

移动生产力应用程序

Contents

移动生产力应用程序发布时间表	21
关于 Secure Mail 和 Secure Web 分阶段发布流程	21
功能标志管理的先决条件	21
移动生产力应用程序支持	22
支持的操作系统	22
其他注意事项和限制	23
安全邮件	23
安全 Web	24
QuickEdit	24
适用于 思杰端点管理 的 思杰内容协作™	24
ShareConnect	24
思杰安全备忘录 和 思杰安全任务	24
管理员任务和注意事项	25
功能标志管理	25
启用流向以下 URL 的流量	25
按域创建允许列表	25
在允许列表中列出 IP 地址	25
LaunchDarkly 系统要求	26
支持的应用商店	26
启用公共应用商店分发	26
Apple 推送通知	27
公共应用商店常见问题	27
安卓	28
iOS	28
适用于移动生产力应用的 MDX 策略	30
适用于 Android 的 Secure Mail 中的双模式	31

先决条件	31
限制	32
用户连接到内部网络	33
网络访问限制	33
Endpoint Management 客户端属性	33
用户密码缓存	33
不活动计时器	34
Citrix PIN 身份验证	34
指纹或触控 ID 身份验证	34
指纹身份验证要求	34
配置指纹身份验证	35
谷歌分析	35
禁用谷歌分析	35
MDX 移动生产力应用程序策略概览	36
身份验证	36
设备密码	36
应用程序密码	36
在线会话所需宽限期（分钟）	36
最长离线时间	36
备用 Citrix 网关	37
设备安全性	37
阻止越狱或已root	37
要求设备锁定	37
网络要求	37
要求 Wi-Fi	37
允许的Wi-Fi网络	38
杂项访问	38
应用程序更新宽限期（小时）	38

禁用强制升级	38
锁定后擦除应用数据	38
活动轮询周期（分钟）	38
加密	39
加密类型	39
不合规设备行为	39
启用 MDX 加密	39
加密密钥	39
私有文件加密	40
私有文件加密排除项	40
公共文件的访问限制	40
公共文件加密	40
公共文件加密排除项	40
公共文件迁移	40
启用加密	41
数据库加密排除项	41
文件加密排除项	41
应用交互	41
安全组	41
剪切和复制	42
粘贴	42
文档交换（在...中打开）	42
从筛选中排除的 URL 域	42
允许的安全 Web 域	42
连接安全级别	42
入站文档交换 (Open In)	43
受限的“打开方式”例外列表	43
应用程序 URL 方案	43

允许的 URL	43
显式注销通知	43
应用交互（出站 URL）	44
从 URL 筛选中排除的域	44
允许的 URL	44
允许的安全 Web 域	44
应用程序限制	44
阻止相机	44
阻止图库	44
阻止照片库	44
阻止麦克风录音	45
阻止听写	45
阻止位置服务	45
阻止短信撰写	45
阻止屏幕捕获	45
阻止设备传感器	45
阻止 NFC	46
阻止 iCloud	46
阻止查找	46
阻止文件备份	46
阻止 AirPrint	46
阻止打印	46
阻止 AirDrop	46
阻止文件附件	47
阻止电子邮件撰写	47
阻止 Facebook 和 Twitter API	47
模糊屏幕内容	47
阻止第三方键盘	47

阻止应用日志	47
启用 ShareFile	48
启用从文件附加	48
应用网络访问	48
网络访问	48
需要微型 VPN 会话	48
需要微型 VPN 会话的宽限期（分钟）	48
排除列表	48
阻止本地主机连接	49
证书标签	49
应用日志	49
默认日志输出	49
默认日志级别	49
最大日志文件数	49
最大日志文件大小	49
重定向应用日志	50
加密日志	50
应用地理围栏	50
中心点经度	50
中心点纬度	50
半径	50
应用程序设置	51
安全邮件 Exchange 服务器	51
Secure Mail 用户域	51
后台网络服务	51
后台服务票证过期	51
后台网络服务网关	52
导出联系人	52

要导出的联系人字段	52
接受所有 SSL 证书	52
控制锁定屏幕通知	52
使用安全连接	52
默认电子邮件通知	53
默认同步间隔	53
邮件搜索限制	53
最大同步间隔	53
启用周数	53
启用通过 Wi-Fi 下载附件	54
允许离线文档	54
信息权限管理	54
电子邮件分类	54
电子邮件分类标记	54
电子邮件分类命名空间	54
电子邮件分类版本	54
默认电子邮件分类	55
启用草稿电子邮件自动保存	55
启用 iOS 数据保护	55
推送通知 EWS 主机名	55
推送通知	55
推送通知区域	55
首次启动 Secure Mail 时启用 S/MIME	56
初始身份验证机制	56
初始身份验证凭据	56
启用周数	56
日历 Web 和音频选项	56
S/MIME 公共证书源	56

LDAP 服务器地址	56
LDAP 基本 DN	57
匿名访问 LDAP	57
允许的电子邮件域	57
身份验证失败时尝试用户名迁移	57
报告网络钓鱼邮件地址	57
报告网络钓鱼机制	57
Skype for Business 会议域	58
导出日历	58
启用 Slack	58
Slack 工作区名称	58
来电显示	58
分析	59
启用 谷歌分析	59
Google Analytics 详细程度	59
报告	59
Citrix 报告	59
上传令牌	59
仅通过 Wi-Fi 发送报告	59
报告文件缓存最大值	60
Office 365 的 OAuth 支持	60
对 Office 365 使用新式身份验证	60
Office 365 身份验证机制	60
受信任的 Exchange Online 主机名	60
受信任的 AD FS 主机名	60
用于现代身份验证的自定义用户代理	60
邮件重定向	61
邮件重定向	61

Slack 集成	61
启用 Slack	61
Slack 工作区名称	61
适用于 Android 移动生产力应用程序的 MDX 策略	61
身份验证	61
应用程序密码	61
最长脱机时间（小时）	62
替代的 Citrix Gateway	62
设备安全性	62
阻止越狱或已获得 root 权限	62
要求设备加密	62
要求设备锁定	63
网络要求	63
要求 Wi-Fi	63
允许的 Wi-Fi 网络	63
杂项访问	63
应用程序更新宽限期（小时）	63
禁用强制升级	64
锁定后擦除应用程序数据	64
活动轮询周期（分钟）	64
加密	64
加密类型	64
不合规设备行为	65
加密密钥	65
私有文件加密	65
私有文件加密排除项	65
公共文件的访问限制	66
公共文件加密	66

公共文件加密排除项	66
公共文件迁移	67
应用程序交互	67
安全组	67
剪切和复制	67
粘贴	67
文档交换 (打开方式)	67
从筛选中排除的 URL 域	68
允许的安全 Web 域	68
受限打开方式例外列表	68
入站文档交换 (打开方式)	68
入站文档交换白名单	69
连接安全级别	69
应用限制	69
阻止相机	69
阻止图库	69
阻止麦克风录音	69
阻止位置服务	70
阻止短信撰写	70
阻止屏幕捕获	70
阻止设备传感器	70
阻止 NFC	70
阻止应用日志	70
阻止打印	70
启用 ShareFile	70
应用网络访问	71
网络访问	71
需要微型 VPN 会话	71

排除列表	71
阻止本地主机连接	71
证书标签	72
应用日志	72
默认日志输出	72
默认日志级别	72
最大日志文件数	72
最大日志文件大小	72
重定向应用日志	72
加密日志	73
应用程序地理围栏	73
中心点经度	73
中心点纬度	73
半径	73
分析	73
Google Analytics 详细信息	73
应用设置	74
安全邮件 Exchange 服务器	74
Secure Mail 用户域	74
后台网络服务	74
后台服务票证过期	74
后台网络服务网关	74
导出联系人	75
要导出的联系人字段	75
接受所有 SSL 证书	75
使用安全连接	75
信息权限管理	75
控制锁定屏幕通知	75

默认同步间隔	75
启用通过 Wi-Fi 下载附件	76
允许脱机文档	76
启用电子邮件草稿自动保存	76
初始身份验证机制	76
初始身份验证凭据	76
启用周数	76
电子邮件分类	76
电子邮件分类标记	76
电子邮件分类命名空间	76
电子邮件分类版本	77
默认电子邮件分类	77
邮件搜索限制	77
最大同步间隔	77
日历网络和音频选项	77
S/MIME 公共证书源	77
LDAP 服务器地址	78
LDAP 基本 DN	78
匿名访问 LDAP	78
允许的电子邮件域	78
推送通知	78
推送通知 EWS 主机名	78
推送通知区域	78
身份验证失败时尝试用户名迁移	78
报告网络钓鱼邮件地址	78
报告网络钓鱼机制	78
Skype for Business 会议域	79
导出日历	79

对 Office 365 的 OAuth 支持	80
对 O365 使用新式身份验证	80
受信任的 Exchange Online 主机名	80
受信任的 AD FS 主机名	80
用于现代身份验证的自定义用户代理	80
Slack 集成	80
启用 Slack	80
Slack 工作区名称	80
适用于 iOS 移动生产力应用的 MDX 策略	81
身份验证	81
设备密码	81
应用密码	81
最长脱机时间 (小时)	81
备用思杰网关	81
设备安全性	82
阻止越狱或 Root 设备	82
网络要求	82
需要 Wi-Fi	82
允许的 Wi-Fi 网络	82
杂项访问	82
禁用强制升级	82
应用程序更新宽限期 (小时)	82
锁定后擦除应用程序数据	83
活动轮询周期 (分钟)	83
加密	83
加密类型	83
不合规设备行为	83
启用 MDX 加密	84

数据库加密排除项	84
文件加密排除项	84
应用交互	85
剪切和复制	85
粘贴	85
文档交换（在以下位置打开）	85
受限的“打开方式”例外列表	85
连接安全级别	85
入站文档交换(打开方式)	85
应用 URL 方案	86
应用交互（出站 URL）	87
从 URL 筛选中排除的域	87
允许的 URL	87
允许的安全 Web 域	89
应用程序限制	89
阻止摄像头	89
阻止照片库	89
阻止麦克风录音	89
阻止听写	90
阻止定位服务	90
阻止短信撰写	90
阻止电子邮件撰写	90
阻止 iCloud	90
阻止查找	90
阻止文件备份	90
阻止隔空打印	90
阻止隔空投送	90
阻止文件附件	91

阻止 Facebook 和 Twitter API	91
模糊屏幕内容	91
阻止第三方键盘 (仅限 iOS 11 及更高版本)	91
阻止应用程序日志	91
启用 ShareFile	91
启用从文件附加	91
应用程序网络访问	91
网络访问	91
需要微型 VPN 会话	92
需要微型 VPN 会话的宽限期 (分钟)	92
证书标签	92
排除列表	92
应用日志	92
默认日志输出	92
默认日志级别	93
最大日志文件数	93
最大日志文件大小	93
应用程序地理围栏	93
中心点经度	93
中心点纬度	93
半径	94
启用谷歌分析	94
分析	94
Google Analytics 详细程度	94
报告	94
Citrix 报告	94
上传令牌	94
仅通过 Wi-Fi 发送报告	94

报告文件缓存最大值	94
应用程序交互	95
显式注销通知	95
应用程序设置	95
安全邮件 Exchange 服务器	95
Secure Mail 用户域	95
后台网络服务	95
后台服务票证过期	95
后台网络服务网关	96
导出联系人	96
要导出的联系人字段	96
接受所有 SSL 证书	96
控制锁定屏幕通知	96
默认电子邮件通知	97
默认同步间隔	97
邮件搜索限制	97
最大同步间隔	97
启用周数	97
启用通过 Wi-Fi 下载附件	97
允许脱机文档	97
信息权限管理	97
电子邮件分类	98
电子邮件分类标记	98
电子邮件分类命名空间	98
电子邮件分类版本	98
默认电子邮件分类	98
启用电子邮件草稿自动保存	98
初始身份验证机制	98

初始身份验证凭据	99
启用用户名的自动填充	99
启用 iOS 数据保护	99
推送通知 EWS 主机名	99
推送通知	99
推送通知区域	99
S/MIME 公共证书源	99
首次启动 Secure Mail 时启用 S/MIME	100
日历 Web 和音频选项	100
S/MIME 公共证书源	100
LDAP 服务器地址	100
LDAP 基本 DN	100
匿名访问 LDAP	100
允许的电子邮件域	100
尝试在身份验证失败时迁移用户名	101
报告网络钓鱼邮件地址	101
报告网络钓鱼机制	101
Skype for Business 会议域	101
导出日历	102
来电显示	102
Office 365 的 OAuth 支持	102
Office 365 身份验证机制	102
受信任的 Exchange Online 主机名	102
受信任的 AD FS 主机名	103
邮件重定向	103
邮件重定向	103
Slack 集成	103
启用 Slack	103

Slack 工作区名称	103
按平台划分的功能	104
Citrix 安全中心™	104
思杰安全邮件	105
Citrix 安全 Web™	115
功能标志管理	117
IP 地址	117
系统要求	117
Citrix 安全中心™	119
管理 Secure Hub	119
Citrix 个人识别码	119
证书锁定	120
为 Secure Hub 配置证书 + 一次性密码身份验证	121
适用于 Android 设备的 ADS 连接端口要求	125
Secure Hub 功能	127
Secure Mail 概述	130
思杰安全 Web™	132
集成和交付 Secure Web	132
配置用户连接	132
Secure Web 策略	134
允许或阻止的网站	134
阻止弹出窗口	134
预加载书签	134
主页 URL	135
浏览器用户界面	135
选项	135
启用 Web 密码缓存	135
代理服务器	136

DNS 后缀	136
为 Secure Web 准备内部网站点	136
内网站点故障排除	137
创建网页存档文件	138
Secure Web 功能	138
Citrix Content Collaboration™ 适用于 端点管理	141
适用于 Endpoint Management 的 Citrix Content Collaboration 客户端与 Citrix Files 移动客户端有何不同	142
用户访问	142
SSO	142
微型 VPN	142
双因素身份验证	143
文件夹权限	143
文档访问保护	143
Citrix Files 帐户访问	143
设备策略	144
MDX 策略	144
数据加密	144
可用性	144
集成和交付适用于 Endpoint Management 客户端的 Citrix Content Collaboration	144
在 Endpoint Management 中配置 Citrix Files 帐户信息以实现 SSO	146
将适用于 Endpoint Management 的 Citrix 内容协作客户端添加到 Endpoint Management	146
必备条件	146
验证思杰内容协作端点管理客户端	147
生命周期结束和已弃用应用	149
允许与 Office 365 应用程序进行安全交互	151
在 iOS 中启用 Office 365	151
在 Android 中启用 Office 365	152

支持的文件格式	152
移动生产力应用程序文档历史记录	153

移动生产力应用程序发布时间表

Citrix® 移动生产力应用程序每两周发布一次。尽管确切日期可能会有所变动，但了解此发布节奏可以帮助您提前规划。我们还希望让您更轻松的管理应用程序部署和更新。

关于 Secure Mail 和 Secure Web 分阶段发布流程

当 Secure Mail 和 Secure Web 的新版本可用时，将按以下分阶段方式推出：

- 对于 iOS 和 Android 用户，Secure Mail 和 Secure Web 更新将在 App Store 和 Google Play 商店中提供，并在一周（七天）内逐步覆盖越来越多的用户。
- iOS 版 Secure Mail 和 Secure Web 的新下载用户将在本周内获得新版本。Android 版 Secure Mail 和 Secure Web 的新下载用户将在一周内运行旧版本，直到新版本发布覆盖所有用户的 100%。
- 对于用户而言，某些功能将分阶段逐步发布。

功能标志管理的先决条件

如果生产环境中 Secure Hub 或 Secure Mail 出现问题，我们可以在应用程序代码中禁用受影响的功能。为此，我们使用功能标志和名为 LaunchDarkly 的第三方服务。您无需进行任何配置即可启用指向 LaunchDarkly 的流量，除非您有防火墙或代理阻止出站流量。在这种情况下，您需要根据策略要求，通过特定的 URL 或 IP 地址启用指向 LaunchDarkly 的流量。有关自移动生产力应用程序 10.6.15 版以来 MDX 中对隧道排除域的支持的详细信息，请参阅 [MDX Toolkit 文档](#)。有关功能标志和 LaunchDarkly 的常见问题解答，请参阅此 [支持知识中心文章](#)。

注意： 有关即将淘汰的 Citrix Endpoint Management 功能的提前通知，请参阅 [弃用](#)。

移动生产力应用程序支持

已启用自动更新的用户将从应用商店接收最新版本。移动生产力应用程序的最新版本如下：

- 23.10.0 (适用于 Android 的 Secure Web)
- 23.9.0 (适用于 iOS 的 Secure Mail 和 Secure Web)
- 23.8.2 (适用于 Android 的 Secure Mail)

Citrix® 支持从移动生产力应用程序的最后两个版本进行升级。移动生产力应用程序的最后两个版本如下：

- 23.8.1 (适用于 Android 的 Secure Mail)
- 23.8.0 (适用于 Android 的 Secure Web)
- 23.7.0 (适用于 Android 的 Secure Mail 和适用于 iOS 的 Secure Mail)
- 23.5.0 (适用于 iOS 的 Secure Mail 和适用于 Android 的 Secure Web)
- 23.2.0 (适用于 iOS 的 Secure Web)
- 22.9.1 (适用于 iOS 的 Secure Web)

重要：

MDX 加密已于 September 1, 2020 终止生命周期 (EOL)。对于已注册旧版设备管理 (DA) 的设备：

- 如果您不使用 MDX 加密，则无需执行任何操作。
- 如果您使用 MDX 加密，请将您的 Android 设备迁移到 Android Enterprise。运行 Android 10 的设备必须使用 Android Enterprise 注册或重新注册。这包括处于仅 MAM 模式的 Android 设备。有关详细信息，请参阅 [将设备管理迁移到 Android Enterprise](#)。

支持的操作系统

移动生产力应用程序支持以下操作系统：

产品名称	操作系统	最低部署版本	可用最新版本
安全中心	安卓	7.x	14.x
	iOS	12.x	17.x
安全邮件	安卓	8.x	14.x
	iOS	13.x	17.x
安全网页	安卓	8.x	14.x
	iOS	13.x	17.x

最新版本的移动生产力应用程序兼容最新版本和之前两个版本的 Citrix Endpoint Management。有关 Citrix Endpoint Management 支持的操作系统详情，请参阅[支持的设备操作系统](#)。

最新版本的移动生产力应用程序需要最新版本的 Secure Hub。请确保 Secure Hub 保持最新。

注意：

在任何时候，Citrix 仅支持最新版本和之前两个版本（N、N-1 和 N-2）的 Android 和 iOS 操作系统。

其他注意事项和限制

有关即将淘汰的 Citrix Endpoint Management 功能的提前通知，请参阅[弃用](#)。

安全邮件

- 由于 Secure Ticket Authority (STA) 和 Secure Mail 存在问题，Endpoint Management 目前不支持 NetScaler 12.0.41.16。此问题已在 NetScaler 12.0 build 41.22 中修复。
- Secure Mail 对 Exchange 2007 和 Lotus Notes 8.5.3 的支持已于 September 30, 2017 终止生命周期 (EOL)。
- 为获得发送 Citrix Files 附件的最佳性能，建议使用最新版本的 Citrix Files。Windows 不支持 Citrix Files。
- 在 IBM Notes 环境中，您必须配置 IBM Domino Traveler 服务器 9.0 版。有关详细信息，请参阅 Integrating Exchange Server or IBM Notes Traveler Server。

注意：

- Citrix Files for XenMobile 已于 July 1, 2023 终止生命周期 (EOL)。有关详细信息，请参阅 [EOL 和已弃用的应用程序](#)

安全 Web

在设备上安装最新版本的 Android WebView。用户可以从 Google Play 商店下载 Android WebView。

QuickEdit

QuickEdit 仍可作为移动生产力应用程序使用。生命周期结束 (EOL) 状态未在之前通知的 September 1, 2018 应用。

适用于 思杰端点管理 的 思杰内容协作™

版本 6.5 之后，用户可以从公共应用商店访问适用于 Endpoint Management 的 Citrix Content Collaboration。

ShareConnect

ShareConnect 已于 June 30, 2020 达到生命周期结束 (EOL) 状态。有关详细信息，请参阅 [EOL 和已弃用应用程序](#)。

思杰安全备忘录 和 思杰安全任务

Citrix Secure Notes 和 Citrix Secure Tasks 已于 December 31, 2018 达到生命周期结束 (EOL) 状态。有关详细信息，请参阅 [EOL 和已弃用应用程序](#)。

管理员任务和注意事项

本文讨论了与移动生产力应用程序管理员相关的任务和注意事项。

功能标志管理

如果在生产环境中移动生产力应用程序出现问题，我们可以在应用程序代码中禁用受影响的功能。我们可以为 iOS 和 Android 上的 Secure Hub、Secure Mail 和 Secure Web 禁用此功能。为此，我们使用功能标志和名为 LaunchDarkly 的第三方服务。您无需进行任何配置即可启用流向 LaunchDarkly 的流量，除非您有防火墙或代理阻止出站流量。在这种情况下，您需要根据策略要求通过特定的 URL 或 IP 地址启用流向 LaunchDarkly 的流量。有关隧道排除域的支持详细信息，请参阅 [MAM SDK 文档](#)。

您可以通过以下方式启用流向 LaunchDarkly 的流量和通信：

启用流向以下 URL 的流量

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

按域创建允许列表

此前，当您的内部策略要求仅列出 IP 地址时，我们提供了一份 IP 地址列表供您使用。现在，由于 Citrix® 进行了基础设施改进，我们将从 July 16, 2018 开始逐步淘汰公共 IP 地址。如果可以，我们建议您按域创建允许列表。

在允许列表中列出 IP 地址

如果您必须在允许列表中列出 IP 地址，请参阅此 [LaunchDarkly 公共 IP 列表](#)，以获取所有当前 IP 地址范围的列表。您可以使用此列表来确保您的防火墙配置与基础设施更新保持同步自动更新。有关基础设施更改状态的详细信息，请参阅 [LaunchDarkly 状态页](#)。

注意：

公共应用商店应用在首次部署时需要全新安装。无法从当前企业打包版本的应用升级到公共商店版本。

通过公共应用商店分发，您无需使用 MDX Toolkit 签名和打包 Citrix 开发的应用。您可以使用 MDX Toolkit 打包第三方或企业应用。

LaunchDarkly 系统要求

- Endpoint Management 10.7 或更高版本。
- 如果您将 Citrix ADC 上的拆分隧道设置为 **OFF**，请确保应用可以与以下服务通信：
 - LaunchDarkly 服务
 - APNs 侦听器服务

支持的应用商店

移动生产力应用可在 Apple App Store 和 Google Play 上获取。

在中国，Google Play 不可用，适用于 Android 的 Secure Hub 可在以下应用商店获取：

- <<https://shouji.baidu.com>>
- <<http://apk.hiapk.com>>
- <<https://apk.91.com>>

启用公共应用商店分发

1. 从 [Endpoint Management 下载页面](#) 下载适用于 iOS 和 Android 的公共商店 .mdx 文件。
2. 将 .mdx 文件上传到 Endpoint Management 控制台。移动生产力应用的公共商店版本仍作为 MDX 应用程序上传。不要将这些应用作为公共商店应用上传到服务器。有关步骤，请参阅 [添加应用](#)。
3. 根据您的安全策略更改默认策略（可选）。
4. 将应用作为必需应用推送（可选）。此步骤要求您的环境已启用移动设备管理。
5. 从 App Store、Google Play 或 Endpoint Management 应用商店在设备上安装应用。
 - 在 Android 上，用户会被定向到 Play 商店安装应用。在 iOS 上，在启用了 MDM 的部署中，应用会在不将用户带到应用商店的情况下安装。

- 当应用从 App Store 或 Play 商店安装时，会发生以下操作。只要相应的 .mdx 文件已上传到服务器，应用就会转换为托管应用。在转换为托管应用时，应用会提示输入 Citrix PIN。当用户输入 Citrix PIN 后，Secure Mail 会显示帐户配置屏幕。

6. 只有当您已注册 Secure Hub 且相应的 .mdx 文件位于服务器上时，应用才可访问。如果这两个条件中的任何一个未满足，用户可以安装应用，但应用的使用将被阻止。

如果您目前使用公共应用商店中来自 Citrix Ready Marketplace™ 的应用，您应该已经熟悉部署过程。移动生产力应用采用了许多 ISV 目前使用的相同方法。将 MDX SDK 嵌入到应用中，使应用做好公共商店部署准备。

注意：

适用于 iOS 和 Android 的 Citrix Files 应用的公共商店版本现在是通用的。Citrix Files 应用在手机和平板电脑上是相同的。

Apple 推送通知

有关配置推送通知的更多信息，请参阅 [配置 Secure Mail 以进行推送通知](#)。

公共应用商店常见问题

- 我可以将公共商店应用的多个副本部署到不同的用户组吗？例如，我想向不同的用户组部署不同的策略。

为每个用户组上传不同的 .mdx 文件。但是，在这种情况下，单个用户不能属于多个组。如果用户确实属于多个组，则会将同一应用的多个副本分配给该用户。公共商店应用的多个副本不能部署到同一设备，因为应用 ID 无法更改。

- 我可以将公共应用商店应用作为必需应用推送吗？

可以。将应用推送到设备需要 MDM；MAM 部署不支持此功能。

- 我是否需要更新任何基于用户代理的流量策略或 Exchange Server 规则？

按平台划分的任何基于用户代理的策略和规则的字符串如下所示。

重要提示：

Secure Notes 和 Secure Tasks 已于 December 31, 2018 达到生命周期终止 (EOL) 状态。有关详细信息，请参阅[EOL 和已弃用应用](#)。

安卓

应用	服务器	用户代理字符串
思杰安全邮件™	交换	WorxMail
	Lotus Notes 旅行者	苹果 - iPhone WorxMail
Citrix 安全 Web™		WorxMail
Citrix 安全任务	交换	WorxMail
Citrix 安全备忘录	交换	WorxMail
	Citrix 文件	安全备忘录

iOS

应用	服务器	用户代理字符串
Citrix 安全邮件	爱克斯昌	WorxMail
	莲花笔记旅行者	苹果 - iPhone WorxMail
思杰安全Web		com.citrix.browser
思杰安全任务	爱克斯昌	WorxTasks
思杰安全备忘录	爱克斯昌	WorxNotes
	思杰文件	安全备忘录

- 我能否阻止应用升级？

不。当更新发布到公共应用商店时，任何启用了自动更新的用户都会收到更新。

- 我可以强制执行应用升级吗？

可以，升级通过“升级宽限期策略”强制执行。当与应用更新版本对应的新的 .mdx 文件上传到 Endpoint Management 时，将设置此策略。

- 如果我无法控制更新时间表，如何在更新到达用户之前测试应用？

与 Secure Hub 的流程类似，在 EAR 期间，iOS 应用可在 TestFlight 上进行测试。对于 Android，应用在 EAR 期间可通过 Google Play 测试版计划获取。您可以在在此期间测试应用更新。

- 如果在自动更新到达用户设备之前我没有更新新的 .mdx 文件，会发生什么？

更新后的应用仍与旧的 .mdx 文件兼容。任何依赖于新策略的新功能都不会启用。

- 如果安装了 Secure Hub，应用会自动转换为托管状态，还是需要注册？

用户必须在 Secure Hub 中注册，公共应用商店应用才能作为托管应用（由 MDX 保护）激活并可用。如果 Secure Hub 已安装但未注册，则用户无法使用公共应用商店应用。

- 公共应用商店应用需要 Apple 企业开发者帐户吗？

不需要。由于 Citrix 现在负责维护移动生产力应用的证书和配置文件，因此部署这些应用给用户不需要 Apple 企业开发者帐户。

- 企业分发结束是否适用于我部署的任何封装应用？

不，它仅适用于移动生产力应用：Secure Mail、Secure Web 和适用于 Endpoint Management 的 Citrix Content Collaboration™、QuickEdit 和 ShareConnect。您部署的任何内部开发或第三方开发的企业封装应用都可以继续使用企业封装。MDX Toolkit 继续支持应用开发者的企业封装。

- 当我从 Google Play 安装应用时，收到错误代码为 505 的 Android 错误。

注意：

对 Android 5.x 的支持已于 December 31, 2018 结束。

这是 Google Play 和 Android 5.x 版本的一个已知问题。如果出现此错误，您可以按照以下步骤清除设备上阻止应用安装的陈旧数据：

1. 重新启动设备。
2. 通过设备设置清除 Google Play 的缓存和数据。
3. 作为最后的手段，删除设备上的 Google 帐户，然后重新添加。

有关详细信息，请使用以下关键字在此[站点](#)上搜索：“修复 Android 中的 Google Play 商店错误 505：未知错误代码”

- 尽管 Google Play 上的应用已发布到生产环境，并且没有新的 Beta 版本可用，为什么我在 Google Play 上的应用标题后看到 Beta？

如果您是我们早期访问发布 (EAR) 计划的一部分，您总会在应用标题旁边看到 Beta。此名称仅通知用户他们对特定应用的访问级别。Beta 名称表示用户收到可用的最新应用版本。最新版本可能是发布到生产轨道或 Beta 轨道的最新版本。

- 安装并打开应用后，用户会看到“应用未授权”消息，即使 .mdx 文件位于 Endpoint Management 控制台中。

如果用户直接从 App Store 或 Google Play 安装应用，并且 Secure Hub 未刷新，则可能会发生此问题。当非活动计时器过期时，必须刷新 Secure Hub。当用户打开 Secure Hub 并重新进行身份验证时，策略会刷新。用户下次打开应用时，应用将获得授权。

- 我需要访问代码才能使用该应用吗？当我从 App Store 或 Play Store 安装应用时，我看到一个屏幕提示我输入访问代码。

如果您看到请求访问代码的屏幕，则表示您尚未通过 Secure Hub 注册 Endpoint Management。请使用 Secure Hub 注册，并确保应用的 .mdx 文件已部署在服务器上。同时确保该应用可以使用。访问代码仅限于 Citrix 内部使用。应用需要 Endpoint Management 部署才能激活。

- 我可以通过 VPP 或 DEP 部署 iOS 公共商店应用吗？

Endpoint Management 已针对非 MDX 启用的公共商店应用的 VPP 分发进行了优化。尽管您可以使用 VPP 分发 Endpoint Management 公共商店应用，但在我们对 Endpoint Management 和 Secure Hub 商店进行进一步增强以解决这些限制之前，部署并非最佳。有关通过 VPP 部署 Endpoint Management 公共商店应用的已知问题列表以及可能的解决方法，请参阅 [Citrix 知识中心](#) 中的这篇文章。

适用于移动生产力应用的 MDX 策略

MDX 策略使您能够配置 Endpoint Management 强制执行的设置。这些策略涵盖身份验证、设备安全性、网络要求和访问、加密、应用程序交互、应用程序限制等。许多 MDX 策略适用于所有移动生产力应用程序。某些策略是特定于应用程序的。

策略文件以 .mdx 文件的形式提供，适用于移动生产力应用程序的公共商店版本。您还可以在添加应用程序时在 Endpoint Management 控制台中配置策略。

有关 MDX 策略的完整说明，请参阅本节中的以下文章：

- [移动生产力应用程序的 MDX 策略概览](#)
- [适用于 Android 的移动生产力应用程序的 MDX 策略](#)
- [适用于 iOS 的移动生产力应用程序的 MDX 策略](#)

以下部分描述了与用户连接相关的 MDX 策略。

适用于 Android 的 Secure Mail 中的双模式

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)。要继续管理您的企业应用程序，您必须集成 MAM SDK。

从版本 20.8.0 开始，Android 应用程序随 MDX 和 MAM SDK 一起发布，为前面提到的 MDX EOL 策略做准备。MDX 双模式旨在提供一种从当前 MDX Toolkit 过渡到新 MAM SDK 的方法。使用双模式，您可以选择：

- 继续使用 MDX Toolkit 管理应用程序（在 Endpoint Management 控制台中现已命名为 Legacy MDX）
- 管理集成新 MAM SDK 的应用程序。

注意：

使用 MAM SDK 时，您无需封装应用程序。

在您切换到 MAM SDK 后，无需其他步骤。

有关 MAM SDK 的更多详细信息，请参阅以下文章：

- [MAM SDK 概述](#)
- [MAM SDK 最新版本](#)
- Citrix Developer 网站上关于[设备管理](#)的部分
- [Citrix 博客文章](#)

先决条件

要成功部署双模式功能，请确保满足以下条件：

- 将 Citrix Endpoint Management 更新到版本 10.12 RP2 及更高版本，或 10.11 RP5 及更高版本。
- 将移动应用程序更新到版本 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。
- 如果您的组织使用第三方应用程序，请务必在为 Citrix 移动生产力应用程序切换到 MAM SDK 选项之前，将 MAM SDK 集成到您的第三方应用程序中。所有托管应用程序必须一次性迁移到 MAM SDK。

注意：

所有基于云的客户均支持 MAM SDK。

限制

- MAM SDK 仅支持在 Citrix Endpoint Management™ 部署中通过 Android Enterprise 平台发布的应用程序。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。
- 如果您不更新 Citrix Endpoint Management，并且策略文件在移动应用程序上运行的版本为 20.8.0 及更高版本，则会为 Secure Mail 创建重复的网络策略条目。

在 Citrix Endpoint Management 中配置 Secure Mail 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，或切换到新的 MAM SDK 进行应用程序管理。Citrix 建议您切换到 MAM SDK，因为 MAM SDK 更具模块化，旨在让您仅使用组织所用 MDX 功能的子集。

您可以在 **MDX 或 MAM SDK 策略容器** 中获得以下策略设置选项：

- **MAM SDK**
- **旧版 MDX**

The screenshot displays the Citrix Cloud Endpoint Management interface. The 'Configure' tab is active, showing the configuration for a 'Secure Mail' application. The left sidebar lists various configuration sections, with 'MDX' expanded. The main configuration area includes fields for 'File name', 'App Description', 'App version', 'Minimum OS version', 'Maximum OS version', and 'Excluded devices'. Below these are toggle switches for 'Remove app if MDM profile is removed', 'Prevent app data backup', 'Force app to be managed', and 'App deployed via Volume purchase'. At the bottom, the 'MDX or MAM SDK policy container' section is highlighted with a red box, showing two radio button options: 'MAM SDK' and 'Legacy MDX'. The 'Legacy MDX' option is currently selected.

