适用于 Mac 的 Citrix Workspace 应用程序

Contents

关于此版本

July 22, 2021

> 重要
>
> 自 macOS Catalina 起，Apple 已经强制执行了对根 CA 证书和管理员必须配置的中间证书的额外要求。有关详细信息，请参阅 Apple 支持文章 HT210176。

2107 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。

2106 中的新增功能

通过 **301** 重定向支持自定义 **URL**

Citrix Workspace 应用程序现在允许您添加通过 HTTP 301 重定向从 StoreFront 或 Citrix Gateway 重定向到 Citrix Workspace 的 URL。

如果要从 StoreFront 迁移到 Citrix Workspace，则可以通过 HTTP 301 重定向将 StoreFront URL 重定向到 Citrix Workspace URL。因此，添加旧的 StoreFront URL 时，系统会自动将您重定向到 Citrix Workspace。

重定向示例：

StoreFront URL `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` 可以重定向到 Citrix Workspace URL `https://<Citrix Workspace url>/Citrix/Roaming/Accounts`。

> 注意：
>
> - 由于 Microsoft 的待定变更，适用于 Mac 的 Citrix Workspace 应用程序不支持 Microsoft Teams 的双音多频 (DTMF) 功能。
> - 自本版本起，Citrix Viewer 的版本号与 Citrix Workspace 应用程序的版本号可能不匹配。此变更不会影响您的体验。

2104 中的新增功能

适用于 Mac 的 Citrix Workspace 应用程序支持用户手动登录网络共享，但贵组织启用了单点登录时除外。要访问共享网络位置，请打开 Citrix Workspace 应用程序，导航到文件 > 网络共享并提供凭据。有关设置网络共享的详细信息，请参阅创建和管理存储区域连接器。

2102 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。

2101 中的新增功能

Apple 芯片（**M1** 芯片）支持

适用于 Mac 的 Citrix Workspace 应用程序现在支持在 macOS Big Sur（11.0 及更高版本）上使用 Rosetta 2 的 Apple 芯片设备（M1 芯片）。因此，所有第三方虚拟通道都必须使用 Rosetta 2。否则，这些虚拟通道可能无法在 macOS Big Sur（11.0 及更高版本）上适用于 Mac 的 Citrix Workspace 应用程序中工作。有关 Rosetta 的详细信息，请参阅Apple 支持文章。

实现无缝应用程序会话的 **Microsoft Teams** 优化支持

适用于 Mac 的 Citrix Workspace 应用程序现在支持 Microsoft Teams 优化，以实现无缝应用程序会话。因此，您可以从 Workspace 应用程序中将 Microsoft Teams 作为应用程序启动。有关详细信息，请参阅以下内容：

- Microsoft Teams 优化
- Microsoft Teams 重定向

Microsoft Teams 支持双音多频 **(DTMF)**

适用于 Mac 的 Citrix Workspace 应用现在支持与 Microsoft Teams 中的电话系统（例如 PSTN）和电话会议进行双音多频 (Dual-Tone Multifrequency, DTMF) 信号交互。默认情况下启用此功能。

2012 中的新增功能

Apple 芯片（**M1** 芯片）支持预览版

适用于 Mac 的 Citrix Workspace 应用程序现在在预览版中支持 Apple 芯片设备（M1 芯片）。

通过 **Microsoft Teams** 进行的屏幕共享优化

适用于 Mac 的 Citrix Workspace 应用程序现在支持通过 Microsoft Teams 进行的屏幕共享优化有关详细信息，请参阅以下主题：

- Microsoft Teams 优化
- Microsoft Teams 重定向

性能改进

此版本解决了多个有助于改进整体性能和稳定性的问题。

2010 中的新增功能

身份验证增强功能

为了提供无缝体验，身份验证对话框现在会显示在 Citrix Workspace 应用程序中。应用商店详细信息显示在登录屏幕上。身份验证令牌已加密并存储，以便您在系统重新启动或会话重新启动时不需要重新输入凭据。

> 注意：
>
> 此身份验证增强功能仅适用于云部署。

macOS Big Sur 支持

macOS Big Sur (11.0.1) 支持适用于 Mac 的 Citrix Workspace 应用程序。

性能改进

此版本解决了多个有助于改进整体性能和稳定性的问题。

2009 中的新增功能

Microsoft Teams 优化（预览版）

使用 Citrix Virtual Apps and Desktops 和 Citrix Workspace 应用程序为基于桌面的 Microsoft Teams 进行优化。Microsoft Teams 优化类似于 Microsoft Skype for Business 的 HDX RealTime 优化。不同的是，我们将 Microsoft Teams 优化所需的所有组件捆绑到 VDA 和适用于 Mac 的 Workspace 应用程序中。适用于 Mac 的 Citrix Workspace 应用程序将支持音频和视频以及 Microsoft Teams 优化。

有关详细信息，请参阅以下主题：

- Microsoft Teams 优化
- Microsoft Teams 重定向
- 已知问题

macOS Big Sur Beta 上的适用于 **Mac** 的 **Citrix Workspace** 应用程序

适用于 Mac 的 Citrix Workspace 应用程序 2009 已在 macOS Big Sur Beta 8 上测试。请在测试环境中使用此设置并提供您的反馈。有关 macOS Big Sur Beta 的特定问题，请参阅已知问题部分。

> 小心：
>
> 请勿在生产环境中在 macOS Big Sur Beta 版本中使用适用于 Mac 的 Citrix Workspace 应用程序。

用于 **USB** 重定向的内核扩展

适用于 Mac 的 Citrix Workspace 应用程序 2009 不再依赖于 USB 重定向的内核扩展 (KEXT)。

2008 中的新增功能

性能改进

此版本解决了多个有助于改进整体性能和稳定性的问题。

macOS 版本支持

适用于 Mac 的 Citrix Workspace 应用程序 2008 是支持 macOS 版本 High Sierra (10.13) 和 Mojave (10.14) 的最后一个版本。

2007 中的新增功能

性能改进

此版本解决了多个有助于改进整体性能和稳定性的问题。

2006 中的新增功能

更新了 **Citrix Analytics** 服务

Citrix Workspace 应用程序经过检测，可以从您从浏览器启动的 ICA 会话安全地将数据传输到 Citrix Analytics 服务。有关 Citrix Analytics 如何使用此信息的详细信息，请参阅性能自助服务和Virtual Apps and Desktops 的自助搜索。

网络摄像头重定向的 **H.264** 支持

适用于 Mac 的 Citrix Workspace 应用程序现在支持 H.264（又称为 MPEG-4 AVC）视频压缩标准。因此，已发布的 64 位应用程序现在可以使用网络摄像头重定向。

稳定性改进

此版本解决了多个有助于改进整体稳定性的问题。

2005 中的新增功能

语言支持

适用于 Mac 的 Citrix Workspace 应用程序现在提供意大利语版本。

性能改进

- 此版本解决了几个有助于提高 Citrix Workspace（云应用商店）的整体性能和稳定性的问题。
- 在本版本中，云用户将注意到登录时间和应用枚举时间都变得更短。

2002 中的新增功能

FIPS 模式下的长度为 **4096** 位的密钥

适用于 Mac 的 Citrix Workspace 应用程序现在支持在美国联邦信息处理标准出版物 (FIPS 140) 加密模式下使用长度为 4096 位的 RSA 密钥。

性能改进

此版本解决了多个有助于改进整体性能和稳定性的问题。

2001 中的新增功能

应用程序保护

适用于 Mac 的 Citrix Workspace 应用程序现在支持应用程序保护。应用程序保护是一项附加功能，可在使用 Citrix Virtual Apps and Desktops 时提供增强的安全性。该功能限制了客户端受键盘记录和屏幕捕获恶意软件影响的能力。应用程序保护可防止泄露屏幕上显示的用户凭据和敏感信息等机密信息。该功能可防止用户和攻击者截取屏幕截图以及使用键盘记录器收集和利用敏感信息。有关 Citrix Virtual Apps and Desktops 上的应用程序保护配置的信息，请参阅应用程序保护。

已知问题或限制：

要使此功能正常运行，请在 VDA 上禁用客户端剪贴板重定向策略。

语言支持

适用于 Mac 的 Citrix Workspace 应用程序现在提供葡萄牙语（巴西）版本。

增强的第三方虚拟通道加载

适用于 Mac 的 Citrix Workspace 应用程序现在支持第三方虚拟通道的更高级加载。这通过以下方式增强了用户体验：

- 卸载并重新安装 Citrix Workspace 应用程序时，无需再次安装第三方虚拟通道（例如，RealTime Media Engine）。
- 具有标准帐户权限的用户也可以获得优化的 RealTime Optimization Pack 体验，即使其 RealTime Media Engine 是由管理员安装的亦如此。

1912 中的新增功能

带智能功能的 **Workspace**

本版本的适用于 Mac 的 Citrix Workspace 应用程序进行了优化，以在发布时利用即将推出的智能功能。有关详细信息，请参阅 Workspace 智能功能 - 微应用。

1910.2 中的新增功能

本版本解决了 Citrix Workspace 更新和 macOS Catalina 存在的问题。

- 使用适用于 Mac 的 Citrix Workspace 应用程序 1910 和 1910.1 的客户必须手动升级到适用于 Mac 的 Citrix Workspace 应用程序 1910.2，才能通过 Citrix Workspace 更新接收将来的更新。
- 使用适用于 Mac 的 Citrix Workspace 应用程序 1906 或更早版本的客户可以通过 Citrix Workspace 更新获取适用于 Mac 的 Citrix Workspace 应用程序 1910.2。

1910.1 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。

1910 中的新增功能

macOS Catalina 支持

macOS Catalina 支持适用于 Mac 的 Citrix Workspace 应用程序。

> 注意：
>
> 在 macOS Catalina 上首次打开适用于 Mac 的 Citrix Workspace 应用程序和 Citrix Viewer 时，操作系统将提示用户允许接收来自 Citrix Viewer 的通知。单击允许可接收与适用于 Mac 的 Citrix Workspace 应用程序有关的通知。

密码套件更新

为了增强安全性，以下密码套件已弃用：

- 前缀为 “TLS_RSA_*” 的密码套件
- 密码套件 RC4 和 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

适用于 Mac 的 Citrix Workspace 应用程序仅支持以下密码套件：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

对于 DTLS 1.0 用户，适用于 Mac 的 Citrix Workspace 应用程序 1910 仅支持以下密码套件：

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

如果要使用 DTLS 1.0，Citrix 建议您将 NetScaler 版本升级到 12.1 或更高版本。否则，将回退到基于 DDC 策略的 TLS。有关详细信息，请参阅知识中心文章 CTX250104。

Citrix Casting 更新

Citrix Casting 现在在用户关闭便携式计算机的电脑盖时自动断开连接。

1906 中的新增功能

Citrix Casting 更新

使用外围设备在 Citrix Ready Workspace Hub 上控制会话。您现在可以使用 Hub 和设备上的键盘和鼠标来管理会话。有关详细信息，请参阅Citrix Ready Workspace Hub。

语言支持

适用于 Mac 的 Citrix Workspace 应用程序现在提供荷兰语版本。

1903.1 中的新增功能

Citrix Casting 更新

Citrix Casting 已通过新增功能和增强功能进行了全面更新。有关 Citrix Casting 的详细信息，请参阅Citrix Casting。

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

Citrix Casting

Citrix Casting 用于将您的 Mac 投射到附近的 Citrix Ready Workspace Hub 设备。在本版本中，提供了用于将您的 Mac 屏幕镜像到连接 Workspace Hub 的显示器的支持。

有关 Citrix Casting 的详细信息，请参阅配置 Citrix Casting。

键盘布局同步

自本版本起，适用于 Mac 的 Citrix Workspace 应用程序在会话中提供从客户端到 Linux VDA 的动态键盘布局同步。这使您能够在客户端设备上在首选键盘布局之间切换，从而（例如）将键盘布局从英语切换到西班牙语时提供一致的用户体验。

有关配置键盘布局的详细信息，请参阅键盘布局。有关在 Linux VDA 上配置键盘布局同步的详细信息，请参阅动态键盘布局同步。

增强的客户端 **IME** 体验

自本版本起，适用于 Mac 的 Citrix Workspace 应用程序将在客户端 IME 输入和 Linux VDA 方面提供更加优异的用户体验。使用此功能时，您可以看到客户端 IME 输入方面的两个改进功能：

- 构件字符列表的候选窗口始终在插入点旁边显示，而非在以前的左下角位置显示。
- 标记 VDA 中显示的构件字符，以便您不会将其与既定字符相混淆。

此功能依赖于键盘布局同步功能。

有关配置此客户端 IME 增强功能的详细信息，请参阅增强的客户端 IME。有关在 Linux VDA 上配置客户端 IME 的详细信息，请参阅客户端 IME 用户界面同步。

选择性 **H264**

选择性 H264 允许屏幕的各个部分快速切换（例如播放视频时）以作为 H264 流接收。要启用“选择性 H264”，请将使用视频编解码器进行压缩策略设置为针对主动变化的区域。

1809 中的新增功能

macOS Mojave 支持

适用于 Mac 的 Citrix Workspace 应用程序完全支持 macOS Mojave，包括深色模式。

WebApp 支持

适用于 Mac 的 Citrix Workspace 应用程序适用的 Secure Browser 现在支持 Cookie 以及在使用 Citrix Gateway 时进行重定向。

1808 中的新增功能

64 位支持

适用于 Mac 的 Citrix Workspace 应用程序现在完全 64 位兼容。

> 注意：
>
> 升级到 Citrix Workspace 应用程序的用户将会因为位数不匹配而无法拥有优化的 Skype for Business (Lync) 体验。适用于 Mac 的 Citrix Workspace 应用程序是 64 位，而当前安装的 RTME 版本是 32 位。解决方法：考虑使用 RTME 技术预览版。
>
> 注意：

> 32 位自定义虚拟通道不再起作用，必须更新到 64 位。

联合身份验证

适用于 Mac 的 Citrix Workspace 应用程序现在支持通过 Azure Active Directory 进行联合身份验证。

显示或隐藏远程语言栏

自此版本起，您可以选择使用 GUI 在应用程序会话中显示或隐藏远程语言栏。语言栏显示会话中的首选输入语言。在早期版本中，只能使用 VDA 上的注册表项更改此设置。自适用于 Mac 的 Citrix Workspace 应用程序版本 1808 起，可以使用首选项对话框更改设置。默认情况下，语言栏在会话中显示。

