



# 适用于 iOS 的 Citrix Workspace 应用程序

## Contents

关于此版本	3
安装必备条件	14
快速入门	20
配置	25
身份验证	30
安全	35
故障排除	40

## 关于此版本

November 22, 2019

### 新增功能

#### 1911 中的新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

#### 1910.5 中的新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

#### 1910 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1909.5 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1909 中的新增功能

### iOS 13 和 iPadOS 支持

iOS 13 和 iPadOS 支持适用于 iOS 的 Citrix Workspace 应用程序，包括 iPadOS 上的多任务处理支持。

#### 重要：

- iOS 13 不支持 CR01 应用程序。如果您使用的是 CR01 应用程序，Citrix 建议您不要升级到 iOS 13。
- 如果使用 SHA-1 证书链，可能需要切换到 SHA-2 证书链。SHA-1 签名证书在 iOS 13 上不再受信任。有关 TLS 服务器证书的详细信息，请参阅 [iOS 13 和 macOS 10.15 中对可信证书的要求](#)。
- 在 iOS 13 中，从 Safari Web 浏览器启动会话已发生变化。有关详细信息，请参阅 [帮助文档](#)。

借助对 AssistiveTouch 的支持，适用于 iOS 的 Citrix Workspace 应用程序现在以不同的方式连接到 Citrix X1 Mouse。Citrix Workspace 应用程序在启动时不再连接到 Citrix X1 Mouse。因此，Citrix X1 Mouse 图标在“设置”图标旁边的工具栏上不再可用。要查看 Citrix Workspace 应用程序是否启用了为 Citrix X1 Mouse 的访问权限，请导航到设置 > **Citrix X1 Mouse**。

### 1908 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

### 1907.5 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

### 1907 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

### 1906 中的新增功能

#### iPad 上的会话漫游

会话漫游现在也可以在 iPad 设备上使用。有关详细信息，请参阅 [iOS 设备](#) 的帮助文档。

#### 键盘布局同步

键盘布局同步允许用户切换客户端设备上的首选键盘布局。默认情况下，此功能处于禁用状态。

要启用键盘布局同步，请转到设置 > 键盘选项并启用键盘布局同步选项。

#### 注意：

使用本地键盘布局选项将激活客户端 IME（输入法编辑器）。如果您使用日语、中文或韩语工作，并且偏向于使用服务器 IME，请通过取消选中首选项 > 键盘中的选项来禁用本地键盘布局选项。

### 1905.5 中的新增功能

#### 支持会话漫游

使用云应用商店时，现在可以在 iPhone 和 iPod touch 设备上使用会话漫游。有关详细信息，请参阅 [iOS 设备](#) 的帮助文档。

### 1905 中的新增功能

#### Workspace Hub 的增强功能

Citrix Workspace 应用程序集成了一个新过程，用于在 iOS 设备上的可信列表中添加或删除 Workspace Hub。有关详细信息，请参阅 [安全连接](#)。

## 主机到客户端重定向

内容重定向功能允许您控制用户是使用在服务器上发布的应用程序来访问信息，还是使用用户设备上本地运行的应用程序来访问信息。

主机到客户端重定向是一种内容重定向。仅在服务器操作系统 VDA（而非桌面操作系统 VDA）上受支持。

启用了主机到客户端重定向时，URL 在服务器 VDA 上被截获并发送至用户设备。用户设备上的 Web 浏览器或多媒体播放器打开这些 URL。

如果您启用主机到客户端重定向，而用户设备无法连接到 URL，则该 URL 被重定向回服务器 VDA。

禁用了主机到客户端重定向时，用户使用服务器 VDA 上的 Web 浏览器或多媒体播放器打开 URL。

启用了主机到客户端重定向时，用户无法禁用它。

主机到客户端重定向以前称为服务器到客户端重定向。

有关详细信息，请参阅[常规内容重定向](#)。

## 1904.5 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

## 1904.2 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

## 1904 中的新增功能

### 增强功能

- 可以在应用程序和桌面的“最近”选项卡下查看最近使用的 SaaS 或 Web 应用程序的列表。
- 出于安全原因，Citrix Ready Workspace Hub 支持在移动设备与 Hub 之间建立的建立的安全套接字层 (SSL) 连接。您需要手动或自动设置完全限定域名 (FQDN)，以唯一标识每个设备。有关详细信息，请参阅 Citrix Ready Workspace Hub 文档中的[安全连接](#)。

## 1903 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

## 1902 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1901 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1812 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1811 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1810.2 中的新增功能

此版本解决了多个有助于改进整体性能和稳定性的问题。

注意：

有关配置 Citrix Ready Workspace Hub 内部信标的详细信息，请参阅知识中心文章 [CTX218708](#)。

#### 1810.1 中的新增功能

##### 支持 Citrix Ready Workspace Hub

Citrix Ready Workspace Hub 将数字环境和物理环境结合在一起，在安全的智能空间中交付应用程序和数据。完整的系统连接了设备（或一些对象），例如移动应用程序和传感器，以创建智能化的响应环境。

Citrix Ready Workspace Hub 在 Raspberry Pi 3 平台上构建而成。运行 Citrix Workspace 应用程序的设备将连接到 Citrix Ready Workspace Hub，并将应用程序或桌面投射到较大的显示器上。

有关适用于 iOS 的 Citrix Workspace 应用程序中的 Citrix Ready Workspace Hub 的详细信息，请参阅[配置 Citrix Ready Workspace Hub](#)。

有关 Citrix Ready Workspace Hub 的详细信息，请参阅 [Citrix Ready Workspace Hub](#) 文档。

#### 1810 中的新增功能

##### 支持 Purebred 派生凭据

此版本引入了支持在适用于 iOS 的 Citrix Workspace 应用程序中使用 Purebred 派生凭据。连接到允许使用派生凭据的应用商店时，用户可以使用虚拟智能卡登录适用于 iOS 的 Citrix Workspace 应用程序。仅本地部署支持此功能。

注意：

要使用此功能，需要运行 Citrix Virtual Apps and Desktops 7 1808 或更高版本。

有关配置派生凭据的信息，请参阅[派生凭据](#)。

## 1809 中的新增功能

### 支持 iOS 12

适用于 iOS 的 Citrix Workspace 应用程序完全支持 iOS 12。

## 1808 中的新增功能

### 更新了最终用户帮助

位于应用程序中的最终用户帮助已完全重新编写并更新以反映适用于 iOS 的 Citrix Workspace 应用程序的所有更改。

## 已修复的问题

### 1911 中已修复的问题

- 当您通过与 StoreFront 服务器的直接连接连接到 Workspace 时，尝试添加帐户可能会失败。[LD2549]
- 升级到 iOS 13 后，尝试打开软令牌 (.sdtid) 和配置 (.cr) 文件可能会失败。因此，无法从任一文件类型导入 Citrix Workspace 应用程序配置。[RFIOS-4788]
- 如果启动 VDA 会话，锁定设备后会话在扩展显示器上将保持活动状态。[LD2016]
- 如果您通过 Citrix Gateway 连接到 Workspace，尝试打开内容链接可能会失败。[LD1378]

### 1910.5 中已修复的问题

- 尝试从喜爱的应用程序列表中启动喜爱的应用程序可能会失败。[LD1007]
- 使用 Active Directory 并通过 Active Directory 联合身份验证服务 (ADFS) 向 Azure 进行身份验证时，尝试添加帐户可能会失败。[RFIOS-4679]

### 1910 中已修复的问题

- 尝试启动适用于 iOS 的 Citrix Workspace 应用程序可能会失败，并显示以下错误消息：`operation hdxsdk error domain session error 8`。[LD0651]
- 在 iOS 键盘设置中启用键盘快捷方式时，日语、中文和韩语客户端 IME 可能无法按预期运行。[LD2329]

#### 1909.5 中已修复的问题

- 在版本 1909 中，客户端驱动器映射 (CDM) 功能可能不起作用。[RFIOS-4655]

#### 1909 中已修复的问题

- 当您使用鼠标指针双击某个应用程序或文件时，该应用程序或文件将打开两次。[LD1160]
- 适用于 iOS 的 Citrix Workspace 应用程序版本 1904 和 1905 有时会意外退出。[RFIOS-4301]
- 此版本解决了 Citrix X1 Mouse 的连接和发现问题。[RFIOS-4529]

#### 1908 中已修复的问题

- 当 Citrix Workspace 应用程序从后台切换到前台时，将显示以下错误消息：“已重新连接到服务器”。[RFIOS-4510]
- 当 Citrix Workspace 应用程序从后台切换到前台时，使用已发布桌面打开的任何窗口都会在屏幕上移动，并且屏幕分辨率看上去很奇怪。当您使用 Citrix Workspace 应用程序版本 1904.2 或更高版本时，会出现此问题。[RFIOS-4401]
- 在设备上配置面容 ID 身份验证后，可能会出现以下问题：刷新应用程序和桌面列表时，Citrix Workspace 应用程序可能会意外退出。[LD1633]
- 断开或重新连接会话后，可能无法重新发现 Citrix X1 Mouse。此外，拖放鼠标操作有时也会失败。[RFIOS-4487]

#### 1907.5 中已修复的问题

- 当您的 Active Directory (AD) 密码过期时，“登录”页面不会提醒您该消息。[LD1849]

#### 1907 中已修复的问题

- 在 iPad 上，当两个资源具有相同的显示名称，并且其中一个资源已在会话中时，启动另一个资源可能会失败。[LD1467]
- 当活动用户会话超时，会话可能无法重新启动，并显示以下错误消息：  
“输入的地址未提供有效的应用程序列表。请检查该地址、网关设置和网络连接。”  
由于 Citrix Workspace 应用程序与 Citrix Gateway 之间的通信不正确，因此出现此问题。
- 在智能键盘上，当您按 Shift 键并使用 Citrix X1 Mouse 滚动时，垂直滚动不成功。[LD1284]



#### 1906 中已修复的问题

- 如果您在将某个应用程序或桌面从云应用商店漫游到 Workspace Hub 时尝试在本地启动同一应用程序或桌面，漫游会话将终止。[WH-2128]。
- 切换到横向模式时，iPad 上的搜索栏将被截断。[RFIOS-2310]
- 将设备旋转到横向模式时，设置菜单可能会异常显示。在多任务模式下最小化 Citrix Workspace 应用程序屏幕时会出现此问题。[RFIOS-3066]

#### 1905.5 中已修复的问题

- 使用 Safari Web 浏览器登录 StoreFront 后，虚拟桌面或应用程序可能无法打开。[RFIOS-4178]

