关于 Citrix Receiver for iOS 6

Jul 13, 2016

本文包含的内容

6.1.5 中的新增功能

净推荐值 (Net Promoter Score, NPS) 增强功能

本版本中已包含 iOS Receiver NPS 功能的增强功能。 Citrix Receiver for iOS 现在会在用户从 Apple App Store 下载此应用程序时提示用户对其体验评分。 这会向 Citrix 提供最终用户反馈以促使其持续开发产品。

支持拆分视图

本版本的 iOS Receiver 引入了对 iPad 和 iPad Pro 设备中的新拆分视图功能的支持。 使用拆分视图，Citrix Receiver for iOS 将允许您同时打开两个应用程序并且并排显示。 此功能通过允许您在与 XenApp 或 XenDesktop 结合使用时，使用自己的 iPad 设备作为独立桌面替换方案来帮助提高工作人员的工作效率，特别是与其他外围设备（例如软键盘、X1 鼠标或 Apple Pencil）结合使用时。

本版本中的其他改进功能

本版本包括以下附加改进功能和增强功能：

- 支持在会话中使用 SITHS 智能卡
- 能够在添加应用商店之前启用“保持唤醒”选项（该选项阻止 iPad 进入睡眠模式）
- 增加了对 WebFront 的支持（适用于未经身份验证的 StoreFront）

> **注意**
>
> Citrix Receiver for iOS 6.1.5 适用于 iOS 9.3。

6.1 中的新增功能

支持 iOS 9。

iOS 设备被越狱时发出警报，并允许您阻止越狱设备通过 StoreFront 或 Web Interface 运行应用程序。 可以阅读以下文章，了解这一新增功能的更多相关信息：阻止越狱设备。

Citrix Receiver for iOS 6.1.1 和 6.1.2 中除了包含 6.1.0 中的新增功能外，不包含任何其他新增功能，但包括问题的修复。

Citrix Receiver for iOS 6.1.3 维护版本提供多种增强功能和修复，包括：

- iPad Pro 兼容性增强功能，同时支持 iPad Pro 的完整屏幕键盘。
- iOS Spotlight 搜索已发布的应用程序内容；通过此功能，您能够使用 Spotlight 搜索机制搜索已发布的应用程序和桌面。
- X1 鼠标速度控制；使用 Citrix Receiver 中的设置可自定义 X1 鼠标的速度。

Citrix Receiver for iOS 6.1.4 维护版本解决了以下问题：
- 修复了 NetScaler 策略存在的身份验证问题。 [#616573]
- 解决了断开会话连接时出现的与意外崩溃有关的问题。 [#616611]

> **注意**
>
> 有关版本 6.1.0（及更高版本）中存在的与修复有关的信息，请参阅本文后面的“已修复的问题”列表。

6.0 中的新增功能

本版本支持 Framehawk 虚拟通道，这是新 ICA 虚拟通道，扩展了 Citrix HDX 技术以改进使用经常出现数据包丢失和延迟问题的宽带无线连接时的用户体验。有关详细信息，请参阅 XenApp 7.6 和 XenDesktop 7.6 中的新增功能。使用 Framehawk 功能时：

- 必须启用通用网关协议 (CGP)。
- 在模板 ICA 文件中，添加 Framehawk=yes。

尽管启用了 CGP 以连接到 Framehawk 会话，会话可靠性仍不可用。

Receiver for iOS 6.0 现在包括 iOS 8 SDK 中内置的 64 位支持，随附在 Xcode 6 或更高版本中。使用此功能时请注意以下事项：包含 Apple A7 和 Apple A8 芯片的 iOS 设备包含 64 位芯片，其中包括：

- iPhone 5S 或更高版本
- iPad Air 或更高版本
- iPad Mini 2 或更高版本

6.1.5 中已修复的问题

- 修复了应用程序无法启动的问题。
- 多项附加测试案例用于验证完整性
- 捕获了其他指标以改进用户体验

6.1.4 中已修复的问题

- 修复了 NetScaler 策略存在的身份验证问题。 [#616573]
- 解决了断开会话连接时出现的与意外崩溃有关的问题。 [#616611]

6.1.3 中已修复的问题

- 修复了与时区有关的问题。
- 修复了与会话崩溃有关的多个问题。

6.1.2 中已修复的问题

- 修复了用户在手动注销后或者会话达到空闲超时时无法重新登录其帐户的问题。
  [#600659]
- 改进了 RSA 令牌身份验证工作流，以便系统不会两次提示用户输入其令牌。
  [#597857]
- 修复了阻止用户在使用 NetScaler 11.0 作为网关时对其应用商店进行身份验证的兼容性问题。
  [#558212]
- 解决了与 iPad Pro 屏幕分辨率有关的问题。

6.1.1 中已修复的问题

- 修复了证书中的公用名是其 IP 地址时，Citrix Receiver 通过 Netscaler Gateway 登录帐户失败的问题。
  [#594157]
- 修复了添加帐户后 Citrix Receiver 持续显示“请稍候...”的问题。
  [#595978]
- 修复了日志记录级别设置为“调试”时，轻按“请求技术支持人员提供帮助”后 Citrix Receiver 崩溃的问题。
  [#595980]
- 修复了应用程序在重新启动后崩溃的问题。
  [#596993]

6.1 中已修复的问题

- 修复了 Citrix Receiver 不识别部分智能卡证书的问题。
  [#587428]
- 修复了与连接或漫游到 Linux VDA 会话有关的问题。
  [#558369]
- 常规软令牌和客户端证书改进功能。
  [#586361]

我们修复了与在 iOS 9 上使用有关的问题：

- 使用蓝牙键盘时，键盘扩展坞的位置不正确。

[#579307]

- 新 iOS 9 撤消和恢复按钮不完全起作用。
  [#579318]
- 使用蓝牙键盘时，Citrix X1 鼠标单击的焦点不在文本字段上。相反，需要轻按文本字段。
  [#579362]
- 在会话中打开或关闭“使用 Unicode 键盘”按钮后键盘显示不正常。
  [#579496]
- 在横向模式下，扩展键列表和 Citrix 键盘重叠。
  [#580117]
- 旋转设备后，应用程序切换器不正常地显示预览。
  [#580980]
- 从键盘使用 Siri 语音输入时，会话无响应。
  [#582046]

6.0.1 中已修复的问题

- 修复了启动无缝应用程序时 Receiver 崩溃的问题。
  [#584383]
- 您现在不需要创建帐户即可访问 Citrix X1 鼠标设置。
  [#587422]
- 修复了 Receiver 无法读取 RSA 软令牌的问题。
  [#587423]
- 修复了使用 Web 前端时无法通过 NetScaler 添加 StoreFront 帐户的问题。
  [#587426]
- 修复了智能卡无法识别证书的问题。
  [#587428]

6.1.1 中的已知问题

- 设置新密码时，显示“凭据不正确”错误。尽管显示此错误消息，新密码仍正确设置。此错误消息可以忽略。请在下一次登录过程中使用新密码。[#70576123]

6.1 中的已知问题

- 注销后，Citrix Receiver 可能无法通过 NetScaler Gateway 使用智能卡启动会话。
  [#586984]
- 使用智能卡注销会话后，您可能会看到连接失败错误。
  [#577175]
- 发送通过智能卡证书加密的电子邮件时，Citrix Receiver 无法读取智能卡。
  [#587869]
- 通过 NetScaler Gateway 手动添加 StoreFront 帐户时，Citrix Receiver 提示错误。
  [#590576]

