



Secure Hub

Contents

Citrix Secure Hub	3
已知问题和已修复的问题	28
身份验证提示情景	30
使用派生凭据注册设备	34

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](https://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，以使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](#)。

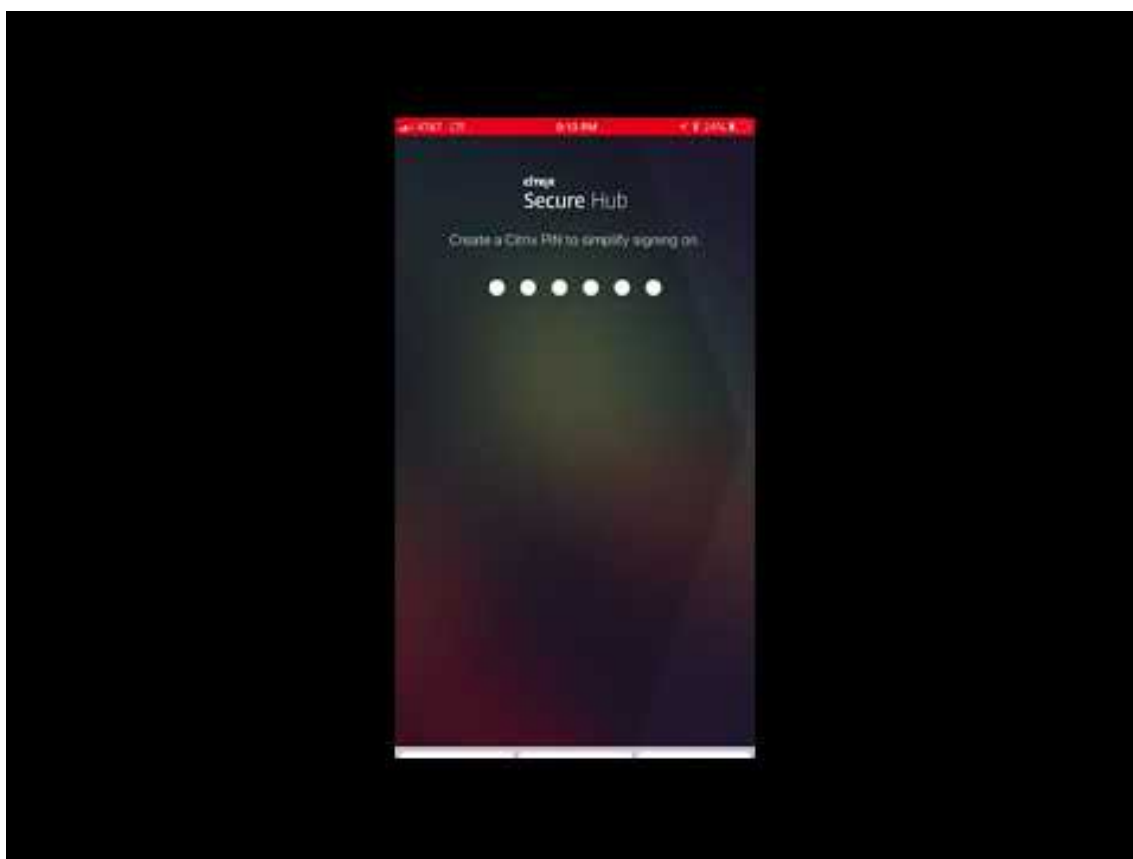
Secure Hub 10.8.60 到 18.9.0

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）。

Create Rewrite Action

Name*
 ?

Type*

Use this action type to insert a header.