#### 1905 中已修复的问题

本版本还解决了多个有助于改进整体性能和稳定性的问题。

#### 1904.5 中已修复的问题

- 首次登录 Citrix Workspace 应用程序时，登录可能会失败并显示以下错误消息：  
“无法连接到服务器。请重试。”  
[RFIOS-3588]
- 无法获取当前的纬度和经度报告详细信息。[RFIOS-3668]
- 从帐户设置中删除客户端证书可能会导致 Workspace 应用程序意外退出。[RFIOS-4212]

#### 1904.2 中已修复的问题

- 轻按自定义工具栏上的“箭头”图标时，自定义箭头键不可见。[RFIOS-4233]

#### 1904 中已修复的问题

- 可以无缝添加 PNAgent 帐户。[RFIOS-3342]
- 可以查看与某些连接中的 WiFi SSID 有关的错误消息。在 WiFi SSID 的帮助下，可以确保您与尝试连接到的 Citrix Ready Workspace Hub 位于相同的网络中。[WH-1903]
- Active Directory (AD) 密码过期后，从 Citrix Workspace 应用程序重置您的 AD 密码失败并显示错误。  
[RFIOS-3241]

- 在日语版 VDA 上运行的会话中，按 Option (Alt) + Return 键可让您在 Microsoft Excel 中的单元格中输入新行，并保留 IME 模式。[RFIOS-4046]
- 重新连接设备和 VDA 时，设备从睡眠模式恢复之后，显示屏在 10 到 20 秒内无响应。[RFIOS-4146]
- 使用 Google 双重身份验证时，从 iOS 设备登录 Citrix Workspace 应用程序失败，并显示以下错误消息：  
用户名、密码或通行码不正确  
[RFIOS-4064]

#### 1903 中已修复的问题

- 在 iPhone X 上使用版本为 1810 的 Citrix Workspace 应用程序时，当客户端设备处于横向视图时，键盘符号将消失。[LD0619]
- 在非英语系统中使用版本为 1812 的 Citrix Workspace 应用程序时，添加新帐户字段标签将以英语显示。[LD1066]
- 客户端设备长时间空闲时，Citrix X1 Mouse 将变得无响应。[LD0842]
- 在版本 1903 及更高版本中，取消了 Citrix Workspace 应用程序初始屏幕对话框。[RFIOS-3509]

#### 1902 中已修复的问题

- 使用 Enlightened Data Transport (EDT) 协议时，设备从睡眠模式恢复之后，显示屏在 10 到 20 秒内无响应。[LD0854]
- 输入用户名和密码进行身份验证时，使用密码字段时，键盘布局会切换到其他语言。[LD0588]

#### 1901 中已修复的问题

- 当外部 Apple 蓝牙键盘已连接并按 Shift + 0 以键入 “)” 符号时，会话将断开连接。[RFIOS-3658]

#### 1812 中已修复的问题

- 如果将屏幕分辨率设置为“自动调整 - 低”且分辨率为 1024x1366，屏幕上的文本间距看上去似乎不正确。[LC9808]
- 如果 Citrix Gateway 指向 Web Interface，则在添加应用商店帐户时，应用商店可能无法正确枚举并且您可能会遇到问题。[RFIOS-3342]
- 当您尝试从收藏的应用程序列表中删除必需应用程序时，Citrix Workspace 应用程序不会显示警告消息。[RFIOS-1556]
- 当虚拟键盘显示时，X1 鼠标坐标可能会出现偏移，以显示不正确的选择。[RFIOS-3418]

- 当您登录到 PNAgent 帐户时，页面将不显示要求您输入域凭据的屏幕。如果最初未输入域凭据，则会出现此问题。[RFIOS-2944]
- 升级到适用于 iOS 的 Citrix Workspace 应用程序 1809 后，当您启动已发布的应用程序时，将显示证书不受信任错误消息。[RFIOS-3368]

#### 1811 中已修复的问题

- 捕获的数字签名可能不正确。要修复此问题，请将 *HandleDoubleTapLocally=no* 参数添加到 default.ica 文件中以禁止该捕获行为。

要修改 StoreFront 或 Web Interface 服务器上的 default.ica 文件，请参阅知识中心文章 [CTX116357](#) 以了解详细步骤。[LD0629]

#### 1810.2 中已修复的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1810.1 中已修复的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1810 中已修复的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 1809 中已修复的问题

- 从 Citrix Receiver 升级到 Citrix Workspace 应用程序后，用户可能无法登录应用商店。[RFIOS-3233]

#### 1808 中已修复的问题

此版本解决了多个有助于改进整体性能和稳定性的问题。

#### 已知问题

#### 1911 中的已知问题

在此版本中没有发现新的已知问题。

### 1910.5 中的已知问题

在此版本中没有发现新的已知问题。

### 1910 中的已知问题

- 会话中的虚拟键盘下方可能会出现空白区域。[LC9314]

### 1909.5 中的已知问题

- 在版本 1904 及更高版本中，可能无法在登录页面上输入凭据。使用面容 ID 进行身份验证时会出现此问题。  
解决方法为，导航到设置 > 密码和帐户，然后禁用自动填充密码。在使用 iOS 12 的 iPhone 设备上已观察到此问题。[RFIOS-4652]
- 在 iOS 键盘设置中启用键盘快捷方式时，日语、中文和韩语客户端 IME 可能无法按预期运行。解决方法为，在 iOS 中，转到设置 > 常规 > 键盘 > 快捷方式并禁用该选项。[LD2329]

### 1909 中的已知问题

- 在使用日语、中文或韩语键盘的 iOS 13 设备上，**Command-C** 和 **Command-V** 键盘快捷方式不成功。[RFIOS-4620]

### 1908 中的已知问题

在此版本中没有发现新问题。

### 1907.5 中的已知问题

在此版本中没有发现新问题。

### 1907 中的已知问题

在此版本中没有发现新问题。

### 1906 中的已知问题

在此版本中没有发现新问题。

#### **1905.5 中的已知问题**

- 如果您在将某个应用程序或桌面从云应用商店漫游到 Workspace Hub 时尝试在本地启动同一应用程序或桌面，漫游会话将终止。[WH-2128]

#### **1905 中的已知问题**

在此版本中没有发现新问题。

#### **1904.5 中的已知问题**

在此版本中没有发现新问题。

#### **1904.2 中的已知问题**

在此版本中没有发现新问题。

#### **1904 中的已知问题**

在此版本中没有发现新问题。

#### **1903 中的已知问题**

- 使用 Safari Web 浏览器登录 StoreFront 后，虚拟桌面或应用程序可能无法打开。[RFIOS-4178]

#### **1902 中的已知问题**

在此版本中没有发现新问题。

#### **1901 中的已知的问题**

在此版本中没有发现新问题。

#### **1812 中的已知问题**

在此版本中没有发现新问题。

#### 1811 中的已知问题

- 在 iPad Pro (12.9 英寸) 上使用自动调整 - 高设置时, 手指轻按可能无法正确起作用。解决方法: 将 Citrix Workspace 应用程序中的“显示选项”更改为其他设置。[RFIOS-1766]

#### 1810.2 中的已知问题

- 在 iPad Pro (12.9 英寸) 上使用自动调整 - 高设置时, 手指轻按可能无法正确起作用。解决方法: 将 Citrix Workspace 应用程序中的“显示选项”更改为其他设置。[RFIOS-1766]
- 切换网络时, 会话可能无法重新连接或重新启动。解决方法: 关闭并重新启动 Citrix Workspace 应用程序。[RFIOS-3246]
- 会话可能无法启动, 并显示 HdxSdkErrorDomain\_Session 错误 8。解决方法: 关闭并重新启动 Citrix Workspace 应用程序。[RFIOS-3374]

#### 1810.1 中的已知问题

在此版本中没有发现新问题。

#### 1810 中的已知问题

在此版本中没有发现新问题。

#### 1809 中的已知问题

在此版本中没有发现新问题。

#### 1808 中的已知问题

- 在 iPhone 上使用智能卡时, 在注销后启动应用程序会显示不变的加载状态。解决方法: 重新启动该应用程序。[RFIOS-2550]
- 使用智能卡时, 在升级到适用于 iOS 的 Citrix Workspace 应用程序后, 可能无法正确进行会话注销。解决方法: 重新启动该应用程序。[RFIOS-3076]

## 安装必备条件

November 22, 2019

## 系统要求和兼容性

### 设备要求

- 适用于 iOS 的 Citrix Workspace 应用程序 1808 或更高版本支持 iOS 10、11 和 12。
- 适用于 iOS 的 Citrix Workspace 应用程序 1909 或更高版本支持 iOS 13 和 iPadOS。
- 此软件更新已在以下设备上通过验证：
  - iPhone 5x 各型号、iPhone 6x 各型号、iPhone 7x 各型号、iPhone 8x 各型号和仅 iPhone X 型号。
  - 除不受支持的 iPad 1 和 iPad 2 以外的所有 iPad 型号（包括 iPad Pro）。
- 外部显示器支持
  - iPhone - 受 iOS 支持。
  - iPad - 与 iOS 支持的对象相同（不使用整个屏幕）。

### 服务器要求

请务必为您的服务器安装所有最新的修补程序。

- 适用于 iOS 的 Citrix Workspace 应用程序支持使用 Citrix StoreFront 和 Web Interface 连接到虚拟桌面和应用程序。

#### StoreFront:

- StoreFront 3.6 或更高版本（推荐使用）。适用于 iOS 的 Citrix Workspace 应用程序已通过最新版本的 StoreFront 的验证；以前支持的版本包括 StoreFront 2.6 或更高版本。

用于直接访问 StoreFront 应用商店。适用于 iOS 的 Citrix Workspace 应用程序还支持早期版本的 StoreFront。

#### 注意：

在 XenApp 和 XenDesktop 7.8 中，Citrix 引入了对 Framehawk 虚拟通道和 3D Pro 的支持。此功能已扩展到适用于 iOS 的 Citrix Workspace 应用程序。

- 配置了适用于 Web 的 Workspace 站点的 StoreFront

用于从 Safari Web 浏览器访问 StoreFront 应用商店。用户必须使用浏览器手动打开 ICA 文件。有关此部署的限制，请参阅 [StoreFront](#) 文档。

#### Web Interface:

- 配置了 Web Interface 站点的 Web Interface 5.4
- 配置了 XenApp Services 站点的 Web Interface 5.4
- Citrix Gateway 上的 Web Interface（基于浏览器的访问仅限使用 Safari）  
必须启用 Citrix Gateway 提供的重写策略。

