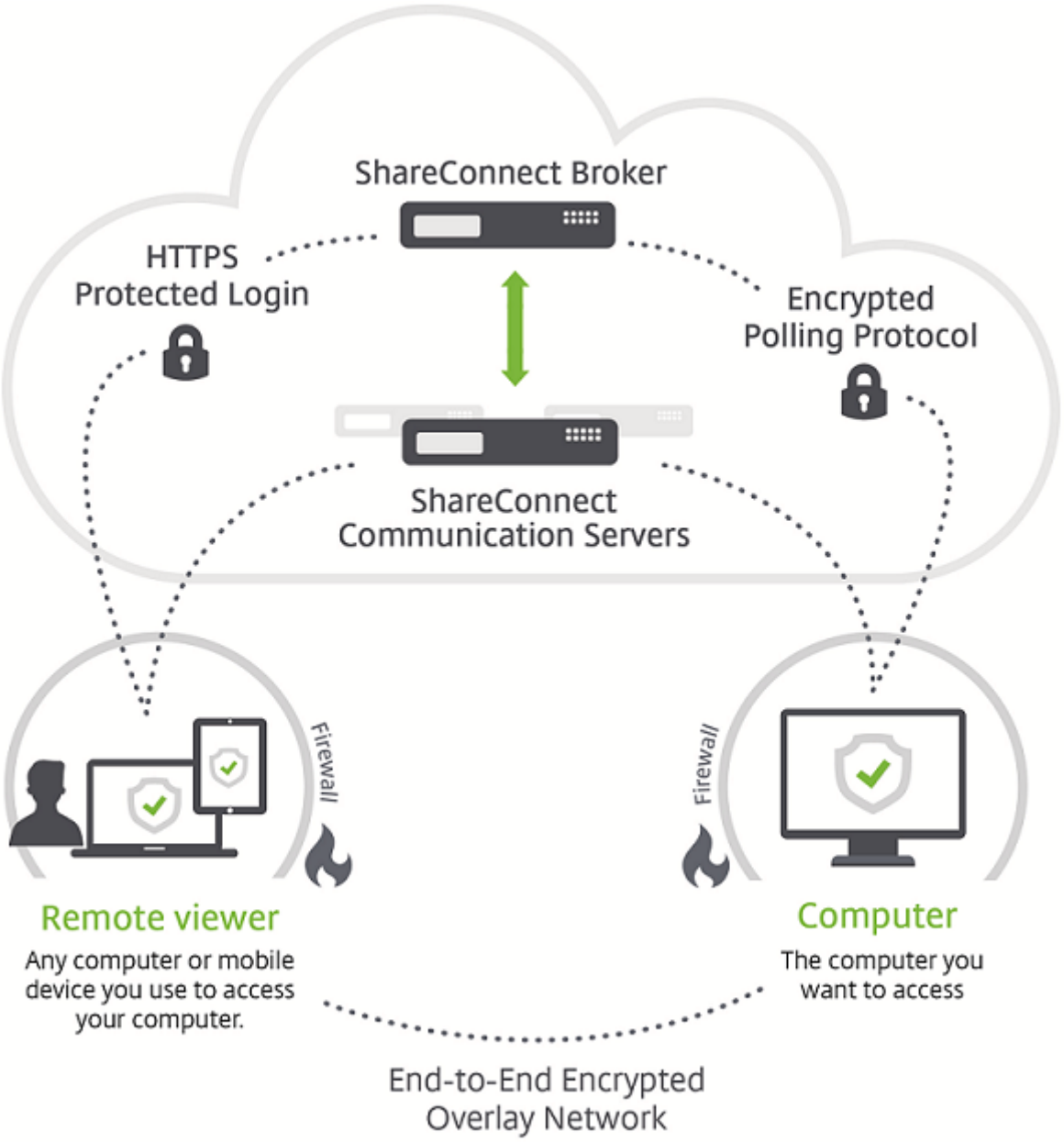
可以从 Endpoint Management 下载页面下载 ShareConnect 的 MDX 版本。

有关如何安装和使用 ShareConnect 的一般信息，请参阅 Citrix 知识中心。

体系结构概述

ShareConnect 组件包括 Citrix 拥有的 ShareConnect Broker 和 ShareConnect Communication Server，如下图所示。ShareConnect Broker 是用于将用户映射到计算机的应用程序服务器和数据库。该应用程序随后告知用户

其主机计算机处于联机还是脱机状态。ShareConnect Communication Server 用于在主机计算机与客户端计算机之间交换数据。根据 **Endpoint Management** 设置，该数据可以通过安全的 Micro VPN 通道在主机计算机与客户端计算机之间传输。