Header Name*

Expression Expression Editor

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

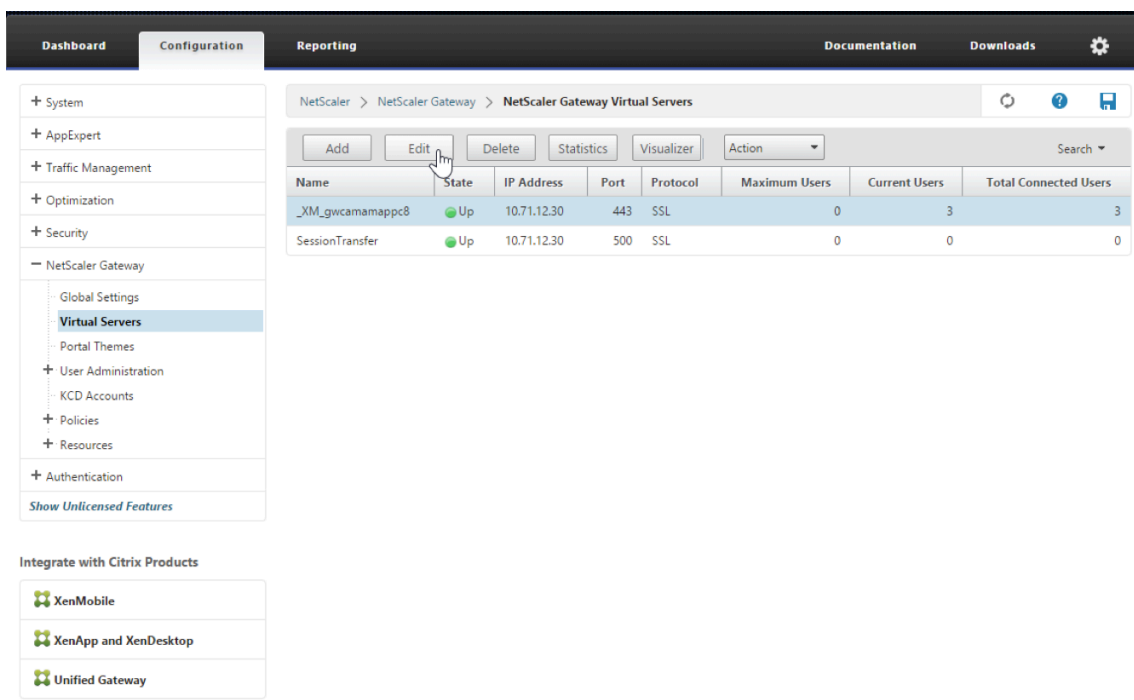
以下结果将显示在主 **Rewrite Actions**（重写操作）屏幕上。

NetScaler > AppExpert > Rewrite > Rewrite Actions ↻ ? 📄

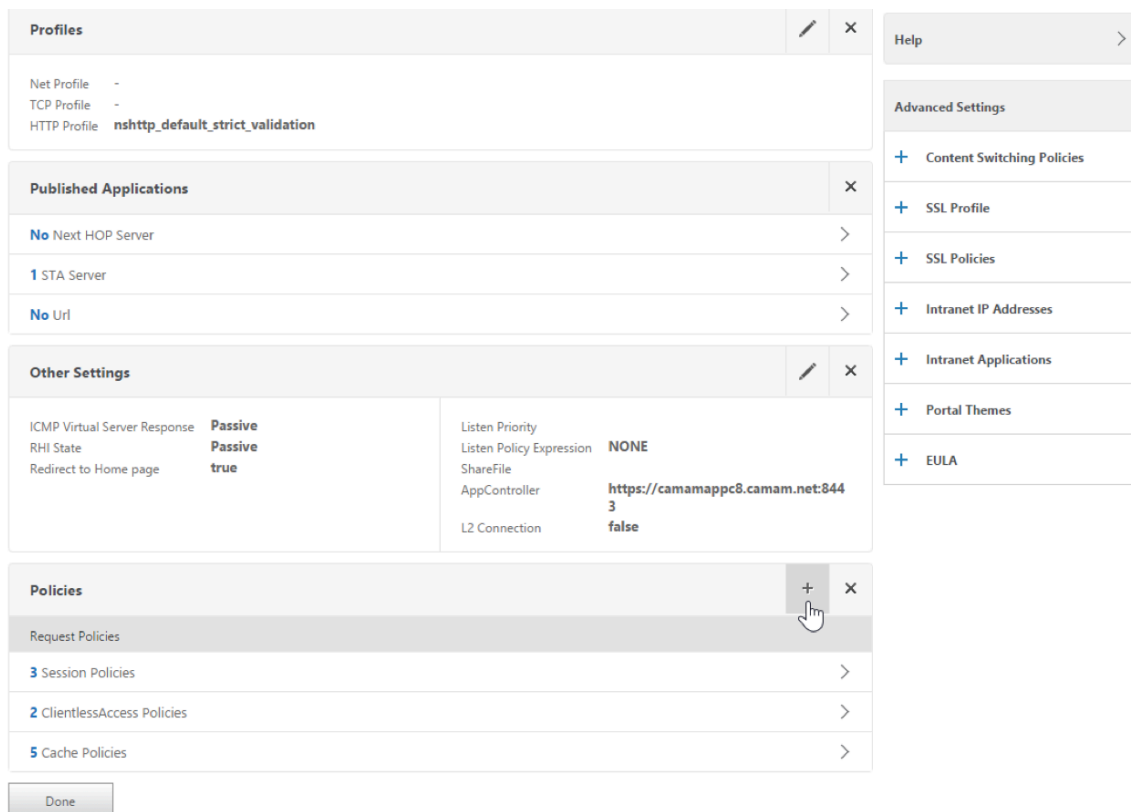
Show built-in Rewrite Actions Search

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\\'+window.location.pathname.split('\\')[1]+'\\'+wi...	re~ a.substr(0,3).toLowerCase(\\)=\\'%2f\\)=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

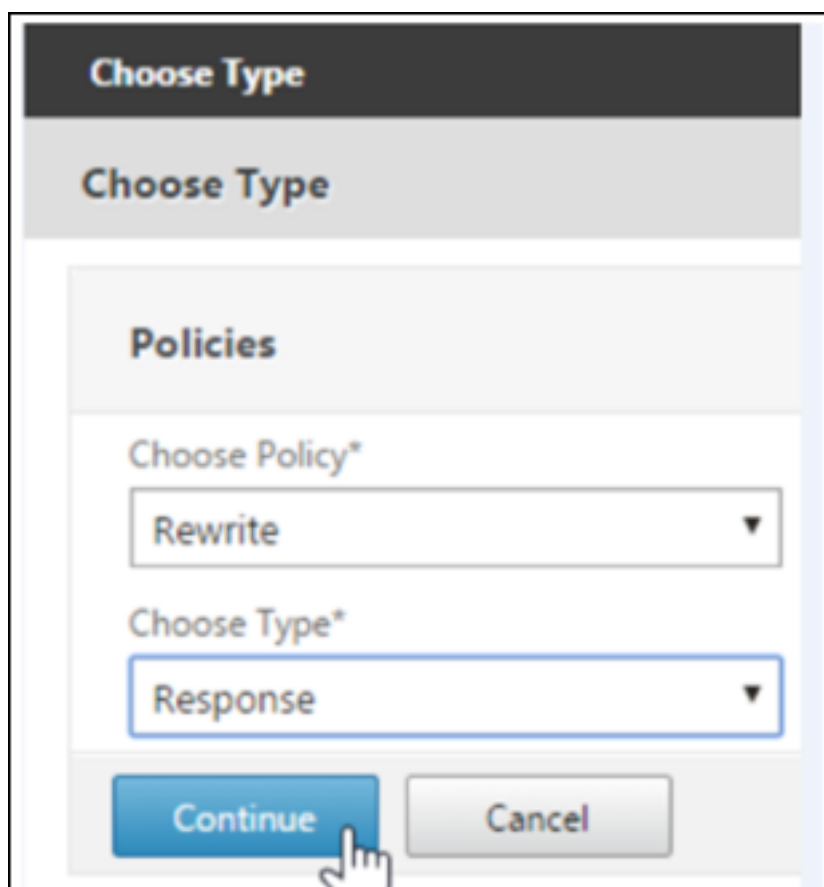
- 然后您需要将重写操作作为重写策略绑定到虚拟服务器。转到 **Configuration (配置) > NetScaler Gateway > Virtual Servers**（虚拟服务器），然后选择您的虚拟服务器。



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)。



The screenshot shows a dialog box titled "Choose Type". Below the title, there is a subtitle "Choose Type". Underneath, there is a section labeled "Policies". This section contains two dropdown menus. The first dropdown is labeled "Choose Policy*" and has "Rewrite" selected. The second dropdown is labeled "Choose Type*" and has "Response" selected. At the bottom of the dialog, there are two buttons: "Continue" (highlighted in blue) and "Cancel" (grey). A mouse cursor is pointing at the "Continue" button.

10. 单击继续。

Policy Binding (策略绑定) 部分将展开。

Choose Type

Choose Type

Policies

Choose Policy
Rewrite

Choose Type
Response

Policy Binding

Select Policy*

Click to select

Binding Details

Priority*

100

Goto Expression*

END

Bind Close

11. 单击 **Select Policy** (选择策略)。

将出现一个包含现有策略的屏幕

Rewrite Policies

Select Add Edit Delete Show Bindings Policy Manager Statistics Action

Show built-in Rewrite Policies Search

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	✕

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)。

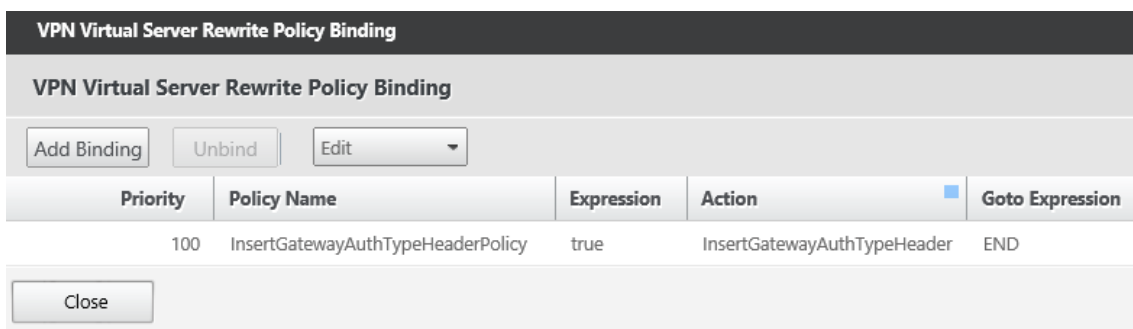
如果绑定成功，将出现主配置屏幕，其中显示了已完成的重写策略。

Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED
Refresh Count	0	Client Authentication	ENABLED	SSLv3	ENABLED
Enable Session Reuse	ENABLED	Client Certificate	Mandatory	TLSv1	ENABLED
Time-out	120	Send Close-Notify	YES	TLSv1.1	ENABLED
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLSv1.2	ENABLED
		SNI Enable	DISABLED		

ICMP Virtual Server Response	Passive	Listen Priority	
RHE State	Passive	Listen Policy Expression	None
Redirect to Home page	true	ShareFile	
		AppController	https://xms3.dm.com:8443
		L2 Connection	false

Policies	+	x
Request Policies		
3 Session Policies		>
2 ClientlessAccess Policies		>
4 Cache Policies		>
Response Policies		>
1 Rewrite Policy		>