- **Citrix Virtual Apps and Desktops、XenApp 和 XenDesktop**（以下任意产品）：

- Citrix Virtual Apps and Desktops 7 1808 或更高版本
- Citrix XenDesktop 7.x 或更高版本
- Citrix XenApp 7.5 或更高版本
- Citrix XenApp 6.5 for Windows Server 2008 R2

连接、证书和身份验证

对于与 StoreFront 的连接，适用于 iOS 的 Citrix Workspace 应用程序支持以下身份验证方法：

	使用浏览器的适用于 Web 的 Workspace	StoreFront 服务站点 (本机)	StoreFront XenApp Services 站点 (本机)	Citrix Gateway 到适用于 Web 的 Workspace (浏览器)	Citrix Gateway 到 StoreFront 服务站点 (本机)
匿名	是	是			
域	是	是	是	是 *	是 *
域直通	是	是	是		
安全令牌				是 *	是 *
双重身份验证 (域 + 安全令牌)				是 *	是 *
SMS				是 *	否
智能卡		是		是 *	是 *
用户证书				是 (Citrix Gateway 插件)	是 (Citrix Gateway 插件)

\* 仅可用于适用于 Web 的 Workspace 站点以及包含 Citrix Gateway 的部署，而不管设备上是否已安装关联的插件。

对于与 Web Interface 5.4 的连接，适用于 iOS 的 Citrix Workspace 应用程序支持以下身份验证方法：

注意：  
Web Interface 使用术语“显式”表示域和安全令牌身份验证。



	Web Interface (浏览器)	Web Interface XenApp Services 站点	Citrix Gateway 到 Web Interface (浏览器)	Citrix Gateway 到 Web Interface XenApp Services 站点
匿名	是			
域	是	是	是 *	
域直通	是			
安全令牌			是 *	
双重身份验证 (域 + 安全令牌)			是 *	
SMS			是 *	
智能卡				
用户证书			是 (需要 Citrix Gateway 插件)	

## 证书

### 专用 (自签名) 证书

远程网关上安装了专用证书时，该设备上必须安装组织的证书颁发机构的根证书，才能使用适用于 iOS 的 Citrix Workspace 应用程序成功访问 Citrix 资源。

#### 注意：

如果连接时无法验证远程网关的证书 (因为本地密钥库中不包含根证书)，系统会显示一条警告，指出该证书不受信任。如果用户选择忽略该警告而继续进行操作，系统将显示应用程序列表，但应用程序无法启动。

### 手动安装的证书

在 iOS 10.3 及更高版本中，手动安装的配置文件中包含的证书不会自动信任 SSL。在 iOS 中信任手动安装的证书配置文件

1. 请确保您已在设备上安装了证书配置文件。
2. 转至设置 > 常规 > 关于 > 证书信任设置。

通过配置文件安装的每个根证书将在 **Enable Full Trust For Root Certificates** (启用对根证书的完全信任) 下显示。

3. 可以打开或关闭每个根证书。

将根证书导入到 **iPad** 和 **iPhone** 设备中

可以获取证书颁发者的根证书，并通过电子邮件将其发送到设备上已配置的电子邮件帐户。单击附件时，系统会要求您导入根证书。

通配符证书

通配符证书用于代替同一域内任意服务器的各个服务器证书。适用于 iOS 的 Citrix Workspace 应用程序支持通配符证书。

中间证书与 **Citrix Gateway**

您的证书链中包含中间证书时，必须将该中间证书附加到 Citrix Gateway（或 Access Gateway）服务器证书。此外，对于 Access Gateway 安装，请参阅与您的版本匹配的知识库文章：

[CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition（如何将中间证书安装到 Access Gateway Enterprise Edition）](#)

Secure Gateway 配置（仅通过 Web Interface 进行的配置）和所有受支持的 Access Gateway 配置均支持 RSA SecurID 身份验证。

适用于 iOS 的 Citrix Workspace 应用程序支持 Access Gateway 所支持的所有身份验证方法。

联合服务器证书验证策略

适用于 iOS 的 Citrix Workspace 应用程序的各版本具有更加严格的服务器证书验证策略。

#### 重要

安装适用于 iOS 的 Citrix Workspace 应用程序之前，请确认服务器或网关端的证书已按本文所述正确配置。以下情况下连接可能会失败：

- 服务器或网关配置包括错误的根证书
- 服务器或网关配置不包括所有中间证书
- 服务器或网关配置包括过期或无效的中间证书
- 服务器或网关配置包括交叉签名的中间证书

验证服务器证书时，适用于 iOS 的 Citrix Workspace 应用程序现在使用验证服务器证书时服务器（或网关）提供的所有证书。与在早期版本的适用于 iOS 的 Citrix Workspace 应用程序中相同，也会检查证书是否可信。如果证书不全部可信，连接将失败。

与 Web 浏览器中的证书策略相比，此策略更加严格。许多 Web 浏览器都包括大量信任的根证书。

必须为服务器（或网关）配置一组正确的证书。一组不正确的证书可能会导致适用于 iOS 的 Citrix Workspace 应用程序连接失败。

假定为网关配置了以下有效的证书。建议需要更加严格的验证的客户使用此配置，方式是准确确定适用于 iOS 的 Citrix Workspace 应用程序使用的根证书：

- “示例服务器证书”
- “示例中间证书”
- “示例根证书”

然后，适用于 iOS 的 Citrix Workspace 应用程序将检查所有这些证书是否都有效。适用于 iOS 的 Citrix Workspace 应用程序还将检查其是否已信任“示例根证书”。如果适用于 iOS 的 Citrix Workspace 应用程序不信任“示例根证书”，连接将失败。

#### 重要

某些证书颁发机构具有多个根证书。如果您需要使用这一更加严格的验证方法，请确保您的配置使用恰当的根证书。例如，当前存在两个可以验证相同的服务器证书的证书（DigiCert/GTE CyberTrust Global Root 和 DigiCert Baltimore Root/Baltimore CyberTrust Root）。在某些用户设备上，这两个根证书都可用。在其他设备上，只有一个可用（DigiCert Baltimore Root/Baltimore CyberTrust Root）。如果您在网关上配置了 GTE CyberTrust Global Root，则这些用户设备上的适用于 iOS 的 Citrix Workspace 应用程序连接将失败。请参阅证书颁发机构的文档以确定应使用的根证书。另请注意，根证书最终会过期，所有证书也是如此。

之后，适用于 iOS 的 Citrix Workspace 应用程序将使用这两个证书。随后将搜索用户设备上的根证书。如果发现一个正确验证的根证书，并且也可信（例如“示例根证书”），连接将成功。否则，连接将失败。请注意，此配置提供适用于 iOS 的 Citrix Workspace 应用程序所需的中间证书，但是还允许适用于 iOS 的 Citrix Workspace 应用程序选择任何有效的可信根证书。

现在假定为网关配置了以下证书：

- “示例服务器证书”
- “示例中间证书”
- “错误的根证书”

Web 浏览器可能会忽略错误的根证书。但是，适用于 iOS 的 Citrix Workspace 应用程序将不忽略错误的根证书，并且连接将失败。

某些证书颁发机构使用多个中间证书。在这种情况下，通常为网关配置所有中间证书（但不配置根证书），例如：

- “示例服务器证书”
- “示例中间证书 1”
- “示例中间证书 2”

#### 重要

某些证书颁发机构使用交叉签名的中间证书。这专用于存在多个根证书，并且同时仍在使用早期版本的根证书作为较高版本的根证书的情形。在这种情况下，将至少存在两个中间证书。例如，早期版本的根证书“Class 3 Public Primary Certification Authority”具有相应的交叉签名的中间证书“VeriSign Class 3 Public Primary Certification Authority - G5”。但是，相应的较高版本的根证书“VeriSign Class 3 Public Primary Certification Authority - G5”也可用，该版本将替换“Class 3 Public Primary Certification Authority”。更高版本的根证书不使用交叉签名的中间证书。

#### 注意

交叉签名的中间证书和根证书具有相同的使用者名称（颁发对象），但交叉签名的中间证书具有不同的颁发者名称（颁发者）。这一差别将交叉签名的中间证书与普通的中间证书（例如“示例中间证书 2”）区分开来。

通常推荐使用此配置（忽略根证书和交叉签名的中间证书）：

- “示例服务器证书”
- “示例中间证书”

请避免将网关配置为使用交叉签名的中间证书，因为适用于 iOS 的 Citrix Workspace 应用程序将选择更早版本的根证书：

- “示例服务器证书”
- “示例中间证书”
- “示例交叉签名中间证书”[不推荐]

不建议仅为网关配置服务器证书：

- “示例服务器证书”

在此情况下，如果适用于 iOS 的 Citrix Workspace 应用程序找不到所有中间证书，连接将失败。

## 快速入门

November 22, 2019

### 设置

适用于 iOS 的 Citrix Workspace 应用程序支持为您的 Citrix Virtual Apps 部署配置 Web Interface。有两种类型的 Web Interface 站点：XenApp Services 站点和 Citrix Virtual Apps and Desktops 站点。Web Interface 站点使客户端设备能够连接到服务器场。可以使用各种解决方案（包括 Citrix Secure Web Gateway）处理适用于 iOS 的 Citrix Workspace 应用程序与 Web Interface 站点之间的身份验证。

此外，可以对 StoreFront 进行配置，使其为适用于 iOS 的 Citrix Workspace 应用程序提供身份验证和资源交付服务，以便您能够创建集中式企业应用商店，用于向用户交付桌面、应用程序及其他资源。

有关配置连接的详细信息，包括视频、博客和支持论坛，请参阅 <http://community.citrix.com>。

在用户访问 Citrix Virtual Apps and Desktops 部署中托管的应用程序之前，请按如下所述在部署中配置以下组件。

- 在场或站点中发布应用程序时，可以使用以下选项提升用户通过 StoreFront 应用商店访问这些应用程序时的体验：
  - 请务必为已发布的应用程序添加有意义的说明，因为用户可以在适用于 iOS 的 Citrix Workspace 应用程序中看到这些说明。

- 可以通过在适用于 iOS 的 Citrix Workspace 应用程序的“精选”列表中列出应用程序，向移动设备用户重点推荐已发布的应用程序。要填充适用于 iOS 的 Citrix Workspace 应用程序的此列表，请编辑在服务器上发布的应用程序的属性，并将字符串 KEYWORDS:Featured 附加到应用程序说明字段的值后面。
  - 要启用能够对应用程序进行调整使其适应移动设备的屏幕大小的屏幕适应模式，请编辑在服务器上发布的应用程序属性，并将字符串 KEYWORDS:mobile 附加到应用程序说明字段的值后面。此关键字还将为应用程序激活自动滚动功能。
  - 要自动为某个应用商店的所有用户订阅某个应用程序，请将 KEYWORDS:Auto 字符串附加到您在 Citrix Virtual Apps 中发布该应用程序时提供的说明后面。用户登录该应用商店时，相应的应用程序将自动预配，而无需用户手动订阅。
- 如果 Citrix Virtual Apps and Desktops 部署的 Web Interface 没有 Web 站点或 Citrix Virtual Apps and Desktops 站点，请创建一个站点。站点的名称及创建方法取决于已安装的 Web Interface 的版本。有关如何创建其中一个站点的说明，请参阅与您的 [Web Interface](#) 版本相对应的“创建站点”主题。