有关详细信息，请参阅配置和知识中心文章 CTX231913。

> 注意：
>
> 此功能在 VDA 7.17 及更高版本上运行的会话中可用。

支持 **Citrix Analytics**

Citrix Workspace 应用程序已经过检测，可以安全地将日志传输到 Citrix Analytics。启用后，将在 Citrix Analytics 上分析和存储日志。有关 Citrix Analytics 的详细信息，请参阅 Citrix Analytics 文档。

已修复的问题

2107 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

2106 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

2104 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

2102 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

2101 中已修复的问题

- 使用 OWA（Outlook Web App）尝试打开 Microsoft Teams 会议可能会失败，并导致所有相关窗口意外退出。[CTXBR-1175]
- 开始视频通话时，Microsoft Teams 可能会变得无响应，显示 “`Citrix HDX not connected`” 错误。[RFMAC-6727]
- 在 macOS Big Sur (11.0.1) 上，尝试连接 USB 设备可能会失败，导致会话意外退出。[RFMAC-7079]
- 在已发布的桌面中，保存到本地 Mac 设备的文件可能会显示文件的创建日期为 1979 年 11 月 30 日，而不是当前日期。[CVADHELP-16309]
- 有时，已发布应用程序中的登录屏幕可能无法正常显示，从而导致窗口大小变小且背景颜色为红色。[CVADHELP-16027]
- 断开连接后再连接音频设备时，您这边的音频通话可能会断开连接。[RFMAC-7371]
- 即使启用了剪贴板限制策略，尝试从 Office 365 应用程序中复制文本也可能会成功。[CTXBR-1166]
- 由于 HDX RealTime Connector 引擎出现问题，尝试启动 Microsoft Teams 可能会失败，并显示以下错误消息。

  ```
  Sorry, we couldn't connect you
  ```

  [CVADHELP-16432]

2012 中已修复的问题

- 使用适用于 Mac 的 Citrix Workspace 应用程序 2008 或更高版本时，尝试启动已发布的应用程序的多个实例可能会失败。[CVADHELP-16019]
- 使用 USB 扩展坞时，尝试启动通用 USB 重定向可能会失败。[RFMAC-6687]
- 尝试在已发布的桌面中使用 Ctrl+O 打开窗口可能会导致出现两个打开的窗口。[CVADHELP-15747]
- 在 macOS Big Sur Beta 上使用适用于 Mac 的 Citrix Workspace 应用程序时，音频通话可能会断开连接。断开音频设备连接并在音频通话过程中连接不同的音频设备时会出现此问题。[RFMAC-6112]
- 打开和关闭 Microsoft Teams 中的相机时，HDX RealTime Connector 引擎可能会意外退出。[RFMAC-6293]
- 尝试从适用于 Mac 的 Workspace 应用程序中启动 Citrix Files 可能会因单点登录问题而失败。[RFMAC-4477]

2010 中已修复的问题

- 尝试启动已发布的桌面或应用程序可能会失败，并显示错误消息。如果您的计算机名称包含特殊字符，则会出现此问题。[CVADHELP-15492]
- 尝试登录已发布的应用程序和桌面会话可能会失败。使用鼠标单击确定以登录时会出现此问题。[CVADHELP-15300]

2009 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

2008 中已修复的问题

如果在 VDA 上添加 EULA，尝试启动已发布的桌面可能会导致出现灰屏或黑屏。[CVADHELP-14986]

2007 中已修复的问题

- 用户在 Citrix Gateway 上启用了 Enlightened Data Transport (EDT) 时，客户端音频设置中的问题可能会导致适用于 Mac 的 Citrix Workspace 应用程序意外退出。[CVADHELP-14686]
- 在启用了使用视频编解码器进行压缩策略的 VDA 上使用 Intel SDK 时，尝试启动已发布的桌面可能会导致绿屏。[CVADHELP-13647]
- 尝试获取 WMI (Windows Management Instrumentation) 延迟数据在适用于 Mac 的 Citrix Workspace 应用程序版本 2002 和 2005 中可能会失败。[RFMAC-4325]

2006 中已修复的问题

- 尝试登录到适用于 Mac 的 Citrix Workspace 应用程序可能会失败，显示不相关的 UI。解决方法是，单击菜单中的刷新应用程序以加载应用商店。[RFMAC-4063]

2005 中已修复的问题

- 尝试使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败，并显示以下错误消息：“无法检测指定的帐户。” [CVADHELP-14155]
- 有时，Microsoft Outlook 的已发布实例的模式窗口处于焦点中时，主窗口可能会变成黑色。[CVADHELP-14169]

2002 中已修复的问题

- 尝试在 macOS Catalina (10.15.2) 上的 Citrix Workspace 应用程序中使用 PIV 智能卡启动会话可能会失败，并显示以下错误消息：“一个或多个根证书无效”。[RFMAC-3365]
- 尝试键入语言设置为中文或日文的已发布应用程序（例如记事本等）可能会失败。[RFMAC-3556]

2001 中已修复的问题

- 尝试在 MacBook 上启用 16 bpp 最大颜色深度策略的情况下启动已发布的桌面可能会显示灰色屏幕，并且变得无响应。[CVADHELP-13605]

- 尝试将在 DingTalk 应用程序中截取的屏幕截图粘贴到 Microsoft 画图和 Microsoft Word 的已发布实例中可能会失败，分别显示空白屏幕或错误消息。[CVADHELP-13938]

1912 中已修复的问题

- 使用适用于 Mac 的 Citrix Workspace 应用程序版本 1812 或 1901 时，尝试在屏幕上移动已发布的应用程序的响应速度很慢。[RFMAC-2300]
- 尝试使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败。[RFMAC-2788]
- 使用适用于 Mac 的 Citrix Workspace 应用程序版本 1909 时，打开使用非英语名称的.ICA 文件可能会导致 Citrix Viewer 意外退出。[RFMAC-2986]
- 升级适用于 Mac 的 Citrix Workspace 应用程序后，尝试启动已发布的 Microsoft Outlook 和 PowerShell 应用程序无响应或响应速度缓慢。[LD1192]
- 在屏幕上移动已发布的应用程序时，其窗口不更新或者更新速度较慢。[LD1485]

1910.2 中已修复的问题

此版本还解决了几个有助于提高整体性能和稳定性的问题。

1910.1 中已修复的问题

- 使用 MacBook Pro 2018 及更高版本和 FaceTime 时，用户可能会在视频预览的底部看到一个绿条。[RFMAC-2317]
- 通过 Citrix Gateway 启动使用智能卡的会话可能会失败，并显示错误消息 “远程 SSL 对等机发送了握手失败警报”。[RFMAC-2727]
- 启用了 SAML 身份验证时，身份验证屏幕可能会速度缓慢或无响应。解决方法为，重新启动设备。[RFMAC-3047]
- 启动已订阅的应用程序后拒绝自动化权限可能会导致适用于 Mac 的 Citrix Workspace 应用程序无响应。[RFMAC-3048]

1910 中已修复的问题

- 将适用于 Mac 的 Citrix Workspace 应用程序的文本复制到其他应用程序可能会显示不正确的字符。[RFMAC-2581]
- 登录适用于 Mac 的 Citrix Workspace 应用程序所需的时间可能比预期时间更长。[RFMAC-2608]
- 使用代理进行连接可能会导致代理意外退出。[RFMAC-2612]
- 使用多个显示器时，无缝应用程序中的鼠标移动可能不同步。[RFMAC-2623]
- 重新登录适用于 Mac 的 Citrix Workspace 应用程序可能会导致应用程序意外退出。[RFMAC-2679]
- 使用 Command-Tab 热键切换选项卡时，虚拟桌面将变得无响应。[RFMAC-2691]
- 启用了增强的安全性时，启动 ShareFile 应用程序将失败。[RFMAC-2724]
- Citrix Viewer 可能会占用过多 CPU。[RFMAC-2777]

1906 中已修复的问题

- 智能卡会话可能会随机断开连接。[RFMAC-1816，RFMAC-2313]
- 断开连接的会话可能会导致适用于 Mac 的 Citrix Workspace 应用程序变得无响应。[RFMAC-2137]
- Web 视图窗口显示在所有应用程序上。[RFMAC-2146]
- 将 MacBook 唤醒后，适用于 Mac 的 Citrix Workspace 应用程序将重复提示进行身份验证。[RFMAC-2161]
- 登录时，可能会出现错误，指出找不到服务器。[RFMAC-2192]
- 在未配置单点登录的情况下启动 WebApp 可能会导致出现 401 错误，而非提示输入凭据。[RFMAC-2194]
- 移动到辅助显示器时，无缝应用程序窗口可能会消失。[RFMAC-2314]
- 有时会显示“无法加载页面”错误页面。[RFMAC-2322]
- 使用已发布的 Microsoft Outlook 应用程序时，用户可能无法选择菜单。[RFMAC-2335]
- 使用 Web 窗体可能会显示身份验证错误。[RFMAC-2349]
- 尝试通过 Citrix Gateway 进行连接时，如果虚拟服务器配置为使用已签名的中间证书，适用于 Mac 的 Citrix Workspace 应用程序将意外退出，并出现 SSL 61 错误。[RFMAC-2393]
- 某些 Web 站点的凭据可能会清除，不允许用户登录。[RFMAC-2394]
- 启动 Outlook Web 应用程序将显示一个空白页。[RFMAC-2395]
- 最小化和最大化无缝应用程序时，应用程序可能无法正确重绘。[RFMAC-2411]
- 作为已发布的应用程序启动时，用户可能无法将文件上载到 Jira。[RFMAC-2467]

1903.1 中已修复的问题

- 启动桌面会话时，适用于 Mac 的 Citrix Workspace 应用程序可能会意外退出。
- 某些自定义应用程序可能无法启动。[RFMAC-2081]
- 移动记事本应用程序时，当两个或更多应用程序处于活动状态时，该应用程序可能会移动到后台。[RFMAC-2107]
- 尝试编辑 Citrix Workspace 应用商店时，将改为显示 Citrix Files UI。[RFMAC-2111]
- 当您在启动某个无缝应用程序之后、该无缝应用程序准备就绪之前单击停靠图标时，会话将不再无缝。[RFMAC-2139]
- 将 MacBook 从睡眠状态唤醒后，Citrix Workspace 将反复要求进行身份验证。[RFMAC-2161]
- 重新连接到无缝 VDA 会话后，会话中的图形可能会失真。[RFMAC-2176]
- 使用本地键盘布局和日语键盘时，删除键入的未提交的字符可能无法正常工作。[RFMAC-2287]

1901 中已修复的问题

- 升级适用于 Mac 的 Citrix Workspace 应用程序后，应用程序可能不会启动。[RFMAC-2003]
- USB 音频重定向可能无法正常工作。[RFMAC-2043]
- 在无缝版本的 Microsoft Outlook 中，您无法选择下拉菜单。[RFMAC-2079]
- 使用无缝应用程序时，会话可能会变得无响应。[RFMAC-2083]
- 在最小化或最大化跨多个显示器的窗口时，会话可能变得无响应。[RFMAC-2103]

1812 中已修复的问题

- 检查 Microsoft Office 应用程序中的某个工具提示后，显示该工具提示的黑色区域将保留。[RFMAC-1793]
- 使用 Retina 显示屏时，会话可能呈模糊显示。[RFMAC-1944]
- 在三个显示器上运行的某个会话中对触摸板使用三个手指轻扫手势可能不起作用。[RFMAC-1968]
- 在后台运行时，Citrix Viewer 可能会使用 App Nap。[RFMAC-1979]
- 网络连接中断后，登录页面可能会在重新连接到网络后需要比平时更长的时间才会重新出现。[RFMAC-2001]
- 按 Delete 可能会删除多个字符。[RFMAC-2011]
- 播放 YouTube 视频超过 3 分钟后，启用了 EDT 的 VDA 可能变得无响应。[RFMAC-2017]
- 如果 Citrix Receiver Launcher 在 Google Chrome 中注册，升级到 Citrix Workspace 应用程序将不允许会话从 Chrome 启动。[RFMAC-2020]
- “使用视频编解码器进行压缩”策略可能无法正常工作。[RFMAC-2021]

1809 中已修复的问题

- 重新连接的会话可能无法保持连接。[RFMAC-1823]

1808 中已修复的问题

- 在双 GPU Mac 中，客户端在依赖电池电源时可能使用离散 GPU，而不是能效更高的集成 GPU。[RFMAC-1439]
- 客户端安装了 JamF 时可能无法正确升级。[RFMAC-1523]
- 尝试使用 USB 设备进行通用 USB 重定向时，这些设备可能不显示在会话中。[RFMAC-1592]
- 检查客户端更新可能会失败并出现“检查更新时出现问题”错误。[RFMAC-1589]
- 打开了多个已发布的应用程序窗口时，激活某个已发布的应用程序窗口可能会导致另一个已发布的应用程序窗口进入前台。[RFMAC-1696]

已知问题

2107 中的已知问题

当您在服务器控制台中更改身份验证域并使用您的凭据登录时，将显示以下错误消息：

“无法连接到服务器”

单击“确定”后，您可以访问应用商店。[RFMAC-9494]

2106 中的已知问题

共享屏幕时，会出现一个黑色窗口。[HDX-30083]

2104 中的已知问题

在此版本中没有发现新问题。

2102 中的已知问题

在此版本中没有发现新问题。

2101 中的已知问题

- 尝试从适用于 Mac 的 Workspace 应用程序中访问网络共享下的文件可能会失败，即使已启用该选项亦如此。[RFMAC-7272]
- 在 macOS Big Sur 上，尝试在适用于 Mac 的 Citrix Workspace 应用程序上启动 Web SAML 单点登录应用程序可能会失败，并显示以下错误消息。

  ```
  Page could not load. Please try again later or contact your administrator
   for assistance. Incident ID:-202
  ```

  [RFMAC-7282]

