citrix

Secure Web

Contents

Secure Web 中的新增功能

April 6, 2021

> 注意：
>
> 对 Android 6.x 和 iOS 11.x 版本的 Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的支持已于 2020 年 6 月结束。

当前版本中的新增功能

Secure Web 21.3.5

Secure Web for Android

此版本包括缺陷修复。

早期版本中的新增功能

Secure Web 21.3.0

Secure Web for Android

此版本包括缺陷修复。

Secure Web 21.2.0

Secure Web for iOS

Secure Web 的颜色改造。Secure Web 符合 Citrix 品牌颜色更新。

Secure Web for Android

- **Secure Web** 的颜色改造。Secure Web 符合 Citrix 品牌颜色更新。
- 在可折叠设备上稳定运行。Secure Web for Android 包括在可折叠设备上稳定运行的修复程序。

Secure Web 21.1.5

Secure Web for iOS

此版本包括缺陷修复。

Secure Web 21.1.0

此版本包括缺陷修复。

Secure Web 20.12.0

Secure Web for iOS

此版本包括缺陷修复。

Secure Web 20.11.0

此版本包括缺陷修复。

Secure Web 20.10.5

Secure Web for Android

支持 **AndroidX** 库。根据 Google 的建议，Secure Web 支持 **AndroidX** 库，这些库是 **android.support** 打包的库的替换库。

Secure Web 20.10.0

Secure Web for Android

Secure Web 支持 Google Play 对 Android 10 的当前目标 API 要求。

Secure Web 20.9.5

Secure Web for iOS

此版本包括缺陷修复。

Secure Web 20.9.0

Secure Web for Android

> 注意：
>
> 对 Android 6.x 的支持已于 2020 年 9 月 15 日结束。

Secure Web 20.8.5

Secure Web for Android

Secure Web for Android 支持 Android 11。

Secure Web 20.8.0

Secure Web for Android

Secure Web 的 **Android** 版本的双模式（预览版）。移动应用程序管理 (MAM) SDK 可用于替换 iOS 和 Android 平台未涵盖的 MDX 功能区域。MDX 封装技术计划于 2021 年 9 月达到生命周期结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。

自 20.8.0 版起，Android 应用程序随 MDX 和 MAM SDK 一起发布，以便为上文提及的 MDX EOL 策略做好准备。MDX 双模式旨在提供一种从旧版 MDX Toolkit 过渡到新 MAM SDK 的方法。使用双模式功能，您将能够继续使用 MDX Toolkit（现为旧版 **MDX**）管理应用程序，或者切换到新 MAM SDK 进行应用程序管理。

切换到 MAM SDK 进行应用程序管理后，Citrix 将实施进一步的更改，并且不需要管理员执行任何操作。

有关 MAM SDK 的详细信息，请参阅以下文章：

- MAM SDK 概述
- 设备管理 上的 Citrix Developer 部分
- Citrix 博客文章
- 当您登录到 Citrix 下载 时下载 SDK

必备条件

要成功部署双模式功能，请确保以下各项：

- 将 Citrix Endpoint Management 更新到 10.12 RP2 及更高版本，或 10.11 RP5 及更高版本。
- 将您的移动应用程序更新到 20.8.0 或更高版本。
- 将策略文件更新到版本 20.8.0 或更高版本。
- 如果贵组织使用第三方应用程序，请务必在切换到 Citrix 移动生产力应用程序的 MAM SDK 选项之前将 MAM SDK 合并到第三方应用程序中。您的所有托管应用程序都必须同时移动到 MAM SDK。

> 注意：
>
> 支持所有基于云的客户使用 MAM SDK。

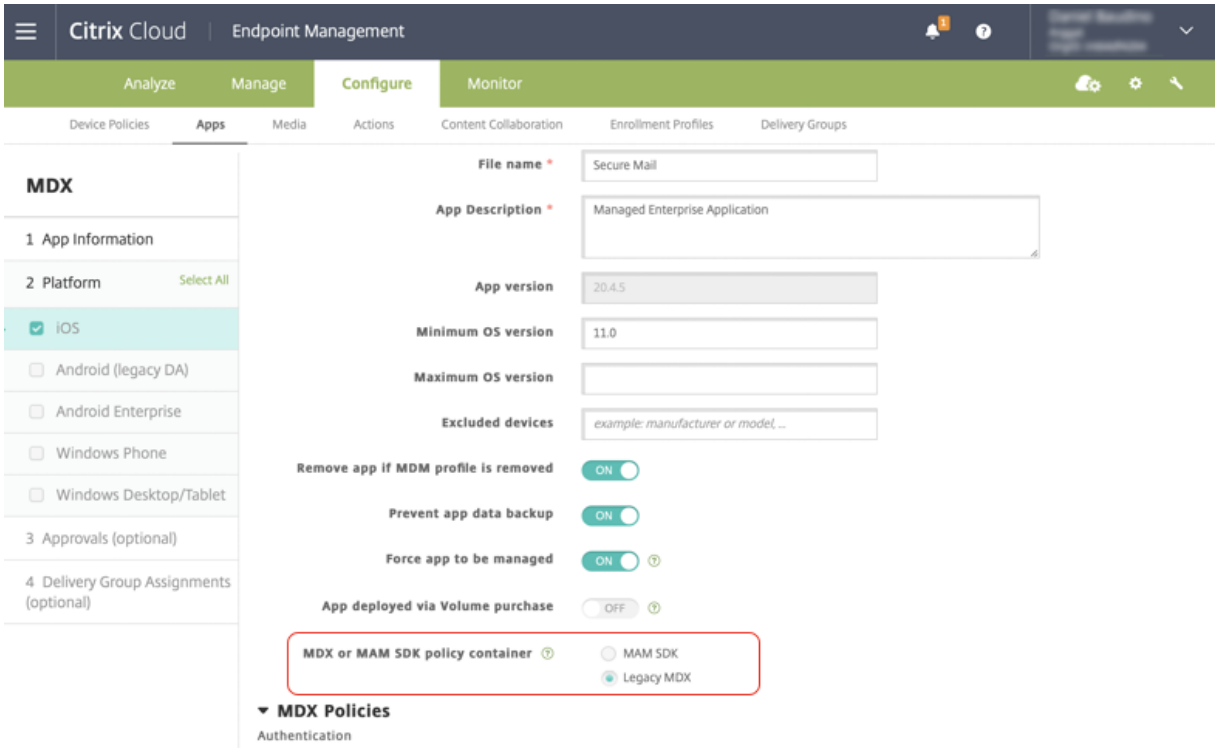
限制

- 只有在 Citrix Endpoint Management 部署中在 Android Enterprise 平台下发布的应用程序才支持 MAM SDK。对于新发布的应用程序，默认加密是基于平台的加密。
- MAM SDK 仅支持基于平台的加密，不支持 MDX 加密。
- 如果不更新 Citrix Endpoint Management，并且策略文件在版本为 20.8.0 及更高版本的移动应用程序上运行，则会为 Secure Web 创建网络策略的重复条目。

