关于 Citrix Receiver for Mac 12.2

Sep 09, 2016

通过 Citrix Receiver for Mac，用户能够自助访问在 XenApp 或 XenDesktop 服务器上发布的资源。 部署和使用 Receiver 非常简单，通过 Receiver，用户可以快速安全地访问托管应用程序和桌面。

从 Citrix Receiver for Mac 下载页面下载最新版本。

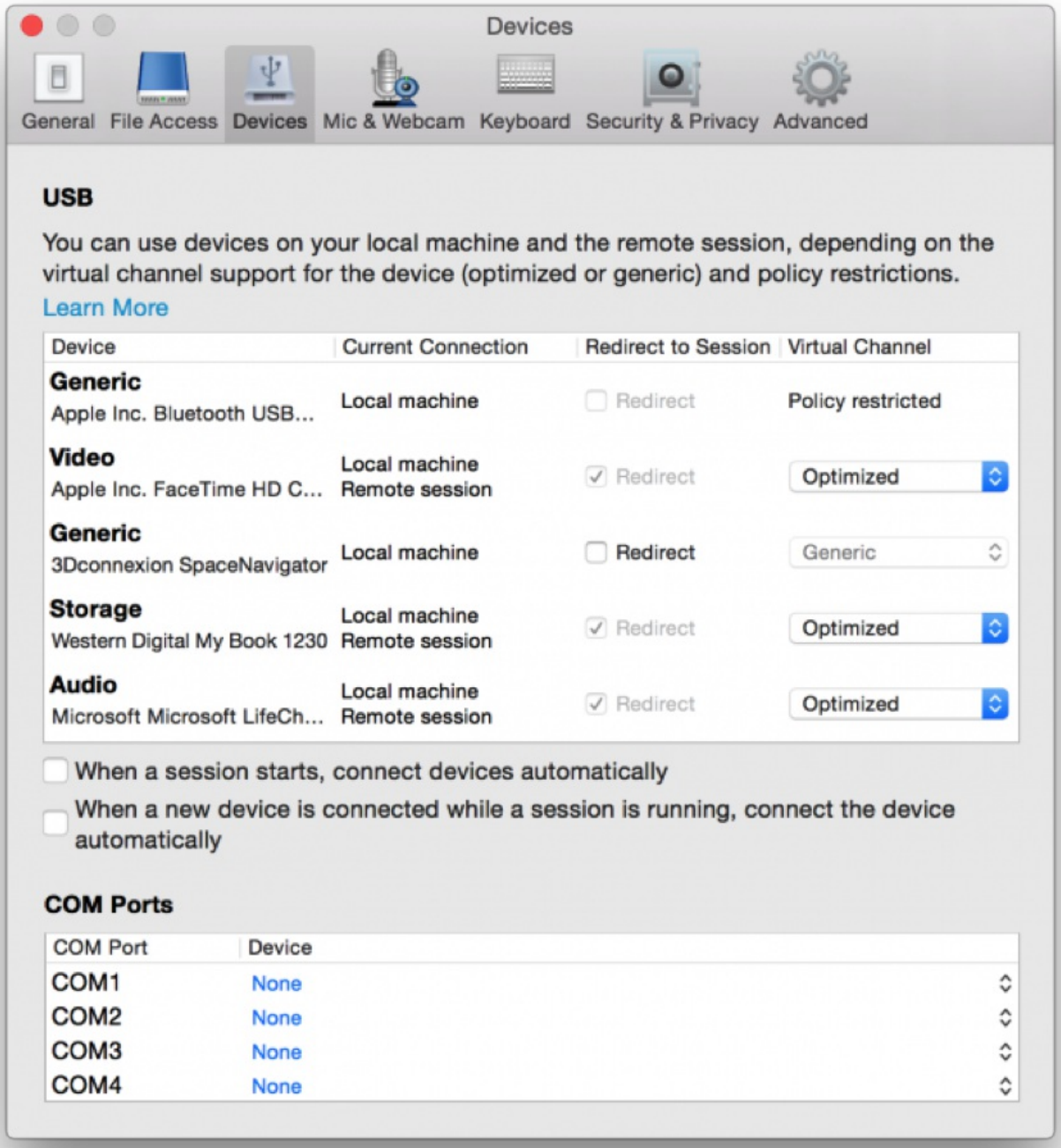
12.2 中的新增功能

通用 USB 重定向

本版本支持通用 USB 重定向。 此功能允许将任意 USB 设备从客户端计算机重定向到 XenDesktop 虚拟桌面。 通过此功能，最终用户能够在其活动的 XenDesktop 会话中与品类繁多的通用 USB 设备进行交互，就像该设备实际插入到虚拟桌面一样。

通用 USB 重定向在低级别运行，在客户端计算机与 XenDesktop 虚拟桌面之间重定向 USB 请求和响应。 避免了对客户端计算机上的设备驱动程序的兼容性要求；驱动程序必须仅在虚拟桌面上受支持。

可以通过 DDC 策略控制和配置通用 USB 重定向。 使用 Citrix Receiver 菜单栏和“首选项”屏幕可控制 USB 设备的设置。



会话可靠性和客户端自动重新连接增强功能

本版本的 Citrix Receiver for Mac 提供了会话可靠性和客户端自动重新连接方面的增强功能。 重新连接过程中活动会话窗口变为灰色；倒计时器显示会话断开连接之前的时间。 会话断开连接/重新连接到会话之前会向用户发出通知。

支持增强功能

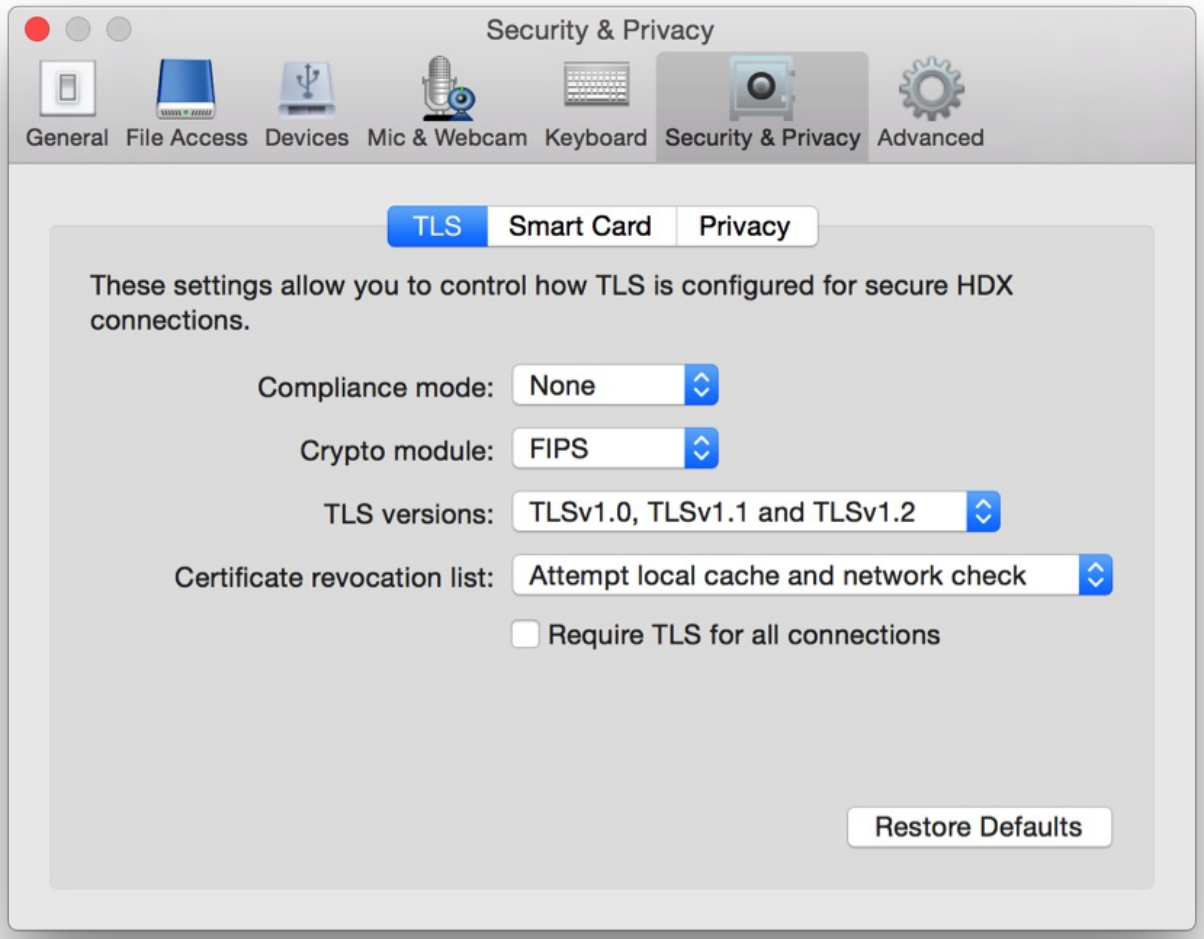
Citrix Receiver for Mac 在本版本中引入了大量支持方面的增强功能，包括：

- AlwaysOn 日志记录。 本版本引入了改进的 AlwaysOn 日志记录功能，可帮助收集重要的一次性事件。
- 会话崩溃期间收集改进的诊断结果。 此功能默认处于启用状态，可以在**首选项**屏幕中将其禁用。

安全功能增强

本版本的 Citrix Receiver for Mac 中包括多项安全增强功能和改进功能，包括：

- **改进了安全性配置用户界面**。 在早期版本中，更改与安全性有关的设置的首选方法是使用命令行；与会话安全性有关的配置设置现在非常简单，可从用户界面进行访问，这改进了为采用安全性有关的首选项创建无缝方法时的用户体验。
- **支持用于通过 NetScaler 进行智能卡身份验证的本机 OS X API**。 这改进了用于通过 NetScaler 进行智能卡身份验证的本机 OS X API 的可用性。 在本版本之前的版本中，用户需要在客户端计算机上安装 PKCS#11 模块才能通过 NetScaler 进行智能卡身份验证。 自本版本起，不再强制安装 PKCS#11。
- **TLS 连接**。Citrix Receiver for Mac 允许您验证与使用特定 TLS 版本的服务器建立的连接，其他信息包括用于连接的加密算法、模式、密钥大小以及是否已启用 SecureICA。 此外，还可以查看用于 TLS 连接的服务器证书。



客户体验改善计划 (CEIP)

Citrix 客户体验改善计划 (CEIP) 从 Receiver for Mac 收集匿名配置和使用数据，并自动将数据发送到 Citrix。 此数据可帮助 Citrix 改善 Receiver 的品质、可靠性和性能。

CEIP 不收集客户环境中的任何用户身份信息；收集的信息包括：

- 系统配置，包括硬件配置、操作系统详细信息、连接的设备、安装的 Receiver 版本、连接的显示器详细信息以及默认浏览器及其版本。
- Receiver 使用详情，包括一周内应用程序启动统计信息、连接故障次数、会话连接时间统计信息以及与崩溃有关的信息。
- 用户环境信息，包括图形模式、首选语言、用户区域设置以及与通过活动 Receiver 会话进行打印有关的统计信息。
- 安装/升级详细信息，包括以前的 Receiver 版本、无提示安装还是用户界面安装。

> ## 提示
>
> 可以使用 Receiver 界面更改您是否要参与 CEIP。 在安装后，您可以在 7 天内禁用 CEIP。

> ## 注意
>
> CEIP 所收集的数据暂时存储在磁盘上，直至每周一次通过 HTTPS 安全传输到 Citrix，传输后将被删除。 上载过程中不会包括用于识别客户或用户的任何信息。 有关 CEIP 的详细信息，请参阅关于 Citrix 客户体验改善计划 (CEIP)。

安排 CEIP 的目的是收集数据并默认每隔 7 天将数据安全地上载到 Citrix。 可以随时使用 Receiver 的“安全性和首选项”屏幕来更改您的 CEIP 参与情况。

有关禁用 CEIP 的信息，请参阅配置 Citrix Receiver for Mac。

Citrix Receiver for Mac 12.2 中已修复的问题

Nov 03, 2016

Citrix Receiver for Mac 12.2 中已修复的问题

比较对象：Citrix Receiver for Mac 12.1.100

Citrix Receiver for Mac 12.2 包含版本 12、12.1 和 12.1.100 中的所有修复以及以下新修复：

- 解决了在 ICA 文件中指定了 ScreenPercent 参数的情况下 Receiver for Mac 在全屏模式下启动会话的问题。

  [#605353]

- 解决了摄像头远程连接到活动会话时会话断开连接的情况下导致 Receiver for Mac 崩溃的问题。

  [#612051]

- 解决了正在重定向的 URL 包含非 ASCII 字符时服务器到客户端重定向失败的问题。

  [#LC4470]

- 本版本解决了下载证书吊销列表时 Receiver or Mac 不使用系统代理配置的问题。

  [#638176]

- 解决了 Ctrl-Tab 组合键不传递到活动桌面会话的问题。

  [#LC5395]

- 本版本解决了在 NetScaler Gateway 上配置了用户证书身份验证时会话重新连接失败的问题。

  [#LC5455]

- 解决了重新连接到现有会话时会话键盘映射不正确的问题。

  [LC5395]

- 解决了智能卡直通身份验证失败的问题。

  [LC4907]

- 本版本解决了 HDX 应用程序窗口在最小化和最大化后显示图形赝像的问题。

  [#LC4668]

- 修复了德语/亚洲语言键盘上 Alt 键在键入 Alt-l 后不松开的问题。

[#LC157]

- 解决了从麦克风远程传输到服务器的音频听起来非常不连贯的问题。

  [#LC5157]

- 修复了 HDX 会话中运行的 Microsoft 远程桌面客户端无法访问智能卡的问题。

  [#LC5454]

Citrix Receiver for Mac 12.1.100 中已修复的问题

比较对象：Citrix Receiver for Mac 12.1

Citrix Receiver for Mac 12.1.100 包含版本 12 和 12.1 中的所有修复以及以下新修复：

- 解决了启动名称开头为 @ 字符的桌面或应用程序时会话将崩溃的问题。

  [#LC4296]