2012 中的已知问题

- 开始视频通话时，Microsoft Teams 可能会变得无响应，显示 “`Citrix HDX not connected`” 错误。解决方法为，重新启动 Microsoft Teams 或 VDA。[RFMAC-6727]
- macOS Big Sur (11.0.1) 不支持 Microsoft Skype for Business 上的视频通话。
- 在 macOS Big Sur (11.0.1) 上，尝试连接 USB 设备可能会失败，导致会话意外退出。解决方法为，重新连接 USB 设备。[RFMAC-7079]

2010 中的已知问题

- 在 Skype for Business 中，传入的视频在 macOS Big Sur (11.0.1) 上不可见。
- 使用适用于 Mac 的 Citrix Workspace 应用程序 2008 或更高版本时，尝试启动已发布的应用程序的多个实例可能会失败。[CVADHELP-16019]
- 使用 USB 扩展坞时，尝试启动通用 USB 重定向可能会失败。[RFMAC-6687]
- 使用 MacBook Pro 2018 及更高版本和 FaceTime 时，用户可能会在视频预览的底部看到一个绿色、黑色或失真的矩形条。[RFMAC-2829]

2009 中的已知问题

macOS Big Sur Beta

- 在云部署中，已发布的桌面启动时背景颜色可能会不匹配。在某些 macOS Big Sur Beta 版本中会间歇性出现此问题。[RFMAC-6343]
- 打开 **CitrixWorkspaceApp.dmg** 文件时，适用于 Mac 的 Citrix Workspace 应用程序的安装程序图标可能会丢失。在某些 macOS Big Sur Beta 版本中会间歇性出现此问题。[RFMAC-6378]

Microsoft Teams 优化（预览版）

- 在适用于 Mac 的 Citrix Workspace 应用程序上的 Microsoft Teams 中使用屏幕共享时，只有第三方应用程序（例如 Microsoft PowerPoint）才能共享。但是，完全支持传入屏幕共享。[RFMAC-3403]
- 打开和关闭 Microsoft Teams 中的相机时，HDX RealTime Connector 引擎可能会意外退出。[RFMAC-6293]
- 在 Microsoft Teams 中优化的视频通话中切换相机设备时，HDX RealTime Connector 引擎可能会意外退出。[RFMAC-6157]
- 在 Microsoft Teams 中切换网络时，音频和视频通话可能会断开连接。[RFMAC-6292]
- 在 macOS Big Sur Beta 上使用适用于 Mac 的 Citrix Workspace 应用程序时，音频通话可能会断开连接。断开音频设备连接并在音频通话过程中连接不同的音频设备时会出现此问题。[RFMAC-6112]

2008 中的已知问题

在此版本中没有发现新问题。

2007 中的已知问题

在此版本中没有发现新问题。

2006 中的已知问题

在此版本中没有发现新问题。

2005 中的已知问题

- 尝试登录到适用于 Mac 的 Citrix Workspace 应用程序可能会失败，显示不相关的 UI。解决方法是，单击菜单中的刷新应用程序以加载应用商店。[RFMAC-4063]

2002 中的已知问题

- 适用于 Mac 的 Citrix Workspace 应用程序仅支持已发布的 32 位应用程序的网络摄像头重定向。因此，不支持已发布的 64 位 Microsoft Teams 应用程序的网络摄像头重定向。[RFMAC-2199]
- 适用于 Mac 的 Citrix Workspace 应用程序不支持高 DPI (Retina) 显示。因此，这些设备上的文本可能会显得模糊不清。[RFMAC-650]
- 尝试使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败，并显示以下错误消息：“无法检测指定的帐户。” [CVADHELP-14155]

2001 中的已知问题

- 尝试使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败，并显示以下错误消息：“无法检测指定的帐户。” [CVADHELP-12609]
- 尝试在 macOS Catalina (10.15.2) 上的 Citrix Workspace 应用程序中使用 PIV 智能卡启动会话可能会失败，并显示以下错误消息：“一个或多个根证书无效”。[RFMAC-3365]

1912 中的已知问题

在此版本中没有发现新问题。

1910.2 中的已知问题

- 使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败。[RFMAC-2788]

1910.1 中的已知问题

- 使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败。[RFMAC-2788]

1910 中的已知问题

- 使用 MacBook Pro 2018 及更高版本和 FaceTime 时，用户可能会在视频预览的底部看到一个绿条。[RFMAC-2317]
- 通过 Citrix Gateway 启动使用智能卡的会话可能会失败，并显示错误消息 “远程 SSL 对等机发送了握手失败警报”。[RFMAC-2727]
- 使用 PIV 智能卡在 macOS Catalina 上登录 Citrix Workspace 应用程序可能会失败。[RFMAC-2788]
- 启用了 SAML 身份验证时，身份验证屏幕可能会速度缓慢或无响应。解决方法为，重新启动设备。[RFMAC-3047]
- 启动已订阅的应用程序后拒绝自动化权限可能会导致适用于 Mac 的 Citrix Workspace 应用程序无响应。解决方法为，转到系统首选项 **>** 安全与隐私 **>** 隐私 **>** 自动化，并允许 Citrix Viewer.app、Citrix Workspace.app 和所有已订阅的应用程序的权限。[RFMAC-3048]

1906 中的已知问题

- 使用 MacBook Pro 2018 及更高版本和 FaceTime 时，用户可能会在视频预览的底部看到一个绿条。[RFMAC-2317]

1903.1 中的已知问题

- 智能卡会话可能会随机断开连接。[RFMAC-1816]
- 登录时，可能会出现错误，指出找不到服务器。[RFMAC-2192]

- 使用 MacBook Pro 2018 及更高版本和 FaceTime 时，用户可能会在视频预览的底部看到一个绿条。[RFMAC-2317]

1901 中的已知的问题

- 智能卡会话可能会随机断开连接。[RFMAC-1816]

1812 中的已知问题

- 智能卡会话可能会随机断开连接。[RFMAC-1816]
- USB 音频重定向可能无法正常工作。[RFMAC-2043]

1809 中的已知问题

- 使用 Safari 版本 12 时，可能无法启动应用程序和桌面会话。解决方法：请参阅知识中心文章 CTX238286。采用该解决方法后，每次启动会话时，Safari 都要求用户必须允许。

1808 中的已知问题

- 如果在使用 Secure SaaS 时应用程序出错，浏览器中显示的错误未本地化。[RFMAC-1836]

第三方声明

Citrix Workspace 应用程序可能包含根据以下文档中定义的条款进行许可的第三方软件：

适用于 Mac 的 Citrix Workspace 应用程序第三方声明

系统要求和兼容性

June 10, 2021

支持的操作系统

适用于 Mac 的 Citrix Workspace 应用程序支持以下操作系统：

- macOS Big Sur 11（包括次要版本和修补程序版本）
- macOS Catalina (10.15)

兼容的 **Citrix** 产品

适用于 Mac 的 Citrix Workspace 应用程序与以下 Citrix 产品的所有当前支持的版本兼容。要获取有关 Citrix 产品生命周期的信息，以及了解何时 Citrix 会停止支持特定的产品版本，请参阅 Citrix 产品生命周期表。

兼容的浏览器

适用于 Mac 的 Citrix Workspace 应用程序与以下浏览器兼容：

- Safari 7.0 及更高版本
- Mozilla Firefox 22.x 及更高版本
- Google Chrome 28.x 及更高版本

硬件要求

- 257.7 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

软件要求

- 部署适用于 Mac 的 Citrix Workspace 应用程序：
  - 适用于 Web 的 Citrix Workspace 2.1、2.5 和 2.6
- StoreFront：
  StoreFront 2.x 或更高版本，用于从适用于 Mac 的 Citrix Workspace 应用程序或 Web 浏览器本机访问应用程序。

连接、证书和身份验证

连接

适用于 Mac 的 Citrix Workspace 应用程序支持与 Citrix Virtual Apps and Desktops 建立以下连接：

- HTTP
- HTTPS
- ICA-over-TLS

适用于 Mac 的 Citrix Workspace 应用程序支持以下配置：

对于 LAN 连接	对于安全的远程连接或本地连接
使用 StoreFront Services 或 Citrix Receiver for Web 站点的 StoreFront；	Citrix Gateway 10.5–12.0，包括 VPX；Enterprise Edition 9.x-10.x，包括 VPX；VPX

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。然后，您可以使用适用于 Mac 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。当用户选择忽略该警告而继续进行操作时，系统将显示应用程序列表。但是，应用程序无法启动。

在适用于 **Mac** 的 **Citrix Workspace** 应用程序设备上导入根证书

可以获取证书颁发者的根证书，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。适用于 Mac 的 Citrix Workspace 应用程序支持通配符证书。

中间证书与 **Citrix Gateway**

如果您的证书链中包含中间证书，必须将该中间证书映射到 Citrix Gateway 服务器证书。有关此任务的信息，请参阅 Citrix Gateway 文档。有关在 Citrix 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 如何在 Citrix Gateway 上安装中间证书并将其与主 CA 链接。

联合服务器证书验证策略

适用于 Mac 的 Citrix Workspace 应用程序引入了更加严格的服务器证书验证策略。

> 重要
>
> 安装此版本的适用于 Mac 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 Mac 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 Mac 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 Mac 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 Mac 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 Mac 的 Citrix Workspace 应用程序将检查所有这些证书是否都有效。适用于 Mac 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 Mac 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 Mac 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必须使用的根证书。另请注意，根证书最终会过期，所有证书也是如此。
>
> 注意
>
> 某些服务器和网关从不发送根证书，即使已配置也是如此。更加严格的验证因而不可行。

现在假定为网关配置了以下有效的证书。通常推荐使用此配置（忽略根证书）：

- “示例服务器证书”
- “示例中间证书”

之后，适用于 Mac 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。此配置提供适用于 Mac 的 Citrix Workspace 应用程序所需的中间证书，但是还允许适用于 Mac 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 Mac 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。这适用于存在多个根证书的情况。较早的根证书仍与更高版本的根证书同时使用。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，因为网关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 Mac 的 Citrix Workspace 应用程序找不到所有中间证书，连接将失败。

身份验证

对于与 StoreFront 的连接，适用于 Mac 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 *

	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）
域直通					
安全令牌				是 *	是 *
双重（域 + 安全令牌）				是 *	是 *
SMS				是 *	是 *
智能卡	是	是		是 *	是
用户证书				是	是（Citrix Gateway 插件）

* 仅适用于包含 Citrix Gateway 的部署，而无论设备上是否已安装关联的插件。

安装、卸载和升级

April 12, 2021

适用于 Mac 的 Citrix Workspace 应用程序包含一个单独的安装包，支持通过 Citrix Gateway 和 Secure Web Gateway 进行远程访问。

可以通过以下任一方式安装适用于 Mac 的 Citrix Workspace 应用程序：

- 从 Citrix Web 站点
- 自动从适用于 Web 的 Workspace
- 使用电子软件分发 (Electronic Software Distribution, ESD) 工具安装。

手动安装

由用户从 **Citrix.com** 安装

作为首次使用的用户，您可以从 Citrix.com 或您自己的下载站点下载适用于 Mac 的 Citrix Workspace 应用程序。然后，您可以通过输入电子邮件地址而非服务器 URL 设置一个帐户。适用于 Mac 的 Citrix Workspace 应用程序将确定与电子邮件地址关联的 Citrix Gateway 或 StoreFront 服务器。然后，系统会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适用于 Mac 的 Citrix Workspace 应用程序的用户。

如果您已从 Citrix.com 以外的位置（例如 Citrix Receiver for Web 站点）下载，则不会对首次使用的用户执行基于电子邮件的帐户发现。

如果您的站点需要配置适用于 Mac 的 Citrix Workspace 应用程序，请使用备用部署方法。

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

首次使用适用于 Mac 的 Citrix Workspace 应用程序的用户必须输入服务器 URL 来设置帐户。

从 **Citrix** 下载页面

可以从网络共享安装适用于 Mac 的 Citrix Workspace 应用程序，也可以直接安装在用户设备上。可以通过从 Citrix Web 站点 (下载) 下载文件来执行此操作。

安装适用于 Mac 的 Citrix Workspace 应用程序：

1. 从 Citrix Web 站点下载要安装的适用于 Mac 的 Citrix Workspace 应用程序版本的.dmg 文件，并将其打开。
2. 在 “Introduction”（简介）页面上，单击 **Continue**（继续）。
3. 在 **License**（许可证）页面上，单击 **Continue**（继续）。
4. 单击同意接受许可协议的条款。
5. 在 **Installation Type**（安装类型）页面上，单击安装。
6. 在添加帐户页面上，选择添加帐户，然后单击继续。
7. 在本地设备上输入管理员的用户名和密码。

卸载

可以通过打开.dmg 文件手动卸载适用于 Mac 的 Citrix Workspace 应用程序。选择卸载 **Citrix Workspace** 应用程序并按照屏幕上的说明进行操作。.dmg 文件是首次安装适用于 Mac 的 Citrix Workspace 应用程序时从 Citrix 下载的文件。如果该文件不再位于您的计算机上，请从 Citrix 下载 下载该文件以卸载应用程序。

升级

当有更新对现有版本可用或升级到较新版本时，适用于 Mac 的 Citrix Workspace 应用程序将向您发送通知。或者，您也可以右键单击 Citrix Workspace 应用程序图标，然后单击检查更新以了解是否有更新或升级可用。

可以从适用于 Mac 的 Citrix Workspace 应用程序的任意早期版本升级适用于 Mac 的 Citrix Workspace 应用程序。

执行升级到适用于 Mac 的 Citrix Workspace 应用程序的较新版本时，会自动卸载以前的版本。您不需要重新启动计算机。

配置

July 7, 2021

在安装适用于 Mac 的 Citrix Workspace 应用程序软件后，用户可按照以下配置步骤来访问其托管应用程序和桌面。

用户可以从 Internet 或远程位置进行连接。对于这些用户，请通过 Citrix Gateway 配置身份验证。

管理员任务和注意事项

本文讨论了与适用于 Mac 的 Citrix Workspace 应用程序的管理员相关的任务和注意事项。

> 重要：
>
> 如果您运行的是 macOS 10.15，请在升级到适用于 Mac 的 Citrix Workspace 应用程序版本 2106 之前，确保您的系统符合 Apple 的 macOS 10.15 中的可信证书应满足的要求。