## 手动设置

一般来说，适用于 iOS 的 Citrix Workspace 应用程序连接到 Citrix Gateway 时，将在通过身份验证后尝试查找 XenApp Services 站点或 Citrix Virtual Apps Web 站点。如果未检测到任何站点，适用于 iOS 的 Citrix Workspace 应用程序将显示一条错误。为避免出现此情况，可以手动配置一个帐户，以便适用于 iOS 的 Citrix Workspace 应用程序能够连接到 Citrix Gateway。

1. 轻按右上角的帐户图标，然后在帐户屏幕中轻按加号 (+)。此时将显示“新建帐户”屏幕。
2. 在屏幕的左下角，依次轻按选项左侧的图标和手动设置。屏幕上将显示其他字段。
3. 在“地址”字段中，键入要连接到的站点或 Citrix Gateway 的安全 URL（例如，agee.mycompany.com）。
4. 选择以下连接选项之一。屏幕上其余的字段将发生变化，具体取决于您所做的选择。
  - Web Interface - 选择此选项后，适用于 iOS 的 Citrix Workspace 应用程序可显示一个与 Web 浏览器类似的 Citrix Virtual Apps Web 站点。此站点又称为 Web View。
  - XenApp Services - 选择此选项后，适用于 iOS 的 Citrix Workspace 应用程序可查找未配置“通过 Citrix Gateway 进行身份验证”的特定 XenApp Services 站点。在此屏幕上显示的其他选项中提供站点登录凭据。
    - <StoreFront FQDN>: 如果存在多个应用商店，系统将显示一个列表，并且用户能够选择要添加的应用商店。
    - <StoreFront FQDN>/citrix/: 这将添加 StoreFront 应用商店。应用商店名称 > 应用商店名称 >
    - <StoreFront FQDN>/citrix/PnAgent/config.xml: 这将添加默认旧 PNAgent 应用商店。
    - <StoreFront FQDN>/citrix//PnAgent/config.xml: 这将添加与关联的旧 PNAgent 应用商店。应用商店名称 > 应用商店名称 >
  - Citrix Gateway - 选择此选项后，适用于 iOS 的 Citrix Workspace 应用程序可通过特定的 Citrix Gateway 连接到 XenApp Services 站点。在此屏幕上显示的其他字段中，请选择服务器版本及其登录凭据，包括进行身份验证时是否需要使用安全令牌。
5. 为确保证书安全，请使用忽略证书警告字段中的设置，以确定即使在具有无效证书、自签名证书或已过期证书的情况下，是否仍要连接到服务器。默认设置为关。

**重要：**如果启用了此选项，请确保您连接到正确的服务器。Citrix 强烈建议所有服务器都具有有效的证书，以保护用户设备免受联机安全攻击。安全服务器使用证书颁发机构颁发的 SSL 证书。Citrix 不支持自签名证书，也不建议绕过证书安全性验证。

6. 轻按“保存”。
7. 键入您的用户名和密码或令牌（如果您选择进行双重身份验证），然后轻按“登录”。此时将显示适用于 iOS 的 Citrix Workspace 应用程序屏幕，在此屏幕中，您可以访问桌面以及添加和打开应用程序。

## StoreFront

**重要：**

- 使用 StoreFront 时，适用于 iOS 的 Citrix Workspace 应用程序支持自 Citrix Access Gateway Enterprise Edition 9.3 至 Citrix Gateway 12 的所有版本。
- 适用于 iOS 的 Citrix Workspace 应用程序仅支持 Web Interface 上的 XenApp Services 站点。
- 适用于 iOS 的 Citrix Workspace 应用程序支持从适用于 Web 的 Workspace 启动会话，前提是 Web 浏览器可用于适用于 Web 的 Workspace。如果无法启动，请直接通过适用于 iOS 的 Citrix Workspace 应用程序配置您的帐户。用户必须使用浏览器的“在 Workspace 中打开”功能手动打开 ICA 文件。有关此部署的限制，请参阅 [StoreFront](#) 文档。

使用 StoreFront 后，您创建的应用商店将由可向适用于 iOS 的 Citrix Workspace 应用程序提供身份验证和资源交付基础结构的各项服务组成。应创建一些应用商店，这些应用商店将枚举 Citrix Virtual Apps and Desktops 站点和 Citrix Virtual Apps 场中的桌面和应用程序，并将这些资源汇集在一起，以提供给用户。

1. 安装并配置 StoreFront。有关详细信息，请参阅 [StoreFront](#) 产品文档。对于需要更大控制权的管理员，Citrix 提供了一个模板，供您用于创建适用于 iOS 的 Citrix Workspace 应用程序下载站点。
2. 为 StoreFront 配置应用商店，方法与为其他 Citrix Virtual Apps and Desktops 应用程序配置应用商店相同。不需要对移动设备进行特殊配置。有关详细信息，请参阅产品文档的“StoreFront”部分中的用户访问选项。对于移动设备，请使用以下方法之一：
  - 预配文件。可以向用户提供包含应用商店连接详细信息的预配文件 (.cr)。安装完成后，用户将打开设备上的预配文件，以自动配置适用于 iOS 的 Citrix Workspace 应用程序。默认情况下，适用于 Web 的 Workspace 站点为用户提供的预配文件仅适用于为其配置站点的单个应用商店。或者，也可以使用 Citrix StoreFront 管理控制台为可手动分发给用户的单个或多个应用商店生成预配文件。
  - 手动配置。可以直接向用户告知访问桌面和应用程序所需的 Citrix Gateway 或应用商店 URL。如果通过 Citrix Gateway 进行连接，用户还需要知道产品版本以及所需的身份验证方法。安装后，用户将这些详细信息键入适用于 iOS 的 Citrix Workspace 应用程序中，该应用程序将尝试验证连接，如果验证成功，将提示用户登录。
  - 自动配置。在“欢迎”屏幕上轻按添加帐户，然后在地址字段中键入 StoreFront 服务器的 URL。帐户的配置将在添加帐户过程中自动执行。

## 配置 Citrix Gateway

如果有用户从外部网络进行连接（例如，用户从 Internet 或远程位置进行连接），请通过 Citrix Gateway 配置身份验证。

- 使用 StoreFront 时，适用于 iOS 的 Citrix Workspace 应用程序支持自 Citrix Access Gateway Enterprise Edition 9.3 至 Citrix Gateway 12 的所有版本。

配置适用于 iOS 的 Citrix Workspace 应用程序以访问应用程序

1. 创建帐户时，如果要使适用于 iOS 的 Citrix Workspace 应用程序配置为自动访问应用程序，请在“地址”字段中键入应用商店的匹配 URL，例如 storefront.organization.com。
2. 使用智能卡进行身份验证时，请选择使用智能卡选项。
3. 对于手动配置（可通过轻按“选项”>“手动设置”进行访问），请继续进行操作，完成其余字段，并选择 Citrix Gateway 身份验证方法，例如，启用安全令牌、选择身份验证类型并保存相关设置。

注意：

登录到应用商店的有效期为一小时。一小时后，用户必须重新登录，以刷新或启动其他应用程序。

## Web Interface

要配置 Web Interface 站点，使用 iPhone 和 iPad 设备的用户可以通过 Web Interface 站点和移动设备上内置的 Safari 浏览器启动应用程序。配置 Web Interface 站点，方法与配置其他 Citrix Virtual Apps 应用程序相同。如果没有为移动设备配置 XenApp Services 站点，则适用于 iOS 的 Citrix Workspace 应用程序会自动使用 Web Interface 站点。不需要对移动设备进行特殊配置。

内置 Safari 浏览器支持 Web Interface 5.x。

在 iOS 设备上启动应用程序

在移动设备上，用户可以使用其常规登录信息和密码登录 Web Interface 站点。

移动设备的自动预配

在 StoreFront 中，可通过执行“导出多应用商店预配文件”和“导出预配文件”任务生成包含应用商店的连接详细信息的文件，包括为应用商店配置的任何 Citrix Gateway 部署和信标。将这些文件提供给用户，以便用户能够利用应用商店的详细信息自动配置适用于 iOS 的 Citrix Workspace 应用程序。用户还可以从适用于 Web 的 Workspace 站点获取适用于 iOS 的 Citrix Workspace 应用程序预配文件。

### 重要：

在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。完成后，请将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Windows“开始”屏幕或“应用程序”屏幕中，找到并单击 Citrix StoreFront 磁贴。在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点。
2. 要生成包含多个应用商店的详细信息的预配文件，请在操作窗格中单击导出多应用商店预配文件，然后选择要包含在此文件中的应用商店。
3. 单击“导出”并使用扩展名.cr 将置备文件保存到网络中的合适位置。

## 用户访问信息

必须向用户提供访问其托管应用程序、桌面和数据所需的适用于 iOS 的 Citrix Workspace 应用程序帐户信息。您可以使用以下方法之一提供此信息：

- 配置基于电子邮件的帐户发现
- 向用户提供预配文件
- 向用户提供需手动输入的帐户信息

### 配置基于电子邮件的帐户发现

可以将适用于 iOS 的 Citrix Workspace 应用程序配置为使用基于电子邮件的帐户发现。配置后，用户在首次安装并配置适用于 iOS 的 Citrix Workspace 应用程序时需要输入自己的电子邮件地址而非服务器 URL。适用于 iOS 的 Citrix Workspace 应用程序将根据域名系统 (DNS) 服务 (SRV) 记录决定与电子邮件地址相关联的是 Access Gateway 或 StoreFront 服务器还是 AppController 虚拟设备，然后提示用户登录以访问自己的托管应用程序、桌面和数据。

### 注意：

如果适用于 iOS 的 Citrix Workspace 应用程序连接到 Web Interface 部署，则不支持基于电子邮件的帐户发现。

### 向用户提供预配文件

您可以使用 StoreFront 来创建包含帐户的连接详细信息的预配文件。将这些文件提供给用户，以使用户能够自动配置适用于 iOS 的 Citrix Workspace 应用程序。安装适用于 iOS 的 Citrix Workspace 应用程序后，用户只需打开设备上的.cr 文件即可配置适用于 iOS 的 Citrix Workspace 应用程序。如果您配置了适用于 Web 的 Workspace 站点，用户还可以从这些站点获取适用于 iOS 的 Citrix Workspace 应用程序预配文件。