- 修复了 IPV6 连接到 NetScaler Gateway 会失败的问题。

  [#LC4512]

- 解决了通过 Cisco ASA 9.32 SSL VPN 连接时 Receiver for Mac 会话失败的问题。

  [#LC3887]

- 修复了会话断开连接并导致显示指示“远程 SSL 对等机发送了 MAC 不正确警报”错误消息的问题。

  [#LC4367]

- 修复了尝试输入单个日语或简体中文字符会导致会话桌面中不显示任何字符的问题。

  [#603635]

Citrix Receiver for Mac 12.1 中已修复的问题

比较对象：Citrix Receiver for Mac 12

Citrix Receiver for Mac 12.1 包含版本 12 中的所有修复以及以下新修复：

- 修复了使用 OS X 中内置的 VPN 支持时，Citrix Receiver 在启用了 VPN 的情况下有时无法连接到已配置的帐户的问题。
- 修复了在 OS X El Capitan 中将会话置于“拆分视图”中时会话不正常显示的问题。

  [#582397]

- 修复了尝试在外部通过 F5 代理连接时信号检测失败的问题。

  [#582885]

- 修复了会话不应用在“系统首选项”中配置的键盘快捷方式的问题。

  [#583033]

- 修复了 Citrix Receiver for Mac 11.9.15 和 12 中导致查看器崩溃的“+”键盘符号的问题。

  [#586179，#577922]

- 修复了启动一个应用程序后，Citrix Receiver 要求对另一个应用程序进行身份验证的问题。

  [#592460]

- 修复了桌面会话中存在的一个问题，即 Ctrl-Q 键盘组合不正确传递的问题。

  [#600601]

Citrix Receiver for Mac 12 中已修复的问题

本版本解决了与智能卡集成有关的几个问题。 某些问题仍未解决，我们将继续调查研究。

本版本中已修复的其他问题：

- 在日语环境中，凭据对话框窗口中显示错误的消息（“デモアカウント にログオンしてください”，意思是“请登录到演示帐户”）。 此消息实际应为“Please log on to My Virtual Desktop”（请登录到我的虚拟桌面）。

  [#LC2682]

- 同时装载多个 Receiver 磁盘映像可能会导致启动错误的安装程序。

  [#551605]

- CIDR 表示法中的 OS X 代理绕过条目被忽略。

  [#564250]

- 仅使用 OS X 绕过列表的前 256 个字符。

  [#567089]

- 对于安装了 Barefruit 开发的 DNS 错误重定向软件的某些 ISP，内部信标误报检查可能会失败。

  [#572456]

Citrix Receiver for Mac 12.2 中的已知问题

Nov 03, 2016

Citrix Receiver for Mac 12.2 中的已知问题

在本版本中发现了以下已知问题：

- 如果重定向智能卡过程中运行了多个并发会话，Receiver 可能会挂起。

  [#511140]

- 用户可能无法在 HDX 应用程序窗口中使用 OS X 拆分视图功能。

  [#637963]

- 通过通用 USB 重定向功能重定向 USB CD/DVD 驱动器时，驱动器可能会被弹出。

  [#645484]

- 如果“USB 优化”策略设置为“捕获”，某些 USB 设备可能在会话中不起作用。

  [#649082]

- 在某些情况下，如果 USB 设备在客户端自动重新连接过程中连接，新 USB 设备通知屏幕可能无法正确显示。

  [#649714]

- 升级到 Receiver for Mac 12.2 后连接到帐户时，系统可能会提示用户提供钥匙串。

  [#649885]

- 在运行 Mac OS X 10.9 的系统中，HDX 会话中运行的 Microsoft 远程桌面客户端可能无法访问智能卡。

  [#650298]

- 会话重新连接后，可能不会重播会话可靠性重新连接过程中的按键。

  [#652154]

Citrix Receiver for Mac 12.1 中的已知问题

在本版本中发现了以下已知问题：

- Windows 登录消息显示时调整桌面窗口的大小可能会使会话失效。

  [#525833]

- 从 Chrome 启动虚拟桌面后，系统可能会显示错误消息。

  [#564961]

- 查看器未向服务器发送正确的键盘布局，导致出现键盘映射问题。

  [#581829]

- 将某个会话平滑漫游到 OS X 10.11 (El Capitan) 计算机时，该会话可能无法成功重新连接。 如果首次重新连接失败，请使用“刷新应用程序”菜单命令再次重新连接到该会话。

  [#601542]

Citrix Receiver for Mac 12 中的已知问题

在本版本中发现了以下已知问题：

- 在 OS X El Capitan (10.11) 上，虚拟桌面和应用程序通常不在拆分视图中显示。

  [#582397]

- 使用智能卡身份验证时，XenDesktop 会话无法启动。

  [#550781]

- 使用 PIV 智能卡时，Receiver 无法重新连接到 XenDesktop 5.6 会话。

  [#550986]

- 如果会话连接断开时已发布的命令提示窗口最小化，重新连接时命令提示窗口可能不重新显示。

  [#411702]

- 如果安装了多个证书，但其中的某些证书已过期，SSL SDK 可能会错误地将证书链标记为“已过期”。 从钥匙串访问中删除过期的证书将修复此问题。

  [#511574]

- 如果更新发生在用户订阅应用程序之后，在 Receiver 上查看到的应用程序名称可能无法反应 Broker 和 StoreFront 上的更新。 如果出现此问题，用户可以删除订阅，然后再重新订阅应用程序。

  [#515097]

- Windows 徽标消息显示时调整桌面窗口的大小可能会使会话失效。

  [#525833]

- 使用 OS X Mountain Lion (10.8) 时，如果将 Receiver 11.9 或 11.9.15 升级到 Receiver 12.0，启动 Receiver 可能会导致同时打开新版本的 Receiver 和旧版本的 Receiver。

  [#552496]

- 在 OS X 中使用 Google Chrome 浏览器时，双击下载栏上的 ICA 文件可能会导致启动多个 ICA 文件，进而导致出现错误消息。

  [#564961]

- 登录到 WI PNA 帐户时，用户可能无法更改过期的密码。 [#568394]
  用户在视频通话会话期间进入全屏模式时，XenDesktop 工具栏按钮的下端可能会被裁剪掉。

  [#570480]

- 计算机运行的是 OS X Mountain Lion (10.8) 的用户可能会在 Receiver 用户界面上看到字符串登录和下载图标重叠。 如果出现此问题，用户可以单击“登录”或用户名字符串，而不要单击下载图标。

  [#504302]

- 在 DirectX 或 OpenGL 应用程序运行期间将查看器更改为全屏可能会导致光标消失。

  [#510745]

- 将服务器语言设置为繁体中文时，用户可能无法在会话内输入“[”或“]”。

  [#511877]

- 如果状态变更是由于用户处于空闲状态所致，通过移动光标不会将 Lync 状态从“离开”更改为“可用”。 如果出现此问题，用户必须手动将状态更改为“可用”。

  [#512074]

- 在多显示器配置中，如果重新配置了某个显示器，无缝应用程序可能会移动到主显示器上。

  [#506532]

- HDX 应用程序可能变为黑屏。 如果出现此问题，请拖动应用程序，并通过单击关闭按钮应该所在的位置关闭这些应用程序。

  [#426991]

- 在 OS X Yosemite (10.10) 中，Safari 的升级版本可能会将 Receiver 作为弹出窗口加以阻止。 通过启用要打开的应用程序/桌面弹出窗口可修复此问题。

系统要求

Nov 03, 2016

支持的操作系统

本版本的 Citrix Receiver for Mac 支持以下操作系统：

- El Capitan (10.11)
- Yosemite (10.10)
- Mavericks (10.9)

> **注意**
>
> Mavericks 之前的 OS X 版本不受支持。

兼容的 Citrix 产品

下表列出了与本版本的 Citrix Receiver for Mac 兼容的 Citrix 产品（以及相应的版本）：

XenApp	XenDesktop	StoreFront	VDI-in-a-Box
Windows Server 2012 R2： • 7.9 • 7.8 • 7.7 • 7.6 • 7.5 Windows Server 2008 R2： • 6.5	7.9 7.8 7.7 7.6 7.5 7.1 7	3.6 3.5 3.0 2.6 2.5 2.1	5.4 5.3

兼容的浏览器

以下浏览器与本版本的 Citrix Receiver for Mac 兼容：

- Safari 6.0（或更高版本）
- Mozilla Firefox 22.x（或更高版本）
- Google Chrome 28.x（或更高版本）

硬件要求

- 130 MB 可用磁盘空间
- 用来连接服务器的正常运行的网络或 Internet 连接

- Web Interface：
  - 带 XenApp Services （又称为 PNAgent Services）站点的 Web Interface 5.4 for Windows，用于从 Receiver 以本机方式

访问应用程序，而非从 Web 浏览器访问。

- 部署 Receiver：
  - Citrix Receiver for Web 2.1、2.5 和 2.6
  - Citrix Web Interface 5.4

连接

如果在 OS X El Capitan 上运行 Citrix Receiver for Mac 12.2 的用户在连接时遇到问题，则需要升级 NetScaler Gateway 插件。有关详细信息，请参阅 Citrix 下载页面上的文章 NetScaler Gateway Plug-in v3.1.4 for Mac OS X (El Capitan Support)（适用于 Mac OS X（支持 El Capitan）的 NetScaler Gateway 插件 v3.1.4）。

Citrix Receiver for Mac 支持与 XenApp 或 XenDesktop 建立以下连接：

- HTTP
- HTTPS
- ICA-over-TLS

Citrix Receiver for Mac 支持以下配置：

对于 LAN 连接	**对于安全的远程连接或本地连接**
• 使用 StoreFront Services 或 Receiver for Web 站点的 StoreFront • 使用 XenApp Services 站点的 Web Interface 5.4 for Windows	Citrix NetScaler Gateway： • 11.1（包括 VPX） • 11.0（包括 VPX） • 10.5（包括 VPX） Citrix Access Gateway： • Enterprise Edition 10.x（包括 VPX） • Enterprise Edition 9.x（包括 VPX） • VPX Citrix Secure Gateway 3.x（仅与 Web Interface 结合使用）

有关使用 StoreFront 部署 Access Gateway 或 NetScaler Gateway 的信息，请参阅 Access Gateway 或 NetScaler Gateway 文档以及 StoreFront 文档。

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*

域直通 安全令牌	**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）** 是*	**NetScaler 到 StoreFront Services 站点（本机）** 是*
双因素（域 + 安全令牌）				是*	是*
SMS				是*	是*
智能卡**	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。

**要在 OS X 10.10 上使用智能卡，必须至少安装 OS X 10.10.2。

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	是
域直通				
安全令牌			是*	是
双因素（域 + 安全令牌）			是*	是
SMS			是*	是
智能卡**	是	是	是	是
用户证书			是（需要 NetScaler Gateway 插件）	是（需要 NetScaler Gateway 插件）

* 仅在包含 NetScaler Gateway 的部署中可用，而不管设备上是否已安装关联的插件。

安装、设置、升级、部署或删除 Citrix Receiver for Mac

Sep 09, 2016

此版本 Citrix Receiver for Mac 包含一个单独的安装包 CitrixReceiver.dmg，并支持通过 NetScaler Gateway、Access Gateway 和 Secure Gateway 进行远程访问。

在本文中：

安装

用户可以通过以下方法安装 Receiver：从 Citrix Web 站点安装、自动从 Receiver for Web 或 Web Interface 安装以及使用电子软件分发 (ESD) 工具安装。

由用户从 Citrix.com 安装：

- 从 Citrix.com 或自有下载站点获取 Receiver 的 Receiver 新用户可以通过输入电子邮件地址（而非服务器 URL）来设置一个帐户。 Receiver 确定与电子邮件地址关联的 NetScaler Gateway 或 StoreFront 服务器，然后提示用户登录并继续安装。此功能称为基于电子邮件的帐户发现。

> **注意**
>
> 首次使用的用户是指未在自己的用户设备上安装 Receiver 的用户。

- 如果 Receiver 是从 Citrix.com 以外的站点（例如 Receiver for Web 站点）下载的，则不会对首次使用的用户执行基于电子邮件的发现。
- 如果您的站点需要配置 Receiver，请使用备用部署方法。

从 Receiver for Web 或 Web Interface 自动安装

- 首次使用 Receiver 的用户可以通过输入服务器 URL 或下载置备文件来设置帐户。

使用电子软件分发 (Electronic Software Distribution, ESD) 工具安装

- 首次使用 Receiver 的用户必须输入服务器 URL 来设置帐户。

手动安装 Receiver for Mac

用户可以从 Web Interface、网络共享或从 Citrix Web 站点（网址为：http://www.citrix.com）将 CitrixReceiver.dmg 文件直接下载到用户设备来安装 Receiver。

安装 Receiver for Mac

1. 从 Citrix Web 站点下载要安装的 Receiver 版本的 .dmg 文件，并将其打开。
2. 在“简介”页面上，单击**继续**。
3. 在**许可证**页面上，单击**继续**。
4. 单击**同意**接受许可协议的条款。
5. 在**安装类型**页面上，单击**安装**。
6. 在本地设备上输入管理员的用户名和密码。

升级到 Receiver for Mac 12.2

支持从 Online Plug-in for Mac 11.x 进行升级。 也可以从 Receiver for Mac 11.3、11.4、11.5、11.6、11.7.x、11.8.x、11.9.x、12.0、12.1、12.1.100 进行升级。

> **Important**
>
> ShareFile 集成将从 11.8 版本中删除。 如果已将 Receiver for Mac 与 ShareFile 相集成，则升级时会提示您下载 ShareFile 应用程序，以便您可以继续访问您的远程数据。

关于部署和配置 Receiver for Mac

对于使用 StoreFront 的部署情形：

- 最佳做法是按照 Netscaler Gateway 和 StoreFront 文档中关于这些产品的描述配置 NetScaler Gateway 和 StoreFront 3.x。 将 StoreFront 创建的置备文件附加到电子邮件中，并通知用户在安装完 Receiver 后如何升级以及如何打开此置备文件。
- 作为使用置备文件的备选方法，也可以通知用户输入 NetScaler Gateway 的 URL。 如果您按 StoreFront 文档中所述配置了基于电子邮件的帐户发现，则可通知用户输入其电子邮件地址。
- 另一种方法是按 StoreFront 文档中所述配置一个 Receiver for Web 站点。 通知用户如何升级 Receiver、访问 Receiver for Web 站点以及从 Receiver for Web 界面下载置备文件（单击用户名，然后单击“激活”）。