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**

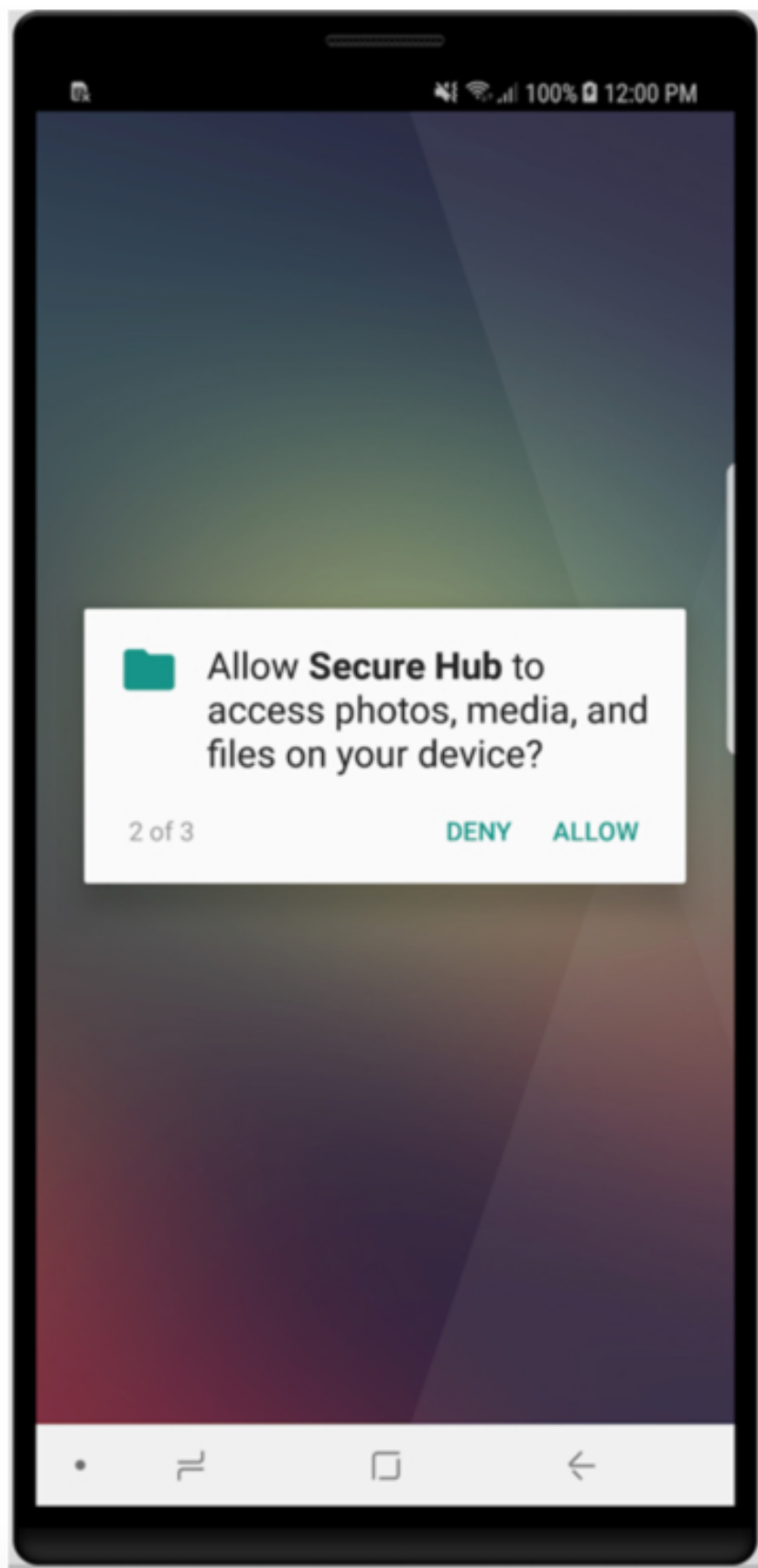
用户首先将 Secure Hub 从 Apple 或 Android 应用商店下载到其设备。

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](#)。

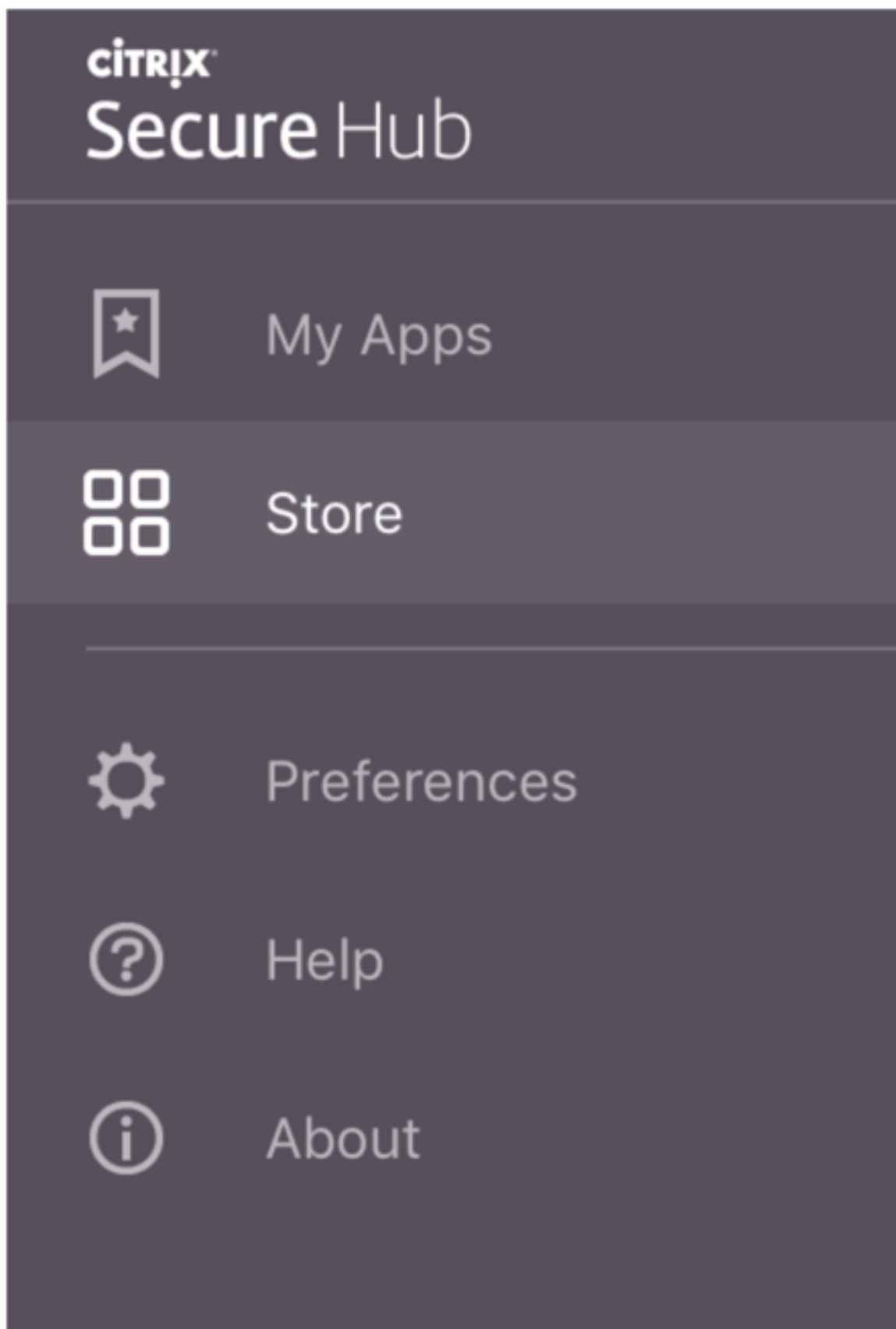
在 Secure Hub for Android 上执行初始安装和注册过程中, 将显示以下消息: Allow Secure Hub to access photos, media, and files on your device? (是否允许 Secure Hub 访问您的设备上的照片、媒体和文件?)