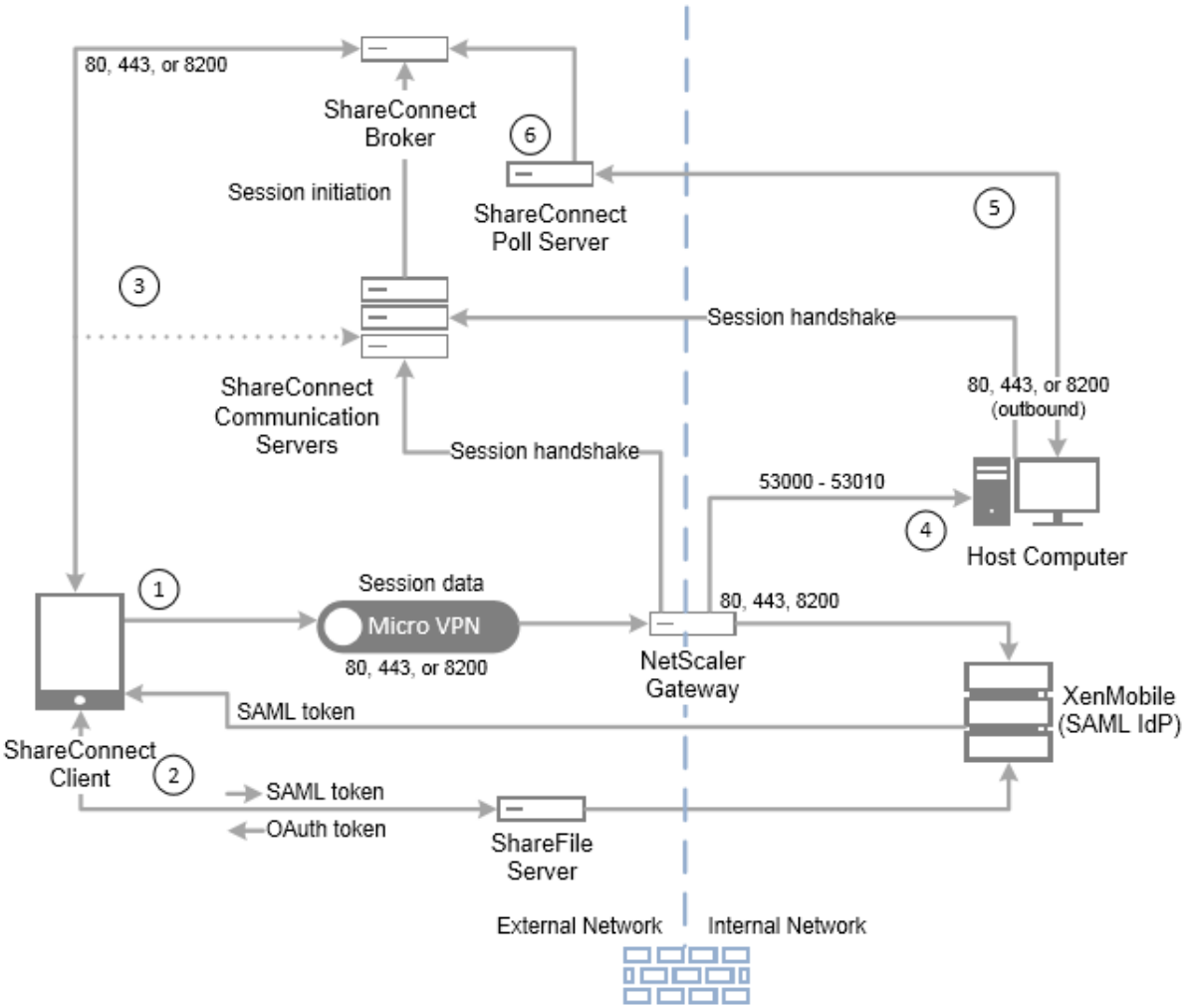
此外，Citrix Files 还可以通过 SAML 身份提供程序 (IdP) 提供通过单点登录 (SSO) 实现的用户身份验证，例如 Endpoint Management 或 Active Directory 联合身份验证服务 (ADFS)。访问网络外部的资源通过 Endpoint Management 部署中的 Citrix Gateway 实现。

连接在 **ShareConnect** 中的工作原理

ShareConnect 建立直接或间接连接：

- 直接连接。如果计算机位于相同的局域网或 Wi-Fi 网络中，ShareConnect 将在客户端计算机与主机计算机之间建立直接连接。在这种情况下，数据直接在客户端计算机与正用于访问主机计算机的移动设备之间传输。数据不通过 ShareConnect Communication Server 传输，因此性能最佳。对于直接连接，Endpoint Management 使用 Citrix Gateway 提供对本地网络外部的资源的安全访问。
- 间接连接。如果无法直接访问计算机，ShareConnect 将在客户端计算机与主机计算机之间建立间接连接。在这种情况下，数据通过 ShareConnect Communication Server 传输。

下图显示了用户从运行使用直接连接的 ShareConnect 的计算机或移动设备访问主机计算机时使用的连接。连接步骤在图下方进行说明。



 在这种情况下，Endpoint Management 配置为用作 Citrix Files 的 SAML IdP，以提供从 Secure Hub 进行 SSO。ShareConnect 从 Secure Hub 请求 SAML 令牌，Secure Hub 转而通过 Citrix Gateway 将请求传递到 Endpoint Management。Endpoint Management 随后将 SAML 令牌发送到 ShareConnect。

 ShareConnect 将 SAML 令牌发送到 Citrix Files 进行验证以及将 SAML 令牌交换成 OAuth 令牌。

 ShareConnect 将 OAuth 令牌发送到 ShareConnect Broker，Broker 随后将会话令牌发送到 ShareConnect。

- ShareConnect 从 ShareConnect Broker 获取主机计算机的列表，并提示输入主计算机的凭据。ShareConnect 随后与 ShareConnect Communication Server 建立直接连接。主机计算机验证凭据后，ShareConnect 将从主机计算机获取文件和应用程序的列表。用户打开某个文件或应用程序后，ShareConnect 与主机计算机之间将建立直接连接。
- 主机计算机上的 ShareConnect 代理将状态消息发送到 ShareConnect Poll Server 以指示其处于联机还是脱机状态。
- ShareConnect Poll Server 将负载平衡的请求从 ShareConnect 代理发送到 ShareConnect Broker，并将主机状态更新发送到 ShareConnect Broker。

ShareConnect 安全性

ShareConnect 使用内置的 128 位 AES 加密，因此，在 ShareConnect 客户端与运行 ShareConnect 代理的主机计算机之间发送的所有数据将从端到端完全加密。加密密钥对每个连接都是唯一的。甚至最复杂的设备也无法拦截解码加密所需的数据。

您通常配置 ShareConnect，以便数据在 ShareConnect 客户端与主机计算机之间直接路由。除非您将“网络访问”策略配置为无限制访问，否则，数据将不通过 ShareConnect 通信服务器路由。有关策略的详细信息，请参阅本文中的“将 ShareConnect 添加到 Endpoint Management”。

对于直接或间接连接，加密的元数据（例如，建立连接所需的 IP 地址和端口）将发送到 ShareConnect 服务器。

此外，ShareConnect 的 MDX 封装通过 MDX Vault 提供数据加密。Vault 加密 MDX 封装的应用程序以及 iOS（iOS 9 之前）和 Android 设备上存储的关联数据。加密使用 OpenSSL 提供的 FIPS 认证加密模块进行。

有关安全设置和管理控制的信息，请参阅下面的安全白皮书。

ShareConnect 安全白皮书

ShareConnect 管理员指南

ShareConnect 的端口要求

打开以下端口以允许 ShareConnect 通信。端口要求因连接类型而异。如果计算机位于相同的局域网或 Wi-Fi 网络中，连接可以是直接连接。或者，如果客户端和主机计算机无法直接相互连接，连接可以是间接连接。