有关详细信息，请参阅 [StoreFront](#) 文档。



向用户提供需手动输入的帐户信息

如果为用户提供了要手动输入的帐户详细信息，请确保您分发了以下信息，以使用户能够成功连接到其托管应用程序和桌面：

- 托管资源的 StoreFront URL 或 XenApp Services 站点；例如：`servername.company.com`。
- 对于使用 Citrix Gateway 访问，提供 Citrix Gateway 地址以及所需的身份验证方法。

用户输入新帐户的详细信息时，适用于 iOS 的 Citrix Workspace 应用程序将尝试验证连接。如果验证成功，适用于 iOS 的 Citrix Workspace 应用程序将提示用户登录该帐户。

## 配置

November 22, 2019

### 保存密码

使用 Citrix Web Interface 管理控制台，可以配置身份验证方法以允许用户保存自己的密码。配置用户帐户时，用户首次连接后才会保存加密密码。请注意以下事项：

- 如果启用了密码保存功能，则适用于 iOS 的 Citrix Workspace 应用程序会在设备上存储密码以供将来登录时使用，并且在用户连接到应用程序时不会提示其输入密码。

注意：

仅当用户在创建帐户时输入密码，才会保存该密码。如果没有为该帐户输入密码，则无论服务器设置如何，都不会保存密码。

- 如果禁用了密码保存功能（默认设置），则适用于 iOS 的 Citrix Workspace 应用程序会在用户每次连接时提示其输入密码。

注意：

对于 StoreFront 直接连接，密码保存功能不可用。

### 覆盖保存的密码

如果将服务器配置为保存密码，偏向于在登录时要求输入密码的用户可以覆盖保存的密码：

- 创建帐户时，将密码字段保留为空。
- 编辑帐户时，删除密码并保存帐户。

## 使用保存密码功能

适用于 iOS 的 Citrix Workspace 应用程序具有一项用于通过允许您保存密码来简化连接过程的功能，这样您将不需要在每次打开适用于 iOS 的 Citrix Workspace 应用程序时额外对会话进行身份验证。

### 注意：

保存密码功能当前适用于 PNA 协议。此功能不适用于 StoreFront 本机模式；但是，此功能在 StoreFront 启用了 PNA 旧模式时适用。

## 配置 StoreFront PNA 旧模式

要配置 StoreFront PNA 旧模式以启用保存密码功能，请执行以下操作：

1. 如果要配置现有应用商店，请转至步骤 3。
2. 要配置新 StoreFront 部署，请按照[安装、设置和卸载 Citrix StoreFront](#) 中所述的最佳做法进行操作。
3. 打开 Citrix StoreFront 管理控制台。请确保基本 URL 使用 HTTPS，并且与在生成 SSL 证书时指定的公用名相同。
4. 选择要配置的应用商店。
5. 单击 **Configure XenApp Service Support**（配置 XenApp 服务支持）。
6. 启用 **Legacy Support**（旧版支持），然后单击 **OK**（确定）。
7. 导航到模板配置文件，位置为 `c:\inetpub\wwwroot\Citrix\\Views\PnaConfig\`。
8. 备份 Config.aspx。
9. 打开原始的 Config.aspx 文件。
10. 编辑行 `<EnableSavePassword>false</EnableSavePassword>`，将 **false** 值更改为 **true**。
11. 保存编辑后的 Config.aspx 文件。
12. 在 StoreFront 服务器上，使用管理权限运行 PowerShell。
13. 在 PowerShell 控制台中：
  - a. `cd "c:\Program Files\Citrix\Receiver StoreFront\Scripts"`
  - b. 键入 `"Set-ExecutionPolicy RemoteSigned"`
  - c. 键入 `".\ImportModules.ps1"`
  - d. 键入 `"Set-DSServiceMonitorFeature -ServiceUrl"https://localhost:443/StorefrontMonitor`
14. 如果您有 StoreFront 组，请在该组中的所有成员上运行相同的命令。

## 配置 Citrix Gateway 以保存密码

注意：

此配置使用 Citrix Gateway 负载均衡服务器。

要配置 Citrix Gateway 以支持保存密码功能，请执行以下操作：

1. 登录 Citrix Gateway 管理控制台。
2. 按照 Citrix 最佳做法进行操作，为您的负载均衡虚拟服务器创建一个证书。
3. 在“配置”选项卡上，导航到“流量管理”->“负载均衡”->“服务器”并单击添加。
4. 输入 StoreFront 服务器的服务器名称和 IP 地址。
5. 单击创建。如果您有 StoreFront 组，请对该组中的所有服务器重复执行步骤 5。
6. 在“配置”选项卡上，导航到流量管理 > 负载均衡 > 监视器并单击添加。
7. 输入监视器的名称。选择类型 **STOREFRONT**。在页面底部，选择安全（需要选择此选项，因为 StoreFront 服务器使用 HTTPS）。
8. 单击 **Special Parameters** (特殊参数) 选项卡。输入以前配置的 StoreFront 名称，然后选择 **Check Backed Services** (检查后台服务) 并单击创建。
9. 在配置选项卡上，导航到流量管理 > 负载均衡 > 服务组并单击添加。
10. 输入服务组的名称，然后将协议设置为 **SSL** 并单击确定。
11. 在“高级设置”下的右侧屏幕上，选择设置。
12. 启用“客户端 IP”，然后输入以下标头值：**X-Forwarded-For**，然后单击确定。
13. 在右侧屏幕上（位于“高级设置”下），选择监视器。单击箭头以添加新监视器。
14. 单击添加按钮，然后选择选择监视器下拉列表，此时将显示一个监视器列表（在 Citrix Gateway 上配置的监视器）。
15. 单击以前创建的监视器旁边的单选按钮，单击选择，然后单击绑定。
16. 在右侧屏幕上（位于“高级设置”下），选择 **Members** (成员)。单击箭头以添加新服务组成员。
17. 单击添加按钮，然后选择 **Select Member** (选择成员) 下拉列表。
18. 选中 **Server Based** (基于服务器) 单选按钮，此时将显示服务器成员的列表（在 Citrix Gateway 上配置的服务器成员）。单击之前创建的 StoreFront 服务器旁边的单选按钮。
19. 输入端口号 443，指定唯一的哈希 ID 编号，单击创建，然后单击完成。如果已正确配置所有设置，**Effective State** (有效状态) 应显示一个绿色灯泡，指示监视功能正常运行。
20. 导航到“流量管理”->“负载均衡”->“虚拟服务器”，然后单击添加。输入服务器的名称，然后选择协议 **SSL**。
21. 输入 StoreFront 负载均衡服务器的 IP 地址并单击确定。

22. 选择 **Load Balancing Virtual Server Service Group** (负载均衡虚拟服务器服务组) 绑定, 单击箭头, 然后添加以前创建的服务组。单击确定两次。
23. 分配为负载均衡虚拟服务器创建的 SSL 证书。选择 **No Server Certificate** (无服务器证书)。
24. 从列表中选择负载均衡服务器证书, 然后单击绑定。
25. 将域证书添加到负载均衡服务器。单击 **No CA certificate** (无 CA 证书)。
26. 选择域证书, 然后单击绑定。
27. 在屏幕右侧, 选择 **Persistence** (持久性)。
28. 将“Persistence”(持久性) 更改为 **SOURCEIP** (源 IP), 然后将超时设置为 **20**。单击保存, 然后单击完成。
29. 在域 DNS 服务器上, 添加负载均衡服务器 (如果尚未创建)。
30. 在您的 iOS 设备上启动适用于 iOS 的 Citrix Workspace 应用程序, 然后输入完整的 XenApp URL。

## Content Collaboration Service 集成

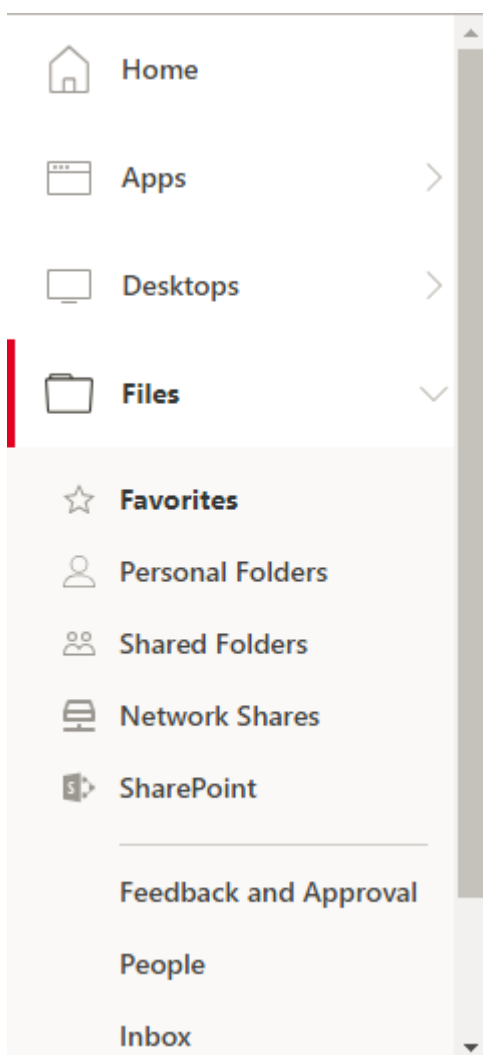
您可以利用 Citrix Content Collaboration 轻松、安全地交换文档、通过电子邮件发送大型文档、安全地处理向第三方的文档传输以及访问协作空间。Citrix Content Collaboration 提供了多种工作方式, 包括基于 Web 的界面、移动客户端、桌面应用程序以及与 Microsoft Outlook 和 Gmail 的集成。

可以使用 Citrix Workspace 应用程序中显示的“文件”选项卡从 Citrix Workspace 应用程序访问 Citrix Content Collaboration 功能。仅当在 Citrix Cloud 控制台中的 Workspace 配置中启用了 Content Collaboration Service 时, 才能看到“文件”选项卡。

### 注意:

Windows Server 2012 和 Windows Server 2016 不支持 Citrix Workspace 应用程序中的 Citrix Content Collaboration 集成, 这是因为操作系统中设置了一个安全选项。

下图显示了全新 Citrix Workspace 应用程序的文件选项卡的内容示例:



#### 限制

- 重置 Citrix Workspace 应用程序不会注销 Citrix Content Collaboration。
- 在 Citrix Workspace 应用程序中切换应用商店不会注销 Citrix Content Collaboration。