对于使用 Web Interface 的部署：

- 升级带有 Receiver for Mac 12.2 的 Web Interface 站点，并告知用户升级 Receiver 的方法。 例如，可以在消息屏幕中向用户提供安装标题，以使用户知晓自己需要升级到最新版本的 Receiver。

从 Receiver for Web 部署 Receiver

可以从 Receiver for Web 部署 Receiver，以确保用户在尝试从浏览器连接到应用程序之前已安装 Receiver。 借助 Receiver for Web 站点，用户可以通过 Web 页面访问 StoreFront 应用商店。 如果 Receiver for Web 站点检测到用户没有 Receiver 的兼容版本，系统会提示用户下载并安装 Receiver。 有关详细信息，请参阅 StoreFront 文档。

从 Web Interface 登录屏幕部署 Receiver

此功能仅适用于支持 Web Interface 的 XenDesktop 和 XenApp 版本。

可以从 Web 页面部署 Receiver，以确保用户在尝试使用 Web Interface 之前安装了 Receiver。 Web Interface 提供了客户端检测和部署过程，用于检测可以将哪些 Citrix 客户端部署在用户环境中，然后引导用户完成部署过程。

可以将客户端检测和部署过程配置为在用户访问 XenApp Web 站点时自动运行。 如果 Web Interface 检测到用户没有

Receiver 的兼容版本，则会提示用户下载并安装 Receiver。

有关详细信息，请参阅 Web Interface 文档中的配置客户端部署。

移除 Receiver for Mac

您可以通过打开 CitrixReceiver.dmg 文件，选择**卸载 Citrix Receiver**，并按屏幕说明操作手动卸载 Receiver。

配置 Citrix Receiver for Mac

Sep 09, 2016

在安装 Receiver 软件之后，用户利用以下配置步骤可访问其托管应用程序和桌面：

- 配置 USB 重定向
- 配置会话可靠性
- 配置 CEIP
- 配置应用程序交付 - 确保您的 XenApp 环境已正确配置。 了解您的选择并向您的用户提供有意义的应用程序说明。
- 配置自助服务模式 — 配置自助服务模式，此模式允许您的用户从 Receiver 用户界面订阅应用程序。
- 配置 StoreFront — 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。
- 向用户提供帐户信息 — 向用户提供设置访问托管其应用程序和桌面的帐户时所需的信息。 在某些环境中，用户必须手动设置帐户的访问权限。
- 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 NetScaler Gateway 配置身份验证。 有关详细信息，请参阅 Netscaler Gateway。

配置 USB 重定向

HDX USB 设备重定向功能可将 USB 设备重定向到用户设备，或从用户设备重定向 USB 设备。 例如，用户可以将闪存驱动器连接到本地计算机，并从虚拟桌面或桌面托管应用程序中远程访问该驱动器。 在会话期间，用户可以使用即插即用设备，包括图片传输协议 (PTP) 设备（例如数码相机）、媒体传输协议 (MTP) 设备（例如数字音频播放器或便携式媒体播放器）、POS 设备以及其他设备（例如 3D Space Mice、扫描仪、签名板等）。

> **注意**
>
> 桌面托管应用程序会话不支持双跳 USB。

以下 Receiver 可使用 USB 重定向功能：

- Windows
- Linux
- Macintosh

默认情况下，会允许某些类型的 USB 设备使用 USB 重定向功能，而拒绝其他类型的 USB 设备使用。 您可以通过更新支持重定向功能的 USB 设备的列表来限制可用于虚拟桌面的 USB 设备类型，如本部分内容后面部分中所述。

> **提示**
>
> 对于需要将用户设备和服务器安全分离的环境，Citrix 建议告知用户应避免使用的 USB 设备类型。

经过优化的虚拟通道可用于重定向最常用的 USB 设备，并可以通过 WAN 提供卓越的性能和带宽效率。 通常情况下，经过优化的虚拟通道即是最佳选择，尤其对于存在高延迟的环境更是如此。

> **注意**

> 为了执行 USB 重定向，Receiver 将以处理鼠标的相同方式来处理 SMART 板。

此产品支持对 USB 3.0 设备和 USB 3.0 端口使用优化的虚拟通道，例如，用于查看摄像机上的文件或向耳麦提供音频的 CDM 虚拟通道。 此产品还支持连接到 USB 2.0 端口的 USB 3.0 设备的通用 USB 重定向。

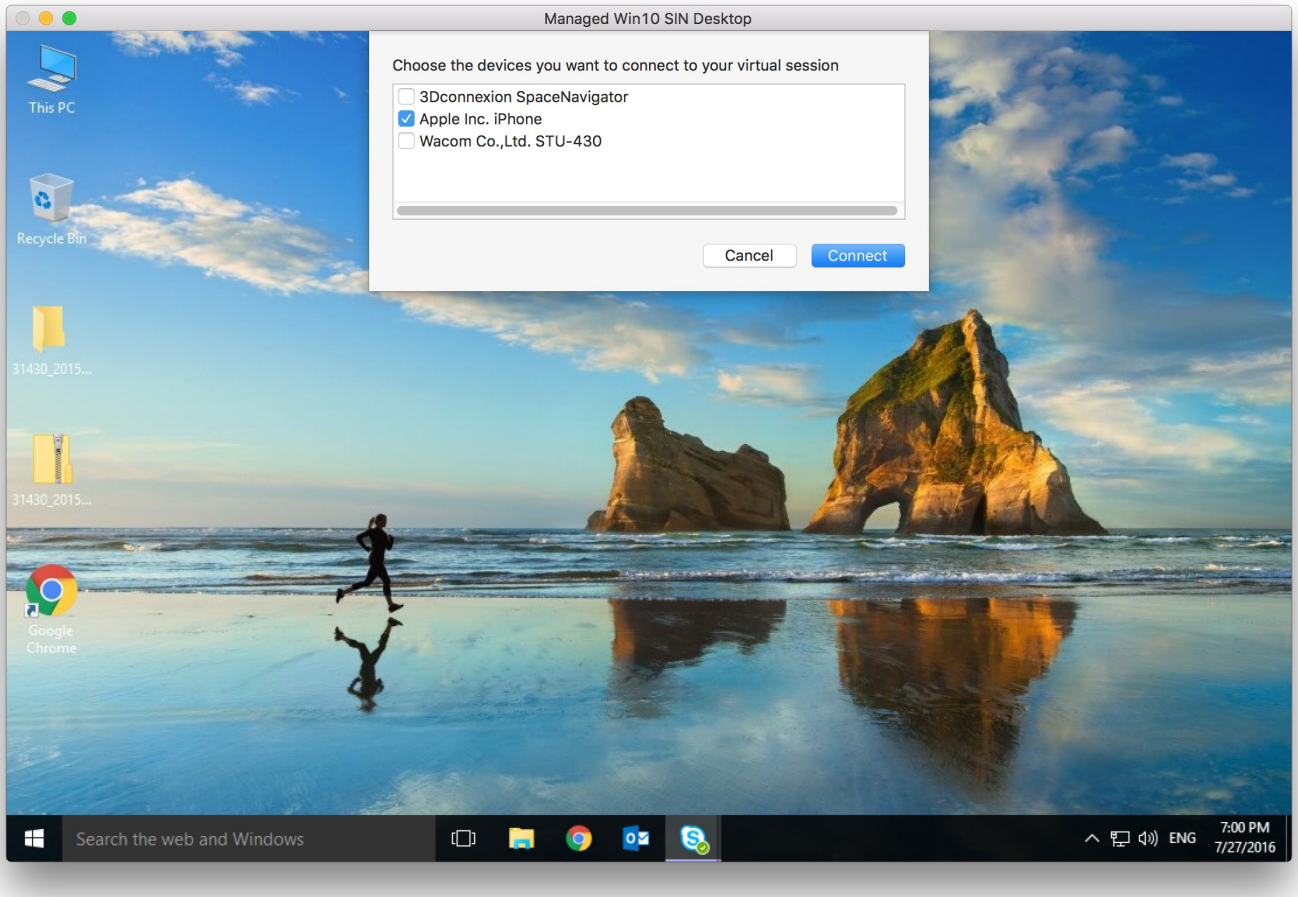
一些特定于设备的高级功能，如网络摄像机上的人体学接口设备 (HID) 按钮，在优化的虚拟通道中可能无法按预期运行；如果发生此问题，请使用通用 USB 虚拟通道。

默认情况下不会重定向某些设备，这些设备只能用于本地会话。 例如，不应对直接通过内部 USB 连接的网络接口卡进行重定向。

要使用 USB 重定向，请执行以下操作：

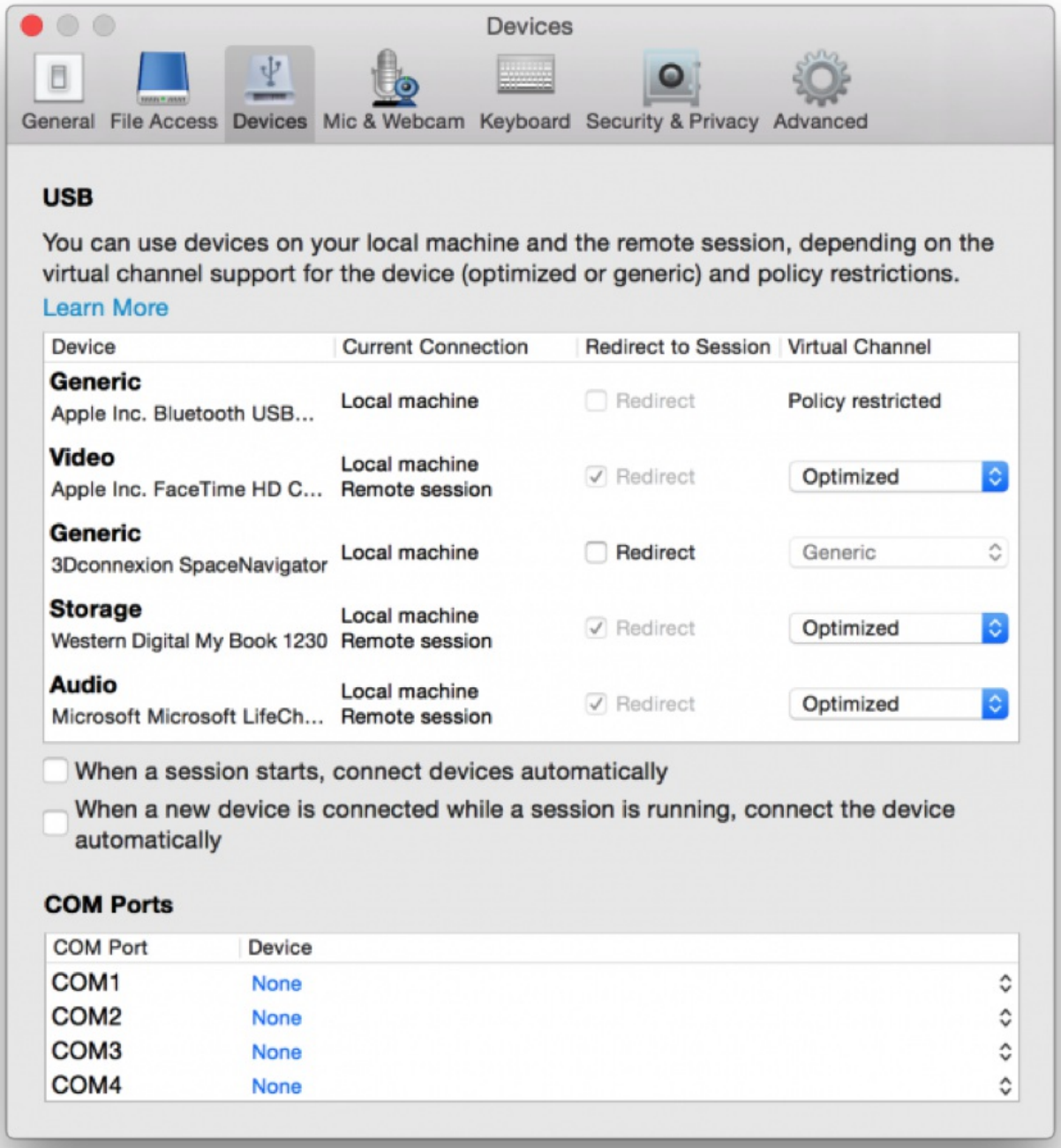
1. 将 USB 设备连接到安装了 Receiver 的设备。

2. 系统将提示您选择本地系统中可用的 USB 设备。



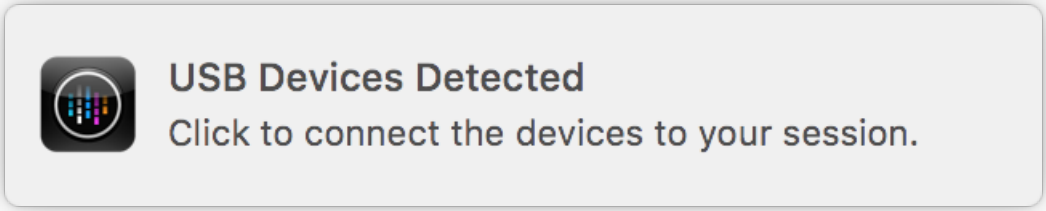
3. 选择要连接的设备，然后单击**连接**。 如果连接失败，则将显示一条错误消息。

4. 在**首选项**窗口中的**设备**选项卡上，连接的 USB 设备将在 USB 面板中列出：



5. 选择适用于 USB 设备的虚拟通道类型，即*通用*或*优化*.