对于直接连接

TCP 端口 80 - 用于从 Citrix Gateway 到 app.shareconnect.com 的出站连接。

源 - Citrix Gateway

目标 - app.shareconnect.com

TCP 端口 80、443、8200 - 对于从 Citrix Gateway 到 ShareConnect Communication Server 的出站连接，至少需要打开其中一个端口。

源 - Citrix Gateway

目标 - ShareConnect Communication Server

TCP 端口 80、443、8200 - 用于从 ShareConnect 主机计算机到 Citrix 服务器的出站连接。

源 - ShareConnect 主机计算机

目标 - poll.shareconnect.com、ShareConnect Communication Server

TCP 端口 443 - 用于从 Citrix Gateway 到所需站点的出站连接。

源 - Citrix Gateway

目标 - crashlytics.com、secure.sharefile.com、ShareFile_sub-domain.sharefile.com

TCP 端口 53000 - 53010 - 用于从 Citrix Gateway 到 ShareConnect 主机计算机的出站连接。

源 - Citrix Gateway

目标 - 基于局域网的 ShareConnect 主机计算机

TCP 端口 53000 - 53010 - 用于从 Citrix Gateway 到 ShareConnect 主机计算机的入站连接。

源 - Citrix Gateway

目标 - 基于局域网的 ShareConnect 主机计算机

对于间接连接

TCP 端口 80 - 用于从 ShareConnect 代理到 app.shareconnect.com 的出站连接。

源 - ShareConnect 代理

目标 - app.shareconnect.com

TCP 端口 80、443、8200 - 对于从 ShareConnect 代理到 ShareConnect Communication Server 的出站连接，至少需要打开其中一个端口。

源 - ShareConnect 代理

目标 - ShareConnect Communication Server

TCP 端口 80、443、8200 - 用于从 ShareConnect 主机计算机到 Citrix 服务器的出站连接。

源 - ShareConnect 主机计算机

目标 - poll.shareconnect.com、ShareConnect Communication Server

TCP 端口 443 - 用于从 ShareConnect 代理到所需站点的出站连接。

源 - ShareConnect 代理

目标 - crashlytics.com、secure.sharefile.com、ShareFile_sub-domain.sharefile.com

集成和交付 **ShareConnect**

要将 ShareConnect 与 Endpoint Management 进行集成并交付，请按照以下常规步骤进行操作：

1. 可以选择启用从 Secure Hub 进行 SSO。为此，请在 Endpoint Management 中配置 Citrix Files 帐户信息，以将 Endpoint Management 用作 Citrix Files 的 SAML IdP。

   在 Endpoint Management 中配置 Citrix Files 帐户信息属于一次性设置。一次性设置用于所有移动生产力应用程序客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端。

2. 下载并打包 ShareConnect。有关详细信息，请参阅关于 MDX Toolkit。
3. 将 ShareConnect 添加到 Endpoint Management 并配置 MDX 策略。
4. 在主机计算机上安装 ShareConnect 代理。ShareConnect 代理是一个 MSI 软件包。因此，您可以使用现有软件部署方法分发和安装该代理。用户必须在安装完成后的一小时内使用其 Citrix Files 凭据登录代理，注册主机计算机。

   或者，用户可以在要通过 ShareConnect 连接到的计算机上安装 ShareConnect 代理。有关详细信息，请参阅文本中的 “在计算机上安装 ShareConnect 代理”。

将 **ShareConnect** 添加到 **Endpoint Management**

请使用与针对其他 MDX 应用程序相同的步骤将 ShareConnect 添加到 Endpoint Management。有关详细信息，请参阅添加 MDX 应用程序。添加 ShareConnect 时，请为其配置 MDX 策略，如下表所示。

策略	值	结果
网络访问	通过通道连接到内部网络或不限制	通过通道连接到内部网络对所有网络访问使用返回到内部网络的 PerApp VPN 通道。此配置在 ShareConnect 与主机计算机之间提供直接连接。不限制使用 Citrix 拥有的 Communication Server 在主机计算机与 ShareConnect 代理之间路由加密数据。请务必使用无限制访问权限测试您的设置，以确保一切正常，即使您计划使用通过通道连接到内部网络进行网络访问也是如此。
首选 VPN 模式	安全浏览	为需要执行 SSO 的连接恰当地设置初始连接模式。
启用加密	开	加密平板电脑上存储的数据。

策略	值	结果
剪切和复制	不限制	为 ShareConnect 启用剪切和复制操作。
粘贴	不限制	为 ShareConnect 启用粘贴操作。
文档交换 (打开方式)	不限制	允许用户从 ShareConnect 中打开已连接的计算机上或已连接的网络驱动器上的任何文件。
保存密码	关	要求用户在每次登录 ShareConnect 时输入其计算机的用户名和密码。

在计算机上安装 **ShareConnect** 代理

以下步骤介绍了用户如何在要从受支持的移动设备连接到的每台物理机或虚拟机上安装 ShareConnect 代理。

在执行这些步骤之前，用户必须先安装 Secure Hub。然后再按照提示进行操作以允许在受支持的移动设备上安装移动生产力应用程序。

1. 在平板电脑上登录 Secure Hub。
2. 打开 ShareConnect。
3. 轻按 Email download link（使用电子邮件发送下载链接）。

   Citrix 将从 no-reply@shareconnect.com 向您发送一封电子邮件。
4. 在要从 ShareConnect 访问的主机计算机上打开该电子邮件。
5. 在该电子邮件，单击 Set up this computer（设置此计算机）。
6. 双击 **ShareConnect_Installer.exe** 开始安装。