### **Citrix Ready Workspace Hub**

满足以下所有系统要求时，可在 Citrix Workspace 应用程序上启用 Citrix Ready Workspace Hub：

- 适用于 iOS 的 Citrix Workspace 应用程序 1810.1 或更高版本
- 启用了蓝牙
- 使用相同 Wi-Fi 网络的移动设备和 Workspace Hub

## 配置

要启用 Citrix Ready Workspace Hub 功能，请转至设置，然后轻按 **Citrix Casting** 即可在设备上启用该功能。有关详细信息，请参阅 [iOS](#) 设备的帮助文档。

## 已知限制

- 在 VDA 7.18 及更低版本上，投射到 Workspace Hub 要求您使用的桌面或其他资源启用了 .h264 全屏策略并禁用旧版图形策略。

## 会话共享

当用户从适用于 iOS 的 Citrix Workspace 应用程序帐户中注销时，如果与应用程序或桌面之间的连接仍然存在，则用户可以选择断开连接或注销：

- 断开连接：从帐户注销，但保留 Windows 应用程序或桌面继续在服务器上运行。用户随后可以启动其他设备，启动适用于 iOS 的 Citrix Workspace 应用程序，以及重新连接到从 iOS 设备断开连接之前的最后一种状态。此选项允许用户从一台设备重新连接到另一台设备，并继续在正在运行的应用程序中工作。
- 注销：从帐户注销，关闭 Windows 应用程序，并从 Citrix Virtual Apps and Desktops 服务器注销。此选项允许用户从服务器断开连接，并注销帐户；用户再次启动适用于 iOS 的 Citrix Workspace 应用程序时，该应用程序将在默认状态下打开。

## 身份验证

November 22, 2019

### 客户端证书身份验证

**重要：**

- 使用 StoreFront 时，适用于 iOS 的 Citrix Workspace 应用程序支持 Citrix Access Gateway Enterprise Edition 版本 9.3 及更高版本以及 NetScaler Gateway 至版本 11。
- 适用于 iOS 的 Citrix Workspace 应用程序支持客户端证书身份验证。
- 只有 Access Gateway Enterprise Edition 9.x 和 10.x（以及后续版本）支持客户端证书身份验证。
- 双来源身份验证类型必须为证书身份验证和 LDAP 身份验证。
- 适用于 iOS 的 Citrix Workspace 应用程序还支持可选的客户端证书身份验证。
- 仅支持 P12 格式的证书。

此外，还可以根据向 Citrix Gateway 虚拟服务器呈现的客户端证书属性对登录此虚拟服务器的用户进行身份验证。也可以将客户端证书身份验证与另一种身份验证类型 LDAP 结合使用，以提供双来源身份验证。

要基于客户端证书属性对用户进行身份验证，应在虚拟服务器上启用客户端身份验证，并申请客户端证书。必须在 Citrix Gateway 上将根证书与虚拟服务器绑定在一起。

用户登录 Citrix Gateway 虚拟服务器并通过身份验证后，将从证书的指定字段中提取用户名和域信息。此信息必须在证书的 **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** 字段中。其格式为“username@domain”。如果成功提取了用户名和域，并且用户提供了必需的其他信息（例如，密码），则用户已通过身份验证。如果用户未提供有效的证书和凭据，或者如果用户名/域提取失败，身份验证将失败。

可以通过将默认身份验证类型设置为使用客户端证书，基于客户端证书对用户进行身份验证。还可以基于客户端 SSL 证书创建一个证书操作，用于定义身份验证过程中要执行的操作。

### 配置 XenApp Services 站点

如果您尚未在 Citrix Virtual Apps 控制台或 Web Interface 控制台（取决于您安装的 Citrix Virtual Apps 版本）中创建 XenApp Services 站点，请为移动设备创建 XenApp Services 站点。

适用于移动设备的适用于 iOS 的 Citrix Workspace 应用程序使用 XenApp Services 站点获取与用户有权访问的应用程序有关的信息，并将这些信息提供给在设备上运行的该应用程序。这与使用 Web Interface 建立传统的基于 SSL 的 Citrix Virtual Apps 连接的方式相似，对于这种连接，可以配置 Citrix Gateway。

为面向移动设备的适用于 iOS 的 Citrix Workspace 应用程序配置 XenApp Services 站点，以支持通过 Citrix Gateway 进行连接。

1. 在 XenApp Services 站点中，选择 **Manage secure client access**（管理安全客户端访问）> **Edit secure client access**（编辑安全客户端访问）设置。
2. 将访问方法改为 Gateway Direct（网关直接）。
3. 输入 Citrix Gateway 设备的 FQDN。
4. 输入 Secure Ticket Authority (STA) 信息。

### 配置 Citrix Gateway 设备

对于客户端证书身份验证，请为 Citrix Gateway 配置使用证书和 LDAP 这两种身份验证策略的双重身份验证方法。

1. 在 Citrix Gateway 上创建会话策略以允许来自适用于 iOS 的 Citrix Workspace 应用程序的传入 Citrix Virtual Apps 连接，并指定新创建的 XenApp Services 站点的位置。
  - 创建一个会话策略来标识该连接来自适用于 iOS 的 Citrix Workspace 应用程序。创建会话策略时，配置以下表达式作为表达式运算符并选择 Match All Expressions（匹配所有表达式）：  

```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace
```
  - 在会话策略关联的配置文件配置中，在 Security（安全）选项卡上，将 Default Authorization（默认授权）设置为 Allow（允许）。

在“Published Applications”（已发布的应用程序）选项卡上，如果不是全局设置（选中了“Override Global”（覆盖全局）复选框），请确保将“ICA Proxy”（ICA 代理）字段设置为“ON”（开）。

在“Web Interface Address”（Web Interface 地址）字段中，键入 URL（其中包含设备用户所使用的 XenApp Services 站点的 config.xml），例如 //XenAppServerName/Citrix/PNAgent/config.xml 或 /XenAppServerName/CustomPath/config.xml。

- 将会话策略绑定到虚拟服务器。
- 为证书身份验证和 LDAP 身份验证创建身份验证策略
- 将身份验证策略绑定到虚拟服务器。
- 将虚拟服务器配置为在 TLS 握手期间请求获取客户端证书，方法为：在 Certificate（证书）选项卡上打开 SSL Parameters（SSL 参数），对于客户端身份验证，应将 Client Certificate（客户端证书）设置为 Mandatory（强制）。

**重要：**

如果 Citrix Gateway 上使用的服务器证书为证书链（含中间证书）的一部分，则确保 Citrix Gateway 上还正确安装了中间证书。有关安装证书的详细信息，请参阅 Citrix Gateway 文档。

## 配置移动设备

如果在 Citrix Gateway 上启用了客户端证书身份验证，则将基于客户端证书的某些属性对用户进行身份验证。成功完成身份验证后，将从证书中提取用户名和域，并应用为该用户指定的所有策略。

1. 从适用于 iOS 的 Citrix Workspace 应用程序打开帐户，并在“服务器”字段中键入 Citrix Gateway 服务器的匹配 FQDN，例如 GatewayClientCertificateServer.organization.com。适用于 iOS 的 Citrix Workspace 应用程序将自动检测是否需要客户端证书。
2. 用户可以安装一个新证书，也可以从已安装的证书列表中选择证书。对于 iOS 客户端证书身份验证，必须只能由适用于 iOS 的 Citrix Workspace 应用程序下载并安装证书。
3. 选择有效的证书后，登录屏幕中的“用户名”和“域”字段已使用证书中的用户名信息预先填充，用户需要键入其余字段，包括密码。
4. 如果将客户端证书身份验证设置为可选，用户可以通过在证书页面上按 Back（返回）跳过证书选项。在此情况下，适用于 iOS 的 Citrix Workspace 应用程序将继续进行连接，并向用户提供登录屏幕。
5. 用户完成初始登录后，无需再次提供证书即可启动应用程序。适用于 iOS 的 Citrix Workspace 应用程序将存储帐户的证书，并自动使用这些证书执行将来的登录请求。

## 智能卡

适用于 iOS 的 Citrix Workspace 应用程序仅支持使用 SITHS 智能卡建立会话中连接。

如果使用 FIPS Citrix Gateway 设备，请将您的系统配置为拒绝 SSL 重新协商。有关详细信息，请参阅 [如何配置 -denySSLReneg 参数](#)。



以下产品和配置受支持：

- 支持的读卡器：
  - Precise Biometrics Tactivo for iPad Mini 固件版本 3.8.0
  - Precise Biometrics Tactivo for iPad（第 4 代）、Tactivo for iPad（第 3 代）以及 iPad 2 固件版本 3.8.0
  - BaiMobile® 301MP 和 301MP-L 智能卡读卡器  
受支持的 VDA 智能卡中间件
  - ActivIdentity
- 支持的智能卡：
  - PIV 卡
  - 通用访问卡 (CAC)
- 支持的配置：
  - 通过智能卡身份验证登录配置了 StoreFront 2.x 的 Citrix Gateway 以及 XenDesktop 7.x 或更高版本或者 XenApp 6.5 或更高版本

## RSA SecurID 身份验证

Secure Web Gateway 配置（仅通过 Web Interface 进行的配置）和所有 Citrix Gateway 配置均支持适用于 iOS 的 Citrix Workspace 应用程序的 RSA SecurID 身份验证。

适用于 **iOS** 的 **Citrix Workspace** 应用程序上软件令牌所需的 **URL** 方案：适用于 iOS 的 Citrix Workspace 应用程序使用的 RSA SecurID 软件令牌仅注册了 URL 方案 com.citrix.securid。

如果用户在自己的 iOS 设备上同时安装了适用于 iOS 的 Citrix Workspace 应用程序和 RSA SecurID 应用程序，则必须选择 URL 方案 com.citrix.securid，以将 RSA SecurID Software Authenticator（软件令牌）导入到其设备上的适用于 iOS 的 Citrix Workspace 应用程序中。

## 导入 RSA SecurID 软令牌

要对适用于 iOS 的 Citrix Workspace 应用程序使用 RSA 软令牌，请要求您的用户按照以下过程进行操作。

PIN 长度、PIN 类型（仅限数字、字母数字）以及 PIN 重用限制的策略在 RSA 管理服务器上指定。

您的用户仅需要在成功对 RSA 服务器进行身份验证后立即执行此操作。您的用户验证其 PIN 后，还将通过 StoreFront 服务器进行身份验证，该服务器将显示可用的已发布应用程序和桌面。