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**。不允许从 **MAM SDK** 切换到 **旧版 MDX**，您需要重新发布应用程序。默认值为 **旧版 MDX**。请确保为在同一设

设备上运行的 Secure Mail 和 Secure Web 设置相同的策略模式。您不能在同一设备上运行两种不同的模式。

用户连接到内部网络

隧道连接到内部网络的连接可以使用完整 VPN 隧道或无客户端 VPN 的变体，称为隧道式 Web SSO。首选 VPN 模式策略控制此行为。默认情况下，连接使用隧道式 Web SSO，建议用于需要 SSO 的连接。完整 VPN 隧道设置建议用于使用客户端证书或端到端 SSL 连接到内部网络中资源的连接。此设置可处理任何基于 TCP 的协议，并可用于 Windows 和 Mac 计算机以及 iOS 和 Android 设备。

允许 VPN 模式切换策略允许根据需要自动在完整 VPN 隧道和隧道式 Web SSO 模式之间切换。默认情况下，此策略处于关闭状态。当此策略处于启用状态时，因首选 VPN 模式无法处理的身份验证请求而失败的网络请求将在备用模式下重试。例如，完整 VPN 隧道模式可以处理客户端证书的服务端质询，但隧道式 Web SSO 模式不能。同样，在使用隧道式 Web SSO 模式时，HTTP 身份验证质询更有可能通过 SSO 进行处理。

网络访问限制

网络访问策略指定是否对网络访问施加限制。默认情况下，Secure Mail 访问不受限制，这意味着不对网络访问施加任何限制。应用程序可以无限制地访问设备连接到的网络。默认情况下，Secure Web 访问通过隧道连接到内部网络，这意味着所有网络访问都使用返回到内部网络的每个应用程序 VPN 隧道，并使用 Citrix ADC 分流隧道设置。您还可以指定阻止访问，以便应用程序在设备没有网络连接的情况下运行。

如果您想允许 AirPrint、iCloud 以及 Facebook 和 Twitter API 等功能，请勿阻止网络访问策略。

网络访问策略还与后台网络服务策略交互。有关详细信息，请参阅[集成 Exchange Server 或 IBM Notes Traveler Server](#)。

Endpoint Management 客户端属性

客户端属性包含直接提供给用户设备上的 Secure Hub 的信息。客户端属性位于 Endpoint Management 控制台的 **Settings > Client > Client Properties** 中。

客户端属性用于配置以下设置：

用户密码缓存

用户密码缓存允许将用户的 Active Directory 密码缓存在移动设备本地。如果启用用户密码缓存，系统会提示用户设置 Citrix PIN 或密码。

不活动计时器

不活动计时器定义了用户可以将其设备置于不活动状态并访问应用程序而无需提示输入 Citrix PIN 或密码的分钟数。要为 MDX 应用程序启用此设置，必须将“应用程序密码策略”设置为 **On**。如果“应用程序密码策略”设置为 **Off**，用户将被重定向到 Secure Hub 以执行完全身份验证。更改此设置后，该值将在用户下次被提示进行身份验证时生效。

Citrix PIN 身份验证

Citrix PIN 简化了用户身份验证体验。PIN 用于保护客户端证书或将 Active Directory 凭据本地保存在设备上。如果配置 PIN 设置，用户登录体验如下：

1. 当用户首次启动 Secure Hub 时，系统会提示他们输入 PIN，该 PIN 会缓存 Active Directory 凭据。
2. 当用户下次启动移动生产力应用程序（例如 Secure Mail）时，他们输入 PIN 并登录。

您可以使用客户端属性启用 PIN 身份验证、指定 PIN 类型以及指定 PIN 强度、长度和更改要求。

指纹或触控 ID 身份验证

适用于 iOS 设备的指纹身份验证（也称为触控 ID 身份验证）是 Citrix PIN 的替代方案。当打包的应用程序（Secure Hub 除外）需要脱机身份验证时（例如，当不活动计时器过期时），此功能非常有用。您可以在以下身份验证方案中启用此功能：

- Citrix PIN + 客户端证书配置
- Citrix PIN + 缓存的 AD 密码配置
- Citrix PIN + 客户端证书配置和缓存的 AD 密码配置
- Citrix PIN 已关闭

如果指纹身份验证失败，或者用户取消了指纹身份验证提示，则封装的应用程序将回退到 Citrix PIN 或 AD 密码身份验证。

指纹身份验证要求

- 支持指纹身份验证并至少配置了一个指纹的 iOS 设备（最低版本 8.1）。
- 用户熵必须关闭。

配置指纹身份验证

重要提示：

如果用户熵已启用，则会忽略“启用触控 ID 身份验证”属性。用户熵通过“使用密码密钥加密机密”启用。

1. 在 Endpoint Management 控制台中，转到 **设置 > 客户端 > 客户端属性**。
2. 单击 **添加**。

“添加新客户端属性”屏幕的图像(/en-us/mobile-productivity-apps/media/add-client-property-endpointmanagement.png)

3. 添加密钥 **ENABLE_TOUCH_ID_AUTH**，将其值设置为 **True**，然后将策略名称设置为 **启用指纹身份验证**。

配置指纹身份验证后，用户无需重新注册其设备。

有关使用密码密钥加密机密和客户端属性的更多信息，请参阅 Endpoint Management 中关于 [客户端属性](#) 的文章。

谷歌分析

Citrix Secure Mail 使用 Google Analytics 收集应用程序统计信息和使用情况分析数据，以提高产品质量。Citrix 不会收集或存储任何其他个人用户信息。

禁用谷歌分析

管理员可以通过配置自定义客户端属性 **DISABLE_GA** 来禁用 Google Analytics。要禁用 Google Analytics，请执行以下操作：

1. 登录 Citrix Endpoint Management 控制台并导航到 **设置 > 客户端属性 > 添加新客户端属性**。
2. 将值 **DISABLE_GA** 添加到 **Key** 字段。
3. 将客户端属性的值设置为 **true**。

注意：

如果您未在 Citrix Endpoint Management 控制台中配置值 **DISABLE_GA**，则 Google Analytics 数据将处于活动状态。

MDX 移动生产力应用程序策略概览

本文介绍了适用于 iOS 和 Android 的 Citrix 移动生产力应用程序的 MDX 应用程序策略以及默认值。您可以在 Citrix Endpoint Management 控制台中更改策略设置。有关详细信息，请参阅 [添加应用程序](#)。

注意：

Secure Hub 在某些操作期间会刷新策略。有关详细信息，请参阅 [管理 Secure Hub](#)。

身份验证

设备密码

- iOS：是
- 安卓：否
- 默认设置：关

注意：

此策略仅适用于 iOS 9 设备，Citrix® 不再支持这些设备。

应用程序密码

- iOS：是
- 安卓：是
- 默认设置：开

在线会话所需宽限期（分钟）

- iOS：是
- Android：不支持
- 默认设置：0

最长离线时间

- iOS：是
- Android：支持
- 默认设置：168 小时 (7 天)

备用 Citrix 网关

注意：

此策略在 Endpoint Management 控制台中的名称为 Alternate NetScaler® Gateway。

- iOS: 是
- Android：支持
- 默认设置: 空

设备安全性

阻止越狱或已root

- iOS: 是
- 安卓: 是
- 默认设置: 开

要求设备锁定

- iOS: 否
- 安卓: 是
- 默认设置: 关

注意:

在 Android M 设备上，设备 PIN 或密码以及设备图案屏幕锁定选项具有相同的效果：使用其中任一选项，如果设备未设置 PIN、密码或图案屏幕锁定，则应用程序将被锁定。

网络要求

要求 Wi-Fi

- iOS: 是
- 安卓：是
- 默认设置: 关

允许的Wi-Fi网络

- iOS: 是
- 安卓: 是
- 默认设置: 空

杂项访问

应用程序更新宽限期（小时）

- iOS: 是
- 安卓: 是
- 默认设置: 168 小时（7 天）

注意：

Citrix 建议使用非零 (0) 值。零值会立即阻止用户未收到警告的情况下使用正在运行的应用程序，直到他们下载并安装更新。此设置可能导致用户被迫退出应用程序并可能丢失工作的情况。

禁用强制升级

- iOS: 是
- 安卓: 是
- 默认设置: 开

锁定后擦除应用数据

- iOS: 是
- Android: 支持
- 默认设置: 关

活动轮询周期（分钟）

- iOS: 是
- Android: 支持
- 默认设置: 60 分钟（1 小时）

注意：

仅对高风险应用将此值设置为低于默认值，否则可能会影响性能。

加密

加密类型

- iOS: 是
- Android: 支持
- 默认设置: MDX 加密

注意：

对于新添加的应用程序，当您从**平台加密（强制合规）**更改为**MDX 加密**时，您将被强制删除并重新安装应用程序。新添加应用程序的默认设置为**平台加密（强制合规）**。

不合规设备行为

- iOS：是
- Android：支持
- 默认设置：警告后允许应用程序

启用 MDX 加密

- iOS：是
- Android：不支持
- 默认设置：开启

注意：

如果您在部署应用程序后更改此策略，用户必须重新安装应用程序。

加密密钥

- iOS：否
- Android：支持
- 默认设置：仅允许离线访问。

私有文件加密

- iOS：否
- 安卓：是
- 默认设置：SecurityGroup

私有文件加密排除项

- iOS：否
- 安卓：是
- 默认设置：空

公共文件的访问限制

- iOS：否
- 安卓：是
- 默认设置：空

注意：

启用公共文件加密策略会强制执行此策略（从“禁用选项”更改为“SecurityGroup”或“应用程序”选项）。此策略仅适用于现有未加密的公共文件，并指定何时加密这些文件。

公共文件加密

- iOS: 否
- Android: 支持
- 默认设置: SecurityGroup

公共文件加密排除项

- iOS: 否
- Android: 支持
- 默认设置: 空

公共文件迁移

- iOS: 否
- Android: 支持

- 默认设置: 写入 (RO/RW)

注意：

加密现有公共文件会使该文件无法供没有相同加密密钥的其他应用使用。

启用加密

- iOS: 是
- Android: 不支持
- 默认设置: 开启

注意：

如果您更改现有应用的此策略，用户必须移除并重新安装该应用才能应用策略更改。

数据库加密排除项

- iOS: 是
- Android: 不支持
- 默认设置: 空

文件加密排除项

- iOS: 是
- Android: 不支持
- 默认设置: 空

应用交互

安全组

- iOS: 否
- Android: 支持
- 默认设置: 空

注意：

如果您更改现有应用的此策略，用户必须卸载并重新安装应用才能应用策略更改。

剪切和复制

- iOS: 是
- Android: 支持
- 默认设置: 受限

粘贴

- iOS: 是
- Android: 支持
- 默认设置: 不受限

文档交换（在...中打开）

- iOS: 是
- 安卓: 是
- 默认设置: 受限

从筛选中排除的 URL 域

- iOS: 否
- 安卓: 是
- 默认设置: 空

允许的安全 Web 域

- iOS: 否
- 安卓: 是
- 默认设置: 空

连接安全级别

- iOS: 是
- 安卓: 是
- 默认设置: TLS

入站文档交换 (Open In)

- iOS: 是
- 安卓: 是
- 默认设置: 不受限制

受限的“打开方式”例外列表

- iOS: 是
- 安卓: 是
- 默认设置: 空（适用于 Android）；Office 365 应用程序（适用于 iOS）

注意：

在 Android 上，此策略以前名为“打开方式排除项”。在 iOS 上，此策略是隐藏的。有关详细信息，请参阅[适用于 iOS 应用程序的 MDX 策略](#)。

应用程序 URL 方案

- iOS: 是
- 安卓: 否
- 默认设置: 空。所有已注册的应用程序 URL 方案均被阻止。

允许的 URL

- iOS: 是
- Android: 不支持
- 默认设置: 有关默认设置的详细信息，请参阅 iOS 应用的 MDX 策略中的“应用交互”部分。

显式注销通知

- iOS: 是
- Android: 不支持
- 默认设置: 仅限共享设备，适用于 Secure Mail

应用交互（出站 URL）

从 URL 筛选中排除的域

- iOS: 是
- Android: 不支持
- 默认设置: 空

允许的 URL

- iOS: 是
- Android: 不支持
- 默认设置: 有关默认设置的详细信息，请参阅[适用于 iOS 应用的 MDX 策略](#)中的“应用交互（出站 URL）”部分。

允许的安全 Web 域

- iOS: 是
- 安卓: 否
- 默认设置: 空

应用程序限制

阻止相机

- iOS: 是
- 安卓: 是
- 默认设置: iOS 为关；Android 为开

阻止图库

- iOS: 否
- 安卓: 是
- 默认设置: 关

阻止照片库

- iOS: 是
- 安卓: 否

- 默认设置: 开启

阻止麦克风录音

- iOS: 是
- 安卓: 是
- 默认设置: 开启

阻止听写

- iOS: 是
- 安卓: 否
- 默认设置: 开启

阻止位置服务

- iOS: 是
- 安卓: 是
- 默认设置: 对于 Android: Secure Mail 的默认值为“关闭”。其他应用的默认值为“开启”。

阻止短信撰写

- iOS: 是
- Android: 支持
- 默认设置: 开启

阻止屏幕捕获

- iOS: 否
- Android: 支持
- 默认设置: 开启

阻止设备传感器

- iOS: 否
- Android: 支持
- 默认设置: 开启

阻止 NFC

- iOS: 否
- Android: 支持
- 默认设置: 开启

阻止 iCloud

- iOS: 是
- 安卓: 否
- 默认设置: 开启

阻止查找

- iOS: 是
- 安卓: 否
- 默认设置: 开启

阻止文件备份

- iOS: 是
- 安卓: 否
- 默认设置: 开启

阻止 AirPrint

- iOS: 是
- Android: 不允许
- 默认设置: 开启

阻止打印

- iOS: 否
- Android: 允许
- 默认设置: 开启

阻止 AirDrop

- iOS: 是
- Android: 不支持

- 默认设置: 开启

阻止文件附件

- iOS: 是
- Android: 不支持
- 默认设置: 关闭

阻止电子邮件撰写

- iOS: 是
- Android: 不支持
- 默认设置: 开启

阻止 Facebook 和 Twitter API

- iOS: 是
- Android: 不支持
- 默认设置: 开启

模糊屏幕内容

- iOS: 是
- Android: 不支持
- 默认设置: 开启

阻止第三方键盘

- iOS: 是
- Android: 不支持
- 默认设置: 开启

注意

iOS 11 及更高版本

阻止应用日志

- iOS: 是

- Android：适用
- 默认设置: 关

启用 ShareFile

- iOS:
- Android：适用
- 默认设置: 开

启用从文件附加

- iOS: 是
- Android：不适用
- 默认设置: 开

应用网络访问

网络访问

- iOS: 是
- Android：支持
- 默认设置：对于新上传的应用程序，除 Secure Mail 外，所有应用程序的默认值为 **已阻止**。由于 Intune 没有阻止状态，Secure Mail 的默认值为 **无限制**。

需要微型 VPN 会话

- iOS: 是
- Android：支持
- 默认设置：使用上一个设置。对于新上传的应用程序，默认值为否。

需要微型 VPN 会话的宽限期（分钟）

- iOS: 是
- Android：支持
- 默认设置：0（无宽限期）

排除列表

- iOS: 是
- Android：支持

- 默认设置：空

阻止本地主机连接

- iOS: 否
- Android: 支持
- 默认设置: 关

证书标签

- iOS: 是
- Android: 支持
- 默认设置: 空

应用日志

默认日志输出

- iOS: 是
- Android: 支持
- 默认设置: 文件

默认日志级别

- iOS: 是
- Android: 支持
- 默认设置: 4 (信息性消息)

最大日志文件数

- iOS: 是
- Android: 支持
- 默认设置: 2

最大日志文件大小

- iOS: 是
- Android: 支持
- 默认设置: 2 MB

重定向应用日志

- iOS: 否
- Android: 支持
- 默认设置: 开启

加密日志

- iOS: 否
- Android: 支持
- 默认设置: 关

应用地理围栏

中心点经度

- iOS: 是
- Android: 支持
- 默认设置: 0

中心点纬度

- iOS: 是
- Android: 支持
- 默认设置: 0

半径

- iOS: 是
- Android: 支持
- 默认设置: 0 (已禁用)

注意：

以米为单位设置半径。当设置为零时，地理围栏将被禁用。

应用程序设置

安全邮件 Exchange 服务器

- iOS: 是
- 安卓: 是
- 默认设置: 空

注意：

如果更改现有应用程序的此策略，用户必须删除并重新安装该应用程序才能应用策略更改。

Secure Mail 用户域

- iOS: 是
- 安卓: 是
- 默认设置: 空

后台网络服务

- iOS: 是
- Android: 支持
- 默认设置: 空

注意：

如果配置此策略，请将“网络访问”策略设置为“隧道连接到内部网络”，此策略随后生效。当 Exchange Server 位于内部网络中时，请使用此策略，并且您希望使用 Citrix Gateway 代理到内部 Exchange Server 的连接。

后台服务票证过期

- iOS: 是
- Android: 支持
- 默认设置: 168 小时（7 天）

后台网络服务网关

- iOS: 是
- Android: 支持
- 默认设置: 空

注意：

如果配置此策略，请将网络访问策略设置为“隧道连接到内部网络”，此策略随后生效。当 Exchange Server 位于内部网络中时，请使用此策略，或者您希望使用 Citrix Gateway 代理到内部 Exchange Server 的连接。配置“网络访问”策略后，此策略生效。

导出联系人

- iOS: 是
- Android: 支持
- 默认设置: 关

要导出的联系人字段

- iOS: 是
- Android: 支持
- 默认设置: 所有

接受所有 SSL 证书

- iOS: 是
- Android: 支持
- 默认设置: 关

控制锁定屏幕通知

- iOS: 是
- Android: 支持
- 默认设置: 允许

使用安全连接

- iOS: 否

- 安卓：是
- 默认设置: 开启

默认电子邮件通知

- iOS: 是
- 安卓：否
- 默认设置: 开启

默认同步间隔

- iOS: 是
- 安卓: 是
- 默认设置: 3 天

注意：

Exchange ActiveSync 邮箱策略设置“最长电子邮件保留时间筛选器”优先于此策略。Secure Mail 仅显示小于“最长电子邮件保留时间筛选器”的同步间隔值。

邮件搜索限制

- iOS: 是
- Android: 支持
- 默认设置: 无限制

最大同步间隔

- iOS: 是
- Android: 支持
- 默认设置: 所有

启用周数

- iOS: 是
- Android: 支持
- 默认设置: 关

启用通过 Wi-Fi 下载附件

- iOS: 是
- Android: 支持
- 默认设置: 关闭

允许离线文档

- iOS: 是
- 安卓: 是
- 默认设置: 无限制

信息权限管理

- iOS: 是
- 安卓: 是
- 默认设置: 关闭

电子邮件分类

- iOS: 是
- 安卓: 否
- 默认设置: 关闭

电子邮件分类标记

- iOS: 是
- 安卓: 否
- 默认设置: 空

电子邮件分类命名空间

- iOS: 是
- 安卓: 否
- 默认设置: 空

电子邮件分类版本

- iOS: 是
- 安卓: 否

- 默认设置: 空

默认电子邮件分类

- iOS: 是
- 安卓: 否
- 默认设置: 非官方

启用草稿电子邮件自动保存

- iOS: 是
- Android: 支持
- 默认设置: 开启

启用 iOS 数据保护

- iOS: 是
- Android: 不支持
- 默认设置: 关闭

推送通知 EWS 主机名

- iOS: 是
- Android: 不支持
- 默认设置: 空

推送通知

- iOS: 是
- Android: 不支持
- 默认设置: 关闭

推送通知区域

- iOS: 是
- 安卓: 否
- 默认设置: 美洲

首次启动 Secure Mail 时启用 S/MIME

- iOS: 是
- Android: 不允许
- 默认设置: 关

初始身份验证机制

- iOS: 是
- Android: 允许
- 默认设置: 使用 MDX 提供的邮件服务器地址

初始身份验证凭据

- iOS: 是
- 安卓：是
- 默认设置: 注册用户名

启用周数

- iOS: 是
- Android: 支持
- 默认设置: 关

日历 Web 和音频选项

- iOS: 是
- Android: 支持
- 默认设置: GoToMeeting 和用户输入

S/MIME 公共证书源

- iOS: 是
- Android: 支持
- 默认设置: Exchange

LDAP 服务器地址

- iOS: 是
- 安卓：是

- 默认设置: 空

LDAP 基本 DN

- iOS: 是
- 安卓: 支持
- 默认设置: 空

匿名访问 LDAP

- iOS: 是
- 安卓: 支持
- 默认设置: 关

允许的电子邮件域

- iOS: 是
- 安卓: 否
- 默认设置: 空

注意

如果为空，则不限制域。

身份验证失败时尝试用户名迁移

- iOS: 是
- 安卓: 是
- 默认设置: 关

报告网络钓鱼邮件地址

- iOS: 是
- 安卓: 是
- 默认设置: 空

报告网络钓鱼机制

- iOS: 否

- 安卓: 是
- 默认设置: 通过附件 (.eml) 报告

Skype for Business 会议域

- iOS: 是
- Android: 支持
- 默认设置: 空

导出日历

- iOS: 是
- Android: 支持
- 默认设置: 会议时间

启用 Slack

- iOS: 是
- Android: 支持
- 默认设置: 关

Slack 工作区名称

- iOS: 是
- Android: 支持
- 默认设置: 空

来电显示

- iOS: 是
- 安卓: 否
- 默认设置: 开启

注意：

如果开启，Secure Mail 会向 iOS 提供您已保存联系人的姓名和电话号码，用于来电识别。

分析

启用 谷歌分析

- iOS: 是
- 安卓: 否
- 默认设置: 开启

Google Analytics 详细程度

- iOS: 是
- 安卓: 是
- 默认设置: 完整

报告

Citrix 报告

- iOS: 是
- Android: 不支持
- 默认设置: 关

注意:

Citrix 也可能通过功能标志控制此功能。此功能要正常运行，必须同时启用功能标志和此策略。

上传令牌

- iOS: 是
- Android: 不支持
- 默认设置: 空

仅通过 Wi-Fi 发送报告

- iOS: 是
- Android: 不支持
- 默认设置: 开

报告文件缓存最大值

- iOS: 是
- Android: 不支持
- 默认设置: 2 MB

Office 365 的 OAuth 支持

对 Office 365 使用新式身份验证

- iOS: 否
- Android: 支持
- 默认设置: 关

Office 365 身份验证机制

- iOS: 是
- 安卓: 否
- 默认设置: 不使用 OAuth

受信任的 Exchange Online 主机名

- iOS: 是
- 安卓: 是
- 默认设置: outlook.office365.com

受信任的 AD FS 主机名

- iOS: 是
- 安卓: 是
- 默认设置: login.microsoftonline.com

用于现代身份验证的自定义用户代理

- iOS: 否
- 安卓: 是
- 默认设置: 空

注意：

如果您未配置此策略，在现代身份验证期间将使用默认的 Secure Mail 用户代理。

邮件重定向

邮件重定向

- iOS: 是
- 安卓：否
- 默认设置: Secure Mail

Slack 集成

启用 Slack

- iOS: 是
- 安卓：是
- 默认设置: 关

Slack 工作区名称

- iOS: 是
- 安卓：是
- 默认设置: 空

适用于 Android 移动生产力应用程序的 MDX 策略

本文介绍了适用于 Android 应用程序的 MDX 策略。您可以在 Citrix Endpoint Management 控制台中更改策略设置。有关详细信息，请参阅 [添加应用程序](#)。

以下列表不包括 Secure Web 特有的 MDX 策略。有关 Secure Web 显示的策略的详细信息，请参阅 [Secure Web 策略](#)。

身份验证

应用程序密码

如果设置为 **开**，则当应用程序启动或在一段时间不活动后恢复时，需要 PIN 或密码才能解锁应用程序。默认值为 **开**。

要为所有应用程序配置不活动计时器，请在 **设置** 选项卡上的 **客户端属性** 中以分钟为单位设置 INACTIVITY_TIMER 值。默认不活动计时器值为 60 分钟。要禁用不活动计时器，以便仅在应用程序启动时显示 PIN 或密码提示，请将值设置为零。

注意：

如果为“加密密钥”策略选择“安全脱机”，此策略将自动启用。

最长脱机时间（小时）

定义应用程序可以脱机运行的最长时间，无需网络登录即可重新确认授权和刷新策略。默认值为 **168 小时**（7 天）。最短时间为 1 小时。

在期限到期前 30、15 和 5 分钟，系统会提醒用户登录。到期后，应用程序将保持锁定状态，直到用户成功完成网络登录。

替代的 Citrix Gateway

注意：

此策略在 Endpoint Management 控制台中的名称为 **备用 NetScaler® Gateway**。

特定备用 Citrix Gateway（以前称为 NetScaler Gateway）的地址，用于身份验证以及与此应用程序的微型 VPN 会话。**备用 NetScaler Gateway** 是一个可选策略，当与“需要在线会话”策略一起使用时，会强制应用程序重新向特定网关进行身份验证。此类网关通常具有不同的（更高保障的）身份验证要求和流量管理策略。如果留空，则始终使用服务器的默认值。默认值为空。

设备安全性

阻止越狱或已获得 root 权限

如果设置为“开”，则当设备已越狱或已获得 root 权限时，应用程序将被锁定。如果设置为“关”，则即使设备已越狱或已获得 root 权限，应用程序也可以运行。默认值为“开”。