6. 此时将显示一条消息。 单击可将 USB 设备连接到您的会话：



使用和删除 USB 设备

用户可以在启动虚拟会话之前或之后连接 USB 设备。 当使用 Receiver for Macintosh 时，以下情况适用：

- 在会话启动后连接的设备将立即显示在 Desktop Viewer 的 USB 菜单中。
- 如果 USB 设备未正确重定向，可等到虚拟会话启动后再连接设备，这样有时候可以解决这一问题。
- 为避免数据丢失，请使用 Windows **安全删除**菜单来移除 USB 设备。

配置会话可靠性

会话可靠性使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。 用户仍然可以看到他们正在使用的应用程序，直至网络连接恢复。

会话可靠性可使会话在服务器上保持活动状态。 为指示连接已断开，用户的显示内容将冻结，直至用户到达通道的另一端后恢复连接。 用户在连接中断期间可继续访问显示内容，在网络连接恢复后可继续与应用程序交互。 会话可靠性可重新连接用户而不提示进行重新身份验证。

> **Important**
>
> Citrix Receiver for Mac 用户无法覆盖服务器设置。

可将会话可靠性与安全套接字层 (SSL) 一起使用。

> **注意**
>
> SSL 仅对用户设备和 NetScaler Gateway 之间发送的数据进行加密。

使用会话可靠性策略

会话可靠性连接策略设置可允许或阻止会话可靠性。

会话可靠性超时策略设置的默认值为 180 秒（3 分钟）。 您可以延长通过会话可靠性使会话保持打开状态的时间长度，此功能的主要目标是为用户提供方便，因此，它不会提示用户重新进行身份验证。

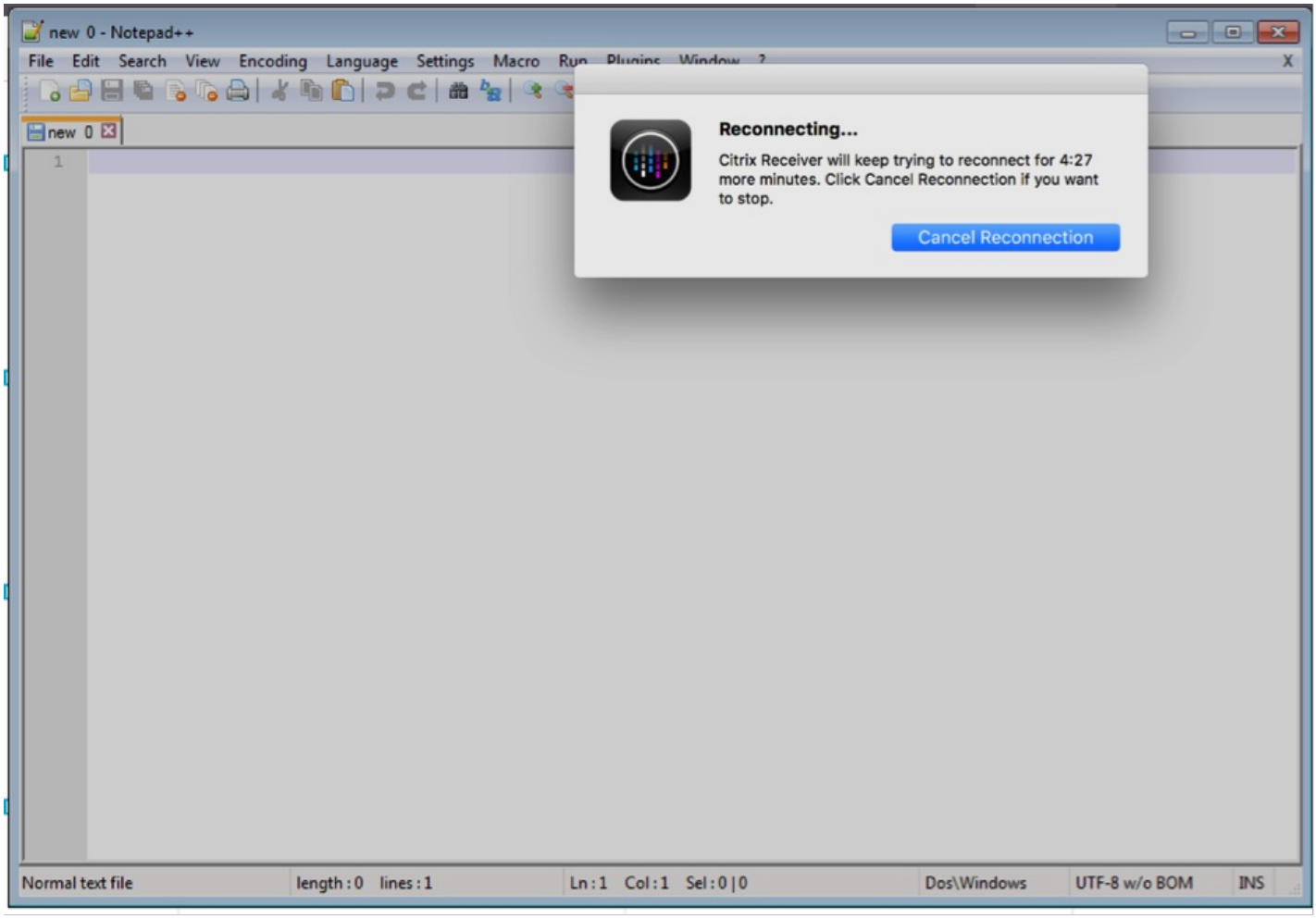
> **提示**
>
> 但是，如果您延长会话保持打开状态的时间，则可能导致用户感到不耐烦而离开用户设备，从而使未经授权的用户有机会访问该会

话。

传入会话可靠性连接使用端口 2598，除非您更改“会话可靠性端口号”策略设置中定义的端口号。

如果您不希望用户无需重新进行身份验证即可重新连接到已中断的会话，请使用客户端自动重新连接功能。 您可以配置“客户端自动重新连接身份验证”策略设置，以便在用户重新连接到中断的会话时提示用户重新进行身份验证。

如果您同时使用了会话可靠性和客户端自动重新连接，这两项功能将按顺序发挥作用。 经过在“会话可靠性超时”策略设置中指定的时间长度之后，会话可靠性将关闭或断开用户会话。 之后，“客户端自动重新连接”策略设置将生效，尝试将用户重新连接到断开连接的会话。



注意

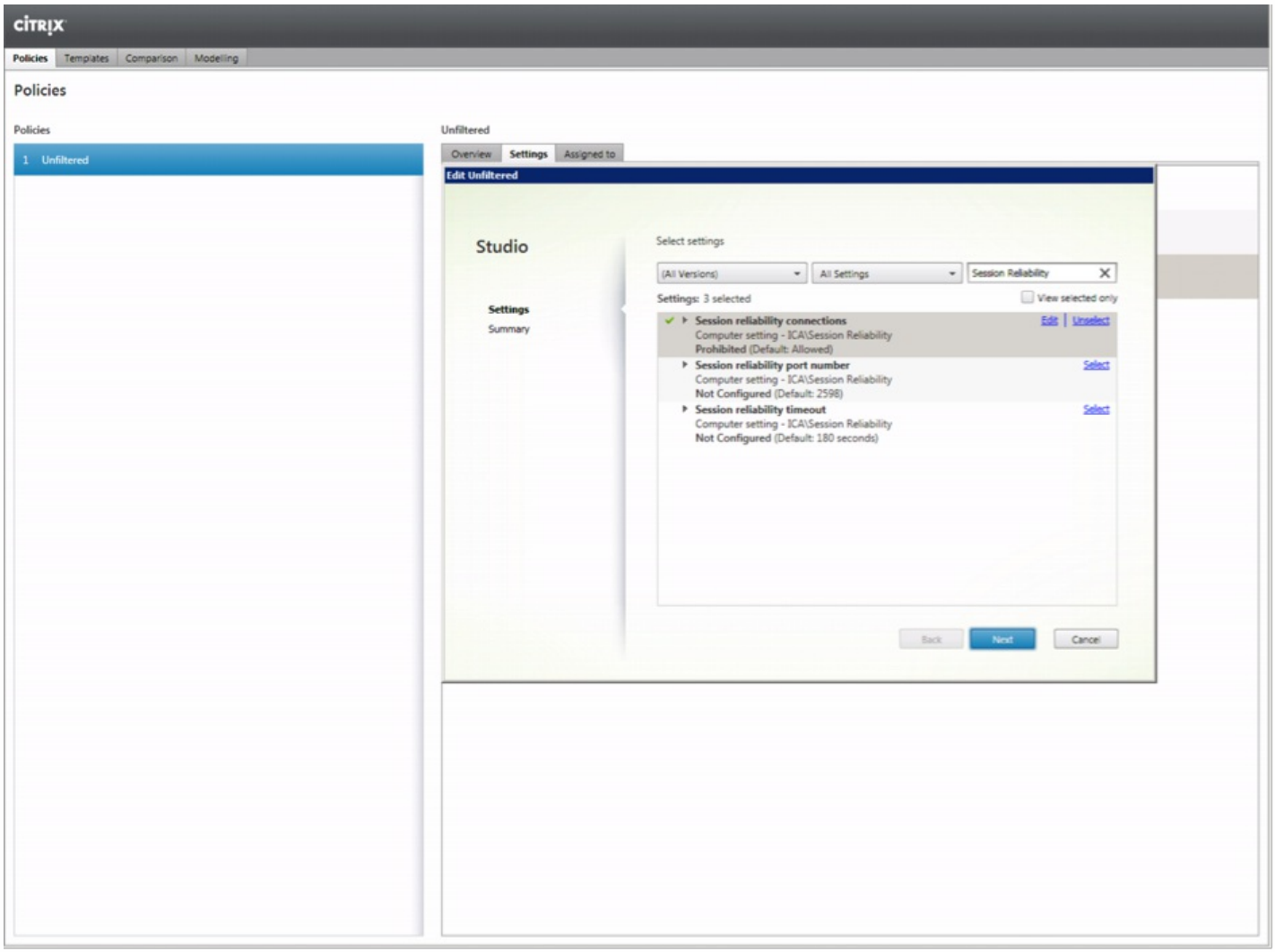
会话可靠性默认在服务器端启用。 要禁用此功能，请配置服务器管理的策略。

配置会话可靠性

默认情况下，会话可靠性处于启用状态。

要禁用会话可靠性，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**会话可靠性连接**策略。
3. 将策略设置为**禁止**。

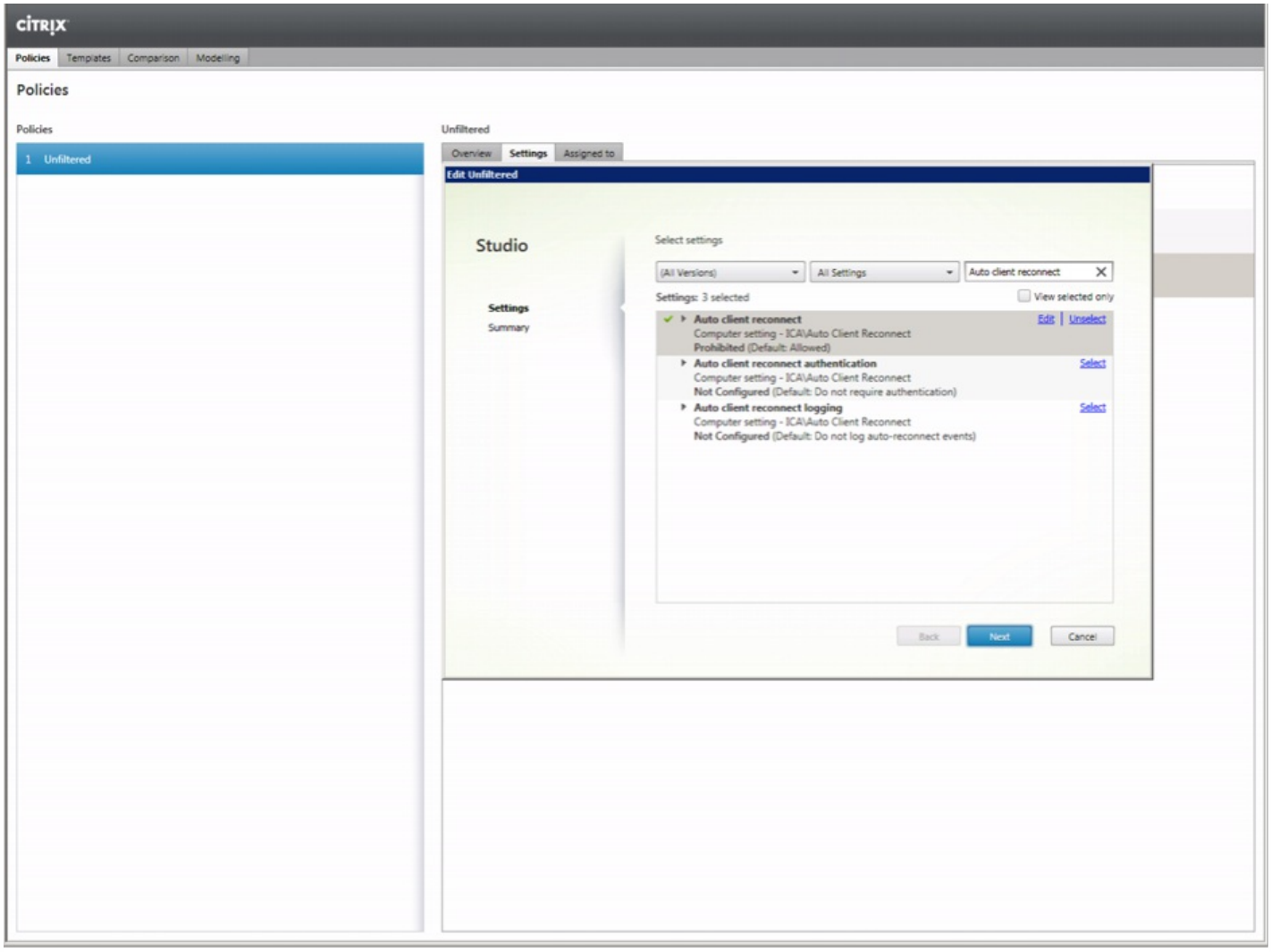


配置客户端自动重新连接

默认情况下，客户端自动重新连接处于启用状态。

要禁用客户端自动重新连接，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开**客户端自动重新连接策略**。
3. 将策略设置为**禁止**。