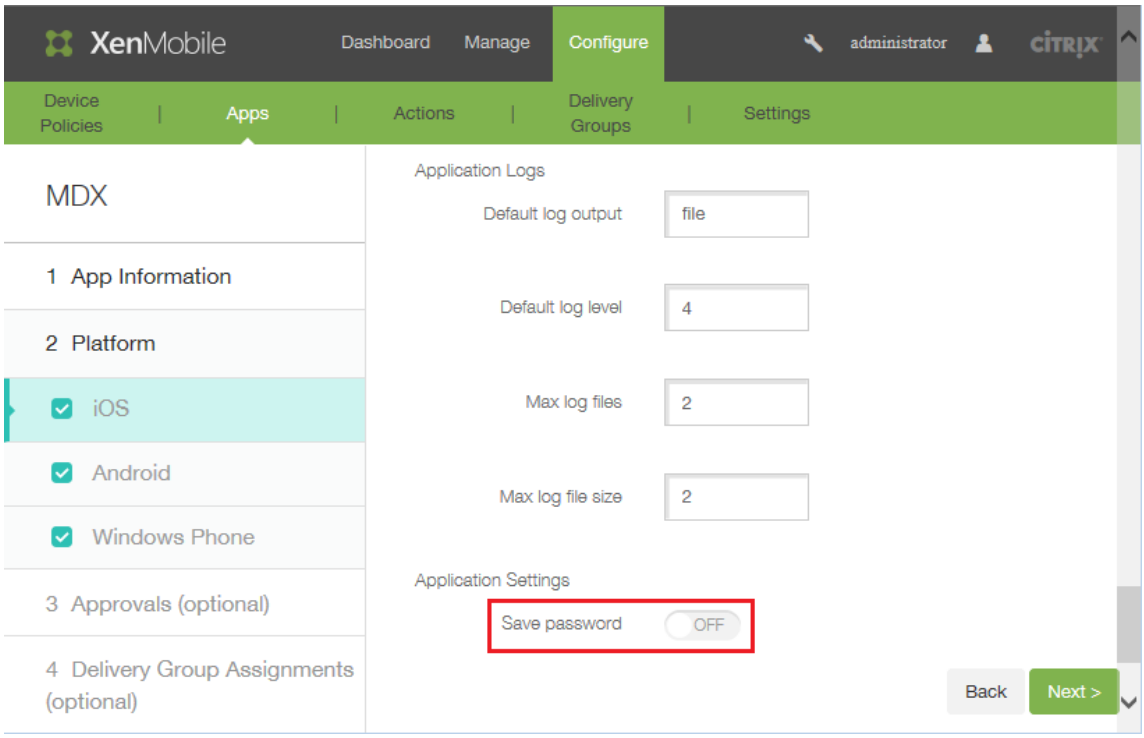
   ShareConnect 代理将安装在您的主机计算机上。安装过程中，ShareConnect 会提示输入电子邮件地址（如果配置了 Citrix Files SSO）。或者，ShareConnect 会提示输入 Citrix Files 凭据（如果未配置 Citrix Files SSO）。
7. 按照 ShareConnect 和入门向导中提供的说明进行操作。

ShareConnect 代理随后将注册主机计算机。主机计算机可以从 ShareConnect 客户端进行连接，前提是主机计算机已打开电源，并且能够在一个已发布的端口（80、443 或 8200）上访问 poll.shareconnect.com。

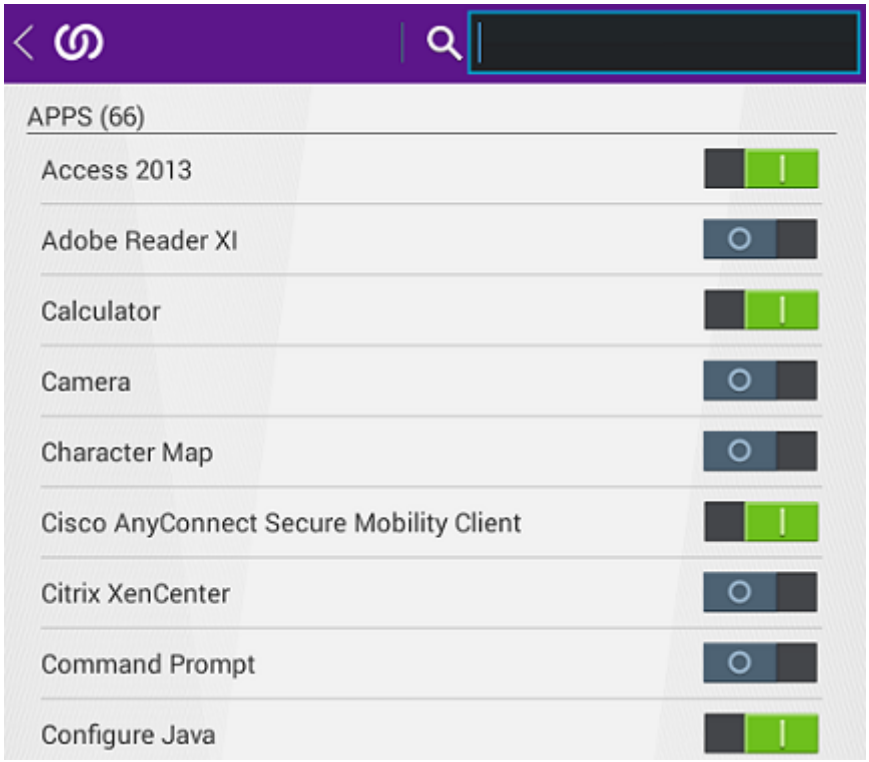
ShareConnect 功能

- 添加主机计算机。使用 ShareConnect，用户可以从受支持的移动设备添加和连接到远程主机计算机。

- 访问文件。用户可以查看最近打开的文件列表，浏览并搜索其主机计算机和已连接的驱动器上的文件。
- 编辑文件。在平板电脑中，用户可以访问主机计算机上的桌面应用程序以编辑文件。用户可以在全屏模式下使用应用程序。
- 屏幕共享。用户可以使用屏幕共享功能查看其主机计算机的桌面，而非仅查看单个文件或应用程序。
- **Citrix Files** 集成。用户可以在主机计算机与 Citrix Files 之间移动或共享文件。
- 主机和键盘。ShareConnect 支持同时使用蓝牙键盘和 Citrix XI Prototype 鼠标。
- 端口受到限制。ShareConnect 仅使用端口 53000 到 53010。
- 每次登录时强制输入密码。为增强安全性，可以配置此选项以要求用户在每次登录 ShareConnect 时输入计算机密码。如果禁用了“保存密码”策略（如下图所示），系统将强制用户在每次连接时都输入其登录凭据。