在 iOS 9 上运行 6.0 和 6.0.1 的已知问题

如果在 iOS 9 上运行 Citrix Receiver for iOS 6.0 或 6.0.1，可能会遇到以下问题：

- 使用蓝牙键盘时，键盘扩展坞的位置不正确。
  [#579307]
- 新 iOS 9 撤消和恢复按钮不完全起作用。
  [#579318]
- 使用蓝牙键盘时，Citrix X1 鼠标单击的焦点不在文本字段上。相反，需要轻按文本字段。
  [#579362]
- 在会话中打开或关闭“使用 Unicode 键盘”按钮后键盘显示不正常。
  [#579496]
- 在横向模式下，扩展键列表和 Citrix 键盘重叠。
  [#580117]
- 旋转设备后，应用程序切换器不正常地显示预览。
  [#580980]
- 从键盘使用 Siri 语音输入时，会话无响应。
  [#582046]

6.0 中的其他已知问题

- 使用 CMP 应用程序时，将 Receiver 设置为使用固定分辨率会导致会话分辨率不正确。要解决此问题，请在配置屏幕分辨率时使用自动适应屏幕。
  [#574443]
- 使用智能卡进行身份验证时，Receiver 无法正常注销会话；注销后，无论注销是否成功，桌面都显示处于活动状态。
  [#577175]
- 将屏幕设置为固定分辨率时，鼠标光标可能会在屏幕边界外部移动。
  [#578081]
- 如果在应用了某些图形策略的情况下使用 NetScaler 直通，Receiver 可能会在播放 1080p 视频时断开会话连接。
  [#569392]
- 在某些应用了“Framehawk 虚拟通道”策略的情况下，使用 Shift 键执行某些键盘序列时，会话可能会呈现较差的性能；这会影响以下字符: %、#、:、!、?。要解决此问题，Citrix 建议您断开连接后重新连接会话。
  [#570236]
- 使用智能卡身份验证时，Receiver 可能无法正确显示在注销后请求输入用户的 PIN 的登录屏幕。此外，注销后添加喜爱的应用程序失败；Receiver 显示一条错误，指出由于用户“无法登录”而无法重新启动会话。
  [#555804, #556580]
- Receiver 可能无法重新连接到 Linux VDA 会话。
  [#558369]
- 在本地化的中文环境中，在应用程序列表搜索区域中插入某些符号（“{”或“}”）时，Receiver 可能会崩溃。
  [#578322]

Citrix Receiver for iOS 6 系统要求

Jan 29, 2016

在本文中：

设备要求

- Citrix Receiver for iOS 6.1、6.1.1 和 6.1.2 支持 iOS 7、8 和 9。
- Citrix Receiver for iOS 6.0 和 6.0.1 支持 iOS 7、8 和 9（有问题）。
- 此软件更新在以下设备上受支持：
  - iPhone 4、4S、5、5c、5s、6、6 Plus、6s 和 6s Plus。
  - 所有 iPad 型号（包括 iPad Pro）。对 iPad Pro 的支持不包括：
    - Apple Pencil
    - 分割视图
    - 本机软键盘
  - 第五代 iPod Touch。
- 外部显示器支持
  - iPhone - 受设备的 iOS 支持。
  - iPad - 与 iOS 支持的对象相同（不使用整个屏幕）。

> ### Important
>
> 有关安全连接到 Citrix 环境的信息，请参阅连接和身份验证（下文）。
>
> 有关在 iOS 9 上运行 Citrix Receiver 6.0 和 6.0.1 的问题的信息，请参阅支持 iOS 9。

服务器要求

请务必为服务器安装所有最新的修补程序。

- Citrix Receiver 支持使用 Citrix StoreFront 和 Web Interface 连接到虚拟桌面和应用程序。
  StoreFront：
  - StoreFront 3.0（推荐使用）
    用于直接访问 StoreFront 应用商店。Receiver 还支持早期版本的 StoreFront。

    注意：本版本的 Receiver for iOS 中包含 Framehawk 虚拟通道。此功能与最新版本的 StoreFront 3.0 相集成。要利用此新增功能，Citrix 建议您安装最新版本的 StoreFront。

  - 配置有 Receiver for Web 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的“使用 Receiver 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。

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
- NetScaler 上的 Web Interface（基于浏览器的访问仅限使用 Safari）必须启用 NetScaler 提供的重写策略。

- **XenDesktop** 和 **XenApp**（以下任意产品）：
  - Citrix XenDesktop 4、5、5.5、5.6、7、7.x、7.5 和 7.6
  - Citrix XenApp 7.5 和 7.6
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - Citrix XenApp 6 for Windows Server 2008 R2
  - Citrix XenApp Fundamentals 6.0 for Windows Server 2008 R2
  - Citrix XenApp 5 for Windows Server 2008
  - Citrix XenApp 5 for Windows Server 2003
  - Citrix Presentation Server 4.5
- VDI-in-a-Box 5.2.x 和 5.3.x

连接性和身份验证

对于到 StoreFront 的连接，Receiver 支持以下身份验证方法：

	Receiver for Web（使用浏览器）	**StoreFront Services 站点（本机）**	**StoreFront XenApp Services 站点（本机）**	**NetScaler 到 Receiver for Web（浏览器）**	**NetScaler 到 StoreFront Services 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*
双因素（域 + 安全令牌）				是*	是*
SMS				是*	否
智能卡		是		是*	是*
用户证书				是（NetScaler Gateway 插件）	是（NetScaler Gateway 插件）

* 仅在 Receiver for Web 站点以及包含 NetScaler Gateway 的部署中可用，而不管设备上是否已安装关联的插件。

有关 StoreFront 支持的 NetScaler Gateway 和 Access Gateway 版本的信息，请参阅 NetScaler Gateway、Access Gateway 和 StoreFront 文档。

对于到 Web Interface 5.4 的连接，Receiver 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	NetScaler 到 Web Interface（浏览器）	NetScaler 到 Web Interface XenApp Services 站点
匿名	是			
域	是	是	是*	
域直通	是			
安全令牌			是*	
双因素（域 + 安全令牌）			是*	
SMS			是*	
智能卡**				
用户证书			是（需要 NetScaler Gateway 插件）	

关于安全连接和证书

私有（自签名）证书

如果远程网关上安装了专用证书，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 Citrix Receiver 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。
将根证书导入到 iPad 和 iPhone 设备中

可以获取证书颁发机构的根证书，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。Receiver for iOS 支持通配符证书。

中间证书与 NetScaler Gateway

如果您的证书链中包含中间证书，必须将该中间证书附加到 NetScaler Gateway（或 Access Gateway）服务器证书。有关在 NetScaler Gateway 或 Access Gateway 上安装中间证书的信息，请参阅 eDocs 中的相关文档。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）

另请参阅：

CTX124937：How to Configure Citrix Access Gateway Enterprise Edition for Use with Citrix Receiver for Mobile Devices（如何配置 Citrix Access Gateway Enterprise Edition，使其与适用于移动设备的 Citrix Receiver 一起使用）

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。

Receiver 支持 Access Gateway 所支持的所有身份验证方法。有关身份验证的信息，请参阅 eDocs 中的 NetScaler Gateway（或 Access Gateway）文档以及 StoreFront 文档中的“管理”主题。有关 Web Interface 支持的其他身份验证方法的信息，请参阅 Web Interface 文档中的“为 Web Interface 配置身份验证”。

智能卡

Citrix Receiver 提供有限的智能卡支持。

如果使用 FIPS NetScaler 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 How to configure the -denySSLReneg parameter（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

  支持的 VDA 智能卡中间件
  - ActiveIdentity
- 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 NetScaler Gateway 以及 XenDesktop 5.6 和更高版本或 XenApp 6.5 和更高版本

配置环境

Jan 29, 2016

Receiver 支持您的 XenApp 部署的 Web Interface 配置。有两种类型的 Web Interface 站点：XenApp Services（以前称为 Program Neighborhood Services）站点和 XenApp Web 站点。Web Interface 站点使客户端设备能够连接到服务器场。可以使用多种解决方案处理 Receiver 与 Web Interface 站点之间的身份验证问题，其中包括 Citrix Access Gateway 和 Citrix Secure Gateway。