要求设备加密

如果设置为“开”，则如果设备未配置加密，应用程序将被锁定。如果设置为“关”，则即使设备未配置加密，应用程序也允许运行。默认值为“关”。

注意：

此策略仅在 Android 3.0 (Honeycomb) 上受支持。将策略设置为“开”会阻止应用程序在旧版本上运行。

要求设备锁定

如果选中“**设备 PIN 或密码**”，则如果设备没有 PIN 或密码，应用程序将被锁定。如果选中“**设备图案屏幕锁定**”，则如果设备没有设置图案屏幕锁定，应用程序将被锁定。如果设置为“关”，则即使设备没有设置 PIN、密码或图案屏幕锁定，应用程序也允许运行。默认值为“关”。

设备 PIN 或密码 需要最低版本为 Android 4.1 (Jelly bean)。将策略设置为“**设备 PIN 或密码**”会阻止应用程序在旧版本上运行。

在 Android M 设备上，“**设备 PIN 或密码**”和“**设备图案屏幕锁定**”选项具有相同的效果：无论选择其中哪个选项，如果设备没有设置 PIN、密码或图案屏幕锁定，应用程序都将被锁定。

网络要求

要求 Wi-Fi

如果设置为“开”，则当设备未连接到 Wi-Fi 网络时，应用程序将被锁定。如果设置为“关”，则如果设备具有活动连接（例如 4G/3G、LAN 或 Wi-Fi 连接），应用程序可以运行。默认值为“关”。

允许的 Wi-Fi 网络

允许的 Wi-Fi 网络的逗号分隔列表。如果网络名称包含任何非字母数字字符（包括逗号），则名称必须用双引号括起来。应用程序仅在连接到列出的其中一个网络时运行。如果留空，则允许所有网络。此值不影响蜂窝网络连接。默认值为空白。

杂项访问

应用程序更新宽限期（小时）

定义系统发现有可用应用程序更新后，应用程序可以使用的宽限期。默认值为 **168 小时**（7 天）。

注意：

不建议使用零，因为它会立即阻止正在运行的应用程序被使用，直到更新下载并安装完成（且不向用户发出任何警告）。此值可能导致用户被迫退出正在运行的应用程序（可能会丢失工作）以遵守所需的更新。

禁用强制升级

禁用用户的应用商店中升级到最新版本应用程序的要求。默认值为 **ON**。

锁定后擦除应用程序数据

应用程序锁定时擦除数据并重置应用程序。如果为 **Off**，则应用程序锁定时不会擦除应用程序数据。默认值为 **Off**。

应用程序可能因以下任何原因被锁定：

- 用户失去应用程序授权
- 应用程序订阅已删除
- 帐户已删除
- Secure Hub 已卸载
- 应用程序身份验证失败次数过多
- 检测到越狱设备（根据策略设置）
- 设备因其他管理操作而处于锁定状态

活动轮询周期（分钟）

当应用程序启动时，MDX 框架会轮询 Citrix Endpoint Management 以确定当前应用程序和设备状态。假设可以访问运行 Endpoint Management 的服务器，该框架会返回有关设备的锁定/擦除状态以及应用程序的启用/禁用状态的信息。无论服务器是否可访问，都会根据活动轮询周期间隔安排后续轮询。周期到期后，将再次尝试新的轮询。默认值为 **60 分钟**（1 小时）。

重要提示：

仅对高风险应用程序将此值设置得更低，否则性能可能会受到影响。

加密

加密类型

允许您选择是由 MDX 还是设备平台处理数据加密。如果选择 **MDX 加密**，则 MDX 会加密数据。如果选择 **带合规性强制的平台加密**，则设备平台会加密数据。默认值为 **MDX 加密**。

不合规设备行为

允许您选择当设备不符合最低加密合规性要求时要执行的操作。选择 **允许应用程序** 以使应用程序正常运行。选择 **警告后允许应用程序** 以使应用程序在警告出现后运行。选择 **阻止** 以阻止应用程序运行。默认值为 **警告后允许应用程序**。

加密密钥

允许用于派生加密密钥的机密在设备上持久保存。仅允许脱机访问是唯一可用的选项。

Citrix 建议您将身份验证策略设置为启用网络登录或离线密码质询，以保护对加密内容的访问。

私有文件加密

控制以下位置中私有数据文件的加密：`/data/data/<appname>` 和 `/mnt/sdcard/Android/data/<appname>`。

禁用选项表示私有文件未加密。**安全组**选项使用同一安全组中所有 MDX 应用程序共享的密钥加密私有文件。**应用程序**选项使用此应用程序独有的密钥加密私有文件。默认值为**安全组**。

私有文件加密排除项

包含一个逗号分隔的文件路径列表。每个路径都是一个正则表达式，表示一个或多个加密文件。文件路径是相对于内部和外部沙盒的。默认值为空。

排除项仅适用于以下文件夹：

- **内部存储：**

`/data/data/<your_package_name>`

- **SD 卡：**

`/storage/emulated/<SD Card Slot>/Android/data/<your_package_name>`

`/storage/emulated/legacy/Android/data/<your_package_name>`

示例

要排除的文件	私有文件加密排除项中的值
<code>/data/data/com.citrix.mail/files/a.txt</code>	<code>\^files/a.txt</code>
<code>/storage/emulated/0/Android/data/com.citrix.mail/files</code> 中的所有文本文件	<code>\^files/(.)+.txt\$</code>

要排除的文件	私有文件加密排除项中的值
/data/data/com.citrix.mail/files 中的所有文件	\\文件/

公共文件的访问限制

包含一个逗号分隔的列表。每个条目都是一个正则表达式路径，后跟 (NA)、(RO) 或 (RW)。与路径匹配的文件被限制为**无访问权限**、**只读**或**读写**访问权限。列表按顺序处理，第一个匹配的路径用于设置访问限制。默认值为空。

此策略仅在**启用公共文件加密**时强制执行（从**禁用**选项更改为**安全组**或**应用程序**选项）。此策略仅适用于现有未加密的公共文件，并指定何时加密这些文件。

要排除的文件	私有文件加密中的值
外部存储上的下载文件夹只读	EXT:\\Download/(RO)
虚拟存储上 Music 文件夹中的所有 MP3 文件 无访问权限	VS:\\Music/(.)+.mp3\$(NA)

公共文件加密

控制公共文件的加密。如果设置为“**禁用**”，则公共文件不加密。如果设置为“**安全组**”，则使用同一安全组中所有 MDX 应用程序共享的密钥加密公共文件。如果设置为“**应用程序**”，则使用此应用程序独有的密钥加密公共文件。

默认值为“**安全组**”。

公共文件加密排除项

包含一个逗号分隔的文件路径列表。每个路径都是一个正则表达式，表示一个或多个不加密的文件。文件路径是相对于默认外部存储和任何设备特定的外部存储的。

公共文件加密排除项仅包括外部文件夹位置。

示例

要排除的文件	公共文件加密排除项中的值
SD 卡上的下载文件夹	下载
音乐文件夹中的所有 MP3 文件	\\Music/(.)+.mp3\$

公共文件迁移

此策略仅在启用公共文件加密策略（从“**禁用**”更改为“**安全组**”或“**应用程序**”）时强制执行。此策略仅适用于现有未加密的公共文件，并指定何时加密这些文件。默认值为“**写入 (RO/RW)**”。

“**禁用**”选项表示现有文件未加密。“**写入 (只写/读写)**”选项仅当以只写或读写访问方式打开现有文件时才对其进行加密。“**任意**”选项在任何模式下打开现有文件时都对其进行加密。选项：

- **禁用**。不加密现有文件。
- **写入 (只写/读写)**。仅当以只写或读写访问方式打开现有文件时才对其进行加密。
- **任意**。在任何模式下打开现有文件时都对其进行加密。

注意：

-新文件或被覆盖的现有未加密文件在任何情况下都会加密替换文件。 -加密现有公共文件会使该文件对没有相同加密密钥的其他应用程序不可用。

应用程序交互

安全组

如果您希望由 Citrix Endpoint Management™ 管理的所有移动应用程序相互交换信息，请将此字段留空。定义一个安全组名称，以管理特定应用程序集（例如，财务或人力资源）的安全设置。

注意：

如果您更改现有应用程序的此策略，用户必须删除并重新安装该应用程序才能应用策略更改。

剪切和复制

阻止、允许或限制此应用程序的剪贴板剪切和复制操作。如果设置为**受限**，则复制的剪贴板数据将放置在仅适用于 MDX 应用程序的专用剪贴板中。默认值为**受限**。

粘贴

阻止、允许或限制此应用程序的剪贴板粘贴操作。如果设置为**受限**，则粘贴的剪贴板数据将来源于仅适用于 MDX 应用程序的专用剪贴板。默认值为**不受限**。

文档交换 (打开方式)

阻止、允许或限制此应用的文档交换操作。如果设置为“**受限**”，则文档只能与其他 MDX 应用以及“受限打开方式例外列表”策略中指定的应用例外进行交换。如果设置为“**不受限**”，请将“私有文件加

密”和“公共文件加密”策略设置为“**已禁用**”，以使用户可以在未封装的应用中打开文档。默认值为“**受限**”。

从筛选中排除的 URL 域

此策略用于将某些出站 URL 从 MDX 筛选中排除。以下逗号分隔的完全限定域名 (FQDN) 或 DNS 后缀列表将从任何 MDX 筛选中排除。如果此策略包含任何条目，则主机字段与列表中至少一个项目匹配（通过 DNS 后缀匹配）的 URL 将未经修改地发送到默认浏览器。默认值为空。

允许的安全 Web 域

此策略仅对未被 URL 筛选策略排除的域有效。添加一个逗号分隔的完全限定域名 (FQDN) 或 DNS 后缀列表，当文档交换受限时，这些域名或 DNS 后缀将重定向到 Secure Web 应用。

如果此策略包含任何条目，则只有主机字段与列表中至少一个项目匹配（通过 DNS 后缀匹配）的 URL 才会在文档交换受限时重定向到 Secure Web 应用。

所有其他 URL 都将发送到默认的 Android Web 浏览器（绕过“文档交换受限”策略）。默认值为空。

受限打开方式例外列表

当“文档交换 (打开方式)”策略设置为“**受限**”时，此 Android Intent 列表允许传递到非托管应用。需要熟悉 Android Intent 才能向列表中添加筛选器。筛选器可以指定操作、包、方案或任意组合。

示例

```
{action=android.intent.action.MAIN}

{package=com.sharefile.mobile}

{action=android.intent.action.DIAL scheme=tel}

{action=android.intent.action.VIEW scheme=msteams
package=com.microsoft.teams}
```

注意

请务必考虑此策略的安全影响。例外列表允许内容在非托管应用和 MDX 环境之间传输。

入站文档交换 (打开方式)

阻止、限制或允许此应用的入站文档交换操作。如果设置为“**受限**”，则文档只能与其他 MDX 应用交换。默认值为“**不受限**”。

如果设置为“**已阻止**”或“**受限**”，您可以使用“入站文档交换白名单”策略来指定可向此应用发送文档的应用。有关其他策略交互的信息，请参阅“阻止图库”策略。

选项：**无限制、已阻止或受限**

入站文档交换白名单

当“入站文档交换”策略设置为受限或已阻止时，此逗号分隔的应用 ID 列表（包括非 MDX 应用）允许向该应用发送文档。此策略处于隐藏状态，无法编辑。

连接安全级别

确定连接使用的最低 TLS/SSL 版本。如果设置为 **TLS**，则连接支持所有 TLS 协议。如果设置为 **SSLv3 和 TLS**，则连接支持 SSL 3.0 和 TLS。默认值为 **TLS**。

应用限制

重要提示：

务必考虑阻止应用访问或使用手机功能的策略所带来的安全隐患。当这些策略设置为“**关闭**”时，内容可以在非托管应用和安全环境之间传输。

阻止相机

如果设置为“**启用**”，则阻止应用直接使用相机硬件。默认值为“**启用**”。

阻止图库

如果设置为“**启用**”，则阻止应用访问设备上的图库。默认值为“**禁用**”。此策略与“入站文档交换 (Open In)”策略协同工作。

- 如果“入站文档交换 (Open In)”设置为“**受限**”，则在托管应用中工作的用户无法从图库附加图像，无论“阻止图库”设置如何。
- 如果“入站文档交换 (Open In)”设置为“**无限制**”，则在托管应用中工作的用户会遇到以下情况：
 - 如果“阻止图库”设置为**关闭**，用户可以附加图像。
 - 如果“阻止图库”设置为**开启**，用户将无法附加图像。

阻止麦克风录音

如果设置为**开启**，则阻止应用直接使用麦克风硬件。默认值为**开启**。

阻止位置服务

如果设置为**开启**，则阻止应用使用位置服务组件（GPS 或网络）。Secure Mail 的默认值为**关闭**。

阻止短信撰写

如果设置为**开启**，则阻止应用使用用于从应用发送短信/文本消息的短信撰写功能。默认值为**开启**。

阻止屏幕捕获

如果设置为**开启**，则阻止用户在应用运行时进行屏幕捕获。此外，当用户切换应用时，会模糊应用屏幕。默认值为**开启**。

使用 Android 近场通信 (NFC) 功能时，某些应用会在传输内容之前截取自身的屏幕截图。要在封装应用中启用该功能，请将“**阻止屏幕捕获**”策略更改为**关闭**。

阻止设备传感器

如果设置为**开启**，则阻止应用使用设备传感器（例如加速计、运动传感器和陀螺仪）。默认值为**开启**。

阻止 NFC

如果设置为**开启**，则阻止应用使用近场通信 (NFC)。默认值为**开启**。

阻止应用日志

如果为“**开**”，则禁止应用使用移动生产力应用诊断日志记录功能。如果为“**关**”，则会记录应用日志，并且可以通过 Secure Hub 电子邮件支持功能进行收集。默认值为“**关**”。

阻止打印

如果为“**开**”，则阻止应用打印数据。如果应用具有“共享”命令，则必须将文档交换（打开方式）设置为“**受限**”或“**已阻止**”才能完全阻止打印。默认值为“**开**”。

启用 ShareFile

允许用户使用 ShareFile 传输文件。默认值为“**开**”。

应用网络访问

网络访问

注意：

“隧道式 - Web SSO”是设置中“安全浏览”的名称。行为相同。

设置选项如下：

- **使用以前的设置**：默认为您在早期策略中设置的值。如果更改此选项，则不得恢复为该选项。另请注意，新策略的更改在用户将应用升级到版本 18.12.0 或更高版本之前不会生效。
- **已阻止**：您的应用使用的网络 API 将失败。根据之前的指导原则，您必须妥善处理此类故障。
- **无限制**：所有网络调用都直接进行，不通过隧道。
- **隧道式 - 完全 VPN**：来自托管应用的所有流量都通过 Citrix Gateway 建立隧道。
- **隧道式 - Web SSO**：HTTP/HTTPS URL 会被重写。此选项仅允许 HTTP 和 HTTPS 流量的隧道传输。**隧道式 - Web SSO** 的一个显著优势是为 HTTP 和 HTTPS 流量提供单点登录 (SSO) 以及 PKINIT 身份验证。在 Android 上，此选项设置开销低，因此是 Web 浏览类型操作的首选选项。

如果选择其中一种**隧道模式**，则在此初始模式下会创建一个每应用 VPN 隧道，并将其连接回企业网络。此处使用 Citrix Gateway 分割隧道设置。Citrix 建议对使用客户端证书或端到端 SSL 连接到企业网络中资源的连接使用**隧道式完整 VPN**。Citrix 建议对需要单点登录 (SSO) 的连接使用**隧道式 - Web SSO**。

需要微型 VPN 会话

如果为**是**，则用户必须连接到企业网络并拥有活动会话。如果为**否**，则不需要活动会话。默认值为**使用上一个设置**。对于新上传的应用，默认值为**否**。在升级到此策略之前选择的任何设置都将保持有效，直到选择**使用上一个设置**以外的选项。

排除列表

以逗号分隔的 FQDN 或 DNS 后缀列表，这些 FQDN 或 DNS 后缀将直接访问，而不是通过 VPN 连接访问。此策略仅适用于 Citrix Gateway 配置为反向分割隧道模式时的**隧道式 - Web SSO** 模式。

阻止本地主机连接

如果为**开**，则不允许应用建立本地主机连接。本地主机是设备上本地通信的地址（例如 127.0.0.1）。本地主机绕过本地网络接口硬件并访问主机上运行的网络服务。如果为**关**，则此策略

将覆盖网络访问策略，这意味着如果设备在本地运行代理服务器，应用可以连接到安全容器外部。默认值为关。

证书标签

与 StoreFront™ 证书集成服务一起使用时，此标签标识此应用所需的特定证书。如果未提供标签，则不会提供证书以用于公钥基础设施 (PKI)。默认值为空（不使用证书）。

应用日志

默认日志输出

确定 Citrix Endpoint Management 应用诊断日志记录工具默认使用的输出介质。可能的值为文件、控制台或两者。默认值为文件。

默认日志级别

控制移动生产力应用诊断日志记录工具的默认详细程度。级别数字越高，日志记录越详细。

- 0 - 未记录任何内容
- 1 - 严重错误
- 2 - 错误
- 3 - 警告
- 4 - 信息性消息
- 5 - 详细信息性消息
- 6 到 15 - 调试级别 1 到 10

默认值为级别 **4**（信息性消息）。

最大日志文件数

限制移动生产力应用诊断日志记录工具在滚动更新前保留的日志文件数量。最小值为 **2**。最大值为 **8**。默认值为 **2**。

最大日志文件大小

限制移动生产力应用诊断日志记录工具在滚动更新前保留的日志文件大小（以 MB 为单位）。最小值为 **1 MB**。最大值为 **5 MB**。默认值为 **2 MB**。

重定向应用日志

如果设置为 **On**，则拦截并将来自应用的系统或控制台日志重定向到移动生产力应用诊断工具。如果此设置设置为 **Off**，则不会拦截应用对系统或控制台日志的使用。默认值为 **On**。

加密日志

如果为 **开**，Citrix Endpoint Management 会在记录诊断日志时对其进行加密。如果为 **关**，诊断日志在应用程序沙盒中保持未加密状态。

注意：

根据配置的日志级别，日志加密可能会对应用程序性能和电池续航时间产生显著影响。

默认值为 **关**。

应用程序地理围栏

中心点经度

应用程序受限运行的点/半径地理围栏中心点的经度（X 坐标）。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。该值必须以带符号的度数格式 (DDD.dddd) 表示，例如“-31.9635”。西经必须以负号开头。默认值为 **0**。

中心点纬度

应用程序受限运行的点/半径地理围栏中心点的纬度（Y 坐标）。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。

该值必须以带符号的度数格式 (DDD.dddd) 表示，例如“43.06581”。南纬必须以负号开头。默认值为 **0**。

半径

应用程序受限运行的地理围栏的半径。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。该值必须以米为单位表示。当设置为零时，地理围栏将被禁用。默认值为 **0**（禁用）。

分析

Google Analytics 详细信息

Citrix 收集分析数据以提高产品质量。选择“匿名”可选择不包含公司可识别信息。

应用设置

安全邮件 Exchange 服务器

Exchange 服务器的完全限定域名 (FQDN)，或者（仅限 iOS）IBM Notes Traveler 服务器的完全限定域名 (FQDN)。默认值为空。如果您在此字段中提供域名，用户将无法编辑它。如果将此字段留空，用户将提供自己的服务器信息。

注意：

如果您更改现有应用程序的此策略，用户必须删除并重新安装该应用程序才能应用策略更改。

Secure Mail 用户域

Exchange 用户或（仅限 iOS）Notes 用户的默认 Active Directory 域名。默认值为空。

后台网络服务

允许后台网络访问的服务地址的 FQDN 和端口。此值可以是 Exchange 服务器或 ActiveSync 服务器，位于您的内部网络中，或位于 Secure Mail 连接到的其他网络中，例如 mail.example.com:443。

如果您配置此策略，请将网络访问策略设置为**隧道连接到内部网络**。此策略在您配置网络访问策略时生效。当 Exchange 服务器位于您的内部网络中，并且您希望使用 NetScaler Gateway 代理连接到内部 Exchange 服务器时，请使用此策略。

默认值为空，这意味着后台网络服务不可用。

后台服务票证过期

后台网络服务票证保持有效的时间段。过期后，需要企业登录才能续订票证。默认值为 **168 小时**（7 天）。

后台网络服务网关

用于后台网络服务的备用网关地址，格式为 FQDN:port。此地址是 Secure Mail 用于连接到内部 Exchange 服务器的 Citrix Gateway FQDN 和端口号。在 Citrix Gateway 配置实用程序中，您必须配置安全票证颁发机构 (STA) 并将策略绑定到虚拟服务器。

默认值为空，表示不存在备用网关。

如果您配置此策略，请将“网络访问策略”设置为**隧道连接到内部网络**。此策略在您配置网络访问策略时生效。当 Exchange Server 位于您的内部网络中并且您希望使用 Citrix Gateway 代理连接到内部 Exchange Server 时，请使用此策略。

导出联系人

重要提示：

如果用户可以直接访问您的 Exchange Server（即在 Citrix Gateway 外部），请勿启用此功能。否则，联系人将在设备和 Exchange 中重复。

如果设置为“关”，则阻止 Secure Mail 联系人单向同步到设备，并阻止共享 Secure Mail 联系人（作为 vCard）。默认值为“关”。

要导出的联系人字段

控制要导出到通讯录的联系人字段。如果设置为“全部”，则导出所有联系人字段。如果设置为“姓名和电话”，则导出所有与姓名和电话相关的联系人字段。如果设置为“姓名、电话和电子邮件”，则导出所有与姓名、电话和电子邮件相关的联系人字段。默认值为“全部”。

接受所有 SSL 证书

如果设置为“开”，Secure Mail 将接受所有 SSL 证书（无论是否有效）并允许访问。如果设置为“关”，当发生证书错误时，Secure Mail 将阻止访问并显示警告。默认值为“关”。

使用安全连接

如果设置为“开”，Secure Mail 将使用安全连接。如果设置为“关”，Secure Mail 将不使用安全连接。默认值为“开”。

信息权限管理

如果设置为“开”，Secure Mail 将支持 Exchange 信息权限管理 (IRM) 功能。默认值为“关”。

控制锁定屏幕通知

控制邮件和日历通知是否显示在锁定的设备屏幕上。如果选择“允许”，则通知中包含的所有信息都会显示。如果选择“阻止”，则不显示通知。如果选择“电子邮件发件人或事件标题”，则仅显示电子邮件发件人的姓名或日历事件的标题。如果选择“仅计数”，则仅显示邮件和会议邀请的数量以及日历提醒的时间。默认值为“允许”。

默认同步间隔

指定 Secure Mail 的默认同步间隔。Secure Mail 用户可以更改默认值。

“Exchange ActiveSync 邮箱”策略设置“最大电子邮件保留期限筛选器”优先于此策略。如果您指定的默认同步间隔大于最大电子邮件保留期限筛选器，则将使用“最大电子邮件保留期限”筛选器设置。Secure Mail 仅显示小于“Active Sync 最大电子邮件保留期限”筛选器设置的同步间隔值。

默认值为“3 天”。

启用通过 Wi-Fi 下载附件

如果为“开”，则启用 Secure Mail 的“下载附件”选项，以使用户默认可以通过内部 Wi-Fi 网络下载附件。如果为“关”，则禁用 Secure Mail 的“下载附件”选项，以使用户默认无法通过 Wi-Fi 下载附件。默认值为“关”。

允许脱机文档

指定用户是否以及可以在设备上存储脱机文档多长时间。默认值为“无限制”。

启用电子邮件草稿自动保存

如果为“开”，则 Secure Mail 支持自动将邮件保存到“草稿”文件夹。默认值为“开”。

初始身份验证机制

此策略指示是使用 MDX 提供的邮件服务器地址填充首次使用预配屏幕上的“地址”字段，还是使用用户电子邮件地址。默认值为“邮件服务器地址”。

初始身份验证凭据

此策略定义必须选择的值作为用户名，以填充到初始首次使用预配屏幕中。默认值为“注册用户名”。

启用周数

如果设置为“开”，日历视图将包含周数。默认值为“关”。

电子邮件分类

如果设置为“开”，Secure Mail 支持 SEC（安全）和 DLM（传播限制标记）的电子邮件分类标记。分类标记在电子邮件标头中显示为 **X-Protective-Marking values**。请务必配置相关的电子邮件分类策略。默认值为“关”。

电子邮件分类标记

指定可供最终用户使用的分类标记。如果列表为空，Secure Mail 不会包含保护性标记列表。标记列表包含由分号分隔的值对。每对都包含在 Secure Mail 中显示的值以及在 Secure Mail 中附加到电子邮件主题和标头的标记值。例如，在标记对 `"UNOFFICIAL, SEC=UNOFFICIAL;"` 中，列表值为“UNOFFICIAL”，标记值为“SEC=UNOFFICIAL”。

电子邮件分类命名空间

指定所用分类标准在电子邮件标头中所需的分类命名空间。例如，命名空间“gov.au”在标头中显示为“NS=gov.au”。默认值为空。

电子邮件分类版本

指定所用分类标准在电子邮件标头中所需的分类版本。例如，版本“2012.3”在标头中显示为“VER=2012.3”。默认值为空。

默认电子邮件分类

指定如果用户未选择标记，Secure Mail 将应用于电子邮件的保护性标记。此值必须在“电子邮件分类标记”策略的列表中。默认值为 **UNOFFICIAL**。

邮件搜索限制

通过限制邮件服务器搜索中包含的天数，限制可从移动设备访问的邮件历史记录量。要限制同步到移动设备的邮件量，请配置“最大同步间隔”策略。默认值为“**无限制**”。

最大同步间隔

通过限制同步周期来控制移动设备上本地存储的邮件量。

要限制设备在邮件服务器上搜索的时间段，请配置“邮件服务器搜索限制”策略。

值包括：

- 3 天
- 1 周
- 2 周
- 1 个月
- 所有

默认值为 **所有**。

日历网络和音频选项

- **GoToMeeting 和用户输入** - 选择此选项后，用户可以选择要设置的会议类型。选项包括 GoToMeeting（打开 GoToMeeting 页面）和其他会议（允许用户手动输入会议信息）。
- **仅用户输入** - 选择此选项后，用户将直接转到“其他会议”页面，可在其中手动输入会议信息。

S/MIME 公共证书源

指定 S/MIME 公共证书的来源。如果为 **Exchange**，Secure Mail 将从 Exchange Server 获取证书。如果为 **LDAP**，Secure Mail 将从 LDAP 服务器获取证书。默认值为 **Exchange**。

LDAP 服务器地址

LDAP 服务器地址，包括端口号。默认值为空。

LDAP 基本 DN

LDAP 基本可分辨名称。默认值为空。

匿名访问 LDAP

如果此策略为“开”，Secure Mail 可以在未经事先身份验证的情况下搜索 LDAP。默认值为“关”。

允许的电子邮件域

以逗号分隔的格式定义允许的电子邮件域列表，例如 server.company.com,server.company.co.uk。默认值为空，这意味着 Secure Mail 不会筛选电子邮件域并支持所有电子邮件域。Secure Mail 将列出的域与电子邮件地址中的域名进行匹配。

例如，当 server.company.com 是列出的域名且电子邮件地址为 user@internal.server.company.com 时，Secure Mail 支持该电子邮件地址。

推送通知

启用基于 FCM 的邮箱活动通知。如果为“开”，Secure Mail 支持推送通知。默认值为“关”。

推送通知 EWS 主机名

为邮件托管 Exchange Web Services (EWS) 的服务器。该值必须是 EWS 的 URL 以及端口号。默认值为空。

推送通知区域

您的 Secure Mail 用户的 FCM 主机所在的区域。选项包括美洲、EMEA 和 PAC。默认值为美洲。

身份验证失败时尝试用户名迁移

此策略尝试将 Exchange 用户名迁移到 UPN 进行身份验证。默认值为 **Off**。

报告网络钓鱼邮件地址

如果已配置，您可以将可疑网络钓鱼邮件报告给指定的电子邮件地址或逗号分隔的电子邮件地址列表。默认值为空。如果您未配置此策略，则无法报告网络钓鱼邮件。

报告网络钓鱼机制

此策略指示用于报告可疑网络钓鱼邮件的机制。

- 通过附件 (.eml) 报告 – 将网络钓鱼邮件作为附件报告。该附件将发送到在“报告网络钓鱼邮件地址”策略中配置的电子邮件地址或逗号分隔的电子邮件地址列表。
- 通过转发报告 – 将网络钓鱼邮件作为转发报告。该邮件将转发到在“报告网络钓鱼邮件地址”策略中配置的电子邮件地址或逗号分隔的电子邮件地址列表。

注意：

此策略仅适用于 Microsoft Exchange 服务器。

默认值为“通过附件 (.eml) 报告”。

Skype for Business 会议域

此策略包含用于 Skype for Business 会议的逗号分隔域列表。Secure Mail 已处理具有以下 URL 前缀的会议：

- `https://join`
- `https://meet`
- `https://lync`

使用此策略，可以按 `https://*domain*` 形式添加其他 Skype for Business 域。域可以是字母数字字符串，不能包含任何特殊字符。请勿输入前面的 `https://` 或后面的点。

示例

如果策略值为 `customDomain1,customDomain2`，则 Skype for Business 支持的 URL 前缀为：

`https://customDomain1` `http://customDomain1` `https://customDomain2` `http://customDomain2`

默认值为空。

导出日历

此策略允许将 Secure Mail 日历事件导出到您的设备或个人日历。您可以在个人日历中查看事件。您可以使用 Secure Mail 编辑事件。默认值为 **会议时间**。

个人日历中显示的日历事件字段可使用以下 MDX 策略值：

- 无（不导出）
- 会议时间
- 会议时间、地点

- 会议时间、主题、地点
- 会议时间、可用性、与会者、主题、地点、备注

对 Office 365 的 OAuth 支持

对 O365 使用新式身份验证

如果此策略为 **开**，则 Secure Mail 在 Office 365 上配置帐户时使用 OAuth 协议进行身份验证。如果为 **关**，则 Secure Mail 使用基本身份验证。默认值为 **关**。

受信任的 Exchange Online 主机名

定义受信任的 Exchange Online 主机名列表，这些主机名在配置帐户时使用 OAuth 机制进行身份验证。此值采用逗号分隔格式，例如 `server.company.com`, `server.company.co.uk`。如果列表为空，则 Secure Mail 将使用基本身份验证进行帐户配置。默认值为 `outlook.office365.com`。