在 Citrix Endpoint Management 中配置 Secure Web 时，双模式功能允许您继续使用 MDX Toolkit（现为旧版 **MDX**）管理应用程序，或者切换到新 **MAM SDK** 进行应用程序管理。Citrix 建议您切换到 **MAM SDK**，因为 MAM SDK 的模块化程度更高，仅允许您使用组织使用的一部分 MDX 功能。它减少了应用程序的整体二进制文件内和运行时占用空间。

可以在 **MDX** 或 **MAM SDK** 策略容器中获取以下策略设置选项：

- **MAM SDK**
- 旧版 **MDX**



在 **MDX** 或 **MAM SDK** 策略容器策略中，您只能将选项从旧版 **MDX** 更改为 “MAM SDK”。不允许使用从 “MAM SDK” 切换到 旧版 **MDX** 的选项，您需要重新发布应用程序。默认值为 “旧版 MDX”。确保为在同一设备上运行的 Secure Mail 和 Secure Web 设置了相同的策略模式。不能在同一设备上运行两种不同的模式。

Secure Web 20.7.5

此版本包括缺陷修复。

Secure Web 20.7.0

支持多任务处理。在 Secure Web for iOS 中，将两个应用程序同时与多任务处理结合使用。要启用此功能，请将某个应用程序拖出基站。将该应用程序滑动到屏幕的右边缘或左边缘，以拆分和启用两个应用程序的屏幕。

有关移动生产力应用程序的最新信息，请参阅文章 最新声明。

Secure Web 20.6.0

此版本包括缺陷修复。

Secure Web 20.5.0

此版本包括缺陷修复。

Secure Web 20.4.5

导航到新选项卡中的书签。在 Secure Web for iOS 中，您可以在打开新选项卡时查看、编辑和导航到书签。

Secure Web 19.10.5 到 20.4.0

这些版本包括缺陷修复。

Secure Web 19.10.0

Secure Web iOS 和 **Android** 支持加密管理。加密管理允许您使用新式设备平台安全性，同时确保设备处于足够的状态，以便有效地使用平台安全性。通过使用加密管理，您可以消除本地数据加密冗余，因为文件系统加密是由各自的 iOS 或 Android 平台提供的。要启用此功能，管理员必须在 Citrix Endpoint Management 控制台中将加密类型 MDX 策略设置为强制合规的平台加密。

加密管理允许您使用新式设备平台安全性，同时确保设备处于足够的状态，以便有效地使用平台安全性。通过使用加密管理，您可以消除本地数据加密冗余，因为文件系统加密是由 iOS 或 Android 平台提供的。要启用此功能，管理员必须在 Citrix Endpoint Management 控制台中将加密类型 MDX 策略设置为强制合规的平台加密。

加密类型

要使用加密管理功能，请在 Citrix Endpoint Management 控制台中，将加密类型策略设置为强制合规的平台加密。这样可以实现加密管理，并且用户设备上的所有现有加密应用程序数据将无缝转换到由设备而非 MDX 加密的状态。在此转换期间，应用程序将暂停以进行一次性数据迁移。成功迁移后，本地存储的数据的加密责任将从 MDX 转移到设备平台。MDX 在每次应用程序启动时都会继续检查设备的合规性。此功能适用于 MDM + MAM 和仅 MAM 环境。

将加密类型策略设置为强制合规的平台加密时，新策略将取代您现有的 MDX 加密。

有关适用于 Secure Web 的加密管理 MDX 策略的详细信息，请参阅以下内容中的加密部分：

- 适用于 iOS 的移动生产力应用程序的 MDX 策略
- 适用于 Android 的移动生产力应用程序的 MDX 策略

不合规设备行为

当设备低于最低合规性要求时，不合规设备行为策略将允许您选择要执行的操作：

- 允许应用程序 — 允许应用程序正常运行。
- 允许应用程序在显示警告后运行 — 警告用户应用程序不符合最低合规性要求，但允许应用程序运行。此为默认值。

- 阻止应用程序 — 阻止应用程序运行。

以下标准确定设备是否满足最低合规性要求。

运行 iOS 的设备：

- iOS 10：应用程序正在运行高于或等于指定版本的操作系统版本。
- 调试器访问：应用程序未启用调试。
- 越狱设备：应用程序不在越狱设备上运行。
- 设备通行码：“设备通行码”设置为“开”。
- 数据共享：未为应用程序启用数据共享。

运行 Android 的设备：

- Android SDK 24 (Android 7 Nougat)：应用程序正在运行高于或等于指定版本的操作系统版本。
- 调试器访问：应用程序未启用调试。
- 已获得 root 权限的设备：应用程序不在已获得 root 权限的设备上运行。
- 设备锁定：“设备通行码”设置为“开”。
- 设备已加密：应用程序在加密设备上运行。

Secure Web 19.9.5

此版本包括缺陷修复。

Secure Web 19.9.0

Secure Web for iOS

Secure Web for iOS 支持 iOS 13。

Secure Web for Android

此版本包括缺陷修复。

Secure Web for Android 19.8.5

Secure Web for Android 支持 Android Q。

Secure Web 19.8.0

此版本包括缺陷修复。

Secure Web 19.7.5

Secure Web for iOS

本版本包括性能增强和缺陷修复。

Secure Web for Android

自本版本起，Secure Web for Android 仅在运行 Android 6 或更高版本的设备上受支持。

Secure Web 19.3.0 到 19.6.5

这些版本包括性能增强和缺陷修复。

Secure Web 19.2.0

允许链接在 **Secure Web** 中打开，确保数据安全。使用 Secure Web 时，专用 VPN 通道允许用户安全地访问包含敏感信息的站点。此功能已对 Secure Web for iOS 可用。此版本增加了对 Android 的支持。有关更多详细信息，请参阅Secure Web 功能。