此外，可以对 StoreFront 进行配置，使其为 Receiver 提供身份验证和资源交付服务，使您能够创建集中的企业应用商店，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），请参考 http://community.citrix.com。

在用户访问 XenApp 或 XenDesktop 部署中托管的应用程序之前，请在部署中按如下所述配置以下组件。

- 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 Citrix Receiver 中看到这些说明。
  - 可以通过在 Citrix Receiver 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 Citrix Receiver 的“精选”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，请将字符串 KEYWORDS:Auto 附加到您在 XenApp 中发布该应用程序时提供的说明后。用户登录到该应用商店时，相应的应用程序将自动置备，而无需用户手动订阅。

  有关详细信息，请参阅 StoreFront 文档。

- 如果 XenApp 或 XenDesktop 部署中的 Web Interface 没有 Web 站点或 XenApp Services 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。

配置 StoreFront

Jan 29, 2016

配置 StoreFront

重要提示：

- 使用 StoreFront 时，Receiver 支持自 Citrix Access Gateway Enterprise Edition 9.3 至 NetScaler Gateway 11 的所有版本。
- Receiver for iOS 仅支持 Web Interface 上的 XenApp Services 站点。
- Receiver for iOS 支持从 Receiver for Web 启动会话，前提是 Web 浏览器可用于 Receiver for Web。如果无法启动，请直接通过 Receiver for iOS 配置您的帐户。用户必须使用浏览器的“使用 Receiver 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 Citrix Receiver 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 XenDesktop 站点和 XenApp 场中的桌面和应用程序，并将这些资源汇集在一起，以使其对用户可用。

1. 安装并配置 StoreFront。 有关详细信息，请参阅 eDocs 的“技术”>“StoreFront”部分中的 StoreFront。对于需要更大控制权限的管理员，Citrix 提供了一个模板，可以使用该模板创建 Receiver for iOS 的下载站点。
2. 为 StoreFront 配置应用商店，具体步骤基本与为其他 XenApp 和 XenDesktop 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 eDocs“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：
   - 置备文件。可以向用户提供包含应用商店连接详细信息的置备文件 (.cr)。安装完成后，用户将打开设备上的置备文件，以自动配置 Citrix Receiver。默认情况下，Receiver for Web 站点为用户提供的置备文件仅适用于站点所对应的单个应用商店。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置备文件。
   - 手动配置。可以直接将访问桌面和应用程序所需要的 Access Gateway 或应用商店 URL 通知给用户。如果通过 Access 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输入 Citrix Receiver 中，该插件将尝试验证连接，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**，然后在地址字段中输入 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 Access Gateway 和 NetScaler Gateway

如果有用户从内部网络外部进行连接（例如，用户从 Internet 或远程位置进行连接），请通过 Access Gateway 或 NetScaler Gateway 配置身份验证。

- 使用 StoreFront 时，Receiver 支持自 Citrix Access Gateway Enterprise Edition 9.3 至 NetScaler Gateway 11 的所有版本。
- 有关详细信息，请参阅 eDocs 中所用版本的 Access Gateway 或 NetScaler Gateway。

配置 Receiver 以访问应用程序

1. 创建新帐户时，如果要将 Receiver 配置为自动访问应用程序，请在地址字段中输入应用商店的匹配 URL，例如 storefront.organization.com。
2. 如果要使用智能卡进行身份验证，请选择“使用智能卡”选项。
3. 对于手动配置（可通过“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 Access Gateway（或 NetScaler 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。

配置客户端证书身份验证

Jan 29, 2016

重要提示：

- 使用 StoreFront 时，Receiver 支持自 Citrix Access Gateway Enterprise Edition 9.3 至 NetScaler Gateway 11 的所有版本。
- 自 Receiver for iOS 5.5 起的所有版本都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。
- Receiver 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 Access Gateway（或 NetScaler Gateway）虚拟服务器呈现的客户端证书属性对登录到该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 Access Gateway 上将根证书与虚拟服务器绑定在一起。

用户登录到 Access 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。

如果用户提供了用户名和域信息（而非提供这些信息的证书，实际上是一个更加安全的范例），请从客户端证书中删除 **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** 字段。

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 XenApp 控制台或 Web Interface 控制台（取决于您安装的 XenApp 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 Receiver 使用 XenApp Services 站点（以前称为 Program Neighborhood 代理站点）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 Receiver。这与使用 Web Interface 建立传统的基于 SSL 的 XenApp 连接的方式相似，对于这种连接，可以配置 Access Gateway。

为适用于移动设备的 Receiver 配置 XenApp Services 站点，以支持通过 Access Gateway 进行连接。

1. 在 XenApp 服务站点中，选择 Manage secure client access（管理安全客户端访问）> Edit secure client access settings（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 Access Gateway 设备的 FQDN。
4. 输入 Secure Ticket Authority (STA) 信息。

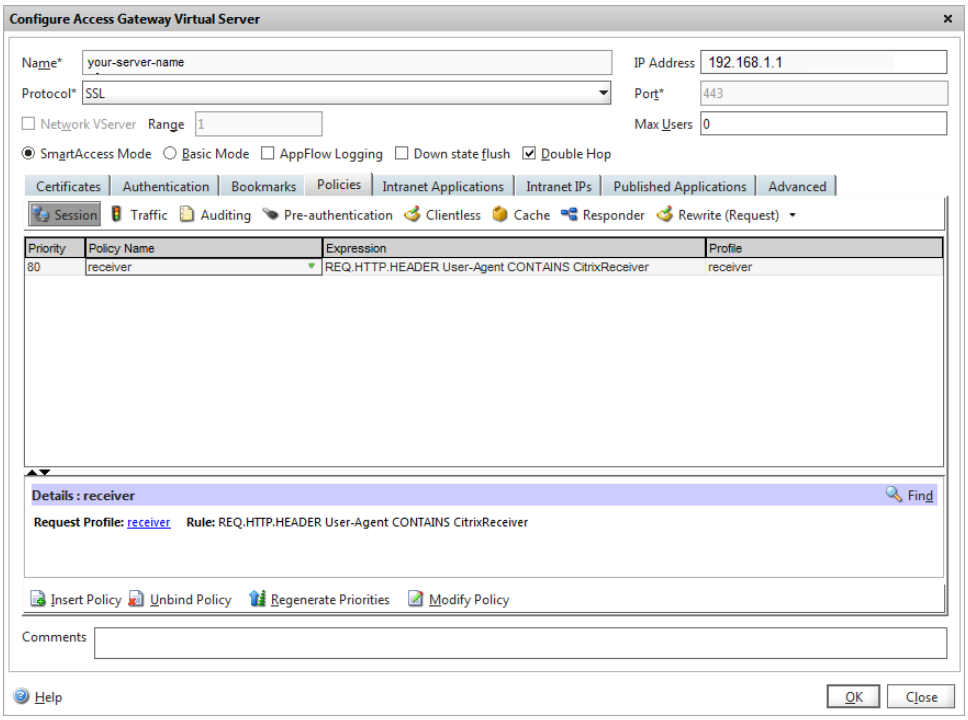
配置 Access Gateway 设备

对于客户端证书身份验证，请使用证书和 LDAP 这两种身份验证策略通过双因素身份验证方法配置 Access Gateway。有关详细信息，请参阅 eDocs 中所用的版本 Access Gateway Enterprise Edition（仅限 9.x）或 Access Gateway 10，并搜索主题

。

1. 在 Access Gateway 上创建会话策略，允许从 Receiver 传入 XenApp 连接，并指定新创建的 XenApp Services 站点的位置。
   - 创建一个新会话策略来标识该连接来自适用于移动设备的 Receiver。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 CitrixReceiver