受信任的 AD FS 主机名

定义网页的受信任 AD FS 主机名列表，在 Office 365 OAuth 身份验证期间，密码会在这些网页中自动填充。此值采用逗号分隔格式，例如 `sts.companyname.com` , `sts.company.co.uk` 。如果列表为空，则 Secure Mail 不会自动填充密码。Secure Mail 会将列出的主机名与在 Office 365 身份验证期间遇到的网页主机名进行匹配，并检查该页面是否使用 HTTPS 协议。

例如，当 `sts.company.com` 是列出的主机名时，如果用户导航到 `https://sts.company.com` ，则如果页面有密码字段，Secure Mail 会填充密码。默认值为 `login.microsoftonline.com` 。

用于现代身份验证的自定义用户代理

此策略允许您更改用于现代身份验证的默认用户代理字符串。如果配置，此用户代理字符串将用于 Microsoft AD FS 身份验证。如果您未配置此策略，则在现代身份验证期间将使用默认的 Secure Mail 用户代理。

Slack 集成

启用 Slack

阻止或允许 Slack 集成。如果设置为“**开**”，Secure Mail 界面将包含 Slack 功能。如果设置为“**关**”，Secure Mail 界面将不包含 Slack 功能。

Slack 工作区名称

贵公司的 Slack 工作区名称。如果您提供名称，Secure Mail 会在登录时预填充工作区名称。如果您不提供名称，用户必须手动输入工作区名称 (`name.slack.com`)。

适用于 iOS 移动生产力应用的 MDX 策略

本文介绍了适用于 iOS 应用的 MDX 策略。您可以在 Citrix Endpoint Management 控制台中更改策略设置。有关详细信息，请参阅[添加应用](#)。

以下列表不包括 Secure Web 特有的 MDX 策略。有关 Secure Web 中显示的策略的详细信息，请参阅[Secure Web 策略](#)。

身份验证

设备密码

如果设置为“开”，则设备在启动或在一段时间不活动后恢复时，需要 PIN 或密码才能解锁。使用 Apple 文件加密对应用数据进行加密需要设备密码。设备上所有应用的数据都将加密。默认值为“关”。

应用密码

如果设置为“开”，则应用在启动或在一段时间不活动后恢复时，需要 PIN 或密码才能解锁。默认值为“开”。

要为所有应用配置不活动计时器，请在“设置”选项卡上的“客户端属性”中以分钟为单位设置 **INACTIVITY_TIMER** 值。默认不活动计时器值为 **60** 分钟。要禁用不活动计时器，以便仅在应用启动时显示 PIN 或密码提示，请将该值设置为零。

注意：

如果为“加密密钥”策略选择“安全脱机”，则此策略将自动启用。

最长脱机时间（小时）

定义应用在不重新确认应用授权和从不 Citrix Endpoint Management 刷新策略的情况下可以运行的最长时间。到期时，如果需要，可能会触发登录服务器。默认值为 **168** 小时（7 天）。最短时间为 **1** 小时。

备用思杰网关

注意：

此策略在 Endpoint Management 控制台名称为 **Alternate NetScaler® Gateway**。

用于此应用程序进行身份验证和微 VPN 会话的特定备用 Citrix Gateway 地址。此策略是可选的。当与“需要联机会话”策略一起使用时，此策略会强制应用程序重新向特定网关进行身份验证。此类网关通常具有不同的（更高保障的）身份验证要求和流量管理策略。如果留空，则始终使用服务器的默认网关。默认值为空。

设备安全性

阻止越狱或 Root 设备

如果设置为 **On**，则当设备越狱或 Root 时，应用程序将被锁定。如果设置为 **Off**，则即使设备越狱或 Root，应用程序也可以运行。默认值为 **On**。

网络要求

需要 Wi-Fi

如果设置为 **On**，则当设备未连接到 Wi-Fi 网络时，应用程序将被锁定。如果设置为 **Off**，则即使设备具有活动连接（例如 4G/3G、LAN 或 Wi-Fi 连接），应用程序也可以运行。默认值为 **Off**。

允许的 Wi-Fi 网络

逗号分隔的 Wi-Fi 网络列表。如果网络名称包含任何非字母数字字符（包括逗号），则名称必须用双引号括起来。应用程序仅在连接到所列网络之一时运行。如果为空，则允许所有网络。此值不影响蜂窝网络连接。默认值为空。

杂项访问

禁用强制升级

禁用要求用户升级到 App Store 中最新版本应用程序的设置。默认值为 **On**。

应用程序更新宽限期（小时）

定义系统发现应用程序更新可用后，应用程序可以继续使用的宽限期。默认值为 **168 小时（7 天）**。

注意：

建议不要使用零值。零值会立即阻止正在运行的应用程序使用，直到下载并安装更新（不向用户发出任何警告）。使用此值可能会导致用户被迫退出应用程序（可能会丢失工作）以遵守所需的更新。

锁定后擦除应用程序数据

应用程序锁定时擦除数据并重置应用程序。如果设置为“关”，则应用程序锁定时不会擦除应用程序数据。默认值为“关”。

应用程序可能因以下任何原因而被锁定：

- 用户失去应用程序授权
- 应用程序订阅已删除
- 帐户已删除
- Secure Hub 已卸载
- 应用程序身份验证失败次数过多
- 检测到越狱设备（根据策略设置）
- 设备因其他管理操作而处于锁定状态

活动轮询周期（分钟）

应用程序启动时，MDX Framework 会轮询 Citrix Endpoint Management 以确定当前应用程序和设备状态。假设可以访问运行 Endpoint Management 的服务器，该框架会返回有关设备的锁定/擦除状态以及应用程序的启用/禁用状态的信息。无论是否可以访问服务器，都会根据活动轮询周期间隔安排后续轮询。周期到期后，将再次尝试新的轮询。默认值为 **60 分钟**（1 小时）。

重要：

仅针对高风险应用降低此值，否则可能会影响性能。

加密

加密类型

允许您选择由 MDX 还是设备平台处理数据加密。如果选择 **MDX encryption**，则 MDX 加密数据。如果选择 **Platform encryption with compliance enforcement**，则设备平台加密数据。默认值为 **MDX encryption**。

不合规设备行为

允许您选择设备不符合最低加密合规性要求时的操作。选择 **Allow app** 以使应用程序正常运行。选择 **Allow app after warning** 以使应用程序在警告出现后运行。选择 **Block** 以阻止应用程序运行。默认值为 **Allow app after warning**。

启用 MDX 加密

如果为 **Off**，则设备上存储的数据不加密。如果为 **On**，则设备上存储的数据已加密。默认值为 **On**。

注意：

如果在部署应用程序后更改此策略，用户必须重新安装该应用程序。

数据库加密排除项

未自动加密的数据库排除列表。要阻止对特定数据库进行加密，请将条目添加到此逗号分隔的正则表达式列表中。如果数据库路径名与任何正则表达式匹配，则该数据库将从加密中排除。排除模式支持 Posix 1003.2 扩展正则表达式语法。模式匹配不区分大小写。

示例

`\\.db$,\\.sqlite$` 排除以 `.db` 或 `.sqlite` 结尾的任何数据库路径名。

`\\Database\\unencrypteddb\\.db` 匹配 Database 子文件夹中的数据库 unencrypteddb.db。

`\\Database\\` 匹配其路径中包含 `/Database/` 的所有数据库。

默认值为空。

文件加密排除项

未自动加密的文件排除列表。要阻止对特定文件集进行加密，请将条目添加到此逗号分隔的正则表达式列表中。如果文件路径名与任何正则表达式匹配，则该文件将从加密中排除。排除模式支持 Posix 1003.2 扩展正则表达式语法。模式匹配不区分大小写。

示例

`\\.log$,\\.dat$` 排除以 `.log` 或 `.dat` 结尾的任何文件路径名。

`\\Documents\\unencrypteddoc\\.txt` 匹配 Documents 子文件夹中文件 unencrypteddoc.txt 的内容。

`\\Documents\\UnencryptedDocs\\*.txt` 匹配子路径 /Documents/UnencryptedDocs/ 下的“.txt”文件。

默认值为空。

应用交互

剪切和复制

阻止、允许或限制此应用的剪贴板剪切和复制操作。如果设置为 **Restricted**，则复制的剪贴板数据将放置在仅 MDX 应用可用的私有剪贴板中。默认值为 **Restricted**。

粘贴

阻止、允许或限制此应用的剪贴板粘贴操作。如果设置为 **Restricted**，则粘贴的剪贴板数据将源自仅 MDX 应用可用的私有剪贴板。默认值为 **Unrestricted**。

文档交换（在以下位置打开）

阻止、允许或限制此应用的文档交换操作。如果为 **受限**，则文档只能与其他 MDX 应用交换。

如果为 **无限制**，请将“启用加密”策略设置为 **开**，以使用户可以在未封装的应用中打开文档。如果接收应用未封装或已禁用加密，Citrix Endpoint Management 会解密文档。默认值为 **受限**。

受限的“打开方式”例外列表

当“文档交换(打开方式)”策略为 **受限** 时，MDX 应用可以与此逗号分隔的非托管应用 ID 列表共享文档。即使“文档交换(打开方式)”策略为 **受限** 且“启用加密”为 **开**，此规则也适用。默认例外列表允许 Office 365 应用：

com.microsoft.Office.Word,com.microsoft.Office.Excel,com.microsoft.Office.Powerpoint,
com.microsoft.onenote,com.microsoft.onenoteiPad,com.microsoft.Office.Outlook

只有 Office 365 应用支持此策略。

注意：

务必考虑此策略的安全隐患。例外列表允许内容在非托管应用和 MDX 环境之间传输。

连接安全级别

确定用于连接的 TLS/SSL 的最低版本。如果为 **TLS**，则连接支持所有 TLS 协议。如果为 **SSLv3** 和 **TLS**，则连接支持 SSL 3.0 和 TLS。默认值为 **TLS**。

入站文档交换(打开方式)

阻止、限制或允许此应用的入站文档交换操作。如果为 **受限**，则文档只能与其他 MDX 应用交换。默认值为 **无限制**。

如果为 **已阻止** 或 **受限**，您可以使用“入站文档交换白名单”策略指定可向此应用发送文档的应用。

选项：无限制、已阻止 或 受限

应用 URL 方案

iOS 应用程序可以将 URL 请求分派给已注册处理特定方案（例如“`http://`”）的其他应用程序。此功能提供了一种机制，使应用程序能够将帮助请求传递给另一个应用程序。此策略用于筛选传递到此应用程序进行处理的方案（即入站 URL）。默认值为空，这意味着所有已注册的应用程序 URL 方案都将被阻止。

策略必须格式化为逗号分隔的模式列表，其中每个模式前面都有一个加号“+”或减号“-”。入站 URL 将按照列出的顺序与模式进行比较，直到找到匹配项。一旦匹配，前缀将决定采取的操作。

- 减号“-”前缀会阻止 URL 传递到此应用程序。
- 加号“+”前缀允许 URL 传递到应用程序进行处理。
- 如果模式中未提供“+”或“-”，则假定为“+”（允许）。
- 如果入站 URL 与列表中的任何模式都不匹配，则该 URL 将被阻止。

下表包含应用程序 URL 方案的示例：

方案	需要 URL 方案的应用程序	用途
<code>ctxmobilebrowser</code>	安全 Web-	允许 Secure Web 处理来自其他应用程序的 HTTP: URL。 -
<code>ctxmobilebrowsers</code>	安全 Web-	允许 Secure Web 处理来自其他应用的 HTTPS: URL。
<code>ctxmail</code>	安全邮件-	允许 Secure Mail 处理来自其他应用的 <code>mailto:</code> URL。
COL-G2M	GoToMeeting-	允许封装的 GoToMeeting 应用处理会议请求。
<code>ctxsalesforce</code>	适用于 Salesforce 的 Citrix -	允许 Citrix for Salesforce 处理 Salesforce 请求。
<code>wbx</code>	WebEx	允许封装的 WebEx 应用处理会议请求。

应用交互（出站 URL）

从 URL 筛选中排除的域

此策略将出站 URL 从任何“允许的 URL”筛选中排除。添加逗号分隔的完全限定域名 (FQDN) 或 DNS 后缀列表，以从“允许的 URL”筛选中排除。如果此策略为空（默认值），则定义的“允许的 URL”筛选进程为 URL。如果此策略包含任何条目，则主机字段与列表中至少一个项目匹配（通过 DNS 后缀匹配）的 URL 将未经修改地发送到 iOS。此通信绕过“允许的 URL”筛选逻辑。默认值为空。

允许的 URL

iOS 应用可以将 URL 请求分派给已注册以处理特定方案（例如 `"http://"`）的其他应用。此功能提供了一种机制，使应用可以将帮助请求传递给另一个应用。此策略用于筛选从本应用传递给其他应用进行处理的 URL（即出站 URL）。

该策略必须格式化为逗号分隔的模式列表，其中每个模式前面可能带有加号“+”或减号“-”。出站 URL 将按照列出的顺序与模式进行比较，直到找到匹配项。一旦匹配，前缀将决定采取的操作。减号“-”前缀会阻止 URL 传递给其他应用。加号“+”前缀允许 URL 传递给其他应用进行处理。如果模式未提供“+”或“-”，则假定为“+”（允许）。由“=”分隔的一对值表示替换，其中第一个字符串的出现将被第二个字符串替换。您可以使用正则表达式“^”前缀搜索字符串，以将其锚定到 URL 的开头。如果出站 URL 与列表中的任何模式都不匹配，则会被阻止。

默认值

`+maps.apple.com`

`+itunes.apple.com`

`\^http:=ctxmobilebrowser::`

`\^https:=ctxmobilebrowsers::`

`\^mailto:=ctxmail::`

`+\\^citrixreceiver::`

`+\\^telprompt::`

`+\\^tel::`

`+\\^lmi-g2m::`

`+\\^maps:ios_addr`

- +\\^mapitem: :
- +\\^sms: :
- +\\^facetime: :
- +\\^ctxnotes: :
- +\\^ctxnotesex: :
- +\\^ctxtasks: :
- +\\^facetime-audio: :
- +\\^itms-apps: :
- +\\^ctx-sf: :
- +\\^sharefile: :
- +\\^lync: :
- +\\^slack: :
- +\\^msteams: :

如果设置为空白，所有 URL 都将被阻止，以下情况除外：

- http: :
- https: :
- +citrixreceiver: +tel: :

下表包含允许的 URL 示例：

URL 格式	描述
\\^mailto:=ctxmail:	所有 mailto: URL 都在 Secure Mail 中打开。
\\^http:	所有 HTTP URL 都在 Secure Web 中打开。
\\^https:	所有 HTTPS URL 都在 Secure Web 中打开。
\\^tel:	允许用户拨打电话。

URL 格式	描述
<code>-//www.dropbox.com</code>	阻止从托管应用分发的 Dropbox URL。
<code>+\\^COL-G2M:</code>	允许托管应用打开 GoToMeeting 客户端应用。
<code>-\\^SMS:</code>	阻止使用消息聊天客户端。
<code>-\\^wbx:</code>	阻止托管应用打开 WebEx 客户端应用。
<code>+\\^ctxsalesforce:</code>	允许 Citrix for Salesforce 与您的 Salesforce 服务器通信。

允许的安全 Web 域

此策略仅影响会将 URL 重定向到 Secure Web 应用程序的“允许的 URL”策略条目 (`\\^http://ctxmobilebrowser:` 和 `\\^https://ctxmobilebrowsers:`)。添加以逗号分隔的完全限定域名 (FQDN) 或允许重定向到 Secure Web 应用程序的 DNS 后缀列表。如果此策略为空 (默认值)，则所有域都可以重定向到 Secure Web 应用程序。如果此策略包含任何条目，则只有主机字段与列表中至少一个项目匹配 (通过 DNS 后缀匹配) 的 URL 才会重定向到 Secure Web 应用程序。所有其他 URL 将未经修改地发送到 iOS，绕过 Secure Web 应用程序。默认值为空。

应用程序限制

重要提示：

请务必考虑阻止应用程序访问或使用手机功能的策略所带来的安全隐患。当这些策略处于 **Off** 状态时，内容可以在非托管应用程序和安全环境之间传输。

阻止摄像头

如果设置为 **On**，则阻止应用程序直接使用摄像头硬件。默认值为 **OFF**。

阻止照片库

如果设置为 **开**，则阻止应用访问设备上的照片库。默认值为 **开**。

阻止麦克风录音

如果设置为 **开**，则阻止应用直接使用麦克风硬件。默认值为 **开**。

阻止听写

如果设置为开，则阻止应用直接使用听写服务。默认值为开。

阻止定位服务

如果设置为开，则阻止应用使用定位服务组件（GPS 或网络）。对于 Secure Mail，默认值为关。

阻止短信撰写

如果设置为开，则阻止应用使用短信撰写功能从应用发送短信/文本消息。默认值为开。

阻止电子邮件撰写

如果设置为开，则阻止应用使用电子邮件撰写功能从应用发送电子邮件。默认值为开。

阻止 iCloud

如果设置为开，则阻止应用使用 iCloud 存储和共享设置及数据。

注意

iCloud 数据文件由“阻止文件备份”策略控制。

默认值为“开”。

阻止查找

如果设置为“开”，则阻止应用程序使用“查找”功能，该功能可在词典、iTunes、App Store、电影放映时间、附近位置等中搜索突出显示的文本。默认值为“开”。

阻止文件备份

如果设置为“开”，则阻止 iCloud 或 iTunes 备份数据文件。默认值为“开”。

阻止隔空打印

如果设置为“开”，则阻止应用程序使用隔空打印功能将数据打印到支持隔空打印的打印机。默认值为“开”。

阻止隔空投送

如果设置为“开”，则阻止应用程序使用隔空投送。默认值为“开”。

阻止文件附件

注意

此策略在 iOS 11 或更高版本上强制执行。

如果设置为“开”，则禁用附件处理。默认值为“关”。

阻止 Facebook 和 Twitter API

如果设置为 开，阻止应用程序使用 iOS Facebook 和 Twitter API。默认值为 开。

模糊屏幕内容

如果设置为 开，当用户切换应用程序时，屏幕内容会被模糊处理。此策略可防止 iOS 录制屏幕内容和显示缩略图。默认值为 开。

阻止第三方键盘 (仅限 iOS 11 及更高版本)

如果设置为 开，阻止应用程序使用 iOS 8+ 上的第三方键盘扩展。默认值为 开。

阻止应用程序日志

如果设置为 开，禁止应用程序使用移动生产力应用程序诊断日志记录功能。如果设置为 关，应用程序日志将被记录，并且可以通过 Secure Hub 电子邮件支持功能进行收集。默认值为 关。

启用 ShareFile

允许用户使用 ShareFile 传输文件。默认值为 开。

启用从文件附加

允许用户从 iOS 文件应用程序添加附件。默认值为 开。

应用程序网络访问

网络访问

注意：

Tunneled - Web SSO 是设置中 Secure Browse 的名称。其行为相同。

设置选项如下：

- **已阻止**：所有网络访问均已阻止。您的应用使用的网络 API 将失败。根据之前的指南，您必须妥善处理此类故障。
- **无限制**：所有网络调用都直接进行，不进行隧道传输。
- **隧道 - Web SSO**：HTTP/HTTPS URL 将被重写。此选项仅允许 HTTP 和 HTTPS 流量的隧道传输。**隧道 - Web SSO** 的一个显著优势是 HTTP 和 HTTPS 流量的单点登录 (SSO) 以及 PKINIT 身份验证。在 Android 上，此选项的设置开销较低，因此是 Web 浏览类型操作的首选选项。

如果您正在使用**隧道 - 完全 VPN** 或**隧道 - 完全 VPN 和 Web SSO** 策略，则必须切换到**隧道 - Web SSO** 策略。如果您继续使用已弃用的策略，您的电子邮件将无法同步。

注意：

如果您正在使用**隧道 - 完全 VPN** 并且已配置安全票证颁发机构 (STA)，则现代身份验证屏幕将无法加载。

需要微型 VPN 会话

如果为**是**，则用户必须连接到企业网络并具有活动会话。如果为**否**，则不需要活动会话。默认值为**使用以前的设置**。对于新上传的应用，默认值为**否**。在升级到此新策略之前选择的任何设置都将保持有效，直到选择**使用以前的设置**以外的选项。

需要微型 VPN 会话的宽限期（分钟）

此值确定用户可以使用应用多少分钟，然后“需要在线会话”策略会阻止他们继续使用（直到在线会话经过验证）。默认值为 **0**（无宽限期）。此策略不适用于与 Microsoft Intune/EMS 的集成。

证书标签

与 StoreFront™ 证书集成服务一起使用时，此标签标识此应用所需的特定证书。如果未提供标签，则不会提供证书以用于公钥基础结构 (PKI)。默认值为空（不使用证书）。

排除列表

以逗号分隔的 FQDN 或 DNS 后缀列表，这些 FQDN 或 DNS 后缀将直接访问，而不是通过 VPN 连接访问。此值仅适用于 Citrix Gateway 配置为反向拆分隧道模式时的**隧道 - Web SSO** 模式。

应用日志

默认日志输出

确定移动生产力应用诊断日志记录功能默认使用的输出介质。可能的值为文件、控制台或两者。默认值为**文件**。

默认日志级别

控制移动生产力应用诊断日志记录功能的默认详细程度。每个级别都包含较低级别的值。可能的级别范围包括：

- 0 - 不记录任何内容
- 1 - 严重错误
- 2 - 错误
- 3 - 警告
- 4 - 信息性消息
- 5 - 详细信息性消息
- 6 到 15 - 调试级别 1 到 10

默认值为级别 4（信息性消息）。

最大日志文件数

限制移动生产力应用诊断日志记录功能在滚动之前保留的日志文件数量。最小值为 2。最大值为 8。默认值为 2。

最大日志文件大小

限制移动生产力应用程序诊断日志记录工具在滚动更新之前保留的日志文件大小（以 MB 为单位）。最小值为 1 MB。最大值为 5 MB。默认值为 2 MB。

应用程序地理围栏

中心点经度

应用程序受限运行的点/半径地理围栏中心点的经度（X 坐标）。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。

该值必须以带符号的度数格式 (DDD.dddd) 表示，例如“-31.9635”。西经必须以负号开头。默认值为 0。

中心点纬度

应用程序受限运行的点/半径地理围栏中心点的纬度（Y 坐标）。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。

该值必须以带符号的度数格式 (DDD.dddd) 表示，例如“43.06581”。南纬必须以负号开头。默认值为 0。

半径

应用程序受限运行的地理围栏半径。当在配置的地理围栏之外运行时，应用程序将保持锁定状态。

该值必须以米为单位表示。设置为零时，地理围栏将被禁用。当“阻止位置服务”策略启用时，地理围栏无法正常工作。默认值为 **0**（已禁用）。

启用谷歌分析

如果设置为“开”，Citrix 会收集匿名数据以提高产品质量。如果设置为“关”，则不收集任何数据。默认值为“开”。

分析

Google Analytics 详细程度

Citrix 收集分析数据以提高产品质量。选择**匿名**可选择不包含公司可识别信息。默认值为“完整”。

报告

Citrix 报告

如果设置为开，Citrix 会收集崩溃报告和诊断信息以帮助解决问题。如果设置为关，Citrix 不会收集数据。

注意

Citrix 也可能通过功能标志控制此功能。此功能要正常运行，功能标志和此策略都必须启用。

默认值为关。

上传令牌

您可以从 Citrix Insight Services (CIS) 帐户获取上传令牌。如果您指定此可选令牌，CIS 将允许您访问从设备上传的崩溃报告和诊断信息。Citrix 可以访问相同的信息。默认值为空。

仅通过 Wi-Fi 发送报告

如果设置为开，Citrix 仅在您连接到 Wi-Fi 网络时发送崩溃报告和诊断信息。默认值为开。

报告文件缓存最大值

限制在清除缓存之前保留的崩溃报告和诊断捆绑包的大小。最小值为 1 MB。最大值为 5 MB。默认值为 2 MB。

应用程序交互

显式注销通知

如果设置为**禁用**，则在用户注销期间不会激活应用程序。如果设置为**仅限共享设备**，则仅当设备配置为共享设备时，应用程序才会在用户注销期间激活。Secure Mail 的默认设置为**仅限共享设备**。

应用程序设置

安全邮件 Exchange 服务器

Exchange Server 的完全限定域名 (FQDN)，或者（仅限 iOS）IBM Notes Traveler 服务器的完全限定域名。默认值为空。如果您在此字段中提供域名，则用户无法对其进行编辑。如果您将此字段留空，则用户将提供自己的服务器信息。

注意

如果您更改现有应用程序的此策略，用户必须删除并重新安装该应用程序才能应用策略更改。

Secure Mail 用户域

Exchange 用户或（仅限 iOS）Notes 用户的默认 Active Directory 域名。默认值为空。

后台网络服务

允许后台网络访问的服务地址的 FQDN 和端口。此值可能是 Exchange Server 或 ActiveSync 服务器，位于您的内部网络中，或位于 Secure Mail 连接到的其他网络中，例如 mail.example.com:443。

如果配置此策略，请将“网络访问策略”设置为**隧道连接到内部网络**。此策略在您配置网络访问策略时生效。当 Exchange Server 位于您的内部网络中并且您希望使用 Citrix Gateway（以前称为 NetScaler Gateway）代理到内部 Exchange Server 的连接时，请使用此策略。

默认值为空，这意味着后台网络服务不可用。

后台服务票证过期

后台网络服务票证的有效期。过期后，需要企业登录才能续订票证。默认值为**168 小时**（7 天）。

后台网络服务网关

用于后台网络服务的备用网关地址，格式为 `fqdn:port`。此值是 Secure Mail 用于连接内部 Exchange Server 的 Citrix Gateway FQDN 和端口号。在 Citrix Gateway 配置实用程序中，您必须配置安全票证颁发机构 (STA) 并将策略绑定到虚拟服务器。默认值为空，表示不存在备用网关。

如果配置此策略，请将“网络访问”策略设置为“**隧道连接到内部网络**”。此策略在您配置网络访问策略时生效。当 Exchange Server 位于您的内部网络中，并且您希望使用 Citrix Gateway 代理连接到内部 Exchange Server 时，请使用此策略。

导出联系人

重要提示：

如果用户可以直接访问您的 Exchange Server（即在 Citrix Gateway 外部），请勿启用此功能。否则，设备和 Exchange 中会创建重复联系人。

如果设置为“关”，则阻止 Secure Mail 联系人单向同步到设备以及共享 Secure Mail 联系人（作为 vCard）。默认值为“关”。

要导出的联系人字段

控制要导出到通讯录的联系人字段。如果设置为“**全部**”，则导出所有联系人字段。如果设置为“**姓名和电话**”，则导出所有与姓名和电话相关的联系人字段。如果设置为“**姓名、电话和电子邮件**”，则导出所有与姓名、电话和电子邮件相关的联系人字段。

默认值为“**全部**”。

接受所有 SSL 证书

如果设置为“**开**”，Secure Mail 将接受所有 SSL 证书（无论是否有效）并允许访问。如果设置为“**关**”，Secure Mail 将在发生证书错误时阻止访问并显示警告。

默认值为“**关**”。

控制锁定屏幕通知

控制邮件和日历通知是否显示在锁定的设备屏幕上。如果设置为“**允许**”，则显示通知中包含的所有信息。如果设置为“**阻止**”，则不显示通知。如果设置为“**电子邮件发件人或事件标题**”，则仅显示电子邮件发件人姓名或日历事件标题。如果设置为“**仅计数**”，则显示邮件和会议邀请的计数以及日历提醒的时间。默认值为“**允许**”。

默认电子邮件通知

如果设置为“开”，Secure Mail 会显示电子邮件的锁定屏幕通知。默认值为“开”。

默认同步间隔

指定 Secure Mail 的默认同步间隔。Secure Mail 用户可以更改默认值。**Exchange ActiveSync 邮箱策略**设置“**最大电子邮件保留期限筛选器**”优先于此策略。如果指定的默认同步间隔大于最大电子邮件保留期限筛选器，则使用“**最大电子邮件保留期限筛选器**”设置。

Secure Mail 仅显示小于“**Active Sync 最大电子邮件保留期限筛选器**”设置的同步间隔值。

默认值为“3 天”。

邮件搜索限制

通过限制邮件服务器搜索中包含的天数，限制可从移动设备访问的邮件历史记录量。默认值为“**无限制**”。

要限制同步到移动设备的邮件量，请配置“**最大客户端同步周期**”策略。

最大同步间隔

通过限制同步周期来控制本地存储在移动设备上的邮件量。默认值为“**所有**”。要限制设备可在邮件服务器上搜索的时间段，请配置“**邮件服务器搜索限制**”策略。

启用周数

如果设置为“开”，日历视图将包含周数。默认值为“关”。

启用通过 Wi-Fi 下载附件

如果设置为“开”，则启用 Secure Mail 的“下载附件”选项，以使用户默认可以通过允许的内部 Wi-Fi 网络下载附件。如果设置为“关”，则禁用 Secure Mail 的“下载附件”选项，以使用户默认无法通过 Wi-Fi 下载附件。

默认值为“关”。

允许脱机文档

指定用户是否以及可以在设备上存储脱机文档多长时间。默认值为“**无限制**”。

信息权限管理

如果设置为“开”，Secure Mail 支持 Exchange 信息权限管理 (IRM) 功能。默认值为“关”。

电子邮件分类

如果设置为“开”，Secure Mail 支持 SEC（安全）和 DLM（传播限制标记）的电子邮件分类标记。分类标记在电子邮件标头中显示为“X-Protective-Marking”值。请务必配置相关的电子邮件分类策略。

默认值为“关”。

电子邮件分类标记

指定要提供给用户的分类标记。如果列表为空，Secure Mail 不会包含保护性标记列表。标记列表包含由分号分隔的值对。每对都包含在 Secure Mail 中显示的值以及作为附加到 Secure Mail 中电子邮件主题和标头的文本的标记值。例如，在标记对“UNOFFICIAL,SEC=UNOFFICIAL;”中，列表值为“UNOFFICIAL”，标记值为“SEC=UNOFFICIAL”。