Secure Web 版本 18.11.5 到 19.1.5

这些版本包括性能增强和缺陷修复。

Secure Web 18.11.0

在 Secure Web for iOS 中，将不再报告站点的缓存大小列表且该列表不会显示在应用程序设置中。默认缓存功能将保持不变。

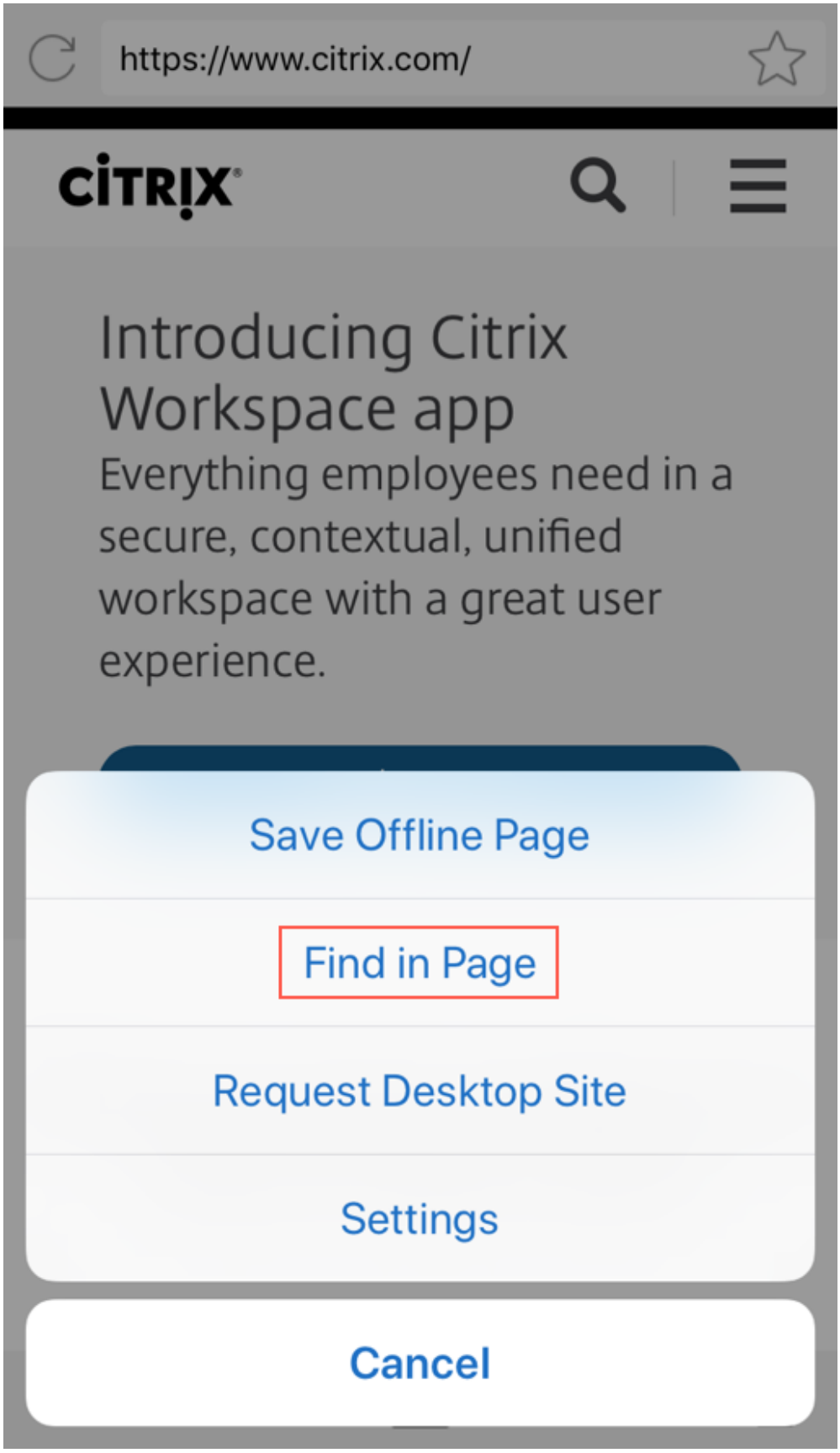
Secure Web 18.9.0 到 18.10.5

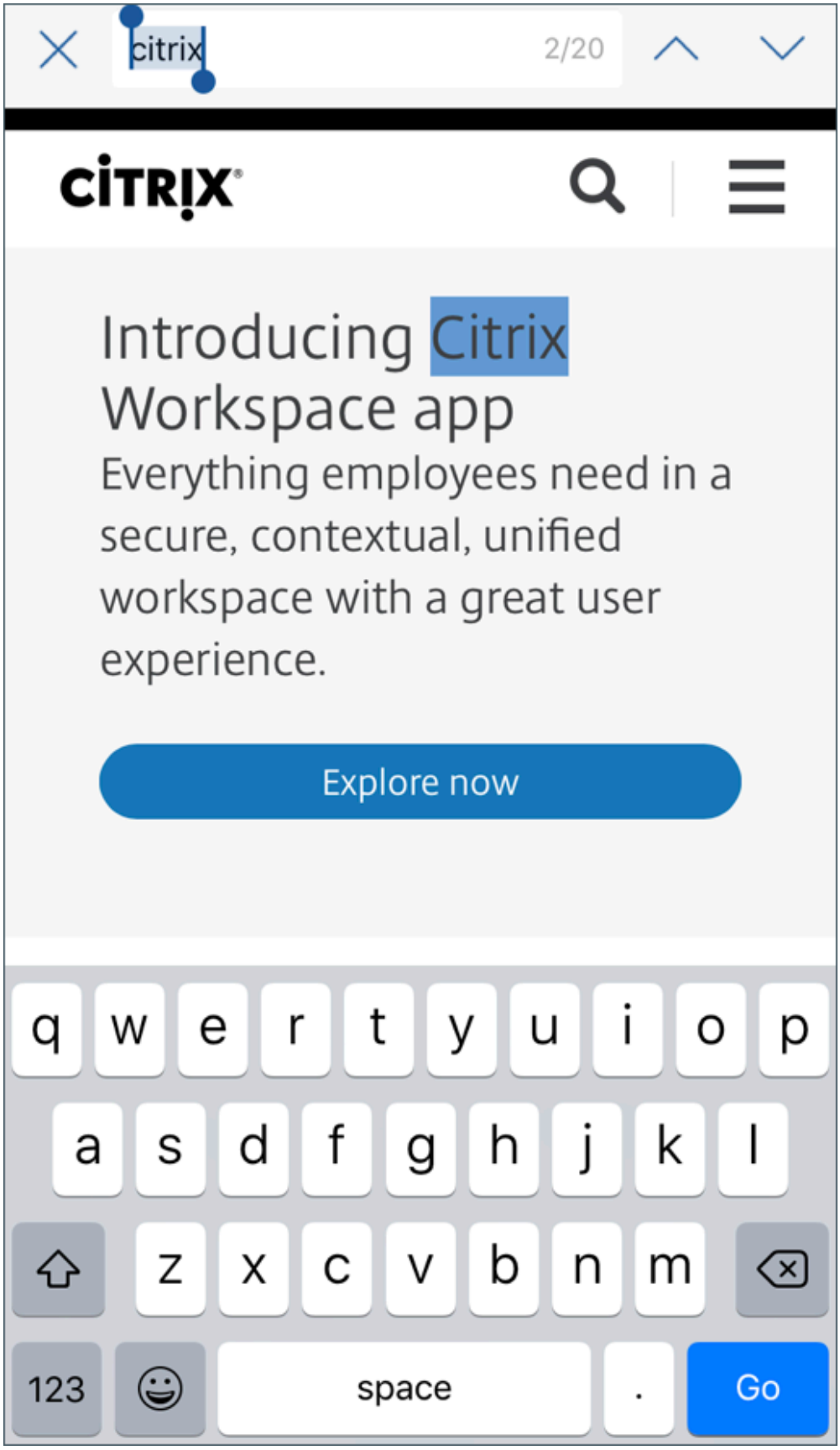
这些版本包括性能增强和缺陷修复。

Secure Web 10.8.65

下列功能是 Secure Web 10.8.65 中的新增功能：

- 下拉刷新。在 Secure Web for iOS 中，用户可以使用下拉刷新功能更新其屏幕上的数据。
- 使用 **“**在网页中查找**”** 选项进行搜索。您可以使用在页面中查找选项即时搜索字符串。此选项会在您搜索时突出显示关键字，并在工具栏右侧显示总匹配数。在重新启动时，此功能保留过去搜索的关键字。