功能标志管理

如果生产环境中的 Citrix Workspace 应用程序出现问题，我们可以在 Citrix Workspace 应用程序中动态禁用受影响的功能，即使该功能已发布亦如此。为此，我们将使用功能标志以及名为 LaunchDarkly 的第三方服务。不需要做任何配置即可启用传输到 LaunchDarkly 的流量，但当您配置了阻止出站流量的防火墙或代理时除外。在这种情况下，您根据策略要求通过特定 URL 或 IP 地址启用传输到 LaunchDarkly 的流量。

可以通过以下方式启用传输到 LaunchDarkly 的流量和通信：

启用传输到以下 **URL** 的流量

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `Firehose.launchdarkly.com`
- `mobile.launchdarkly.com`

在允许列表中列出 **IP** 地址

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

LaunchDarkly 系统要求

如果您在 Citrix ADC 上将以下服务的拆分通道设置为关，请确保应用程序能够与以下服务通信：

- LaunchDarkly 服务。
- APNs 侦听器服务

Content Collaboration Service 集成

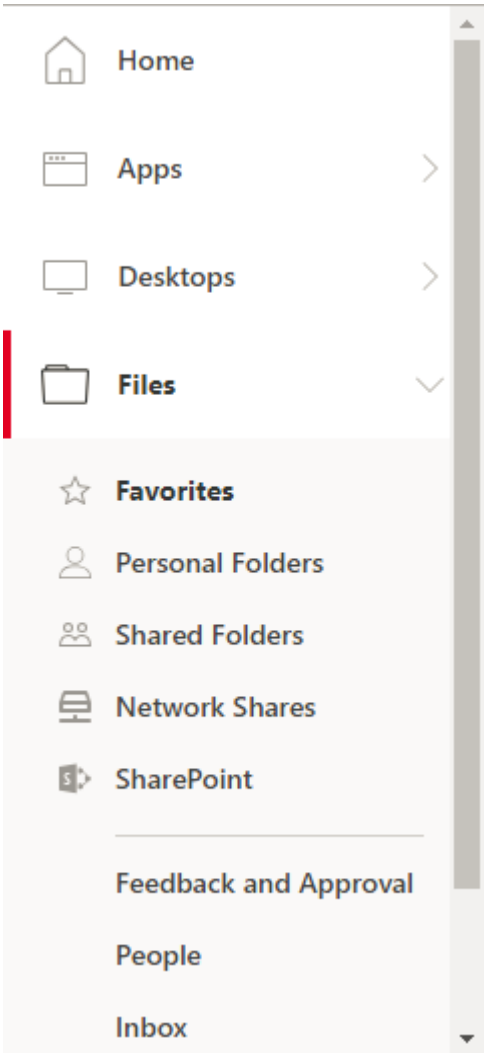
您可以利用 Citrix Content Collaboration 轻松、安全地交换文档、通过电子邮件发送大型文档、安全地处理向第三方的文档传输以及访问协作空间。

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。这是在操作系统中设置的一个安全选项导致的。

下图显示了新 Citrix Workspace 应用程序的文件选项卡的示例内容：



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。

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 设备和其他设备，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。

USB 重定向适用于以下操作系统：

- Windows
- Linux
- Mac

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。更多信息将在本部分后面的部分中提供。

> 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，适用于 Mac 的 Citrix Workspace 应用程序将以处理鼠标的相同方式来处理 SMART 板。

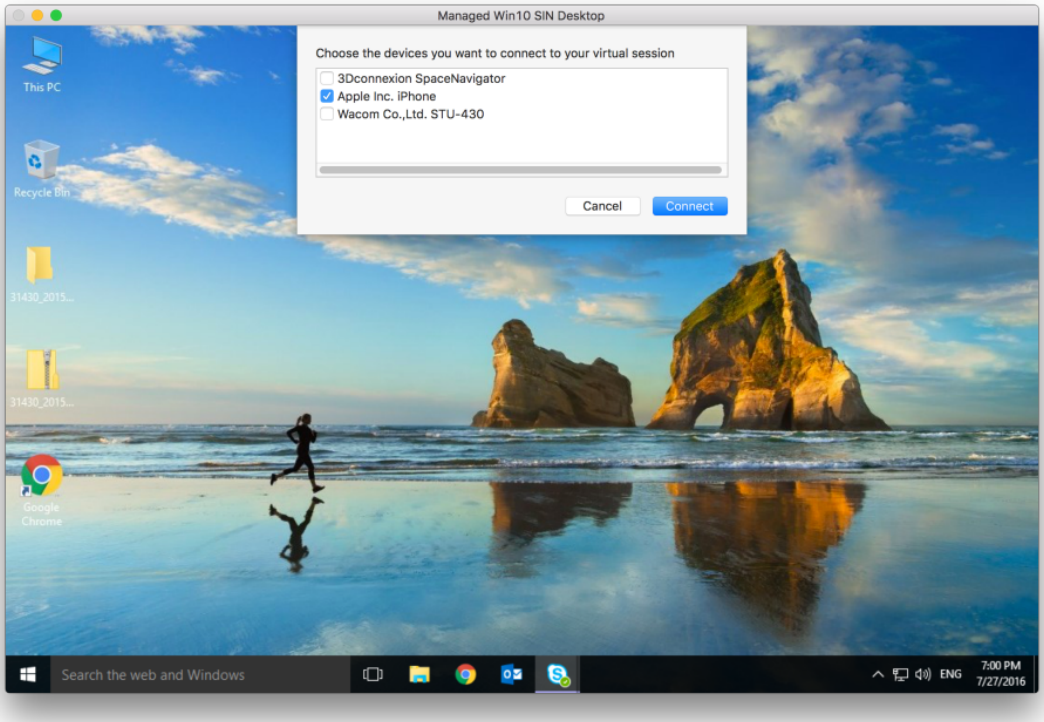
该产品支持优化的虚拟通道，配备 USB 3.0 设备和 USB 3.0 端口。例如，CDM 虚拟通道用于查看相机中的文件或向耳机提供音频。此产品还支持连接到 USB 2.0 端口的 USB 3.0 设备的通用 USB 重定向。

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。如果出现此问题，请使用通用 USB 虚拟通道。

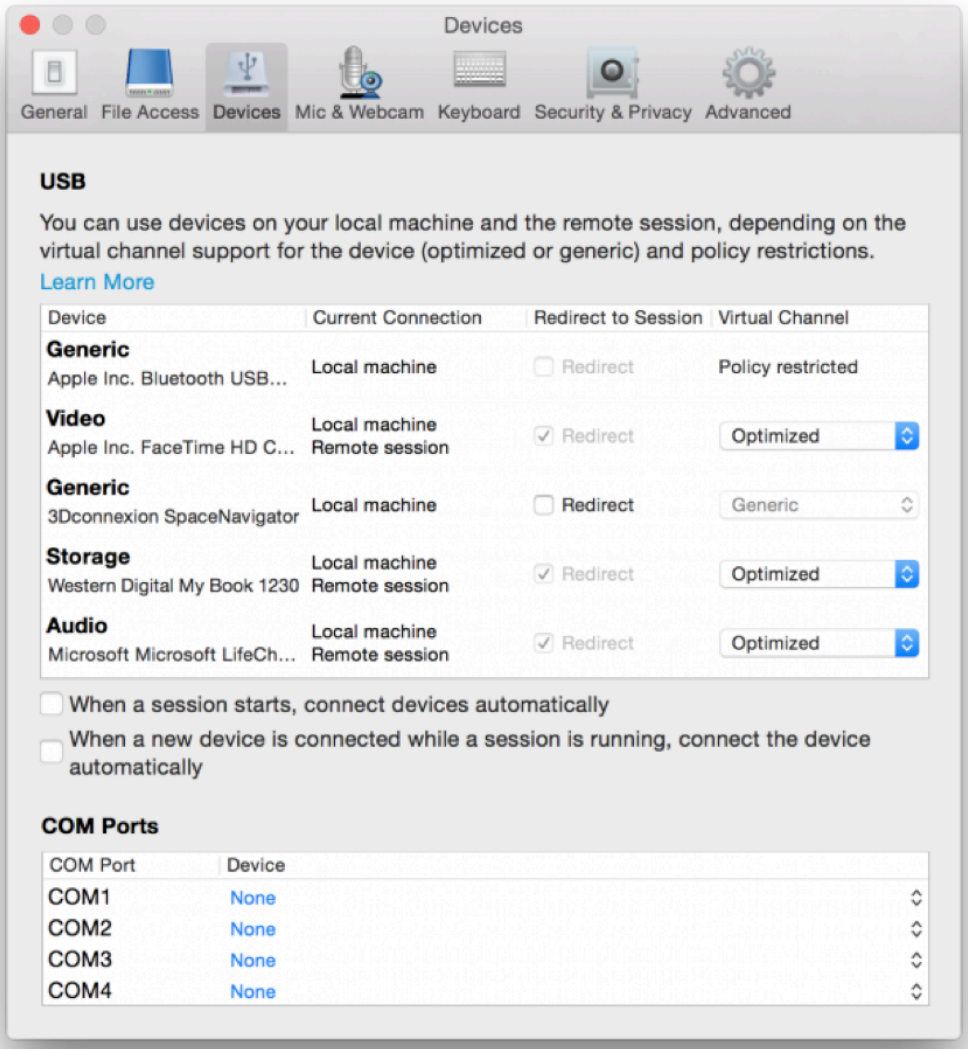
默认情况下不会重定向某些设备，这些设备只能用于本地会话。例如，不应对直接通过内部 USB 连接的 NIC 进行重定向。

要使用 USB 重定向，请执行以下操作：

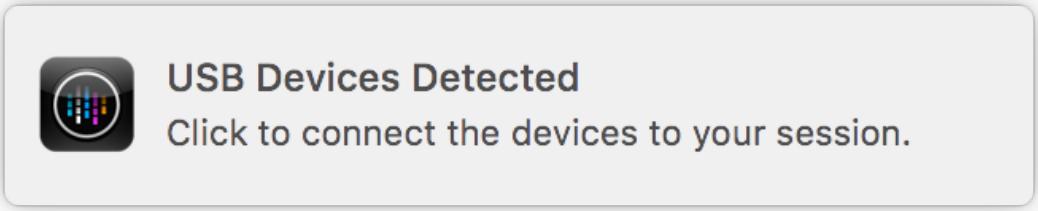
1. 将 USB 设备连接到安装了适用于 Mac 的 Citrix Workspace 应用程序的设备。
2. 系统将提示您选择本地系统中可用的 USB 设备。



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中，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（“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。使用适用于 Mac 的 Citrix Workspace 应用程序时，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 设备不能正确重定向，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。

Enlightened Data Transport (EDT)

默认情况下，EDT 在适用于 Mac 的 Citrix Workspace 应用程序中处于启用状态。

适用于 Mac 的 Citrix Workspace 应用程序读取在 default.ica 文件中设置的 **EDT** 设置并相应地应用。

要禁用 EDT，请在终端运行以下命令：

```
defaults write com.citrix.receiver.nomas HDXOverUDPAllowed -bool NO
```

支持的 **USB** 设备

随着 Apple 宣布弃用内核扩展 (KEXT)，适用于 Mac 的 Citrix Workspace 应用程序迁移到 Apple 提供的新用户模式 USB 框架 `IOUSBHost`。本文列出了受支持的 USB 设备。

使用 **USB** 重定向的 **USB** 设备

以下 USB 设备可以与 USB 重定向无缝协作：

- 3D Connexion SpaceMouse
- 大容量存储设备
- Kingson Data Traveller USB 闪存驱动器
- Seagate 外部 HDD
- Kingston/Transcend 闪存驱动器 32 GB/64 GB
- NIST PIV 智能卡/阅读器
- YubiKeys

USB 重定向失败的 **USB** 设备

以下设备不适用于 USB 重定向：

- Transend SSD 外部硬盘

未验证的 **USB** 设备

很多设备未经 Citrix 验证是否能够成功将 USB 重定向与适用于 Mac 的 Citrix Workspace 应用程序结合使用。其中一些设备如下：

- 其他硬盘
- 键盘上的特殊键和使用自定义 HID 协议的耳机

支持大容量存储设备

我们已经看到，并非所有类型的大容量存储设备都可以成功重定向。对于无法重定向的设备，有一个名为客户端驱动器映射的优化虚拟通道。使用客户端驱动器映射时，可以通过 Delivery Controller 上的策略完全控制对大容量存储设备的访问。

支持常时等量设备

适用于 Mac 的 Citrix Workspace 应用程序中的通用 USB 重定向尚不支持常时等量级 USB 设备。USB 规范中的常时等量数据传输模式表示以恒定速率传输带时间戳的数据的设备。例如：网络摄像机、USB 耳机等。

对复合设备的支持

USB 复合设备是可以执行多项功能的一个小工具。例如：多功能打印机、iPhone 等。目前，适用于 Mac 的 Citrix Workspace 应用程序不支持将复合设备重定向到 Citrix Virtual Apps and Desktops 会话。

不受支持的 **USB** 设备的替代方案

存在优化的虚拟通道，可以用来处理通用 USB 重定向不支持的设备。与通用 USB 重定向相比，这些虚拟通道针对速度进行了优化。下面是一些示例：

- 网络摄像机重定向：针对原始网络摄像机流量进行了优化。请注意，Microsoft Teams Optimization Pack 有自己的网络摄像机重定向方法。因此，它不属于网络摄像机重定向虚拟通道的范围。
- 音频重定向：已优化以传输音频流。
- 客户端驱动器映射：针对将大容量存储设备重定向到 Citrix Virtual Apps and Desktops 会话进行了优化。例如：闪存驱动器、硬盘、DVD ROM/RW 等

会话可靠性和客户端自动重新连接

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。

> 重要
>
> - 适用于 Mac 的 Citrix Workspace 应用程序用户无法覆盖服务器设置。
> - 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。

结合使用会话可靠性与传输层安全性 (TLS)。

> 注意
>
> TLS 仅对用户设备和 Citrix 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）。尽管您可以延长会话可靠性保持会话处于打开状态的时间，但是此功能为用户提供了方便。因此，它不会提示用户重新进行身份验证。