客户端自动重新连接和会话可靠性交互

尝试保持活动 Citrix Receiver 会话的链路完整性时，在各种接入点之间切换、网络中断以及与延迟有关的显示超时方面的移动性挑战使得环境非常具有挑战性。 为解决此问题，Citrix 增强了本版本的 Receiver for Mac 中使用的会话可靠性和自动重新连接技术。

客户端自动重新连接以及会话可靠性允许用户在从网络中断恢复时自动重新连接到其 Citrix Receiver 会话。 可以使用这些通过 Citrix Studio 中的策略启用的功能来大大改进用户体验。

> ## 注意
>
> 可以使用 StoreFront 中的 **default.ica** 文件来修改客户端自动重新连接和会话可靠性超时值。

客户端自动重新连接

可以使用 Citrix Studio 策略启用或禁用客户端自动重新连接。 默认情况下，此功能处于启用状态。 有关修改此策略的信息，请参阅本文前面的客户端自动重新连接部分。

使用 StoreFront 中的 default.ica 文件可修改 AutoClientReconnect 的连接超时值；默认情况下，此超时值设置为 120 秒（或 2 分钟）。

设置	示例	默认值
TransportReconnectRetryMaxTimeSeconds	TransportReconnectRetryMaxTimeSeconds=60	120

会话可靠性

可以使用 Citrix Studio 策略启用或禁用会话可靠性。 默认情况下，此功能处于启用状态。 有关修改此策略的信息，请参阅本文前面的会话可靠性部分。

使用 StoreFront 中的 **default.ica** 文件可修改会话可靠性的连接超时值；默认情况下，此超时值设置为 180 秒（或 3 分钟）。

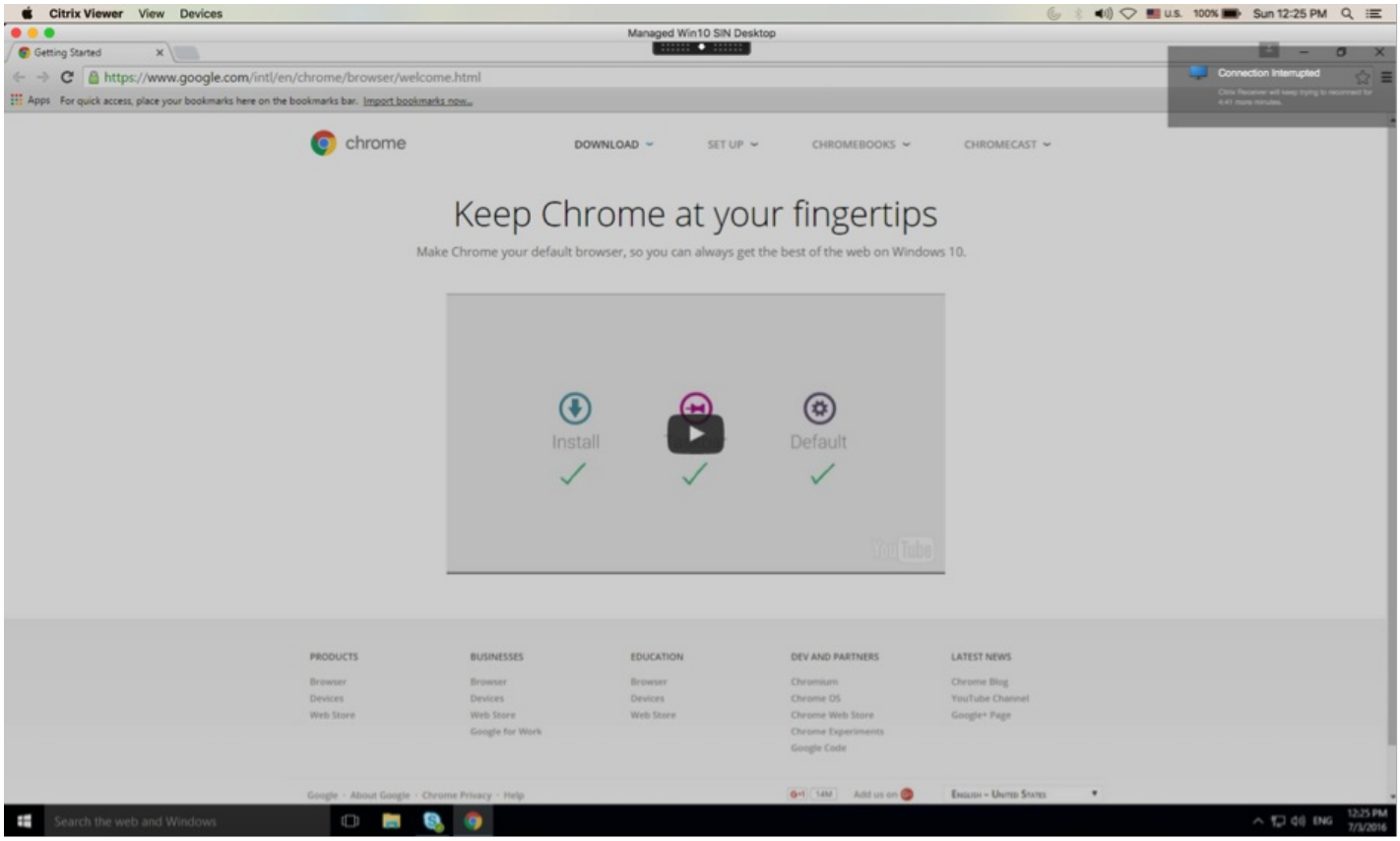
设置	示例	默认值
SessionReliabilityTTL	SessionReliabilityTTL=120	180

客户端自动重新连接和会话可靠性的工作原理

为 Citrix Receiver 启用客户端自动重新连接和会话可靠性时，请注意以下事项：

- 重新连接过程中会话窗口变为灰色；倒计时器显示重新连接会话之前的剩余时间。 会话超时后将断开连接。

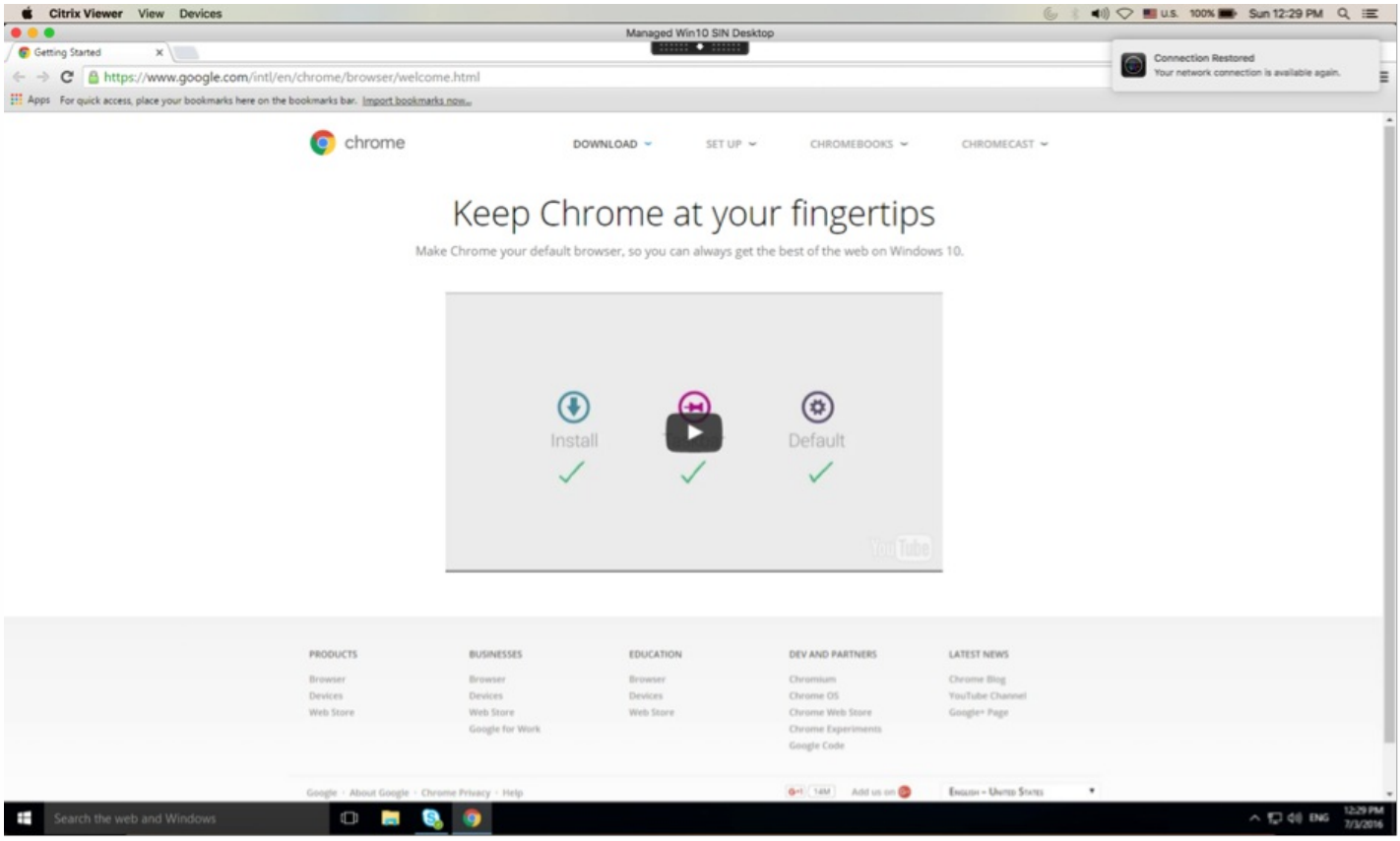
默认情况下，重新连接倒计时器通知从 5 分钟开始倒计时；此时间值表示每个计时器（客户端自动重新连接和会话可靠性）的总默认值，即分别为 2 分钟和 3 分钟。 下图显示了在会话界面的右上角显示的倒计时器通知：



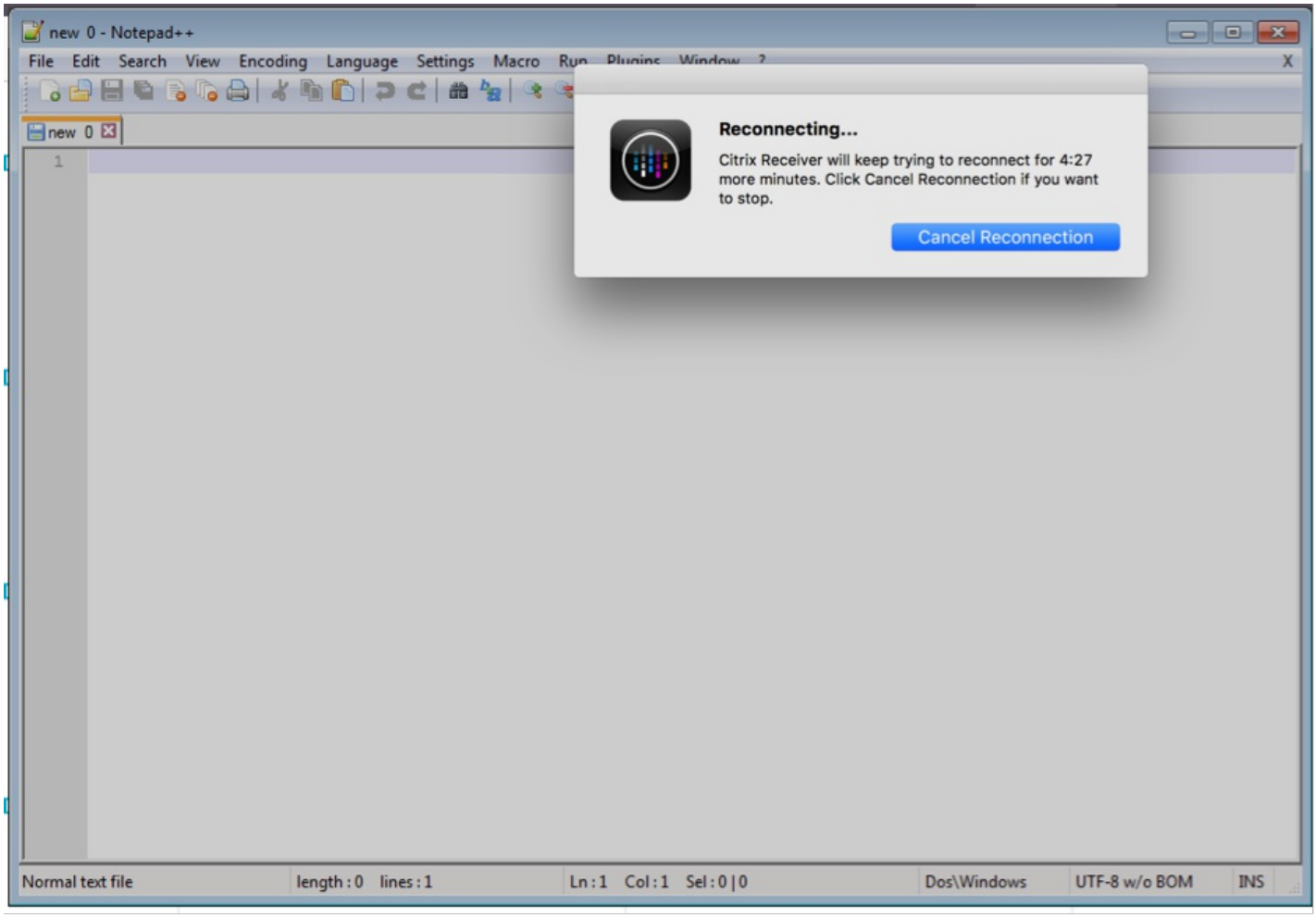
提示

可以使用命令提示符更改用于不活动会话的灰度亮度。 例如，默认写入 com.citrix.receiver.nomas NetDisruptBrightness 为 80。 默认情况下，此值设置为 80。 最大值不能超过 100（表示透明窗口），可以将最小值设置为 0（完全显示黑屏）。

