



Secure Hub

Contents

Citrix 安全中心™	19
管理 Secure Hub	19
Citrix 个人识别码	19
证书锁定	20
为 Secure Hub 配置证书 + 一次性密码身份验证	21
适用于 Android 设备的 ADS 连接端口要求	25
Secure Hub 功能	27
思杰安全中心™	30
当前版本中的新增功能	30
适用于 iOS 的 Secure Hub 26.8.1	30
适用于 Android 的 Secure Hub 26.8.0	30
在 COSU 模式下，在启动器配置策略中设置自动启动应用程序	30
MDM 设备证书的自动检测和续订	30
早期版本中的新增功能	31
适用于 iOS 的 Secure Hub 26.8.0	31
支持 iOS/iPadOS 27	31
适用于 Android 的 Secure Hub 26.5.0	31
支持 Android 17	31
适用于 Android 的 Secure Hub 26.2.0	31
设备证书故障排除增强功能	31
适用于 iOS 的 Secure Hub 25.8.0	31
支持 iOS 26	31
适用于 Android 的 Secure Hub 25.10.0	32
支持 16KB 内存页面大小	32
适用于 Android 的 Secure Hub 25.7.0	32
适用于 iOS 的 Secure Hub 25.6.0	32

适用于 Android 的 Secure Hub 25.4.0	32
支持 Android 16	32
支持 TLS 1.3 协议	32
适用于 Android 的 Secure Hub 25.1.0	32
适用于 iOS 的 Secure Hub 25.1.0	33
适用于 iOS 的 Secure Hub 24.11.0	33
适用于 Android 的 Secure Hub 24.10.0	33
支持 Android 15	33
适用于 iOS 的 Secure Hub 24.9.0	33
在设备注册计划中显示条款和条件	33
适用于 Android 的 Secure Hub 24.8.0	33
Android 设备上的合规性检查（技术预览版）	33
适用于 Android 的 Secure Hub 24.6.0	34
改进的日志收集和报告	34
适用于 iOS 的 Secure Hub 24.5.0	35
支持 iOS 17 返回服务	35
适用于 Android 的 Secure Hub 24.3.0	35
支持 Samsung Knox 增强型认证 v3	35
适用于 Android 的 Secure Hub 23.12.0	36
使用 Samsung Knox 增强安全性	36
从用户的个人资料访问 Secure Mail	36
适用于 iOS 的 Secure Hub 24.1.0	37
适用于 Android 的 Secure Hub 23.12.0	37
在登录页面上添加有关身份验证 PIN 的提示	37
nFactor 身份验证支持单点登录功能	37
在直接启动模式下支持完全擦除	37
优化了 Secure Hub 应用商店的加载速度	37
适用于 iOS 的 Secure Hub 23.11.0	37

在登录页面上添加有关身份验证 PIN 的提示	37
nFactor 身份验证支持单点登录功能	38
安全中心 23.10.0	38
适用于 Android 的 Secure Hub	38
安全中心 23.9.0	38
适用于 Android 的 Secure Hub	38
安全中心 23.8.1	38
适用于 iOS 的 Secure Hub	38
安全中心 23.8.0	38
适用于 iOS 的 Secure Hub	38
安全中心 23.7.0	38
适用于 Android 的 Secure Hub	38
安全中心 23.4.0	39
适用于 iOS 的 Secure Hub	39
安全中心 23.4.1	40
适用于 Android 的 Secure Hub	40
安全中心 23.4.0	40
适用于 Android 的 Secure Hub	40
安全中心 23.2.0	40
适用于 Android 的 Secure Hub	40
安全中心 22.11.0	41
适用于 Android 的 Secure Hub	41
安全中心 22.9.0	41
适用于 Android 的 Secure Hub	41
安全中心 22.7.0	42
适用于 Android 的 Secure Hub	42
安全中心 22.6.0	42
适用于 Android 的 Secure Hub	42

安全中心 22.5.0	42
适用于 iOS 的 Secure Hub	42
安全中心 22.4.0	42
适用于 Android 的 Secure Hub	42
安全中心 22.2.0	42
适用于 iOS 的 Secure Hub	42
适用于 Android 的 Secure Hub	43
安全中心 21.11.0	43
适用于 Android 的 Secure Hub	43
安全中心 21.10.0	43
适用于 iOS 的 Secure Hub	43
适用于 Android 的 Secure Hub	43
安全中心 21.8.0	43
适用于 iOS 的 Secure Hub	43
安全中心 21.7.1	43
适用于 Android 的 Secure Hub	43
安全中心 21.7.0	44
适用于 iOS 的 Secure Hub	44
适用于 Android 的 Secure Hub	44
安全中心 21.6.0	44
适用于 iOS 的 Secure Hub	44
适用于 Android 的 Secure Hub	44
安全中心 21.5.1	44
适用于 iOS 的 Secure Hub	44
适用于 Android 的 Secure Hub	44
安全中心 21.5.0	44
适用于 iOS 的 Secure Hub	44
安全中心 21.4.0	44

安全中心 21.3.2	45
适用于 iOS 的 Secure Hub	45
安全枢纽 21.3.0	45
安全枢纽 21.2.0	45
适用于 Android 的 Secure Hub	45
Secure Hub 21.1.0 版本	45
适用于 iOS 的 Secure Hub	45
适用于 Android 的 Secure Hub	45
Secure Hub 20.12.0 版本	45
适用于 iOS 的 Secure Hub	45
适用于 Android 的 Secure Hub	45
安全中心 20.11.0	45
适用于 Android 的 Secure Hub	45
安全中心 20.10.5	45
Secure Hub 20.9.0 版本	46
适用于 iOS 的 Secure Hub	46
适用于 Android 的 Secure Hub	46
Secure Hub 20.7.5 版本	46
适用于 Android 的 Secure Hub	46
安全中心 20.6.5	46
适用于 Android 的 Secure Hub	46
适用于 iOS 的 Secure Hub	47
安全中心 20.3.0	47
适用于 iOS 的 Secure Hub	47
安全枢纽 20.2.0	47
适用于 iOS 的 Secure Hub	47
安全枢纽 20.1.5	47
安全枢纽 19.12.5	48

安全枢纽 19.11.5	48
安全枢纽 19.10.5	48
适用于 Android 的 Secure Hub	48
安全中心 19.10.0	48
安全中心 19.9.5	48
适用于 iOS 的 Secure Hub	48
适用于 Android 的 Secure Hub	48
安全中心 19.9.0	48
适用于 iOS 的 Secure Hub	48
适用于 Android 的 Secure Hub	48
适用于 Android 的 Secure Hub 19.8.5	49
安全中心 19.8.0	49
适用于 iOS 的 Secure Hub	49
适用于 Android 的 Secure Hub	49
安全中心 19.7.5	49
适用于 iOS 的 Secure Hub	49
适用于 Android 的 Secure Hub	49
Secure Hub 版本 19.3.5 到 19.6.6	49
Secure Hub 版本 19.3.0	49
安全中心 19.2.0	50
安全中心 19.1.5	50
安全中心 19.1.0	50
安全中心 18.12.0	50
安全中心 18.11.5	50
安全中心 18.10.0	50
安全中心 10.8.60 到 18.9.0	51
安全中心 10.8.60	51
Secure Hub 10.8.55 版本	52

管理 Secure Hub	53
Citrix 个人识别码	53
证书锁定	53
证书 + 一次性密码身份验证	54
Android 设备连接 ADS 的端口要求	57
禁用“删除帐户”选项	59
使用 Secure Hub	59
自动注册 Secure Mail	61
自定义应用商店	62
配置的帮助选项	63
位置策略	64
崩溃收集和分析	64
生成 Secure Hub 的设备端日志	64
已知和已修复的问题	66
适用于 iOS 的 Secure Hub 26.8.1	66
已修复的问题	66
已知问题	66
适用于 Android 的 Secure Hub 26.8.0	66
已修复的问题	66
已知问题	66
适用于 iOS 的 Secure Hub 26.8.0	67
已修复问题	67
已知问题	67
适用于 Android 26.5.0 的 Secure Hub	67
已修复问题	67
已知问题	67
适用于 Android 的 Secure Hub 26.2.0	67
已修复问题	67

已知问题	67
适用于 Android 的 Secure Hub 25.10.0	68
已修复问题	68
已知问题	68
适用于 iOS 的 Secure Hub 25.8.0	68
已修复问题	68
已知问题	68
适用于 Android 的 Secure Hub 25.7.0	68
已修复问题	68
已知问题	68
适用于 iOS 的 Secure Hub 25.6.0	68
已修复问题	68
已知问题	69
适用于 Android 的 Secure Hub 25.4.0	69
已修复问题	69
已知问题	69
适用于 iOS 的 Secure Hub 25.1.0	69
已修复问题	69
已知问题	69
适用于 Android 的 Secure Hub 25.1.0	69
已修复问题	69
已知问题	69
适用于 iOS 的 Secure Hub 24.11.0	70
已修复的问题	70
已知问题	70
适用于 Android 的 Secure Hub 24.10.0	70
已修复的问题	70
已知问题	70

适用于 iOS 的 Secure Hub 24.9.0	70
已修复的问题	70
已知问题	70
适用于 Android 的 Secure Hub 24.8.0	70
已修复的问题	70
已知问题	70
适用于 Android 的 Secure Hub 24.6.0	71
已修复的问题	71
已知问题	71
适用于 iOS 的 Secure Hub 24.5.0	71
已修复的问题	71
已知问题	71
适用于 Android 的 Secure Hub 24.3.0	71
已修复问题	71
已知问题	71
适用于 iOS 的 Secure Hub 24.1.0	71
已修复问题	71
适用于 Android 23.12.0 的 Secure Hub	72
已修复的问题	72
适用于 iOS 23.11.0 的 Secure Hub	72
已修复的问题	72
适用于 Android 23.10.0 的 Secure Hub	72
已修复的问题	72
已知问题	72
适用于 Android 23.9.0 的 Secure Hub	73
已修复问题	73
已知问题	73
适用于 iOS 23.8.1 的 Secure Hub	73

已修复问题	73
已知问题	73
适用于 iOS 23.8.0 的 Secure Hub	73
已修复问题	73
已知问题	73
旧版本中的已知和已修复问题	73
Secure Hub 已知和已修复问题的历史记录	74
适用于 Android 23.7.0 的 Secure Hub	74
已修复的问题	74
已知问题	74
适用于 iOS 23.4.0 的 Secure Hub	74
已修复的问题	74
已知问题	74
适用于 Android 23.4.1 的 Secure Hub	75
已修复问题	75
已知问题	75
适用于 Android 23.4.0 的 Secure Hub	75
已修复问题	75
已知问题	75
适用于 Android 的 Secure Hub 23.2.0	75
已修复的问题	75
Secure Hub 22.11.0 版本	76
Secure Hub 22.9.0 版本	76
安全中心 22.7.0	76
已修复的问题	76
安全中心 22.6.0	76
安全中心 22.5.0	76
安全中心 22.4.0	76

安全中心 22.2.0	77
Secure Hub 22.2.0 中的已知问题	77
Secure Hub 22.2.0 中已修复的问题	77
适用于 iOS 的 Secure Hub	77
适用于 Android 的 Secure Hub	77
Secure Hub 21.11.0 版本	77
Secure Hub 21.11.0 中的已知问题	77
Secure Hub 21.11.0 中已修复的问题	78
适用于 Android 的 Secure Hub	78
安全中心 21.10.0	78
Secure Hub 21.10.0 中的已知问题	78
Secure Hub 21.10.0 中已修复的问题	78
适用于 iOS 的 Secure Hub	78
适用于 Android 的 Secure Hub	78
安全中心 21.8.0	78
适用于 iOS 的 Secure Hub	78
Secure Hub 21.8.0 中的已知问题	78
Secure Hub 21.8.0 中已修复的问题	78
安全中心 21.7.1	79
适用于 Android 的 Secure Hub	79
早期版本中的已知和已修复问题	79
安全中心 21.7.1	79
适用于 Android 的 Secure Hub	79
安全中心 21.7.0	79
适用于 iOS 的 Secure Hub	79
适用于 Android 的 Secure Hub	79
Secure Hub 21.7.0 中的已知问题	79
Secure Hub 21.7.0 中已修复的问题	79

安全中心 21.6.0	79
适用于 iOS 的 Secure Hub	79
Secure Hub 21.6.0 中的已知问题	79
Secure Hub 21.6.0 中已修复的问题	80
适用于 Android 的 Secure Hub	80
Secure Hub 21.6.0 中的已知问题	80
Secure Hub 21.6.0 中已修复的问题	80
安全中心 21.5.1	80
适用于 iOS 的 Secure Hub	80
适用于 Android 的 Secure Hub	80
安全中心 21.5.0	80
Secure Hub 21.5.0 中的已知问题	80
Secure Hub 21.5.0 中已修复的问题	80
安全中心 21.4.0	80
安全中心 21.3.2	81
适用于 iOS 的 Secure Hub	81
Secure Hub 21.3.2 中的已知问题	81
Secure Hub 21.3.2 中已修复的问题	81
安全中心 21.3.0	81
Secure Hub 21.3.0 中的已知问题	81
Secure Hub 21.3.0 中已修复的问题	81
安全中心 21.2.0	81
适用于 Android 的 Secure Hub	81
Secure Hub 21.2.0 中的已知问题	81
Secure Hub 21.2.0 中已修复的问题	81
安全中心 21.1.0	82
Secure Hub 21.1.0 中的已知问题	82
Secure Hub 21.1.0 中已修复的问题	82

安全中心 20.12.0	82
Secure Hub 20.12.0 中的已知问题	82
Secure Hub 20.12.0 中已修复的问题	82
安全中心 20.11.0	82
适用于 Android 的 Secure Hub	82
Secure Hub 20.11.0 中的已知问题	82
Secure Hub 20.11.0 中已修复的问题	83
安全中心 20.10.5	83
Secure Hub 20.10.5 中的已知问题	83
Secure Hub 20.10.5 中已修复的问题	83
安全中心 20.9.0	83
Secure Hub 20.9.0 中的已知问题	83
Secure Hub 20.9.0 中已修复的问题	83
安全中心 20.7.5	84
Secure Hub 20.7.5 中的已知问题	84
Secure Hub 20.7.5 中已修复的问题	84
安全中心 20.6.5	84
安全中心 20.3.0	84
适用于 iOS 的 Secure Hub	84
安全中心 20.2.0	84
适用于 iOS 的 Secure Hub	84
Secure Hub 20.2.0 中的已知问题	84
Secure Hub 20.2.0 中已修复的问题	84
安全中心 20.1.5	85
安全中心 19.12.5	85
Secure Hub 19.12.5 中的已知问题	85
Secure Hub 19.12.5 中已修复的问题	85
安全中心 19.11.5	85

Secure Hub 19.11.5 中的已知问题	85
Secure Hub 19.11.5 中已修复的问题	85
安全中心 19.10.5	85
适用于 Android 的 Secure Hub	85
Secure Hub 19.10.5 中的已知问题	85
Secure Hub 19.10.5 中已修复的问题	85
安全中心 19.10.0	86
Secure Hub 19.10.0 中的已知问题	86
Secure Hub 19.10.0 中已修复的问题	86
安全中心 19.9.5	86
安全中心 19.9.0	86
Secure Hub 19.9.0 中的已知问题	86
Secure Hub 19.9.0 中已修复的问题	86
安全中心 19.8.5	86
安全中心 19.8.0	86
Secure Hub 19.8.0 中的已知问题	86
Secure Hub 19.8.0 中已修复的问题	87
Secure Hub 19.7.5 版本	87
Secure Hub 19.7.5 中的已知问题	87
Secure Hub 19.7.5 中已修复的问题	87
安全中心 19.6.5	87
Secure Hub 19.6.5 中的已知问题	87
Secure Hub 19.6.5 中已修复的问题	87
安全中心 19.5.5	88
Secure Hub 19.5.5 中的已知问题	88
Secure Hub 19.5.5 中的已修复问题	88
安全中心 19.5.0	88
Secure Hub 19.5.0 中的已知问题	88

Secure Hub 19.5.0 中的已修复问题	88
安全中心 19.4.5	89
Secure Hub 19.4.5 中的已知问题	89
Secure Hub 19.4.5 中已修复的问题	89
安全中心 19.3.5	89
Secure Hub 19.3.5 中的已知问题	89
Secure Hub 19.3.5 中已修复的问题	89
安全中心 19.3.0	90
Secure Hub 19.3.0 中的已知问题	90
Secure Hub 19.3.0 中已修复的问题	90
安全中心 19.2.0	90
Secure Hub 19.2.0 中的已知问题	90
Secure Hub 19.2.0 中已修复的问题	90
安全中心 19.1.5	91
Secure Hub 19.1.5 中的已知问题	91
Secure Hub 19.1.5 中已修复的问题	91
安全中心 19.1.0	91
Secure Hub 19.1.0 中的已知问题	91
Secure Hub 18.12.0 中已修复的问题	91
安全中心 18.11.0	92
Secure Hub 18.11.0 中已修复的问题	92
安全中心 18.10.5	92
Secure Hub 18.10.5 中已修复的问题	92
Secure Hub 版本 10.8.25 到 18.10.6	92
Secure Hub 版本 10.8.25 到 18.10.6 中已修复的问题	92
安全中心 18.10.0	92
Secure Hub 18.10.0 中已修复的问题	92
安全中心 10.8.60	92