   - 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 OFF（关）。

     在 Web Interface Address（Web Interface 地址）字段中，输入 URL（其中包含设备用户所使用的 XenApp Services 站点的 config.xml），例如 http://XenAppServerName/Citrix/PNAgent/config.xml 或 http://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 Access Gateway 上使用的服务器证书为证书链（含中间证书）的一部分，则要确保 Access 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 Access Gateway 文档。

为 Receiver 应用程序配置移动设备

如果在 Access 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 Receiver 打开帐户，并在“服务器”字段中输入 Access Gateway 服务器的匹配 FQDN，例如 GatewayClientCertificateServer.organization.com。Receiver 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一个证书。 对于 iOS 客户端证书身份验证，必须只能由 Receiver 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，用户需要输入其余字段，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）按钮跳过证书选项。 在此种情况下，Receiver 将继续进行连接，为用户显示登录屏幕。
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。 Receiver 将存储帐户的证书，并自动使用这些证书满足将来的登录请求。

配置 Secure Gateway

Jan 29, 2016

配置 XenApp Services 站点

重要提示：

- 使用 XenApp Services 站点的支持 Secure Gateway 3.x。
- 使用 XenApp Web 站点的支持 Secure Gateway 3.x。
- 在 XenApp Services 站点上仅支持单因素身份验证方法，在 XenApp Web 站点上同时支持单因素和双因素身份验证方法。
- 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，安装并配置与 Web Interface 一起运行的 Secure Gateway。您可以修改这些指令来适合您的具体环境。

如果使用 Secure Gateway 连接，则不要在 Receiver 上配置 Citrix Access Gateway 设置。

适用于移动设备的 Receiver 使用 XenApp Services 站点（以前称为 Program Neighborhood 代理站点）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 Receiver。这与使用 Web Interface 建立传统的基于 SSL 的 XenApp 连接的方式相似，对于这种连接，可以配置 Access Gateway。在 Web Interface 5.x 上运行的 XenApp 服务站点已内置此配置功能。

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

1. 在 XenApp 服务站点中，选择 Manage secure client access（管理安全客户端访问）> Edit secure client access settings（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 Gateway 的 FQDN。
4. 输入 Secure Ticket Authority (STA) 信息。
   注意：对于 Secure Gateway，Citrix 建议为该站点使用 Citrix 默认路径 (http://XenAppServerName/Citrix/PNAgent)。用户可以利用默认路径指定他们所连接的 Secure Gateway 的 FQDN，而不必指定到驻留在 XenApp 服务站点上的 config.xml 文件的完整路径（例如http://XenAppServerName/CustomPath/config.xml）。

配置 Secure Gateway

1. 在 Secure Gateway 上，使用“Secure Gateway Configuration”（Secure Gateway 配置）向导将 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 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，以验证是否已根据网络连接和证书分配对 Secure Gateway 进行了正确配置。

为 Receiver 应用程序配置移动设备

1. 添加 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 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 Access Gateway 选项**新建帐户**对话框。

配置 Access Gateway Enterprise Edition

Jan 29, 2016

重要：

- 使用 XenApp Services 站点或在 StoreFront 服务器上使用旧版模式的 Receiver for iOS 支持 Access Gateway Enterprise Edition 9.x 和 10.x。
- 使用 XenApp Web 站点的 Receiver for iOS 支持 Access Gateway Enterprise Edition 9.x 和 10.x。
- ReceiverforWeb不受 Receivers for iOS 支持。
- Receiver for iOS 支持 Access Gateway Enterprise Edition 9.x 和 10.x，以访问 StoreFront 应用商店。
- 在 Web Interface 站点和 StoreFront 上同时支持单来源和双来源身份验证方法。
- 必须使用 Web Interface 5.4，该版本受所有内置浏览器支持。
- 可以在同一虚拟服务器上创建多个会话策略，具体取决于连接类型（例如 ICA、CVPN 或 VPN）和 Receiver 的类型（Web Receiver 或本地安装的 Receiver）。所有策略都可以从一台虚拟服务器进行配置。
- 用户在 Receiver 上创建帐户时，需输入帐户凭据，如电子邮件地址或与 Access Gateway 服务器匹配的 FQDN。例如，如果使用默认路径时连接失败，则用户应输入 Access Gateway 服务器的完整路径。

要使远程用户能够通过 Access Gateway 连接到 CloudGateway 部署，您可以配置 Access Gateway 以用于 StoreFront。启用访问权限的方法取决于部署中使用的 CloudGateway 版本：

- 如果在网络中部署 CloudGateway Express，应通过将 Access Gateway 与 StoreFront 相集成的方式，允许内部用户或远程用户通过 Access Gateway 与 StoreFront 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 Citrix Receiver 进行连接。

有关配置这些连接的信息，请参考 eDocs 中的 Integrating Access Gateway with CloudGateway（将 Access Gateway 与 CloudGateway 相集成）以及该节点下的其他主题。

以下主题提供了有关适用于移动设备的 Receiver 所需设置的信息：

- 创建 Receiver for CloudGateway Enterprise 的会话配置文件
- 创建 Receiver for CloudGateway Express 的会话配置文件
- 配置 Receiver 的自定义无客户端访问策略
- 在 Access Gateway 中配置安全浏览（仅限 iOS 设备，Android 设备无需此配置）
- 允许使用移动设备进行访问
- 适用于移动应用程序的 MDX Toolkit

要使远程用户能够通过 Access Gateway 连接 Web Interface 部署，应将 Access Gateway 配置为与 Web Interface 配合使用，如 Citrix eDocs 中 Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface（将 Access Gateway Enterprise Edition 配置为与 Web Interface 通信）及其子主题所述。

配置 Web Interface

Jan 29, 2016

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 XenApp 应用程序相同。如果没有为移动设备配置 XenApp Services 站点，Receiver 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。

自动配置移动设备

Jan 29, 2016

可在 PC 或 Mac 上使用 Citrix Mobile Receiver Setup URL Generator 针对适用移动设备快速配置 Citrix Receiver。使用此实用程序可配置 XenApp 帐户设置，然后立刻使用电子邮件将配置发送到许多设备上。

由于用户名和密码是由用户输入的，因此，进行配置时只需要服务器名称、服务器地址、域名以及 Access Gateway 信息（如果适用）。

1. 在 PC 或 Mac 上，从 http://community.citrix.com/MobileReceiverSetupUrlGenerator/ 打开 Mobile Receiver Setup URL Generator。
2. 对于帐户说明，请输入帐户名称（例如组或部门）；示例：产品或销售。
3. 对于服务器地址，请键入您的 XenApp 服务器场的地址，例如，gateway.myserverfarm.net。
4. 对于域，请键入要与用户连接的服务器场的域名。
5. 要启用 Access Gateway 配置，请选择使用网关复选框。
    1. 在网关类型下，选择部署在要与用户连接的服务器场中的 Access Gateway 版本。 （如果不知道正确的版本，请与管理员联系。）
    2. 在网关身份验证类型下，选择您的基础结构中使用的身份验证方法。
6. 单击生成 URL。
7. 在您的结果中，单击配置链接，并复制生成的链接。

使用电子邮件将链接直接发送到用户的移动设备上，以完成其在该设备上的 Receiver 帐户配置。
重要：一些 BlackBerry 设备要求使用纯文本格式的邮件以使得预配置的 URL 可以与 Receiver 正确地关联。因此，建议总是将 URL 以纯文本格式邮件信息发送给 BlackBerry 用户。

手动配置帐户

Jan 29, 2016

一般来说，连接到 Access Gateway 时，Receiver 将在通过身份验证后尝试查找 XenApp Services 站点或 XenApp Web 站点。如果未检测到任何站点，Receiver 将显示一条错误。为避免出现此种情况，可以手动配置一个帐户，以便 Receiver 能够连接到 Access Gateway。