- 添加或删除应用程序。用户可以通过切换每个应用程序旁边的开关以选择或取消选择该应用程序，从而在 ShareConnect 的应用程序托盘中添加或删除应用程序。



- 缓存预览的文件。ShareConnect 缓存已访问的文件，以便在用户预览其他文件后返回较早预览的文件时不会再次下载文件。此功能缩短了用户后续访问文件时的加载时间。

ShareConnect 故障排除

ShareConnect 代理安装问题

问题	说明和解决办法
如果用户下载了 ShareConnect 代理，但等待一小时或更长时间后开始安装，则必须输入其 Citrix Files 帐户名称和密码，才能注册 ShareConnect 代理。	ShareConnect 代理安装程序包括一个在下载一小时后过期的令牌。如果用户在令牌过期之前未启动安装，则必须登录其 Citrix Files 帐户两次，第一次为注册 ShareConnect 代理，然后在安装完成后登录该代理。如果用户在一小时内下载并安装 ShareConnect 代理，系统仅提示用户登录一次。
注册 ShareConnect 代理过程中，该代理不连接并显示错误消息，例如 “Please check your connection and try again”（请检查您的连接并重试）。	请确认 poll.shareconnect.com 的端口未被阻止。有关详细信息，请参阅上文中的 “系统要求”。

ShareConnect 连接问题

> 重要：
>
> 我们建议您将“网络访问”策略设置为不限制以排除端口和网络设置问题，以便测试 ShareConnect。不限制访问将强制 ShareConnect 通过 ShareConnect Communication Server 进行连接，在 ShareConnect 移动设备和主机计算机具有 Internet 连接时，这样通常使您能够测试连接。

问题	说明和解决办法
ShareConnect 启动，但不连接到主机计算机，也不提示输入凭据。	验证设置是否满足上文“系统要求”下详述的端口要求。
用户无法使用其 Citrix Files 帐户凭据登录 ShareConnect。	通过 SSO 登录 ShareConnect 要求为您的 Citrix Files 帐户配置 SAML IdP。有关将 Endpoint Management 用作 SAML IdP 的详细信息，请参阅适用于 Endpoint Management 的 Citrix Content Collaboration。有关配置其他 IdP 的详细信息，请参阅此知识中心文章。如果没有为您的帐户配置 SSO，ShareConnect for iOS 将提示输入用户的 Citrix Files 用户名和密码。
用户登录到 ShareConnect 后，ShareConnect 将无法连接到主机计算机。	将 ShareConnect 配置为直接连接（即，将“网络访问”策略设置为“通过通道连接到内部网络”）后，如果网络设置（例如，防火墙阻止）或配置的代理服务器中存在限制，连接可能会失败。

Citrix ShareFile Workflows

October 18, 2018

> 注意：
>
> Secure Forms 已于 2018 年 3 月 31 日达到生命周期结束 (EOL)。我们建议您使用 Citrix Files Platinum 和 Premium 帐户随附的 ShareFile WorkFlows。

ShareFile Workflows 是 Citrix Files 自定义工作流功能的移动组件。此功能允许用户创建包含多个触发器和操作的自定义工作流。可以将自定义表单添加到工作流模板并分配给用户。

向某个用户分配了表单时，该用户可以通过 ShareFile Workflows 移动应用程序完成并提交该表单。表单数据存储与 Citrix Files 安全地集成，工作流文件存储在其中以便用户查看、参考和检索。

工作流和表单模板在 Citrix Files Web 应用程序内部创建和管理。

用户文档

可以在 Citrix 知识中心中查找与创建和管理工作流和表单模板有关的用户文档：

- 创建工作流模板
- 创建表单模板
- 通过 Workflows 移动应用程序提交表单

适用于 **Endpoint Management** 的 **Citrix Content Collaboration**

March 26, 2021

适用于 Endpoint Management 的 Citrix Content Collaboration 客户端是支持 MDX 版本的 Citrix Files 移动客户端。通过这些客户端，用户可以安全地集中访问 MDX 打包的其他应用程序中的数据。适用于 Endpoint Management 的 Citrix Content Collaboration 客户端还可以从 MDX 功能中受益，例如 Micro VPN、通过 Secure Hub 实现的单点登录 (SSO) 以及双重身份验证。

Citrix Files 是企业文件同步和共享服务，用户可以通过其轻松安全地交换文档。Citrix Files 向用户提供各种访问方案，包括 Citrix Files 移动客户端（例如 Citrix Files for Android Phone 和 Citrix Files for iPad）。

您可以将 Citrix Files 与 Endpoint Management 集成，以提供完整的 Citrix Files 功能集或仅提供对存储区域连接器的访问权限。默认情况下，Citrix Endpoint Management 控制台仅支持对 Citrix Files 进行配置。要配置 Endpoint Management 以与存储区域连接器结合使用，请参阅 Citrix Endpoint Management 文档中的将 Citrix Content Collaboration 与 Endpoint Management 结合使用。

可按如下所示使用 Endpoint Management、Citrix Files、存储区域控制器和 Citrix ADC 来部署和管理适用于 Endpoint Management 的 Citrix Content Collaboration 客户端：

- 在 Endpoint Management 中配置了 Citrix Files 时，Endpoint Management 用作 SAML 身份提供程序 (IdP)，并部署适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。Citrix Files 负责管理 Citrix Files 数据。Citrix Files 数据不通过 Endpoint Management 传输。
- 在 Endpoint Management 中配置了 Citrix Files 或存储区域连接器时，存储区域控制器将提供与网络共享和 SharePoint 中的数据的连接。用户将通过 Citrix Files 移动生产力应用程序访问您存储的数据。用户还可以从移动设备编辑 Microsoft Office 文档、预览和批注 Adobe PDF 文件。
- Citrix ADC 负责管理来自外部用户的请求、保护连接安全、对请求进行负载平衡以及处理存储区域连接器的内容交换。

要下载适用于 Endpoint Management 的 Citrix Content Collaboration 客户端，请参阅 Citrix.com 下载。

有关适用于 Endpoint Management 的 Citrix Content Collaboration 及其他移动生产力应用程序的系统要求，请参阅支持移动生产力应用程序。