Secure Hub 10.8.60 中已修复的问题	92
安全中心 10.8.55	93
Secure Hub 10.8.55 中已修复的问题	93
版本 10.8.55 中与 MDX 相关的已修复问题	93
安全中心 10.8.55	93
Secure Hub 10.8.55 中的已知问题	93
安全中心 10.8.50	93
Secure Hub 10.8.50 中的已知问题	93
安全中心 10.8.35	93
Secure Hub 10.8.35 中已修复的问题	93
安全中心 10.8.25	94
Secure Hub 10.8.25 中已修复的问题	94
安全中心 10.8.20	94
Secure Hub 10.8.20 中已修复的问题	94
安全中心 10.8.15	94
Secure Hub 10.8.15 中已修复的问题	94
安全中心 10.8.10	94
Secure Hub 10.8.10 中已修复的问题	94
适用于 Android 和 iOS 的 Secure Hub - 预览版	95
功能标志管理	96
身份验证提示场景	97
凭据类型	98
关于 Secure Hub 屏幕翻转	100
设备密码的密码复杂性 (Android 12+)	101
使用派生凭据注册设备	102
使用派生凭据时的设备注册步骤	102
通过 Citrix Endpoint Management™ 控制台配置提示	108
将提示配置为文本	108

配置带网页链接的提示文本	108
在 Android 设备上合规性检查（技术预览版）	110

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

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

Integrate with Citrix Products

- XenMobile
- XenApp and XenDesktop
- Unified Gateway

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**。

The screenshot shows the 'Profiles' configuration interface. It includes sections for 'Profiles' (Net Profile, TCP Profile, HTTP Profile), 'Published Applications' (Next HOP Server, STA Server, Url), 'Other Settings' (ICMP Virtual Server Response, RHI State, Redirect to Home page, Listen Priority, Listen Policy Expression, ShareFile, AppController, L2 Connection), and 'Policies' (Request Policies, Session Policies, ClientlessAccess Policies, Cache Policies). A '+' icon in the Policies section is being clicked, opening a 'Choose Type' dialog box.

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**。

The 'Choose Type' dialog box is shown. It has a title bar 'Choose Type' and a section 'Policies'. Under 'Policies', there are two dropdown menus: 'Choose Policy*' with 'Rewrite' selected, and 'Choose Type*' with 'Response' selected. At the bottom, there are 'Continue' and 'Cancel' buttons. A hand icon is pointing at the 'Continue' button.

10. 点击 **继续**。

策略绑定 部分展开。

Choose Type

Choose Type

Policies

Choose Policy
Rewrite

Choose Type
Response

Policy Binding

Select Policy*
Click to select

Binding Details

Priority*
100

Goto Expression*
END

Bind Close

11. 点击 **选择策略**。

出现一个包含可用策略的屏幕。

Choose Type > Rewrite Policies

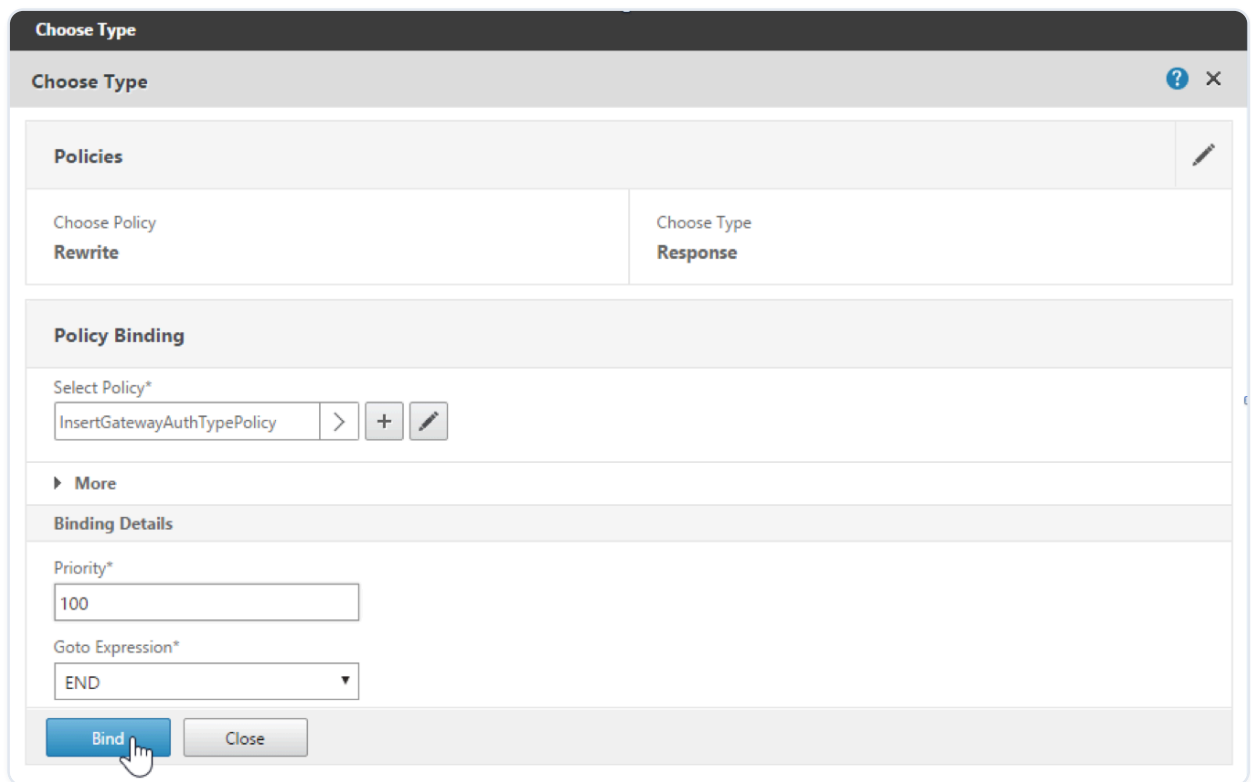
Rewrite Policies

Select Add Edit Delete Show Bindings Policy Manager Statistics Action

Show built-in Rewrite Policies Search

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	X

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.zenprise.com</code>	52.5.138.94	443	Secure Hub - ADS 通信
<code>discovery.mdm.zenprise.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。

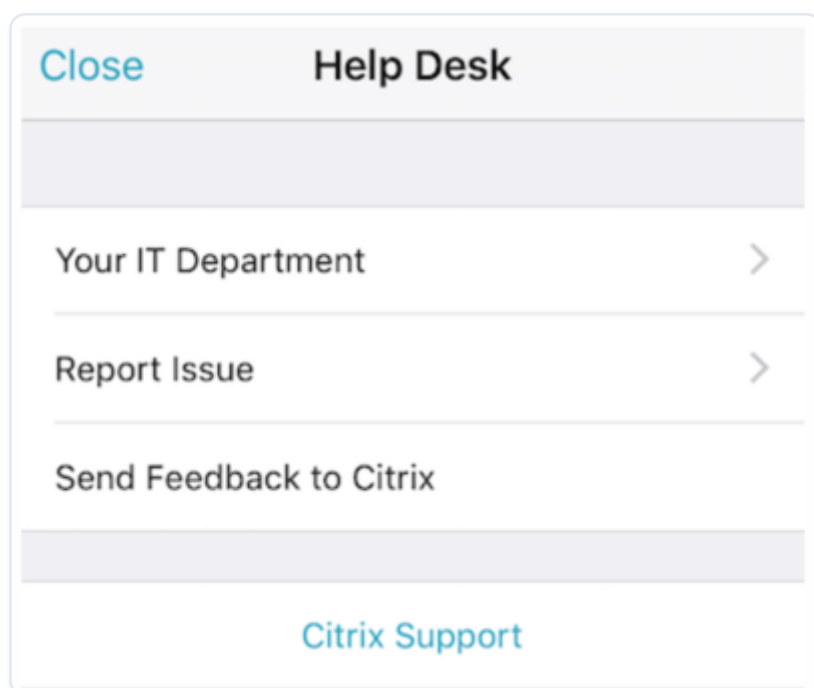
客户端品牌图像(/en-us/mobile-productivity-apps/media/worxhome-client-branding.png)

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。

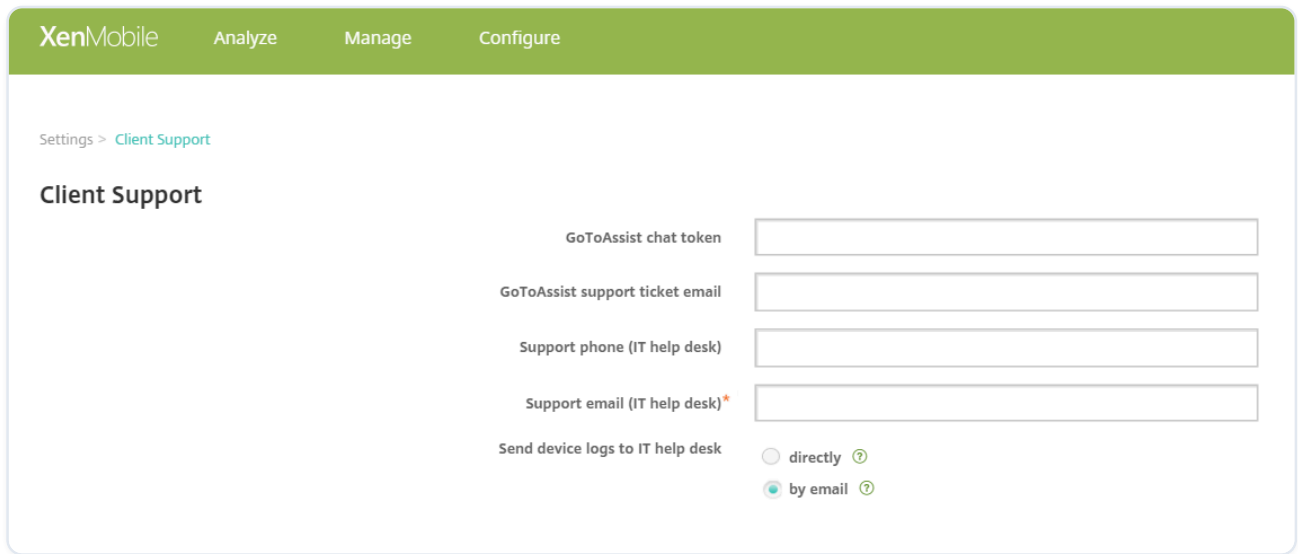
说明框的图像(/en-us/mobile-productivity-apps/media/worxhome-edit-app-descriptions-xm.png)

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，用户点击“**详细信息**”，然后点击“**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，用户点击左上角的汉堡菜单图标，然后点击“**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。



“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。

思杰安全中心™

Citrix Secure Hub 是移动生产力应用程序的启动平台。用户在 Secure Hub 中注册其设备以访问应用商店。从应用商店中，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。

您可以从 [Citrix Endpoint Management 下载页面](#) 下载 Secure Hub 和其他组件。

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

有关移动生产力应用程序的最新信息，请参阅 [最新公告](#)。

以下各节列出了 Secure Hub 当前版本和早期版本中的新功能。

注意：

Secure Hub 的 Android 9.x 和 iOS 11.x 版本的支持已于 2025 年 4 月结束。

当前版本中的新增功能

适用于 iOS 的 Secure Hub 26.8.1

此版本解决了一些有助于提高整体性能和稳定性的问题。

有关错误修复的更多信息，请参阅 [已知和已修复问题](#)。

适用于 Android 的 Secure Hub 26.8.0

在 COSU 模式下，在启动器配置策略中设置自动启动应用程序

在运行 Citrix Launcher 的 Android Enterprise 信息亭 (COSU) 设备上，管理员现在可以在启动器配置策略中设置一个自动启动应用程序，以在设备启动时自动启动一个托管应用程序。Secure Hub 会将此设置转发给 Citrix Launcher，由后者执行启动。

MDM 设备证书的自动检测和续订

适用于 Android 的 Secure Hub 现在可自动检测无效、缺失或过期的 MDM 设备证书，并在后台续订。这可在用户无需手动运行证书故障排除或重新注册设备的情况下恢复设备连接。

有关错误修复的更多信息，请参阅[已知问题和已修复问题](#)。

早期版本中的新增功能

适用于 iOS 的 Secure Hub 26.8.0

支持 iOS/iPadOS 27

从适用于 iOS 的 Secure Hub 26.8.0 版本开始，该应用程序与 iOS/iPadOS 27 兼容。您可以将设备升级到 iOS/iPadOS 27 并继续使用最新版本的 Secure Hub。

有关错误修复的更多信息，请参阅[已知问题和已修复问题](#)。

适用于 Android 的 Secure Hub 26.5.0

支持 Android 17

从适用于 Android 的 Secure Hub 26.5.0 版本开始，该应用程序与 Android 17 兼容。您可以将设备升级到 Android 17 并继续使用最新版本的 Secure Hub。

有关错误修复的更多信息，请参阅[已知问题和已修复问题](#)。

适用于 Android 的 Secure Hub 26.2.0

设备证书故障排除增强功能

从适用于 Android 的 Secure Hub 26.2.0 版本开始，Secure Hub 包含一个自助式设备证书故障排除工具，可帮助诊断和解决由吊销或无效客户端证书引起的设备连接问题。

当检测到证书问题时，该工具会自动尝试续订证书以恢复连接。要访问此工具，请转到 **帮助 > 故障排除 > 设备证书**，然后点击 **故障排除**。

设备证书故障排除图像(/en-us/mobile-productivity-apps/media/device-certificate-troubleshooting.png)

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 iOS 的 Secure Hub 25.8.0

支持 iOS 26

从适用于 iOS 的 Secure Hub 25.8.0 版本开始，该应用程序支持运行 iOS 26 的设备。升级到 Secure Hub 25.8.0 版本可确保对已更新到 iOS 26 的设备提供持续支持和兼容性。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 Android 的 Secure Hub 25.10.0

支持 16KB 内存页面大小

从适用于 Android 的 Secure Hub 25.10.0 版本开始，该应用程序支持 16KB 内存页面大小，以优化性能并符合 Google Play 要求。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 Android 的 Secure Hub 25.7.0

此版本解决了一些有助于提高整体性能和稳定性的问题。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 iOS 的 Secure Hub 25.6.0

此版本解决了若干问题，有助于提高整体性能和稳定性。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 Android 的 Secure Hub 25.4.0

支持 Android 16

从适用于 Android 的 Secure Hub 25.4.0 版本开始，此应用兼容 Android 16。您可以将设备升级到 Android 16 并继续使用最新版本的 Secure Hub。

支持 TLS 1.3 协议

从适用于 Android 的 Secure Hub 25.4.0 版本开始，此应用在 Android 设备上支持 TLS 1.3 协议。TLS 1.3 是 TLS 协议的最新版本，与 TLS 1.2 相比，它提供更快的性能、增强的安全性以及更强的抵御网络攻击的能力。TLS 1.3 还可降低网络延迟，从而实现更快的 HTTPS 连接和更好的用户体验。

要了解有关 TLS 1.3 的更多信息，请参阅[传输层安全 \(TLS\) 协议版本 1.3](#)。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 Android 的 Secure Hub 25.1.0

此版本解决了若干问题，有助于提高整体性能和稳定性。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 iOS 的 Secure Hub 25.1.0

此版本解决了若干问题，有助于提高整体性能和稳定性。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 iOS 的 Secure Hub 24.11.0

此版本解决了若干问题，有助于提高整体性能和稳定性。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 Android 的 Secure Hub 24.10.0

支持 Android 15

将 Secure Hub 版本升级到 24.10.0 可确保持续支持已更新到 Android 15 的设备。

有关错误修复的更多信息，请参阅[已知和已修复问题](#)。

适用于 iOS 的 Secure Hub 24.9.0

在设备注册计划中显示条款和条件

从适用于 iOS 的 Secure Hub 24.9.0 开始，管理员可以通过 Citrix Endpoint Management (CEM) 配置条款和条件设备策略。配置后，通过 Apple 设备注册计划 (DEP) 注册的设备在注册过程中将显示 **条款和条件** 页面。这可确保用户在完成注册之前查看并确认条款和条件，从而在设备载入期间增强合规性和安全性措施。