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。

XenMobile Analyze Manage Configure administrator

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name*

Default store view Category A-Z

Device Phone Tablet

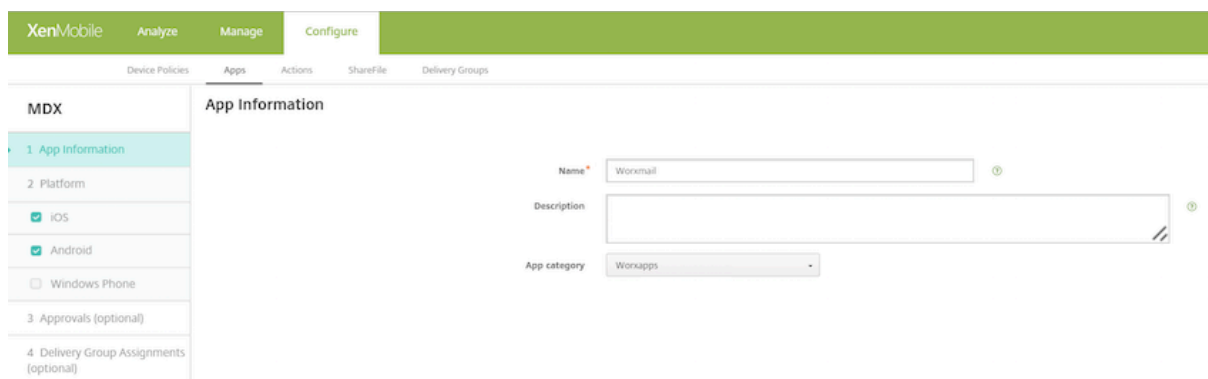
Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

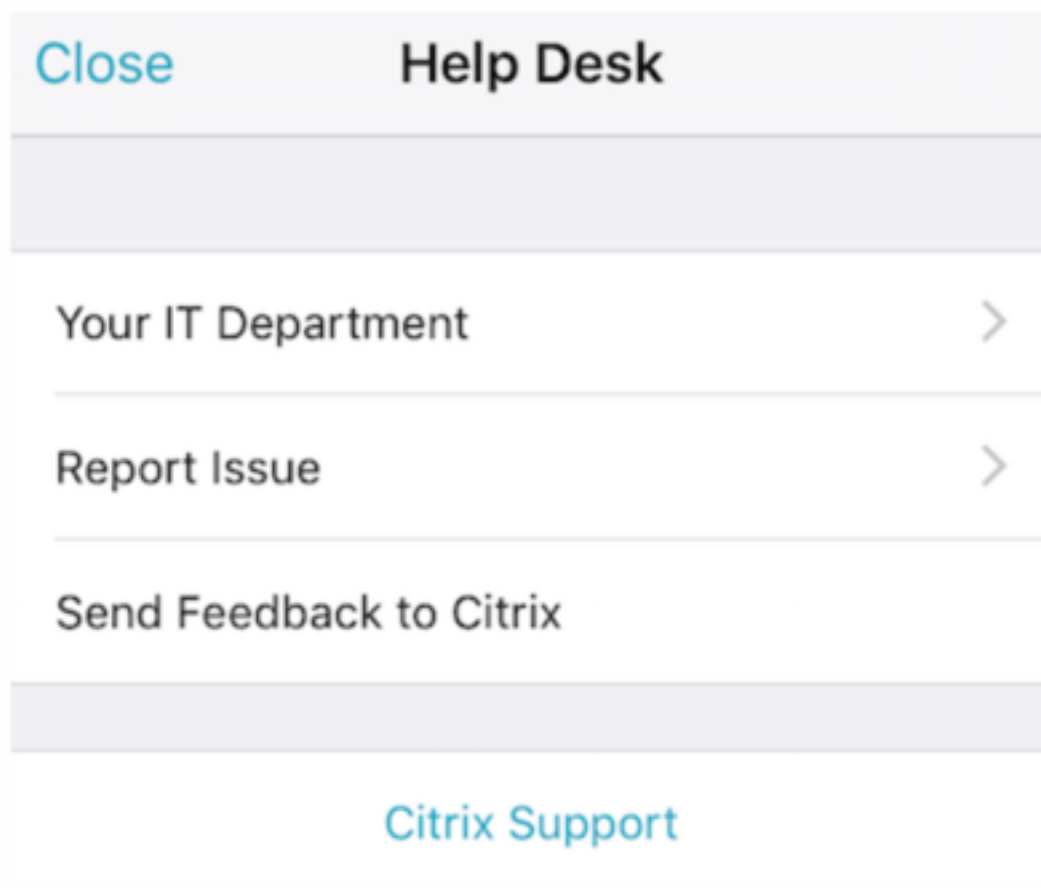
可以在 Endpoint Management 控制台中编辑应用程序说明。单击配置，然后单击应用程序。从表格中选择应用程序，然后单击编辑。选择正在编辑其说明的应用程序的平台，然后在说明框中键入文本。



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。

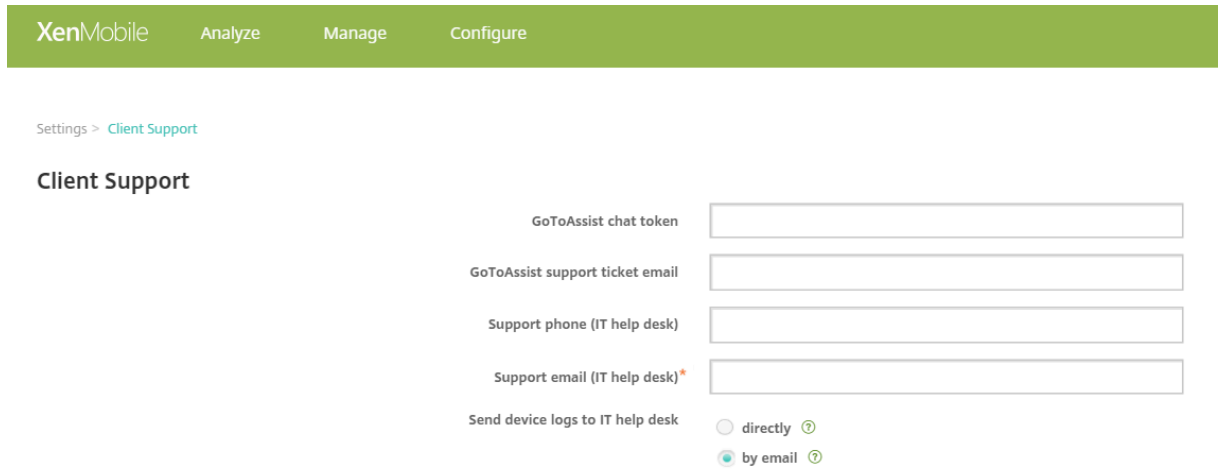
配置的帮助选项

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](#)。用户可以从其中搜索所有 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”。

已知问题和已修复的问题

November 16, 2021

Citrix 支持从最后两个版本的移动生产力应用程序进行升级。

Secure Hub 21.11.0

Secure Hub 21.11.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.11.0 中已修复的问题

Secure Hub for Android

-在 Secure Hub for Android 中注册期间，将显示未找到证书错误消息。单击安装证书时，将显示一个空链接，没有任何证书。如果单击取消，将显示身份验证屏幕。注销并登录 Secure Hub 时也会出现此问题。[CXM-101126]

Secure Hub 21.10.0

Secure Hub 21.10.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.10.0 中已修复的问题