电子邮件分类命名空间

指定所用分类标准在电子邮件标头中要求的分类命名空间。例如，命名空间“gov.au”在标头中显示为“NS=gov.au”。

默认值为空。

电子邮件分类版本

指定所用分类标准在电子邮件标头中要求的分类版本。例如，版本“2012.3”在标头中显示为“VER=2012.3”。

默认值为空。

默认电子邮件分类

指定如果用户未选择标记，Secure Mail 将应用于电子邮件的保护性标记。此值必须在“电子邮件分类标记”策略的列表中。

默认值为 **UNOFFICIAL**。

启用电子邮件草稿自动保存

如果为 **开**，Secure Mail 支持自动将邮件保存到“草稿”文件夹。

默认值为 **开**。

初始身份验证机制

此策略指示是使用 MDX 提供的邮件服务器地址还是用户的电子邮件地址，在首次使用预配屏幕上填充“地址”字段。

默认值为“**邮件服务器地址**”。

初始身份验证凭据

此策略定义必须选择作为用户名的值，以填充到初始首次使用预配屏幕中。

默认值为“**注册用户名**”。

启用用户名的自动填充

如果启用，用户名将自动填充到帐户预配用户界面中。默认值为 **ON**。

启用 iOS 数据保护

注意：

此策略适用于必须满足澳大利亚信号局 (ASD) 计算机安全要求的企业。

在处理文件时启用 iOS 数据保护。如果设置为“**开**”，则指定在应用沙盒中创建和打开文件时的文件保护级别。默认值为“**关**”。

推送通知 EWS 主机名

托管用于邮件的 Exchange Web Services (EWS) 的服务器。该值必须是 EWS 的 URL 以及端口号。默认值为空。

推送通知

启用基于 APNs 的邮箱活动通知。如果设置为“**开**”，Secure Mail 将支持推送通知。

默认值为“**关**”。

推送通知区域

Secure Mail 用户 APNs 主机所在的区域。选项包括“**美洲**”、“**EMEA**”和“**亚太地区**”。默认值为“**美洲**”。

S/MIME 公共证书源

指定 S/MIME 证书的来源。如果设置为“**电子邮件**”，则必须将用户证书通过电子邮件发送给用户，然后用户在 Secure Mail 中打开电子邮件并导入附加的证书。

如果设置为“**共享保管库**”，则受支持的数字身份提供商会将证书提供给 Secure App 共享保管库。与第三方提供商的集成要求您向用户发布相关应用程序。有关用户体验的详细信息，请参阅“首次启动 Secure Mail 时启用 S/MIME”策略的说明。

默认值为“电子邮件”。

首次启动 Secure Mail 时启用 S/MIME

确定 Secure Mail 是否在首次启动 Secure Mail 时启用 S/MIME，前提是 S/MIME 证书源策略为 **共享保管库**。如果设置为 **开**，则当共享保管库中存在用户证书时，Secure Mail 会启用 S/MIME。如果共享保管库中没有证书，系统会提示用户导入证书。在这两种情况下，用户都必须先从受支持的数字身份提供商应用配置证书，然后才能在 Secure Mail 中创建帐户。

如果设置为 **关**，Secure Mail 不会启用 S/MIME，用户可以在 Secure Mail 设置中启用它。默认值为 **关**。

日历 Web 和音频选项

- **GoToMeeting 和用户输入**：用户可以选择他们想要设置的会议类型。选项包括 **GoToMeeting**（打开 GoToMeeting 页面）和 **其他会议**（允许用户手动输入会议信息）。
- **仅用户输入**：用户将直接转到“其他会议”页面，在那里他们可以手动输入会议信息。

S/MIME 公共证书源

指定 S/MIME 公共证书的来源。如果为 **Exchange**，Secure Mail 会从 Exchange Server 获取证书。如果为 **LDAP**，Secure Mail 会从 LDAP 服务器获取证书。默认值为 **Exchange**。

LDAP 服务器地址

LDAP 服务器地址，包括端口号。默认值为空。

LDAP 基本 DN

LDAP 基本专有名称。默认值为空。

匿名访问 LDAP

如果此策略设置为 **开**，Secure Mail 可以在未经事先身份验证的情况下搜索 LDAP。默认值为 **关**。

允许的电子邮件域

定义允许的电子邮件域列表，采用逗号分隔格式，例如

server.company.com,server.company.co.uk。默认值为空，这意味着 Secure Mail 不会筛选电子邮件域并支持所有电子邮件域。Secure Mail 将列出的域与电子邮件地址中的域名进行匹配。例如，当 server.company.com 是列出的域名，并且电子邮件地址是 user@internal.server.company.com 时，Secure Mail 支持该电子邮件地址。

尝试在身份验证失败时迁移用户名

尝试将 Exchange 用户名迁移到 UPN 进行身份验证。默认值为 **Off**。

报告网络钓鱼邮件地址

如果已配置，您可以将可疑网络钓鱼邮件报告给指定的电子邮件地址或逗号分隔的电子邮件地址列表。默认值为空。如果您未配置此策略，将无法报告网络钓鱼邮件。

报告网络钓鱼机制

此策略指示用于报告可疑网络钓鱼邮件的机制。

- **通过附件报告**：将网络钓鱼邮件作为附件报告。附件将发送到在“报告网络钓鱼邮件地址”策略中配置的电子邮件地址或逗号分隔的电子邮件地址列表。
- **通过转发报告**：将网络钓鱼邮件作为转发报告。邮件将转发到在“报告网络钓鱼邮件地址”策略中配置的电子邮件地址或逗号分隔的电子邮件地址列表。

注意：

此策略仅适用于 Microsoft Exchange Server。

默认值为 **通过附件报告**。

Skype for Business 会议域

此策略包含用于 Skype for Business 会议的逗号分隔域列表。

Secure Mail 已处理具有以下 URL 前缀的会议：

- `https://join`
- `https://meet`
- `https://lync`

通过此策略，可以添加其他 Skype for Business 域，形式为 `https://*domain*`。域可以是字母数字字符的字符串，不能包含任何特殊字符。不要输入前面的 `https://` 或后面的点。

示例：

如果策略值为 **customDomain1,customDomain2**，则 Skype for Business 支持的 URL 前缀为：

- `https://customDomain1`
- `http://customDomain1`

- `https://customDomain2`
- `http://customDomain2`

默认值为空。

导出日历

此策略允许将 Secure Mail 日历事件导出到您的设备或个人日历。您可以在个人日历中查看事件。您可以使用 Secure Mail 编辑事件。默认值为 **Meeting Time**。

以下 MDX 策略值可用于显示在您的个人日历中的日历事件字段：

- 无（不导出）
- 会议时间
- 会议时间、地点
- 会议时间、主题、地点
- 会议时间、主题、地点、备注

来电显示

如果设置为“开”，Secure Mail 会将您已保存联系人的姓名和联系电话提供给 iOS，用于来电显示。此数据仅用于识别和显示来自您已保存的 Secure Mail 联系人列表的来电详细信息。默认值为“开”。

Office 365 的 OAuth 支持

Office 365 身份验证机制

此策略指示在 Office 365 上配置帐户时用于身份验证的 OAuth 机制。

- **不使用 OAuth**：不使用 OAuth，Secure Mail 使用基本身份验证进行帐户配置。
- **使用带用户名和密码的 OAuth**：用户必须提供其用户名和密码，并且可以选择提供 MFA 代码以进行 OAuth 流程。
- **使用带客户端证书的 OAuth**：用户使用客户端证书对 OAuth 流程进行身份验证。

默认值为“不使用 OAuth”。

受信任的 Exchange Online 主机名

定义一个受信任的 Exchange Online 主机名列表，这些主机名在配置帐户时使用 OAuth 机制进行身份验证。此值采用逗号分隔格式，例如 server.company.com, server.company.co.uk。如果列表为空，Secure Mail 将使用基本身份验证进行帐户配置。默认值为 **outlook.office365.com**。

受信任的 AD FS 主机名

定义一个受信任的 AD FS 主机名列表，用于在 Office 365 OAuth 身份验证期间自动填充密码的网页。此值采用逗号分隔格式，例如 sts.companyname.com, sts.company.co.uk。如果列表为空，Secure Mail 不会自动填充密码。Secure Mail 会将列出的主机名与 Office 365 身份验证期间遇到的网页主机名进行匹配，并检查该页面是否使用 HTTPS 协议。例如，当 sts.company.com 是列出的主机名，并且用户导航到 `https://sts.company.com` 时，如果页面包含密码字段，Secure Mail 会填充密码。默认值为 **login.microsoftonline.com**。

邮件重定向

邮件重定向

阻止或限制任何邮件撰写。Secure Mail 将邮件撰写重定向到 Secure Mail。如果设置了帐户，本机邮件会将邮件撰写重定向到本机邮件。默认值为 **Secure Mail**。

Slack 集成

启用 Slack

阻止或允许 Slack 集成。如果设置为 **ON**，Secure Mail 界面将包含 Slack 功能。如果设置为 **OFF**，Secure Mail 界面将不包含 Slack 功能。默认值为 **OFF**。

Slack 工作区名称

贵公司的 Slack 工作区名称。如果您提供名称，Secure Mail 会在登录时预填充工作区名称。如果您不提供名称，用户必须键入工作区名称 (name.slack.com)。默认值为空。

按平台划分的功能

下表总结了 Citrix 移动生产力应用程序的功能。X 表示该功能适用于该平台。有关 QuickEdit 中的功能，请参阅 [Citrix QuickEdit](#)。

Citrix 安全中心™

功能	IOS	安卓
登录以进行身份验证	X	X
监控策略合规性	X	X
访问应用程序和桌面	X	X
HDX™ 应用程序和桌面	X	X
创建并发送问题日志	X	X
将屏幕截图附加到日志	X	X
在应用程序内联系帮助台	X	X
在应用程序内联系 Citrix® 支持	X	X
崩溃收集和分析	X	X
离线身份验证	X	X
使用 Citrix Secure Mail™ 发送日志	X	X
Google 分析	X	X
纵向和横向模式	X	X
应用内信任应用指南	X	X

功能	IOS	安卓
通过电子邮件注册时，自动注册 Secure Mail（仅限 MAM）	X	X
Touch ID 离线身份验证	X	X
使用派生凭据注册	X	
生物特征身份验证		X
使用 Workspace 应用商店	X	X

思杰安全邮件

功能	IOS	安卓
电子邮件效率		
最小化草稿	X	X
撤销已发送邮件		X
加密管理	X	X
日历议程小组件		X
Secure Mail 中的联系人图片	X	X
支持响应式电子邮件	X	X
草稿文件夹自动同步	X	X
附件在草稿文件夹中同步		X
发送、接收、回复、全部回复、转发邮件	X	X
创建、编辑、删除草稿	X	X
标记邮件	X	X
标记为未读	X	X

功能	IOS	安卓
查看所有文件夹和子文件夹	X	X
应用置于后台时自动保存草稿	X	X
借助 Citrix Secure Notes 将电子邮件转为笔记。 重要提示： Secure Notes 已于 December 31, 2018 达到生命周期终止 (EOL) 状态。有关详细信息，请参阅 EOL 和 已弃用应用 。	X	X
搜索邮件（本地和服务端）	X	X
选择邮件同步周期（最长 1 个月或所有邮件）	X	X
查看未读邮件	X	X
安全地查看/播放图像、视频和音频附件	X	X
多个附件	X	X
回复和转发附件	X	X
从 Citrix Files 附加文件	X	X
从 Citrix Files 受限区域和连接器附加文件	X	X
附件存储库	X	X
富文本编辑	X	X
邮件通知，带主题，锁屏预览	X	X
从通知屏幕回复和删除邮件及邀请	X	
附加或拍摄照片	X	X
选择多封邮件	X	X

功能	IOS	安卓
下载附件	X	X
内联加载图片	X	X
快速排序	X	X
发送、接收、打开和保存 .zip 文件附件	X	X
纵向和横向模式	X；适用于邮件列表、邮件阅读、撰写、日历和联系人视图	X：仅适用于邮件阅读和撰写视图
粘贴文本保留格式	X	X
来自联系人的短信	X	X
来自联系人的 FaceTime	X	
因连接问题或邮箱已满而未发送的邮件存储在发件箱中	X	X
最近使用的文件夹浮现		X
下拉刷新邮件	X	X
上次刷新时间戳	X	X
向左滑动以执行邮件操作	X	X
支持微软易捷和 IBM 笔记旅行者	X	X
轻按以刷新邮件、日历和联系人	X	X
在邮件视图中遵循设备辅助功能/字体大小设置	X	X
S/MIME 签名和加密	X	X
通过电子邮件导入 S/MIME 证书	X	X

功能	IOS	安卓
S/MIME, Intercede 集成	X	
S/MIME, Entrust 集成	X	
针对邮件正文的 Microsoft IRM 保护	X	X
推送通知	X	X
推送到收件箱的通知会自动更新所有文件夹, 包括日历	X	
打开 Office 365 文档	X	X
3D Touch 操作	X	
锁定屏幕上的上下文图标	X	X
搜索文件夹	X	X
VIP 邮件文件夹	X	X
动态字体支持	X	X
保持文件夹展开	X	X
邮件分类标记	X	X
拼写检查	X	
附加最后拍摄的照片	X	X
URL 预览	X	X
在 Citrix Files 中打开 Citrix Files 链接	X	X
支持 <code>.pass</code> 文件	X	
在搜索模式下选择多封电子邮件	X	X

功能	IOS	安卓
内联插入图像	X	X
升级到 Exchange ActiveSync (EAS) 版本 16	X	X
限制用户使用未知或个人域	X	
支持超宽设备屏幕		X
配置多个 Exchange 帐户	X	X
向左或向右滑动以执行更多操作	X	X
加密对加密邮件的回复或转发	X	
打印电子邮件和内联图像	X	
在“设置”中使用“预览行”来配置电子邮件正文在邮箱视图中显示为预览的行数	X	
支持响应式电子邮件	X	X
附件（MS Office 或图像）的应用内预览	X	X
个人联系人组	X	X
将用户名迁移到电子邮件地址 (UPN)	X	X
报告网络钓鱼电子邮件	X	X
现代身份验证 (OAuth)	X	X
打印附件	X	
Android 企业版 (Android 工作版)	X	
富文本签名	X	

功能	IOS	安卓
富推送通知	X	
动态	X	X
照片附件改进	X	X
群组通知	X	
Slack 集成（预览版）	X	X
管理动态	X	
内部域	X	X
管理您的订阅源	X	X
MS Teams 集成	X	X
自诊断 (Troubleshoot) 选项		X
双模式 (MAM SDK)	X	X
自诊断工具		X
日历		
预览并导入 ICS 文件作为日历事件		X
拖放日历事件	X	X
日、周、月和议程视图	X	X
锁屏上的详细提醒	X	X
同步六个月	X	X
将事件设置为私人	X	X
滚动到第一个事件前一小时	X	
手动刷新选项	X	X

功能	IOS	安卓
设置提醒	X	X
点击以映射地址	X	X
周数	X	X
动态字体支持	X	X
安全分类标记	X	X
长按地址	X	
设置工作周开始日期	X	X
将视图聚焦到所选日期的周	X	
始终突出显示当前日期	X	X
来自附件存储库的日历附件	X	X
个人日历支持	X	X
显示与个人日历事件的冲突		X
打印日历事件	X	
点击日历主题行中的电话号码和网址	X	
搜索日历	X	
会议		
回复、全部回复、转发会议	X	X
组织者查看邀请回复	X	X
组织者查看受邀者的可用性以及建议的可用时间	X	X
轻按以加入在线会议。 注意： 对于 WebEx 和 Lync，您必须在 Citrix Endpoint	X	X

功能	IOS	安卓
Management™ 中配置策略才能启用这些应用程序。		
轻按以加入音频会议	X	X
在新邀请中安排在线会议、音频会议、电话会议	X	X
将 ShareFile 链接添加到新邀请	X	X
转发带附件的邀请	X	X
点击发送“迟到”电子邮件	X	X
点击回复会议组织者	X	X
轻按以回复所有会议邀请	X	X
轻按以回复所有会议受邀者	X	X
轻按以回复所有带附件的会议受邀者	X	X
拨入 GoToMeeting	X	X
从锁定屏幕或通知屏幕回复邀请	X	X
拨入 WebEx 或 Lync 会议	X	X
隐藏已拒绝的事件	X	X
显示 3 个以上同时发生的事件	X	X
快速查看受邀者状态	X	X
删除、回复、全部回复、对已取消的事件添加评论	X	X
在转发的邀请中显示组织者姓名	X	X

功能	IOS	安卓
共享设备	X	X
加入 Skype for Business 会议	X	X
响应会议通知，例如接受、拒绝和暂定。	X	X
通过“回复”和“删除”响应消息通知	X	
联系人		
在 联系人 中创建文件夹		X
双向联系人同步	X	X
详细联系人信息 GAL 搜索	X	X
将 Secure Mail 联系人导出并同步到本地联系人	X	X
联系人：收藏和类别		X
控制导出哪些联系人字段	X	X
非安全邮件联系人详细信息	X	X
动态类型支持	X	X
将联系人标记为 VIP	X	X
与 .vcards 共享联系人	X	X
长按查看联系人		X
即使存在本机邮件帐户，也可导出联系人	X	X
查看文件夹和子文件夹	X	
设备上配置的设置		

功能	IOS	安卓
iMessage 支持	X	
控制通知的高级选项	X	X
锁屏通知控制	X	X
邮件和日历通知声音	X	X
自动刷新文件夹	X	X
设置内部和外部外出通知	X	X
删除前询问	X	X
会话视图或按时间顺序视图	X	X
在 Wi-Fi 上加载附件	X	X
将 Wi-Fi 上加载附件设为默认	X	X
设置邮件同步周期	X	X
无限同步/同步所有邮件		X
设置电子邮件签名	X	X
按名字或姓氏列出联系人	X	X
自动前进	X	X
使用本地时区		X
快速回复模板		X
推送邮件配置频率		X
导出/导入设置	X	X
点击设备上的返回按钮以关闭 浮动操作按钮选项		X
微软 Teams	X	X

Citrix 安全 Web™

功能	IOS	安卓
使用多任务同时运行两个应用程序	X	
下载文件	X	X
添加收藏夹	X	X
清除已保存的用户名和密码	X	X
删除缓存/历史记录/Cookie	X	X
阻止弹出窗口	X	X
保存离线页面	X	X
在地址栏中搜索	X	X
从通知中打开下载的项目	X	X
密码自动保存	X	X
代理支持		
企业代理	X	X
URL 阻止列表和允许列表	X	X
历史记录	X	X
默认主页	X	X
选项卡	X	X
推送书签	X	X
阻止屏幕截图		X
在当前页面中搜索	X	X
3D Touch 操作	X	

功能	IOS	安卓
共享设备	X	X
共享设备的文件防篡改保护	X	
导出/导入设置	X	X
纵向和横向模式	X	X
安卓企业版 (安卓企业版)		X
下拉刷新屏幕内容	X	X
Secure Web 作为默认浏览器		X

功能标志管理

为确保功能标志下的功能正常运行，您需要为 URL `features.netscalergateway.net` 启用流量。

功能标志用于动态启用或禁用功能。如果在生产环境中移动生产力应用程序出现问题，即使功能已发布，也可以动态禁用受影响的功能。为此，我们使用 Citrix 管理的功能标志。

除了防火墙或代理阻止出站流量的情况外，无需手动配置即可启用功能管理的流量。在这种情况下，您需要根据策略要求使用特定的 URL 或 IP 地址启用流量。

IP 地址

如果您必须在允许列表中列出 IP 地址，请包含以下 IP 地址以允许流量流向

`features.netscalergateway.net`：

- 57.153.121.183（适用于欧洲西部区域）
- 172.202.161.151（适用于美国中南部区域）
- 48.218.128.128（适用于日本东部区域）

您可以添加这些 IP 地址，以确保您的防火墙配置与基础设施更新保持同步自动更新。

系统要求

如果使用 NetScaler Gateway 且分流隧道设置为 **OFF**，请确保 NetScaler 可以通过端口 443 解析并连接到 `features.netscalergateway.net`。

下表列出了支持功能标志管理的移动生产力应用程序的最低版本。

移动生产力应用程序	操作系统	支持的最低版本
安全中心	安卓	24.8.0 及更高版本
安全中心	iOS	24.9.0 及更高版本
MAM SDK	安卓	24.9.0 及更高版本

移动生产力应用程序	操作系统	支持的最低版本
MAM SDK	iOS	24.7.1 及更高版本
安全邮件	安卓、iOS	24.9.0 及更高版本
安全网页	安卓	24.8.0 及更高版本
安全网页	iOS	24.9.0 及更高版本

Citrix 安全中心™

Citrix Secure Hub 是 Citrix Endpoint Management™（以前称为 XenMobile）体验的启动平台。用户在 Secure Hub 中注册其设备以访问应用商店。通过应用商店，他们可以添加 Citrix 开发的移动生产力应用程序和第三方应用程序。

有关 Secure Hub 和其他移动生产力应用程序的系统要求，请参阅[系统要求](#)。

管理 Secure Hub

您在 Endpoint Management 的初始配置期间执行与 Secure Hub 相关的大部分管理任务。要向用户提供 Secure Hub，对于 iOS 和 Android，请将 Secure Hub 上传到 iOS App Store 和 Google Play Store。

除了提供 Citrix 应用程序门户之外，当用户使用 Citrix Gateway 身份验证后，其 Citrix Gateway 会话续订时，Secure Hub 还会刷新存储在 Endpoint Management 中用于已安装应用程序的大多数 MDX 策略。

重要提示：

对以下任何策略的更改都要求用户删除并重新安装应用程序以应用更新后的策略：安全组、启用加密和 Secure Mail Exchange Server。

Citrix 个人识别码

您可以将 Secure Hub 配置为使用 Citrix PIN，这是一项在 Endpoint Management 控制台的**设置 > 客户端属性**中启用的安全功能。此设置要求已注册的移动设备用户登录 Secure Hub 并通过使用个人识别码 (PIN) 激活任何 MDX 封装的应用程序。

Citrix PIN 功能简化了用户在登录受保护的封装应用程序时的身份验证体验。用户无需重复输入其他凭据，例如其 Active Directory 用户名和密码。

首次登录 Secure Hub 的用户必须输入其 Active Directory 用户名和密码。登录期间，Secure Hub 会将 Active Directory 凭据或客户端证书保存在用户设备上，然后提示用户输入 PIN。当用户再次登录时，他们输入 PIN 以安全地访问其 Citrix 应用程序和应用商店，直到活动用户会话的下一个空闲

超时期限结束。相关的客户端属性使您能够使用 PIN 加密密钥、指定 PIN 的密码类型以及指定 PIN 强度和长度要求。有关详细信息，请参阅[客户端属性](#)。

启用指纹身份验证后，当由于应用程序不活动而需要脱机身份验证时，用户可以使用指纹登录。用户仍然需要输入 PIN，例如首次登录 Secure Hub 时、重新启动设备时以及不活动计时器到期后。有关启用指纹身份验证的信息，请参阅[指纹或触控 ID 身份验证](#)。

证书锁定

适用于 iOS 和 Android 的 Secure Hub 支持 SSL 证书锁定。此功能可确保在 Citrix 客户端与 Endpoint Management 通信时使用您的企业签名的证书。当设备上安装的根证书危及 SSL 会话时，证书锁定可阻止客户端连接到 Endpoint Management。当 Secure Hub 检测到服务器公钥的任何更改时，Secure Hub 会拒绝连接。

从 Android N 开始，操作系统不再允许用户添加的证书颁发机构 (CA)。Citrix 建议使用公共根 CA 代替用户添加的 CA。

如果用户使用私有或自签名 CA，升级到 Android N 的用户可能会遇到问题。在以下情况下，Android N 设备上的连接会中断：

- 私有/自签名 CA，并且 AutoDiscovery Service 中的 Endpoint Management 所需受信任 CA 选项设置为 **ON**。有关详细信息，请参阅 [Endpoint Management AutoDiscovery Service](#)。
- 私有/自签名 CA，并且 AutoDiscovery Service (ADS) 不可访问。出于安全考虑，当 ADS 不可访问时，即使最初设置为 **OFF**，所需受信任 CA 也会变为 **ON**。

在注册设备或升级 Secure Hub 之前，请考虑启用证书锁定。此选项默认处于 **关闭** 状态，由 Endpoint Management Auto Discovery Service (ADS) 管理。启用证书锁定后，用户无法使用自签名证书注册到 Endpoint Management。如果用户尝试使用自签名证书注册，系统会警告他们该证书不受信任。如果用户不接受证书，注册将失败。

要使用证书锁定，请请求 Citrix 将证书上传到 Citrix ADS 服务器。使用 [Citrix 支持门户](#) 打开技术支持案例。然后，提供以下信息：

- 包含用户将注册的帐户的域。
- Endpoint Management 完全限定域名 (FQDN)。
- Endpoint Management 实例名称。默认情况下，实例名称为 zdm 且区分大小写。
- 用户 ID 类型，可以是 UPN 或电子邮件。默认情况下，类型为 UPN。
- 如果您将端口号从默认端口 8443 更改，则用于 iOS 注册的端口。
- 如果您将端口号从默认端口 443 更改，则 Endpoint Management 接受连接的端口。

- 您的 Citrix Gateway 的完整 URL。
- （可选）您的 Endpoint Management 管理员的电子邮件地址。
- 您希望添加到域的 PEM 格式证书。

为 Secure Hub 配置证书 + 一次性密码身份验证

您可以配置 Citrix ADC，以便 Secure Hub 使用证书和用作一次性密码的安全令牌进行身份验证。此配置提供了一种强大的安全选项，不会在设备上留下 Active Directory 足迹。

要使 Secure Hub 能够使用此类身份验证，请在 Citrix ADC 中添加一个重写操作和重写策略，以插入形式为 **X-Citrix-AM-GatewayAuthType: CertAndRSA** 的自定义响应标头，以指示 Citrix Gateway 登录类型。

通常，Secure Hub 使用在 Endpoint Management 控制台中配置的 Citrix Gateway 登录类型。但是，在 Secure Hub 首次完成登录之前，此信息对 Secure Hub 不可用。因此，需要自定义标头才能允许 Secure Hub 执行此操作。

注意：

如果在 Endpoint Management 和 Citrix ADC 中设置了不同的登录类型，则 Citrix ADC 配置将覆盖该配置。有关详细信息，请参阅 [Citrix Gateway and Endpoint Management](#)。

1. 在 Citrix ADC 中，导航到 **配置 > AppExpert > 重写 > 操作**。
2. 单击 **Add**。

出现 **Create Rewrite Action** 屏幕。

3. 填写下图所示的每个字段，然后单击 **Create**。

Create Rewrite Action

Name*

InsertGatewayAuthTypeHeader

Type*

INSERT_HTTP_HEADER

Use this action type to insert a header.