适用于 Android 的 Secure Hub 24.8.0

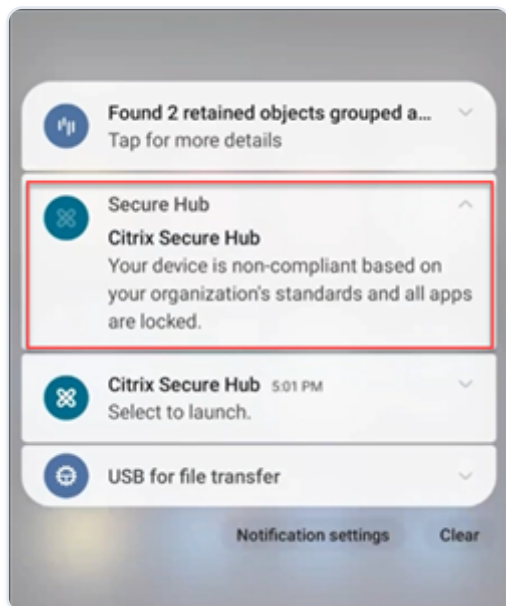
Android 设备上的合规性检查（技术预览版）

注意：

此功能适用于以 *设备所有者* 模式注册的 Android 设备。

从本版本开始，Secure Hub 会根据管理员通过 Citrix Endpoint Management 配置的策略验证 Android 设备的合规性。这些合规性检查包括确保设备密码强度、验证强制应用程序的安装以及确认禁止应用程序的删除。

如果设备被发现不符合管理员设置的策略，Secure Hub 会锁定其所有应用程序，并提示用户解决合规性问题以将其解锁。当设备不合规时，用户设备上会出现以下通知。

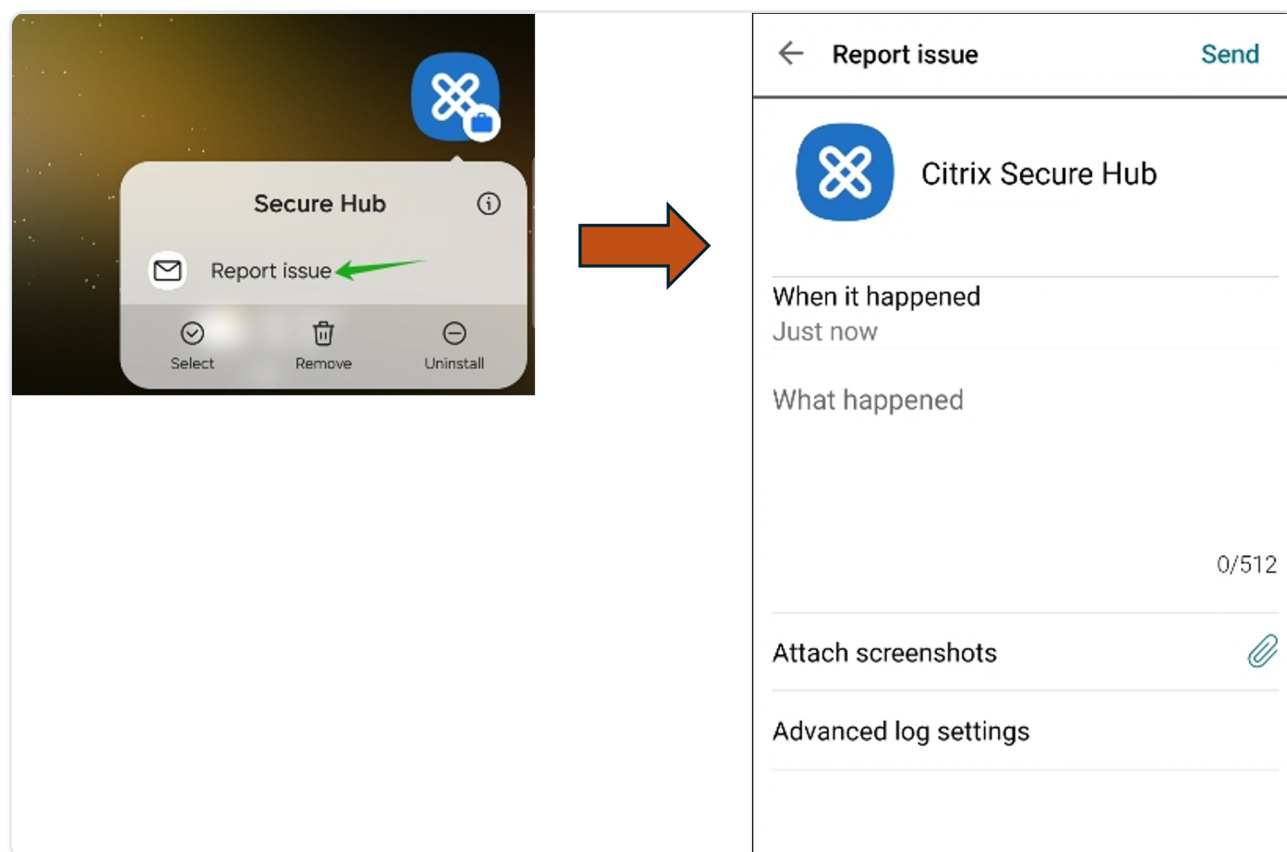


有关详细信息，请参阅[Android 设备上的合规性检查](#)。

适用于 Android 的 Secure Hub 24.6.0

改进的日志收集和报告

Secure Hub 引入了增强功能，无需打开 Secure Hub 即可无缝报告问题和发送日志。在此版本中，用户可以通过长按 Secure Hub 应用程序图标来访问“**报告问题**”选项。单击“**报告问题**”选项后，Secure Hub 会直接打开“**报告问题**”页面。



适用于 iOS 的 Secure Hub 24.5.0

支持 iOS 17 返回服务

Secure Hub 支持 iOS 17 中的“返回服务”功能，该功能可提供更高效、更安全的移动设备管理 (MDM) 体验。以前，在擦除设备后，需要手动配置才能为新用户设置此功能。现在，“返回服务”功能可自动执行此过程，无论是重新利用公司设备还是将个人设备 (BYOD) 与正确的安全策略集成。

借助“返回服务”功能，MDM 服务器可以向用户设备发送擦除命令，其中包含 Wi-Fi 详细信息和默认 MDM 注册配置文件。然后，设备会自动擦除所有用户数据，连接到指定的 Wi-Fi 网络，并使用提供的注册配置文件重新注册到 MDM 服务器。

适用于 Android 的 Secure Hub 24.3.0

支持 Samsung Knox 增强型认证 v3

Secure Hub 现在支持 Samsung Enhanced Attestation v3，利用 Knox 认证来加强通过 Citrix Endpoint Management 管理的三星设备的安全措施。这种高级认证协议可验证设备的完整性和安全状态，确保它们未被 root 且正在运行授权固件。此功能提供了针对安全威胁的重要保护层，并确保遵守企业安全策略。

适用于 Android 的 Secure Hub 23.12.0

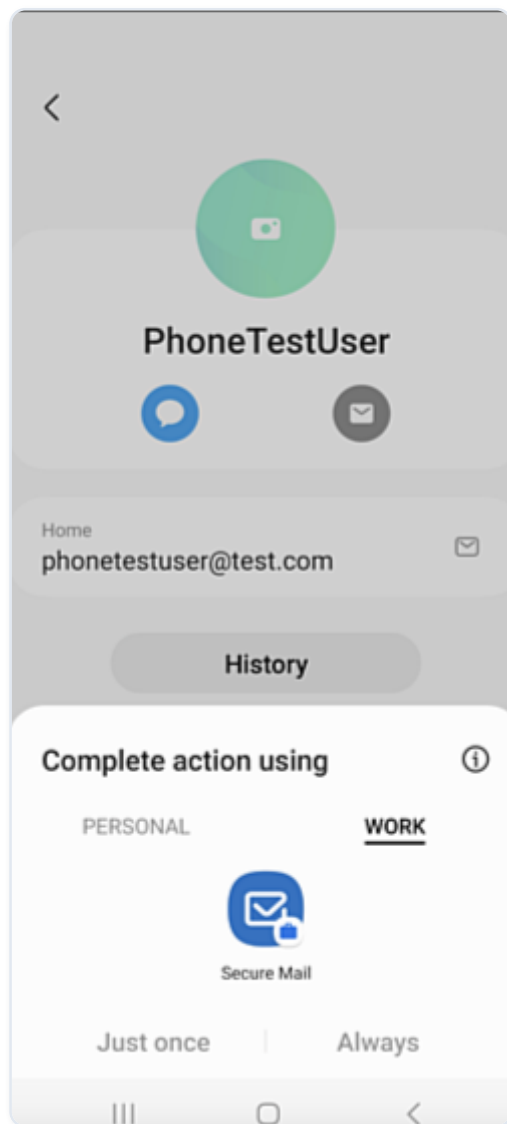
使用 Samsung Knox 增强安全性

在 Citrix Endpoint Management 中添加 Knox Platform for Enterprise Key 设备策略显著增强了 Secure Hub 在 Samsung 设备上的安全功能。此策略允许您提供所需的 Samsung Knox Platform for Enterprise (KPE) 许可证信息，并使用 KPE 许可证来增强 Samsung 设备的安全性。Samsung Knox 确保企业数据受到保护，同时保持易于管理和流畅的用户体验。

有关详细信息，请参阅 [Knox Platform for Enterprise Key 设备策略](#)。

从用户的个人资料访问 Secure Mail

用户现在可以从其个人资料访问和使用其工作资料中的 Secure Mail。当用户在其个人资料通讯录中单击电子邮件地址时，他们会获得一个选项，可以在其工作资料中使用 Secure Mail。此功能提供了便利，允许用户从其个人资料发送电子邮件。此功能适用于 BYOD 或 WPCOD 设备。



适用于 iOS 的 Secure Hub 24.1.0

此版本解决了若干问题，有助于提高整体性能和稳定性。

适用于 Android 的 Secure Hub 23.12.0

在登录页面上添加有关身份验证 PIN 的提示

从 23.12.0 版本开始，您可以在登录页面上添加有关身份验证 PIN 的提示。此功能是可选的，适用于已注册双因素身份验证的设备。该提示可让您了解如何访问 PIN。

您可以将提示配置为文本或链接。提示文本提供有关 PIN 的简洁信息，而链接则提供有关如何访问 PIN 的详细信息。有关如何配置提示的详细信息，请参阅 [通过 Citrix Endpoint Management 控制台配置提示](#)。

nFactor 身份验证支持单点登录功能

从适用于 Android 的 Secure Hub 23.12.0 版本开始，用于移动应用程序管理 (MAM) 注册或登录的 nFactor 支持单点登录 (SSO) 功能。此功能允许以前输入的登录凭据通过 MAM 注册或登录过程，从而无需用户再次手动输入。有关 nFactor SSO 属性的详细信息，请参阅 Citrix Endpoint Management 文档中的 [客户端属性参考](#)。

在直接启动模式下支持完全擦除

以前，您需要解锁设备才能在重启的设备上运行完全擦除命令。现在，即使设备已锁定，您也可以在直接启动模式下运行完全擦除命令。此功能从安全角度来看很有用，尤其是在设备被未经授权的个人持有之时。有关完全擦除命令的更多信息，请参阅 Citrix Endpoint Management 文档中的 [安全操作](#)。

优化了 Secure Hub 应用商店的加载速度

Secure Hub 中的应用商店现在加载速度比以前更快，用户可以更快地访问它。

适用于 iOS 的 Secure Hub 23.11.0

在登录页面上添加有关身份验证 PIN 的提示

从 23.11.0 版本开始，您可以在登录页面上添加有关身份验证 PIN 的提示。此功能是可选的，适用于已注册双因素身份验证的设备。该提示可让您了解如何访问 PIN。

您可以将提示配置为文本或链接。提示文本提供有关 PIN 的简洁信息，而链接则提供有关如何访问 PIN 的详细信息。有关如何配置提示的更多信息，请参阅[通过 Citrix Endpoint Management 控制台配置提示一文](#)。

nFactor 身份验证支持单点登录功能

从适用于 iOS 的 Secure Hub 23.11.0 版本开始，用于移动应用程序管理 (MAM) 注册或登录的 nFactor 支持单点登录 (SSO) 功能。此功能允许以前输入的登录凭据通过 MAM 注册或登录过程，从而无需用户再次手动输入。

有关 nFactor SSO 属性的更多信息，请参阅 Citrix Endpoint Management 文档中的[客户端属性参考](#)。

安全中心 23.10.0

适用于 Android 的 Secure Hub

适用于 Android 的 Secure Hub 23.10.0 支持 Android 14。将 Secure Hub 版本升级到 23.10.0 可确保持续支持已更新到 Android 14 的设备。

安全中心 23.9.0

适用于 Android 的 Secure Hub

本版本解决了可提高整体性能和稳定性的方面。

安全中心 23.8.1

适用于 iOS 的 Secure Hub

本版本解决了一些有助于提高整体性能和稳定性的问题。

安全中心 23.8.0

适用于 iOS 的 Secure Hub

本版本解决了一些有助于提高整体性能和稳定性的问题。

安全中心 23.7.0

适用于 Android 的 Secure Hub

Play 完整性 API

根据弃用时间表，Google 将很快弃用 SafetyNet Attestation API，并迁移到建议的 Play Integrity API。

有关详细信息，请参阅 Citrix Endpoint Management 文档中的 [Play Integrity API](#)。

有关弃用详细信息，请参阅 Citrix Endpoint Management 文档中的 [弃用和删除](#)。

要了解有关 Android SafetyNet 功能的信息，请参阅 [SafetyNet](#)

安全中心 23.4.0

适用于 iOS 的 Secure Hub

改进的用户体验

从 23.4.0 版本开始，适用于 iOS 的 Secure Hub 改进了以下用户体验：

- 应用商店体验：

- ◆ 以前，“我的应用”页面首先出现。在 23.4.0 版本中，“应用商店”页面首先出现。

- ◆ 以前，每当用户单击“应用商店”选项时，Secure Hub 应用商店都会执行重新加载操作。

在 23.4.0 版本中，用户体验得到了改进。现在，当用户首次启动应用程序、重新启动应用程序或向下滑动屏幕时，应用程序会重新加载。

- 用户界面：以前，“注销”选项位于屏幕左下角。在 23.4.0 版本中，“注销”选项是主菜单的一部分，位于“关于”选项上方。
- 超链接：以前，应用程序详细信息页面上的超链接显示为纯文本。在 23.4.0 版本中，超链接可单击并带有下列线格式以指示链接。

MDX 到 MAM SDK 的过渡体验

从 23.4.0 版本开始，适用于 iOS 双模式应用程序的从旧版 MDX 到 MAM SDK 的过渡体验得到了增强。此功能通过减少警报消息和切换到 Secure Hub 来改善使用移动生产力应用程序时的用户体验。

使用 Citrix PIN 解锁应用程序

以前，最终用户输入设备密码来解锁基于移动应用程序管理 (MAM) 的应用程序。

从 23.4.0 版本开始，最终用户可以输入 Citrix PIN 作为密码来解锁基于 MAM 的应用程序。管理员可以使用 CEM 服务器上的客户端属性配置密码的复杂性。

每当应用程序不活动时间超过允许的时间时，最终用户可以根据管理员设置的配置输入 Citrix PIN 来解锁应用程序。

对于适用于 Android 的 Secure Hub，有一个单独的客户端属性用于配置如何在 MAM 应用程序中处理不活动计时器。有关详细信息，请参阅[适用于 Android 的单独不活动计时器](#)。

安全中心 23.4.1

适用于 Android 的 Secure Hub

此版本解决了一些问题，有助于提高整体性能和稳定性。

安全中心 23.4.0

适用于 Android 的 Secure Hub

此版本解决了一些问题，有助于提高整体性能和稳定性。

安全中心 23.2.0

适用于 Android 的 Secure Hub

注意：

- 不收集欧盟 (EU)、欧洲经济区 (EEA)、瑞士和英国 (UK) 用户的任何分析数据。

MDX 全隧道模式 VPN

MDX 微型 VPN（全隧道模式）已弃用。

有关详细信息，请参阅 Citrix Endpoint Management 文档中的[弃用](#)。

适用于 Android 的单独不活动计时器

以前，**不活动计时器**客户端属性适用于 Android 和 iOS 版 Secure Hub。

从 23.2.0 版本开始，IT 管理员可以使用新的客户端属性 **Inactivity_Timer_For_Android** 将不活动计时器与 iOS 分开。IT 管理员可以将 **Inactivity_Timer_For_Android** 的值设置为 0，以独立禁用 Android 不活动计时器。通过这种方式，工作配置文件中的所有应用程序（包括 Secure Hub）将仅要求输入工作 PIN。

适用于 Android 的独立不活动计时器(/en-us/mobile-productivity-apps/media/separate-inactivity-timer-for-android.png)