手动配置帐户

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，键入要连接的站点或 Access 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 - 为 Receiver 选择此选项可显示一个与 Web 浏览器类似的 XenApp Web 站点。此站点又称为 Web View。
   - XenApp Services - 为 Receiver 选择此选项可定位未配置“通过 Access 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。
     - http:// ：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。
     - http:///citrix/<应用商店名称> ：这将添加 StoreFront 应用商店 <应用商店名称>。
     - http:///citrix/PnAgent/config.xml ：这将添加默认旧 PNAgent 应用商店。
     - http:///citrix/<应用商店名称>/PnAgent/config.xml ：这将添加与 <应用商店名称> 关联的旧 PNAgent 应用商店。
   - Access Gateway - 为 Receiver 选择此选项可通过特定的 Access 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（如果您选择进行双因素身份验证），然后轻按登录。 此时将显示 Citrix Receiver 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。

为 iOS 设备提供 RSA SecurID 身份验证

Jan 29, 2016

Secure Gateway 配置（仅通过 Web Interface 进行的配置）和所有 NetScaler Gateway 配置均支持 Citrix Receiver 的 RSA SecurID 身份验证。

有关在 NetScaler Gateway 上配置 RSA SecurID 身份验证的说明，请参阅：

- 在 NetScaler Gateway 11.0 上配置 RSA SecurID 身份验证
- 在 NetScaler Gateway 10.5 上配置 RSA SecurID 身份验证
- 在 NetScaler Gateway 10.1 上配置 RSA SecurID 身份验证

Receiver 上软件令牌所需的 URL 方案：Receiver 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 Citrix Receiver 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 Receiver 中。

将 RSA SecurID 软令牌导入 Citrix Receiver

要对 Citrix Receiver 使用 RSA 软令牌，请要求您的用户按照以下过程进行操作。

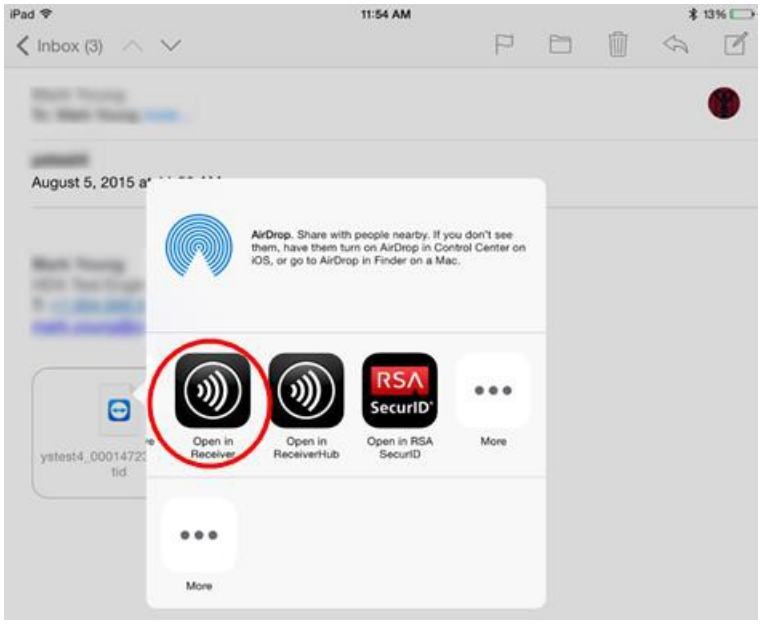
PIN 长度、PIN 类型（仅限数字、字母数字）以及 PIN 重用限制的策略在 RSA 管理服务器上指定。

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。

对 Citrix Receiver 使用 RSA 软令牌

1. 导入贵组织向您提供的 RSA 软令牌。

在附加了 SecurID 文件的电子邮件中，选择 **Open in Receiver**（在 Receiver 中打开）作为导入目标位置。



导入软令牌后，Citrix Receiver 将自动打开。

2. 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**。

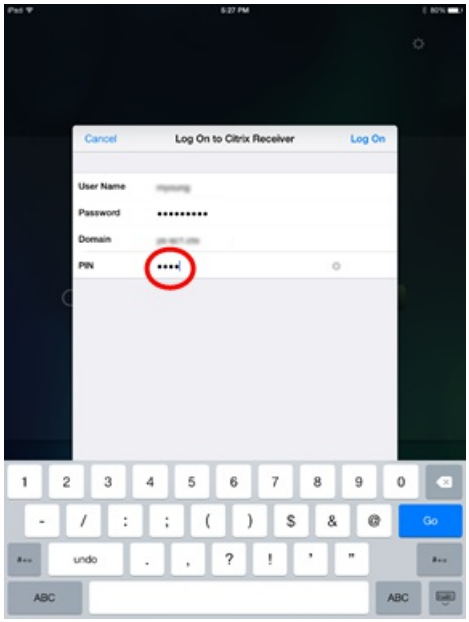
单击**确定**后，系统将显示一条消息，提示您令牌已成功导入。

3. 关闭导入消息，然后在 Citrix Receiver 中单击**添加帐户**。

- 输入贵组织提供的应用商店的 URL。
- 单击**下一步**。

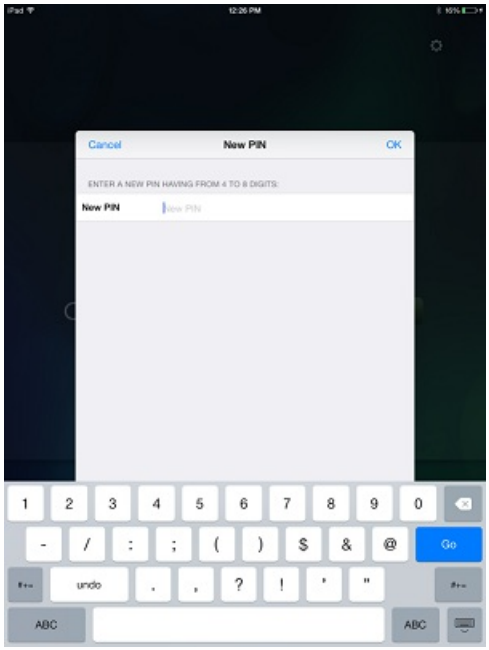
4. 在“登录”屏幕中：

- 输入您的凭据：用户名、密码和域（例如 example.com）。
- 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。）
- 单击左上角的**登录**。



5. 单击“登录”按钮后，系统将提示您创建一个新 PIN。

输入一个 4 到 8 位数字的 PIN，然后单击**确定**。



6. 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。

下一个令牌模式支持

如果您将 Access Gateway 配置为进行 RSA SecurID 身份验证，Receiver 将支持“下一个令牌”模式。 启用此功能后，如果用户输入三次（默认）错误密码，Access 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。

向 iOS 设备的最终用户提供访问信息

Jan 29, 2016

必须向用户提供访问其托管应用程序、桌面和数据所需的 Receiver 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
- 向用户提供置备文件
- 向用户提供自动生成的设置 URL
- 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 Receiver 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 Receiver 时需要输入自己的电子邮件地址而非服务器 URL。Receiver 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 Receiver 连接到 Web Interface 部署，则不支持基于电子邮件的发现。
要将 DNS 服务器配置为支持基于电子邮件的发现，请参阅 StoreFront 文档中的配置基于电子邮件的帐户发现。

要配置 Access Gateway 以通过使用电子邮件地址发现 StoreFront 或 Access Gateway URL 接受用户连接，请参阅 Access Gateway 文档中的 Connecting to StoreFront by Using Email-Based Discovery（使用基于电子邮件的发现连接到 StoreFront）。

向用户提供置备文件

您可以使用 StoreFront 来创建包含帐户的连接详细信息的置备文件。您将这些文件提供给用户，以便用户能够自动配置 Receiver。安装 Receiver 后，用户只需打开设备上的 .cr 文件即可配置 Receiver。如果您配置了 Receiver for Web 站点，用户还可以从这些站点获取 Receiver 置备文件。