Secure Hub for iOS

- 在 Secure Hub for iOS 中，系统会提示您使用 PIN 通过 Apple 部署计划在设备上注册。[CXM-99240]

Secure Hub for Android

- 创建 Android 设备的注册配置文件以在企业拥有的设备模式下在工作配置文件中注册时，必须启用 **BYOD** 工作配置文件设置。如果不启用此设置，设备将无法注册。[CXM-100418]
- 登录 Secure Hub for Android 时，系统将自动填充电子邮件 ID。[CXM-100517]

Secure Hub 21.8.0

Secure Hub for iOS

Secure Hub 21.8.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.8.0 中已修复的问题

- 当您在设备空闲后登录到 Secure Mail 时，Secure Hub for iOS 将打开并尝试登录，但登录请求失败。Secure Mail 将继续提示用户登录并创建登录循环。[CXM-96825]
- 用户名或密码中包含某些特殊字符的用户无法注册。[CXM-98778]

Secure Hub 21.7.1

Secure Hub for Android

本版本中没有已知问题或已修复的问题。

早期版本中的已知问题和已修复的问题

有关早期版本的 Secure Hub 中的已知问题和已修复的问题，请参阅 [Secure Hub 已知问题和已修复的问题的历史记录](#)。

身份验证提示情景

June 29, 2021

不同情景会提示用户在其设备上输入凭据以在 Secure Hub 中执行身份验证。

这些情景将随以下因素而变化：

- Endpoint Management 控制台设置中的 MDX 应用程序策略和客户端属性配置。
- 执行脱机身份验证，还是执行联机身份验证（设备需要通过网络连接到 Endpoint Management）。

此外，用户输入的凭据类型（例如 Active Directory 密码、Citrix PIN 码或通行码、一次性密码、指纹身份验证，后者在 iOS 中称为 Touch ID）也会根据身份验证的类型和频率而变化。

首先说明会生成身份验证提示的情景。

- 设备重新启动：用户启动其设备时，必须通过 Secure Hub 重新进行身份验证。
- 脱机不活动 (超时)：在启用了”应用程序通行码 MDX”策略的情况下（默认），称为“不活动计时器”的 Endpoint Management 客户端属性开始起作用。不活动计时器会限制时间长度，在此期限内，任何使用安全容器的应用程序中可不存在用户活动。

当不活动计时器到期时，用户必须在设备上对安全容器重新进行身份验证。例如，如果用户设定了其设备然后离开，则当不活动计时器已经到期时，别人无法取走设备并访问容器内的敏感数据。您可以在 Endpoint Management 控制台中设置不活动计时器客户端属性。默认值为 15 分钟。通过将应用程序通行码设置为开以及使用“不活动计时器”客户端属性，可控制最常见的身份验证提示情景。

- 从 **Secure Hub** 注销：。当用户从 Secure Hub 注销后，如果应用程序要求使用通行码（由应用程序通行码 MDX 策略和不活动计时器状态决定），用户在下次访问 Secure Hub 或任何 MDX 应用程序时必须重新进行身份验证。
- 最长脱机期限：。此情景由 MDX 策略控制，因此特定于每个应用程序。最长脱机期限 MDX 策略的默认设置为 3 天。如果应用程序在 Secure Hub 中运行而无需进行联机身份验证的时间期限已过，需要在 Endpoint Management 中执行签入以确认应用程序授权和刷新策略。当执行此签入时，应用程序会触发 Secure Hub 进行联机身份验证。用户必须重新进行身份验证才能访问 MDX 应用程序。

请注意最长脱机期限和活动轮询期限 MDX 策略之间的关系：

- 活动轮询期限是指应用程序在 Endpoint Management 中执行签入以执行安全操作（例如应用程序锁定和应用程序擦除）的期限。此外，应用程序还会检查更新的应用程序策略。
- 在通过活动轮询期限策略成功检查策略后，最长脱机期限计时器重置并再次开始倒计时。

在 Endpoint Management 中针对活动轮询期限和最长脱机期限过期执行的签入均要求在设备上使用有效 Citrix Gateway 令牌。如果设备具有有效的 Citrix Gateway 令牌，则应用程序会从 Endpoint Management 检索新策略，而不会导致用户服务发生任何中断。如果应用程序需要使用 Citrix Gateway 令牌，则会切换到 Secure Hub，并且用户会在 Secure Hub 中看到身份验证提示。

在 Android 设备上，Secure Hub 活动屏幕会直接在当前应用程序屏幕的上方打开。但是，在 iOS 设备上，Secure Hub 必须在前台运行，这会暂时取代当前的应用程序。

用户输入其凭据后，Secure Hub 将切换回原始应用程序。在这种情况下，如果您允许使用缓存的 Active Directory 凭据，或者您配置了客户端证书，用户可以输入 PIN、密码或指纹身份验证。否则，用户必须输入其完整 Active Directory 凭据。

Citrix ADC 令牌可能由于 Citrix Gateway 会话处于不活动状态或强制执行的会话超时策略而变得无效，如下面的 Citrix Gateway 策略列表中所述。当用户再次登录 Secure Hub 时，他们可以继续运行应用程序。

- **Citrix Gateway** 会话策略：当系统提示用户进行身份验证时，两个 Citrix Gateway 策略也会产生影响。在这些情况下，用户将执行身份验证以与 Citrix ADC 创建联机会话，以连接到 Endpoint Management。
 - 会话超时：如果在设定的时段内没有发生网络活动，Endpoint Management 的 Citrix ADC 会话将断开连接。默认值为 30 分钟。但是，如果您使用 Citrix Gateway 向导配置该策略，默认值将为 1440 分钟。系统会向用户显示身份验证提示以重新连接其企业网络。
 - 强制超时：如果设置为开，Endpoint Management 的 Citrix ADC 会话将在超过强制超时期限后断开连接。实施的超时将使得在设定的时段后强制重新执行身份验证。然后，在用户下次使用时，会向用户显示身份验证提示以重新连接到其企业网络。默认值为关。但是，如果您使用 Citrix Gateway 向导配置该策略，默认值将为 1440 分钟。

凭据类型

上一节讨论系统会在何时提示用户进行身份验证。本部分内容探讨用户必须输入的各种凭据。必须通过多种身份验证方法执行身份验证以访问设备上的加密数据。要初始解锁设备，您需要解锁主要容器。在执行此操作并且再次保护容器（以重新获取访问权限）之后，您需要解锁次要容器。