有关如何添加和修改客户端属性的更多信息，请参阅 XenMobile 文档中的[客户端属性](#)。

安全中心 22.11.0

适用于 Android 的 Secure Hub

此版本包括错误修复。

安全中心 22.9.0

适用于 Android 的 Secure Hub

此版本包括：

- 针对设备密码的密码复杂性 (Android 12+)
- 支持 SDK 31
- 错误修复

针对设备密码的密码复杂性 (Android 12+)

密码复杂性优于自定义密码要求。密码复杂性级别是预定义级别之一。因此，最终用户无法设置较低复杂性级别的密码。

Android 12+ 设备上的密码复杂性如下：

- **应用密码复杂性：**要求密码具有平台定义的复杂性级别，而不是自定义密码要求。仅适用于 Android 12+ 设备和使用 Secure Hub 22.9 或更高版本的设备。
- **复杂性级别：**预定义的密码复杂性级别。
 - **无：**无需密码。
 - **低：**密码可以是：
 - 图案
 - 至少包含四位数字的 PIN
 - **中：**密码可以是：
 - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含四位数字的 PIN
 - 至少包含四个字符的字母
 - 至少包含四个字符的字母数字
 - **高：**密码可以是：
 - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含八位数字的 PIN

- 至少包含六个字符的字母
- 至少包含六个字符的字母数字

备注：

- 对于 BYOD 设备，密码设置（例如最小长度、所需字符、生物识别和高级规则）不适用于 Android 12 及更高版本。请改用密码复杂性。
- 如果为工作配置文件启用了密码复杂性，那么设备端的密码复杂性也必须启用。

有关详细信息，请参阅 Citrix Endpoint Management 文档中的[Android Enterprise 设置](#)。

安全中心 22.7.0

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 22.6.0

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 22.5.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

安全中心 22.4.0

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 22.2.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 21.11.0

适用于 Android 的 Secure Hub

支持公司拥有设备的“工作资料”

在 Android Enterprise 设备中，您现在可以将 Secure Hub 注册到公司拥有设备的“工作资料”模式。此功能适用于运行 Android 11 或更高版本的设备。以前注册到“公司拥有个人启用 (COPE)”模式的设备在设备从 Android 10 升级到 Android 11 或更高版本时，会自动迁移到公司拥有设备的“工作资料”模式。

安全中心 21.10.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

支持 Android 12。从本版本开始，Secure Hub 支持运行 Android 12 的设备。

安全中心 21.8.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

安全中心 21.7.1

适用于 Android 的 Secure Hub

支持已注册设备上的 **Android 12**。如果您正在考虑升级到 Android 12，请确保先将 Secure Hub 更新到版本 21.7.1。Secure Hub 21.7.1 是升级到 Android 12 所需的最低版本。此版本可确保已注册用户从 Android 11 无缝升级到 Android 12。

注意：

如果在升级到 Android 12 之前未将 Secure Hub 更新到版本 21.7.1，您的设备可能需要重新注册或恢复出厂设置才能恢复以前的功能。

Citrix 致力于为 Android 12 提供首日支持，并将向 Secure Hub 的后续版本添加更多更新以全面支持 Android 12。

安全中心 21.7.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 21.6.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 21.5.1

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

此版本包含错误修复。

安全中心 21.5.0

适用于 iOS 的 Secure Hub

在此版本中，使用 MDX Toolkit 19.8.0 或更早版本打包的应用程序将不再工作。请确保使用最新版本的 MDX Toolkit 打包您的应用程序，以恢复正常功能。

安全中心 21.4.0

Secure Hub 颜色焕新。Secure Hub 符合 Citrix 品牌颜色更新。

安全中心 21.3.2

适用于 iOS 的 Secure Hub

此版本包含错误修复。

安全枢纽 21.3.0

此版本包含错误修复。

安全枢纽 21.2.0

适用于 Android 的 Secure Hub

此版本包含错误修复。

Secure Hub 21.1.0 版本

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

此版本包含错误修复。

Secure Hub 20.12.0 版本

适用于 iOS 的 Secure Hub

此版本包含错误修复。

适用于 Android 的 Secure Hub

适用于 Android 的 Secure Hub 支持直接启动模式。有关直接启动模式的更多信息，请参阅 [Developer.android.com](https://developer.android.com) 上的 Android 文档。

安全中心 20.11.0

适用于 Android 的 Secure Hub

Secure Hub 支持 Google Play 当前针对 Android 10 的 API 要求。

安全中心 20.10.5

此版本包含错误修复。

Secure Hub 20.9.0 版本

适用于 iOS 的 Secure Hub

适用于 iOS 的 Secure Hub 支持 iOS 14。

适用于 Android 的 Secure Hub

此版本包含错误修复。

Secure Hub 20.7.5 版本

适用于 Android 的 Secure Hub

- 适用于 Android 的 Secure Hub 支持 Android 11。
- **Secure Hub 32 位到 64 位应用程序的过渡。** 在 Secure Hub 20.7.5 版中，对应用程序的 32 位架构支持已结束，Secure Hub 已更新到 64 位。Citrix 建议客户从 20.6.5 版升级到 20.7.5 版。如果用户跳过升级到 Secure Hub 20.6.5 版，而是直接从 20.1.5 版更新到 20.7.5 版，则必须重新进行身份验证。重新身份验证包括输入凭据和重置 Secure Hub PIN。Secure Hub 20.6.5 版可在 Google Play 商店中获取。
- **从 App Store 安装更新。** 在适用于 Android 的 Secure Hub 中，如果有可用的应用程序更新，则该应用程序会突出显示，并且 **Updates available** 功能会显示在 App Store 屏幕上。

当您点击 **Updates available** 时，您将导航到显示待处理更新的应用程序列表的商店。点击应用程序旁边的 **Details** 以安装更新。应用程序更新后，**Details** 中的向下箭头会变为复选标记。

安全中心 20.6.5

适用于 Android 的 Secure Hub

应用程序从 32 位到 64 位的过渡。 Secure Hub 20.6.5 版本是支持 Android 移动应用程序 32 位架构的最终版本。在后续版本中，Secure Hub 将支持 64 位架构。Citrix 建议用户升级到 Secure Hub 20.6.5 版，以使用户无需重新进行身份验证即可升级到更高版本。如果用户跳过升级到 Secure Hub 20.6.5 版，而是直接更新到 20.7.5 版，则需要重新进行身份验证。重新身份验证包括输入凭据和重置 Secure Hub PIN。

注意：

20.6.5 版本不会阻止在设备管理员模式下运行 Android 10 的设备注册。

适用于 iOS 的 Secure Hub

启用在 iOS 设备上配置的代理。适用于 iOS 的 Secure Hub 要求您启用新的客户端属性

`ALLOW_CLIENTSIDE_PROXY`，如果您希望允许用户使用他们在 **Settings > Wi-Fi** 中配置的代理服务器。有关详细信息，请参阅[客户端属性参考](#) 中的 `ALLOW_CLIENTSIDE_PROXY`。

安全中心 20.3.0

注意：

Secure Hub、Secure Mail、Secure Web 和 Citrix Workspace 应用程序的 Android 6.x 和 iOS 11.x 版本将于 2020 年 6 月停止支持。

适用于 iOS 的 Secure Hub

- **网络扩展已禁用。** 由于 App Store 审核指南的近期更改，从 20.3.0 版本开始，Secure Hub 不支持在运行 iOS 的设备上使用网络扩展 (NE)。NE 对 Citrix 开发的移动生产力应用程序没有影响。但是，移除 NE 对已部署的企业 MDX 封装应用程序有一定影响。最终用户在同步授权令牌、计时器和 PIN 重试等组件时，可能会遇到额外的 Secure Hub 翻转。

注意：

新用户不会收到安装 VPN 的提示。

- **支持增强型注册配置文件。** Secure Hub 支持在 [注册配置文件支持](#) 中为 Citrix Endpoint Management 宣布的增强型注册配置文件功能。

安全枢纽 20.2.0

适用于 iOS 的 Secure Hub

此版本包含错误修复。

安全枢纽 20.1.5

此版本包括：

- 更新了用户隐私策略的格式和显示。此功能更新更改了 Secure Hub 注册流程。
- 错误修复。

安全枢纽 19.12.5

此版本包含错误修复。

安全枢纽 19.11.5

此版本包含错误修复。

安全枢纽 19.10.5

适用于 Android 的 Secure Hub

在 COPE 模式下注册 Secure Hub。在 Android Enterprise 设备中，当 Citrix Endpoint Management 在 COPE 注册配置文件中配置时，在企业所有个人启用 (COPE) 模式下注册 Secure Hub。

安全中心 19.10.0

此版本包括错误修复。

安全中心 19.9.5

适用于 iOS 的 Secure Hub

此版本包括错误修复。

适用于 Android 的 Secure Hub

支持管理 Android Enterprise 工作配置文件和完全托管设备的锁屏功能。Android 锁屏功能管理设备和工作挑战锁屏。在 Citrix Endpoint Management 中使用“锁屏管理”设备策略来控制工作配置文件设备上的锁屏管理以及完全托管和专用设备上的锁屏管理。通过锁屏管理，您可以在用户解锁锁屏界面之前指定可用的功能，例如信任代理和安全摄像头。或者，您可以选择禁用所有锁屏功能。

有关功能设置以及如何配置设备策略的更多信息，请参阅[锁屏管理设备策略](#)。

安全中心 19.9.0

适用于 iOS 的 Secure Hub

适用于 iOS 的 Secure Hub 支持 iOS 13。

适用于 Android 的 Secure Hub

此版本包括错误修复。

适用于 Android 的 Secure Hub 19.8.5

此版本包含错误修复。

安全中心 19.8.0

适用于 iOS 的 Secure Hub

此版本包含性能增强和错误修复。

适用于 Android 的 Secure Hub

支持 Android Q。 此版本包含对 Android Q 的支持。在升级到 Android Q 平台之前：请参阅 [从设备管理迁移到 Android Enterprise](#)，了解 Google 设备管理 API 的弃用如何影响运行 Android Q 的设备。另请参阅博客 [Citrix Endpoint Management and Android Enterprise - a Season of Change](#)。

安全中心 19.7.5

适用于 iOS 的 Secure Hub

此版本包含性能增强和错误修复。

适用于 Android 的 Secure Hub

支持 Samsung Knox SDK 3.x。 适用于 Android 的 Secure Hub 支持 Samsung Knox SDK 3.x。有关迁移到 Samsung Knox 3.x 的更多信息，请参阅 Samsung Knox 开发者文档。此版本还包含对新 Samsung Knox 命名空间的支持。有关旧 Samsung Knox 命名空间更改的更多信息，请参阅 [Changes to old Samsung Knox namespaces](#)。

注意：

适用于 Android 的 Secure Hub 不支持在运行 Android 5 的设备上使用 Samsung Knox 3.x。

Secure Hub 版本 19.3.5 到 19.6.6

这些版本包括性能增强和错误修复。

Secure Hub 版本 19.3.0

支持三星 Knox Platform for Enterprise。 适用于 Android 的 Secure Hub 在 安卓企业版 设备上提供对 Knox Platform for Enterprise (KPE) 的支持。

安全中心 19.2.0

此版本包括性能增强和错误修复。

安全中心 19.1.5

适用于 Android Enterprise 的 Secure Hub 现在支持以下策略：

- **Wi-Fi 设备策略。** Wi-Fi 设备策略现在支持 Android Enterprise。有关此策略的更多信息，请参阅[Wi-Fi 设备策略](#)。
- **自定义 XML 设备策略。** 自定义 XML 设备策略现在支持 Android Enterprise。有关此策略的更多信息，请参阅[自定义 XML 设备策略](#)。
- **文件设备策略。** 您可以在 Citrix Endpoint Management 中添加脚本文件，以在 Android Enterprise 设备上执行功能。有关此策略的更多信息，请参阅[文件设备策略](#)。

安全中心 19.1.0

Secure Hub 改进了字体、颜色和其他 UI。 此次改版为您带来了更丰富的用户体验，同时与我们全套移动生产力应用程序中的 Citrix 品牌美学保持高度一致。

安全中心 18.12.0

此版本包括性能增强和错误修复。

安全中心 18.11.5

- **Android Enterprise 的限制设备策略设置。** 限制设备策略的新设置允许用户在 Android Enterprise 设备上访问以下功能：状态栏、锁屏键盘保护、帐户管理、位置共享以及保持 Android Enterprise 设备屏幕常亮。有关详细信息，请参阅[限制设备策略](#)。

Secure Hub 18.10.5 到 18.11.0 包含性能增强和错误修复。

安全中心 18.10.0

- **支持 Samsung DeX 模式：** Samsung DeX 允许用户将支持 KNOX 的设备连接到外部显示器，以便在类似 PC 的界面上使用应用程序、查看文档和观看视频。有关 Samsung DeX 设备要求和设置 Samsung DeX 的信息，请参阅[Samsung DeX 的工作原理](#)。

要在 Citrix Endpoint Management 中配置 Samsung DeX 模式功能，请更新 Samsung Knox 的限制设备策略。有关详细信息，请参阅[限制设备策略](#)中的**Samsung KNOX 设置**。

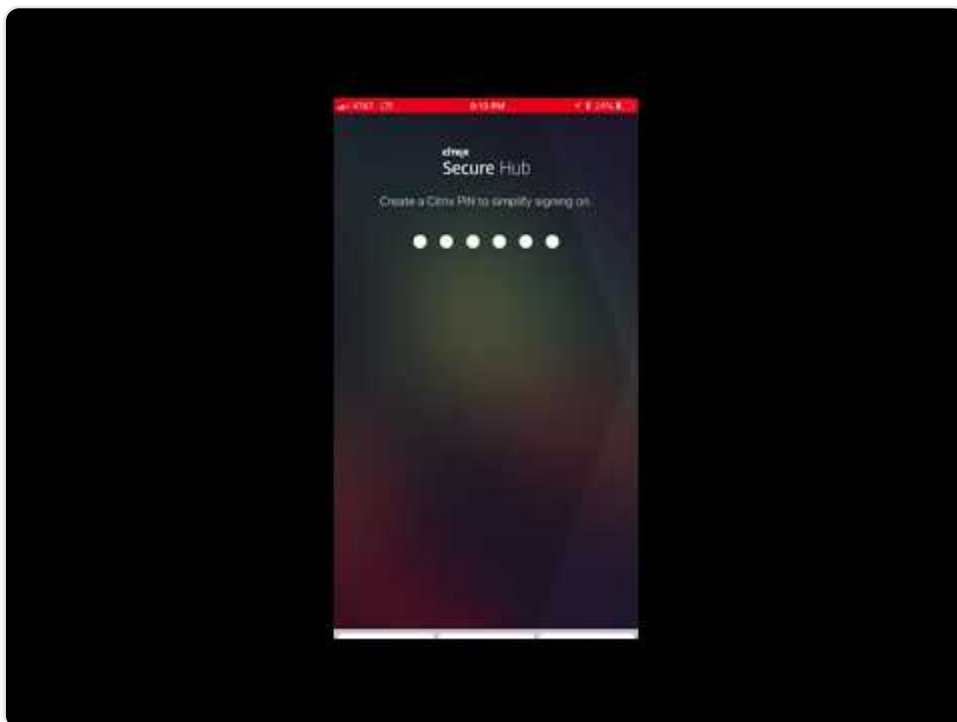
- **支持 Android SafetyNet**：您可以将 Endpoint Management 配置为使用 **Android SafetyNet** 功能来评估已安装 Secure Hub 的 Android 设备的兼容性和安全性。结果可用于触发设备上的自动化操作。有关详细信息，请参阅[Android SafetyNet](#)。
- **阻止 Android Enterprise 设备使用摄像头**：限制设备策略的新**允许使用摄像头**设置可阻止用户在其 Android Enterprise 设备上使用摄像头。有关详细信息，请参阅[限制设备策略](#)。

安全中心 10.8.60 到 18.9.0

这些版本包含性能增强和错误修复。

安全中心 10.8.60

- 支持波兰语。
- 支持 Android P。
- 支持使用 Workspace 应用程序商店。打开 Secure Hub 时，用户不再看到 Secure Hub 商店。**添加应用程序**按钮会将用户带到 Workspace 应用程序商店。以下视频显示了 iOS 设备使用 Citrix Workspace™ 应用程序执行 Citrix Endpoint Management 注册。



重要：

此功能仅适用于新客户。我们目前不支持现有客户的迁移。

要使用此功能，请配置以下内容：

- 启用密码缓存和密码身份验证策略。有关配置策略的详细信息，请参阅(/zh-cn/mobile-productivity-apps/administrator-tasks/policies-platform-mobile-productivity-apps.html)。
- 将 Active Directory 身份验证配置为 AD 或 AD+Cert。我们支持这两种模式。有关配置身份验证的详细信息，请参阅(/zh-cn/citrix-endpoint-management/authentication/authentication-domain-security-token.html)。
- 为 Endpoint Management 启用 Workspace 集成。有关 Workspace 集成的详细信息，请参阅(/zh-cn/citrix-cloud/workspace-configuration.html)。