> 提示
>
> 如果延长会话保持打开状态的时间长度，用户可能会因感到不耐烦而离开用户设备。这可能使未经授权的用户能够访问该会话。

传入会话可靠性连接使用端口 2598，除非您更改在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。

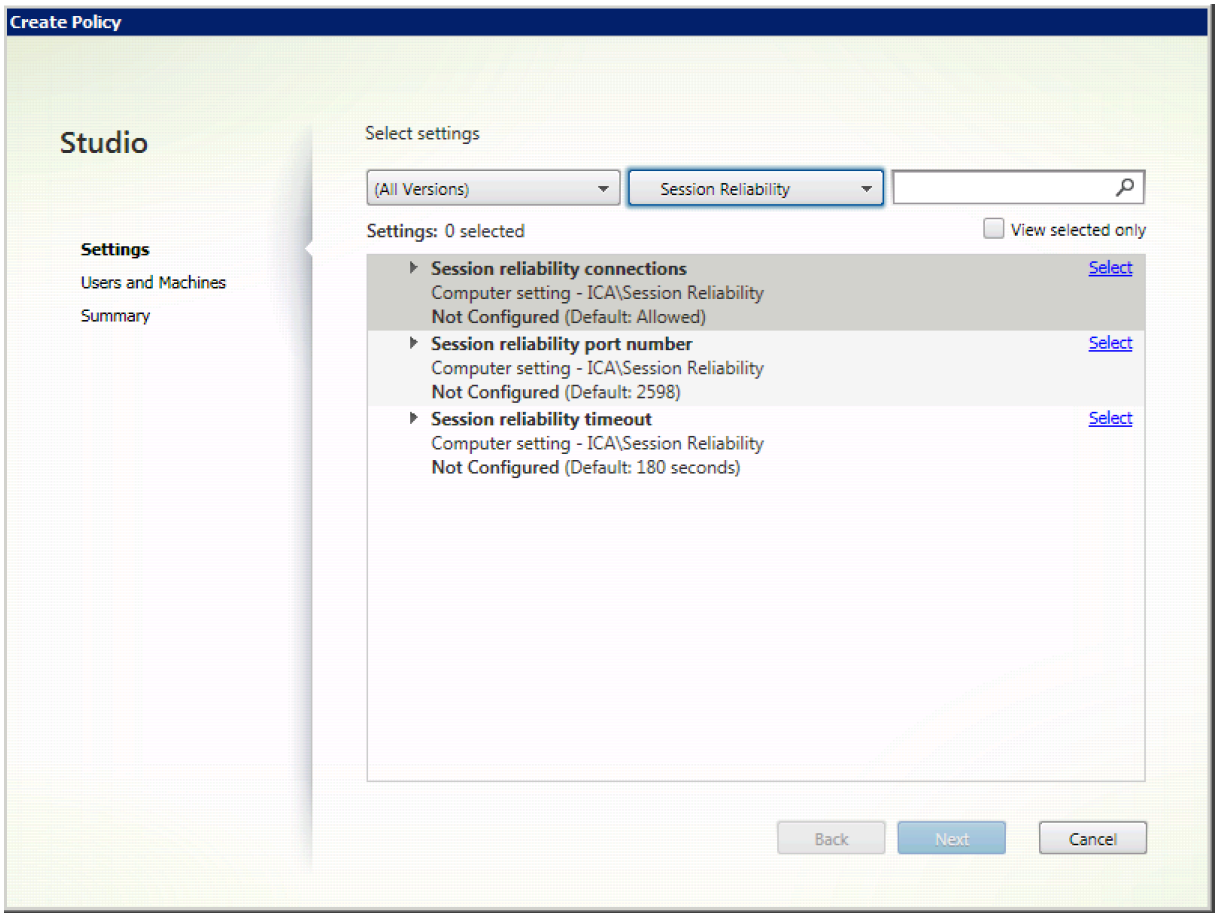
> 注意
>
> 会话可靠性默认在服务器端启用。要禁用此功能，请配置服务器管理的策略。

从 **Citrix Studio** 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。



配置会话可靠性超时

默认情况下，会话可靠性超时设置为 180 秒。

> 注意：
>
> 只能在 XenApp 和 XenDesktop 7.11 及更高版本中配置会话可靠性超时策略。

要修改会话可靠性超时，请执行以下操作：

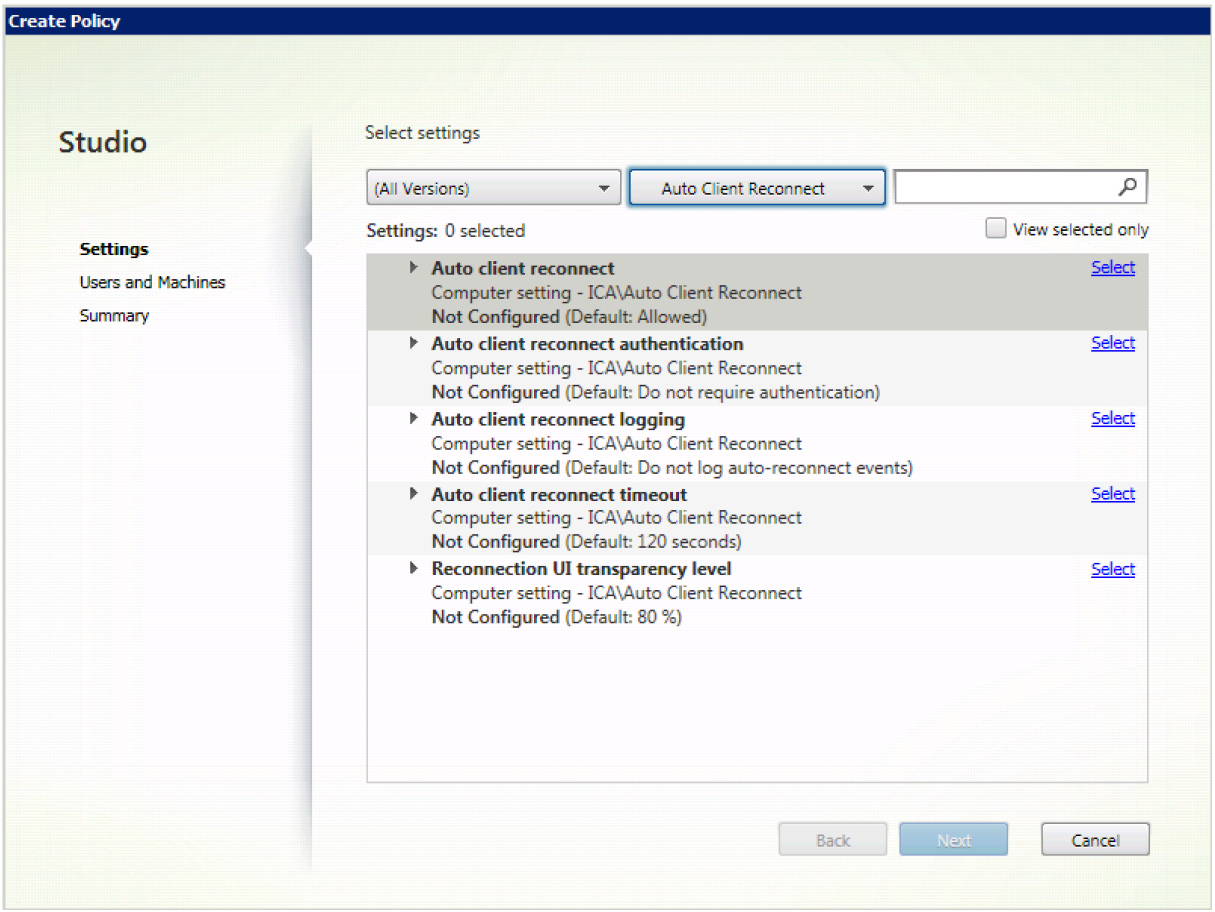
1. 启动 Citrix Studio。
2. 打开会话可靠性超时策略。
3. 编辑超时值。
4. 单击确定。

使用 **Citrix Studio** 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。



配置客户端自动重新连接超时

默认情况下，客户端自动重新连接超时设置为 120 秒。

> 注意：
>
> 只能在 XenApp 和 XenDesktop 7.11 及更高版本中配置客户端自动重新连接超时策略。

要修改客户端自动重新连接超时，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. 编辑超时值。
4. 单击确定。

> 限制：
>
> 在终端服务器 VDA 上，适用于 Mac 的 Citrix Workspace 应用程序使用 120 秒作为超时值，与用户设置无关。

配置重新连接用户界面透明度

会话可靠性和客户端自动重新连接尝试期间将显示会话用户界面。可以使用 Studio 策略修改用户界面的透明度级别。

默认情况下，重新连接用户界面透明度设置为 80%。

要修改重新连接用户界面透明度级别，请执行以下操作：

1. 启动 Citrix Studio。
2. 打开重新连接 **UI** 透明度级别策略。
3. 编辑值。
4. 单击确定。

客户端自动重新连接和会话可靠性交互

存在与在各种接入点之间切换、网络中断以及与延迟相关的显示超时关联的移动难题。尝试维护活动的适用于 Mac 的 Citrix Workspace 应用程序会话的链接完整性时，这些都会创建具有挑战性的环境。为了解决此问题，Citrix 增强了此版本的适用于 Mac 的 Citrix Workspace 应用程序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后自动重新连接到其适用于 Mac 的 Citrix Workspace 应用程序会话。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，启用此功能。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 AutoClienreconnect 的连接超时值。默认情况下，此超时设置为 120 秒（或两分钟）。

设置	示例	默认值
TransportReconnectRetryMaxT‍S	TransportReconnectRetryMaxT‍S	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，启用此功能。

请使用 StoreFront 中的 **default.ica** 文件修改会话可靠性的连接超时值。默认情况下，此超时设置为 180 秒或 3 分钟。

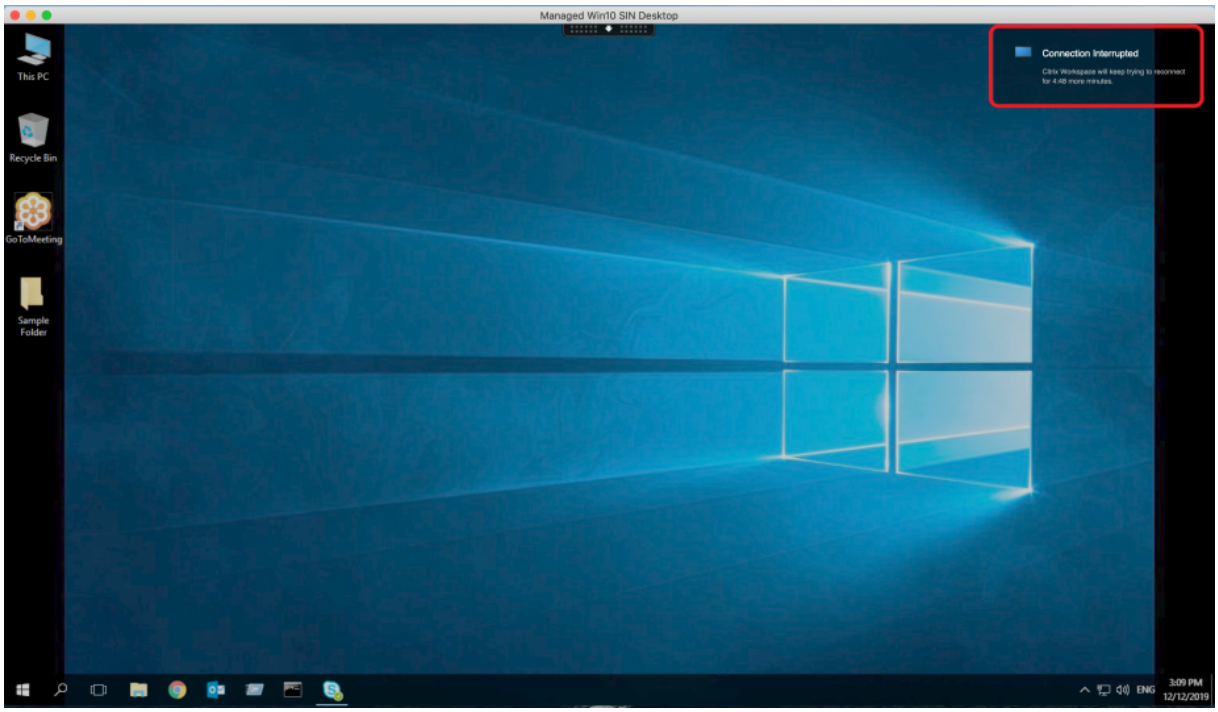
设置	示例	默认值
SessionReliabilityTTL	SessionReliabilityTTL=120	180

客户端自动重新连接和会话可靠性的工作原理

为适用于 Mac 的 Citrix Workspace 应用程序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：