- 向上滚动时隐藏页眉和页脚栏。在 Secure Web for iOS 中，向上滚动时页眉和页脚栏处于隐藏状态。这样，查看 Web 页面时，移动设备的屏幕上可显示更多信息。

Secure Web 10.8.60

- 支持波兰语

Secure Web 10.8.35

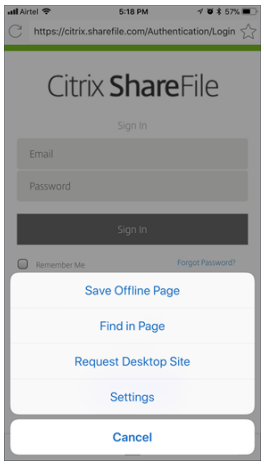
- 下拉刷新。在 Secure Web for Android 中，用户可以使用下拉刷新功能更新其屏幕上的数据。

Secure Web 10.8.15

- **Secure Web** 支持 **Android Enterprise**（以前称为 **Android for Work**）。可以在 Secure Mail 中使用 Android Enterprise 应用程序创建单独的工作配置文件。有关详细信息，请参阅Secure Mail 中的 Android Enterprise。
- **Secure Web for Android** 可以在桌面模式下呈现 **Web** 页面。从溢出菜单中，选择请求桌面网站。Secure Web 将显示该 Web 站点的桌面版本。

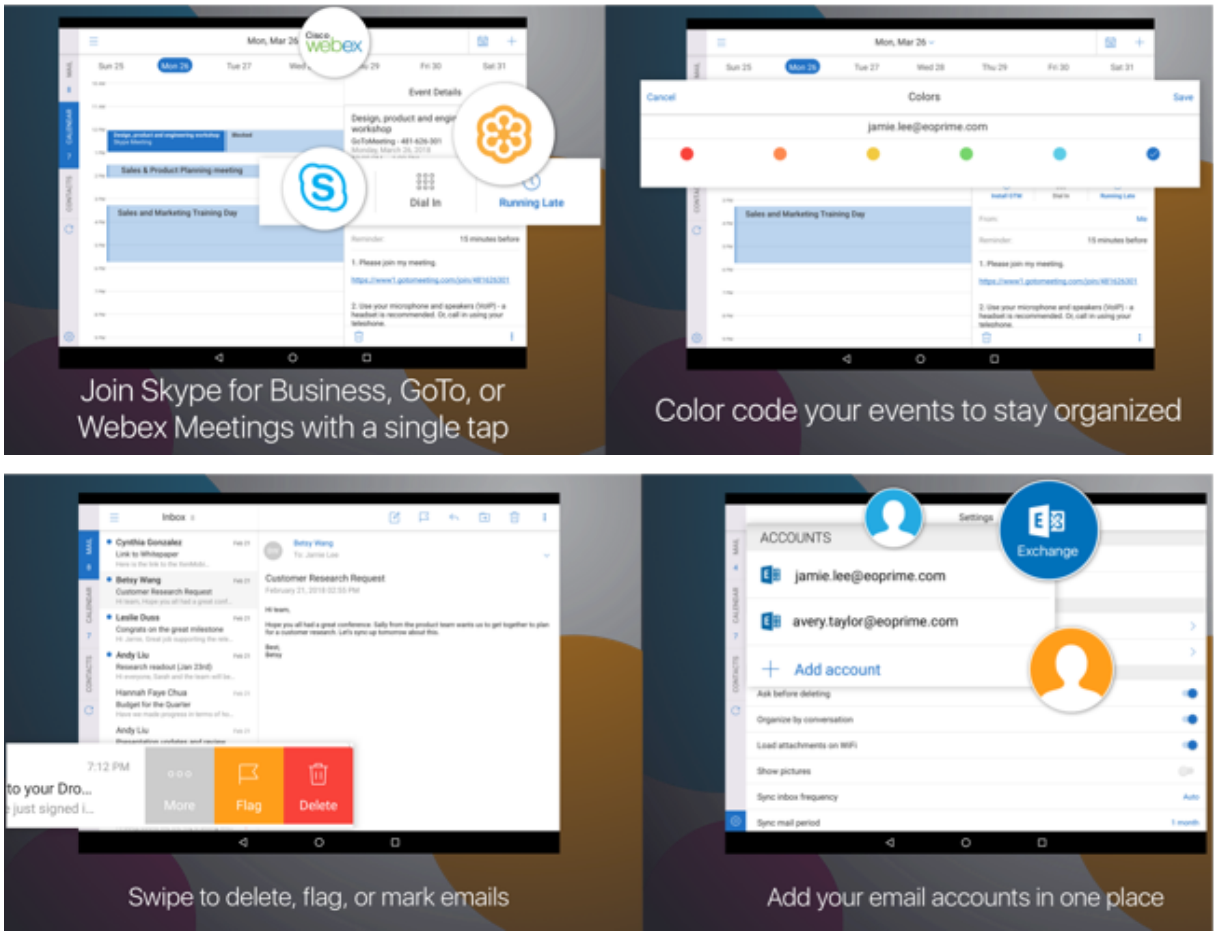
Secure Web 10.8.10

- **Secure Web for iOS** 可以在桌面模式下呈现 **Web** 页面。从汉堡菜单中，选择请求桌面网站，Secure Web 将显示 Web 站点的桌面版本。



Secure Web 10.8.5

适用于 **iOS** 和 **Android** 的 **Secure Mail** 和 **Secure Web** 修改了字体、颜色以及其他 **UI** 改进功能。此修改丰富了您的用户体验，同时与纵贯我们全套应用程序的 Citrix 品牌美学非常一致。



已知问题和已修复的问题

April 6, 2021

Citrix 支持从最后两个版本的移动生产力应用程序进行升级。

Secure Web 21.3.5

Secure Web for Android

本版本中没有已知问题或已修复的问题。

Secure Web 21.3.0

Secure Web for Android

本版本中没有已知问题或已修复的问题。

Secure Web 21.2.0

本版本中没有已知问题或已修复的问题。

较旧版本中的已知问题和已修复的问题

有关 Secure Web 的较旧版本中的已知问题和已修复的问题，请参阅较旧版本中的已知问题和已修复的问题。

集成和部署 Secure Web

March 26, 2021

要集成并交付 Secure Web，请按照以下常规步骤进行操作：

1. 要对内部网络启用 SSO，请配置 Citrix Gateway。

   对于 HTTP 流量，Citrix ADC 可以向 Citrix ADC 支持的所有代理身份验证类型提供 SSO。对于 HTTPS 流量，“Web 密码缓存”策略允许 Secure Web 进行身份验证并通过 MDX 提供对代理服务器的 SSO。MDX 仅支持基本身份验证、摘要式身份验证和 NTLM 代理身份验证。密码使用 MDX 缓存并存储在 Endpoint Management 共享保管库（用于存储敏感应用程序数据的安全存储区域）中。有关 Citrix Gateway 配置的详细信息，请参阅 Citrix Gateway。