## 使用 RSA 软令牌

1. 导入贵组织向您提供的 RSA 软令牌。
2. 在附加了 SecurID 文件的电子邮件中，选择 **Open in Workspace**（在 Workspace 中打开）作为导入目标位置。导入软令牌后，适用于 iOS 的 Citrix Workspace 应用程序将自动打开。

3. 如果贵组织提供了密码以完成导入，请输入贵组织向您提供的密码，然后单击确定。单击确定后，系统将显示一条消息，提示您令牌已成功导入。
4. 关闭导入消息，然后在适用于 iOS 的 Citrix Workspace 应用程序中单击添加帐户。
5. 输入贵组织提供的应用商店的 URL 并单击下一步。
6. 在“登录”屏幕上，输入您的凭据：用户名、密码和域。对于“PIN”字段，除非贵组织向您提供了不同的默认 PIN，否则，请输入 **0000**。（PIN 0000 是 RSA 的默认值，但贵组织可能会更改该值，使其遵从安全策略。）
7. 单击左上角的登录。单击登录后，系统将提示您创建一个新 PIN。
8. 输入一个 4 到 8 位数字的 PIN，然后单击确定。
9. 系统随后将提示您验证新 PIN。重新输入您的 PIN，然后单击确定。单击“确定”后，您将能够访问自己的应用程序和桌面。

#### 下一个令牌代码

如果您将 Citrix Gateway 配置为进行 RSA SecurID 身份验证，适用于 iOS 的 Citrix Workspace 应用程序将支持下一个令牌代码。启用此功能后，如果用户输入三次（默认）错误密码，Citrix Gateway 插件将提示用户等到下一个令牌激活才能登录。可将 RSA 服务器配置为在用户使用错误密码登录次数过多时，禁用该用户帐户。

#### 派生凭据

支持在适用于 iOS 的 Citrix Workspace 应用程序中使用 Purebred 派生凭据。连接到允许使用派生凭据的应用商店时，用户可以使用虚拟智能卡登录适用于 iOS 的 Citrix Workspace 应用程序。仅本地部署支持此功能。

##### 注意：

要使用此功能，需要运行 Citrix Virtual Apps and Desktops 7 1808 或更高版本。

要在适用于 iOS 的 Citrix Workspace 应用程序中启用派生凭据，请执行以下操作：

1. 转至设置 > 高级 > 派生凭据。
2. 轻按使用派生凭据。

然后，创建虚拟智能卡以与派生凭据结合使用：

1. 在设置 > 高级 > 派生凭据中，轻按 **Add New Virtual Smart Card**（添加新虚拟智能卡）。
2. 编辑虚拟智能卡的名称。
3. 输入 8 位仅限数字的 PIN 并进行确认。
4. 轻按下一步。
5. 在“身份验证证书”下方，轻按导入证书...
6. 此时将显示文档选取器。轻按浏览。
7. 在“位置”下方，选择 **Purebred Key Chain**（Purebred 钥匙串）。
8. 从列表中选择所需的身份验证证书。

9. 轻按导入密钥。
10. 如果需要，对数字签名证书和加密证书重复执行步骤 5-9。
11. 轻按保存。

最多可以为虚拟智能卡导入三个证书。需要身份验证证书，虚拟智能卡才能正确运行。可以添加加密证书和数字签名证书以在 VDA 会话内部使用。

**注意：**

连接到 HDX 会话时，创建的虚拟智能卡会重定向到该会话。

#### 已知限制

- 用户一次只能有一个活动卡。
- 虚拟智能卡创建后不能编辑。要更改虚拟智能卡，用户必须删除该卡，然后创建新卡。
- 最多可以输入 10 次无效 PIN。在第 10 次尝试后，虚拟智能卡将被删除。
- 选择了派生凭据后，当某个会话中需要智能卡时，虚拟智能卡将覆盖物理智能卡。

## 安全

November 22, 2019

要保护服务器场与适用于 iOS 的 Citrix Workspace 应用程序之间的通信安全，可以将与服务器场建立的连接与一系列的安全技术（包括 Citrix Gateway）集成在一起。

**注意：**

Citrix 建议使用 Citrix Gateway 以保护 StoreFront 服务器与用户设备之间的通信安全。

- SOCKS 代理服务器或安全代理服务器（也称为安全代理服务器、HTTPS 代理服务器）。可以使用代理服务器来限制网络的入站和出站访问，并处理适用于 iOS 的 Citrix Workspace 应用程序与服务器之间的连接。适用于 iOS 的 Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。
- Secure Web Gateway。您可以结合使用 Secure Web Gateway 和 Web Interface，通过 Internet 为企业内部网络中的服务器提供单一、安全的加密访问点。
- 采用传输层安全性 (TLS) 协议的 SSL Relay 解决方案。
- 防火墙。网络防火墙可以根据目标地址和端口允许或阻止数据包通过。在使用适用于 iOS 的 Citrix Workspace 应用程序时，如果要经过将服务器内部网络 IP 地址映射到外部 Internet 地址（即网络地址转换，或 NAT）的网络防火墙，则应配置外部地址。

## Citrix Gateway

要使远程用户能够通过 Citrix Gateway 连接到您的 Citrix Endpoint Management 部署，可以将证书配置为与 StoreFront 配合使用。启用访问权限的方法取决于部署中使用的 Citrix Endpoint Management 版本。

如果在网络中部署 Citrix Endpoint Management，应通过将 Citrix Gateway 与 StoreFront 相集成的方式来允许内部用户或远程用户通过 Citrix Gateway 与 StoreFront 建立连接。这种部署方法允许用户连接 StoreFront，从而通过 XenApp 访问已发布的应用程序，通过 XenDesktop 访问虚拟桌面。用户通过适用于 iOS 的 Citrix Workspace 应用程序进行连接。

## Secure Web Gateway

本主题仅适用于使用 Web Interface 的部署。

可以在普通模式或中继模式下使用 Secure Web Gateway，来为适用于 iOS 的 Citrix Workspace 应用程序与服务 器之间的通信提供安全通道。如果在普通模式下使用 Secure Web Gateway，并且用户通过 Web Interface 进行连接，则不需要配置适用于 iOS 的 Citrix Workspace 应用程序。

适用于 iOS 的 Citrix Workspace 应用程序使用在 Web Interface 服务器上远程配置的设置连接到运行 Secure Web Gateway 的服务器。

如果安全网络中的服务器上安装了 Secure Web Gateway 代理，则可以在中继模式下使用 Secure Web Gateway 代理。如果使用中继模式，Secure Web Gateway 服务器将相当于一个代理，并且必须配置适用于 iOS 的 Citrix Workspace 应用程序才能使用：

- Secure Web Gateway 服务器的完全限定的域名 (FQDN)。
- Secure Web Gateway 服务器的端口号。请注意，Secure Web Gateway 版本 2.0 不支持中继模式。

FQDN 必须按顺序列出以下三个组成部分：

- 主机名
- 中间域
- 顶级域

例如，my\_computer.my\_company.com 是一个 FQDN，因为它依次列出主机名 (my\_computer)、中间域 (example) 和顶级域 (com)。中间域和顶级域的组合 (example.com) 通常称为“域名”。

## 代理服务器

代理服务器用于限制网络的入站和出站访问，并处理适用于 iOS 的 Citrix Workspace 应用程序与服务器之间的连接。适用于 iOS 的 Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。

与 Citrix Virtual Apps and Desktops 服务器通信时，适用于 iOS 的 Citrix Workspace 应用程序使用在 Web Interface 服务器上远程配置的代理服务器设置。

在与 Web 服务器进行通信时，适用于 iOS 的 Citrix Workspace 应用程序使用在用户设备上为默认 Web 浏览器配置的代理服务器设置。您必须相应地在用户设备上为默认 Web 浏览器配置代理服务器设置。

## 防火墙

网络防火墙可以根据目标地址和端口允许或阻止数据包通过。如果在部署中使用防火墙，则适用于 iOS 的 Citrix Workspace 应用程序必须能够经由防火墙与 Web 服务器和 Citrix 服务器通信。对于用户设备到 Web 服务器的通信，防火墙必须允许 HTTP 流量（如果正在使用安全 Web 服务器，则通常通过标准 HTTP 端口 80 或 443 传输流量）。对于 Citrix 服务器通信，防火墙必须允许在端口 1494 和 2598 上进行入站 ICA 通信。

如果为防火墙配置了网络地址转换 (NAT)，您可以使用 Web Interface 定义从内部地址到外部地址的映射和端口。例如，如果没有为 Citrix Virtual Apps and Desktops 服务器配置备选地址，则可以将 Web Interface 配置为向适用于 iOS 的 Citrix Workspace 应用程序提供备选地址。然后，适用于 iOS 的 Citrix Workspace 应用程序使用外部地址和端口号连接服务器。

## TLS

适用于 iOS 的 Citrix Workspace 应用程序支持与 XenApp/XenDesktop 的 TLS 连接使用 TLS 1.0、1.1 和 1.2 及以下密码套件：

- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

注意：

iOS 9 及更高版本上运行的适用于 iOS 的 Citrix Workspace 应用程序不支持以下 TLS 密码套件：

- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5

传输层安全性 (TLS) 是 TLS 协议的最新标准化版本。互联网工程工作小组 (IETF) 在接管 TLS 开放式标准的开发任务后，将其更名为 TLS。

TLS 通过提供服务器身份验证、数据流加密和消息完整性检查，来保障数据通信的安全。有些组织（包括美国政府组织）要求使用 TLS 来保障数据通信的安全。这些组织可能还要求使用验证的加密，例如联邦信息处理标准 (FIPS) 140。FIPS 140 是一个加密标准。

适用于 iOS 的 Citrix Workspace 应用程序支持 1024、2048 和 3072 位长度的 RSA 密钥。此外，还支持 RSA 密钥长度为 4096 位的根证书。

**注意：**

适用于 iOS 的 Citrix Workspace 应用程序对适用于 iOS 的 Citrix Workspace 应用程序与 StoreFront 之间的连接使用平台 (iOS) 加密。

## 配置并启用 TLS

TLS 的设置主要涉及两个步骤：

1. 在 Citrix Virtual Apps and Desktops 服务器和 Web Interface 服务器上设置 SSL Relay，以及获取并安装所需的服务器证书。
2. 在用户设备上安装等效根证书。