- 会话成功重新连接时（或者会话断开连接时）用户会收到通知。 此通知在会话界面的右上角显示：



- 客户端自动重新连接和会话可靠性控制的会话窗口提供一条指示会话重新连接状态的信息性消息。 单击**取消重新连接**可移回活动会话。



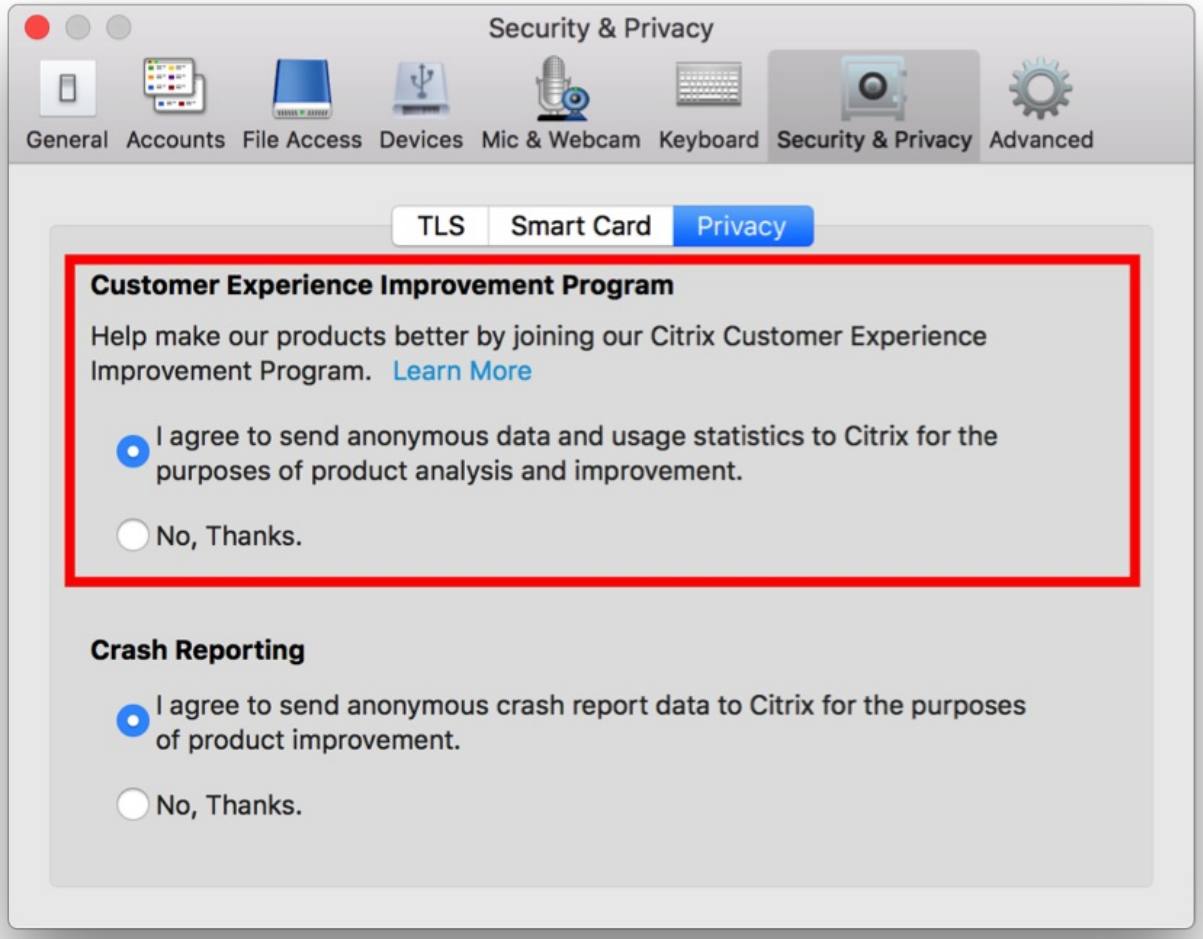
配置 CEIP

安排 CEIP 的目的是收集数据并默认每隔 7 天将数据安全地上载到 Citrix。 可以随时使用 Receiver 的“安全性和首选项”屏幕来更改您的 CEIP 参与情况。

> ### 提示
>
> 禁用 CEIP 时，将上载仅包含所安装的 Receiver for Mac 版本的最少信息；仅上载一次。 此最少信息对 Citrix 非常有价值，因为这可以提供客户使用的不同版本的分布情况。 此信息仅在禁用 CEIP 时上载一次。

要禁用 CEIP，或者要放弃参与，请执行以下操作：

1. 在**首选项**屏幕中，选择**安全性和隐私**。
2. 选择**隐私**选项卡。
3. 更改恰当的单选按钮。 例如，要禁用 CEIP，请单击**不，谢谢**。
4. 单击**确定**。



配置应用程序交付

通过 XenDesktop 或 XenApp 交付应用程序时，请考虑采用以下方案增强用户访问其应用程序时的体验：

Web 访问模式

如果未执行任何配置，Receiver for Mac 将提供 Web 访问模式：基于浏览器访问应用程序和桌面。 用户只需要打开浏览器访问 Receiver for Web 或 Web Interface 站点，选择并使用所需的应用程序。 在 Web 访问模式下，不会将任何应用程序快捷方式放置在用户设备上的应用程序文件夹中。

自助服务模式

通过将 StoreFront 帐户添加到 Receiver 中或将 Receiver 配置为指向 StoreFront 站点，可以配置自助服务模式，在此模式下，用户可以从 Receiver 订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。 在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。 当其中一个用户选择应用程序时，该应用程序的快捷方式将放置到用户设备上的应用程序文件夹中。

访问 StoreFront 3.0 站点时，您的用户将看到 Receiver 技术预览版用户体验。 有关 Receiver 技术预览版用户体验的详细信

息，请参阅 Receiver 和 StoreFront 3.0 技术预览版。

在 XenApp 场中发布应用程序时，要增强通过 StoreFront 应用商店访问这些应用程序的用户的体验，请务必包含已发布的应用程序的有意义的说明。 这些说明通过 Citrix Receiver 向用户显示。

配置自助服务模式

如上文所述，通过将 StoreFront 帐户添加到 Receiver 中或将 Receiver 配置为指向 StoreFront 站点，可以配置自助服务模式，在此模式下，用户可以从 Receiver 用户界面订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。

在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。

- 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的末尾。 用户登录到该应用商店时，将自动置备相应的应用程序，无需用户手动订阅。
- 要向用户公告应用程序，或者在 Receiver 的精选列表中列出常用的应用程序，以使其更易于查找，请将字符串 KEYWORDS:Featured 附加到应用程序说明后面。

有关详细信息，请参阅 StoreFront 文档。

如果 XenApp 部署中的 Web Interface 没有 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。 有关详细信息，请参阅 Web Interface 文档。

配置 StoreFront

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 StoreFront 文档。

   注意：对于需要更大控制权的管理员，Citrix 提供了一个模板，供您创建 Receiver 下载站点。
2. 为 CloudGateway 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 Receiver 进行特殊配置。 有关详细信息，请参阅 StoreFront 文档中的
   — 配置应用商店
   。

向用户提供帐户信息

安装后，必须向用户提供访问其托管应用程序和桌面所需的帐户信息。 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) 记录确定与电子邮件地址相关联的 NetScaler Gateway、Access Gateway 或 StoreFront 服务器，然后提示用户登录以访问其托管的应用程序和桌面。

要配置 DNS 服务器以支持基于电子邮件的发现，请参阅 StoreFront 文档中的
— Configuring Email-based Account Discovery
（配置基于电子邮件的帐户发现）主题。

要配置 NetScaler Gateway 或 Access Gateway 以接受用户通过使用电子邮件地址发现 StoreFront、NetScaler Gateway 或 Access Gateway URL 来进行连接，请参阅 NetScaler Gateway 或 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，用户只需打开此文件即可配置 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

您可以使用 Citrix Receiver for Mac Setup URL Generator 创建包含帐户信息的 URL。 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。

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 应用商店或 XenApp Services 站点的 URL；例如：https://servername.example.com
- 要使用 NetScaler Gateway 或 Access Gateway 进行访问：NetScaler Gateway 或 Access Gateway 地址、产品版本以及所需的身份验证方法
  有关配置 NetScaler Gateway 或 Access Gateway 的详细信息，请参阅 NetScaler Gateway 或 Access 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。

优化 Citrix Receiver for Mac 环境

Nov 03, 2016

可以按以下各项进行操作来优化您的环境，以从 Receiver 获得最佳性能：

- 自动重新连接用户
- 重新启动桌面
- 提供会话可靠性
- 为漫游用户提供连续性
- 映射客户端设备
- 映射客户端驱动器
- 映射客户端 COM 端口

自动重新连接用户

由于网络不稳定、网络延迟变化无常或者无线设备的覆盖范围受限等原因，用户可能会从其会话断开连接。 通过客户端自动重新连接功能，Citrix Receiver 可以检测到 ICA 会话的意外断开连接，并自动将用户重新连接到受影响的会话。

在服务器上启用此功能后，用户无需手动进行重新连接即可继续工作。 Citrix Receiver 将一直尝试重新连接会话，直到重新连接成功或者用户取消重新连接尝试为止。 如果需要进行用户身份验证，则在自动重新连接过程中会向用户显示一个请求凭据的对话框。 如果用户未经注销而退出应用程序，则不会进行自动重新连接。

使用服务器上的策略设置配置客户端自动重新连接。 有关详细信息，请参阅 XenApp 和 XenDesktop 文档。

重新启动桌面

如果虚拟桌面无法启动、建立连接的时间过长或遭到破坏，用户可以重新启动虚拟桌面。 您需要在 XenDesktop 中配置此功能。

用户订阅的所有桌面上以及用户的“应用程序”页面上均提供了上下文菜单项**重新启动**。 如果没有为桌面启用重新启动，则将禁用此菜单项。 当用户选择“重新启动”时，Receiver 会关闭桌面，然后再启动桌面。

> **Important**
>
> 重新启动桌面会导致数据丢失，请知悉。

提供会话可靠性

启用会话可靠性功能后，如果连接中断，用户仍然可以继续看到托管应用程序和桌面窗口。 例如，无线用户在进入通道时可能会失去他们的连接，而当它们出现在通道另一头时，将会重新获得连接。 在这样的中断期间，会话可靠性功能使会话窗口在恢复连接的过程中一直保持显示状态。

您可以将系统配置为在不能获得连接时向用户显示一个警告对话框。

使用服务器上的策略设置配置会话可靠性。 有关会话可靠性和 Receiver 交互的详细信息，请参阅与确保提供最高质量的服务和可靠性有关的文档。

有关策略特定的其他信息，请参阅客户端自动重新连接策略设置和会话可靠性策略设置。

> **提示**
>
> Receiver 用户无法覆盖会话可靠性对应的服务器设置。

> **Important**
>
> 如果启用了会话可靠性，则用于会话通信的默认端口将由 1494 转变为 2598。

为漫游用户提供连续性

工作区控制功能使桌面和应用程序可以随用户在设备之间移动。 例如，可使医院的临床医生在使用不同的工作站时，无需在每个设备上都重新启动自己的桌面和应用程序。

换到新的用户设备时，策略和客户端驱动器映射会相应地发生变化。 策略和映射的应用要取决于当前用来登录会话的用户设备。 例如，如果医护人员从医院急救室的用户设备注销，然后登录到医院 X 光实验室中的工作站，那么在用户登录到此 X 光实验室中的用户设备后，适用于 X 光实验室中会话的策略、打印机映射和客户端驱动器映射就会立即针对此会话生效。

配置工作区控制设置

1. 单击 Receiver 窗口中的下箭头图标，然后选择“首选项”。
2. 单击“常规”选项卡。
3. 选择以下方法之一：
   - Reconnect apps when I start Receiver（我启动 Receiver 时重新连接应用程序）。 允许用户在启动 Receiver 时重新连接到中断的应用程序。
   - 我启动或刷新应用程序时重新连接应用程序。 允许用户在启动应用程序或从 Citrix Receiver 菜单中选择“刷新应用程序”时重新连接到中断的应用程序。

映射客户端设备

Receiver 会自动映射本地驱动器和设备，使其在会话中可用。 如果已在服务器上启用，则客户端设备映射会允许在服务器上运行的远程应用程序或桌面访问连接到本地用户设备的设备。 可以执行以下操作：

- 访问本地驱动器、COM 端口和打印机
- 收听从会话播放的音频（系统声音和音频文件）

> **注意**
>
> 客户端音频映射和客户端打印机映射不需要在用户设备上进行任何配置。

映射客户端驱动器

客户端驱动器映射允许您在会话期间访问用户设备上的本地驱动器，例如，CD-ROM 驱动器、DVD 和 USB 内存条。 如果服务器配置为允许客户端驱动器映射，用户将可以访问本地存储的文件，在会话期间处理这些文件，然后将其保存在本地驱动器或服务器驱动器上。

Receiver 负责监视 CD-ROM、DVD 和 USB 内存条等硬件设备在用户设备上的常规装载目录，在会话期间出现的任何新设备装载目录都将自动映射服务器上下一个可用的驱动器盘符。

可以使用 Receiver 的首选项配置映射驱动器的读取和写入访问权限级别。

配置映射驱动器的读取和写入访问权限

1. 在 Receiver 主页中，单击下箭头图标，然后单击“首选项”。
2. 单击“设备”。
3. 从以下选项中选择映射驱动器的读取和写入访问权限的级别：
   - 读写
   - 只读
   - 无访问权限
   - 每次都询问
4. 从打开的会话中注销，并重新连接以应用更改。

映射客户端 COM 端口

通过客户端 COM 端口映射，在会话期间将可以使用与用户设备 COM 端口连接的设备。 可以像使用任何其他网络映射那样使用这些映射。

Macintosh 串行端口不提供 Windows 应用程序使用的所有控制信号线。 不提供 DSR（数据设置就绪）、DCD（设备载波检测）、RI（振铃指示）和 RTS（请求发送）线。 依靠这些信号进行硬件握手和流控制的 Windows 应用程序可能无法运行。 串行通信的 Macintosh 实现仅依靠 CTS（清除发送）和 DTR（数据终端就绪）线进行输入和输出硬件握手。