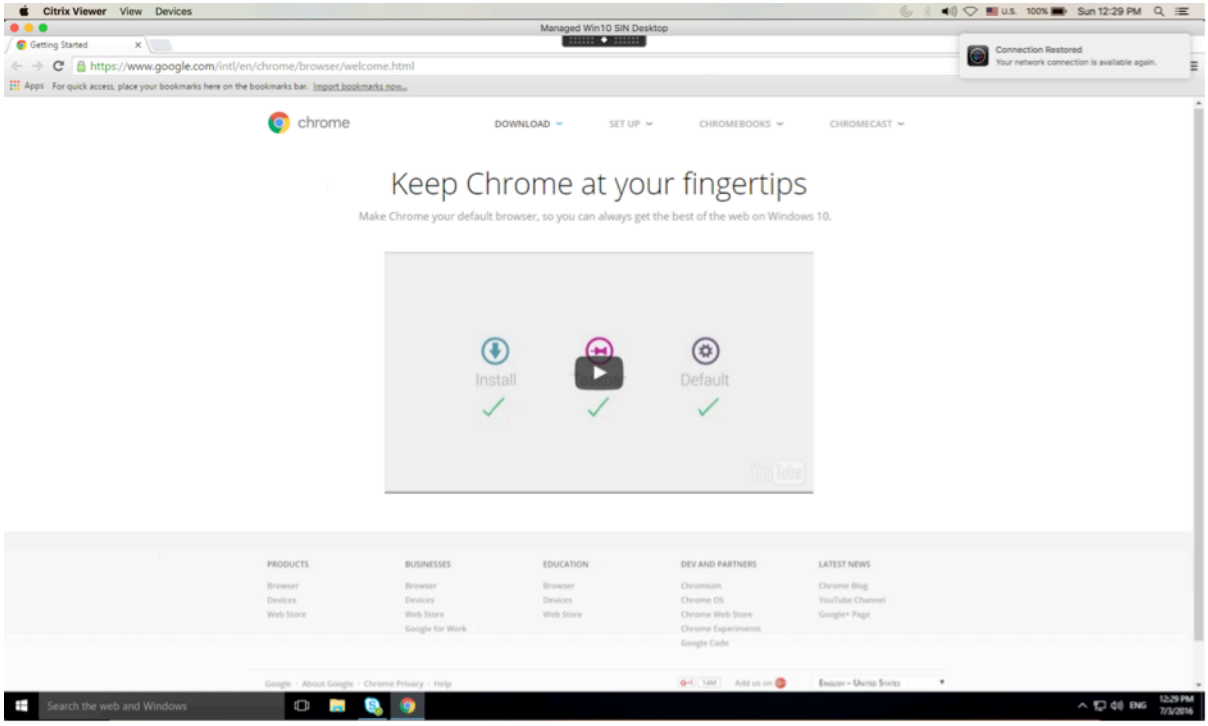
- 重新连接过程中，会话窗口将显示为灰色。倒计时器显示重新连接会话之前的剩余时间。会话超时后将断开连接。

默认情况下，重新连接倒计时通知从 5 分钟开始。此计时器值表示每个计时器（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通知：



> 提示
>
> 可以使用命令提示窗口更改用于不活动会话的灰度亮度。例如，默认写入 com.citrix.receiver.nomasNetDisruptBrightness 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。

客户体验改善计划 **(CEIP)**

收集的数据	说明	我们用它来做什么
配置和使用数据	Citrix 客户体验改善计划 (CEIP) 从适用于 Mac 的 Workspace 应用程序收集配置和使用数据，并自动将数据发送到 Citrix 和 Google Analytics。	此数据可帮助 Citrix 提高 Workspace 应用程序的质量、可靠性和性能。

其他信息

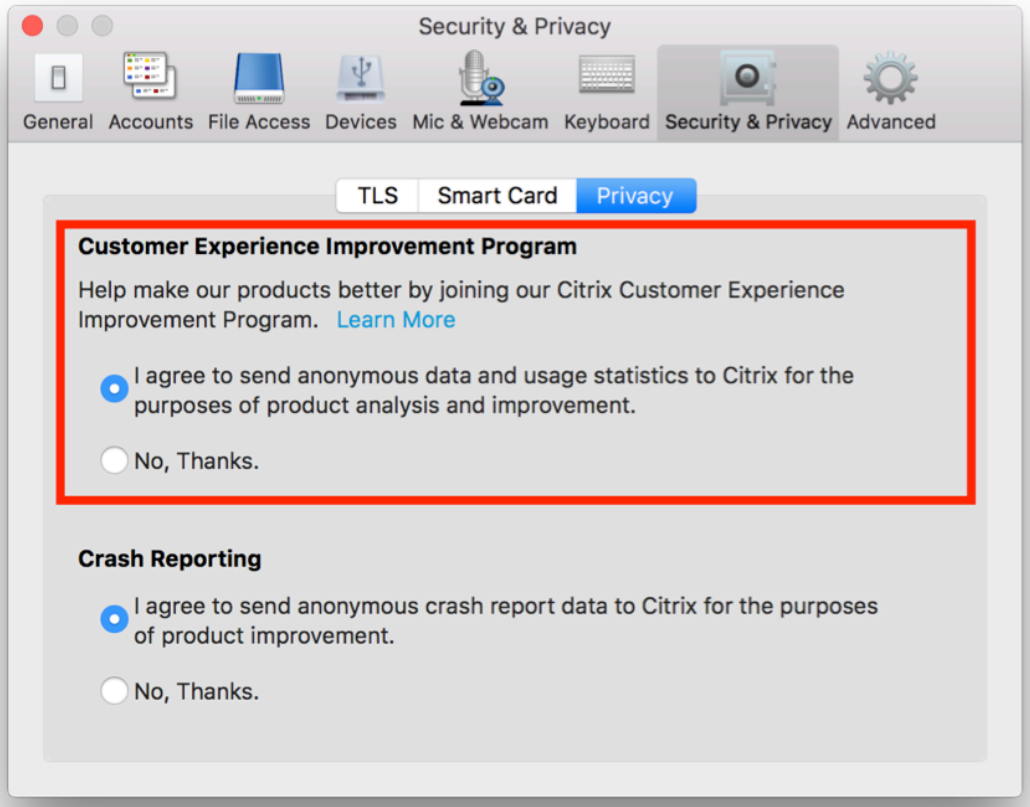
Citrix 将根据您与 Citrix 签订的合同条款处理您的数据，并按照 Citrix Trust Center 上提供的 Citrix Services Security Exhibit 中所指定的方式对其进行保护。

Citrix 使用 Google Analytics 从 Citrix Workspace 应用程序收集某些数据作为 CEIP 的一部分。请查看 Google 如何 处理为 Google Analytics 收集的数据。

可以关闭将 CEIP 数据发送到 Citrix 和 Google Analytics 的功能。为此，您需要：

1. 在首选项窗口中，选择安全和隐私。

2. 选择隐私选项卡。
3. 选择不，谢谢以禁用 CEIP 或者放弃参与。
4. 单击确定。



或者，您可以通过运行终端命令禁用 CEIP：

```
defaults write com.citrix.receiver.nomas "CEIPEnabled"-bool NO
```

Google Analytics 收集的特定数据元素包括：

操作系统版本	会话启动	通用 USB 重定向使用情况

应用程序交付

通过 Citrix Virtual Apps and Desktops 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，适用于 Mac 的 Citrix Workspace 应用程序将提供 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适用于 Web 的 Workspace，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

将 StoreFront 帐户添加到适用于 Mac 的 Citrix Workspace 应用程序，或者将适用于 Mac 的 Citrix Workspace 应用程序配置为指向 StoreFront 站点。然后，您可以配置自助服务模式，此模式使您的用户能够通过适用于 Mac 的 Citrix Workspace 应用程序订阅应用程序。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。

当用户访问 StoreFront 3.0 站点时，您的用户将看到适用于 Mac 的 Citrix Workspace 应用程序预览版。

在 Citrix Virtual Apps 场中发布应用程序时，可以增强通过 StoreFront 应用商店访问这些应用程序的用户的体验。要执行此操作，请务必包含已发布的应用程序的有意义的说明。这些说明通过适用于 Mac 的 Citrix Workspace 应用程序向用户显示。

配置自助服务模式

如前所述，可以将 StoreFront 帐户添加到适用于 Mac 的 Citrix Workspace 应用程序，或者将适用于 Mac 的 Citrix Workspace 应用程序配置为指向 StoreFront 站点。因此，您可以配置自助服务模式，此模式允许用户从适用于 Mac 的 Citrix Workspace 应用程序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、自动预配的以及精选应用程序关键字设置。

- 自动为某个应用商店的所有用户订阅某个应用程序，方法是将字符串 KEYWORDS:Auto 附加到您在 Citrix Virtual Apps 中发布该应用程序时提供的说明后面。用户登录到该应用商店时，将自动置备相应的应用程序，而无需手动订阅该应用程序。
- 向用户公告应用程序，或者在适用于 Mac 的 Citrix Workspace 应用程序的 “精选” 列表中列出常用的应用程序以使其更易于查找。为此，请将字符串 KEYWORDS:Featured 附加到应用程序说明的末尾。

有关详细信息，请参阅 StoreFront 文档。

Citrix Workspace 更新

使用 **GUI** 进行配置

个人用户可以使用首选项对话框覆盖 **Citrix Workspace** 更新设置。这是一项基于用户的配置，并且这些设置仅适用于当前用户。

1. 在适用于 Mac 的 Citrix Workspace 应用程序中转至首选项对话框。

2. 在高级窗格中，单击更新。此时将显示 “Citrix Workspace 更新” 对话框。
3. 选择以下选项之一：
    - 是，通知我
    - 否，不要通知我
    - 使用管理员指定的设置
4. 关闭对话框可保存所做的更改。

使用 **StoreFront** 配置 **Citrix Workspace** 更新

管理员可以使用 StoreFront 配置 Citrix Workspace 更新。适用于 Mac 的 Citrix Workspace 应用程序仅对选中了 “使用管理员指定的设置” 的用户使用此配置。要手动配置，请执行以下步骤。

1. 使用文本编辑器打开 web.config 文件。默认位置为 `C:\inetpub\wwwroot\Citrix\Roaming\web.config`
2. 在该文件中找到用户帐户元素（您的部署的帐户名称为 Store）

    例如：<account id=... name=”Store”>

    在 *</account>* 标记之前，导航到该用户帐户的属性：

    <properties>

    <clear />
    </properties>
3. 在 *<clear />* 标记后面添加自动更新标记。

auto-update-Check

此标记决定适用于 Mac 的 Citrix Workspace 应用程序能够检测更新是否可用。

有效值包括：

- 自动 - 使用此选项可在更新可用时获取通知。
- 手动 - 使用此选项不会在更新可用时获取通知。用户必须通过选择检查更新来手动检查更新。
- 已禁用 - 使用此选项将禁用 Citrix Workspace 更新。

auto-update-DeferUpdate-Count

此标记决定在强制用户更新到最新版本的适用于 Mac 的 Citrix Workspace 应用程序之前通知其升级的次数。默认情况下，此值设置为 7。

有效值包括：

- -1 - 用户始终有权选择以后在更新可用时获得提醒。

- 0 - 更新可用时强制用户更新到最新版本的适用于 Mac 的 Citrix Workspace 应用程序。
- 负整数 - 强制用户更新之前提醒其这么多次。Citrix 建议您不要将此值设置为大于 7 的值。

auto-update-Rollout-Priority

此标记决定设备看到更新可用的速度。

有效值包括：

- 自动 - Citrix Workspace 更新系统决定何时向用户推出可用更新。
- 快 - 根据适用于 Mac 的 Citrix Workspace 应用程序的决定，向用户推出可用更新的优先级为高。
- 中 - 根据适用于 Mac 的 Citrix Workspace 应用程序的决定，向用户推出可用更新的优先级为中。
- 慢 - 根据适用于 Mac 的 Citrix Workspace 应用程序的决定，向用户推出可用更新的优先级为低。

键盘布局同步

使用 Windows 或 Linux VDA 时，键盘布局同步允许用户在客户端设备上的首选键盘布局之间切换。默认情况下，此功能处于禁用状态。

要启用键盘布局同步，请转至首选项 **>** 键盘并选择 “Use local keyboard layout, rather than the remote server keyboard layout”（使用本地键盘布局，而不是远程服务器键盘布局）。

> 注意：
>
> 1. 使用本地键盘布局选项将激活客户端 IME（输入法编辑器）。使用日语、中文或韩语工作的用户可以使用服务器 IME。这些用户必须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。连接到下一个会话时，会话将还原为远程服务器提供的键盘布局。
> 2. 仅当客户端中的开关处于打开状态并在 VDA 上启用了相应的功能时，此功能才在会话中起作用。在设备 > 键盘 > 国际中添加了一个菜单项使用客户端键盘布局，以显示启用状态。

限制

- 在使用此功能时，可以使用 **Mac** 中支持的键盘布局中列出的键盘布局。将客户端键盘布局更改为非兼容布局时，该布局可能会在 VDA 端同步，但无法确认功能。
- 使用提升的权限（例如，以管理员身份运行应用程序）运行的远程应用程序无法与客户端键盘布局同步。要解决此问题，请手动更改 VDA 上的键盘布局或者禁用 UAC。
- RDP 作为应用程序部署时，如果用户在 RDP 会话中工作，则无法使用 Alt+Shift 快捷方式更改键盘布局。要解决此问题，用户可以使用 RDP 会话中的语言栏切换键盘布局。

针对 **Windows VDA** 的键盘布局支持

Supported keyboard layouts on Mac

Language on Mac	Input source on Mac
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Right
	British
	British - PC
	Canadian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Bulgarian	Bulgarian
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Romanian	Romanian - Standard
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Latvian	Latvian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	
Chinese, Traditional	

针对 **Linux VDA** 的键盘布局支持

Language in MAC	Input Source in MAC
English	US.
	U.S. International - PC
	Dvorak
	Dvorak - Left
	Dvorak - Reft
	British
	British - PC
	Candian English
	Australian
	Irish
French	French
	French - Numerical
	Canadian French - CSA
	Swiss French
	French - PC
German	German
	Austrian
	Swiss German
Spanish	Spanish
	Spanish - ISO
Swedish	Swedish
Czech	Czech
Danish	Danish
Finnish	Finnish
Hungarian	Hungarian
Italian	Italian
Greek	Greek
Dutch	Belgian
	Dutch
Russian	Russian - PC
Croatian	Croatian - PC
Slovak	Slovak
	Slovak - QWERTY
Turkish	Turkish
	Turkish - QWERTY PC
Portuguese	Brazilian
	Brazilian - ABNT2
	Portuguese
Ukrainian	Ukrainian - PC
Belarusian	Belarusian
Slovenian	Slovenian
Estonian	Estonian
Polish	Polish Pro
Icelandic	Icelandic
Norwegian	Norwegian
Japanese	Hiragana
	Katakana
	Romaji
Korean	2-Set Korean
	3-Set Korean
Chinese, Simplified	Pinyin -Simplified
Chinese, Traditional	Pinyin - Traditional

增强的客户端取决于键盘布局同步功能。默认情况下，打开了键盘布局同步功能时启用增强的功能。要单独控制此功能，请打开 ~/**Library**/**Application Support**/**Citrix Workspace**/ 文件夹中的 **Config** 文件，找到 **EnableIMEEnhancement** 设置，然后通过将值分别设置为 “true” 或 “false” 来开启或关闭此功能。