重要提示：

启用此功能后，Citrix Files 单点登录将通过 Workspace 而非 Endpoint Management（以前称为 XenMobile®）进行。建议您在启用 Workspace 集成之前，在 Endpoint Management 控制台中禁用 Citrix Files 集成。

Secure Hub 10.8.55 版本

- 能够通过配置 JSON 为 Google zero-touch 和 Samsung Knox Mobile Environment (KME) 门户传递用户名和密码。有关详细信息，请参阅(/zh-cn/citrix-endpoint-management/device-management/android/samsung-knox-bulk-enrollment.html)。
- 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到 Endpoint Management，他们将收到证书不受信任的警告。

Secure Hub 10.8.25：适用于 Android 的 Secure Hub 包含对 Android P 设备的支持。

注意：

在升级到 Android P 平台之前：请确保您的服务器基础架构符合安全证书要求，即在 subjectAltName (SAN) 扩展中具有匹配的主机名。要验证主机名，服务器必须提供具有匹配 SAN 的证书。不包含与主机名匹配的 SAN 的证书将不再受信任。有关详细信息，请参阅 Android 开发者文档。

Secure Hub for iOS 于 March 19, 2018 更新：适用于 iOS 的 Secure Hub 10.8.6 版已发布，用于修复 VPP 应用程序策略问题。

Secure Hub 10.8.5：Secure Hub for Android 支持 Android Work (Android for Work) 的 COSU 模式。有关详细信息，请参阅(/zh-cn/citrix-endpoint-management/whats-new.html)。

管理 Secure Hub

您在 Endpoint Management 的初始配置期间执行与 Secure Hub 相关的大多数管理任务。要使 Secure Hub 对 iOS 和 Android 用户可用，请将 Secure Hub 上传到 iOS App Store 和 Google Play Store。

当用户的 Citrix Gateway 会话在使用 Citrix Gateway 身份验证后续订时，Secure Hub 还会刷新 Endpoint Management 中为已安装应用程序存储的大多数 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 Active Directory 用户名和密码等其他凭据。

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 即可安全地访问其 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（触控 ID）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，用户可以通过指纹登录。用户在首次登录 Secure Hub、重新启动设备以及不活动计时器到期后仍需输入 PIN。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，从而在设备上安装根证书危及 SSL 会话时阻止客户端连接到 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 替代用户添加的 CA。

如果使用私有或自签名 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 Endpoint Management 的所需受信任 CA 选项设置为 **ON**。有关详细信息，请参阅 [设备管理](#)。
- 私有/自签名 CA 和 Endpoint Management 自动发现服务 (ADS) 不可达。出于安全考虑，当 ADS 不可达时，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 **Off** 状态，并由 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。确保不要将私钥发送给 Citrix。然后，提供以下信息：

- 包含用户注册所用帐户的域。
- 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，并且区分大小写。
- 用户 ID 类型，可以是 UPN 或电子邮件。默认情况下，类型为 UPN。
- 如果更改了 iOS 注册的端口号（默认端口为 8443），则为用于 iOS 注册的端口。
- 如果更改了端口号（默认端口为 443），则为 Endpoint Management 接受连接的端口。
- Citrix Gateway 的完整 URL。
- （可选）管理员的电子邮件地址。
- 要添加到域的 PEM 格式证书，这些证书必须是公共证书，而不是私钥。
- 如何处理任何现有服务器证书：是立即删除旧服务器证书（因为它已泄露），还是继续支持旧服务器证书直到其过期。

当您的详细信息和证书已添加到 Citrix 服务器时，您的技术支持案例将更新。

证书 + 一次性密码身份验证

您可以配置 Citrix ADC，以便 Secure Hub 使用证书加安全令牌（用作一次性密码）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 能够使用证书 + 一次性密码类型的身份验证，请执行以下操作：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。

注意：

如果为 Endpoint Management 和 Citrix ADC 设置了不同的登录类型，则 Citrix ADC 配置将覆盖。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**添加**。

此时将显示“**创建重写操作**”屏幕。

3. 按照下图所示填写每个字段，然后单击**创建**。

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.

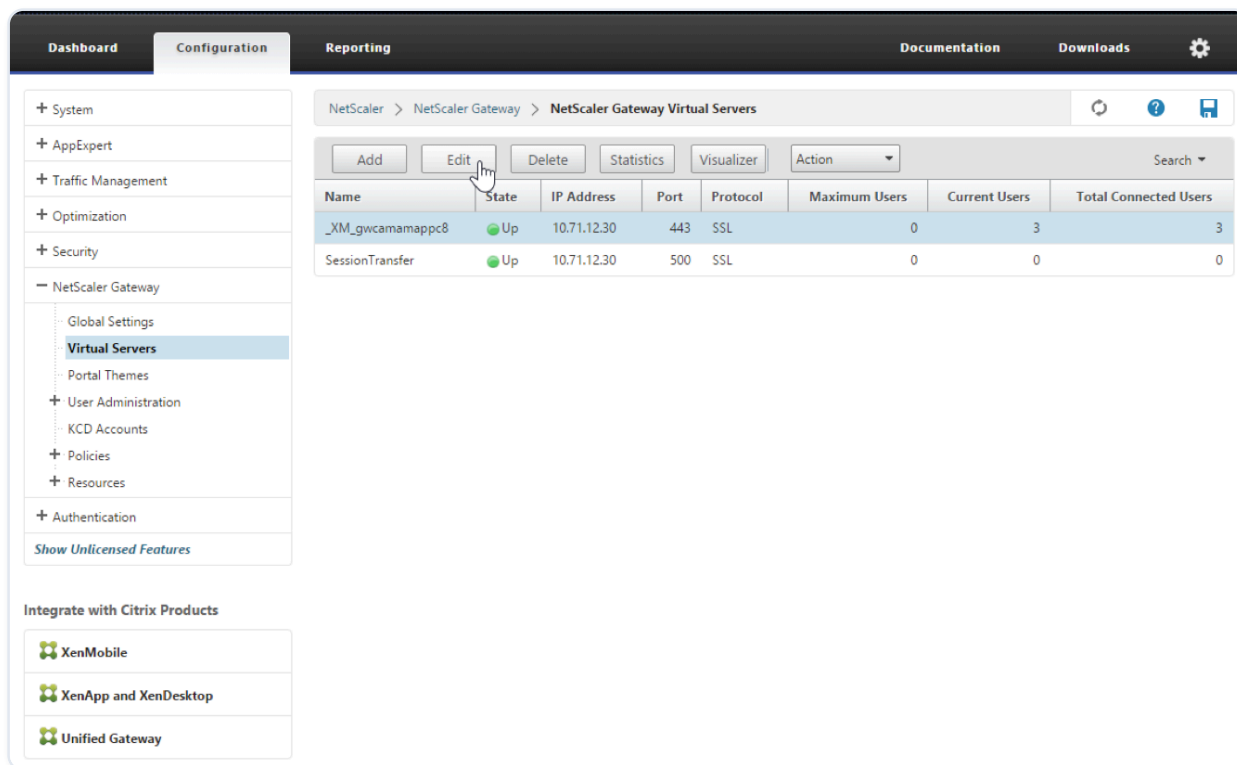
Comments
[Text Box]

Create Close

以下结果将显示在主“**重写操作**”屏幕上。

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()=,"%2f")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。



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

添加策略选项的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-virtual-server-configuration-screen.png)

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**”。

响应选项的图像(/en-us/mobile-productivity-apps/media/netcaler-policy-settngs-response.png)

10. 单击“**继续**”。

“**策略绑定**”部分展开。

策略绑定部分的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-policy-click-to-select.png)

11. 单击“**选择策略**”。

将显示一个包含可用策略的屏幕。

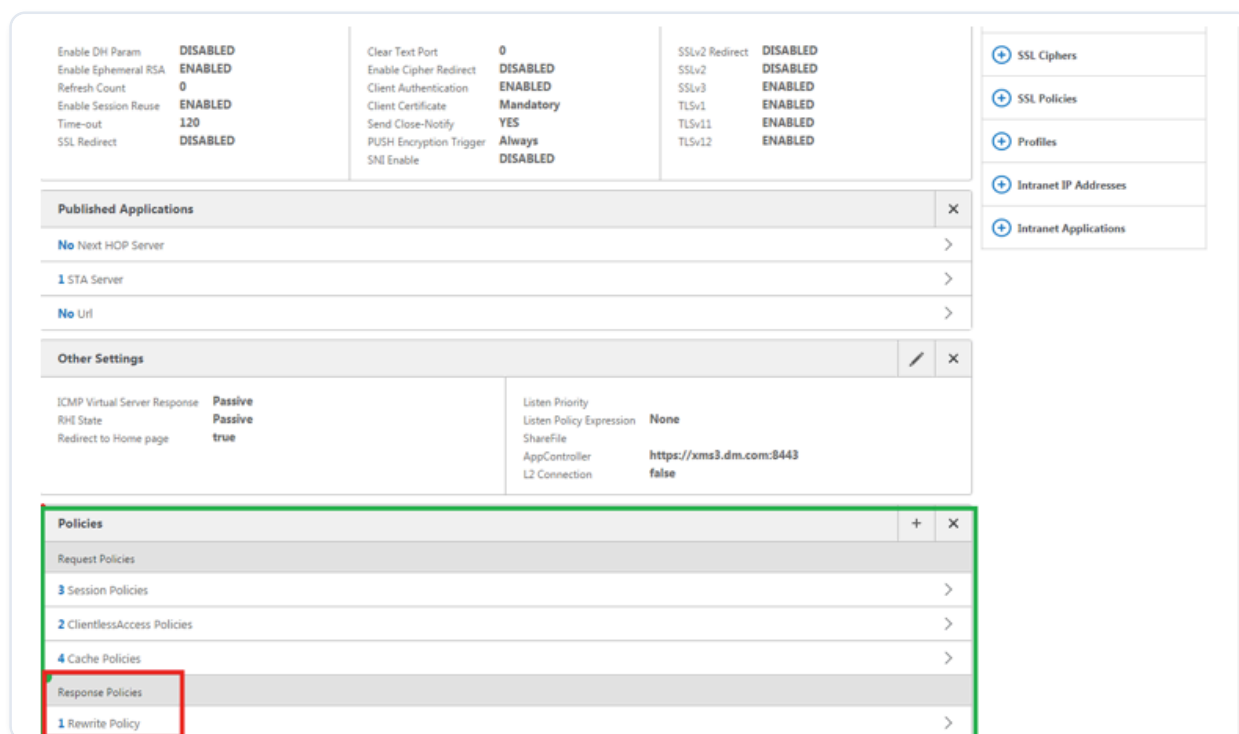
可用策略的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-rewrite-policies.png)

12. 单击您创建的策略行，然后单击“选择”。“策略绑定”屏幕再次出现，其中已填充您选择的策略。

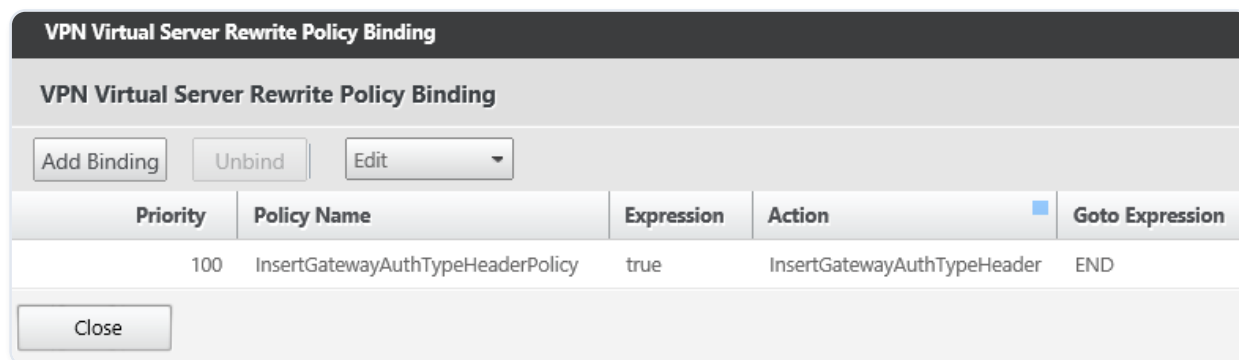
所选策略的图像(/en-us/mobile-productivity-apps/media/Worx-Home-cert-auth-NS-policy-binding-policy-showing.png)

13. 单击“绑定”。

如果绑定成功，主配置屏幕将显示已完成的重写策略。



14. 要查看策略详细信息，请单击重写策略。



Android 设备连接 ADS 的端口要求

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。当通过 ADS 下载安全更新时，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，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 Citrix Endpoint Management 文档中的[端口要求](#)。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。不保证此通信的客户不建议升级到 Secure Hub 10.2。如果您有任何疑问，请联系 Citrix 支持。

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 支持并提出启用证书固定请求。在此过程中，系统会要求您提供证书。

新的证书固定改进要求设备在注册之前连接到 ADS。此先决条件可确保 Secure Hub 能够获取设备注册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：

FQDN	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，Secure Hub 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，Secure Hub 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。

- 如果证书公钥未更改，则证书续订不需要重新注册。

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。

禁用“删除帐户”选项

在启用了自动发现服务 (ADS) 的环境中，您可以禁用 Secure Hub 中的**删除帐户**选项。

执行以下步骤以禁用**删除帐户**选项：

1. 为您的域配置 ADS。
2. 在 Citrix Endpoint Management 中打开**自动发现服务信息**，并将 `displayReenrollLink` 的值设置为 **False**。默认情况下，此值为 **True**。
3. 如果您的设备已注册 MDM+MAM (ENT) 模式，请注销并重新登录以使更改生效。如果您的设备已注册其他模式，则必须重新注册设备。

使用 Secure Hub

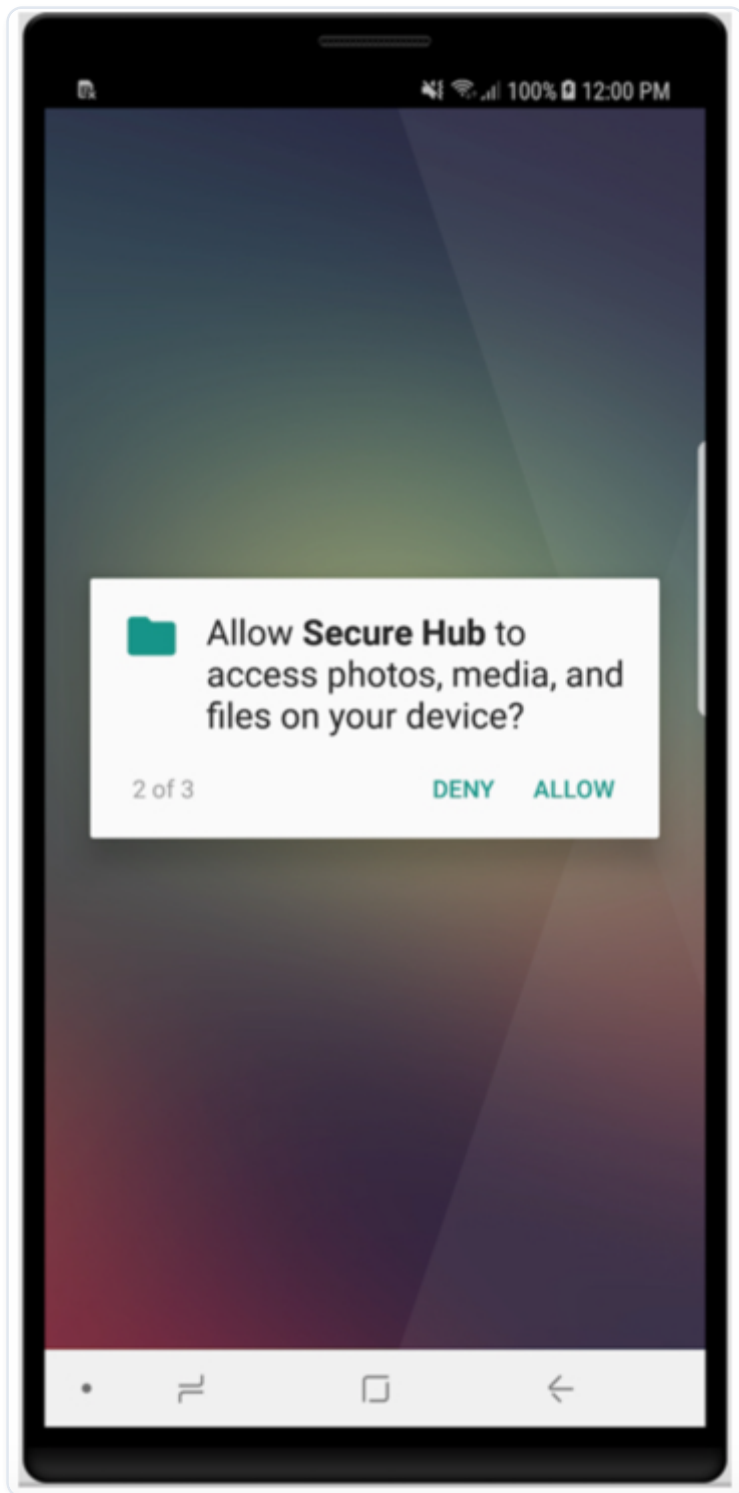
用户首先从 Apple 或 Android 商店下载 Secure Hub 到其设备上。