映射客户端 COM 端口

1. 在 Receiver 主页中，单击下箭头图标，然后单击首选项。
2. 单击设备。
3. 从映射的 COM 端口列表中选择您要映射的 COM 端口。 这是在会话中显示的虚拟 COM 端口，而非本地计算机上显示的物理端口。
4. 从设备弹出菜单中选择要与虚拟 COM 端口相关联的设备。
5. 启动 Receiver 并登录到服务器。
6. 运行命令提示窗口。 在提示窗口中，键入
   net use comx: \\client\comz:

   其中，x 是服务器上的 COM 端口号（端口 1 到 9 可用于映射），z 是客户端 COM 端口号（端口 1 到 4 可用）。
7. 要确认该映射，请在提示符下键入net use 。 此时会显示映射的驱动器、LPT 端口和映射的 COM 端口的列表。

改进 Citrix Receiver for Mac 中的用户体验

Sep 09, 2016

可以通过支持的以下功能提升用户的体验：

- 客户体验改善计划 (CEIP)
- ClearType 字体平滑
- 客户端麦克风输入
- Windows 特殊按键
- Windows 快捷方式和按键组合
- 使用输入法编辑器 (IME) 和国际键盘布局
- 使用多个显示器
- 使用桌面工具栏

客户体验改善计划 (CEIP)

Citrix 客户体验改善计划 (CEIP) 从 Receiver for Mac 收集匿名配置和使用数据，并自动将数据发送到 Citrix。 此数据可帮助 Citrix 改善 Receiver 的品质、可靠性和性能。 有关详细信息，请参阅配置 CEIP。

ClearType 字体平滑

ClearType 字体平滑功能（又称为子像素字体渲染功能）可提高所显示字体的质量，实现传统字体平滑或消除锯齿功能所无法实现的效果。

如果在服务器上启用 ClearType 字体平滑，并不是要强制用户设备使用 ClearType 字体平滑， 而是允许服务器在本地已启用 ClearType 字体平滑且使用 Receiver 的用户设备上提供对该功能的支持。

Receiver 将自动检测用户设备的字体平滑设置，并将其发送到服务器。 会话将使用此设置进行连接。 会话断开连接或终止后，服务器的设置将还原为其原始设置。

客户端麦克风输入

Receiver 支持多客户端麦克风输入。 本地安装的麦克风可用于：

- 实时活动，例如软件电话通话和网络会议。
- 托管的录制应用程序，例如听写程序。
- 视频和音频录制。

Receiver 支持数字听写。 有关配置此功能的信息，请参阅产品文档站点上的音频功能信息。

通过在 Receiver“首选项”的“麦克风和网络摄像机”选项卡中选择以下选项之一，可以选择在会话中是否使用连接到用户设备的麦克风：

- 使用我的麦克风和网络摄像机
- 不使用我的麦克风和网络摄像机
- 每次都询问

如果您选中**每次都询问**，每次您连接到托管应用程序或桌面时都会出现一个对话框，询问您是否要在该会话中使用您的麦克风。

Windows 特殊按键

Receiver 提供了许多额外的选项和更为方便的方式来用 Mac 按键替换 Windows 应用程序中的特殊按键（如功能键）。 可以使用键盘选项卡按以下方式配置各选项：

- “发送 Control 字符时使用”使您能够选择在会话中是否发送 Command-字符键组合作为 Ctrl+字符键组合。 如果从弹出菜单中选择“Command 或 Control”，则可将 Mac 上熟悉的 Command-字符或 Ctrl-字符键组合作为 Ctrl+字符键组合发送到 PC。 如果选择 Control，则必须使用 Ctrl-字符键组合。
- “发送 Alt 字符时使用”使您能够选择在会话中如何复制 Alt 键。 如果选择 Command-Option，则可以在会话中发送 Command-Option-键组合作为 Alt+键组合。 或者，如果选择 Command，则可以使用 Command 键作为 Alt 键。
- 利用“使用 Command (右侧)发送 Windows 徽标键”，按下键盘右侧的 Command 键，即可将 Windows 徽标键发送至远程桌面和应用程序。 如果禁用此选项，根据首选项面板中的以上两个设置，右侧的 Command 键行为将与左侧的 Command 键相同，但您仍可以使用“键盘”菜单发送 Windows 徽标键；选择“键盘”>“发送 Windows 快捷方式”>“开始”。
- “发送未更改的特殊按键”使您能够禁用特殊按键的转换。 例如，组合选项-1（在数字键盘上）相当于特殊按键 F1。 通过选中“发送未更改的特殊按键”复选框，您可以更改此行为，并在会话中将此特殊按键设置为表示 1（数字键盘上的数字一）。 默认情况下，不会选中此复选框，因此会将选项-1 作为 F1 发送到会话。

可以使用键盘菜单向会话发送功能和其他特殊按键。

如果您的键盘上有数字键盘，您还可以使用以下按键：

PC 按键或操作	Mac 选项
插入	数字键盘上的 0（数字零）。 必须关闭 Num Lock；您可以使用 Clear 按键将其打开或关闭。 Option-Help
删除	数字键盘上的小数点。 必须关闭 Num Lock；您可以使用 Clear 按键将其打开或关闭。 Clear
F1 至 F9	数字键盘上的选项-1 至 -9（数字一至九）
F10	数字键盘上的选项-0（数字零）
F11	数字键盘上的选项-减号
F12	数字键盘上的选项-加号

Windows 快捷方式和按键组合

远程会话会识别文本输入的大部分 Mac 键盘组合，例如 Option-G 用于输入版权符号 ©。 但是，在会话期间您按下的一些按键不会显示在远程应用程序或桌面上，而是由 Mac 操作系统解析。 这可能转而演变成触发 Mac 响应的按键。

您可能不希望使用某些 Windows 键，如很多 Mac 键盘没有的 Insert 键。 同样，有些 Windows 8 键盘快捷方式显示超级按钮和应用程序命令，可以捕获和切换应用程序。 这些快捷方式是 Mac 键盘本身无法模仿的，但是可以使用“键盘”菜单发送到远程桌面或应用程序。

不同机器之间，键盘和按键的配置方式可能大不相同。 因此，Receiver 提供了多个选项，以确保可以将按键正确地转发给托管

应用程序和桌面。 下表中列出了这些选项。 其中说明了默认行为。 如果您调整默认行为（使用 Receiver 或其他首选项），可能会转发不同的按键组合，并可能会在 Remote PC 上观察到其他行为。

> **Important**
>
> 使用较新的 Mac 键盘时，下表中列出的某些按键组合不可用。 在大多数情况下，可以使用“键盘”菜单将键盘输入发送到会话。

下表中使用的约定：

- 字母键大写，这并不表示应同时按下 Shift 键。
- 按键之间的连字符表示应同时按这些键（例如，Control-C）。
- 字符键是创建文本输入的键，包括所有字母、数字和标点符号；特殊键是本身不产生输入，但起到修改和控制作用的键。 特殊键中包括 Control、Alt、Shift、Command、Option、箭头键和功能键。
- 菜单说明与会话中的菜单相关。
- 根据用户设备的配置，一些键组合可能不会产生预期的效果，此时会列出备用组合。
- Fn 指的是 Mac 键盘上的 Fn (Function) 键；功能键指 PC 或 Mac 键盘上的 F1 至 F12 键。

Windows 键或按键组合	Mac 上具有相同作用的按键
Alt+字符键	Command–Option–字符键（例如，要发送 Alt-C，则使用 Command-Option-C）
Alt+特殊键	Option–特殊键（例如，Option-Tab） Command–Option–特殊键（例如，Command-Option-Tab）
Ctrl+字符键	Command–字符键（例如，Command-C） Control–字符键（例如，Control-C）
Ctrl+特殊键	Control–特殊键（例如，Control-F4） Command–特殊键（例如，Command-F4）
Ctrl/Alt/Shift/Windows 徽标键 + 功能键	选择“键盘”>“发送功能键”>“Control/Alt/Shift/Command-功能键”
Ctrl+Alt	Control-Option-Command
Ctrl+Alt+Delete	Control–Option–向前删除键 Control-Option-Fn-Delete（在 MacBook 键盘上） 选择“键盘”>“发送 Ctrl-Alt-Del”

Delete	Delete 选择“键盘”>“发送按键”> Delete Fn-Backspace（有些美国键盘上为 Fn-Delete）
End	End Fn-右箭头键
Esc	Escape 选择“键盘”>“发送按键” > Escape
F1 至 F12	F1 至 F12 选择“键盘”>“发送功能键”> F1 至 F12
Home	Home Fn–左箭头键
Insert	选择“键盘”>“发送按键”> Insert
Num Lock	Clear
Page Down	Page Down Fn–下箭头键
Page Up	Page Up Fn–上箭头键
空格键	选择“键盘”>“发送按键”> Space
Tab	选择“键盘”>“发送按键” > Tab
Windows 徽标	右侧的 Command 键（键盘首选项，默认情况下已启用） 选择“键盘”>“发送 Windows 快捷方式”>“开始”
显示超级按钮的按键组合	选择“键盘”>“发送 Windows 快捷方式”>“超级按钮”
显示应用程序命令的按键组合	选择“键盘”>“发送 Windows 快捷方式”>“应用命令”

捕获应用程序的按键组合	选择“键盘”>“发送 Windows 快捷方式”>“贴靠”
切换应用程序的按键组合	选择“键盘”>“发送 Windows 快捷方式”>“切换应用”

使用输入法编辑器 (IME) 和国际键盘布局

Receiver 允许您在用户设备或服务器上使用输入法编辑器 (IME)。

启用客户端 IME 时，用户可以在插入点，而不是单独的窗口编写文本。

Receiver 还允许用户指定自己要使用的键盘布局。

启用客户端 IME

1. 从 Citrix Viewer 菜单栏，选择键盘 > 国际化 > 使用客户端 IME。
2. 请确保将服务器端 IME 设置为直接输入或字母模式。
3. 使用 Mac IME 来编写文本。

在编写文本时明确指示起点

- 从 Citrix Viewer 菜单栏，选择键盘 > 国际化 > 使用组合标记。

使用服务器端 IME

- 请确保将客户端 IME 设置为字母数字模式。

映射的服务器端 IME 输入模式键

Receiver 会为 Mac 键盘上没有的服务器端 Windows IME 输入模式键提供键盘映射。 在 Mac 键盘上，Option 键会映射到以下服务器端 IME 输入模式键，具体取决于服务器端区域设置：

服务器端系统区域设置	服务器端 IME 输入模式键
日语	**汉字键**（Alt + 日语键盘的半角/全角）
韩语	**右侧 Alt 键**（韩语键盘上的朝鲜语/英语切换）

使用国际键盘布局

- 请确保将客户端和服务器端键盘布局都设置为与默认服务器端输入语言相同的区域设置。

使用多个显示器

用户可以通过菜单选项**在全屏模式下使用所有显示器**，将 Receiver for Mac 设置为跨多个显示器在全屏模式下运行。

已知限制

全屏模式仅在一个显示器或所有显示器上受支持，这可以通过菜单项进行配置。

使用桌面工具栏

用户现在可以在窗口模式和全屏模式两种模式下访问桌面工具栏。 之前，工具栏仅在全屏模式下可见。 其他工具栏变更还包括：

- 已从工具栏删除 **Home**（主页）按钮。 可以通过使用以下命令执行此功能：
  - 按 Cmd-Tab 以切换到上一个活动应用程序。
  - 按 Ctrl-向左箭头键以切换到上一个空间。
  - 使用内置触控板或 Magic Mouse 手势以切换到其他空间。
  - 在全屏模式下将光标移动到屏幕边缘，从而显示一个基站，您可以在此处选择要处于活动状态的应用程序。
- 已从工具栏删除 **Windowed**（窗口）按钮。 可以通过以下方式离开全屏模式以进入窗口模式：
  - 对于 OS X 10.10，单击下拉菜单栏上的绿色窗口按钮。  或 
  - 对于 OS X 10.7、10.8 和 10.9，单击下拉菜单栏上的蓝色菜单按钮。 
  - 对于 OS X 的所有版本，从下拉菜单栏的**查看**菜单中选择**退出全屏幕**。
- 已更新工具栏的拖放行为，可支持在采用多个显示器的全屏模式中的窗口之间拖放。

智能卡身份验证的要求

Nov 03, 2016

Receiver for Mac 支持在以下配置中使用智能卡身份验证：

- 对使用基于浏览器的访问的 Receiver for Web/StoreFront 2.x 及更高版本、XenDesktop 5.6 及更高版本或 XenApp 6.5 及更高版本进行智能卡身份验证。
- 支持智能卡的应用程序（例如 Microsoft Outlook 和 Microsoft Office）允许用户对虚拟桌面或应用程序会话中的文档进行数字签名或加密。
- 使用多个证书 — Receiver for Mac 支持将多个证书与一个或多个智能卡结合使用。 如果用户将智能卡插入读卡器，这些证书可用于在用户设备上运行的所有应用程序，包括 Citrix Receiver。
- 在双跳会话中 – 如果需要使用双跳，则需要在 Receiver 与用户的虚拟桌面之间建立更进一步的连接。

关于对 NetScaler 进行智能卡身份验证

如果智能卡上存在多个可用证书，则使用智能卡对连接进行身份验证时，Citrix Receiver 会提示您选择证书。 选择证书时，Citrix Receiver 会提示您输入智能卡密码；通过身份验证后，会话将启动。

如果智能卡上只有一个适用证书，Citrix Receiver 会使用该证书，不提示您进行选择。 但是，您仍必须输入与该智能卡关联的密码以对连接进行身份验证以及启动会话。

为智能卡身份验证指定 PKCS#11 模块

使用 Citrix Receiver 的“首选项”窗口中的高级配置选项时，可以指定使用 PKCS#11 模块进行身份验证：

1. 在 Citrix Receiver 中，选择**首选项**。
2. 在“首选项”窗口中，单击**安全性和隐私**。
3. 在**安全性和隐私**部分中，单击**智能卡**。
4. 在“PKCS#11”字段中，选择恰当的模块；单击**其他**浏览到 PKCS#11 模块所在的位置（如果未列出所需模块）。
5. 选择恰当的模块后，单击**添加**。