适用于 **Endpoint Management** 的 **Citrix Content Collaboration** 客户端与 **Citrix Files** 移动客户端的区别

下面介绍了适用于 Endpoint Management 的 Citrix Content Collaboration 客户端与 Citrix Files 移动客户端之间的差别。

用户访问

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

用户从 Secure Hub 获取并打开适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。

Citrix Files 移动客户端：

用户从应用商店获取 Citrix Files 移动客户端。

SSO

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

对于 Endpoint Management 与 Citrix Files 的集成：您可以将 Endpoint Management 配置为 Citrix Files 的 SAML IdP。在此配置中，Secure Hub 将 Endpoint Management 用作 SAML IdP，为适用于 Endpoint Management 的 Citrix Content Collaboration 客户端获取 SAML 令牌。如果用户启动了适用于 Endpoint Management 的 Citrix Content Collaboration 客户端，但未登录 Secure Hub，系统会提示其登录 Secure Hub。该用户不需要知晓其 Citrix Files 域或帐户配置。

Citrix Files 移动客户端：

您可以将 Endpoint Management 和 Citrix Gateway 配置为 Citrix Files 的 SAML IdP。在此配置中，使用 Web 浏览器或其他 Citrix Files 客户端登录 Citrix Files 的用户将被重定向到 Endpoint Management 环境以进行用户身份验证。成功通过 Endpoint Management 进行身份验证后，用户将收到用于登录其 Citrix Files 帐户的有效 SAML 令牌。

Micro VPN

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

远程用户可以通过 Citrix Gateway 使用 VPN 或 Micro VPN 连接进行连接，以访问内部网络中的应用程序和桌面。此功能（通过 Citrix ADC 与 Endpoint Management 的集成提供）对用户不可见。

Citrix Files 移动客户端：

不适用。

双重身份验证

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

Citrix ADC 与 Endpoint Management 的集成还支持使用客户端证书身份验证和其他身份验证类型的组合（例如 LDAP 或 RADIUS）进行身份验证。

Citrix Files 移动客户端：

不适用。

文件夹权限

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端和 *Citrix Files* 移动客户端：

对于 Endpoint Management 与 Citrix Files 的集成：由 Citrix Files 确定。

文档访问保护

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

用户可以打开在 Secure Mail 中接收的附件或通过 MDX 打包的任何应用程序下载的附件。用户执行“打开方式”操作时，仅显示 MDX 打包的应用程序。适用于 Endpoint Management 的 Citrix Content Collaboration 客户端无法获取未打包的应用程序中的数据。Secure Mail 用户可以附加 Citrix Files 存储库中的文件，而不需要将文件下载到设备。如果用户的设备上安装了打包的和未打包的 Citrix Files，打包的 Citrix Files 客户端将无法访问用户的个人 Citrix Files 帐户中的文件。打包的 Citrix Files 客户端只能访问 Endpoint Management 中配置的 Citrix Files 子域。

Citrix Files 移动客户端：

用户可以从任何应用程序打开附件。

Citrix Files 帐户访问

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

对于 Endpoint Management 与 Citrix Files 的集成：要访问个人 Citrix Files 帐户或第三方 Citrix Files 帐户，用户必须在该设备上使用非 MDX 版本的 Citrix Files。

Citrix Files 移动客户端：

对于 Endpoint Management 与 Citrix Files 的集成：可从 Citrix Files 客户端获取。

设备策略

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端和 *Citrix Files* 移动客户端：

Endpoint Management 和 Citrix Files 设备策略都适用于适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。例如，您可以从 Endpoint Management 控制台执行设备擦除。您可以从 Citrix Files 控制台远程擦除 Citrix Files 应用程序。

MDX 策略

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

通过 MDX 策略，您可以在 Citrix Endpoint Management 中配置 Endpoint Management 应用商店强制执行的设置。只能通过 MDX 执行的策略包括阻止相机、麦克风、电子邮件编写、屏幕捕获以及剪贴板剪切、复制和剪贴操作的功能。

Citrix Files 移动客户端：

不适用。

数据加密

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端和 *Citrix Files* 移动客户端：

使用 AES-256 加密存储的所有数据，通过 SSL 3.0 以及最低 128 位加密保护正在传输的数据。

可用性

适用于 *Endpoint Management* 的 *Citrix Content Collaboration* 客户端：

适用于 Endpoint Management 的 Citrix Content Collaboration 客户端随附在 Endpoint Management Advanced Edition 和 Enterprise Edition 中。

Citrix Files 移动客户端：

所有 Endpoint Management 版本都包含 Citrix Files 功能。可以将 Endpoint Management 与完整的 Citrix Files 功能集集成，或仅与存储区域连接器集成。

集成并交付适用于 **Endpoint Management** 的 **Citrix Content Collaboration** 客户端

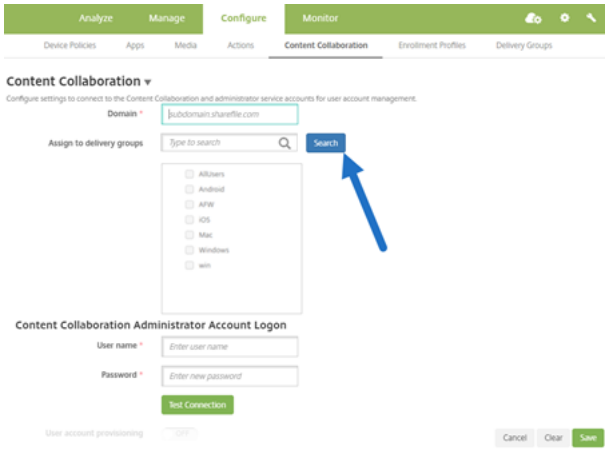
要集成并交付适用于 Endpoint Management 的 Citrix Content Collaboration 客户端，请按照以下常规步骤进行操作：

1. 将 Endpoint Management 用作 Citrix Files 的 SAML IdP，以提供从 Citrix Files 客户端到 Citrix Files 的 SSO。为此，必须在 Endpoint Management 中配置 Citrix Files 帐户信息。有关详细信息，请参阅“在 Endpoint Management 中配置 Citrix Files 帐户信息以用于 SSO”部分。