Header Name*

X-Citrix-AM-GatewayAuthType

Expression

Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

"CertAndRSA"

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

Create

Close

以下结果显示在主 Rewrite Actions 屏幕上。

NetScaler > AppExpert > Rewrite > Rewrite Actions

Add Edit Delete Action

Show built-in Rewrite Actions Search

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\/'+'window.location.pathname.split('\')[1]+'\'+'wi...	re~a.substr(0,3).toLowerCase()\ =~"%2A")a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

4. 将重写操作作为重写策略绑定到虚拟服务器。转到 **Configuration > NetScaler® Gateway > Virtual Servers**，然后选择您的虚拟服务器。

Dashboard Configuration Reporting Documentation Downloads

+ System

+ AppExpert

+ Traffic Management

+ Optimization

+ Security

NetScaler Gateway

Global Settings

Virtual Servers

Portal Themes

+ User Administration

KCD Accounts

+ Policies

+ Resources

+ Authentication

Show Unlicensed Features

Integrate with Citrix Products

XenMobile

XenApp and XenDesktop

Unified Gateway

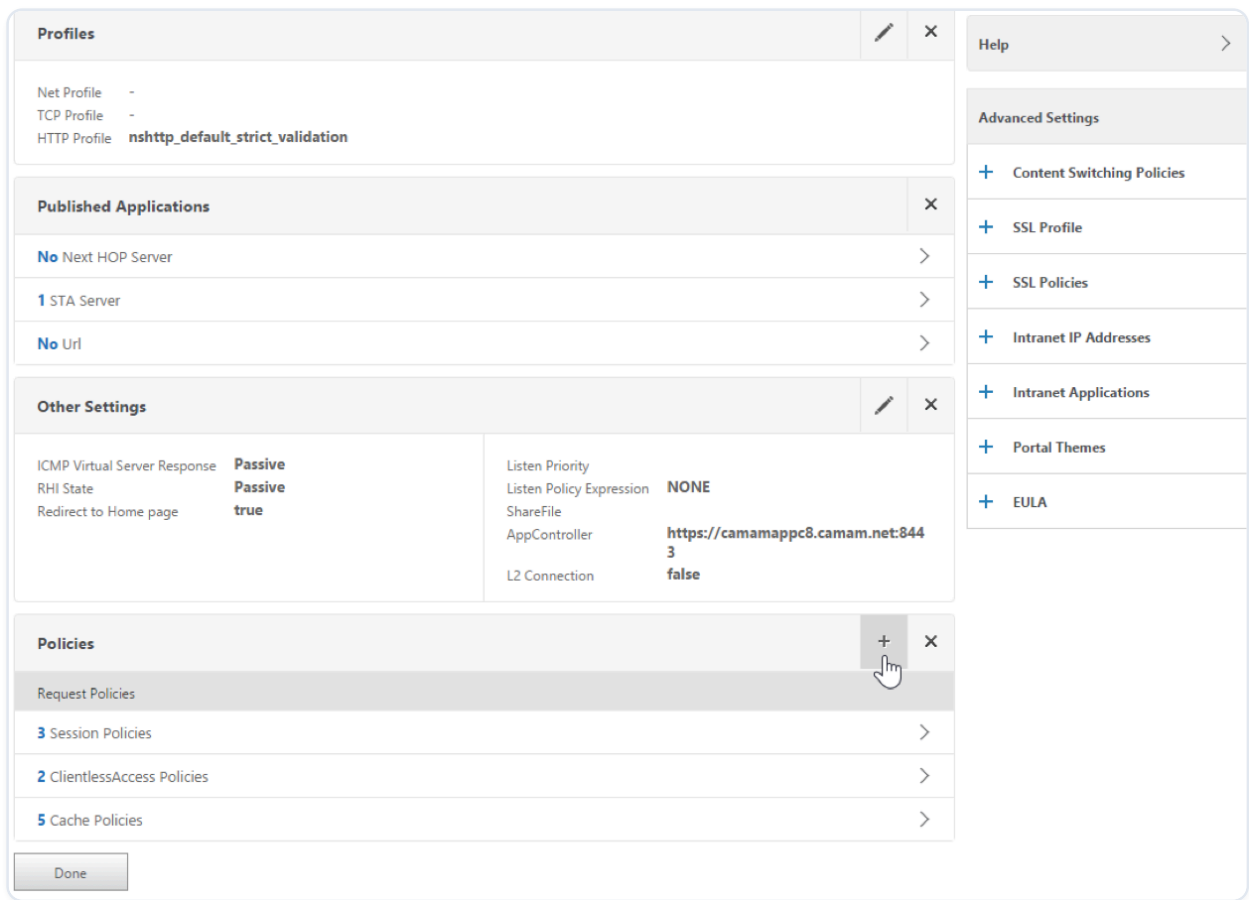
NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

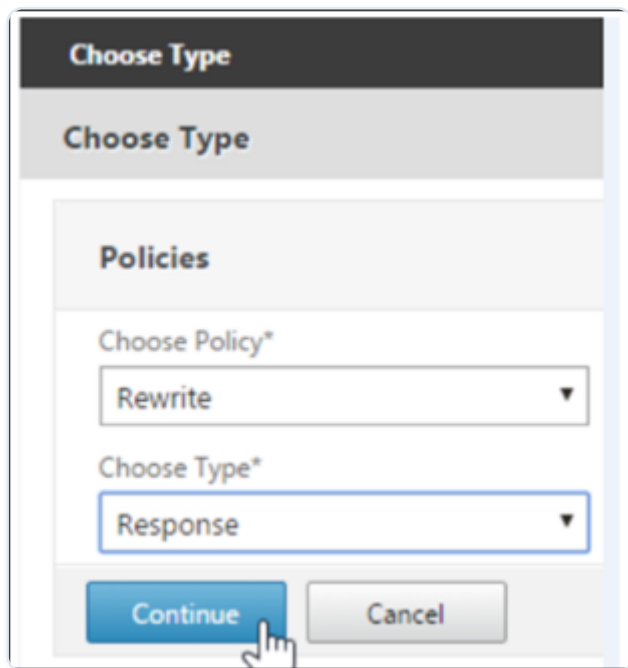
Search

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users	Total Connected Users
_XM_gwcamamappc8	Up	10.71.12.30	443	SSL	0	3	3
SessionTransfer	Up	10.71.12.30	500	SSL	0	0	0

- 5. 点击 **编辑**。
- 6. 在 **虚拟服务器配置** 屏幕上，向下滚动到 **策略**。
- 7. 点击 **+ 添加策略**。



- 8. 在 **选择策略** 字段中，选择 **重写**。
- 9. 在 **选择类型** 字段中，选择 **响应**。



10. 点击 **继续**。

策略绑定 部分展开。

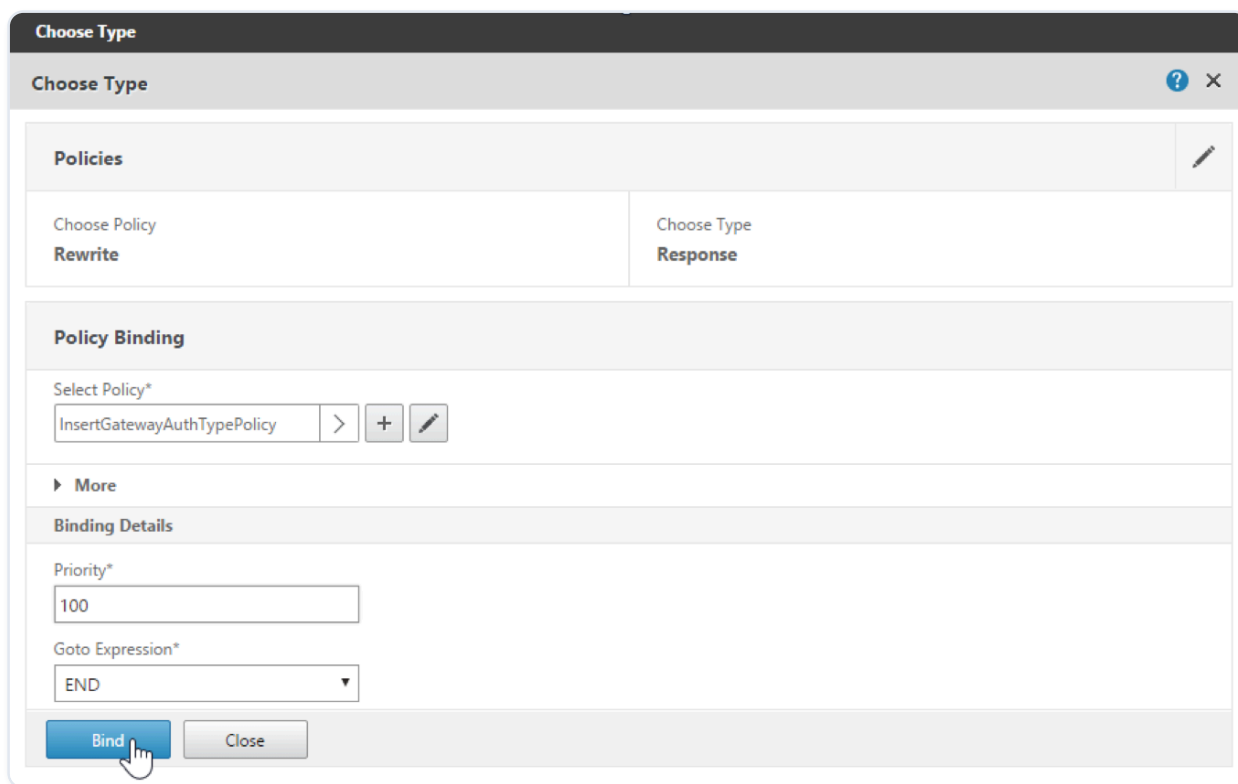
The screenshot shows a 'Choose Type' dialog box. It has a title bar 'Choose Type' with a close button. Below the title bar, there's a 'Choose Type' section with two tabs: 'Choose Policy' and 'Choose Type'. Under 'Choose Policy', 'Rewrite' is selected. Under 'Choose Type', 'Response' is selected. Below this is a 'Policy Binding' section with a 'Select Policy*' dropdown menu. A hand cursor is pointing to the dropdown. To the right of the dropdown are three icons: a plus sign, a pencil, and a question mark. Below the dropdown is a 'Binding Details' section with a 'Priority*' input field containing '100' and a 'Goto Expression*' dropdown menu set to 'END'. At the bottom are 'Bind' and 'Close' buttons.

11. 点击 **选择策略**。

出现一个包含可用策略的屏幕。

The screenshot shows a 'Rewrite Policies' screen. It has a title bar 'Choose Type > Rewrite Policies' with a help icon and a close button. Below the title bar, there's a 'Rewrite Policies' section with a 'Select' button highlighted by a hand cursor. To the right of the 'Select' button are buttons for 'Add', 'Edit', 'Delete', 'Show Bindings', 'Policy Manager', and 'Statistics'. There's also an 'Action' dropdown menu and a 'Show built-in Rewrite Policies' link. Below these buttons is a table with columns: Name, Expression, Action, Undefined-Result Action, Hits, Undefined Hits, and Active. The first row is selected, showing 'InsertGatewayAuthTypePolicy' with a 'true' expression and 'InsertGatewayAuthTypeHeader' action. The table also shows 'Use Global' for Undefined-Result Action, '0' for Hits, and '0' for Undefined Hits. There's a search bar and a close button at the bottom right.

12. 点击您刚刚创建的策略行，然后点击 **选择**。**策略绑定** 屏幕再次出现，其中已填入您选择的策略。



13. 点击 **Bind**。

如果绑定成功，将显示主配置屏幕，其中显示已完成的重写策略。

成功绑定的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-bind-successful.png)

14. 要查看策略详细信息，请点击 **Rewrite Policy**。

重写策略详细信息的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policy.png)

适用于 Android 设备的 ADS 连接端口要求

端口配置可确保从 Secure Hub 连接的 Android 设备可以从公司网络内部访问 Citrix ADS。在下载通过 ADS 提供的安全更新时，访问 ADS 的能力非常重要。ADS 连接可能与您的代理服务器不兼容。在这种情况下，请允许 ADS 连接绕过代理服务器。

重要提示：

适用于 Android 和 iOS 的 Secure Hub 要求您允许 Android 设备访问 ADS。有关详细信息，请参阅 Endpoint Management 文档中的[端口要求](#)。请注意，此通信通过出站端口 443 进行。您的现有环境很可能已设计为允许此访问。强烈建议无法保证此通信的客户不要升级到 Secure Hub 10.2。如果您有任何疑问，请联系 Citrix 支持。

要启用证书锁定，您必须完成以下先决条件：

- 收集 Endpoint Management 和 Citrix ADC 证书。证书必须采用 PEM 格式，并且必须是公共证书，而不是私钥。
- 联系 Citrix 支持并提交启用证书锁定的请求。在此过程中，系统会要求您提供证书。

新的证书锁定改进要求设备在注册之前连接到 ADS。这可确保 Secure Hub 能够获取设备注册所在环境的最新安全信息。如果设备无法访问 ADS，Secure Hub 将不允许设备注册。因此，在内部网络中开放 ADS 访问对于启用设备注册至关重要。

要允许适用于 Android 的 Secure Hub 访问 ADS，请为以下 IP 地址和 FQDN 打开端口 443：

完全限定域名	IP 地址	端口	IP 和端口使用情况
<code>discovery.mdm.ze nprise.com</code>	52.5.138.94	443	Secure Hub - ADS 通 信
<code>discovery.mdm.ze nprise.com</code>	52.1.30.122	443	Secure Hub - ADS 通 信
<code>ads.xm.cloud.com</code> ：请注意， SecureHub 10.6.15 及更高版本使用 <code>ads.xm.cloud.com</code> 。	34.194.83.188	443	Secure Hub - ADS 通 信
<code>ads.xm.cloud.com</code> ：请注意， SecureHub 10.6.15 及更高版本使用 <code>ads.xm.cloud.com</code> 。	34.193.202.23	443	Secure Hub - ADS 通 信

如果启用了证书锁定：

- Secure Hub 在设备注册期间锁定您的企业证书。
- 在升级期间，Secure Hub 会丢弃所有当前锁定的证书，然后在已注册用户首次连接时锁定服务器证书。

注意：

如果在升级后启用证书锁定，用户必须重新注册。

- 证书续订不需要重新注册，前提是证书公钥未更改。

证书锁定支持叶证书，不支持中间证书或颁发者证书。证书锁定适用于 Citrix 服务器（例如 Endpoint Management 和 Citrix Gateway），而不适用于第三方服务器。

Secure Hub 功能

Secure Hub 允许您监控和实施移动策略，同时提供对 Store 和实时支持的访问。用户首先从 Apple、Android 或 Windows 应用商店将 Secure Hub 下载到其设备上。

Secure Hub 打开后，用户输入公司提供的凭据，以在 Secure Hub 中注册其设备。有关设备注册的更多详细信息，请参阅[用户、帐户、角色和注册](#)。

在 Android 版 Secure Hub 上，在首次安装和注册期间，会出现以下消息：允许 Secure Hub 访问您设备上的照片、媒体和文件吗？

请注意，此消息来自 Android 操作系统，而非 Citrix。当您点击**允许**时，Citrix 和管理 Secure Hub 的管理员不会在任何时候查看您的个人数据。但是，如果您与管理员进行远程支持会话，管理员可以在会话中查看您的个人文件。

注册后，用户将在其**我的应用**选项卡中看到您推送的任何应用和桌面。用户可以从应用商店添加更多应用。在手机上，应用商店链接位于左上角的“设置”汉堡图标下。

应用商店链接的图像(/en-us/mobile-productivity-apps/media/secure-hub-settings.png)

在平板电脑上，应用商店是一个单独的选项卡。

平板电脑上应用商店的图像(/en-us/mobile-productivity-apps/media/secure-hub-ipad-myapps.png)

当运行 iOS 9 或更高版本的 iPhone 用户从 Endpoint Management 应用商店安装移动生产力应用时，他们会看到一条消息，指出企业开发者 Citrix 在该 iPhone 上不受信任，并且在开发者受信任之前，该应用将无法使用。当此消息出现时，Secure Hub 会提示用户查看一份指南，指导他们完成信任其 iPhone 上的 Citrix 企业应用的过程。

对于仅限 MAM 的部署，您可以配置 Endpoint Management，以便使用电子邮件凭据注册 Secure Hub 的 Android 或 iOS 设备用户自动注册 Secure Mail。用户无需输入更多信息或执行更多步骤即可注册 Secure Mail。

首次使用 Secure Mail 时，Secure Mail 会从 Secure Hub 获取用户的电子邮件地址、域和用户 ID。Secure Mail 使用电子邮件地址进行自动发现。Exchange 服务器通过域和用户 ID 进行识别，这使得 Secure Mail 能够自动验证用户。如果策略设置为不传递密码，系统会提示用户输入密码，但用户无需输入任何其他信息。

要启用此功能，请创建三个属性：

- 服务器属性 MAM_MACRO_SUPPORT。有关说明，请参阅[服务器属性](#)。
- 客户端属性 ENABLE_CREDENTIAL_STORE 和 SEND_LDAP_ATTRIBUTES。有关说明，请参阅[客户端属性](#)。

如果要自定义应用商店，请转到[设置 > 客户端品牌](#)以更改名称、添加徽标并指定应用的显示方式。

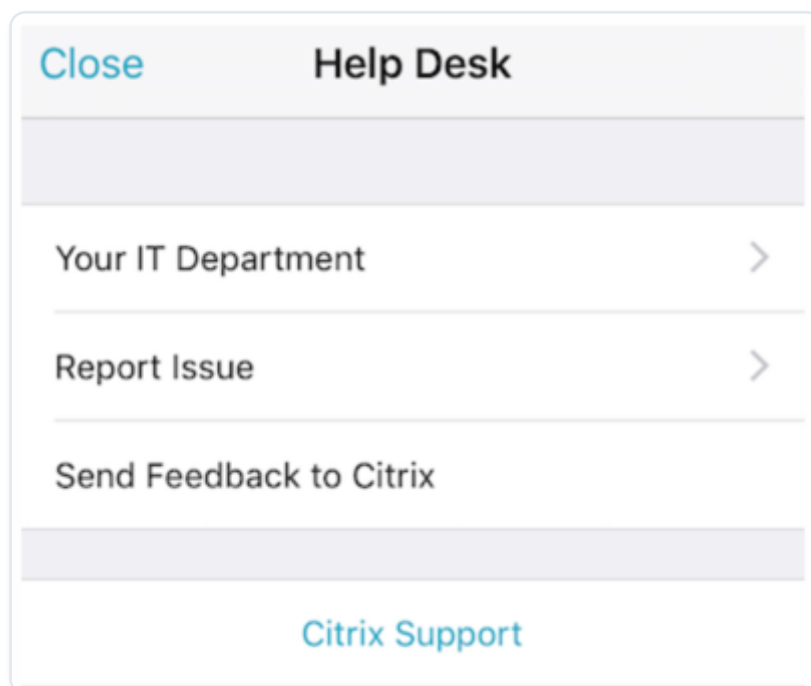
客户端品牌图像(/en-us/mobile-productivity-apps/media/worxhome-client-branding.png)

您可以在 Endpoint Management 控制台中编辑应用说明。单击[配置](#)，然后单击[应用](#)。从表中选择应用，然后单击[编辑](#)。选择要编辑说明的应用的平台，然后在[说明框](#)中键入文本。

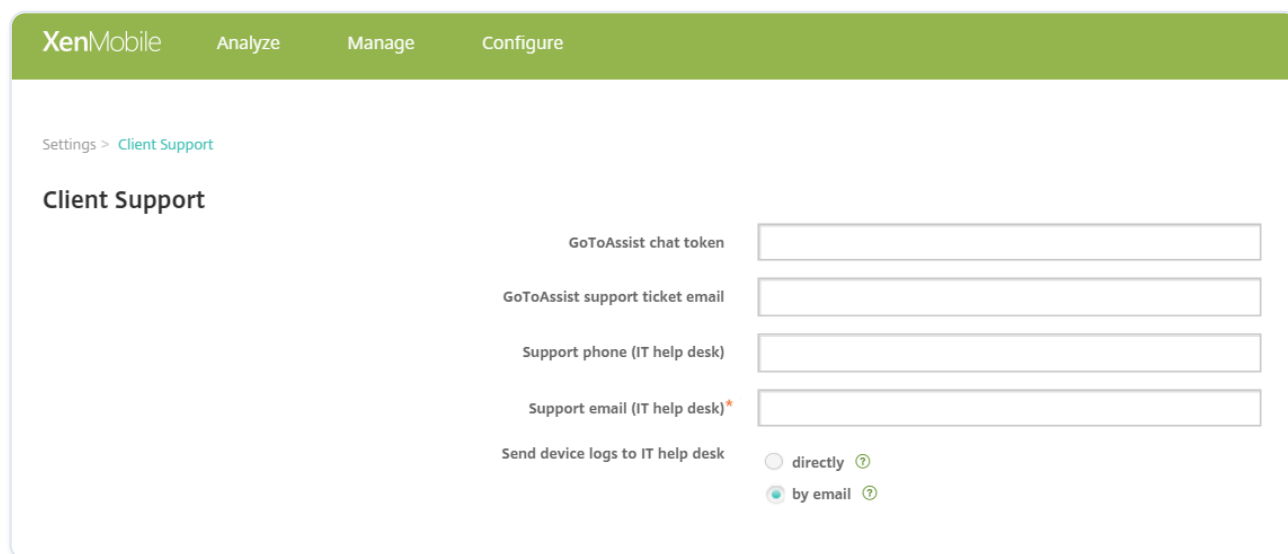
说明框的图像(/en-us/mobile-productivity-apps/media/worxhome-edit-app-descriptions-xm.png)

在应用商店中，用户只能浏览您在 Endpoint Management 中配置和保护的应用和桌面。要添加应用，用户单击“[详细信息](#)”，然后单击“[添加](#)”。

Secure Hub 还为用户提供了多种获取帮助的方式。在平板电脑上，点击右上角的问号可打开帮助选项。在手机上，用户单击左上角的汉堡菜单图标，然后单击“[帮助](#)”。



“您的 IT 部门”显示您公司帮助台的电话和电子邮件，用户可以直接从应用访问。您可以在 Endpoint Management 控制台中输入电话号码和电子邮件地址。点击右上角的齿轮图标。此时将显示“设置”页面。点击“更多”，然后点击“客户端支持”。此时将显示输入信息的屏幕。



XenMobile Analyze Manage Configure

Settings > Client Support

Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)*

Send device logs to IT help desk

☐ directly ?

☒ by email ?

“报告问题”显示应用列表。用户选择出现问题的应用。Secure Hub 会自动生成日志，然后在 Secure Mail 中打开一封邮件，并将日志作为 zip 文件附件。用户添加主题行和问题描述。他们还可以附加屏幕截图。

“向 Citrix 发送反馈”在 Secure Mail 中打开一封邮件，其中已填写 Citrix 支持地址。在邮件正文中，用户可以输入改进 Secure Mail 的建议。如果设备上未安装 Secure Mail，则会打开本机邮件程序。

用户还可以点击“Citrix 支持”，这将打开 Citrix 知识中心。用户可以在其中搜索所有 Citrix 产品的支持文章。

在“首选项”中，用户可以找到有关其帐户和设备的信息。

Secure Hub 还提供地理位置和地理跟踪策略，例如，如果您想确保公司拥有的设备不超出某个地理范围。有关详细信息，请参阅[位置设备策略](#)。此外，Secure Hub 会自动收集和分析故障信息，以便您了解导致特定故障的原因。此功能由 Crashlytics 软件支持。

Secure Mail 概述

Citrix Secure Mail™ 允许用户在其移动电话和平板电脑上管理其电子邮件、日历和联系人。为了保持与 Microsoft Outlook 或 IBM Notes 帐户的连续性，Secure Mail 与 Microsoft Exchange Server 和 IBM Notes Traveler Server 同步。

作为 Citrix 应用程序套件的一部分，Secure Mail 受益于与 Citrix Secure Hub 的单点登录 (SSO) 兼容性。用户登录 Secure Hub 后，他们可以无缝地进入 Secure Mail，而无需重新输入其用户名和密码。您可以配置 Secure Mail，使其在设备注册 Secure Hub 时自动推送到用户的设备，或者用户可以从应用商店添加该应用程序。

注意：

- 对 Exchange Server 2010 的支持已于 October 13, 2020 结束。
- 对 Exchange Server 2013 的支持已于 April 11, 2023 结束。

Secure Mail 兼容以下版本：

- Exchange 服务器 SE RTM
- Exchange Server 2019 累积更新 15
- Exchange Server 2019 累积更新 14
- Exchange Server 2019 累积更新 13
- Exchange Server 2019 累积更新 12
- Exchange Server 2019 累积更新 11
- Exchange Server 2019 累积更新 10
- Exchange Server 2019 累积更新 9
- Exchange Server 2019 累积更新 8
- Exchange Server 2019 累积更新 7
- Exchange Server 2019 累积更新 6
- Exchange Server 2016 累积更新 23

- Exchange Server 2016 累积更新 22
- Exchange Server 2016 累积更新 21
- Exchange Server 2016 累积更新 20
- Exchange Server 2016 累积更新 19
- Exchange Server 2016 累积更新 18
- Exchange Server 2016 累积更新 17
- HCL Domino 版本 14.0 FP1
- HCL Domino 版本 12.0.2 FP2
- HCL Traveler 版本 12.0.2.1 构建 202302010413_30
- HCL Domino 11 （前身为 Lotus Notes）
- HCL Domino 10.0.1 （前身为 Lotus Notes）
- HCL Domino 9.0.1 FP10 HF197 （以前称为 Lotus Notes）
- HCL Domino 10.0.1.0 构建版本 201811191126_20 （以前称为 Lotus Notes）
- HCL Domino 9.0.1.21 （以前称为 Lotus Notes）
- 微软 Office 365 (Exchange 在线)

首先，从 [Citrix Endpoint Management 下载](#) 下载 Secure Mail 和其他 Endpoint Management 组件。

有关 Secure Mail 和其他移动应用程序的系统要求，请参阅 [系统要求](#)。

有关 Secure Mail 适用于 iOS 和 Android 的通知（当应用程序在后台运行或关闭时）的信息，请参阅 [Secure Mail 的推送通知](#)。

有关 Secure Mail 支持的 iOS 功能，请参阅 [Secure Mail 的 iOS 功能](#)。

有关 Secure Mail 支持的 Android 功能，请参阅 [Secure Mail 的 Android 功能](#)。

有关 Secure Mail 支持的 iOS 和 Android 功能，请参阅 [Secure Mail 的 iOS 和 Android 功能](#)。

有关用户帮助文档，请参阅 Citrix 用户帮助中心中的 [Citrix Secure Mail](#) 页面。

思杰安全 Web™

Citrix Secure Web 是一款兼容 HTML5 的移动 Web 浏览器，可提供对内部和外部站点的安全访问。您可以将 Secure Web 配置为在设备注册到 Secure Hub 时自动推送到用户设备。或者，您可以从 Endpoint Management 应用商店添加该应用。

有关 Secure Web 和其他移动生产力应用程序的系统要求，请参阅 [系统要求](#)。

集成和交付 Secure Web

注意：

MDX Toolkit 10.7.10 是支持移动生产力应用程序包装的最终版本。用户可以从公共应用商店访问 10.7.5 及更高版本的移动生产力应用程序。

要集成和交付 Secure Web，请按照以下一般步骤操作：

1. 要为内部网络启用单点登录 (SSO)，请配置 Citrix Gateway。

对于 HTTP 流量，Citrix ADC 可以为 Citrix ADC 支持的所有代理身份验证类型提供 SSO。对于 HTTPS 流量，Web 密码缓存策略使 Secure Web 能够通过 MDX 对代理服务器进行身份验证并提供 SSO。MDX 仅支持基本、摘要和 NTLM 代理身份验证。密码使用 MDX 缓存，并存储在 Endpoint Management 共享保管库中，这是一个用于敏感应用程序数据的安全存储区域。有关 Citrix Gateway 配置的详细信息，请参阅 [Citrix Gateway](#)。

2. 下载 Secure Web。
3. 确定您希望如何配置用户与内部网络的连接。
4. 将 Secure Web 添加到 Endpoint Management，采用与其他 MDX 应用程序相同的步骤，然后配置 MDX 策略。有关 Secure Web 特有策略的详细信息，请参阅本文后面的“关于 Secure Web 策略”。

配置用户连接

Secure Web 支持以下用户连接配置：

- **隧道式 - Web SSO**：隧道连接到内部网络的连接可以使用无客户端 VPN 的变体，称为隧道式 - Web SSO。这是为 **首选 VPN 模式** 策略指定的默认配置。建议将隧道式 - Web SSO 用于需要单点登录 (SSO) 的连接。
- **完整 VPN 隧道**：隧道连接到内部网络的连接可以使用完整 VPN 隧道，该隧道由**首选 VPN 模式** 策略配置。建议将完整 VPN 隧道用于使用客户端证书或端到端 SSL 连接到内部网络资源的连接。但是，Secure Web 不是一个可以读取存储在移动设备上的客户端证书的应用程序。可以安装一些第三方封装的企业应用程序来提供此功能。完整 VPN 隧道处理 TCP 上的任何协议，除了 iOS 和 Android 设备外，还可以与 Windows 和 Mac 计算机一起使用。
- **允许 VPN 模式切换**策略允许根据需要自动在完整 VPN 隧道和隧道式 - Web SSO 模式之间切换。默认情况下，此策略处于关闭状态。当此策略开启时，由于首选 VPN 模式无法处理的身份验证请求而失败的网络请求将以备用模式重试。例如，完整 VPN 隧道模式可以适应客户端证书的服务器质询，但隧道式 - Web SSO 模式不能。同样，在使用隧道式 - Web SSO 模式时，HTTP 身份验证质询更有可能通过 SSO 进行处理。

下表说明了 Secure Web 是否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	首次访问网站时 SECURE WEB 提示输入凭据	后续访问网站时 SECURE WEB 提示输入凭据	密码更改后 SECURE WEB 提示输入凭据
隧道式 - Web SSO	HTTP	否	是	否	否	否
隧道式 - Web SSO	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”为“开”。	否	是；需要在 Secure Web 中缓存凭据。	否	是

Secure Web 策略

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

允许或阻止的网站

Secure Web 通常不筛选 Web 链接。您可以使用此策略配置允许或阻止的特定站点列表。您可以配置 URL 模式以限制浏览器可以打开的网站，格式为逗号分隔列表。列表中的每个模式前面都有一个加号 (+) 或减号 (-)。浏览器将 URL 与按列出顺序的模式进行比较，直到找到匹配项。找到匹配项后，前缀将决定要执行的操作，如下所示：

- 减号 (-) 前缀指示浏览器阻止 URL。在这种情况下，URL 被视为 Web 服务器地址无法解析。
- 加号 (+) 前缀允许 URL 正常处理。
- 如果模式未提供 + 或 -，则假定为 +（允许）。
- 如果 URL 不匹配列表中的任何模式，则允许该 URL

要阻止所有其他 URL，请在列表末尾添加一个减号，后跟一个星号 (-*)。例如：

- 策略值 `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` 允许 `mycorp.com` 域内的 HTTP URL，但在其他地方阻止它们；允许任何位置的 HTTPS 和 FTP URL；并阻止所有其他 URL。
- 策略值 `+http://*.training.lab/*,+https://*.training.lab/*,-*` 允许用户通过 HTTP 或 HTTPS 打开 Training.lab 域（内网）中的任何站点。但是，无论协议如何，您都无法打开 Facebook、Google 和 Hotmail 等公共 URL。

默认值为空（允许所有 URL）。

阻止弹出窗口

弹出窗口是网站未经您许可打开的新选项卡。此策略确定 Secure Web 是否允许弹出窗口。如果为“开”，Secure Web 会阻止网站打开弹出窗口。默认值为“关”。

预加载书签

定义 Secure Web 浏览器的一组预加载书签。该策略是一个逗号分隔的元组列表，其中包括文件夹名称、友好名称和网址。每个三元组必须采用 folder, name, url 的形式，其中 folder 和 name 可以选择用双引号 (") 括起来。

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。第一个是主链接（无文件夹名称），标题为“Mycorp, Inc. home page”。第二个链接放在名为“MyCorp Links”的文件夹中，并标记为“Account logon”。第三个链接放在“MyCorp Links”文件夹的“Investor Relations”子文件夹中，并显示为“Contact us”。

默认值为空。

主页 URL

定义 Secure Web 启动时加载的网站。默认值为空（默认起始页）。

仅适用于受支持的 Android 和 iOS 设备：

浏览器用户界面

规定 Secure Web 浏览器用户界面控件的行为和可见性。通常，所有浏览控件都可用。其中包括前进、后退、地址栏以及刷新/停止控件。您可以配置此策略以限制其中某些控件的使用和可见性。默认值为“所有控件可见”。

选项

- 所有控件可见。所有控件均可见，用户可以不受限制地使用它们。
- 只读地址栏。所有控件均可见，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。隐藏整个工具栏以提供无边框浏览体验。