2. 下载 Secure Web。
3. 确定如何配置与内部网络之间的用户连接。
4. 将 Secure Web 添加到 Endpoint Management 中（操作步骤与其他 MDX 应用程序相同），然后配置 MDX 策略。有关 Secure Web 的特定策略的详细信息，请参阅关于 Secure Web 策略。

配置用户连接

Secure Web 支持以下用户连接配置：

- 安全浏览：通过通道连接到内部网络的连接可以使用无客户端 VPN 的变体（称为“安全浏览”）。此配置是为首选 **VPN** 模式策略指定的默认配置。建议对需要单点登录 (SSO) 的连接使用安全浏览。
- 完整 **VPN** 通道：通过通道连接到内部网络的连接可以使用首选 **VPN** 模式策略配置的完整 VPN 通道。建议对通过客户端证书或端到端 SSL 与内部网络中的资源建立的连接使用完整 VPN 通道。完整 VPN 通道通过 TCP 处理任何协议，并且可以在 Windows 和 Mac 计算机以及 iOS 和 Android 设备上使用。

> 注意：
>
> MDX 封装技术计划于 2021 年 9 月达到生命周期结束 (EOL) 状态。要继续管理您的企业应用程序，必须合并 MAM SDK。
> 旧版 MDX 模式不支持完整 VPN 通道。

- 允许 **VPN** 模式切换策略允许用户根据需要在完整 VPN 通道模式与安全浏览模式之间自动切换。默认情况下，此策略设置为“关”。如果此策略设置为“开”，则将在备选模式下尝试重新处理由于无法在首选 VPN 模式下处理身份验证请求而失败的网络请求。例如，完整 VPN 通道模式（而非安全浏览模式）可以接受服务器对客户端证书的质询。同样，使用安全浏览模式时，通过 SSO 向 HTTP 身份验证质询提供服务的可能性更大。
- 使用 **PAC** 的完整 **VPN** 通道：可以对 iOS 和 Android 设备的完整 VPN 通道部署使用代理自动配置 (PAC) 文件。PAC 文件中包含的规则用于定义 Web 浏览器如何选择代理以访问指定 URL。PAC 文件规则可以指定对外部和内部站点的处理方式。Secure Web 解析 PAC 文件规则并将代理服务器信息发送到 Citrix Gateway。
- 使用 PAC 文件时，完整 VPN 通道的性能可以与安全浏览模式相媲美。有关 PAC 配置的详细信息，请参阅使用 PAC 的完整 VPN 通道。
- 反向拆分通道：在反向模式下，Intranet 应用程序的流量会绕过 VPN 通道，而其他流量均通过 VPN 通道。此策略可以用于记录所有非本地 LAN 流量。

反向拆分通道的配置步骤

要在 Citrix Gateway 上配置拆分通道反向模式，请执行以下操作：

1. 导航到策略 **>** 会话策略。
2. 选择 Secure Hub 策略，然后导航到客户端体验 **>** 拆分通道。
3. 选择反向。

反向拆分隧道模式排除列表 **MDX** 策略

在 Citrix Endpoint Management 内部使用“排除”范围配置反向拆分通道模式策略。该范围基于 DNS 后缀和 FQDN 的逗号分隔列表。此列表定义其流量必须通过设备的 LAN 发出且不会发送到 Citrix ADC 的 URL。

下表说明了 Secure Web 是否会根据配置和站点类型提示用户输入凭据：

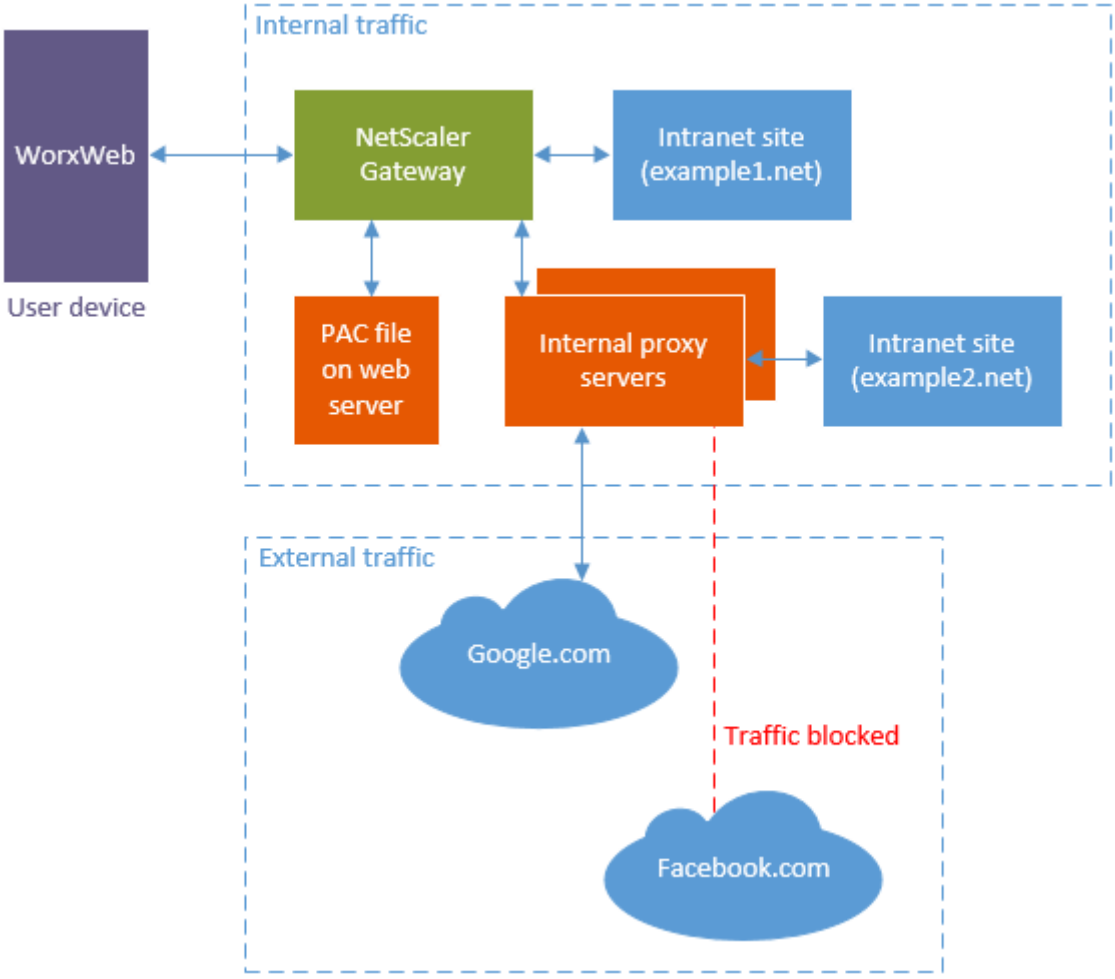
连接模式	站点类型	密码缓存	为 Citrix Gateway 配置的 SSO	在首次访问 Web 站点时，Secure Web 提示输入凭据	在之后访问 Web 站点时，Secure Web 提示输入凭据	在更改密码后，Secure Web 提示输入凭据
安全浏览	HTTP	否	是	否	否	否
安全浏览	HTTPS	否	是	否	否	否
完整 VPN	HTTP	否	是	否	否	否
完整 VPN	HTTPS	是，如果 Secure Web MDX 策略“启用 Web 密码缓存”设置为“开”。	否	是；在 Secure Web 中缓存凭据时需要。	否	是