> 注意：
>
> 对设置所做的更改将在重新启动会话后生效。

语言栏

您可以选择使用 GUI 在应用程序会话中显示或隐藏远程语言栏。语言栏显示会话中的首选输入语言。在早期版本中，只能在 VDA 上使用注册表项更改此设置。自适用于 Mac 的 Citrix Workspace 版本 1808 起，可以使用首选项对话框更改设置。默认情况下，语言栏在会话中显示。

> 注意：
>
> 此功能在 VDA 7.17 及更高版本上运行的会话中可用。

配置显示或隐藏远程语言栏

1. 打开 “首选项”。
2. 单击 “键盘”。
3. 单击或取消选中 “显示已发布的应用程序的远程语言栏”。

> 注意：
>
> 设置更改将立即生效。可以在活动会话中更改设置。如果仅存在一种输入语言，远程语言栏将不在会话中显示。

Citrix Casting

Citrix Casting 用于将您的 Mac 投射到附近的 Citrix Ready Workspace Hub 设备。适用于 Mac 的 Citrix Workspace 应用程序支持 Citrix Casting 将您的 Mac 屏幕投射到连接 Workspace Hub 的显示器。

有关详细信息，请参阅 Citrix Ready Workspace Hub 文档。

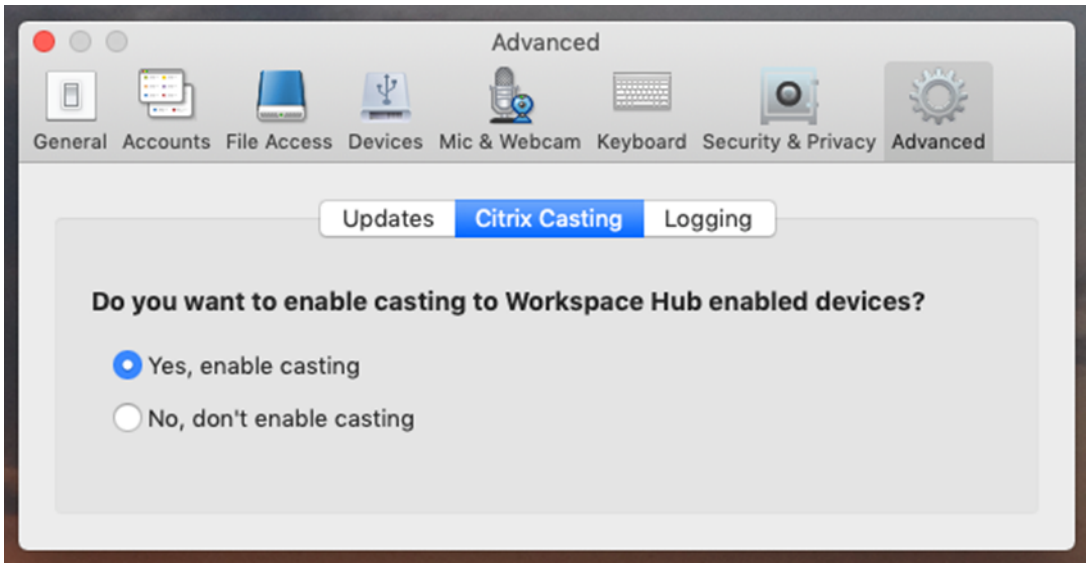
必备条件

- 适用于 Mac 的 Citrix Workspace 应用程序 1812 或更高版本。
- 在设备上启用了蓝牙以便发现 Hub。
- Citrix Ready Workspace Hub 和 Citrix Workspace 应用程序都必须位于同一网络中。
- 确保在运行 Citrix Workspace 应用程序的设备与 Citrix Ready Workspace Hub 之间不阻止端口 55555。
- 端口 55556 为移动设备与 Citrix Ready Workspace Hub 之间的 SSL 连接的默认端口。可以在 Raspberry Pi 的设置页面上配置不同的 SSL 端口。如果阻止了 SSL 端口，用户将无法与 Workspace Hub 之间建立 SSL 连接。
- 对于 Citrix Casting，请确保端口 1494 未被阻止。

启用 **Citrix Casting**

默认情况下，Citrix Casting 处于禁用状态。要使用适用于 Mac 的 Citrix Workspace 应用程序启用 Citrix Casting，请执行以下操作：

1. 转到首选项。
2. 在面板中选择高级，然后选择 **Citrix Casting**。
3. 选择 **Yes, enable casting**（是，启用 Casting）。



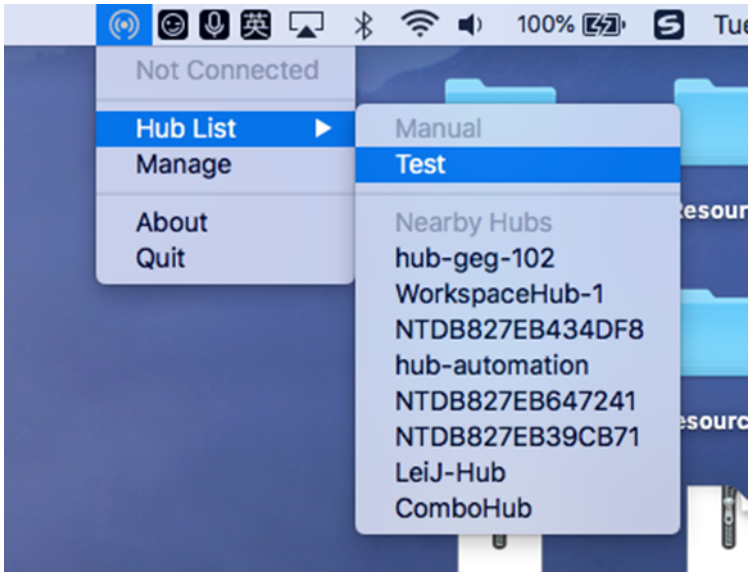
启动 Citrix Casting 且菜单栏中显示 Citrix Casting 图标时，将显示一条通知。

> 注意：
>
> 启用后，Citrix Casting 每次都将与适用于 Mac 的 Citrix Workspace 应用程序一起启动，直到在首选项 **>** 高级 **> Citrix Casting** 中选择 **No, don’t enable casting**（否，不启用 Casting）为止。

自动发现 **Workspace Hub** 设备

要自动连接到 Workspace Hub，请执行以下操作：

1. 在 Mac 上，登录 Citrix Workspace 应用程序并确保蓝牙已打开。使用蓝牙发现附近的 Workspace Hub。
2. 在菜单栏中选择 **Citrix Casting** 图标。所有 Citrix Casting 功能都将通过此菜单执行。
3. **Hub** 列表子菜单将显示同一网络上所有附近的 Workspace Hub。按照 Hub 与您的 Mac 的距离降序列出 Hub，并显示配置了 Workspace Hub 的名称。所有自动发现的 Hub 都显示在附近的 **Hub** 下面。
4. 通过选择其名称来选择要连接到的 Hub。



要在连接过程中取消选择 Workspace Hub，请选择取消。如果网络连接不佳且连接花费的时间比平常长，您也可以使用取消。

> 注意：
>
> 有时，所选的 Hub 可能不会显示在菜单中。请过一段时间后再次查看 **Hub** 列表菜单，或者手动添加您的 Hub。Citrix Casting 会定期接收 Workspace Hub 的广播。

手动发现 **Workspace Hub** 设备

如果在 **Hub** 列表菜单中找不到 Citrix Ready Workspace Hub 设备，请添加 Workspace Hub 的 IP 地址以手动访问该设备。要添加 Workspace Hub，请执行以下操作：

1. 在 Mac 上，登录 Citrix Workspace 应用程序并确保蓝牙已打开。使用蓝牙发现附近的 Workspace Hub。
2. 在菜单栏中选择 **Citrix Casting** 图标。
3. 在菜单中选择管理。此时将显示管理 **Hub** 窗口。
4. 单击新增以输入 Hub 的 IP 地址。
5. 成功添加设备后，**Hub** 名称列将显示 Hub 的友好名称。使用此名称可标识 **Hub** 列表子菜单中的手动部分。

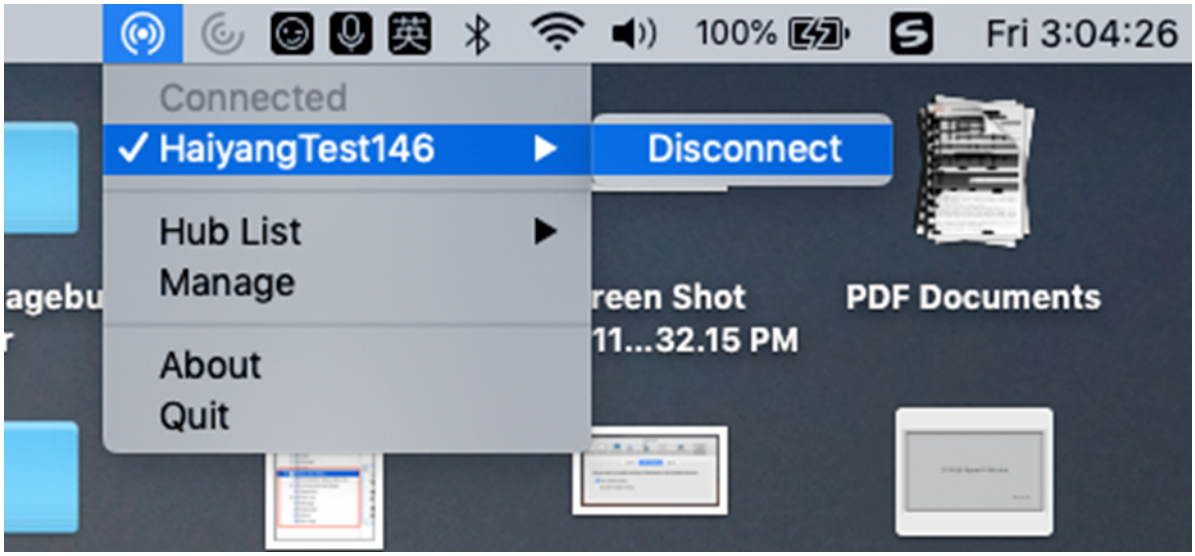
> 注意：
>
> 目前，仅支持镜像模式。镜像是显示模式列中唯一可用的选项。

断开 **Workspace Hub** 设备的连接

可以断开当前会话的连接并自动或手动退出 Citrix Ready Workspace Hub。

- 要自动断开屏幕投射会话的连接，请关闭您的便携式计算机。
- 要手动断开屏幕投射会话的连接，请执行以下操作：

1. 选择 **Citrix Casting** 图标。
2. 在 Hub 列表中，选择 Workspace Hub 的名称。断开连接选项显示在右侧。
3. 选择断开连接以退出 Hub。



已知问题

- 查看镜像屏幕时，存在轻微延迟问题。在网络条件较差的情况下，延迟时间甚至可能会更长。
- 在 Citrix Ready Workspace Hub 中启用 SSL 且 Hub 的证书不受信任时，将显示一个警报窗口。要解决此问题，请使用钥匙串工具将证书添加到受信任的证书列表中。

客户端麦克风输入

适用于 Mac 的 Citrix Workspace 应用程序支持多客户端麦克风输入。本地安装的麦克风可用于：

- 实时事件，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。

适用于 Mac 的 Citrix Workspace 应用程序支持数字听写。

通过在适用于 **Mac** 的 **Citrix Workspace** 应用程序 > 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

适用于 Mac 的 Citrix Workspace 应用程序提供了多个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（例如功能键）。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。从弹出菜单中选择 “Command 或 Control”，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 和键组合作为 Alt+ 键组合。或者，如果选择 Command，则可以使用 Command 键作为 Alt 键。
- “使用 Command (右侧) 发送 Windows 徽标键”。按下键盘右侧的 Command 键，允许您将 Windows 徽标键发送到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。但是，您仍然可以使用 “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。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）。要执行此操作，请选中 “原样发送特殊键” 复选框。默认未选中此复选框，因此，Option-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
INSERT	数字键盘上的 0（数字零）。Num Lock 必须关闭；可以使用 **Clear** 键打开和关闭此按键；Option-Help
DELETE	数字键盘上的小数点。必须关闭 Num Lock；可以使用 **Clear** 键打开和关闭此按键；Clear
F1 到 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。Mac 操作系统对其进行解释。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。Mac 键盘不会模仿这些快捷方式。但是，可以使用键盘菜单将这

些快捷方式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，适用于 Mac 的 Citrix Workspace 应用程序提供了多个选项，以确保可以将按键正确地转发给托管应用程序和桌面。表中列出了这些按键。其中说明了默认行为。如果您调整默认行为（使用适用于 Mac 的 Citrix Workspace 应用程序或其他首选项），可能会转发不同的按键组合，并且可能会在 Remote PC Access 上观察到其他行为。

> 重要
>
> 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，这并不表示必须同时按下 Shift 键。
- 按键之间的连字符表示必须同时按这些键（例如，Control-C）。
- 字符键是指创建文本输入并包含所有字母、数字和标点符号的字符键。特殊键是指不自行创建输入但充当修饰符或控制器的键。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 是指 Mac 键盘上的 Fn（功能）键。功能键是指 PC 或 Mac 键盘上的 F1 到 F12。

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-Fn-Command-Delete；选择 “键盘”>“发送 Ctrl-Alt-Del”
删除	Delete；选择 “键盘”>“发送按键”>“Delete”；Fn-Backspace（某些美国键盘上的 Fn-Delete）
End	End；Fn-右箭头键

Windows 键或按键组合	Mac 上具有相同作用的按键
Esc	Escape；选择 “键盘”>“发送按键”>“Escape”
F1 至 F12	F1 到 F12；选择 “键盘”>“发送功能键”> F1 至 F12
主页	Home；Fn-左箭头键
Insert	选择 “键盘”>“发送按键”> Insert
Num Lock	Clear
PgDn	Page Down；Fn-下箭头键
PgUp	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”>“启动”
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

适用于 Mac 的 Citrix Workspace 应用程序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。