Secure Hub 打开后，用户输入公司提供的凭据以将其设备注册到 Secure Hub 中。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](#)。

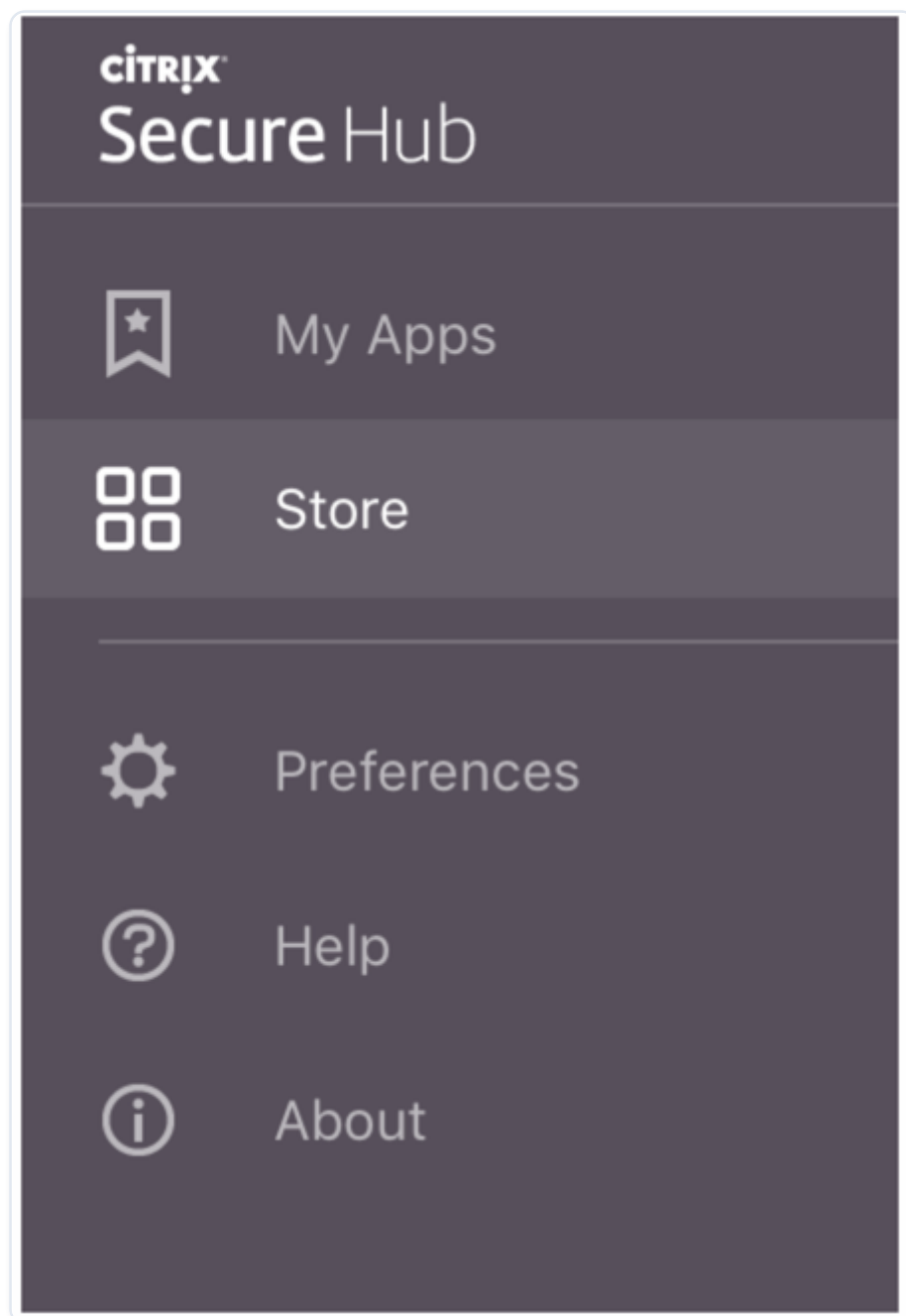
在 Android 版 Secure Hub 上，在首次安装和注册期间，将显示以下消息：允许 Secure Hub 访问您设备上的照片、媒体和文件吗？

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



在平板电脑上，应用商店是一个单独的选项卡。



当运行 iOS 9 或更高版本的 iPhone 用户从应用商店安装移动生产力应用程序时，他们会看到一条消息。该消息指出，企业开发人员 Citrix 在该 iPhone 上不受信任。该消息指出，在开发人员受信任之前，该应用程序不可用。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 版 Citrix 企业应用程序的过程。

自动注册 Secure Mail

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。

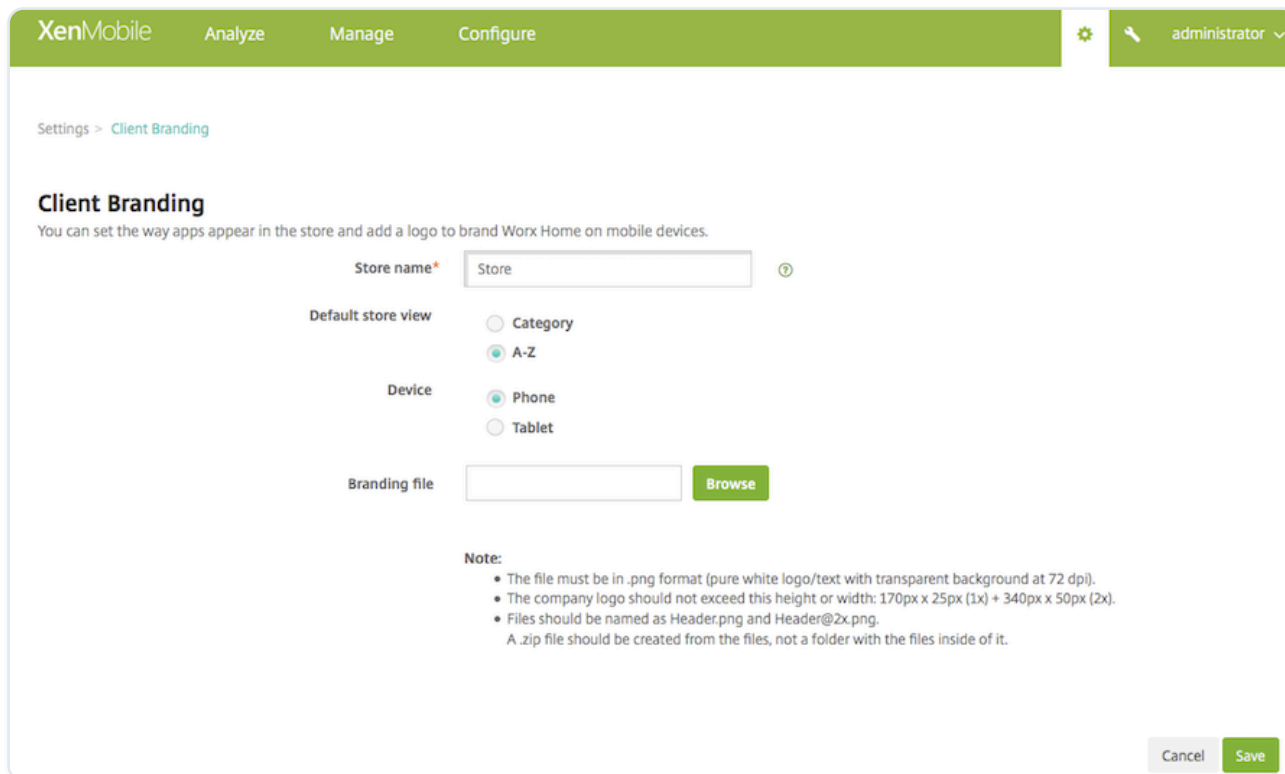
首次使用 Secure Mail 时，Secure Mail 会从 Secure Hub 获取用户的电子邮件地址、域和用户 ID。Secure Mail 使用电子邮件地址进行自动发现。Exchange Server 通过域和用户 ID 进行识别，这使得 Secure Mail 能够自动验证用户。如果策略设置为不传递密码，则会提示用户输入密码。但是，用户无需输入更多信息。

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](#)。

自定义应用商店

如果要自定义应用商店，请转至 **Settings > Client Branding** 以更改名称、添加徽标并指定应用程序的显示方式。



XenMobile Analyze Manage Configure administrator

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name*

Default store view

☐ Category

☒ A-Z

Device

☒ Phone

☐ Tablet

Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
A .zip file should be created from the files, not a folder with the files inside of it.

您可以在 Endpoint Management 控制台中编辑应用程序说明。单击 **Configure**，然后单击 **Apps**。从表中选择应用程序，然后单击 **Edit**。选择要编辑其说明的应用程序的平台，然后在 **Description** 框中键入文本。

The screenshot shows the XenMobile Configure page. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Apps' tab is selected, and the 'App Information' section is active. On the left, there is a sidebar with a list of steps: '1 App Information' (selected), '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main content area shows the 'App Information' form with fields for 'Name' (set to 'Workmail'), 'Description' (empty), and 'App category' (set to 'Workapps').

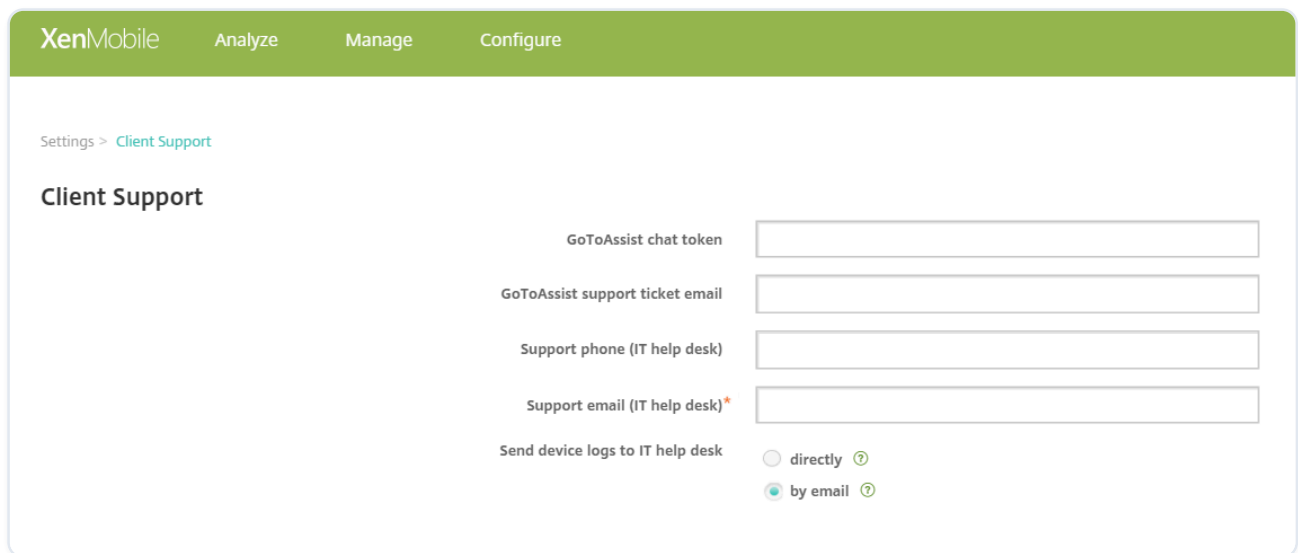
在应用商店中，用户只能浏览您在 Endpoint Management 中配置和保护的应用程序和桌面。要添加应用程序，用户需点击 **Details**，然后点击 **Add**。

配置的帮助选项

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，用户点击左上角的汉堡菜单图标，然后点击 **Help**。

The screenshot shows the 'Help Desk' interface. It has a 'Close' button in the top left corner. The main content area lists three options: 'Your IT Department', 'Report Issue', and 'Send Feedback to Citrix'. Each option has a right-pointing arrow. At the bottom, there is a 'Citrix Support' link.

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程序访问。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。**Settings** 页面随即显示。点击 **More**，然后点击 **Client Support**。随即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 显示应用程序列表。用户选择出现问题的应用程序。Secure Hub 自动生成日志，然后在 Secure Mail 中打开一条消息，并将日志作为 zip 文件附加。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 中打开一条消息，其中已填写 Citrix 支持地址。在消息正文中，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**。在那里，他们可以搜索所有 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。

位置策略

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边界。有关详细信息，请参阅[位置设备策略](#)。

崩溃收集和分析

Secure Hub 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。Crashlytics 软件支持此功能。

有关适用于 iOS 和 Android 的更多功能，请参阅[Citrix Secure Hub](#) 的按平台划分的功能矩阵。

生成 Secure Hub 的设备端日志

本节介绍如何生成 Secure Hub 设备端日志以及如何在其上设置正确的调试级别。

要获取 Secure Mail 日志，请执行以下操作：

1. 转到**Secure Hub > 帮助 > 报告问题**。从应用程序列表中选择 Secure Mail。将打开一封发送给您组织帮助台的电子邮件。
2. 仅当您的支持团队指示您更改日志设置时才进行更改。务必确认设置已正确配置。
3. 返回 Secure Mail 并重现问题。记下问题开始重现的时间，以及问题发生或显示错误消息的时间。
4. 返回**Secure Hub > 帮助 > 报告问题**。从应用程序列表中选择 Secure Mail。将打开一封发送给您组织帮助台的电子邮件。
5. 在主题行和正文中填写一些描述您问题的内容。包括在步骤 3 中收集的时间戳，然后点击**发送**。完成的邮件将打开，并附带压缩的日志文件。
6. 再次点击**发送**。

发送的 zip 文件包含以下日志：

- CtxLog_AppInfo.txt (适用于 iOS), Device_And_AppInfo.txt (适用于 Android), logx.txt, 和 WH_logx.txt (适用于 Windows Phone)

应用信息日志包含有关设备和应用的信息。

已知和已修复的问题

Citrix® 支持从移动生产力应用程序的最后两个版本进行升级。

适用于 iOS 的 Secure Hub 26.8.1

已修复的问题

- 通过 Citrix Workspace 应用程序从适用于 iOS 的 Secure Hub 启动 HDX 应用程序时，应用程序可能无法启动。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 26.8.0

已修复的问题

- 在 Android Enterprise 限制策略中，配置特定的系统应用程序白名单可能会覆盖 **All#** 设置并重新隐藏已列入白名单的系统应用程序。
- 在 Android Enterprise 信息亭 (COSU) 设备上，当设备离开地理围栏边界时 Secure Hub 应用的设备锁定 PIN 码可能在设备返回允许区域后未被移除。因此，设备会持续提示输入 PIN 码，管理员必须从控制台检索并手动解锁设备。
- 在运行 Android 16 和 Android 17 的设备上，包括运行 One UI 8.5 的三星设备，在完全托管设备或专用设备注册完成后，设备可能会保持锁定任务（信息亭）模式。因此，用户无法离开 Secure Hub 屏幕，注册似乎不完整，并且设备必须重新启动。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Hub 26.8.0

已修复问题

- 调用 Microsoft 身份验证库 (MSAL) 注销时，Secure Hub 可能会由于争用条件或死锁而崩溃。
- 当 `mam-app-data-sharing` 功能标志启用时，Secure Mail 和 Secure Web 首次使用可能会失败。
- 在 DEP 设备上，安全应用程序触发选择性擦除时，MDM 配置文件可能不会被删除。
- 当用户从 Secure Hub 提交反馈时，反馈可能会发送到过时的支持电子邮件地址。
- 即使在帐户被删除后，PIN 弹出窗口也可能会持续存在。
- 轻触时，发送日志按钮可能没有响应。
- Secure Hub 可能包含不必要的 `NSAppleMusicUsageDescription` 权限。
- 对于拥有 2100 多个许可证的租户，安装批量采购计划 (VPP) 应用程序可能会将用户重定向到 App Store，而不是安装应用程序。
- 在加载共享密钥链保管库时，Secure Hub 可能会因 SIGABRT 错误而崩溃。

已知问题

此版本中没有已知问题。

适用于 Android 26.5.0 的 Secure Hub

已修复问题

当 ADS 服务器 URL 包含无效端口值时，Secure Hub 自动发现可能会失败。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 26.2.0