注意：

术语托管应用程序是指由 MDX Toolkit 封装的应用程序，其中，您已保留默认启用的“应用程序通行码 MDX”策略，并使用“不活动计时器”客户端属性。

需确定凭据类型的情形如下所示：

- 主容器解锁：需要 Active Directory 密码、Citrix PIN 或通行码、一次性密码、Touch ID 或指纹 ID 才能解锁主要容器。

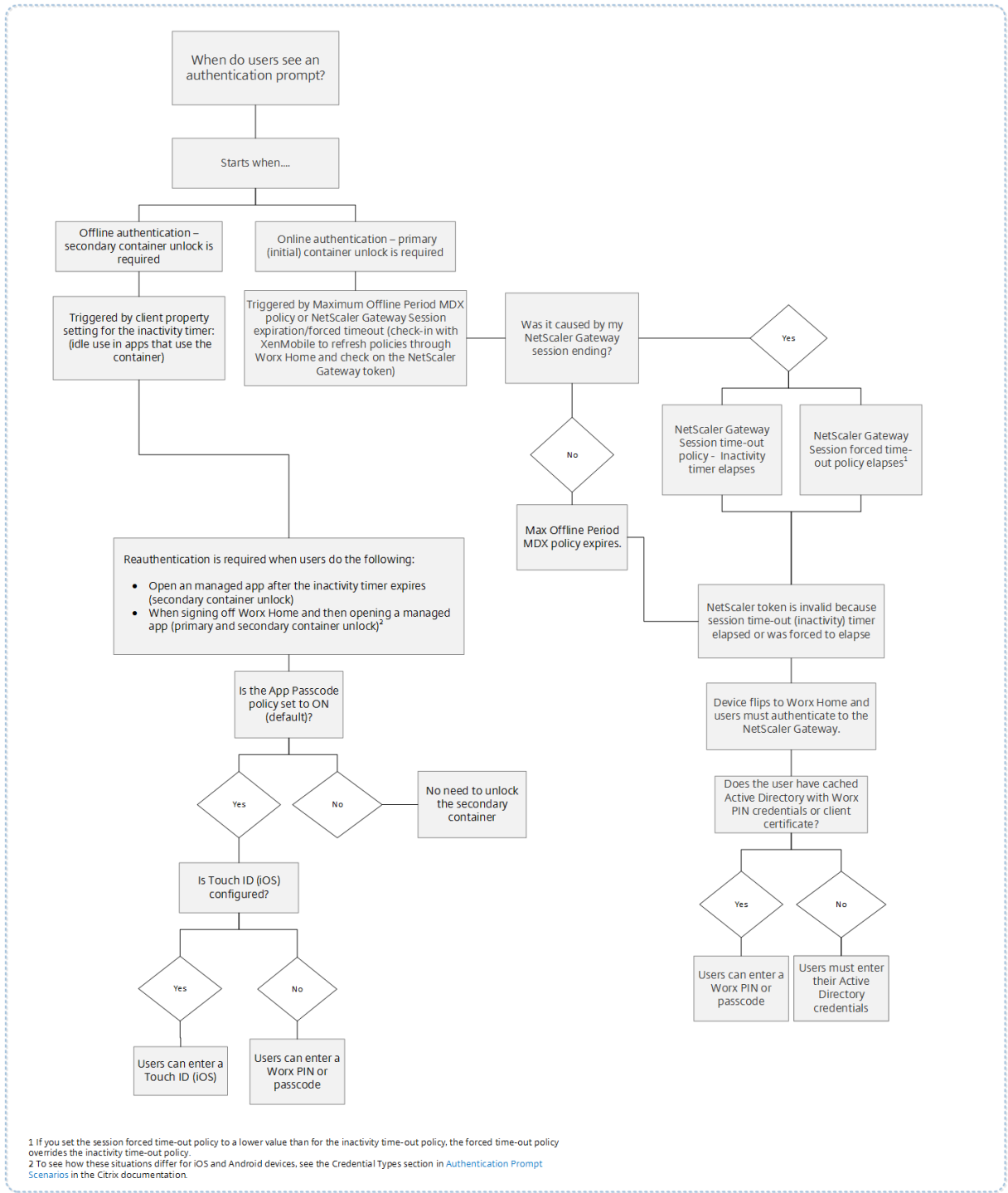
- 在 iOS 上，当用户打开 Secure Hub 或在设备上安装托管应用程序后首次打开该应用程序时。
- 在 iOS 上，当用户重新启动设备然后打开 Secure Hub 时。
- 在 Android 上，当用户在 Secure Hub 未运行的情况下打开托管应用程序时。
- 在 Android 上，当用户因任何理由（包括设备重启）重新启动 Secure Hub 时。
- 次要容器解锁：需要指纹身份验证（如果已配置）、Citrix PIN 或通行码或者 Active Directory 凭据才能解锁次要容器。
 - 当用户在不活动计时器到期后打开托管应用程序时。
 - 当用户从 Secure Hub 注销然后打开托管应用程序时。

当满足下列条件时，需为任一种容器解锁过程使用 Active Directory 凭据：

- 用户更改与其公司帐户相关联的通行码时。
- 当您未在 Endpoint Management 控制台中设置客户端属性以启用 Citrix PIN 时：ENABLE_PASSCODE_AUTH 和 ENABLE_PASSWORD_CACHING。
- 当 NetScaler Gateway 会话结束时，会话结束在以下情况下发生：会话超时或实施的超时策略计时器超时，如果设备不缓存凭据或不具有客户端证书。

启用了指纹身份验证时，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，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](#)。

下面的流程图概述了用于确定用户在系统提示进行身份验证时必须输入哪些凭据的决策流程。



¹ If you set the session forced time-out policy to a lower value than for the inactivity time-out policy, the forced time-out policy overrides the inactivity time-out policy.
² To see how these situations differ for iOS and Android devices, see the Credential Types section in [Authentication Prompt Scenarios](#) in the Citrix documentation.

关于 **Secure Hub** 屏幕切换

还需要注意的是，当从应用程序切换到 **Secure Hub** 然后需切回到应用程序的情况。切换过程会显示一条必须由用户响应的通知。在这种情况下不需要执行身份验证。在 **Endpoint Management** 中执行签入（由最长脱机期限和活动轮询期限 MDX 策略指定），并且 **Endpoint Management** 检测到需要通过 **Secure Hub** 推送到设备的更新后的策略后，

会出现此情况。

使用派生凭据注册设备

January 25, 2019

派生凭据提供适用于移动设备的加强的身份验证。从智能卡派生的凭据驻留在移动设备上，而非智能卡上。智能卡为个人身份验证 (Personal Identity Verification, PIV) 卡或通用访问卡 (Common Access Card, CAC)。

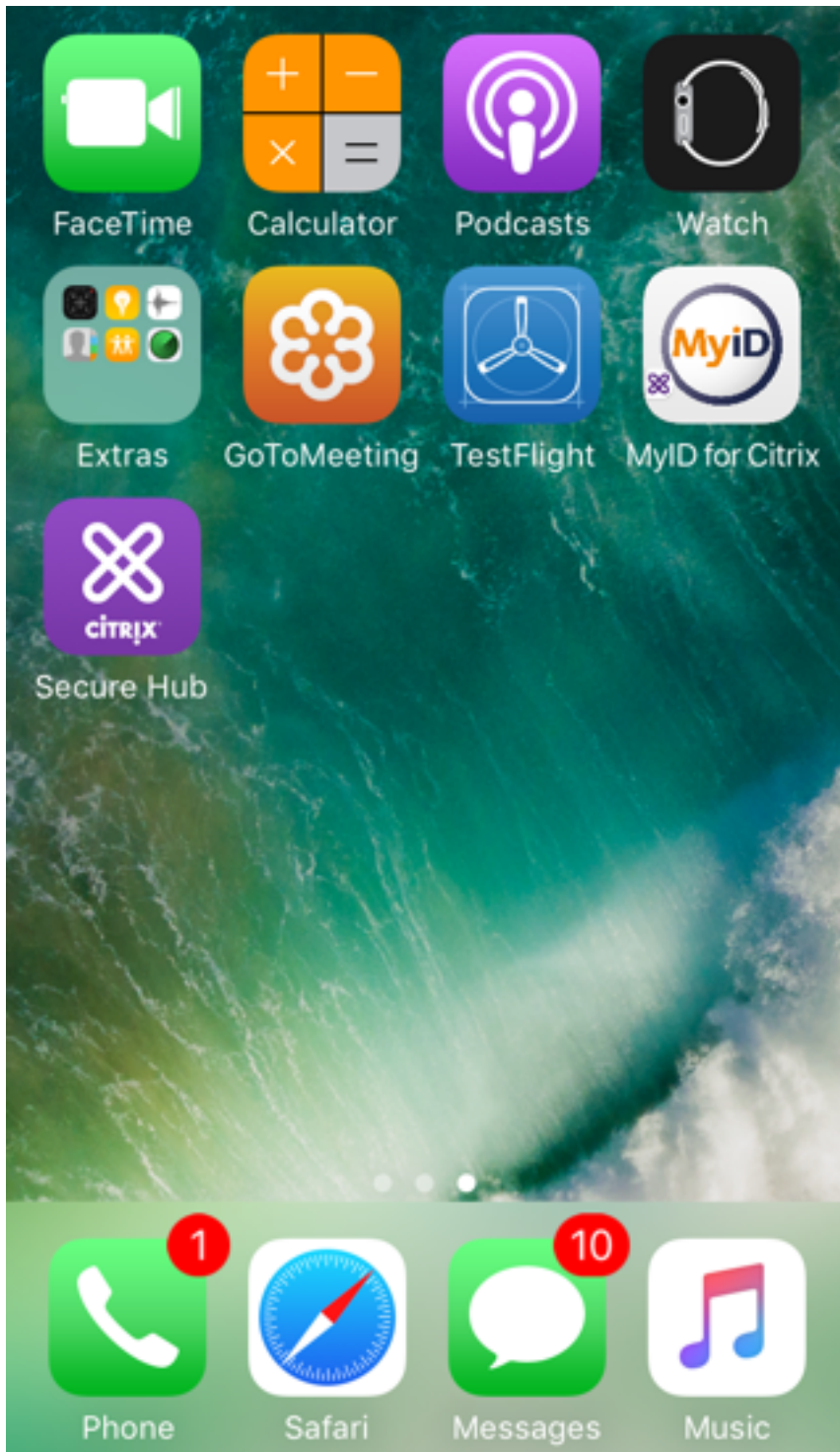
派生凭据为包含用户标识符 (例如 UPN) 的注册证书。Endpoint Management 将从凭据提供程序获取的凭据存储在设备上的一个安全保管库中。