启用 Web 密码缓存

当 Secure Web 用户在访问或请求 Web 资源时输入凭据时，此策略决定 Secure Web 是否在设备上静默缓存密码。此策略适用于在身份验证对话框中输入的密码，而不适用于在 Web 表单中输入的密码。

如果为 **On**，Secure Web 会缓存用户在请求 Web 资源时输入的所有密码。如果为 **Off**，Secure Web 不会缓存密码并删除现有缓存密码。默认值为 **Off**。

仅当您还将首选 VPN 策略设置为此应用程序的“完整 VPN 隧道”时，此策略才启用。

代理服务器

在隧道式 – Web SSO 模式下使用 Secure Web 时，您还可以为其配置代理服务器。有关详细信息，请参阅这篇[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[通过使用 Android 设备的 DNS 后缀支持 DNS 查询](#)。

为 Secure Web 准备内部网站点

本节面向需要准备内网站点以便与适用于 Android 和 iOS 的 Secure Web 配合使用的网站开发人员。专为桌面浏览器设计的内网站点需要进行更改才能在 Android 和 iOS 设备上正常运行。

Secure Web 依赖于 Android WebView 和 iOS WkWebView 提供 Web 技术支持。Secure Web 支持的部分 Web 技术包括：

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets

Secure Web 不支持的部分 Web 技术包括：

- 弗莱士
- 爪哇

下表显示了 Secure Web 支持的 HTML 呈现功能和技术。X 表示该功能适用于平台、浏览器和组件的组合。

技术	IOS 安全 WEB	ANDROID 6.X/7.X 安全 WEB
JavaScript 引擎	JavaScriptCore	V8
本地存储	X	X
AppCache	X	X

技术	IOS 安全 WEB	ANDROID 6.X/7.X 安全 WEB
IndexedDB		X
SPDY	X	
WebP		X
源	X	X
WebGL		X
requestAnimationFrame API		X
导航计时 API		X
资源计时 API		X

技术在不同设备上工作方式相同；但是，Secure Web 会为不同设备返回不同的用户代理字符串。要确定 Secure Web 使用的浏览器版本，可以查看其用户代理字符串。在 Secure Web 中，导航到 `<https://whatsmyuseragent.com/>`。

内网站点故障排除

要解决在 Secure Web 中查看内网站点时的渲染问题，请比较该网站在 Secure Web 和兼容的第三方浏览器中的渲染方式。

对于 iOS，兼容的第三方测试浏览器是 Chrome 和 Dolphin。

对于 Android，兼容的第三方测试浏览器是 Dolphin。

注意：

Chrome 是 Android 上的原生浏览器。请勿将其用于比较。

在 iOS 中，请确保浏览器支持设备级 VPN。您可以通过导航到 **Settings > VPN > Add VPN Configuration** 在设备上配置 VPN。

您还可以使用 App Store 上提供的 VPN 客户端应用程序，例如 [Citrix VPN](#)、[Cisco AnyConnect](#) 或 [Pulse Secure](#)。

- 如果网页在两个浏览器中呈现相同，则问题出在您的网站。请更新您的网站，并确保它在操作系统上运行良好。
- 如果网页问题仅出现在 Secure Web 中，请联系 Citrix 支持以开具支持工单。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 存在渲染问题，请按照以下步骤所述包含页面的网页存档。这样做有助于 Citrix 更快地解决问题。

创建网页存档文件

在 macOS 10.9 或更高版本上使用 Safari，您可以将网页保存为网页存档文件（称为阅读列表）。网页存档文件包含所有链接文件，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 **Menu** 栏中的 **Go** 菜单，选择 **Go to Folder**，键入路径名 `~/Library/Safari/ReadingListArchives/`，然后删除该位置中的所有文件夹。
2. 在 **Menu** 栏中，转到 **Safari > Preferences > Advanced**，然后启用 **Show Develop menu**。
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 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/10.1.0(build 1.4.0) Safari/8536.25)。
4. 在 Safari 中，打开您要保存为阅读列表（网页存档文件）的网站。
5. 在 **Menu** 栏中，转到 **Bookmarks > Add to Reading List**。存档在后台进行，可能需要几分钟。
6. 找到已存档的阅读列表：在 **Menu** 栏中，转到 **View > Show Reading List Sidebar**。
7. 验证存档文件：
 - 关闭 Mac 的网络连接。
 - 从阅读列表中打开网站。

网站完全呈现。

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**，键入路径名 `~/Library/Safari/ReadingListArchives/`。现在压缩文件名为随机十六进制字符串的文件夹。您可以在开具支持票证时将此文件发送给 Citrix 支持。

Secure Web 功能

Secure Web 使用移动数据交换技术为用户创建专用 VPN 隧道，以访问内部和外部网站以及所有其他网站。这包括在由贵组织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 容器中提供了无缝的用户体验。以下是一些集成功能的示例：

- 当用户点击 **Mailto** 链接时，Citrix Secure Mail™ 中会打开一封新电子邮件，无需额外身份验证。
- 在 iOS 中，用户可以通过在 URL 前面插入 **ctxmobilebrowser://** 从本机邮件应用程序在 Secure Web 中打开链接。例如，要从本机邮件应用程序打开 `example.com`，请使用 URL `ctxmobilebrowser://example.com`。
- 当用户点击电子邮件中的内网链接时，Secure Web 会转到该站点，无需额外身份验证。
- 用户可以将他们在 Secure Web 中从网络下载的文件上传到 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 的大部分内存都用于渲染弹出窗口，因此在“设置”中阻止弹出窗口通常可以提高性能。

- 收藏他们喜欢的网站。
- 下载文件。
- 离线保存页面。
- 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。
- 允许他们通过 Secure Web 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，而无需下载文件。要启用此功能，请在 Endpoint Management 的“允许的 URL”策略中添加 **ctx-sf:**。
- 在 iOS 中，使用 3D Touch 操作直接从主屏幕打开新选项卡并访问离线页面、收藏网站和下载内容。
- 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它们。

注意：

将 Secure Web 置于后台会导致下载停止。

- 使用 **在页面中查找** 在当前页面视图中搜索术语。

在页面中查找选项的图像(/en-us/mobile-productivity-apps/media/worxweb-findinpage.png)

Secure Web 还支持动态文本。该应用会显示用户在其设备上设置的字体。

注意：

- Citrix Files for XenMobile 已于 July 1, 2023 达到 EOL。有关详细信息，请参阅 [EOL 和已弃用的应用](#)

Citrix Content Collaboration™ 适用于 端点管理

适用于 Endpoint Management 的 Citrix Content Collaboration 客户端是 Citrix Files 移动客户端的 MDX 兼容版本。这些客户端提供对其他 MDX 封装应用程序中数据的安全集成访问。适用于 Endpoint Management 的 Citrix Content Collaboration 客户端还受益于 MDX 功能，例如微型 VPN、通过 Secure Hub 实现的单点登录 (SSO) 和双因素身份验证。

Citrix Files 是一种企业文件同步和共享服务，可让用户轻松安全地交换文档。Citrix Files 为用户提供各种访问选项，包括 Citrix Files 移动客户端，例如适用于 Android 手机的 Citrix Files 和适用于 iPad 的 Citrix Files。

您可以将 Citrix Files 与 Endpoint Management 集成，以提供完整的 Citrix Files 功能集，或仅提供对存储区域连接器的访问。默认情况下，Citrix Endpoint Management 控制台仅支持配置 Citrix Files。要改为配置 Endpoint Management 以与存储区域连接器配合使用，请参阅 Citrix Endpoint Management 文档中的 [将 Citrix Content Collaboration 与 Endpoint Management 结合使用](#)。

您按如下方式使用 Endpoint Management、Citrix Files、存储区域控制器和 Citrix ADC 来部署和管理适用于 Endpoint Management 的 Citrix Content Collaboration 客户端：

- 当 Endpoint Management 配置了 Citrix Files 时，Endpoint Management 充当 SAML 身份提供程序 (IdP) 并部署适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。Citrix Files 管理 Citrix Files 数据。没有 Citrix Files 数据通过 Endpoint Management 传输。
- 当 Endpoint Management 配置了 Citrix Files 或存储区域连接器时，存储区域控制器提供与网络共享和 SharePoint 中数据的连接。用户通过 Citrix Files 移动生产力应用程序访问您存储的数据。用户可以从移动设备编辑 Microsoft Office 文档、预览和批注 Adobe PDF 文件。
- Citrix ADC 管理来自外部用户的请求，确保其连接安全，对请求进行负载平衡，并处理存储区域连接器的内容切换。

有关适用于 Endpoint Management 的 Citrix Content Collaboration 和其他移动生产力应用程序的系统要求，请参阅 [支持移动生产力应用程序](#)。

适用于 Endpoint Management 的 Citrix Content Collaboration 客户端与 Citrix Files 移动客户端有何不同

以下介绍了适用于 Endpoint Management 的 Citrix Content Collaboration 客户端与 Citrix Files 移动客户端之间的差异。

用户访问

Citrix Content Collaboration 适用于端点管理客户端：

用户从 Secure Hub 获取并打开适用于 Endpoint Management 的 Citrix Content Collaboration 客户端。

Citrix Files 移动客户端：

用户从应用商店获取 Citrix Files 移动客户端。

SSO

适用于端点管理的 Citrix 内容协作客户端：

适用于 Endpoint Management 与 Citrix Files 的集成：您可以将 Endpoint Management 配置为 Citrix Files 的 SAML IdP。在此配置中，Secure Hub 使用 Endpoint Management 作为 SAML IdP，为适用于 Endpoint Management 的 Citrix Content Collaboration 客户端获取 SAML 令牌。启动适用于 Endpoint Management 的 Citrix Content Collaboration 客户端但未登录 Secure Hub 的用户将收到登录 Secure Hub 的提示。用户无需知道其 Citrix Files 域或帐户信息。

Citrix Files 移动客户端：

您可以将 Endpoint Management 和 Citrix Gateway 配置为 Citrix Files 的 SAML IdP。在此配置中，使用 Web 浏览器或其他 Citrix Files 客户端登录 Citrix Files 的用户将被重定向到 Endpoint Management 环境进行用户身份验证。经 Endpoint Management 成功验证后，用户将收到一个 SAML 令牌，该令牌可用于登录其 Citrix Files 帐户。

微型 VPN

适用于端点管理的 Citrix 内容协作客户端：

远程用户可以通过 Citrix Gateway 使用 VPN 或微型 VPN 连接来访问内部网络中的应用程序和桌面。此功能通过 Citrix ADC 与 Endpoint Management 的集成提供，对用户是透明的。

Citrix Files 移动客户端：

不适用。

双因素身份验证

适用于 端点管理 的 Citrix Content Collaboration 客户端：

Citrix ADC 与 Endpoint Management 的集成还支持结合使用客户端证书身份验证和另一种身份验证类型（例如 LDAP 或 RADIUS）进行身份验证。

Citrix Files 移动客户端：

不适用。

文件夹权限

适用于 Endpoint Management 客户端的 Citrix Content Collaboration 和 Citrix Files 移动客户端：

对于 Endpoint Management 与 Citrix Files 的集成：由 Citrix Files 决定。

文档访问保护

适用于 端点管理 的 Citrix Content Collaboration 客户端：

用户可以打开在 Secure Mail 中收到的附件或由任何 MDX 封装的应用程序下载的附件。当用户执行“打开方式”操作时，只会显示 MDX 封装的应用程序。来自非封装应用程序的数据不适用于适用于 Endpoint Management 客户端的 Citrix Content Collaboration。Secure Mail 用户可以从其 Citrix Files 存储库附加文件，而无需将文件下载到设备。如果用户在设备上同时安装了封装和非封装的 Citrix Files，则封装的 Citrix Files 客户端无法访问用户个人 Citrix Files 帐户中的文件。封装的 Citrix Files 客户端只能访问在 Endpoint Management 中配置的 Citrix Files 子域。

Citrix Files 移动客户端：

用户可以从任何应用程序打开附件。

Citrix Files 帐户访问

适用于 端点管理 客户端的 Citrix Content Collaboration：

对于 Endpoint Management 与 Citrix Files 的集成：要访问个人 Citrix Files 帐户或第三方 Citrix Files 帐户，用户必须在设备上使用非 MDX 版本的 Citrix Files。

Citrix Files 移动客户端：

对于 Endpoint Management 与 Citrix Files 的集成：可从 Citrix Files 客户端获取。

设备策略

适用于 Endpoint Management 客户端的 Citrix Content Collaboration 和 Citrix Files 移动客户端:

Endpoint Management 和 Citrix Files 设备策略均适用于适用于 Endpoint Management 客户端的 Citrix Content Collaboration。例如，您可以从 Endpoint Management 控制台执行设备擦除。从 Citrix Files 控制台，您可以远程擦除 Citrix Files 应用程序。

MDX 策略

适用于 端点管理 客户端的 Citrix Content Collaboration :

MDX 策略允许您在 Citrix Endpoint Management™ 中配置由 Endpoint Management 应用商店强制执行的设置。仅通过 MDX 可用的策略包括阻止摄像头、麦克风、电子邮件撰写、屏幕捕获以及剪贴板剪切、复制和粘贴操作的功能。

Citrix Files 移动客户端:

不适用。

数据加密

适用于 Endpoint Management 客户端的 Citrix Content Collaboration 和 Citrix Files 移动客户端:

使用 AES-256 加密所有存储数据，并使用 SSL 3.0 和至少 128 位加密保护传输中的数据。

可用性

适用于端点管理客户端的 Citrix Content Collaboration:

适用于端点管理客户端的 Citrix Content Collaboration 包含在端点管理高级版和企业版中。

Citrix Files 移动客户端:

所有 Endpoint Management 版本都包含所有 Citrix Files 功能。您可以将 Endpoint Management 与完整的 Citrix Files 功能集或仅存储区域连接器集成。

集成和交付适用于 Endpoint Management 客户端的 Citrix Content Collaboration

要集成和交付适用于 Endpoint Management 客户端的 Citrix Content Collaboration，请执行以下常规步骤：

1. 将 Endpoint Management 启用为 Citrix Files 的 SAML IdP，以提供从 Citrix Files 客户端到 Citrix Files 的 SSO。为此，您必须在 Endpoint Management 中配置 Citrix Files 帐户信息。有关详细信息，请参阅“在 Endpoint Management 中配置 Citrix Files 帐户信息以实现 SSO”部分。

重要提示：

要将 Endpoint Management 用作非 MDX Citrix Files 客户端（例如 Citrix Files Web 应用程序和 Citrix Files Sync 客户端）的 SAML IdP，需要进行额外配置。

2. 下载 Citrix Files 客户端。
3. 将 Citrix Files 客户端添加到 Endpoint Management。有关详细信息，请参阅本文后面的“将 Citrix Files 添加到 Endpoint Management”。
4. 验证您的配置。有关详细信息，请参阅本文后面的“验证 Citrix Files 客户端”。

关于设置：

- 域是用于客户端的 Citrix Files 子域。
- 只有所选 DG 中的用户才能从客户端 SSO 访问 Citrix Files。

如果 DG 中的用户没有 Citrix Files 帐户，则在您将 Citrix Files 客户端添加到 Endpoint Management 时，Endpoint Management 会将该用户预配到 Citrix Files 中。

- Endpoint Management 使用 Citrix Files 管理员帐户登录信息将 SAML 设置保存在 Citrix Files 控制平面中。

重要提示：

从 Citrix Files 客户端到 Citrix Files 启用 SSO 的配置不会对用户进行网络共享或 SharePoint 文档库的身份验证。访问这些连接器数据源需要对网络共享或 SharePoint 服务器所在的 Active Directory 域进行身份验证。

在 Endpoint Management 中配置 Citrix Files 帐户信息以实现 SSO

要从 Secure Hub 启用 SSO 到移动生产力应用程序，请在 Endpoint Management 控制台中指定 Citrix Files 帐户和 Citrix Files 管理员服务帐户信息。通过该配置，Endpoint Management 可作为 Citrix Files 的 SAML IdP，用于移动生产力应用程序客户端、Citrix Files 客户端和非 MDX Citrix Files 客户端。当用户启动移动生产力应用程序客户端时，Secure Hub 会从 Endpoint Management 获取用户的 SAML 令牌并将其发送到 Citrix Files 客户端。

在 Endpoint Management 控制台中，单击“配置”>“内容协作”（这是 Citrix Files 的旧名称）。

将适用于 Endpoint Management 的 Citrix 内容协作客户端添加到 Endpoint Management

将 Citrix Content Collaboration for Endpoint Management 客户端添加到 Endpoint Management 后，您可以从 Citrix Content Collaboration for Endpoint Management 客户端启用对连接器数据源的 SSO 访问。为此，请按照本节所述配置“网络访问”策略和“首选 VPN 模式”策略。

必备条件

- Endpoint Management 必须能够访问您的 Citrix Files 子域。要测试连接，请从 Endpoint Management 服务器 ping 您的 Citrix Files 子域。
- 为您的 Citrix Files 帐户和运行 Endpoint Management 的虚拟机管理程序配置的时区必须相同。如果时区不同，SSO 请求可能会失败，因为 SAML 令牌可能无法在预期时间内到达 Citrix Files。要为 Endpoint Management 配置 NTP 服务器，请使用 Endpoint Management 命令行界面。

注意：

Hyper-V 主机将 Linux VM 上的时间设置为本地时区，而不是 UTC。

- 以管理员身份登录到 ShareFile 帐户，并在“设置”>“管理员设置”>“安全”>“登录和安全策略”>“单点登录/SAML 2.0 配置”中验证 SAML SSO 设置。
- 下载适用于 Endpoint Management 的 Citrix 内容协作客户端。

步骤：

1. 在 Endpoint Management 控制台中，单击“**配置 > 应用程序**”，然后单击“**添加**”。
2. 单击 **MDX**。
3. 输入 **名称**，以及（可选）**描述** 和 **应用程序类别** 用于该应用程序。
4. 单击 **下一步**，然后上传用于 Citrix Content Collaboration for Endpoint Management 客户端的 .mdx 文件。
5. 单击 **下一步** 以配置应用程序信息和策略。

启用从 Citrix Content Collaboration for Endpoint Management 客户端到 Citrix Files 的 SSO 的配置不会对用户进行身份验证以访问网络共享或 SharePoint 文档库。

6. 要在 Secure Hub 微型 VPN 和存储区域控制器之间启用 SSO，请完成以下策略配置：

- 将网络访问策略设置为 **隧道连接到内部网络**。

在此模式下，MDX 框架会拦截来自 Citrix Content Collaboration for Endpoint Management 客户端的所有网络流量。然后，网络流量会通过 Citrix Gateway 使用特定于应用程序的微型 VPN 进行重定向。

- 将首选 VPN 模式策略设置为 **隧道连接 – Web SSO**。

在此隧道模式下，MDX 框架会终止来自 MDX 应用程序的 SSL/HTTP 流量，然后会代表用户发起新的连接以连接到内部连接。此策略设置使 MDX 框架能够检测并响应由 Web 服务器发出的身份验证质询。

7. 根据需要完成批准和交付组 (DG) 分配。

只有所选 DG 中的用户才能从 Citrix Content Collaboration for Endpoint Management 客户端访问 Citrix Files 的 SSO。如果 DG 中的用户没有 Citrix Files 帐户，当您将 Citrix Content Collaboration for Endpoint Management 客户端添加到 Endpoint Management 时，Endpoint Management 会将该用户预配到 Citrix Files 中。

验证思杰内容协作端点管理客户端

1. 完成本文所述的配置后，启动 Citrix Content Collaboration for Endpoint Management 客户端。Citrix Files 不会提示您登录。
2. 在 Secure Mail 中，撰写电子邮件并从 Citrix Files 添加附件。您的 Citrix Files 主页会打开，而不会提示您登录。

注意：

- Citrix Files for XenMobile 已于 July 1, 2023 终止服务 (EOL)。有关详细信息，请参阅 [EOL 和已弃用应用](#)

生命周期结束和已弃用应用

以下应用已达到或即将达到生命周期结束 (EOL) 状态。当产品版本达到 EOL 时，您可以在产品许可协议的条款范围内使用该产品，但可用的支持选项将受到限制。历史信息会出现在知识中心或其他在线资源中。文档不再更新，并按“原样”提供。有关产品生命周期里程碑的更多信息，请参阅[产品矩阵](#)。

注意：

有关即将淘汰的 Citrix Endpoint Management 功能的提前通知，请参阅[弃用](#)。

适用于 XenMobile® (MDX) 的 Citrix Files： 适用于 XenMobile 的 Citrix Files 已于 July 1, 2023 达到 EOL。

我们建议客户使用 Apple App Store 和 Google Play 中提供的 Citrix Files。它已支持 MAM SDK。

适用于 Intune SDK 的 Secure Mail (iOS 和 Android)： Secure Mail 已于 April 30, 2023 达到 EOL。

适用于 Intune 的 Citrix Files： 已于 December 31, 2020 弃用。

我们鼓励您探索利用平台功能，通过 Android Enterprise（带工作配置文件）和 iOS 用户注册来容器化常规 Citrix Files 应用（可在应用商店中获取）。

ShareConnect： ShareConnect 已于 June 30, 2020 达到 EOL。

Secure Notes： EOL 生命周期日期为 December 31, 2018。

如果您需要 Secure Notes 和 Secure Tasks 的功能，我们推荐 Notate for Citrix，这是一款您可以使用 MDX 策略进行保护的第三方应用。

如果 Secure Notes 和 Secure Tasks 的用户将数据存储在 Outlook 中，他们可以在 Notate 中访问这些数据。如果用户将数据存储在 ShareFile（现为 Citrix Files）中，则数据不会迁移。

用户可以在 EOL 日期之后继续运行 Secure Notes，直到其平台操作系统停止支持用户界面。但是，我们不建议您使用不受支持的产品。

Secure Tasks： EOL 生命周期日期为 December 31, 2018。

****Secure Forms：****EOL 生命周期日期为 March 31, 2018。建议客户过渡到 Citrix Files Platinum 和 Premium 帐户中包含的 Citrix ShareFile Workflows。有关详细信息，请参阅 [Citrix ShareFile Workflows](#)。

****ScanDirect：****ScanDirect 于 September 1, 2018 达到 EOL。

****Full VPN tunnel：****EOL 日期为 2021 年 9 月。有关详细信息，请参阅 Citrix Endpoint Management 产品文档中的[弃用](#)。

****Full VPN tunnel- Android：****于 2020 年 3 月弃用。EOL 日期为 2021 年 9 月。我们建议客户使用 MAM SDK Web SSO 模式作为替代方案。

****Permit VPN mode switching - Android：****于 2020 年 3 月弃用。EOL 日期为 2021 年 9 月。

****Inbound Document Exchange - Android：****于 2020 年 3 月弃用。EOL 日期为 2021 年 9 月。

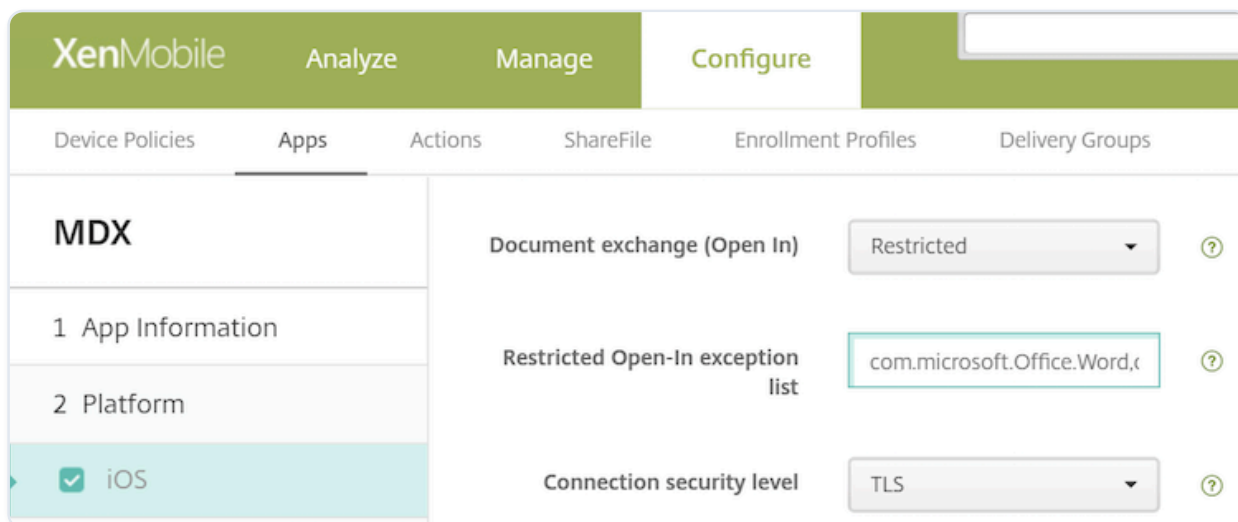
允许与 Office 365 应用程序进行安全交互

Citrix Secure Mail™、Citrix Secure Web 和 Citrix Files 提供了打开 MDX 容器的选项，以允许用户将文档和数据传输到 Microsoft Office 365 应用程序。您可以通过 Endpoint Management 控制台上的打开方式策略来管理 iOS 和 Android 平台上的此功能。

一旦在 Microsoft 应用程序中打开，数据在 MDX 容器中将不再受到保护或加密。在启用此功能之前，请考虑其安全隐患。特别是，关注数据丢失防护或受 HIPAA 或其他严格合规性要求约束的客户应权衡打开容器的利弊。

在 iOS 中启用 Office 365

1. 从 [Endpoint Management 下载页面](#) 下载最新版本的 Secure Mail、Secure Web 或 Citrix Files 应用程序。
2. 将文件上传到 Endpoint Management 控制台。
3. 找到文档交换（打开方式）策略并将其设置为受限。在受限打开方式例外 列表中，Microsoft Word、Excel、PowerPoint、OneNote 和 Outlook 会自动列出。例如：
com.microsoft.Office.Word、com.microsoft.Office.Excel、com.microsoft.Office.Powerpoint、com.microsoft.onenote、com.microsoft.onenoteiPad、com.microsoft.Office.Outlook



在 MDM 注册中，iOS 设备有更多可用控件。

您可以将 iTunes 应用程序上传到 Endpoint Management 控制台并将应用程序推送到设备。如果选择此选项，请将以下策略设置为开：

- 如果 MDM 配置文件被移除，则移除应用程序
- 阻止应用程序数据备份
- 强制管理应用程序（请注意，选择性擦除会移除应用程序和任何数据）

为防止文档和数据从 Microsoft 应用程序流向设备上的非受管应用程序，请在 Endpoint Management 控制台上转到**配置 > 设备 > 限制 > iOS**，然后将将受管应用程序中的文档传输到非受管应用程序和将非受管应用程序中的文档传输到受管应用程序设置为关。

在 Android 中启用 Office 365

1. 从 [Endpoint Management 下载页面](#) 下载 Secure Mail、Secure Web 或 Citrix Files 应用程序的最新版本。
2. 将文件上传到 Endpoint Management 控制台。
3. 向下滚动到 **文档交换 (打开方式)** 策略，然后选择 **受限**。
4. 在 **受限打开方式例外列表** 中，添加以下程序包 ID：

```
{package=com.microsoft.office.word} {package=com.microsoft.office.powerpoint}  
{package=com.microsoft.office.excel}
```

5. 照常配置其他应用程序策略，然后保存应用程序。

用户必须将其设备上的 Secure Mail、Secure Web 或 Citrix Files 中的文件保存，然后使用 Office 365 应用程序打开这些文件。

对于 iOS 和 Android，用户可以在其设备上打开和编辑以下类型的文件：

支持的文件格式

有关支持的文件格式，请参阅 Microsoft Office 文档。

移动生产力应用程序文档历史记录

下表介绍了对移动生产力应用程序产品文档所做的重要变更。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
30 May 2025	Secure Mail for iOS 25.5.0 的 EAR	下一版本预览
30 May 2025	Secure Web for iOS 25.5.0 的 EAR	下一版本预览
21 May 2025	发布 Secure Hub for Android 版本 25.4.0	当前版本中的新增功能
02 Apr 2025	发布 Secure Mail for Android 版本 25.3.0	当前版本中的新增功能
02 Apr 2025	发布 Secure Web for Android 版本 25.3.0	当前版本中的新增功能
17 Feb 2025	发布 Secure Mail for Android 版本 25.1.0	当前版本中的新增功能
17 Feb 2025	发布 Secure Hub for iOS 版本 25.1.0	当前版本中的新增功能
12 Feb 2025	发布 Secure Mail for iOS 25.1.0	当前版本中的新增功能
10 Feb 2025	发布 Secure Hub for Android 版本 25.1.0	当前版本中的新增功能
10 Feb 2025	发布 Secure Web for iOS 版本 25.1.0	当前版本中的新增功能
10 Feb 2025	发布 Secure Web for Android 版本 25.1.0	当前版本中的新增功能

日期	更改	说明
09 Dec 2024	发布 Secure Mail for iOS 24.11.0	当前版本中的新增功能
09 Dec 2024	发布 Secure Hub for iOS 版本 24.11.0	当前版本中的新增功能
06 Dec 2024	发布 Secure Web for iOS 版本 24.11.0	当前版本中的新增功能
05 Dec 2024	发布 Secure Mail for Android 版本 24.11.0	当前版本中的新增功能
04 Dec 2024	Secure Mail for Android 24.11.0 的 EAR	下一版本预览
04 Dec 2024	Secure Mail for iOS 24.11.0 的 EAR	下一版本预览
26 Nov 2024	Secure Web for iOS 24.11.0 的 EAR	下一版本预览
26 Nov 2024	Secure Hub for iOS 24.11.0 的 EAR	下一版本预览
25 Nov 2024	新章节：功能标志管理	功能标志管理
05 Nov 2024	发布 Secure Hub for Android 版本 24.10.0	当前版本中的新增功能
24 Oct 2024	Secure Hub for Android 24.10.0 的 EAR	下一版本预览
22 Oct 2024	发布 Secure Mail for Android 版本 24.9.1	当前版本中的新增功能
15 Oct 2024	发布 Secure Hub for iOS 版本 24.9.0	当前版本中的新增功能
09 Oct 2024	发布 Secure Web for Android 版本 24.9.0	当前版本中的新增功能