已修复问题

此版本解决了可提高整体性能和稳定性的方面。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 25.10.0

已修复问题

当未安装所需应用程序以解除策略部署的阻止时，Secure Hub 会向 CEM 服务器报告部署失败。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Hub 25.8.0

已修复问题

- 当您打开和关闭移动应用程序管理 (MAM) 应用程序数据共享功能标志时，某些 MAM 应用程序可能会显示一个弹出警报，指出“应用程序已删除”。
- 当您取消注册 Secure Hub 时，某些 MAM 应用程序可能仍可使用。
- 当您从 Secure Hub 更改 MAM 应用程序的日志设置时，更改可能不会生效。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 25.7.0

已修复问题

此版本解决了可提高整体性能和稳定性的方面。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Hub 25.6.0

已修复问题

- 使用 Secure Hub 应用程序时，您可能会遇到偶尔的崩溃，或者在访问商店时收到以下错误消息，即使在多次重试后也是如此：“无法加载商店。请重试。”
- 当您在仅限移动设备管理 (MDM) 模式下使用设备注册计划 (DEP) 或恢复服务 (RTS) 时，该过程可能不受支持。

- 对于由本地 Active Directory 注册的设备，您在 Azure Active Directory (AAD) 注册期间可能会遇到故障。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Hub 25.4.0

已修复问题

当用户在未先擦除设备并从 CEM 控制台删除设备的情况下重新注册同一设备时，如果服务已禁用，则无法手动刷新策略。

已知问题

本版本中没有已知问题。

适用于 iOS 的 Secure Hub 25.1.0

已修复问题

此版本解决了可提高整体性能和稳定性的问题。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Hub 25.1.0

已修复问题

此版本解决了可提高整体性能和稳定性的问题。

已知问题

本版本中没有已知问题。

适用于 iOS 的 Secure Hub 24.11.0

已修复的问题

尽管设备已注册到设备注册计划 (DEP)，但 iOS 设备在打开 Secure Hub 时仍提示用户输入其用户主体名称 (UPN)。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Hub 24.10.0

已修复的问题

本版本中没有已修复的问题。

已知问题

本版本中没有已知问题。

适用于 iOS 的 Secure Hub 24.9.0

已修复的问题

本版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 24.8.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 24.6.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Hub 24.5.0

已修复的问题

此版本中没有已修复的问题。

已知问题

此版本中没有已知问题。

适用于 Android 的 Secure Hub 24.3.0

已修复问题

用户可以在公司拥有的 Android Enterprise 设备上执行恢复出厂设置，即使恢复出厂设置的限制策略设置为“否”。当用户重新启动 Secure Hub 时，会出现此问题。

已知问题

此版本中没有已知问题。

适用于 iOS 的 Secure Hub 24.1.0

已修复问题

- 当您使用 Palera1n 应用程序越狱 iOS 设备时，Citrix Endpoint Management™ 服务器不会将设备检测为已越狱。因此，Endpoint Management 服务器无法对已越狱的设备执行恢复出厂设置。此外，Endpoint Management 服务器无法从服务器控制台中清除已越狱的设备条目。
- 当您使用 MAM SDK 管理 iOS 应用程序时，Secure Hub 商店会遇到以下问题之一：
 - 当应用程序有可用更新时，它不会发出通知。

- 即使应用程序已更新，它也会持续通知更新。

- 当您使用 MAM SDK 管理 iOS 应用程序时，可能会出现以下合规性警报：

“此应用程序已从您的帐户中删除。您可以将其从设备中删除。”

当您在同一 iOS 设备上同时安装 MAM SDK 和 MDX 工具包时，会出现此问题。

适用于 Android 23.12.0 的 Secure Hub

已修复的问题

当 Citrix Gateway 凭据过期时，Secure Hub 可能无法生成新证书以连接到 Citrix Gateway 服务器。因此，Secure Hub 无法启动并显示以下错误消息。

“您的连接出现错误。请尝试重新连接”

适用于 iOS 23.11.0 的 Secure Hub

已修复的问题

- Secure Hub 在 iOS 设备上身份验证失败，因为 Citrix Gateway 客户端证书过期后不会自动续订。当 Citrix Gateway 使用 TLSv1.3 协议时，会出现此问题。
- 当您通过 Citrix Gateway 登录 Secure Hub 时，可能会收到以下错误消息：

“无法登录。凭据不正确。正在结束会话”

当您使用 nFactor 将 iOS 设备注册到 Citrix Endpoint Management (CEM) 时，会出现此问题。

适用于 Android 23.10.0 的 Secure Hub

已修复的问题

在 Android 11 及更高版本上，Android Enterprise 设备上的 Wi-Fi 策略可能无法部署。当 Wi-Fi 策略的“匿名”字段中未指定域值时，会出现此问题。

已知问题

此版本中没有已知问题。

适用于 Android 23.9.0 的 Secure Hub

已修复问题

此版本解决了可提高整体性能和稳定性的方面。

已知问题

此版本中没有已知问题。

适用于 iOS 23.8.1 的 Secure Hub

已修复问题

- 当用户尝试使用 Secure Hub 23.8.0 注册设备，且用户名为 `sAMAccount` 格式时，该过程可能会失败并显示以下错误消息：

“注册失败，MAM 登录用户与注册用户不匹配，请重试注册。”

已知问题

此版本中没有已知问题。

适用于 iOS 23.8.0 的 Secure Hub

已修复问题

- 当您使用 nFactor 将 iOS 设备注册到 Citrix Endpoint Management (CEM) 时，您可能会在建立微型 VPN 隧道时遇到问题。

已知问题

此版本中没有已知问题。

旧版本中的已知和已修复问题

有关 Secure Hub 旧版本中的已知和已修复问题，请参阅 [Secure Hub 已知和已修复问题历史记录](#)。

Secure Hub 已知和已修复问题的历史记录

本文列出了 Secure Hub 早于最新支持版本的已修复和已知问题。有关最新文档，请参阅 [Citrix Secure Hub](#)。

适用于 Android 23.7.0 的 Secure Hub

已修复的问题

- 在 Android Enterprise 平台上，托管配置策略可能在注册后未应用于设备。
- 在 Android Enterprise 平台上，所需的公共应用商店应用程序可能在注册后未自动安装到设备上。
- 当您重新启动设备但未解锁时，可能无法通过 IT 管理员发出的锁定命令重置设备密码。

如果最终用户丢失了设备密码或丢失了设备，此方法很有用，他们可以要求管理员重置设备密码或通过锁定命令锁定设备。

- 当最终用户在某些 Android 设备上打开 Secure Hub 进行注册时，Secure Hub 应用程序无响应
- 当 MDM 注册因许可证过期而失败时，会出现此问题。因此，Secure Mail 应用程序不可用。
- 当您 Citrix Gateway 配置为用于身份验证的身份提供程序 (IdP)，并且与网关的网络连接不稳定时，身份验证会失败，最终用户无法登录 Secure Hub。

已知问题

此版本中没有已知问题。

适用于 iOS 23.4.0 的 Secure Hub

已修复的问题

本版本解决了一些有助于提高整体性能和稳定性的问题。

已知问题

本版本中没有已知问题。

适用于 Android 23.4.1 的 Secure Hub

已修复问题

- 启动 Secure Hub 应用程序时，会出现加载微调器 UI。此问题是由于死锁条件引起的。

已知问题

本版本中没有已知问题。

适用于 Android 23.4.0 的 Secure Hub

已修复问题

- 将设备从 Android 11 升级到 Android 12，然后再升级到 Android 13 后，Secure Hub 应用程序无法启动。
- 在企业拥有的单用途 (COSU) 设备中注册后，Secure Hub 应用程序会请求 Active Directory (AD) 密码而不是 Citrix PIN。此问题可能是由于 Secure Hub 23.2.0 及更早版本中缓存凭据丢失所致。
- Secure Hub 应用程序无响应，因为代码中出现异常导致 PIN 未被接受。

已知问题

本版本中没有已知问题。

适用于 Android 的 Secure Hub 23.2.0

已修复的问题

- 在注册企业拥有的单用途 (COSU) 设备后，且限制策略允许使用 SD 卡，您可能仍然无法访问这些设备上的外部 SD 卡。问题在于它是一个专用设备。
- Android Enterprise 设备上密码过期设置的密码策略未按预期工作。密码更改提示未出现。相反，您必须手动更改密码。
- 有时，在将设备从 Android 11 升级到 Android 13 后，Secure Hub 应用程序变得无响应。
- 每次登录 Secure Hub 时，应用程序都会请求 Active Directory (AD) 密码而不是 Citrix PIN。此问题在您更改 AD 密码后发生。
- 更改 Active Directory (AD) 密码后，登录 Secure Hub 失败并显示以下错误消息：

凭据不正确。

Secure Hub 22.11.0 版本

- 当从 CEM 控制台向“注册应用程序”通道发送推送消息时，消息会到达设备，但不会触发声音警报。
- 配置“凭据策略”并定义证书别名时，使用自定义证书别名时，Citrix SSO 应用程序无法连接到 VPN，并出现身份验证错误。出现以下错误消息：

连接错误：无法连接到 证书 ID。检查您的 Internet 连接并验证 证书 ID 的设置。

当您允许应用程序使用 Citrix SSO 应用程序的证书时，会出现此问题。

Secure Hub 22.9.0 版本

此版本中没有已知或已修复的问题。

安全中心 22.7.0

已修复的问题

- 从移动设备体验 (MDX) 切换到 Citrix 移动应用程序管理 (MAM) SDK 并将 XenMobile Server 升级到 10.13 RP4 后，您可能无法通过 Secure Hub/Secure Web 访问内网站点。

出现以下错误消息：“Err_Name_not_resolved”。

- 托管配置策略设置未应用于注册配置为公司拥有设备的工作配置文件 (WPCOD) 的工作配置文件。当身份验证通过身份提供程序 (IdP) 进行，并且工作配置文件未标记为已预配时，会出现此问题。

安全中心 22.6.0

此版本中没有已知或已修复的问题。

安全中心 22.5.0

此版本中没有已知或已修复的问题。

安全中心 22.4.0

此版本中没有已知或已修复的问题。

安全中心 22.2.0

Secure Hub 22.2.0 中的已知问题

此版本中没有已知问题。

Secure Hub 22.2.0 中已修复的问题

适用于 iOS 的 Secure Hub

- 在适用于 iOS 的 Secure Hub 中，系统会提示您在通过 Apple 部署计划注册的设备上使用 PIN 注册。
- 设备空闲后，当您登录 Secure Mail 时，适用于 iOS 的 Secure Hub 会打开并显示以下错误消息：

“Secure Hub 需要授权此应用程序。”

单击授权并提供凭据后，身份验证会进入循环。即使重新启动后，您也无法重新进行身份验证或登录。

- 在运行 iOS 15.1 的设备上报告错误时，适用于 iOS 的 Secure Hub 会无响应。
- 在适用于 iOS 的 Secure Hub 中，即使没有新通知，徽章计数也会显示为 1 或 2。
- 在适用于 iOS 的 Secure Hub 中，某些设备上的注册可能会失败。
- 如果将 Citrix Gateway 会话超时策略值配置为 30 天，适用于 iOS 的 Secure Hub 会提示用户每 24-72 小时重新进行身份验证。

适用于 Android 的 Secure Hub

- 在 Samsung DeX 模式下，输入 PIN 时 Secure Hub 会无响应。
- 在完全托管模式下将 Samsung S20 设备注册到 Android Enterprise 时，会出现以下错误：“无效的服务器证书”
- 运行 Android 10 或 11 的设备注册失败，并显示以下错误消息：“安全策略不允许您连接”。
- 当您注册适用于 Android 的 Secure Hub 时，如果您从纵向模式切换到横向模式，您的凭据将被随机数字替换。

Secure Hub 21.11.0 版本

Secure Hub 21.11.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.11.0 中已修复的问题

适用于 Android 的 Secure Hub

- 在适用于 Android 的 Secure Hub 注册期间，出现“未找到证书”错误消息。当您单击“**安装证书**”时，会出现一个空链接，其中不包含任何证书。如果您单击“**取消**”，将出现身份验证屏幕。当您从 Secure Hub 注销并重新登录时，也会出现此问题。

安全中心 21.10.0

Secure Hub 21.10.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.10.0 中已修复的问题

适用于 iOS 的 Secure Hub

- 在适用于 iOS 的 Secure Hub 中，系统会提示您在通过 Apple 部署计划注册的设备上使用 PIN 注册。

适用于 Android 的 Secure Hub

- 为 Android 设备创建注册配置文件以在公司拥有的设备模式下注册工作配置文件时，您必须启用“**BYOD 工作配置文件**”设置。如果您不启用此设置，设备将无法注册。
- 登录适用于 Android 的 Secure Hub 时，电子邮件 ID 会自动填充。

安全中心 21.8.0

适用于 iOS 的 Secure Hub

Secure Hub 21.8.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.8.0 中已修复的问题

- 设备空闲后，当您登录 Secure Mail 时，适用于 iOS 的 Secure Hub 会打开并尝试登录，但登录请求失败。Secure Mail 会继续提示登录并创建登录循环。
- 用户名或密码中包含某些特殊字符的用户无法注册。

安全中心 21.7.1

适用于 Android 的 Secure Hub

此版本中没有已知或已修复的问题。

早期版本中的已知和已修复问题

有关 Secure Hub 早期版本中的已知和已修复问题，请参阅[Secure Hub 已知和已修复问题历史记录](#)。

安全中心 21.7.1

适用于 Android 的 Secure Hub

此版本中没有已知或已修复的问题。

安全中心 21.7.0

适用于 iOS 的 Secure Hub

此版本中没有已知问题或已修复问题。

适用于 Android 的 Secure Hub

Secure Hub 21.7.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.7.0 中已修复的问题

- 在适用于 Android 的 Secure Hub 中，重启设备后，导航到“帮助”>“报告问题”时，Secure Mail 和 Secure Web 日志会丢失。

安全中心 21.6.0

适用于 iOS 的 Secure Hub

Secure Hub 21.6.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.6.0 中已修复的问题

在适用于 iOS 的 Secure Hub 中，使用用户主体名称 (UPN) 注册设备时，用户名不会自动填充。启用自动发现服务时会出现此问题。

适用于 Android 的 Secure Hub

Secure Hub 21.6.0 中的已知问题

在适用于 Android 的 Secure Hub 中，如果提供的 FQDN 包含大写字母，则无法在 MDM+MAM 模式下注册设备。相反，设备将注册到 MAM 模式。

Secure Hub 21.6.0 中已修复的问题

在适用于 Android 的 Secure Hub 中，您无法在设备管理员模式下注册运行 Samsung Knox 的出厂重置设备。

安全中心 21.5.1

适用于 iOS 的 Secure Hub

此版本中没有已知或已修复的问题。

适用于 Android 的 Secure Hub

此版本中没有已知或已修复的问题。

安全中心 21.5.0

Secure Hub 21.5.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.5.0 中已修复的问题

在适用于 Android 的 Secure Hub 中，您无法在 Android Enterprise 设备上部署 Wi-Fi 设备策略。该策略仍处于“待处理”状态。

安全中心 21.4.0

此版本中没有已知或已修复的问题。

安全中心 21.3.2

适用于 iOS 的 Secure Hub

Secure Hub 21.3.2 中的已知问题

此版本中没有已知问题。

Secure Hub 21.3.2 中已修复的问题

输入 Citrix PIN 后，您无法在 Citrix Endpoint Management™ 上注册设备。Secure Hub 未显示 PIN 要求的正确消息。

安全中心 21.3.0

Secure Hub 21.3.0 中的已知问题

在 Secure Hub for Android 20.9.0 及更高版本中，您无法在 Google Pixel 2 设备上以 VPN 模式连接。

Secure Hub 21.3.0 中已修复的问题

- 在 Secure Hub for Android 中，未插入 SIM 卡的设备会显示集成电路卡 ID (ICCID)。
- 在 Secure Hub for Android 中，重新启动设备后，已安装的移动生产力应用程序不会显示在“我的应用程序”屏幕上。
- 在 Secure Hub for Android 中，如果您多次输入错误的密码并尝试重新启动设备，则无法解锁 Android Enterprise 设备。将显示以下错误消息：**手机已关机，请联系您的 IT 管理员。**

安全中心 21.2.0

适用于 Android 的 Secure Hub

Secure Hub 21.2.0 中的已知问题

在适用于 Android 的 Secure Hub 中，重新启动设备后，已安装的移动生产力应用程序不会显示在“我的应用程序”屏幕上。

Secure Hub 21.2.0 中已修复的问题

- 适用于 Android 的 Secure Hub 在设备注册期间挂起。

- 在某些版本的适用于 Android 的 Secure Hub 中，在 Samsung Knox 设备上完成注册后，“主页”和“返回”按钮不可见。

安全中心 21.1.0

Secure Hub 21.1.0 中的已知问题

此版本中没有已知问题。

Secure Hub 21.1.0 中已修复的问题

- 在运行 Android 的设备上，当启用“连接计划设备策略”时，Secure Hub 无法连接到 Citrix Endpoint Management。
- 在某些已注册的 Samsung 设备上，Citrix Endpoint Management 控制台报告的序列号不正确。