使用 **PAC** 的完整 **VPN** 通道

> 重要：
>
> 如果为 Secure Web 配置了 PAC 文件，并且为代理操作配置了 Citrix ADC，Secure Web 将超时。使用“使用 PAC 的完整 VPN 通道”之前，请删除为代理配置的 Citrix Gateway 流量策略。

为 Secure Web 配置使用 PAC 文件或代理服务器的完整 VPN 通道时，Secure Web 通过 Citrix Gateway 将所有流量发送到代理。Citrix Gateway 随后根据代理配置规则路由流量。在此配置中，Citrix Gateway 无法识别 PAC 文件或代理服务器。该通信流与不使用 PAC 文件的完整 VPN 通道的通信流相同。

下图显示了 Secure Web 用户导航到某个 Web 站点时的通信流：



在该示例中，流量规则指定以下内容：

- Citrix Gateway 直接连接到 Intranet 站点 `example1.net`。
- 流向 Intranet 站点 `example2.net` 的流量通过内部代理服务器代理。
- 外部流量通过内部代理服务器代理。代理规则阻止流向以下站点的外部流量 `Facebook.com`.

配置使用 **PAC** 的完整 **VPN** 通道

1. 验证并测试 PAC 文件。

   > 注意：
   >
   > 有关创建和使用 PAC 文件的详细信息，请参阅 *findproxyforurl.com/*。

   使用 PAC 验证工具（例如 Pacparser）验证 PAC 文件。读取 PAC 文件时，请确保 Pacparser 结果与您的预期相同。如果 PAC 文件包含语法错误，移动设备将在无提示的情况下忽略 PAC 文件。（PAC 文件仅存储在移动设备上的内存中。）

   PAC 文件按照从上到下的顺序处理，有规则与当前查询匹配时停止处理。

   请在将 PAC 文件 URL 输入 Endpoint Management 的 **PAC/**代理字段之前，在 Web 浏览器中测试此 URL。确保计算机可以访问 PAC 文件所在的网络。

   ```
   https://webserver.local/GenericPAC.pac
   https://webserver.local/GenericPAC.pac
   ```

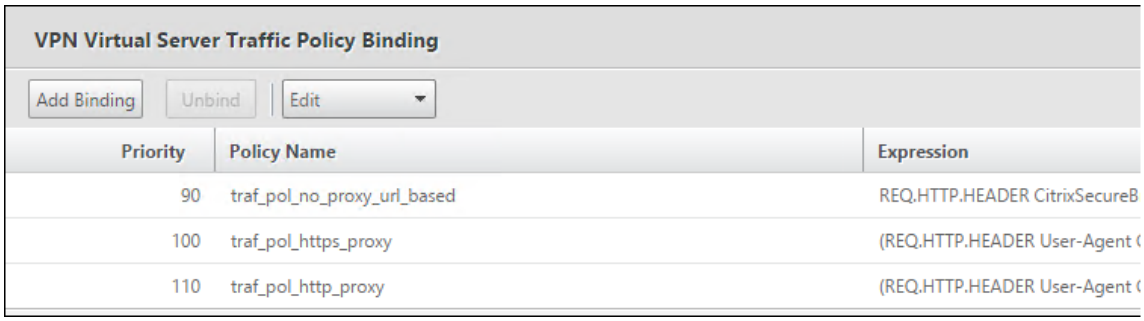
   经过测试的 PAC 扩展名为.txt 或.pac。

   PAC 文件必须在 Web 浏览器中显示其内容。

   > 重要：
   >
   > 每次更新用于 Secure Web 的 PAC 文件时，都会通知用户必须关闭并重新打开 Secure Web。

2. 配置 Citrix Gateway：

   - 禁用 Citrix Gateway 拆分通道。如果启用了拆分通道并且配置了 PAC 文件，PAC 文件规则将覆盖 Citrix ADC 拆分通道规则。代理不会覆盖 Citrix ADC 拆分通道规则。
   - 删除为代理配置的 Citrix Gateway 流量策略。此步骤是 Secure Web 正常运行必需的。下图显示了要删除的策略规则示例。

3. 配置 Secure Web 策略：

   - 将“首选 VPN 模式”策略设置为完整 **VPN** 通道。
   - 将“允许 VPN 模式切换”策略设置为关。
   - 配置 PAC 文件 URL 或代理服务器策略。Secure Web 支持 HTTP 和 HTTPS 以及默认端口和非默认端口。对于 HTTPS，如果证书为自签名证书或者不受信任，则必须在设备上安装根证书颁发机构。

请务必在配置策略之前，先在 Web 浏览器中测试 URL 或代理服务器地址。

PAC 文件 URL 示例：

```
http[s]://example.com/proxy.pac
http[s]://10.10.0.100/proxy.txt
```

示例代理服务器（需要配置端口）：

```
myhost.example.com:port
```

```
10.10.0.100:port
```

> 注意：
>
> 如果配置了 PAC 文件或代理服务器，请不要在 Wi-Fi 的系统代理设置中配置 PAC。

- 将“启用 Web 密码缓存”策略设置为开。Web 密码缓存处理 HTTPS 站点的 SSO。

  如果代理支持相同的身份验证基础结构，Citrix ADC 可以对内部代理执行 SSO。

PAC 文件支持的限制

Secure Web 不支持：

- 从一台代理服务器故障转移到另一台代理服务器。PAC 文件评估可以返回某个主机名对应的多台代理服务器。Secure Web 仅使用返回的第一个代理服务器。
- PAC 文件中的协议（例如 FTP 和 gopher）。
- PAC 文件中的 SOCKS 代理服务器。
- Web 代理自动发现协议 (Web Proxy AutoDiscovery Protocol, WPAD)。

Secure Web 忽略 PAC 文件功能警报，以使 Secure Web 能够解析不包括这些调用的 PAC 文件。

Secure Web 策略

添加 Secure Web 时，请注意 Secure Web 特定的这些 MDX 策略。对于所有受支持的移动设备：

允许或阻止的 **Web** 站点

Secure Web 通常不过滤 Web 链接。您可以使用此策略配置特定的允许或阻止站点的列表。可以对 URL 模式进行配置，以限制浏览器可以打开的 Web 站点，其格式为逗号分隔的列表。加号 (+) 或减号 (-) 作为前缀添加到列表中的每种模式前面。浏览器按列出顺序将 URL 与模式进行比较，直至找到一个匹配项。找到匹配项后，前缀指示操作按如下所示执行：