Endpoint Management 可以使用适用于 iOS 设备注册的派生凭据。如果配置为使用派生凭据，Endpoint Management 将对 iOS 设备不支持注册邀请或其他注册模式。但是，您可以使用相同的 Endpoint Management 服务器通过注册邀请和其他注册模式注册 Android 设备。

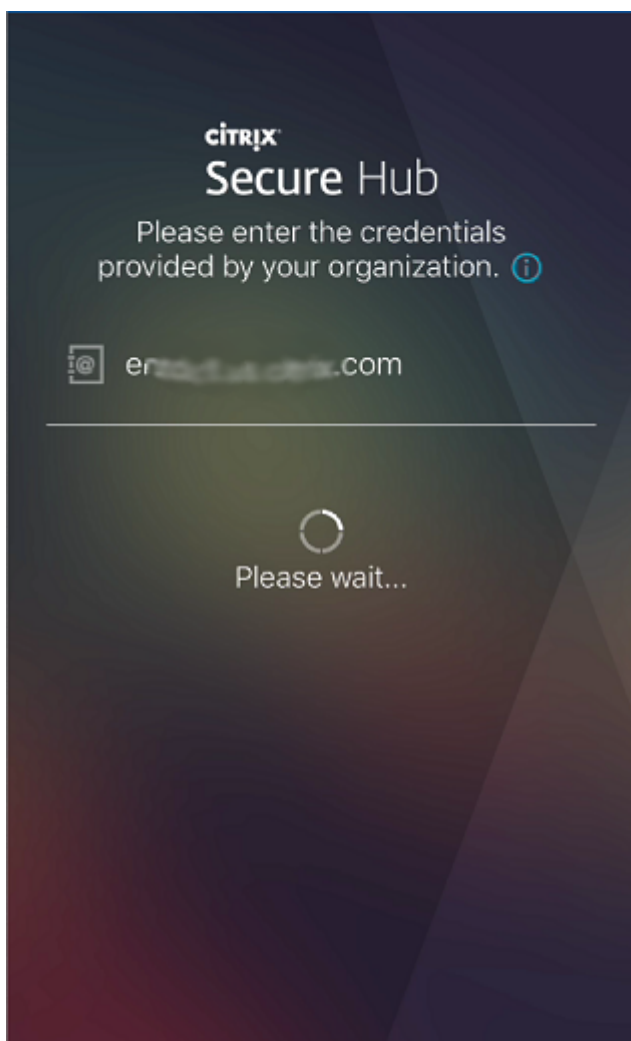
使用派生凭据时的设备注册步骤

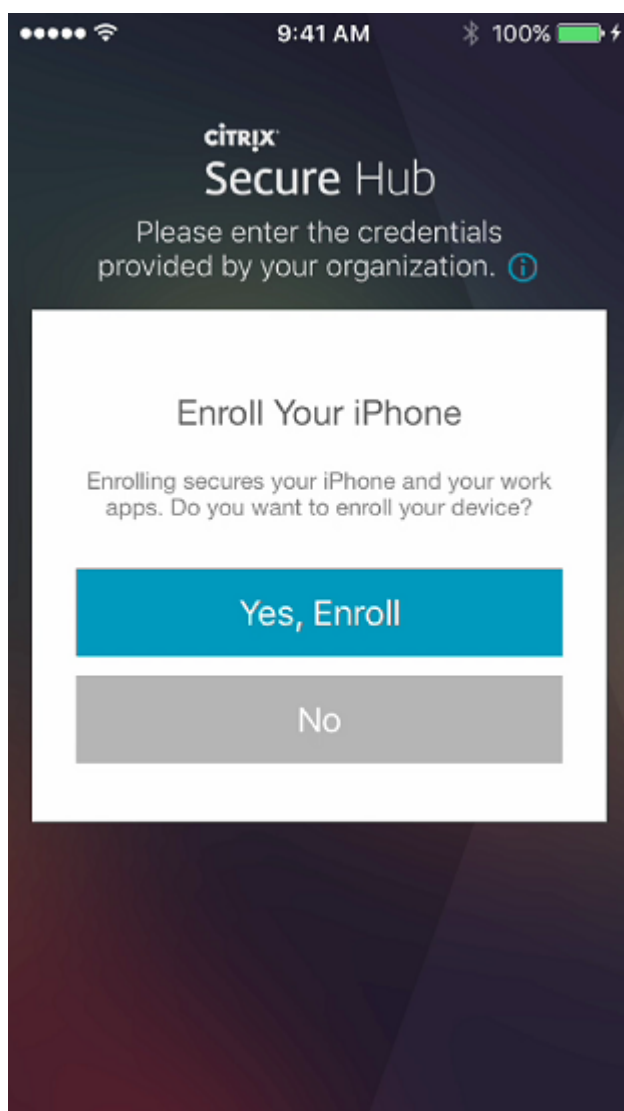
注册要求用户向连接到其桌面的读卡器中插入智能卡。

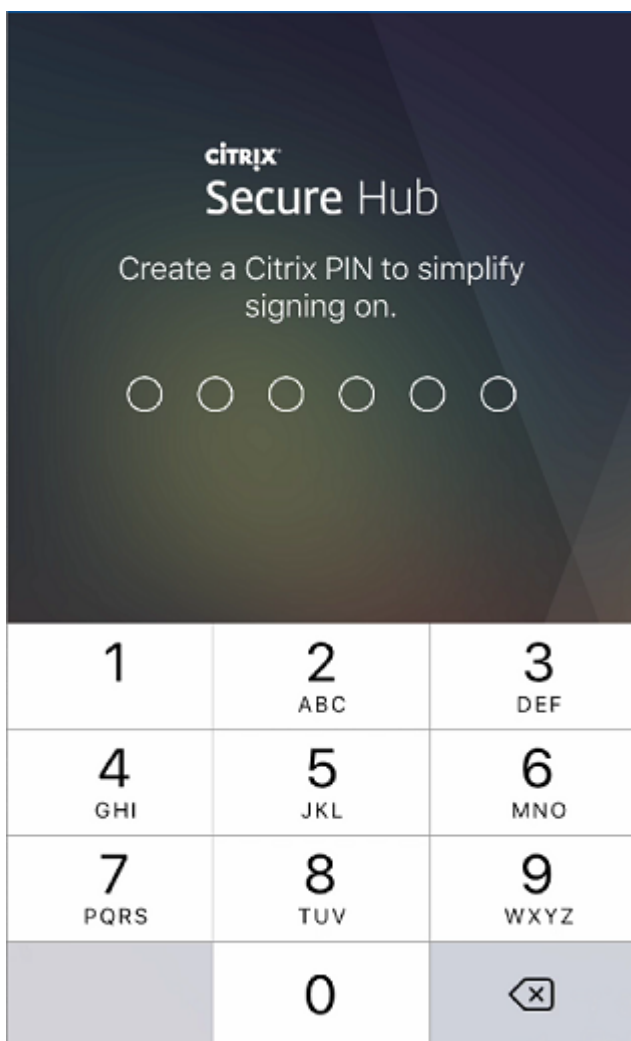
1. 用户安装 Secure Hub 以及您的派生凭据提供程序提供的应用程序。在此示例中，身份提供程序应用程序为 Intercede MyID Identity Agent。



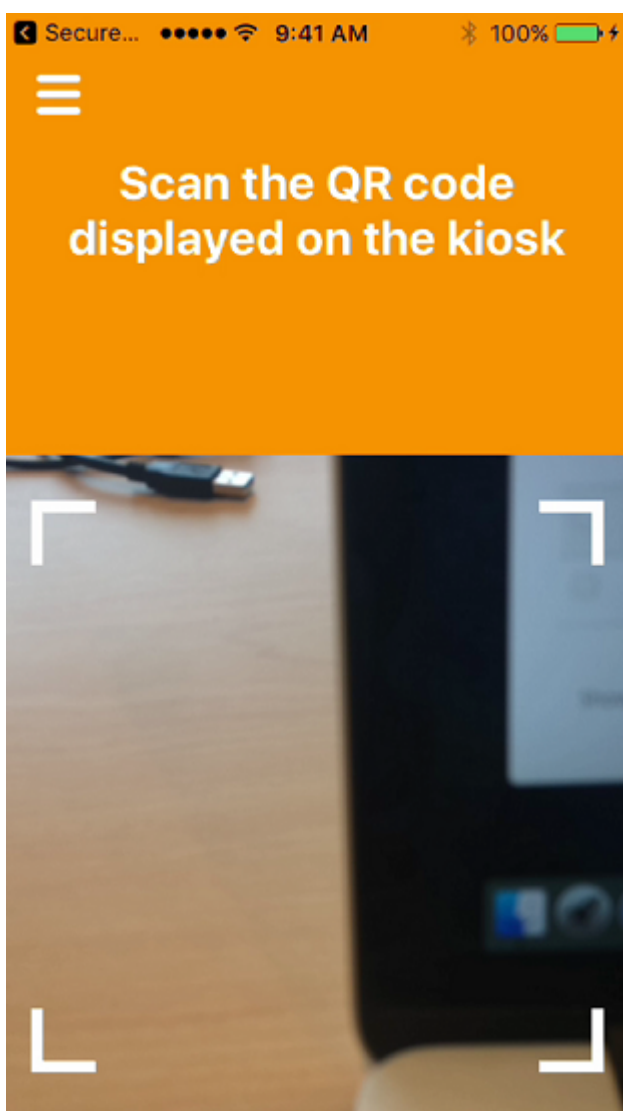
2. 用户启动 Secure Hub。系统提示时，用户键入 Endpoint Management 的完全限定域名 (FQDN)，然后单击下一步。在 Secure Hub 中的注册将开始运行。如果 Endpoint Management 支持派生凭据，Secure Hub 将提示用户创建一个 Citrix PIN。