### 在用户设备上安装根证书

在启用了 TLS 的适用于 iOS 的 Citrix Workspace 应用程序与 Citrix Virtual Apps and Desktops 之间，如果要使用 TLS 来保护通信安全，用户设备上需要有可以验证服务器证书上的证书颁发机构签名的根证书。

iOS 附带了约 100 个预安装的商用根证书，如果您要使用其他证书，可以从证书颁发机构获得证书并将其安装在每个用户设备上。

有时候，您可能需要亲自在每个用户设备上安装根证书，而不是让用户进行安装，这要取决于所在组织的策略和规程。最方便和最安全的方法是将根证书添加到 iOS 钥匙串中。

### 将根证书添加到钥匙串中

1. 向您自己发送一封包含证书文件的电子邮件。
2. 在设备上打开证书文件。这会启动“钥匙串访问”应用程序。
3. 按照提示进行操作，添加证书。
4. 自 iOS 10 起，请通过转至 iOS 的“设置”>“关于”>“证书信任设置”来验证证书是否可信。在“证书信任设置”下，查看“针对根证书启用完全信任”部分。请确保您的证书已被选定为接受完全信任。

根证书安装完毕，可供启用了 TLS 的客户端和使用 TLS 的其他应用程序使用。

## XenApp Services 站点

要配置 XenApp Services 站点，请执行以下操作：

**重要：**

- 使用 XenApp Services 站点的适用于 iOS 的 Citrix Workspace 应用程序支持 Citrix Secure Gateway 3.x。
- 使用 Citrix Virtual Apps Web 站点的适用于 iOS 的 Citrix Workspace 应用程序支持 Citrix Secure

Gateway 3.x。

- 在 XenApp Services 站点上仅支持单重身份验证方法，在 Citrix Virtual Apps Web 站点上同时支持单重和双重身份验证方法。
- 必须使用 Web Interface 5.4，该版本受所有内置浏览器支持。

在开始此配置之前，安装并配置要与 Web Interface 一起运行的 Citrix Gateway。您可以修改这些指令来适合您的具体环境。

如果使用 Citrix Secure Gateway 连接，则不要在适用于 iOS 的 Citrix Workspace 应用程序上配置 Citrix Gateway 设置。

适用于 iOS 的 Citrix Workspace 应用程序使用 XenApp Services 站点获取与用户有权访问的应用程序有关的信息，并将这些信息提供给在设备上运行的适用于 iOS 的 Citrix Workspace 应用程序。这与使用 Web Interface 建立传统的基于 SSL 的 Citrix Virtual Apps 连接的方式相似，对于这种连接，可以配置 Citrix Gateway。在 Web Interface 5.x 上运行的 XenApp Services 站点内置了此配置功能。

将 XenApp Services 站点配置为支持通过 Citrix Secure Gateway 进行的连接：

1. 在 XenApp Services 站点中，选择 Manage secure client access（管理安全客户端访问）> Edit secure client access（编辑安全客户端访问）设置。
2. 将访问方法改为 Gateway Direct（网关直接）。
3. 输入 Secure Web Gateway 的 FQDN。
4. 输入 Secure Ticket Authority (STA) 信息。

注意：

对于 Citrix Secure Gateway，Citrix 建议为该站点使用 Citrix 默认路径 (//XenAppServerName/Citrix/PNAgent)。用户可以利用默认路径指定自己连接的 Secure Web Gateway 的 FQDN，而不必指定驻留在 XenApp Services 站点上的 config.xml 文件的完整路径（例如 //XenAppServerName/CustomPath/config.xml）。

## 配置 Citrix Secure Gateway

1. 在 Citrix Secure Gateway 上，使用“Citrix Secure Gateway Configuration”（Citrix Secure Gateway 配置）向导将 Citrix Secure Gateway 配置为使用托管 XenApp Services 站点的安全网络中的服务器。选择“Indirect”（间接）选项后，输入 Secure Web Gateway 服务器的 FQDN 路径，并继续执行向导步骤。
2. 测试与用户设备之间的连接，以验证是否已针对网络连接和证书分配正确配置了 Secure Web Gateway。

### 配置移动设备

1. 添加 Citrix Secure Gateway 帐户时，请在地址字段中输入 Secure Gateway 服务器的匹配 FQDN：
  - 如果使用默认路径 (/Citrix/PNAgent) 创建了 XenApp Services 站点，请输入 Secure Web Gateway 的 FQDN: FQDNofSecureGateway.companyName.com
  - 如果自定义了 XenApp Services 站点路径，请输入 config.xml 文件的完整路径，例如: FQDNofSecureGateway.companyName.com/CustomPath/config.xml

2. 如果要手动配置帐户，请关闭 Citrix Gateway 选项新建帐户对话框。

## 故障排除

November 22, 2019

### **App Switcher** 不运行

应用程序必须由 IT 管理员在同一个服务器上发布。否则，应用程序切换将不起作用。

#### 应用程序在多个会话中打开

即使已启用应用程序共享功能，也可能会出现此服务器端问题。此问题偶尔出现，且没有解决方法。

#### 会话断开连接

用户可以通过以下方式从适用于 iOS 的 Citrix Workspace 应用程序会话中断开连接（但不注销）：

- 在会话中查看已发布的应用程序或桌面过程中：
  - 轻按屏幕顶部的箭头可显示会话中下拉菜单。
  - 轻按主页按钮可返回到启动盘。
  - 请注意仍在活动会话中的其中一个已发布应用程序的图标下方的白色阴影；轻按该图标。
  - 轻按“断开连接”。
- 关闭适用于 iOS 的 Citrix Workspace 应用程序：
  - 双击设备的主页按钮。
  - 在 iOS 应用程序切换器视图中找到适用于 iOS 的 Citrix Workspace 应用程序。
  - 在显示的对话框中轻按“断开连接”。
- 按其移动设备上的主页按钮。
- 轻按应用程序下拉菜单中的主页或切换。

会话会保持断开连接状态。虽然用户可以稍后重新连接，但您仍然可以确保断开连接的会话在特定时间间隔之后呈现非活动状态。为此，请在远程桌面会话主机配置（以前称为“终端服务配置”）中为 ICA-tcp 连接配置会话超时。有关配置远程桌面服务（以前称为“终端服务”）的详细信息，请参阅 Microsoft Windows Server 产品文档。

#### 密码过期

适用于 iOS 的 Citrix Workspace 应用程序为用户提供更改过期密码的功能。系统会提示用户输入所需的信息。



## 已越狱的设备

如果您的用户通过越狱 iOS 设备进行连接，则会危及部署安全。越狱设备是指所有者修改过的设备，这些设备通常能够绕过某些安全保护。

适用于 iOS 的 Citrix Workspace 应用程序检测到越狱 iOS 设备时，将向用户显示警报。要进一步帮助确保您的环境安全，可以将 StoreFront 或 Web Interface 配置为帮助阻止越狱设备运行应用程序。

### 要求

- Citrix Receiver for iOS 6.1 或更高版本
- StoreFront 3.0 或 Web Interface 5.4 或更高版本
- 通过管理员帐户访问 StoreFront 或 Web Interface

### 帮助阻止检测到的越狱设备运行应用程序

1. 以具有管理员权限的用户身份登录您的 StoreFront 或 Web Interface 服务器。
2. 找到文件 default.ica，该文件位于以下位置之一：
  - **C:\inetpub\wwwroot\Citrix\storename\conf** (Microsoft Internet Information Services)
  - **C:\inetpub\wwwroot\Citrix\storename\App\_Data** (Microsoft Internet Information Services)
  - **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)
3. 在 **[Application]** 部分下，添加以下内容：**AllowJailBrokenDevices=OFF**
4. 保存该文件并重新启动您的 StoreFront 或 Web Interface 服务器。

重新启动 StoreFront 服务器后，看到了与越狱设备有关的警报的用户将无法从您的 StoreFront 或 Web Interface 服务器启动应用程序。

### 允许检测到的越狱设备运行应用程序

如果未设置 AllowJailBrokenDevices，则默认设置为向越狱设备的用户显示警报，但仍允许其启动应用程序。

如果要明确允许您的用户在越狱设备上运行应用程序，请执行以下操作：

1. 以具有管理员权限的用户身份登录您的 StoreFront 或 Web Interface 服务器。
2. 找到文件 default.ica，该文件位于以下位置之一：
  - **C:\inetpub\wwwroot\Citrix\storename\conf** (Microsoft Internet Information Services)
  - **C:\inetpub\wwwroot\Citrix\storename\App\_Data** (Microsoft Internet Information Services)

- `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)

3. 在 **[Application]** 部分下，添加以下内容：**AllowJailBrokenDevices=ON**

4. 保存该文件并重新启动您的 StoreFront 或 Web Interface 服务器。

将 AllowJailBrokenDevices 设置为 ON 时，您的用户将看到与使用已越狱的设备有关的警报，但其能够通过 StoreFront 或 Web Interface 运行应用程序。

## HDX 音频质量损失

在 Citrix Virtual Apps and Desktops 中，使用音频加视频时，适用于 iOS 的 Citrix Workspace 应用程序的 HDX 音频可能会损失质量。Citrix Virtual Apps and Desktops HDX 策略无法处理视频数据和音频数据量时将发生此问题。有关如何创建策略以提高音频质量方面的建议，请参阅知识中心文章 [CTX123543](#)。

可以从 **Citrix Cloud** 获取演示帐户

当前没有帐户的用户可以在 Citrix Cloud 演示站点 <http://cloud.citrix.com/> 上创建一个演示用户帐户。

用户可以通过 Citrix Cloud 体验到 Citrix 解决方案的强大功能，而无需设置和配置他们自己的环境。Citrix Cloud 演示环境使用一定数量的 Citrix 关键解决方案，其中包括 Citrix Virtual Apps and Desktops 和 Citrix Gateway。

但是，在此演示环境中，数据不会被保存，并且断开连接后，您可能无法返回到会话。

## 数字键

如果用户在已发布的应用程序中遇到数字键无法正常使用的问题，可以尝试在适用于 iOS 的 Citrix Workspace 应用程序中禁用 Unicode 键盘。要执行此操作，请轻按“设置”选项卡中的键盘选项，对于“使用 Unicode 键盘”，请将开关切换到关。

## 连接速度缓慢

如果您连接到 XenApp Services 站点时速度非常缓慢，或者遇到应用程序图标丢失或系统显示“Protocol Driver Error”（协议驱动程序错误）消息等问题，可以通过以下方法解决问题：在 Citrix Virtual Apps 服务器和 Citrix Secure Web Gateway 或 Web Interface 服务器上，对网络接口禁用以下 Citrix PV 以太网适配器属性（默认情况下均处于启用状态）：

- 大量发送卸载
- 卸载 IP 校验和
- 卸载 TCP 校验和
- 卸载 UDP 校验和

无需重新启动服务器。上述解决方法适用于 Windows Server 2003 和 Windows Server 2008 32 位操作系统。Windows Server 2008 R2 不受此问题影响。



**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

© 2019 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).