- 减号 (-) 前缀指示浏览器阻止打开 URL。在这种情况下，该 URL 被视为 Web 服务器地址无法解析。
- 加号 (+) 前缀允许按常规处理 URL。
- 如果随模式提供 + 或 -，则会假定提供 +（允许）。

- 如果 URL 与列表中的任何模式都不匹配，则允许打开该 URL。

要阻止所有其他 URL，请在列表结尾添加减号后跟星号 (-*)。例如：

- 策略值 +http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-* 允许在 mycorp.com 域中使用 HTTP URL，但在其他位置阻止这些 URL，允许在任何位置使用 HTTPS 和 FTP URL，但阻止所有其他 URL。
- 策略值 +http://*.training.lab/*,+https://*.training.lab/*,-* 允许用户通过 HTTP 或 HTTPS 打开 Training.lab 域 (Intranet) 中的任何站点。但该策略值不允许用户打开公用 URL，例如 Facebook、Google、Hotmail 等，无论协议为何都是如此。

默认值为空（允许打开所有 URL）。

阻止弹出窗口

弹出窗口是在未经您允许的情况下 Web 站点打开的新选项卡。此策略确定 Secure Web 是否允许弹出窗口。如果设为“开”，Secure Web 将阻止 Web 站点打开弹出窗口。默认值为关。

预加载的书签

为 Secure Web 浏览器定义一组预加载的书签。此策略是一组用逗号分隔的元组列表，包括文件夹名称、友好名称和 Web 地址。每个元组必须采用 folder, name, url 格式，其中 folder 和 name 可能会有选择地用双引号 (“) 引起。

例如，策略值 ,”Mycorp, Inc. home page”,https://www.mycorp.com, ”MyCorp Links”,Account logon,https://www.mycorp.com/Accounts ”MyCorp Links/Investor Relations”,”Contact us”,https://www.mycorp.com/IR/Contactus.aspx 定义了三个书签。第一个为主链接（无文件夹名称），标题为 “Mycorp, Inc. home page”。第二个链接放置在标题为 “MyCorp Links”、标签为 “Account logon” 的文件夹中。第三个链接放置在 “MyCorp Links” 文件夹的 “Investor Relations” 子文件夹中，显示为 “Contact us”。

默认值为空。

主页 **URL**

定义 Secure Web 在启动时加载的 Web 站点。默认值为空（默认启动页面）。

仅限受支持的 Android 和 iOS 设备：

浏览器用户界面

规定 Secure Web 的浏览器用户界面控件的行为和可见性。通常情况下，所有浏览控件都可用。这些控件包括前进、后退、地址栏和刷新/停止控件。可以配置此策略以限制这些控件的使用和可见性。默认值为所有控件都可见。

选项：

- 所有控件都可见。所有控件都可见，并且不限制用户使用。
- 只读地址栏。所有控件都可见，但用户无法编辑浏览器地址字段。
- 隐藏地址栏。隐藏地址栏，但不隐藏其他控件。
- 隐藏所有控件。禁止显示整个工具栏以提供无框浏览体验。

启用 **Web** 密码缓存

当 Secure Web 用户为访问或请求 Web 资源输入凭据时，此策略确定 Secure Web 是否以无提示方式在设备上缓存密码。此策略适用于在身份验证对话框中输入的密码，不适用于在 Web 表单中输入的密码。

如果设置为开，Secure Web 将缓存用户在请求 Web 资源时输入的所有密码。如果设置为关，Secure Web 将不缓存密码并删除已缓存的现有密码。默认值为关。

仅当您同时将“首选 VPN”策略设置为此应用程序的完整 VPN 通道时才能启用此策略。

代理服务器

在安全浏览模式下使用时，还可以为 Secure Web 配置代理服务器。有关详细信息，请参阅此 博客文章。

DNS 后缀

在 Android 上，如果未配置 DNS 后缀，VPN 可能会失败。有关配置 DNS 后缀的详细信息，请参阅支持使用面向 Android 设备的 DNS 后缀进行 DNS 查询。

准备用于 **Secure Web** 的 **Intranet** 站点

此部分面向 Web 站点开发人员，他们需要准备用于 Secure Web for Android 和 Secure Web for iOS 的 Intranet 站点。旨在用于桌面浏览器的 Intranet 站点需要更改才能在 Android 和 iOS 设备上正常使用。

Secure Web 依靠 Android WebView 和 iOS WkWebView 来提供 Web 技术支持。Secure Web 支持的一些 Web 技术包括：

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSocket（仅在非限制模式下）

Secure Web 不支持的一些 Web 技术包括：

- Flash
- Java

下表显示了 Secure Web 支持的 HTML 呈现功能和技术。X 表示相应功能适用于某个平台、浏览器和组件组合。

技术	Secure Web for iOS	Secure Web for Android
JavaScript 引擎	JavaScriptCore	V8
本地存储	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
导航计时 API		X
资源计时 API		X

技术在不同设备上作用方式相同；但 Secure Web 对不同的设备返回不同的用户代理字符串。要确定用于 Secure Web 的浏览器版本，可以查看其用户代理字符串。从 Secure Web 导航到 https://whatsmyuseragent.com/。

Intranet 站点故障排除

要解决在 Secure Web 中查看 Intranet 站点时遇到的呈现问题，请将 Web 站点在 Secure Web 上的呈现情况与在兼容的第三方浏览器中的呈现情况进行比较。

对于 iOS，用于测试的兼容第三方浏览器为 Chrome 和 Dolphin。

对于 Android，用于测试的兼容第三方浏览器为 Dolphin。

> 注意：
>
> Chrome 是 Android 上的本机浏览器。请勿将其用于比较。

在 iOS 中，请确保浏览器支持设备级 VPN。可以在设备上的设置 **> VPN >** 添加 **VPN** 配置中配置此支持。

还可以使用应用商店中提供的 VPN 客户端应用程序，例如 Citrix VPN、Cisco AnyConnect 或 Pulse Secure。

- 如果 Web 页面在两个浏览器上的呈现情况相同，则问题源于您的 Web 站点。请更新此站点，并确保它可以很好地适用于操作系统。
- 如果 Web 页面上的问题仅出现在 Secure Web 中，请联系 Citrix 技术支持，以打开一个支持票证。请提供您的故障排除步骤，包括测试的浏览器和操作系统类型。如果 Secure Web for iOS 存在呈现问题，请按以下步骤所述将页面的 Web 存档包括在内。这样可帮助 Citrix 更加快速地解决该问题。

验证 **SSL** 连接

确保 SSL 证书链已正确配置。可以使用 SSL 证书检查器检查移动设备上未链接或未安装的缺失根 CA 或中间 CA。

许多服务器证书由多个分层证书颁发机构 (CA) 签名，这意味着证书形成了一个链。您必须链接这些证书。有关安装或链接证书的信息，请参阅 安装、链接和更新证书。

创建 **Web** 存档文件

通过在 macOS 10.9 或更高版本上使用 Safari，可以将 Web 页面另存为 Web 存档文件（又称为“阅读列表”）。Web 存档文件包括所有链接的文件，例如图像、CSS 和 JavaScript。