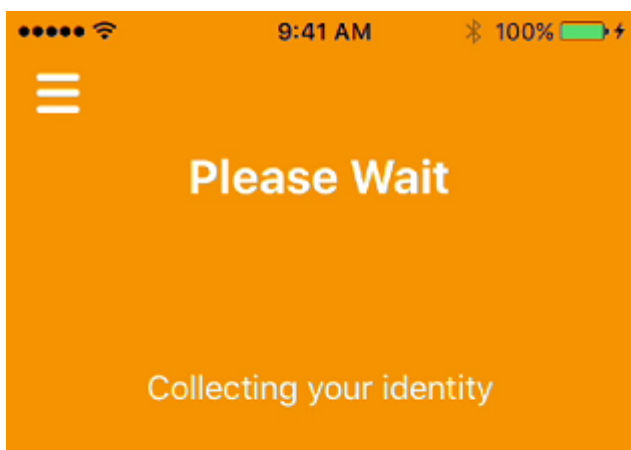




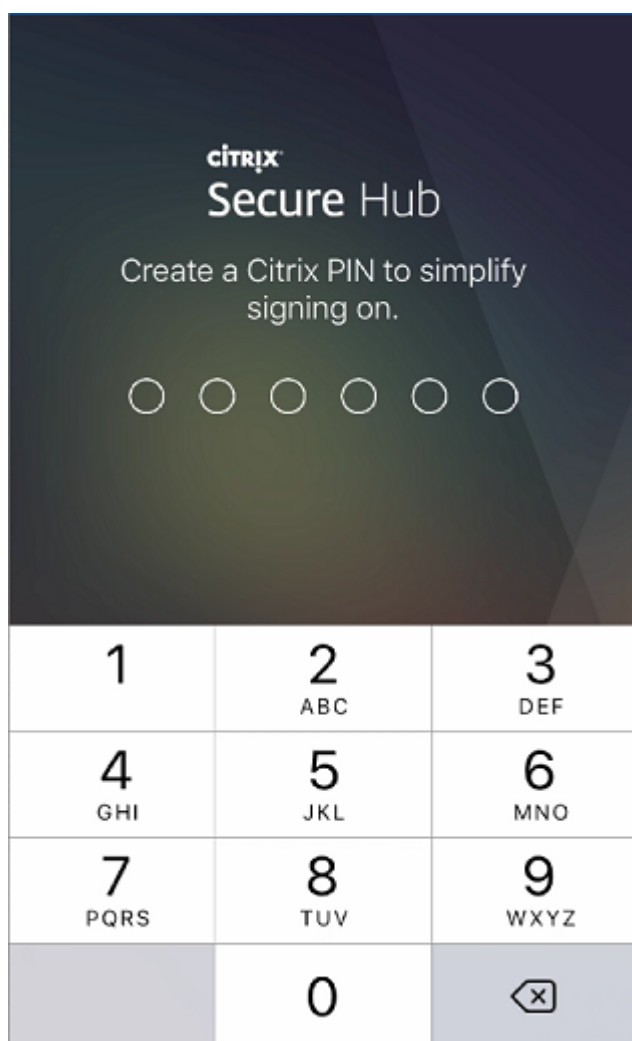
3. 用户按照说明进行操作，激活其智能凭据。此时将显示一个启动屏幕，然后显示扫描 QR 代码的提示。



4. 用户将卡插入连接到桌面的智能卡读卡器中。桌面应用程序随后将显示一个 QR 代码，并提示用户使用其移动设备扫描该代码。



系统提示时，用户输入其 Secure Hub PIN。



对该 PIN 进行身份验证后，Secure Hub 将下载证书。用户随后将按照提示完成注册。

要在 Endpoint Management 控制台中查看设备信息，请执行以下操作之一：

- 转至管理 > 设备，然后选择一个设备以显示命令框。单击显示更多。
- 转至分析 > 控制板。

**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

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).