日期	更改	说明
09 Oct 2024	发布 Secure Mail for Android 版本 24.9.0	当前版本中的新增功能
09 Oct 2024	Secure Hub for iOS 24.9.0 的 EAR	下一版本预览
27 Sep 2024	Secure Web for Android 24.9.0 的 EAR	下一版本预览
27 Sep 2024	Secure Mail for Android 24.9.0 的 EAR	下一版本预览
20 Sep 2024	发布 Secure Mail for iOS 24.9.0	当前版本中的新增功能
16 Sep 2024	发布 Secure Web for iOS 版本 24.9.0	当前版本中的新增功能
06 Sep 2024	修订了 Secure Hub for Android 版本 24.8.0 的发布	当前版本中的新增功能
04 Sep 2024	Secure Mail for iOS 24.9.0 的 EAR	下一版本预览
03 Sep 2024	Secure Web for iOS 24.9.0 的 EAR	下一版本预览
02 Sep 2024	发布 Secure Hub for Android 版本 24.8.0	当前版本中的新增功能
28 Aug 2024	发布 Secure Web for Android 版本 24.8.0	当前版本中的新增功能
23 Aug 2024	Secure Web for Android 24.8.0 的 EAR	下一版本预览
21 Aug 2024	Secure Hub for Android 版本 24.8.0 的 EAR	下一版本预览
29 Jul 2024	发布 Secure Mail for Android 版本 24.7.0	Secure Mail 24.7.0：当前版本中的新增功能

日期	更改	说明
16 Jul 2024	Secure Mail for Android 24.7.0 的 EAR	下一版本预览
01 Jul 2024	发布 Secure Hub for Android 版本 24.6.0	Secure Hub 24.6.0：当前版本中的新增功能
06 May 2024	发布 Secure Hub for iOS 版本 24.5.0	Secure Hub 24.5.0：当前版本中的新增功能
22 Apr 2024	修订了适用于 Android 的 Secure Hub 版本 24.3.0，发布了一项新功能。	Secure Hub 24.3.0：当前版本中的新增功能
22 Apr 2024	修订了适用于 Android 的 Secure Hub 版本 23.12.0，发布了几项新功能。	Secure Hub 23.12.0：当前版本中的新增功能
11 Apr 2024	发布 Secure Hub for Android 版本 24.3.0	Secure Hub 24.3.0：缺陷修复
25 Mar 2024	发布 Secure Web for iOS 版本 24.3.0	Secure Web 24.3.0：缺陷修复
25 Mar 2024	发布 Secure Mail for iOS 版本 24.3.0	Secure Mail 24.3.0：缺陷修复
18 Mar 2024	发布 Secure Web for Android 版本 24.3.0	Secure Web 24.3.0：缺陷修复
21 Feb 2024	发布 Secure Web for iOS 版本 24.2.0	Secure Web 24.2.0：缺陷修复
21 Feb 2024	发布 Secure Web for iOS 版本 24.2.0	Secure Web 24.2.0：当前版本中的新增功能
21 Feb 2024	发布 Secure Mail for iOS 版本 24.2.0	Secure Mail 24.2.0：缺陷修复
21 Feb 2024	发布 Secure Mail for iOS 版本 24.2.0	Secure Mail 24.2.0：当前版本中的新增功能

日期	更改	说明
19 Feb 2024	发布 Secure Web for Android 版本 24.1.0	Secure Web 24.1.0：缺陷修复
19 Feb 2024	发布 Secure Mail for Android 版本 24.1.0	Secure Mail 24.1.0：缺陷修复
19 Feb 2024	发布 Secure Mail for Android 版本 24.1.0	Secure Mail 24.1.0：当前版本中的新增功能
16 Jan 2024	发布 Secure Hub for iOS 版本 24.1.0	Secure Hub 24.1.0：当前版本中的新增功能
16 Jan 2024	发布 Secure Hub for iOS 版本 24.1.0	Secure Hub 24.1.0：缺陷修复
16 Jan 2024	发布 Secure Hub for Android 版本 23.12.0	Secure Hub 23.12.0：当前版本中的新增功能和缺陷修复
04 Dec 2023	添加了遮蔽屏幕文档	Secure Mail：模糊屏幕内容
28 Nov 2023	发布 Secure Hub for iOS 版本 23.11.0	Secure Hub 23.11.0：当前版本中的新增功能
28 Nov 2023	发布 Secure Hub for iOS 版本 23.11.0	Secure Hub 23.11.0：缺陷修复
17 Nov 2023	发布 Secure Web for Android 版本 23.10.0	Secure Web 23.10.0：当前版本中的新增功能
17 Nov 2023	发布 Secure Mail for Android 版本 23.10.0	Secure Mail 23.10.0：缺陷修复
27 Oct 2023	发布 Secure Mail for Android 版本 23.8.2	Secure Mail 23.8.2：当前版本中的新增功能
19 Oct 2023	发布 Secure Hub for Android 版本 23.10.0	Secure Hub 23.10.0：当前版本中的新增功能
04 Oct 2023	发布 Secure Mail for Android 版本 23.7.0	Secure Mail 23.7.0：当前版本中的新增功能

日期	更改	说明
04 Oct 2023	发布 Secure Mail for iOS 版本 23.7.0	Secure Mail 23.7.0：当前版本中的新增功能
29 Sep 2023	发布 Secure Mail for Android 版本 23.8.1	Secure Mail 23.8.1：当前版本中的新增功能
20 Sep 2023	发布 Secure Web for iOS 版本 23.9.0	Secure Web 23.9.0：当前版本中的新增功能
20 Sep 2023	发布 Secure Mail for iOS 版本 23.9.0	Secure Mail 23.9.0：当前版本中的新增功能
20 Sep 2023	发布 Secure Web for Android 版本 23.8.0	Secure Web 23.8.0：当前版本中的新增功能
20 Sep 2023	发布 Secure Mail for Android 版本 23.8.0	Secure Mail 23.8.0：当前版本中的新增功能
01 Sep 2023	发布 Secure Hub for Android 版本 23.9.0	Secure Hub 23.9.0：当前版本中的新增功能
25 Aug 2023	发布 Secure Hub for iOS 版本 23.8.1	Secure Hub 23.8.1：当前版本中的新增功能
08 Aug 2023	发布 Secure Hub for iOS 版本 23.8.0	Secure Hub 23.8.0：当前版本中的新增功能
31 Jul 2023	发布 Secure Web for Android 版本 23.7.0	Secure Web 23.7.0：当前版本中的新增功能
31 Jul 2023	发布 Secure Mail for Android 版本 23.7.0	Secure Mail 23.7.0：当前版本中的新增功能
26 Jul 2023	发布 Secure Hub for Android 版本 23.7.0	Secure Hub 23.7.0：当前版本中的新增功能
07 Jul 2023	发布 Secure Hub for iOS 版本 23.4.0	Secure Hub 23.4.0：当前版本中的新增功能
22 Jun 2023	添加了已知问题 CXM-110137	Secure Mail for Android 已知问题

日期	更改	说明
07 Jun 2023	发布 Secure Mail for Android 版本 23.6.0	Secure Mail 23.6.0：当前版本中的新增功能
31 May 2023	发布 Secure Web for iOS 版本 23.5.0	Secure Web 23.5.0：当前版本中的新增功能
31 May 2023	发布 Secure Mail for iOS 版本 23.5.0	Secure Mail 23.5.0：当前版本中的新增功能
26 May 2023	发布 Secure Hub for Android 版本 23.4.0	Secure Hub 23.4.0：当前版本中的新增功能
23 May 2023	发布 Secure Hub for Android 版本 23.2.0	Secure Hub 23.2.0：当前版本中的新增功能
12 Apr 2023	发布 Secure Web for Android 版本 23.3.5	添加了已知问题
28 Mar 2023	发布 Secure Web for Android 版本 23.3.5	Secure Web 23.3.5：当前版本中的新增功能
28 Mar 2023	发布 Secure Mail for Android 版本 23.3.5	Secure Mail 23.3.5：当前版本中的新增功能
09 Jan 2023	发布 Secure Hub for Android 版本 22.11.0	Secure Hub 22.11.0：当前版本中的新增功能
01 Feb 2023	发布 Secure Web for iOS 和 Secure Mail for Android 版本 23.2.0	Secure Web 23.2.0：当前版本中的新增功能
01 Feb 2023	发布 Secure Mail for Android 版本 23.2.0	Secure Mail 23.2.0：当前版本中的新增功能
28 Oct 2022	发布 Secure Mail for Android 版本 22.11.0	Secure Mail 22.11.0：当前版本中的新增功能
12 Oct 2022	发布 Secure Hub for Android 版本 22.9.0	Secure Hub 22.9.0：当前版本中的新增功能
28 Sep 2022	发布 Secure Mail for Android 版本 22.9.0	Secure Mail 22.9.0：当前版本中的新增功能

日期	更改	说明
28 Sep 2022	发布 Secure Web for Android 版本 22.9.0	Secure Web 22.9.0：当前版本中的新增功能
08 Sep 2022	发布 Secure Web for iOS 版本 22.9.1	Secure Web 22.9.1：当前版本中的新增功能
07 Sep 2022	发布 Secure Web for iOS 版本 22.9.0	Secure Web 22.9.0：当前版本中的新增功能
07 Sep 2022	Secure Mail 22.9.0 的发布	Secure Mail 22.9.0：当前版本中的新增功能
01 Sep 2022	发布 Secure Web for iOS 版本 22.9.0	Secure Web 22.9.0 已于 2022 年 9 月 2 日回滚，我们正在进行积极修复，很快将公布该版本。
01 Sep 2022	Secure Mail 22.9.0 的发布	Secure Mail 22.9.0 已于 2022 年 9 月 2 日回滚，我们正在积极进行修复，很快将公布该版本。
26 Jul 2022	发布 Secure Hub for Android 版本 22.7.0	Secure Hub 22.7.0：当前版本中的新增功能
13 Jul 2022	发布 Secure Web for iOS 版本 22.6.0	Secure Web 22.6.0：当前版本中的新增功能
14 Jun 2022	Secure Mail 22.6.0 的发布	Secure Mail 22.6.0：当前版本中的新增功能
14 Jun 2022	发布 Secure Web for Android 版本 22.6.0	Secure Web 22.6.0：当前版本中的新增功能
14 Jun 2021	发布 Secure Hub for Android 版本 22.6.0	Secure Hub 22.6.0：当前版本中的新增功能
09 Feb 2022	Secure Mail 22.2.0 的发布	Secure Mail 22.2.0：当前版本中的新增功能

日期	更改	说明
09 Feb 2022	发布 Secure Web 22.2.0	Secure Web 22.2.0：当前版本中的新增功能
08 Dec 2021	Secure Mail 21.12.0 的发布	Secure Mail 21.12.0：当前版本中的新增功能
08 Dec 2021	发布 Secure Web 21.12.0	Secure Web 21.12.0：当前版本中的新增功能
27 Oct 2021	Secure Mail 21.10.5 的发布	Secure Mail 21.10.5：当前版本中的新增功能
27 Oct 2021	发布 Secure Web 21.10.5	Secure Web 21.10.5：当前版本中的新增功能
13 Oct 2021	Secure Hub 21.10.0 的发布	Secure Hub 21.10.0：当前版本中的新增功能
13 Oct 2021	Secure Mail 21.10.0 的发布	Secure Mail 21.10.0：当前版本中的新增功能
13 Oct 2021	发布 Secure Web 21.10.0	Secure Web 21.10.0：当前版本中的新增功能
20 Sep 2021	Secure Mail 21.9.1 的发布	Secure Mail 21.9.1：当前版本中的新增功能
20 Sep 2021	发布 Secure Web 21.9.1	Secure Web 21.9.1：当前版本中的新增功能
08 Sep 2021	Secure Mail 21.9.0 的发布	Secure Mail 21.9.0：当前版本中的新增功能
08 Sep 2021	发布 Secure Web 21.9.0	Secure Web 21.9.0：当前版本中的新增功能
24 Aug 2021	发布 Secure Mail for Android 版本 21.8.5	Secure Mail 21.8.5：当前版本中的新增功能
24 Aug 2021	发布 Secure Web for Android 版本 21.8.5	Secure Web 21.8.5：当前版本中的新增功能

日期	更改	说明
13 Aug 2021	发布 Secure Hub for iOS 版本 21.8.0	Secure Hub 21.8.0：当前版本中的新增功能
13 Aug 2021	Secure Mail 21.8.0 的发布	Secure Mail 21.8.0：当前版本中的新增功能
13 Aug 2021	发布 Secure Web 21.8.0	Secure Web 21.8.0：当前版本中的新增功能
10 Aug 2021	发布 Secure Hub for Android 版本 21.7.1	Secure Hub 21.7.1：当前版本中的新增功能
15 Jul 2021	Secure Mail 21.7.0 的发布	Secure Mail 21.7.0：当前版本中的新增功能
15 Jul 2021	发布 Secure Web 21.7.0	Secure Web 21.7.0：当前版本中的新增功能
07 Jul 2021	发布 Secure Hub for iOS 版本 21.7.0	Secure Hub 21.7.0：当前版本中的新增功能
06 Jul 2021	发布 Secure Hub for Android 版本 21.7.0	Secure Hub 21.7.0：当前版本中的新增功能
24 Jun 2021	发布 Secure Mail for iOS 版本 21.6.0	Secure Mail 21.6.0：当前版本中的新增功能
16 Jun 2021	Secure Hub 21.6.0 的发布	Secure Hub 21.6.0：当前版本中的新增功能
16 Jun 2021	发布 Secure Mail for Android 版本 21.6.0	Secure Mail 21.6.0：当前版本中的新增功能
16 Jun 2021	发布 Secure Web 21.6.0	Secure Web 21.6.0：当前版本中的新增功能
20 May 2021	Secure Hub 21.5.1 的发布	Secure Hub 21.5.1：当前版本中的新增功能
12 May 2021	发布 Secure Hub 21.5.0	Secure Hub 21.5.0：当前版本中的新增功能

日期	更改	说明
12 May 2021	发布 Secure Mail 21.5.0	Secure Mail 21.5.0：当前版本中的新增功能
12 May 2021	发布 Secure Web for iOS 版本 21.5.0	Secure Web 21.5.0：缺陷修复
04 May 2021	发布 Secure Mail for Android 版本 21.4.5	Secure Mail 21.4.5：当前版本中的新增功能
04 May 2021	发布 Secure Web for Android 版本 21.4.5	Secure Web 21.4.5：缺陷修复
15 Apr 2021	发布 Secure Hub 版本 21.4.0	Secure Hub 21.4.0：当前版本中的新增功能
15 Apr 2021	发布 Secure Mail for iOS 版本 21.4.0	Secure Mail 21.4.0：缺陷修复
31 Mar 2021	发布 Secure Hub for iOS 版本 21.3.2	Secure Hub 21.3.2：缺陷修复
30 Mar 2021	发布 Secure Mail for Android 版本 21.3.5	Secure Mail 21.3.5：当前版本中的新增功能
30 Mar 2021	发布 Secure Web for Android 版本 21.3.5	Secure Web 21.3.0：缺陷修复
22 Mar 2021	发布 Secure Mail for iOS 版本 21.3.0	Secure Mail 21.3.0：当前版本中的新增功能
17 Mar 2021	Secure Hub 21.3.0 的发布	Secure Hub 21.3.0：缺陷修复
17 Mar 2021	发布 Secure Mail for Android 版本 21.3.0	Secure Mail 21.3.0：当前版本中的新增功能
17 Mar 2021	发布 Secure Web for Android 版本 21.3.0	Secure Web 21.3.0：缺陷修复
24 Feb 2021	发布 Secure Mail 21.2.0	Secure Mail 21.2.0：当前版本中的新增功能

日期	更改	说明
24 Feb 2021	发布 Secure Web 21.2.0	Secure Web 21.2.0：当前版本中的新增功能
18 Feb 2021	发布 Secure Hub for Android 版本 21.2.0	Secure Hub 21.2.0：缺陷修复
01 Feb 2021	发布 Secure Mail for iOS 版本 21.1.5	Secure Mail 21.1.5：缺陷修复
01 Feb 2021	发布 Secure Web for iOS 版本 21.1.5	Secure Web 21.1.5：缺陷修复
14 Jan 2021	发布 Secure Mail 21.1.0	Secure Mail 21.1.0：缺陷修复
14 Jan 2021	发布 Secure Web 21.1.0	Secure Web 21.1.0：缺陷修复
12 Jan 2021	Secure Hub 21.1.0 的发布	Secure Web 21.1.0：缺陷修复
15 Dec 2020	发布 Secure Hub 20.12.0	Secure Hub 20.12.0：当前版本中的新增功能
15 Dec 2020	发布 Secure Mail for iOS 版本 20.12.0	Secure Mail 20.12.0：缺陷修复
15 Dec 2020	发布 Secure Web for iOS 版本 20.12.0	Secure Web 20.12.0：缺陷修复
19 Nov 2020	发布 Secure Hub for Android 版本 20.11.0	Secure Hub 20.11.0：当前版本中的新增功能
19 Nov 2020	发布 Secure Mail for Android 版本 20.11.0	Secure Mail 20.11.0：当前版本中的新增功能
19 Nov 2020	发布 Secure Web for Android 版本 20.11.0	Secure Web 20.11.0：缺陷修复
17 Nov 2020	发布 Secure Mail for iOS 版本 20.11.0	Secure Mail 20.11.0：当前版本中的新增功能

日期	更改	说明
17 Nov 2020	发布 Secure Web for iOS 版本 20.11.0	Secure Web 20.11.0：缺陷修复
27 Oct 2020	Secure Mail 20.10.5 的发布	Secure Mail 20.10.5：当前版本中的新增功能
27 Oct 2020	发布 Secure Web for Android 版本 20.10.5	Secure Web 20.10.5：当前版本中的新增功能
27 Oct 2020	发布 Secure Hub for iOS 版本 20.10.5	Secure Hub 20.10.5：缺陷修复
21 Oct 2020	发布 Secure Hub for Android 版本 20.10.5	Secure Hub 20.10.5：缺陷修复
15 Oct 2020	发布 Secure Mail 20.10.0	Secure Mail 20.10.0：当前版本中的新增功能
15 Oct 2020	发布 Secure Web for Android 版本 20.10.0	Secure Mail 20.10.0：当前版本中的新增功能
29 Sep 2020	发布 Secure Mail for Android 版本 20.9.5	Secure Mail 20.9.5：缺陷修复
29 Sep 2020	发布 Secure Web for iOS 版本 20.9.5	Secure Web 20.9.5：缺陷修复
17 Sep 2020	发布 Secure Mail 20.9.0	Secure Mail 20.9.0：缺陷修复
17 Sep 2020	发布 Secure Web for Android 版本 20.9.0	Secure Web 20.9.0：当前版本中的新增功能
04 Sep 2020	发布 Secure Hub 20.9.0	Secure Hub 20.9.0：当前版本中的新增功能
27 Aug 2020	发布 Secure Mail 20.8.5	Secure Mail 20.8.5：当前版本中的新增功能
27 Aug 2020	发布 Secure Web 20.8.5	Secure Web 20.8.5：当前版本中的新增功能

日期	更改	说明
20 Aug 2020	发布 Secure Hub 20.7.5	Secure Hub 20.7.5：当前版本中的新增功能
19 Aug 2020	发布 Secure Mail 20.8.0	Secure Mail 20.8.0：当前版本中的新增功能
19 Aug 2020	发布 Secure Web 20.8.0	Secure Web 20.8.0：当前版本中的新增功能
12 Aug 2020	Citrix ShareConnect 已达到生命周期已结束 (EOL) 状态。	有关详细信息，请参阅产品列表中的产品生命周期里程碑。
29 Jul 2020	发布 Secure Mail 版本 20.7.5	Secure Mail 20.7.5：当前版本中的新增功能
29 Jul 2020	发布 Secure Web 版本 20.7.5	Secure Web 20.7.5：缺陷修复
14 Jul 2020	发布 Secure Mail 版本 20.7.0	Secure Mail 20.7.0：缺陷修复
14 Jul 2020	发布 Secure Web 版本 20.7.0	Secure Web 20.7.0：当前版本中的新增功能
10 Jul 2020	启用在 iOS 设备上配置的代理，以使用在 Wi-Fi 设置中配置的代理服务器。	请参阅 Secure Hub 中的新增功能中的详细信息
06 Jul 2020	应用程序从 32 位转换为 64 位。将 Android 设备升级到 Secure Hub 版本 20.6.5，以避免升级到更高版本时重新进行身份验证。	请参阅 Secure Hub 中的新增功能中的详细信息
01 Jul 2020	Secure Hub 20.6.5 的发布	Secure Hub 20.6.5：缺陷修复
01 Jun 2020	发布 Secure Mail 20.6.5	Secure Mail 20.6.5：缺陷修复

日期	更改	说明
19 Jun 2020	适用于 QuickEdit 的平台加密	请参阅 适用于 QuickEdit 的加密 中的详细信息
16 Jun 2020	发布 Secure Mail 20.6.0	Secure Mail 20.6.0： 缺陷修复
16 Jun 2020	发布 Secure Web 20.6.0	Secure Web 20.6.0： 缺陷修复
02 Jun 2020	MDX 加密生命周期即将结束。所有设备都必须在 2020 年 9 月 1 日之前迁移到平台加密	请参阅 最新声明 中的详细信息
19 May 2020	发布 Secure Mail for iOS 版本 20.5.0	Secure Mail 20.5.0： 缺陷修复
19 May 2020	发布 Secure Web for iOS 版本 20.5.0	Secure Web 20.5.0： 缺陷修复
11 May 2020	发布 Secure Mail for iOS 版本 20.4.5	Secure Mail 20.4.5： 当前版本中的新增功能
11 May 2020	发布 Secure Web for iOS 版本 20.4.5	Secure Web 20.4.5： 当前版本中的新增功能
28 Apr 2020	发布 Secure Mail for Android 版本 20.4.5	Secure Mail 20.4.5： 当前版本中的新增功能
28 Apr 2020	发布 Secure Web for Android 版本 20.4.5	Secure Web 20.4.5： 缺陷修复
21 Apr 2020	发布 Secure Mail for iOS 版本 20.4.0	Secure Mail 20.4.0： 当前版本中的新增功能
21 Apr 2020	发布 Secure Web for iOS 版本 20.4.0	Secure Web 20.4.0： 缺陷修复
14 Apr 2020	发布 Secure Mail for Android 版本 20.4.0	Secure Mail 20.4.0： 当前版本中的新增功能

日期	更改	说明
14 Apr 2020	发布 Secure Web for Android 版本 20.4.0	Secure Web 20.4.0：缺陷修复
31 Mar 2020	发布 Secure Hub for iOS 版本 20.3.0	Secure Hub 20.3.0：当前版本中的新增功能
24 Mar 2020	发布 Secure Mail 版本 20.3.0	Secure Mail 20.3.0：当前版本中的新增功能
24 Mar 2020	发布 Secure Web 版本 20.3.0	Secure Web 20.3.0：缺陷修复
11 Feb 2020	发布 Secure Hub for iOS 版本 20.2.0	Secure Hub 20.2.0：缺陷修复
11 Feb 2020	发布 Secure Mail 版本 20.2.0	Secure Mail 20.2.0：当前版本中的新增功能
29 Jan 2020	发布 Secure Hub 版本 20.1.5	Secure Hub 20.1.5：缺陷修复
29 Jan 2020	发布 Secure Mail 版本 20.1.5	Secure Mail 20.1.5：当前版本中的新增功能
07 Jan 2020	发布 Secure Mail 20.1.0	Secure Mail 20.1.0：当前版本中的新增功能
12 Dec 2019	发布 Secure Hub 19.12.5	Secure Hub 19.12.5：缺陷修复
12 Dec 2019	发布 Secure Mail 版本 19.12.5	Secure Mail 19.12.5：当前版本中的新增功能
12 Dec 2019	发布 Secure Web 19.10.5	Secure Web 19.12.5：缺陷修复
13 Nov 2019	发布 Secure Mail 19.11.5	Secure Mail 19.11.5：当前版本中的新增功能
13 Nov 2019	发布 Secure Web 19.11.5	Secure Web 19.11.5：缺陷修复

日期	更改	说明
06 Nov 2019	发布 Secure Hub 19.11.5	Secure Hub 19.11.5：缺陷修复
22 Oct 2019	发布 Secure Mail for iOS 19.10.6	Secure Mail for iOS 19.10.6：缺陷修复
15 Oct 2019	发布 Secure Mail 19.10.5	Secure Mail 19.10.5：当前版本中的新增功能
15 Oct 2019	发布 Secure Web 19.10.5	Secure Web 19.10.5：缺陷修复
14 Oct 2019	发布 Secure Hub for Android 版本 19.10.5	Secure Hub 19.10.5：当前版本中的新增功能
03 Oct 2019	发布 Secure Hub for iOS 版本 19.10.0	Secure Hub 19.10.0：缺陷修复
03 Oct 2019	发布 Secure Mail for iOS 版本 19.10.0	Secure Mail 19.10.0：当前版本中的新增功能
03 Oct 2019	发布 Secure Web for iOS 版本 19.10.0	Secure Web 19.10.0：当前版本中的新增功能
01 Oct 2019	发布 Secure Mail for Android 版本 19.10.0	Secure Mail 19.10.0：当前版本中的新增功能
01 Oct 2019	发布 Secure Web for Android 版本 19.10.0	Secure Web 19.10.0：当前版本中的新增功能
24 Sep 2019	发布 Secure Hub for Android 版本 19.10.0	Secure Hub 19.10.0：缺陷修复
19 Sep 2019	发布 Secure Mail for iOS 版本 19.9.5	Secure Mail 19.9.5：当前版本中的新增功能
19 Sep 2019	发布 Secure Web for iOS 版本 19.9.5	Secure Web 19.9.5：缺陷修复
17 Sep 2019	发布 Secure Mail for Android 版本 19.9.5	Secure Mail 19.9.5：当前版本中的新增功能

日期	更改	说明
17 Sep 2019	发布 Secure Web for Android 版本 19.9.5	Secure Web 19.9.5：当前版本中的新增功能
11 Sep 2019	发布 Secure Hub for Android 版本 19.9.5	Secure Hub 19.9.5：当前版本中的新增功能
04 Sep 2019	发布 Secure Mail 19.9.0	Secure Mail 19.9.0：当前版本中的新增功能
04 Sep 2019	发布 Secure Web 19.9.0	Secure Web 19.9.0：当前版本中的新增功能
03 Sep 2019	发布 Secure Hub 19.9.0	Secure Hub 19.9.0：当前版本中的新增功能
23 Aug 2019	发布 Secure Hub 19.8.5	Secure Hub 19.8.5：当前版本中的新增功能
23 Aug 2019	发布 Secure Mail for Android 版本 19.8.5	Secure Mail 19.8.5：性能增强和缺陷修复
23 Aug 2019	发布 Secure Web for Android 版本 19.8.5	Secure Web 19.8.5：性能增强和缺陷修复
09 Aug 2019	发布 Secure Mail for Android 版本 19.8.0	Secure Mail 19.8.0：当前版本中的新增功能
09 Aug 2019	发布 Secure Web for Android 版本 19.8.0	Secure Web 19.8.0：性能增强功能和缺陷修复
31 Jul 2019	Secure Hub 19.8.0 的发布	Secure Hub 19.8.0：当前版本中的新增功能
02 Aug 2019	发布 Secure Mail for iOS 版本 19.8.0	Secure Mail 19.8.0：当前版本中的新增功能
02 Aug 2019	发布 Secure Web for iOS 版本 19.8.0	Secure Web 19.8.0：性能增强功能和缺陷修复
18 Jul 2019	发布 Secure Hub 版本 19.7.5	Secure Hub 19.7.5：当前版本中的新增功能

日期	更改	说明
18 Jul 2019	发布 Secure Mail 版本 19.7.5	Secure Mail 19.7.5： 当前版本中的新增功能
18 Jul 2019	发布 Secure Web 版本 19.7.5	Secure Web 19.7.5： 性能增强功能和缺陷修复
30 Jun 2019	发布 Secure Hub iOS 19.6.6	Secure Hub for iOS 19.6.6： 性能增强和缺陷修复
27 Jun 2019	Secure Mail 19.6.5 for Android 的新增功能列表	Secure Mail 19.6.5： 当前版本中的新增功能
27 Jun 2019	发布 Secure Web 19.6.5	Secure Web 19.6.5： 性能增强功能和缺陷修复
26 Jun 2019	发布 Secure Hub 19.6.5	Secure Hub 19.6.5： 已知问题
17 Jun 2019	Secure Mail for iOS 19.5.5 的新增功能列表	Secure Mail 19.5.5： 当前版本中的新增功能
05 Jun 2019	发布了适用于 Android 的 Secure Hub、Secure Mail 和 Secure Web 版本 19.5.5	要了解 Secure Mail 和 Secure Web 的分阶段发布过程，请参阅 移动生产力应用程序发布时间表
23 May 2019	有关适用于 Android 的 Secure Mail 草稿同步功能的时长为一分钟的视频	添加了有关在版本 19.5.0 中发布的 Secure Mail for Android 的草稿文件夹同步功能的视频： 草稿文件夹自动同步
08 May 2019	发布 Secure Hub 19.5.0	Secure Hub 19.5.0 已知问题和已修复的问题
08 May 2019	发布 Secure Mail 19.5.0	Secure Mail 19.5.0 已修复的问题
08 May 2019	发布 Secure Web 19.5.0	Secure Web 19.5.0 已修复的问题

日期	更改	说明
05 Apr 2019	Secure Hub 19.3.5 的发布	Secure Hub 19.3.5 已知问题和已修复的问题
05 Apr 2019	Secure Mail 19.3.5 的发布	Secure Mail 19.3.5 已修复的问题
05 Apr 2019	Secure Web 19.3.5 的发布	Secure Web 19.3.5 已修复的问题