   > 重要：
   >
   > 要将 Endpoint Management 用作非 MDX Citrix Files 客户端（例如 Citrix Files Web 应用程序和

> Citrix Files Sync 客户端）的 SAML IdP，需要进行额外的配置。有关详细信息，请参阅 Citrix Files 支持站点上的文章
>
> Citrix Files (ShareFile) Single Sign-On SSO。本文包含指向 Endpoint Management 配置指南的下载链接。

2. 下载 Citrix Files 客户端。
3. 将 Citrix Files 客户端添加到 Endpoint Management。有关详细信息，请参阅本文中后面的 “将 Citrix Files 客户端添加到 Endpoint Management”。
4. 验证您的配置。有关详细信息，请参阅本文中后面的 “验证 Citrix Files 客户端”。



关于设置：

- 域是指要用于客户端的 Citrix Files 子域。
- 只有选定 DG 中的用户才能从客户端通过 SSO 访问 Citrix Files。

  如果 DG 中的用户没有 Citrix Files 帐户，则当您将 Citrix Files 客户端添加到 Endpoint Management 时，Endpoint Management 将用户预配到 Citrix Files 中。
- Endpoint Management 使用 Citrix Files 管理员帐户登录信息在 Citrix Files 控制平面中保存 SAML 设置。

> 重要：
>
> 允许从 Citrix Files 客户端通过 SSO 登录 Citrix Files 的配置不对访问网络共享或 SharePoint 文档库的用户进行身份验证。访问这些连接器数据源需要通过身份验证，才能连接到网络共享或 SharePoint 服务器所在的 Active Directory 域。

在 **Endpoint Management** 中配置 **Citrix Files** 帐户信息以用于 **SSO**

要启用从 Secure Hub 到移动生产力应用程序的 SSO，请在 Endpoint Management 控制台中指定 Citrix Files 帐户和 Citrix Files 管理员服务帐户信息。使用该配置后，Endpoint Management 将用作 Citrix Files、移动生产力应用程序客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端的 SAML IdP。用户启动移动生产力应用程序客户端时，Secure Hub 将从 Endpoint Management 获取用户的 SAML 令牌，并将其发送到 Citrix Files 客户端。

在 Endpoint Management 控制台中，单击配置 > **Content Collaboration**（这是 Citrix Files 的以前的名称）。

将适用于 **Endpoint Management** 的 **Citrix Content Collaboration** 客户端添加到 **Endpoint Management**

将适用于 Endpoint Management 的 Citrix Content Collaboration 客户端添加到 Endpoint Management 时，可以启用从适用于 Endpoint Management 的 Citrix Content Collaboration 客户端对 Connector 数据源的 SSO 访问。为此，请按本部分中所述配置“网络访问”策略和“首选 VPN 模式”策略。

必备条件

- Endpoint Management 必须能够访问您的 Citrix Files 子域。要测试连接，请从 Endpoint Management 服务器 ping 您的 Citrix Files 子域。
- 为 Citrix Files 帐户以及运行 Endpoint Management 的虚拟机管理程序配置的时区必须相同。如果时区不同，SSO 请求可能会失败，因为 SAML 令牌可能无法在预期期限内到达 Citrix Files。要为 Endpoint Management 配置 NTP 服务器，请使用 Endpoint Management 命令行接口。

  > 注意：
  >
  > Hyper-V 主机将 Linux VM 上的时间设置为本地时区，而非设置为 UTC。

- 以管理员身份登录 ShareFile 帐户并验证设置 > 管理员设置 > 安全 > 登录和安全策略 > 单点登录**/SAML 2.0** 配置中的 SAML SSO 设置。
- 下载适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。

步骤：

1. 在 Endpoint Management 控制台中，单击配置 **>** 应用程序，然后单击添加。
2. 单击 **MDX**。
3. 输入应用程序的名称并（可选）输入说明和应用程序类别。
4. 单击下一步，然后上载适用于 Endpoint Management 的 Citrix Content Collaboration 客户端的.mdx 文件。
5. 单击下一步配置应用程序信息和策略。

   允许从适用于 Endpoint Management 的 Citrix Content Collaboration 客户端通过 SSO 登录 Citrix Files 的配置不对访问网络共享或 SharePoint 文档库的用户进行身份验证。
6. 要在 Secure Hub Micro VPN 与存储区域控制器之间启用 SSO，请完成以下策略配置：
   - 将网络访问策略设置为通过通道连接到内部网络。

     在此模式下，MDX 框架将拦截来自适用于 Endpoint Management 的 Citrix Content Collaboration 客户端的所有网络流量。然后使用应用程序特定的 Micro VPN 通过 Citrix Gateway 重定向网络流量。

- 将“首选 VPN 模式”策略设置为安全浏览。

  在此通道模式下，MDX 框架将终止来自 MDX 应用程序的 SSL/HTTP 流量，MDX 框架随后将代表用户启动与内部网络的新连接。此策略设置允许 MDX 框架检测和响应 Web 服务器发出的身份验证质询。

7. 根据需要完成审批和交付组 (DG) 分配。

只有选定 DG 中的用户才能从适用于 Endpoint Management 的 Citrix Content Collaboration 客户端通过 SSO 访问 Citrix Files。如果 DG 中的用户没有 Citrix Files 帐户，则当您将适用于 Endpoint Management 的 Citrix Content Collaboration 客户端添加到 Endpoint Management 时，Endpoint Management 将用户预配到 Citrix Files 中。

验证适用于 **Endpoint Management** 的 **Citrix Content Collaboration** 客户端

1. 完成本文中介绍的配置后，启动适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。Citrix Files 不提示您登录。
2. 在 Secure Mail 中，编写电子邮件并从 Citrix Files 添加附件。您的 Citrix Files 主页将打开，但不提示您登录。

EOL 和已弃用的应用程序

November 16, 2021

以下应用程序已达到生命周期结束或达到 EOL 状态。当产品版本达到 EOL 时，您可以根据产品许可协议的条款使用该产品，但可用的支持选项将受到限制。历史信息在知识中心或其他联机资源中显示。文档不再更新，并且按原样提供。有关产品生命周期里程碑的详细信息，请参阅 Product Matrix（产品列表）。