1. 在 Safari 中，清空阅读列表文件夹：在 **Finder** 中，单击菜单栏中的前往菜单，选择前往文件夹，键入路径名称 ~/Library/Safari/ReadingListArchives/。现在将删除该位置中的所有文件夹。
2. 在菜单栏中，转到 **Safari >** 偏好设置 **>** 高级并启用“在菜单栏中显示 **“**开发**”** 菜单”。
3. 在菜单栏中，转到开发 **>** 用户代理并输入 Secure Web 用户代理：（Mozilla/5.0（iPad，CPU OS 8_3，例如 macOS）AppleWebKit/600.1.4（KHTML，例如 Gecko）Mobile/12F69 Secure Web/10.1.0 （内部版本 1.4.0）Safari/8536.25)。
4. 在 Safari 中，打开要另存为阅读列表（Web 存档文件）的 Web 站点。
5. 在菜单栏中，转到书签 **>** 添加到阅读列表。此步骤可能需要几分钟时间。存档在后台进行。
6. 找到存档的阅读列表：在菜单栏中，转到查看 **>** 显示阅读列表边栏。
7. 验证存档文件：
   - 关闭与 Mac 之间的网络连接。
   - 打开阅读列表中的 Web 站点。

     该 Web 站点完全呈现。
8. 压缩存档文件：在 **Finder** 中，单击菜单栏中的前往菜单，选择前往文件夹，然后键入路径名称 ~/Library/Safari/ReadingListArchives/。然后压缩使用随机十六进制字符串作为文件名的文件夹。打开支持票证时，可以将此文件发送给 Citrix 技术支持。

Secure Web 功能

Secure Web 利用移动数据交换技术创建专用 VPN 通道，以便用户能够访问内部和外部 Web 站点以及所有其他 Web 站点。这些站点包括受贵公司的策略保护的环境中包含敏感信息的站点。

Secure Web 与 Secure Mail 和 Citrix Files 的集成在安全的 Endpoint Management 容器中提供无缝的用户体验。下面是集成功能的几个示例：

- 用户轻按 **Mailto** 链接时，将在 Secure Mail 中打开一封新电子邮件，不需要进一步进行身份验证。

- 允许链接在 **Secure Web** 中打开，确保数据安全。使用 Secure Web for iOS 和 Secure Web for Android 时，专用 VPN 通道允许用户安全地访问包含敏感信息的站点。用户可以单击来自 Secure Mail、来自 Secure Web 内部或者来自第三方应用程序的链接。该链接将在 Secure Web 中打开，数据被安全地包含在内。用户可以在 Secure Web 中打开具有 ctxmobilebrowser 方案的内部链接。这样，Secure Web 会将 `ctxmobilebrowser://` 前缀转换为 `http://`。要打开 HTTPS 链接，Secure Web 会将 `ctxmobilebrowsers://` 转换为 `https://`。

此功能取决于名为入站文档交换的应用程序交互 MDX 策略。默认情况下，此策略设置为不受限制。此设置允许在 Secure Web 中打开 URL。您可以更改策略设置，以便只有允许列表中包含的应用程序能够与 Secure Web 通信。

- 当用户单击电子邮件中的 Intranet 链接时，Secure Web 会转到该站点而无需进行额外的身份验证。
- 用户可以将其在 Secure Web 中从 Web 下载的文件上载到 Citrix Files。

Secure Web 用户还可以执行以下操作：

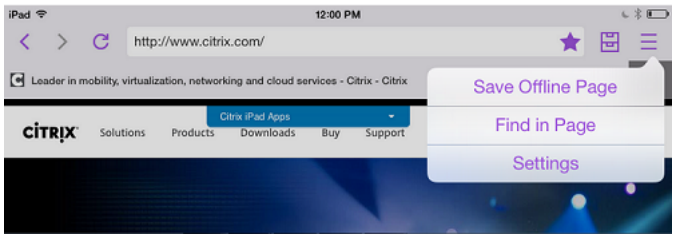
- 阻止弹出窗口。

  > 注意：
  >
  > Secure Web 的大多数内存用于呈现弹出窗口，因此，通常可通过在“设置”中阻止弹出窗口来提高性能。

- 为收藏的站点添加书签。
- 下载文件。
- 脱机保存页面。
- 自动保存密码。
- 清除缓存/历史记录/cookie。
- 禁用 Cookie 和 HTML5 本地存储。
- 与其他用户安全地共享设备。
- 在地址栏中搜索。
- 允许他们在 Secure Web 中运行的 Web 应用程序访问其位置。
- 导出和导入设置。
- 直接在 Citrix Files 中打开文件，而不必下载文件。要启用此功能，请在 Endpoint Management 中将 **ctx-sf:** 添加到“允许的 URL ”策略。
- 在 iOS 中，请使用三维触控操作来打开新选项卡，并直接从主屏幕访问脱机页面、收藏的站点和下载内容。
- 在 iOS 中，下载任意大小的文件并在 Citrix Files 或其他应用程序中打开。

  > 注意：
  >
  > 将 Secure Web 置于后台将导致下载停止。

- 使用在网页中查找在当前页面视图中搜索词语。



Secure Web 也支持动态文本，因此可显示用户在其设备上设置的字体。

iOS 数据保护

August 6, 2019

必须满足澳大利亚信号局 (ASD) 数据保护要求的企业可以对 Secure Mail 和 Secure Web 使用启用 **iOS** 数据保护策略。默认情况下，策略设置为关。

对于 Secure Web，启用 **iOS** 数据保护设置为开时，Secure Web 为沙盒中的所有文件使用 A 类保护级别。有关 Secure Mail 数据保护的详细信息，请参阅澳大利亚信号局 (Australian Signals Directorate) 数据保护。如果启用此策略，将使用最高数据保护类，因此无需再指定最低数据保护类策略。

要更改启用 **iOS** 数据保护策略，请执行以下操作：

1. 使用 Endpoint Management 控制台将 Secure Web 和 Secure Mail MDX 文件加载到 Endpoint Management：对于新应用程序，请导航到配置 **>** 应用程序 **>** 添加，然后单击 **MDX**。有关升级的信息，请参阅升级 MDX 或企业应用程序。
2. 使用 Endpoint Management 控制台将 MDX 文件加载到 Endpoint Management：对于新应用程序，请导航到配置 **>** 应用程序 **>** 添加，然后单击 **MDX**。有关升级的信息，请参阅添加应用程序。
3. 对于 Secure Mail，请浏览到应用程序设置，找到启用 **iOS** 数据保护策略，然后将其设置为开。启用此策略不会影响运行较低操作系统版本的设备。
4. 对于 Secure Web，请浏览到应用程序设置，找到启用 **iOS** 数据保护策略，然后将其设置为开。启用此策略不会影响运行较低操作系统版本的设备。
5. 正常配置应用程序策略并保存设置，以将应用程序部署到 Endpoint Management 应用商店。

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