有关详细信息，请参阅 StoreFront 文档。

向用户提供自动生成的设置 URL

可以使用 Setup URL Generator 配置适用于移动设备的 Receiver。在安装 Receiver 之后，用户只需单击 URL 即可配置其帐户和访问其资源。使用此实用程序可配置帐户和电子邮件的设置，或将该信息立刻发布给您的所有用户。

有关详细信息，请参阅自动配置移动设备。

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。
- 要使用 Access Gateway 进行访问，请提供 Access Gateway 地址以及所需的身份验证方法。
  有关配置 Access Gateway 或 Secure Gateway 的详细信息，请参阅 Access Gateway 或 XenApp（用于 Secure Gateway）文档。

用户输入新帐户的详细信息时，Receiver 将尝试验证连接。如果验证成功，Receiver 将提示用户登录到该帐户。

会话共享

在 iPad 上，当用户从 Receiver 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**：从帐户中注销，但将 Windows 应用程序或桌面保留为继续在服务器上运行，并且用户随后可以启动其他设备，启动 Receiver，以及重新连接到从 iPad 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**：从帐户中注销，关闭 Windows 应用程序，并从 XenApp 或 XenDesktop 服务器中注销。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 Receiver 时，Receiver 将在默认状态下打开。

启用 Citrix X1 鼠标、外部显示器和演示功能

Jan 29, 2016

要使其更容易在 iOS 设备上使用 Windows 应用程序，可以将 Citrix Receiver 配置为对 XenApp 或 XenDesktop 会话中运行的 HDX 应用程序使用特殊 Citrix X1 鼠标。

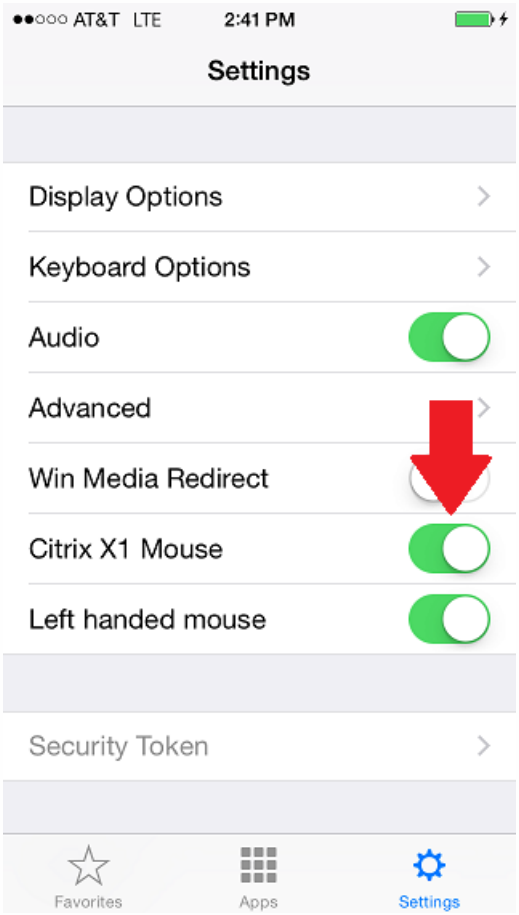
还可以配置 Receiver 设置以使用外部显示器，并使用您的 iOS 设备控制将设备用作键盘或触控板时的显示屏幕。这样可使您能够在 iOS 设备上运行演示。

允许在 Receiver 中使用 Citrix X1 鼠标

可以在 Citrix HDX 会话中连接并使用 Citrix X1 鼠标。Receiver 当前仅支持一种鼠标型号。有关 Citrix X1 鼠标的详细信息，请参阅 http://www.citrix.com/products/mouse/overview.html。

Citrix X1 鼠标属于蓝牙设备，因此，要使用该鼠标，必须在 iOS 设备上启用蓝牙。

要连接并启用 Citrix X1 鼠标，请在 Receiver 中轻按**设置**并打开 **Citrix X1 鼠标**。



可以为惯用左手的用户切换鼠标按钮：在 Receiver 中，轻按**设置**，并切换**左手专用鼠标**。

如果要在 Windows 虚拟桌面中使用 Citrix X1 鼠标，还可以从 Windows 控制面板中启用左手专用鼠标。转至“鼠标属性”以配置您的鼠标。

允许 Receiver 使用外部显示器

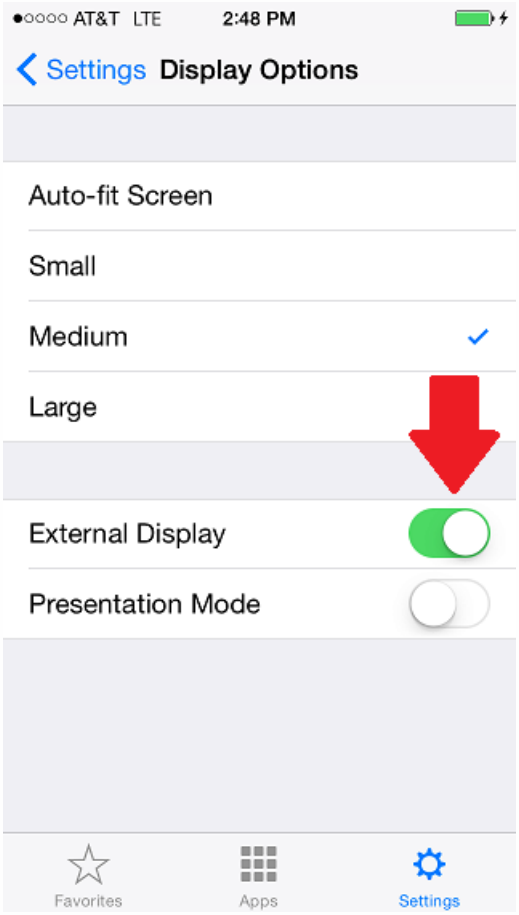
Receiver for iOS 支持对 iPhone 和 iPad 使用外部显示器。

可以通过以下方法使用外部显示器功能：

- AirPlay
- Lightning to VGA 适配器
- Lightning Digital AV 适配器

由于处理要求非常高，因此不建议对较旧的 iPad（非 Air 型号）和 iPhone（5c 及早期版本）使用外部显示器。

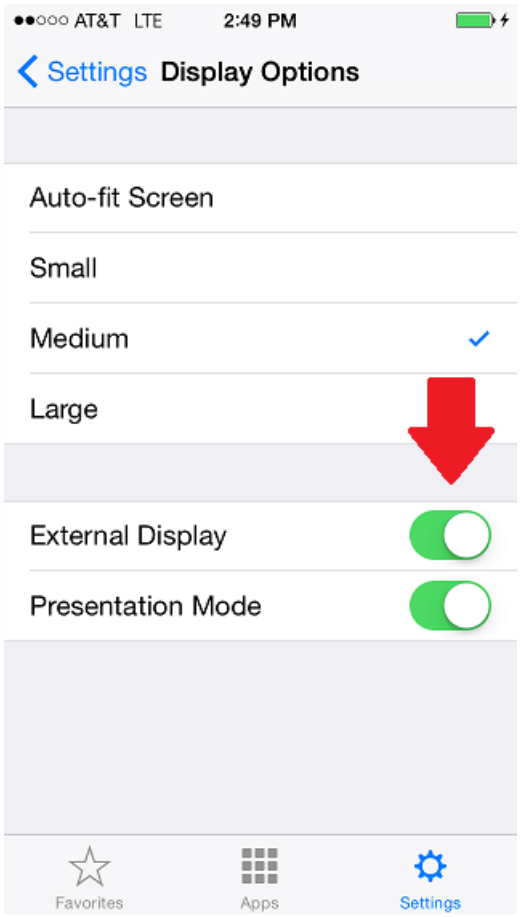
要启用外部显示器，请在 Receiver 中轻按**设置**，然后轻按**显示选项**。 打开**外部显示器**。