适用于 Mac 的 Citrix Workspace 应用程序还允许用户指定自己要使用的键盘布局。

启用客户端 IME

1. 在 “Citrix Viewer” 菜单栏中，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

- 在 “Citrix Viewer” 菜单栏中，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

适用于 Mac 的 Citrix Workspace 应用程序会为 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。

多显示器

用户可以将适用于 Mac 的 Citrix Workspace 应用程序设置为跨多个显示器在全屏模式下运行。

1. 选择 Desktop Viewer 并单击下箭头。
2. 选择窗口。
3. 在显示器之间拖动 Citrix Virtual Desktops 屏幕。确保每个显示器中大约显示一半屏幕。
4. 在 Citrix Virtual Desktop 工具栏中，选择全屏。

屏幕现在将扩展到所有显示器。

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。
- Citrix 建议最多使用 2 个显示器。使用 2 个以上的显示器可能会降低会话性能或导致出现可用性问题。

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。其他工具栏变更包括：

- 已从工具栏删除 **Home**（主页）按钮。可以通过使用以下命令运行此功能：
  - 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。可以通过以下方式运行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。
  - 对于 OS X 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。

工作区控制

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，医护人员从医院急诊室的用户设备注销，然后登录到医院 X 射线实验室的工作站。当用户在 X 射线实验室中登录到用户设备时，适用于 X 射线实验室中的会话的策略、打印机映射和客户端驱动器映射在会话中生效。

配置工作区控制设置

1. 单击适用于 Mac 的 Citrix Workspace 应用程序窗口中的下箭头键图标，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 Citrix Workspace app（当我启动 Citrix Workspace 应用程序时重新连接应用程序）。允许用户在启动 Citrix Workspace 应用程序时重新连接到已断开连接的应用程序。
   - 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适用于 Mac 的 Citrix Workspace 应用程序菜单中选择“刷新应用程序”时重新连接到已断开连接的应用程序。

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。

适用于 Mac 的 Citrix Workspace 应用程序负责监视 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。

可以使用适用于 Mac 的 Citrix Workspace 应用程序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. 在适用于 Mac 的 Citrix Workspace 应用程序主页中，依次单击下箭头键图标和首选项。
2. 单击文件访问。

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。

身份验证

August 14, 2020

智能卡

适用于 Mac 的 Citrix Workspace 应用程序支持在以下配置中使用智能卡身份验证：

- 对适用于 Web 的 Workspace 或 StoreFront 2.x 及更高版本进行智能卡身份验证
- Citrix Virtual Apps and Desktops 7 1808 及更高版本
- XenDesktop 7.1 及更高版本或 XenApp 6.5 及更高版本
- 启用了智能卡的应用程序，例如 Microsoft Outlook 和 Microsoft Office。这些功能允许用户对虚拟桌面或应用程序会话中可用的文档进行数字签名或加密。
- 适用于 Mac 的 Citrix Workspace 应用程序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，这些证书可用于在设备上运行的所有应用程序，包括适用于 Mac 的 Citrix Workspace 应用程序。
- 对于双跳场景，需要在适用于 Mac 的 Citrix Workspace 应用程序与用户的虚拟桌面之间建立更进一步的连接。

关于对 **Citrix Gateway** 进行智能卡身份验证

使用智能卡对连接进行身份验证时，有多个可用证书。适用于 Mac 的 Citrix Workspace 应用程序会提示您选择证书。选择证书后，适用于 Mac 的 Citrix Workspace 应用程序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，适用于 Mac 的 Citrix Workspace 应用程序将使用该证书，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

> 注意：
>
> 不强制安装 PKCS#11 模块。本节仅适用于 ICA 会话。不适用于在需要智能卡的情况下 Citrix Workspace 对 Citrix Gateway 或 StoreFront 的访问。

要为智能卡身份验证指定 PKCS#11 模块，请执行以下操作：

1. 在适用于 Mac 的 Citrix Workspace 应用程序中，选择首选项。
2. 单击安全和隐私。
3. 在安全和隐私部分中，单击智能卡。
4. 在 **PKCS#11** 字段中，选择相应的模块。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。

支持的读卡器、中间件和智能卡配置文件

适用于 Mac 的 Citrix Workspace 应用程序支持大部分 macOS 兼容的智能卡读卡器和加密中间件。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：

- Clarify
- ActivIdentity 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 macOS 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。
- 适用于 Mac 的 Citrix Workspace 应用程序不保存用户所做的证书选择。
- 适用于 Mac 的 Citrix Workspace 应用程序不存储或保存用户的智能卡 PIN。操作系统负责处理 PIN 获取，而操作系统可能有自己的缓存机制。
- 插入智能卡后，适用于 Mac 的 Citrix Workspace 应用程序不会重新连接会话。
- 要将智能卡身份验证与 VPN 通道结合使用，必须安装 Citrix Gateway 插件并通过 Web 页面登录。使用智能卡和 PIN 在每个步骤中进行身份验证。使用 Citrix Gateway 插件通过直通身份验证访问 StoreFront 不适用于智能卡用户。

安全通信

May 24, 2021

要确保您的站点与适用于 Mac 的 Citrix Workspace 应用程序之间的通信安全，可以将连接与一系列的安全技术（包括 Citrix Gateway）集成在一起。有关通过 Citrix StoreFront 配置 Citrix Gateway 的信息，请参阅 StoreFront 文档。

> 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 Citrix Workspace 与服务器之间的连接。适用于 Mac 的 Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。
- Citrix Secure Web Gateway。可以使用 Citrix Secure Web Gateway，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。
- 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。在使用适用于 Mac 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。

> 注意：
>
> 自 macOS Catalina 起，Apple 已经强制执行了对根 CA 证书和管理员必须配置的中间证书的额外要求。有关详细信息，请参阅 Apple 支持文章 HT210176。

Citrix Gateway

要使远程用户能够通过 Citrix Gateway 连接到您的 XenMobile 部署，可以将 Citrix Gateway 配置为支持 StoreFront。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 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 Mac 的 Citrix Workspace 应用程序进行连接。

通过 **Citrix Secure Web Gateway** 进行连接

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

如果使用中继模式，Citrix Secure Web Gateway 服务器将相当于一个代理，并且必须配置适用于 Mac 的 Citrix Workspace 应用程序才能使用：

- Citrix Secure Web Gateway 服务器的完全限定的域名 (FQDN)。

- Citrix Secure Web Gateway 服务器的端口号。Citrix Secure Web Gateway 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) 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，并处理适用于 Mac 的 Citrix Workspace 应用程序与服务器之间的连接。适用于 Mac 的 Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。

在与 Web 服务器进行通信时，适用于 Mac 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。请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。

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。适用于 Mac 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（对于 Secure Web 服务器，则通常通过标准 HTTP 端口 80 或 443 传输流量）。对于 Citrix Workspace 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。

TLS

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

为了增强安全性，以下密码套件已弃用：

- 前缀为 “TLS_RSA_*” 的密码套件

- 密码套件 RC4 和 3DES
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_RSA_WITH_RC4_128_SHA (0x0005)
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

适用于 Mac 的 Citrix Workspace 应用程序仅支持以下密码套件：

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

对于 DTLS 1.0 用户，适用于 Mac 的 Citrix Workspace 应用程序 1910 及更高版本仅支持以下密码套件：

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

如果要使用 DTLS 1.0，请将您的 Citrix Gateway 版本升级到 12.1 或更高版本。否则，将回退到基于 DDC 策略的 TLS。

以下列表提供了内部和外部网络连接的详细信息：

		Direct connections								
		TLS			DTLS v1.0			DTLS v1.2		
Client cipher set	VDA cipher set	Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			Y		
	COM	Y	X	X	Y			Y		
	GOV	Y	Y	Y	Y			Y		
COM	ANY	Y	X	X	Y					
	COM	Y	X	X	Y					
	GOV	Y	X	X	Y					
GOV	ANY	Y	Y	Y	X			Y		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			Y		

Client cipher set	VDA cipher set	External connections with Citrix Gateway								
		TLS			DTLS v1.0			DTLS v1.2		
		Open	FIPS	SP800-52	Open	FIPS	SP800-52	Open	FIPS	SP800-52
Any	ANY	Y	Y	Y	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	Y	Y	Y			X		
COM	ANY	Y	X	X	Y			X		
	COM	Y	X	X	Y			X		
	GOV	Y	X	X	Y			X		
GOV	ANY	Y	Y	Y	X			X		
	COM	X	X	X	X			X		
	GOV	Y	Y	Y	X			X		

> 注意：
>
> - 请使用 Citrix Gateway 12.1 或更高版本，以便 EDT 正常运行。较旧的版本在 DTLS 模式下不支持 ECDHE 密码套件。
> - Citrix Gateway 不支持 DTLS 1.2。因此，不支持 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 和 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384。Citrix Gateway 必须配置为使用 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 才能在 DTLS 1.0 中正常运行。

为 **TLS** 配置并启用 **Citrix Workspace** 应用程序

TLS 的设置主要涉及两个步骤：

1. 在 Citrix Virtual Apps and Desktops 服务器上设置 SSL Relay，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

要在启用了 TLS 的适用于 Mac 的 Citrix Workspace 应用程序与服务器场之间使用 TLS 来确保通信安全，需要使用用户设备上的根证书。此根证书验证证书颁发机构在服务器证书上的签名。

macOS X 附带约 100 个已安装的商用根证书。但是，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 macOS 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（证书只应用于当前用户。）
   - 系统（证书应用于设备的所有用户。）
3. 单击确定。
4. 在“身份验证”对话框中键入密码，然后单击“确定”。

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。

关于 **TLS** 策略

本节介绍与在适用于 Mac 的 Citrix Workspace 应用程序中通过 TLS 为 ICA 会话配置安全策略有关的信息。可以配置在适用于 Mac 的 Citrix Workspace 应用程序中用于 ICA 连接的某些 TLS 设置。这些设置不会在用户界面中显示。更改这些策略需要在运行适用于 Mac 的 Citrix Workspace 应用程序的设备上运行命令。

> 注意
>
> 可以通过其他方式管理 TLS 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。

TLS 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：

- 无。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

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

SecurityAllowedTLSVersions。此设置指定协议协商期间接受的 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。

```
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颁发机构。

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 或 Citrix Secure Web 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 或 Citrix Secure Web 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**。将执行证书吊销列表检查，但不包括根证书颁发机构。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。
>
> ```
> defaults write com.citrix.receiver.nomas SSLCertificateRevocationCheckPolicy
>  FullAccessCheckAndCRLRequired
> ```

配置 **TLS** 策略

要在非托管计算机上配置 TLS 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 首选项列表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 **>** 实用程序 **\ >** 终端。
2. 在“终端”中，运行以下命令：

```
defaults write com.citrix.receiver.nomas <name> <type> <value>
```

其中：

<name>：上述设置的名称。

<type>：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。

<value>：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。

```
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 **>** 实用程序 **\ >** 终端。
2. 在“终端”中，运行以下命令：

```
defaults delete com.citrix.receiver.nomas <name>
```

其中：

<name>：上述设置的名称。

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

安全设置

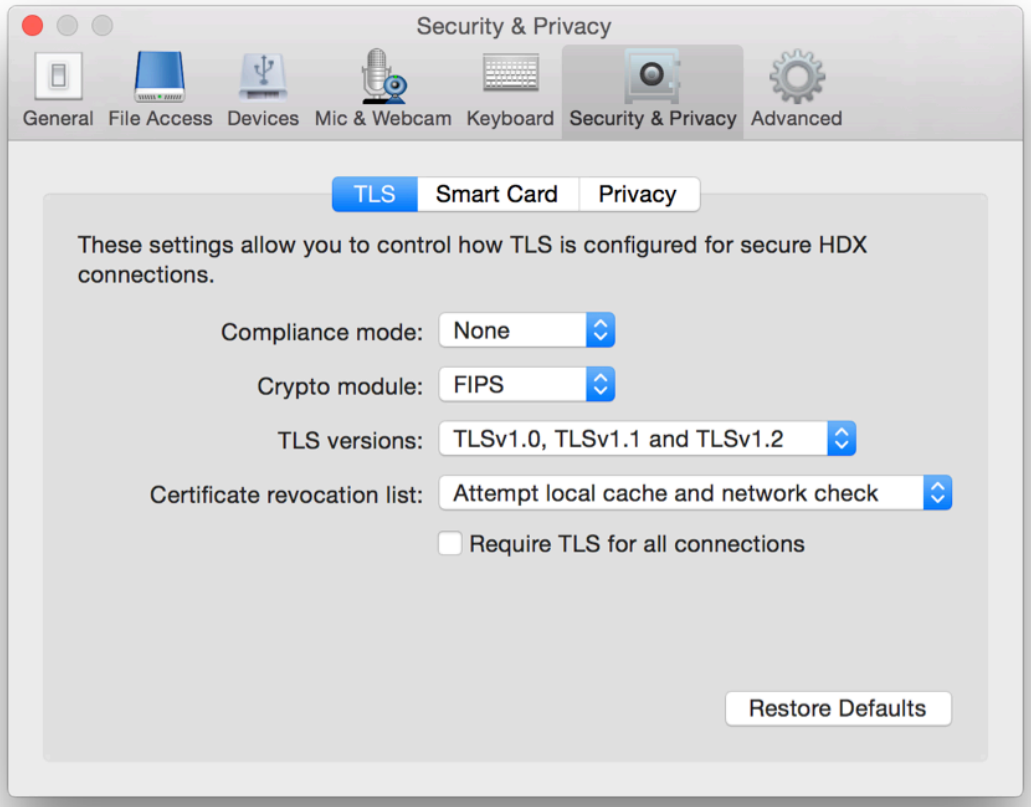
Citrix Receiver for Mac 12.3 中引入了多项安全性改进功能和增强功能，其中包括：

- 改进了安全性配置用户界面。在早期版本中，命令行是进行与安全相关的更改的首选方法。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。可以验证与使用特定 TLS 版本、用于连接的加密算法、模式、密钥大小和 SecureICA 状态的服务器建立的连接。此外，还可以查看用于 TLS 连接的服务器证书。

改进后的安全和隐私屏幕包括 **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和隐私设置：



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