> **注意**
>
> 不强制安装 PKCS#11 模块。

支持的读卡器、中间件和智能卡配置文件

Receiver for Mac 支持大部分 Mac OS X 兼容的智能卡读卡器和加密的中间件。 Citrix 已验证以下各项的操作。

支持的读卡器：

- 通用 USB 连接智能卡读卡器

支持的中间件：

- Clariify
- Activeidentity 客户端版本
- Charismathics 客户端版本

支持的智能卡：

- PIV 卡
- 通用访问卡 (CAC)
- Gemalto .NET 卡

请按照供应商的 Mac OS X 兼容智能卡读卡器和加密中间件提供的配置用户设备的说明进行操作。

限制

- 证书必须存储在智能卡上，而非存储在用户设备上。
- Receiver for Mac 不保存用户所做的证书选择。
- Receiver for Mac 不存储或保存用户的智能卡 PIN。 PIN 的获取由操作系统进行处理，而操作系统可能有自己的缓存机制。
- 插入智能卡后，Receiver for Mac 不重新连接会话。
- 要将智能卡身份验证与 VPN 隧道结合使用，用户必须安装 NetScaler Gateway 插件并通过 Web 页登录，在每一步都使用智能卡和 PIN 进行身份验证。 使用 NetScaler Gateway 插件通过直通身份验证访问 StoreFront 不适用于智能卡用户。

相关详细信息

请参阅：

- Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV SmartCard Authentication (PDF)（为 Citrix XenDesktop 7.6 和 NetScaler Gateway 10.5 配置 PIV 智能卡身份验证）(PDF)
- Smart Card Support with Citrix Receiver for Mac 11.9.15 on OS X 10.10.2（OS X 10.10.2 上 Mac 11.9.15 的智能卡支持）

确保 Citrix Receiver 通信安全

Sep 09, 2016

在本文中：

要确保服务器场与 Citrix Receiver 之间的通信安全，可将与服务器场建立的连接与一系列的安全技术集成在一起，其中包括 Citrix NetScaler Gateway。 有关通过 Citrix StoreFront 配置此连接的信息，请参阅 StoreFront 文档。

> **注意**
>
> Citrix 推荐使用 NetScaler Gateway 以确保 StoreFront 服务器和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 Citrix Receiver 与服务器之间的连接。 Citrix Receiver 支持 SOCKS 和安全代理协议。
- Secure Gateway。 您可以使用 Secure Gateway 和 Web Interface，通过 Internet 为公司内部网络的服务器提供单一、安全的加密访问点。
- SSL Relay 解决方案与传输层安全性 (TLS) 协议
- 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 Receiver 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。

关于证书

专用（自签名）证书

如果远程网关上安装了专用证书，用户设备上必须安装组织的证书颁发机构颁发的根证书，才能使用 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。

在 Receiver for Mac 设备上导入根证书

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给设备上已配置的帐户。 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 Mac 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，则必须将该中间证书映射到 NetScaler Gateway 服务器证书。 有关此任务的信息，请参阅 NetScaler Gateway 文档。 有关在 NetScaler Gateway 设备上安装中间证书并将其与主 CA 链接的详细信息，请参阅 How to Install and Link Intermediate Certificate with Primary CA on NetScaler Gateway（如何在 NetScaler Gateway 上安装中间证书并将其与主 CA 链接）一文。

通过 NetScaler Gateway 进行连接

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

如果在网络中部署 XenMobile，应通过将 NetScaler 与 StoreFront 相集成的方式来允许内部用户或远程用户通过 NetScaler 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 Citrix Receiver 进行连接。

有关通过 NetScaler Gateway 配置这些连接的信息，请参阅将 NetScaler Gateway 与 NetScaler 相集成文档。

与 Secure Gateway 连接

本主题仅适用于使用 Web Interface 的部署。

可以在 Normal（普通）模式或 Relay（中继）模式下使用 Secure Gateway，来为 Receiver 与服务器之间的通信提供安全通道。 如果在“Normal”（普通）模式下使用 Secure Gateway，并且用户通过 Web Interface 进行连接，则不需要对 Receiver 进行任何配置。

Receiver 使用在 Web Interface 服务器上远程配置的设置连接到运行 Secure Gateway 的服务器。 有关为 Receiver 配置代理服务器设置的详细信息，请参阅 Web Interface 文档。

如果安全网络中的服务器上安装了 Secure Gateway 代理，则可以在“Relay”（中继）模式下使用 Secure Gateway 代理。 有关“Relay”（中继）模式的详细信息，请参阅 XenApp 和 Secure Gateway 文档。

如果使用“Relay”（中继）模式，Secure Gateway 服务器将相当于一个代理，并且必须对 Receiver 进行配置才能使用：

- Secure Gateway 服务器的完全限定的域名 (FQDN)。
- Secure Gateway 服务器的端口号。 请注意，Secure Gateway 2.0 版本不支持“Relay”（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。

通过代理服务器进行连接

代理服务器用于限制网络的入站和出站访问，并处理 Receiver 与服务器之间的连接。 Receiver 既支持 SOCKS 又支持安全代理

协议。

与 XenApp 或 XenDesktop 服务器通信时，Receiver 使用在 Web Interface 服务器上远程配置的代理服务器设置。 有关为 Receiver 配置代理服务器设置的信息，请参阅 Web Interface 文档。

在与 Web 服务器进行通信时，Receiver 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配置默认 Web 浏览器的代理服务器设置。

通过防火墙进行连接

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，Receiver 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 通信（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 进行通信）。 对于 Receiver 到 Citrix 服务器的通信，防火墙必须允许在端口 1494 和 2598 上进行入站 ICA 通信。

如果防火墙进行了网络地址转换 (NAT) 配置，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 XenApp 或 XenDesktop 服务器未配置有备选地址，则可以将 Web Interface 配置为向 Receiver 提供备选地址。 然后，Receiver 使用外部地址和端口号连接服务器。 有关详细信息，请参阅 Web Interface 文档。

使用安全套接字层 (SSL) 中继进行连接

可以将 Receiver 与 Receiver for Mac 12.0 中包含的安全套接字层 (SSL) Relay 服务相集成；Receiver for Mac 12.0 支持 TLS 1.0、1.1 和 1.2，并且支持对 Citrix Receiver 与 XenApp/XenDesktop 之间的 TLS 连接使用以下密码套件：

- 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

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

默认情况下，Citrix SSL Relay 使用 Citrix 服务器上的 TCP 端口 443 进行 TLS 安全通信。 SSL Relay 收到 TLS 连接时，会先将数据解密，然后再重定向到服务器，或者，如果用户选择了 TLS+HTTPS 浏览，则重定向到 Citrix XML Service。

可以使用 Citrix SSL Relay 来保障以下情况下的通信安全：

- 在启用 TLS 的 Receiver 与服务器之间。
- 在 XenApp 服务器与 Web 服务器之间（通过运行 Web Interface 的服务器）。

有关配置和使用 SSL Relay 来确保安装安全或将 Web Interface 服务器配置为使用 TLS 加密的信息，请参阅 XenApp 和 Web Interface 文档。

注意

Citrix Receiver for Mac 对 Receiver 与 StoreFront 之间的连接使用平台 (OS X) 加密。

为 TLS 配置并启用 Receiver

TLS 的设置主要涉及两个步骤：

1. 在 XenApp 或 XenDesktop 服务器和 Web Interface 服务器上设置 SSL Relay，以及获取和安装所需的服务器证书。 有关详细信息，请参阅 XenApp 和 Web Interface 文档。
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 TLS 的 Receiver 与服务器场之间，如果要使用 TLS 来确保通信安全，用户设备上必须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。

Mac OS X 附带了约 100 个已安装的商用根证书，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 Mac OS X 钥匙串中。

将根证书添加到钥匙串中

1. 双击包含证书的文件。 这会自动启动“钥匙串访问”应用程序。
2. 在“添加证书”对话框中，从“钥匙串”弹出菜单中选择以下各项之一：
   - 登录（证书仅适用于当前用户。）
   - 系统（证书适用于设备的所有用户。）
3. 单击“确定”。
4. 在“鉴定”对话框中键入密码，然后单击“好”。

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

关于 SSL 策略

本部分内容介绍与在 Citrix Receiver for Mac 12.0 中通过 SSL 为 ICA 会话配置安全策略有关的信息。 您可以配置在 Citrix Receiver 中用于 ICA 连接的某些 SSL 设置。 这些策略不在用户界面中显示；更改这些策略需要在运行 Receiver 的设备上运行命令。

注意

可以通过其他方式管理 SSL 策略，例如当设备由 OS X 服务器或其他移动设备管理解决方案控制时。

SSL 策略包括以下设置：

SecurityComplianceMode。 为策略设置安全合规性模式。 如果未配置 SecurityComplianceMode，FIPS 将用作默认值。 此设置的适用值包括：

- **None**。 不强制使用合规性模式
- **FIPS**。 使用 FIPS 加密模块
- **SP800-52**。 强制使用 NIST SP800-52r1 合规性

将 SecurityComplianceMode 设置为 SP800-52： 复制

```
defaults write com.citrix.receiver.nomas SecurityComplianceMode SP800-52
```

SecurityAllowedTLSVersions。 此设置指定协议协商期间应接受的 TLS 协议版本。 此信息以阵列方式表示，支持可能值的任意组合。 如果未配置此设置，值 TLS10、TLS11 和 TLS12 将用作默认值。 此设置的适用值包括：

- **TLS10**。 指定允许使用的 TLS 1.0 协议。
- **TLS11**。 指定允许使用的 TLS 1.1 协议。
- **TLS12**。 指定允许使用的 TLS 1.2 协议。

将 SecurityAllowedTLSVersions 设置为 TLS 1.1 和 TLS 1.2： 复制

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

SSLCertificateRevocationCheckPolicy。 此功能可以改善 Citrix 服务器的加密身份验证，提高客户端设备与服务器之间的 SSL/TLS 连接的整体安全性。 此设置控制使用 OS X 客户端时尝试通过 SSL 打开远程会话期间如何对待指定的可信根证书授权机构。

启用此设置时，客户端将检查服务器的证书是否已吊销。 存在多种级别的证书吊销列表检查。 例如，可以将客户端配置为只检查其本地证书列表，也可以配置为同时检查本地和网络证书列表。 此外，还可以将证书检查机制配置为只有在验证了所有证书吊销列表之后才允许用户登录。

证书吊销列表 (CRL) 检查是部分证书颁发者支持的高级功能。 CRL 检查允许管理员在出现证书私钥的密码泄漏时或者只是 DNS 名称意外变更时吊销安全证书（在过期日期之前已失效）。

此设置的适用值包括：

- **NoCheck**。 不执行证书吊销列表检查。
- **CheckWithNoNetworkAccess**。 执行证书吊销列表检查。 仅使用本地证书吊销列表存储。 所有分发点都被忽略。 对于目标 SSL Relay/Secure Gateway 服务器出示的服务器证书验证来说，查找证书吊销列表并不重要。
- **FullAccessCheck**。 执行证书吊销列表检查。 使用本地证书吊销列表存储和所有分发点。 对于目标 SSL Relay/Secure Gateway 服务器出示的服务器证书验证来说，查找证书吊销列表并不重要。
- **FullAccessCheckAndCRLRequired**。 执行证书吊销列表检查，但根 CA 除外。 使用本地证书吊销列表存储和所有分发点。 查找所有必要的证书吊销列表对验证非常重要。
- **FullAccessCheckAndCRLRequiredAll**。 执行证书吊销列表检查，包括根 CA。 使用本地证书吊销列表存储和所有分发点。 查找所有必要的证书吊销列表对验证非常重要。

> **注意**
>
> 如果未设置 SSLCertificateRevocationCheckPolicy，FullAccessCheck 将用作默认值。

将 SSLCertificateRevocationCheckPolicy 设置为 FullAccessCheckAndCRLRequred： 复制

```
defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy FullAccessCheckAndCRLRequired
```

配置 SSL 策略

要在非托管计算机上配置 SSL 设置，请在 Terminal.app 中运行 **defaults** 命令。

defaults 是可用于添加、编辑和删除 OS X 首选项 plist 文件中的应用程序设置的命令行应用程序。

要更改设置，请执行以下操作：

1. 打开“应用程序”>“实用工具”>“终端”。

2. 在“终端”中，运行以下命令：

    defaults write com.citrix.receiver.nomas

其中：

：上述设置的名称。

：用于标识设置类型的开关，-string 或 -array。 如果设置类型为字符串，则可以忽略此开关。

：设置的值。 如果值为阵列，并且您指定了多个值，则必须使用空格分隔各个值。

例如： 复制

```
defaults write com.citrix.receiver.nomas SecurityAllowedTLSVersions -array TLS11 TLS12
```

还原为默认配置

要将设置重置回其默认值，请执行以下操作：

1. 打开“应用程序”>“实用工具”>“终端”。

2. 在“终端”中，运行以下命令：

    defaults delete com.citrix.receiver.nomas

其中：

：上述设置的名称。

例如：

复制

```
defaults delete com.citrix.receiver.nomas SecurityAllowedTLSVersions
```

使用用户界面配置安全性设置

最新版本的 Citrix Receiver for Mac（版本 12.2）中引入了多项安全性改进功能和增强功能，其中包括：

- 改进了安全性配置用户界面。 在早期版本中，更改与安全性有关的设置的首选方法是使用命令行；与会话安全性有关的配置设置现在非常简单，可从用户界面进行访问，这改进了为采用安全性有关的首选项创建无缝方法时的用户体验。
- 查看 TLS 连接。Citrix Receiver for Mac 允许您验证与使用特定 TLS 版本的服务器建立的连接，其他信息包括用于连接的加密算法、模式、密钥大小以及是否已启用 SecureICA。 此外，还可以查看用于 TLS 连接的服务器证书。

改进后的**安全性和隐私**屏幕包括 **TLS** 选项卡中的下列几个新选项：

- 设置合规模式
- 配置加密模块
- 选择恰当的 TLS 版本
- 选择证书吊销列表
- 对所有 TLS 连接启用设置

下图说明了可从用户界面访问的“安全性和隐私”设置：