为 Receiver 启用键盘和触控板以便在外部显示器中使用

与外部显示器建立连接后，可以将 iPad 用作键盘和触控板（就像 AppleTV 或 Lightning to HDMI 电缆），来代替使用蓝牙键盘。

要启用演示模式，请在 **Receiver** 中轻按**设置**，然后轻按**显示选项**。打开**外部显示器***和***演示模式**。



外部显示器和演示模式与 Citrix X1 鼠标兼容。

阻止越狱设备从 StoreFront 运行应用程序

Jan 29, 2016

在本文中：

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。

Citrix Receiver 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
- StoreFront 3.0 或 Web Interface 5.4
- 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. 以具有管理员特权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]** 部分下添加以下行：

AllowJailBrokenDevices=OFF

下面是文件 default.ica file 中的一个代码段，显示 AllowJailBrokenDevices 设置为 OFF：

```
[Application]
Launcher=PNAgent
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
EnableIPCSessionControl=TRUE
AllowJailBrokenDevices=OFF

[EncRC5-0]
DriverNameWin32=pdc0n.dll
```

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. 以具有管理员特权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]** 部分下添加以下行：

    AllowJailBrokenDevices=ON

下面是文件 default.ica file 中的一个代码段，显示 AllowJailBrokenDevices 设置为 ON：

```
[Application]
Launcher=PNAgent
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
EnableIPCSessionControl=TRUE
AllowJailBrokenDevices=ON

[EncRC5-0]
DriverNameWin32=pdc0n.dll
```

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越狱设备有关的警报，但其能够通过 StoreFront 或 Web Interface 运行应用程序。

保存密码

Jan 29, 2016

使用 Citrix Web Interface 管理控制台，可以配置 XenApp 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的密码。 请注意以下事项：

- 如果启用了密码保存功能，Citrix Receiver 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），Citrix Receiver 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

自版本 6.1.2 起，Citrix Receiver for iOS 引入了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 Citrix Receiver 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。

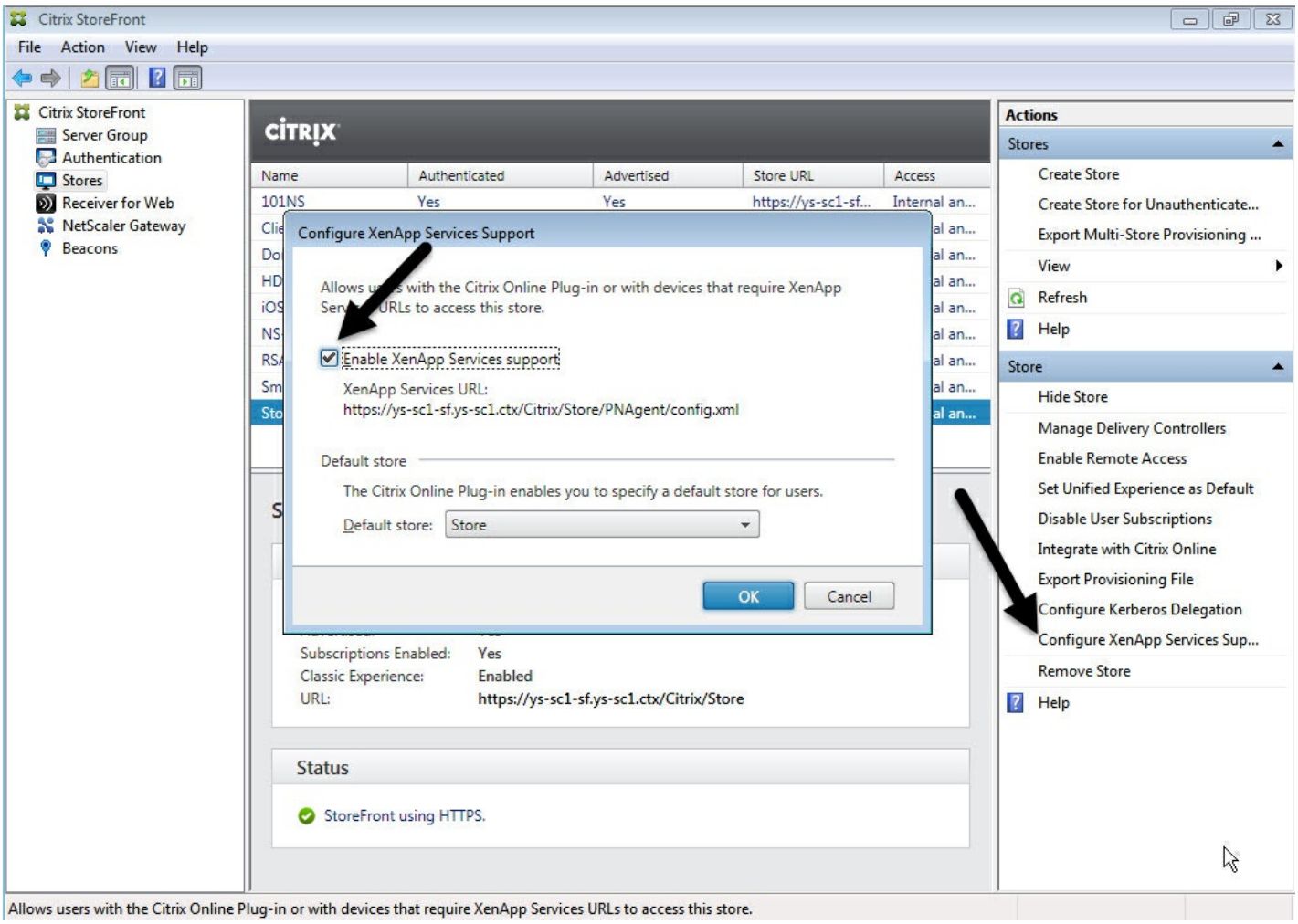
2. 要配置新 StoreFront 部署，请按照安装、设置和卸载 Citrix StoreFront 中介绍的最佳实践进行操作。

3. 打开 Citrix StoreFront 管理控制台。

> **提示**
>
> 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）。



7. 启用**旧版支持**，然后单击**确定**。

8. 导航到模板配置文件，位置为 c:\inetpub\wwwroot\Citrix\\Views\PnaConfig\。

9. 备份 Config.aspx。

10. 打开原始的 Config.aspx 文件。

11. 编辑行 **false**，将 **false** 值更改为 **true**。

12. 保存编辑后的 Config.aspx 文件。

13. 在 StoreFront 服务器上，使用管理权限运行 PowerShell。

14. 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-DSDerviceMonitorFeature –ServiceUrl https://localhost:443/StorefrontMonitor

15. 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 NetScaler

要配置 NetScaler 以支持保存密码功能，请执行以下操作：

1. 登录到 NetScaler 管理控制台。

> ### 注意
>
> 此配置使用 NetScaler 负载平衡服务器。 如果您的环境中尚未配置 NetScaler，请按照 Citrix NetScaler and Citrix XenDesktop 7 deployment guide（《Citrix NetScaler 和 Citrix XenDesktop 7 部署指南》）中的 Citrix 最佳实践部署指南进行操作。

2. 按照 Citrix 最佳实践进行操作，为您的负载平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”->“负载平衡”->“服务器”。 单击**添加**。