> 注意：
> 有关正在逐步淘汰的 Citrix Endpoint Management 功能的高级通知，请参阅弃用。

Citrix Files for Intune：已于 2020 年 12 月 31 日弃用。

我们鼓励您探索利用平台功能的选项，以便通过 Android Enterprise（具有工作配置文件）和 iOS 用户注册对常规 Citrix Files 应用程序（在应用商店中提供）进行容器化。

Secure Notes： EOL 生命周期日期为 2018 年 12 月 31 日。

如果您需要使用 Secure Notes 和 Secure Tasks 的功能，建议使用 Notate for Citrix，这是可以使用 MDX 策略保护的第三方应用程序。

如果 Secure Notes 和 Secure Tasks 用户在 Outlook 中存储了数据，他们可以在 Notate 中访问这些数据。如果用户在 ShareFile（现已更名为 Citrix Files）中存储了数据，则这些数据未迁移。

用户可以在 EOL 日期之后继续运行 Secure Notes，直到其平台操作系统不再支持用户界面为止。但是，我们不建议使用不受支持的产品。

Secure Tasks： EOL 生命周期日期为 2018 年 12 月 31 日。

Secure Forms：EOL 生命周期日期为 2018 年 3 月 31 日。我们鼓励客户转换到 Citrix Files Platinum 和 Premium 帐户附带的 Citrix ShareFile Workflows。有关详细信息，请参阅 Citrix ShareFile Workflows。

ScanDirect： ScanDirect 已于 2018 年 9 月 1 日达到 EOL。

ShareConnect： ShareConnect 已于 2020 年 6 月 30 日达到 EOL 状态。

允许与 **Office 365** 应用程序的安全交互

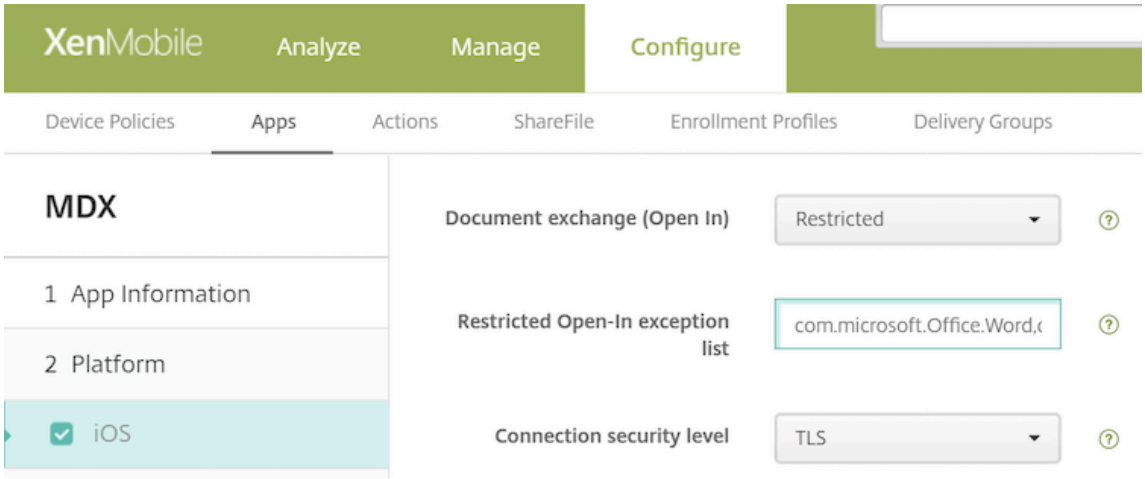
August 21, 2020

Citrix Secure Mail、Citrix Secure Web 和 Citrix Files 提供用于打开 MDX 容器的选项以允许用户向 Microsoft Office 365 应用程序传输文档和数据。可以在 Endpoint Management 控制台上通过 “打开方式” 策略为 iOS 和 Android 平台管理此功能。

在 Microsoft 应用程序中打开后，数据在 MDX 容器中将不再受保护或被加密。启用此功能之前，请注意安全隐患。特别是，关注数据丢失防护的客户或者需要遵守 HIPAA 或其他严格的合规要求的客户应权衡打开容器的得失。

在 **iOS** 中启用 **Office 365**

1. 从 Endpoint Management 下载页面下载最新版本的 Secure Mail、Secure Web 或 Citrix Files 应用程序。
2. 将文件上载到 Endpoint Management 控制台。
3. 找到文档交换 **(**打开方式**)** 策略并将其设置为限制。在受限制的打开方式例外列表中，Microsoft Word、Excel、PowerPoint、OneNote 和 Outlook 自动列出。例如：com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



在 MDM 注册中，提供了适用于 iOS 设备的更多控件。

您可以将 iTunes 应用程序上载到 Endpoint Management 控制台并将这些应用程序推送到设备。如果选择此选项，请将以下策略设置为开：

- 删除 MDM 配置文件时也删除应用程序
- 阻止备份应用程序数据
- 强制管理应用程序（请注意，选择性擦除将删除应用程序及所有数据）

要阻止文档和数据从 Microsoft 应用程序传输到设备上的非托管应用程序，请在 Endpoint Management 控制台上转至配置 **>** 设备 **>** 限制 **> iOS**，然后将在非托管应用程序中使用托管应用程序中的文档和在托管应用程序中使用非托管应用程序中的文档设置为关。

在 **Android** 中启用 **Office 365**

1. 从 Endpoint Management 下载页面下载最新版本的 Secure Mail、Secure Web 或 Citrix Files 应用程序。
2. 将文件上载到 Endpoint Management 控制台。
3. 向下滚动到文档交换 **(**打开方式**)** 策略，然后选择限制。
4. 在受限制的打开方式例外列表中，添加以下软件包 ID：

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.office.
   powerpoint } { package=com.microsoft.office.excel }
   ```

5. 正常配置其他应用程序策略并保存应用程序。

用户必须将来自 Secure Mail、Secure Web 或 Citrix Files 的文件保存在其设备上，并使用 Office 365 应用程序打开这些文件。

对于 iOS 和 Android，用户可以在其设备上打开并编辑以下类型的文件：

支持的文件格式

有关受支持的文件格式，请参阅 Microsoft Office 文档。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States