4. 输入 StoreFront 服务器的服务器名称和 IP 地址。 单击**创建**。

> ### 提示
>
> 如果您有 StoreFront 组，请对该组中的所有服务器重复步骤 5。

5. 在“配置”选项卡上，导航到“流量管理”->“负载平衡”->“监视器”。 单击**添加**。

6. 输入监视器的名称。 选择类型 **STOREFRONT**。

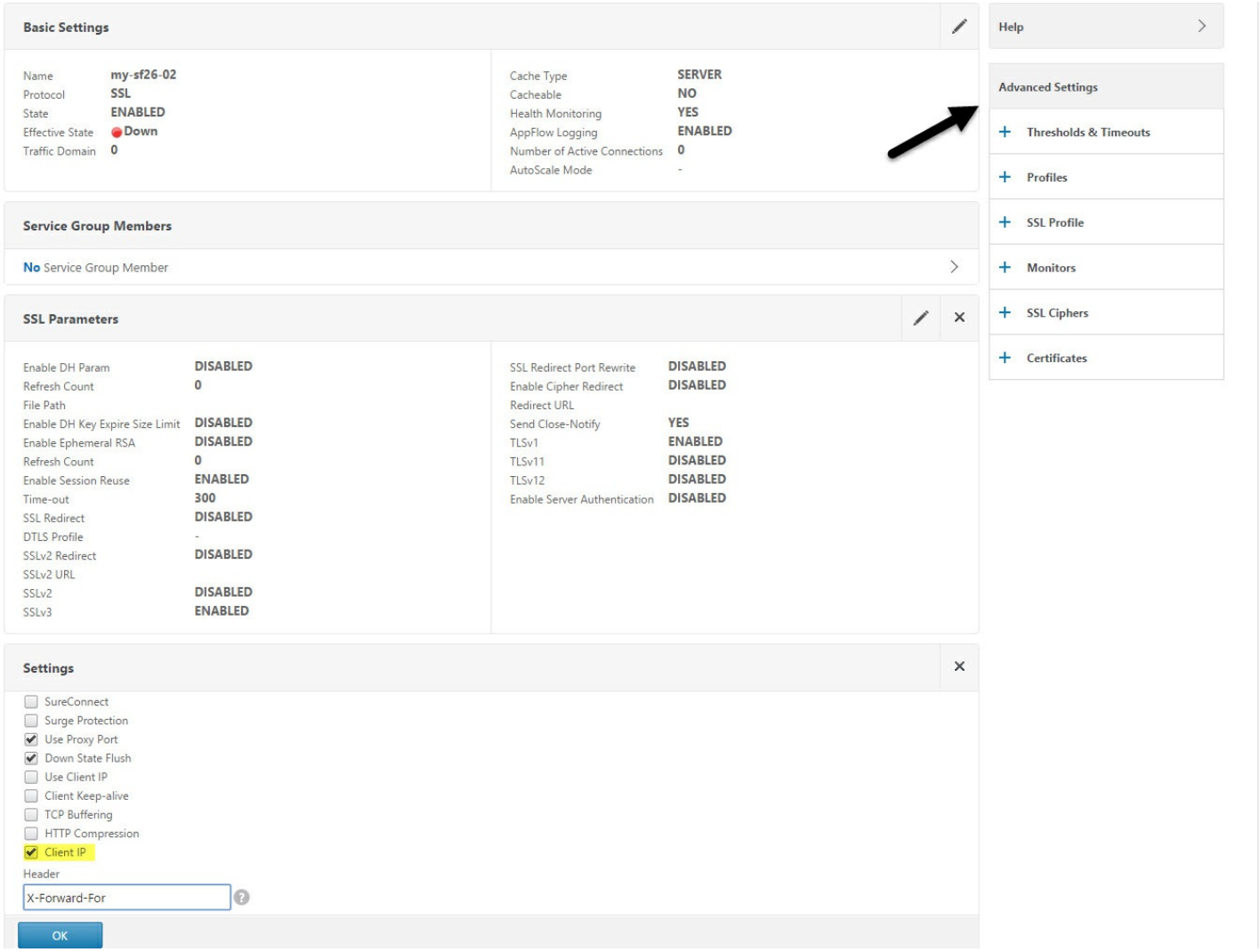
7. 在页面底部，选择**安全**（需要选择此选项，因为 StoreFront 服务器使用 HTTPS）。

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）。 单击**创建**。

9. 在**配置**选项卡上，导航到“流量管理”->“负载平衡”->“服务组”。 单击**添加**。

10. 输入服务组的名称，然后将协议设置为 **SSL**。 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**。 单击**确定**。

13. 在右侧屏幕上（位于“高级设置”下），选择**监视器**。

14. 单击箭头以添加新监视器。

15. 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 NetScaler 上配置的监视器）。

16. 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**。

17. 在右侧屏幕上（位于“高级设置”下），选择 **Members**（成员）。

18. 单击箭头以添加新服务组成员。

19. 单击**添加**按钮，然后选择 **Select Member**（选择成员）下拉列表。

20. 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 NetScaler 上配置的服务器成员）。

21. 单击以前创建的 StoreFront 服务器旁边的单选按钮。

22. 输入端口号 443，指定唯一的哈希 ID 编号，然后单击**创建**。

23. 单击**完成**。

> **提示**
>
> 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。

24. 导航到“流量管理”->“负载平衡”->“虚拟服务器”，然后单击**添加**。

25. 输入服务器的名称，然后选择协议 **SSL**。

26. 输入 StoreFront 负载平衡服务器的 IP 地址。 单击**确定**。

27. 选择 **Load Balancing Virtual Server Service Group**（负载平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。

28. 单击**确定**两次。

29. 分配为负载平衡虚拟服务器创建的 SSL 证书。 选择 **No Server Certificate**（无服务器证书）。

30. 从列表中选择负载平衡服务器证书，然后单击**绑定**。

31. 将域证书添加到负载平衡服务器。 单击 **No CA certificate**（无 CA 证书）。

32. 选择域证书，然后单击**绑定**。

33. 在屏幕右侧，选择 **Persistence**（持久性）。

34. 将“持久性”更改为 **SOURCEIP**（源 IP），然后将超时设置为 **20**。 单击**保存**。

35. 单击**完成**。

37. 在域 DNS 服务器上，添加负载平衡服务器（如果尚未创建）。

38. 在您的 iOS 设备上启动 Citrix Receiver，然后输入完整的 XenApp URL。 例如：

    https:// Virtual Server>/Citrix/PNAgent/Config.xml

> **提示**
>
> 有关其他信息，请参阅 Citrix NetScaler and Citrix XenDesktop 7 deployment guide（《Citrix NetScaler 和 Citrix XenDesktop 7 部署指南》）以及安装、设置和卸载 Citrix StoreFront。

尝试使用演示站点

Jan 29, 2016

用户首次启动 Citrix Receiver 时，欢迎页面将提供一个选项，用于启动 Citrix Cloud 中的演示帐户。

用户可以通过输入自己的名称和电子邮件地址（在某些设备上，电子邮件地址已预先填充）完成帐户注册。演示站点已配置有已发布的应用程序，因此用户可以立即尝试使用 Citrix Receiver。

用户可以在 Receiver 中添加、更改和删除自己的帐户。

故障排除

Jan 29, 2016

会话断开连接

用户可以通过以下方式从 Receiver 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 Receiver：
  - 双击设备的 **Home** 按钮。
  - 在 iOS 应用程序切换器视图中找到 Receiver。
  - 在显示的对话框中轻按“断开连接”。
- 按其移动设备上的主按钮。
- 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。

在应用程序中数字键出现问题

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 Receiver 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。

XenDesktop 中丢失 HDX 音频质量

在 XenDesktop 中，使用音频加视频时，Receiver for iOS 的 HDX 音频可能会丢失质量。XenDesktop 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 http://support.citrix.com/article/ctx123543。

可以从 Citrix Cloud 获取的演示帐户

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

Citrix Cloud 可使用户体验到 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 XenServer、XenApp、NetScaler 和 Access 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。

密码过期

Receiver 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。

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 XenApp 服务器和 Citrix Secure 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）：

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

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。

应用程序可能会在多个会话中打开

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。