安全中心 20.12.0

Secure Hub 20.12.0 中的已知问题

此版本中没有已知问题。

Secure Hub 20.12.0 中已修复的问题

- 在适用于 iOS 的 Secure Hub 中，您无法注册设备。您收到以下错误：**您的设备未注册。**
- 在适用于 iOS 的 Secure Hub 中，用户代理字符串不包含已注册 MAM+MDM 的设备的操作系统版本。
- 在 Android Enterprise 设备上，Secure Hub 在注册期间崩溃。
- 适用于 Android 的 Secure Hub 20.11.0 版本在某些三星设备上崩溃。

安全中心 20.11.0

适用于 Android 的 Secure Hub

Secure Hub 20.11.0 中的已知问题

此版本中没有已知问题。

Secure Hub 20.11.0 中已修复的问题

在某些三星设备上，适用于 Android 的 Secure Hub 崩溃，并显示以下错误：**Secure Hub 持续停止运行。**

安全中心 20.10.5

Secure Hub 20.10.5 中的已知问题

此版本中没有已知问题。

Secure Hub 20.10.5 中已修复的问题

- 在运行 Android 11 的企业自有单用途 (COSU) 设备上，无法将 Secure Hub 设置为默认启动器。
- 在运行 Android 的设备上，工作配置文件在某些三星设备上创建失败。您会收到以下错误：**无法配置工作配置文件。**
- Android 设备的移动应用程序管理 (MAM) 注册通过 Citrix Endpoint Management 自动发现服务失败。
- 在运行 iOS 的设备上，您无法启动某些应用程序。即使 Secure Hub 没有可用更新，您也会收到错误：**请更新 Secure Hub 以使用此应用程序。**
- 在运行 iOS 的设备上，Secure Mail 在最长离线期限到期后会提示授权。Secure Mail 随后切换到 Secure Hub，阻止您使用它。

安全中心 20.9.0

Secure Hub 20.9.0 中的已知问题

此版本中没有已知问题。

Secure Hub 20.9.0 中已修复的问题

- 在适用于 iOS 的 Secure Hub 中，启用证书锁定后，即使服务器之一锁定的证书不正确，也会在服务器之间建立连接。
- 在适用于 iOS 的 Secure Hub 中，您无法接收通知。您会收到以下错误：**没有具有有效 Secure Hub 令牌的设备。**

安全中心 20.7.5

Secure Hub 20.7.5 中的已知问题

在运行 Android 11 的企业拥有的单用途 (COSU) 设备上，您无法将 Secure Hub 设置为默认启动器。

Secure Hub 20.7.5 中已修复的问题

- 在适用于 Android 的 Secure Hub 中，启用证书锁定后，注册 Android 设备失败。
- 在适用于 Android 的 Secure Hub 中，限制策略中的**日期时间更改**功能在三星设备上不起作用。
- 在适用于 Android 的 Secure Hub 中，防火墙策略在运行 19.12.5 及更高版本的三星设备上不起作用。
- 在适用于 Android 的 Secure Hub 中，您无法从**我的应用**中卸载应用。

安全中心 20.6.5

此版本中没有已知或已修复的问题

安全中心 20.3.0

适用于 iOS 的 Secure Hub

此版本中没有已知或已修复的问题。

安全中心 20.2.0

适用于 iOS 的 Secure Hub

Secure Hub 20.2.0 中的已知问题

此版本中没有已知问题。

Secure Hub 20.2.0 中已修复的问题

- 在适用于 iOS 的 Secure Hub 中，移动应用程序管理 (MAM) 注册在部分 iOS 设备上失败。
- 在适用于 iOS 的 Secure Hub 中，应用会从设备中随机删除。

安全中心 20.1.5

此版本中没有已知或已修复的问题。

安全中心 19.12.5

Secure Hub 19.12.5 中的已知问题

此版本中没有已知问题。

Secure Hub 19.12.5 中已修复的问题

在运行 iOS 13 的设备上，XenMobile® Server 的用户证书会在实际到期日期进行检查和续订，而不是依靠 SSL 错误代码来检查用户证书是否到期。

安全中心 19.11.5

Secure Hub 19.11.5 中的已知问题

此版本中没有已知问题。

Secure Hub 19.11.5 中已修复的问题

在适用于 iOS 的 Secure Hub 中，禁用用户熵后，MDX 封装的应用程序注册失败。

安全中心 19.10.5

适用于 Android 的 Secure Hub

Secure Hub 19.10.5 中的已知问题

此版本中没有已知问题。

Secure Hub 19.10.5 中已修复的问题

在 Android 版 Secure Hub 中，当凭据策略已配置时，您无法在运行 Secure Hub 19.10.5 版本的设备上安装业务应用程序。

安全中心 19.10.0

Secure Hub 19.10.0 中的已知问题

- 在 Android 版 Secure Hub 中，运行 Android 10 版本的 Google Pixel 2 设备在设备所有者模式下注册失败，原因是权限失败。
- 在 Android 版 Secure Hub 中，运行 Android 10 版本的 Google Pixel 设备在设备所有者模式下注册失败，原因是位置权限验证失败。

Secure Hub 19.10.0 中已修复的问题

此版本中没有已修复的问题。

安全中心 19.9.5

此版本中没有已知或已修复的问题。

安全中心 19.9.0

Secure Hub 19.9.0 中的已知问题

在启用了 Android Enterprise 的 Android 版 Secure Hub 19.9.0 中，Pixel 2 设备上会出现以下问题：凭据策略部署不成功。因此，系统不会提示用户输入证书和密码，并且不会安装证书。作为一种解决方法，用户可以从应用程序中的“**首选项 > 设备信息**”手动刷新其策略。在此处，他们可以按“**刷新策略**”，输入其凭据，然后确认成功消息。

Secure Hub 19.9.0 中已修复的问题

此版本中没有已修复的问题。

安全中心 19.8.5

此版本中没有已知问题或已修复问题。

安全中心 19.8.0

Secure Hub 19.8.0 中的已知问题

在适用于 iOS 的 Secure Hub 中，当您在共享设备上输入不正确的密码并轻按“**切换用户**”以再次登录时，“**请稍候**”消息会无限期显示。

Secure Hub 19.8.0 中已修复的问题

通过完整 VPN 连接时，移动设备管理网络路由不正确。

Secure Hub 19.7.5 版本

Secure Hub 19.7.5 中的已知问题

此版本中没有已知问题。

Secure Hub 19.7.5 中已修复的问题

- 在适用于 Android 的 Secure Hub 中，安装 Web 剪辑的提示会快速出现，干扰 Secure Hub PIN 的配置。
- 在 Samsung Knox 3 及更高版本的设备上，当您在配置文件所有者模式下注册 Secure Hub 并为 Android Enterprise 平台推送“**Samsung MDM 许可证密钥**”策略时，“**设备容器密码重置**”命令会失败。
- 在适用于 iOS 的 Secure Hub 中，当您尝试使用 Apple Store 中的新应用程序 URL 在 MAM 模式下配置公共应用程序时，会出现以下错误：“**无法加载商店。请重试。**”请参阅 <https://support.citrix.com/article/CTX256704> 中的解决方法。
- 在适用于 Android 的 Secure Hub 中，建立完整 VPN 隧道后，您无法安装 MDX 应用程序。
- 在共享设备模式下运行适用于 Android 的 Secure Hub 的 Point Mobile PM80 设备上发生会话超时，您无法再次登录。
- 在适用于 Android 的 Secure Hub 中，安装并启动内部封装的应用程序后，您会收到以下错误：此应用程序中数据加密的方式已更改。请删除此应用程序并重新安装。

安全中心 19.6.5

Secure Hub 19.6.5 中的已知问题

此版本中没有已知问题

Secure Hub 19.6.5 中已修复的问题

- 在运行 iOS 的设备上，当发生全局服务器负载平衡故障转移时，Secure Hub 不会加载商店。
- 在适用于 Android 的 Secure Hub 中，刷新策略失败。因此，您无法部署任何新的设备策略。
- 在适用于 Android 的 Secure Hub 中，Samsung S10 设备上的注册或刷新策略操作需要很长时间。

- 在运行 Android 的设备上，当 Secure Hub 建立完整的 VPN 连接时，非托管应用程序会失去连接。

安全中心 19.5.5

Secure Hub 19.5.5 中的已知问题

- 在适用于 Android 的 Secure Hub 中，处于企业拥有单用途 (COSU) 模式的设备在注册几分钟后会失去连接，即使启用了 GCM 也无法接收通知。
- 当您同时在设备上为配置文件所有者和设备所有者模式部署位置策略时，设备所有者模式中的用户帐户将被删除。此问题在 NFC 碰撞注册期间以及在 MDM 模式下配置 Endpoint Management 时发生。

Secure Hub 19.5.5 中的已修复问题

- 从本版本开始，Secure Hub 仅支持运行 Android 5.0 及更高版本的设备。
- 在适用于 Android 的 Secure Hub 中，以设备所有者模式注册设备并设置新密码。设备在首次尝试时未锁定。

安全中心 19.5.0

Secure Hub 19.5.0 中的已知问题

- 注册后，OnePlus Android 7.1.1 和 OnePlus 5T Android 9.0.3 设备需要手动重新启动 Secure Hub 才能提示输入 Citrix PIN。
- 在适用于 Android 的 Secure Hub 中，除非刷新策略或刷新应用商店，否则不会在 Android 设备上部署所需的应用程序。

Secure Hub 19.5.0 中的已修复问题

- 从本版本开始，Secure Hub 仅支持运行 Android 5.0 及更高版本的设备。
- 在适用于 Android 的 Secure Hub 中，如果服务器证书中存在多个主题备用名称，则 Android 6.0 设备无法注册。
- 在适用于 Android 的 Secure Hub 中，设备取消注册后，托管应用程序不会卸载。
- 在 Samsung S9 设备上，用户更新到 Android P 后，会出现以下问题：通过 Endpoint Management 更改设备密码时，设备上的密码不会更改。相反，屏幕会变黑，并且 Endpoint Management 控制台会显示设备已锁定状态。

安全中心 19.4.5

Secure Hub 19.4.5 中的已知问题

此版本中没有已知问题。

Secure Hub 19.4.5 中已修复的问题

在 iOS 设备上，当您单击设备注册链接时，Secure Hub 中不会自动填充 Endpoint Management FQDN 实例名称。设备注册请求失败。

安全中心 19.3.5

Secure Hub 19.3.5 中的已知问题

当从适用于 iOS 的 Secure Hub 发送通知时，Secure Hub 的通知徽章计数不会更新。

Secure Hub 19.3.5 中已修复的问题

- 在适用于 Android 的 Secure Hub 中，当您注册共享设备、部署 **Webclip** 策略并添加 Web 和 SaaS 应用程序时，部署成功。但是，此部署在 Citrix Endpoint Management 控制台的应用程序清单屏幕中显示为失败。
- 在适用于 Android 的 Secure Hub 中，当用户使用安全 PIN 登录时，会建立 VPN 隧道，但 Secure Web 不会加载任何网站。但是，当 Secure Web 关闭并重新打开时，网站会按预期加载。
- 配置了 Microsoft Intune 策略的适用于 Android 的 Secure Mail 在身份验证后返回空白屏幕。
- 在适用于 Android 的 Secure Hub 中，已禁用加密的应用程序正在尝试从 Secure Hub 获取加密密钥。
- 当安装 Intune Company Portal 版本 5.0.4324.0 时，适用于 Android 的 Secure Mail 在启动时崩溃。
- 在适用于 Android 的 Secure Hub 中，您无法在运行 Android 7.1.1 的企业自有单用途 (COSU) Android Enterprise 设备上使用系统应用程序。
- 在适用于 Android 的 Secure Hub 中，当您将在 Google Play 中的多个应用程序配置为“必需应用程序”并尝试注册时，系统会提示您安装第一个应用程序。初始提示后会立即出现另一个提示，要求安装第二个应用程序，依此类推。

安全中心 19.3.0

Secure Hub 19.3.0 中的已知问题

- 在适用于 Android 的 Secure Hub 中，当您注册共享设备、部署 Webclip 策略并添加 Web 和 SaaS 应用程序时，部署会成功。但是，此部署在 Citrix Endpoint Management 控制台的应用程序清单屏幕中显示为失败。
- 在 Android Enterprise 设备上，当在位置策略中为地理围栏违规设置锁定操作时，设备会提示您设置新密码，而不是使用系统生成的密码。

Secure Hub 19.3.0 中已修复的问题

使用“锁定并设置密码”安全操作远程锁定完全托管的 Android Enterprise 设备可能会失败，且不会通知您失败。要确保设备已锁定，请设置两次“锁定并设置密码”。设备将使用您设置的第二个密码锁定。

安全中心 19.2.0

Secure Hub 19.2.0 中的已知问题

此版本中没有已知问题。

Secure Hub 19.2.0 中已修复的问题

- 在适用于 iOS 的 Secure Hub 中，当用户从 Secure Hub 商店注销时，会重复出现以下 SSL 握手失败消息：从服务器获取应用程序的网络请求超时。
- 适用于 Android Enterprise 的文件设备策略未部署到工作配置文件模式下的 Android 设备。
- 在适用于 Android 的 Secure Hub 中，新用户共享设备上的登录授权时间很长。当您作为已注册用户注销并尝试以新用户身份登录时，Secure Hub 会一直加载，直到您重新启动设备。
- 在适用于 Android 的 Secure Hub 中，云客户无法使用外部身份提供程序注册 Android Enterprise 设备。
- 在适用于 Android 的 Secure Hub 中，当您处于企业拥有单用途 (COSU) 模式时，Secure Hub 中的应用程序图标会重叠。
- 在适用于 Android 的 Secure Hub 中，如果为现有设备启用了证书锁定，并且证书具有多个主题备用名称，则身份验证会失败并返回到首次用户屏幕。

安全中心 19.1.5

Secure Hub 19.1.5 中的已知问题

- 在适用于 Android 的 Secure Hub 中，当您因密码策略更改而更新密码时，带徽章的应用程序不会显示在 Samsung Galaxy S8 设备上。
- 在适用于 Android 的 Secure Hub 中，文件设备策略 Android Enterprise 未部署到工作配置文件模式下的设备。

Secure Hub 19.1.5 中已修复的问题

- 在适用于 Android 的 Secure Hub 中，当用户使用 Secure PIN 登录时，会建立 VPN 隧道，但 Secure Web 不会加载任何网站。但是，当 Secure Web 关闭并重新打开时，网站会按预期加载。
- 在适用于 Android 的 Secure Hub 中，当您使用 Secure PIN 登录时，会建立 VPN 隧道，但 Secure Web 不会加载任何网站。但是，当 Secure Web 关闭并重新打开时，网站会按预期加载。
- 在适用于 Android 的 Secure Hub 中，当您尝试捕获名为 TechXpert 的内部应用程序的日志时，Secure Hub 会重新启动并要求您重新进行身份验证。

安全中心 19.1.0

Secure Hub 19.1.0 中的已知问题

在适用于 iOS 的 Secure Hub 中，当您部署 MDX 和 Web 或 SaaS 应用程序时，它们会显示在“我的应用程序”屏幕中。当您点击“更多”时，会弹出一个包含“删除”和“取消”选项的窗口，这些选项采用旧版 UI 品牌格式。

Secure Hub 18.12.0 中已修复的问题

- 在已注册 Android For Work 的 Samsung Knox 设备上，当密码策略配置为在一两天内过期时，“密码已过期”消息会反复出现。
- 您无法使用 QR 码注册方法为 Android Enterprise 注册 OnePlus 5T 设备。

安全中心 18.11.0

Secure Hub 18.11.0 中已修复的问题

- 您无法在注册到共享设备模式的 Android 设备上执行单点登录。出现以下错误：**此时无法检索您的企业凭据**。由于管理员策略，已阻止手动登录 ShareFile。
- 您无法在企业拥有的单用途 (COSU) 设备上编辑 Android 音量级别。

安全中心 18.10.5

Secure Hub 18.10.5 中已修复的问题

- 如果在 XenMobile Server 中启用了 FIPS 模式，则在用户将 Secure Hub for iOS 更新到版本 18.10.5 后，当用户打开应用程序时，会出现与加密相关的错误消息。

Secure Hub 版本 10.8.25 到 18.10.6

Secure Hub 版本 10.8.25 到 18.10.6 中已修复的问题

- Secure Hub 版本 10.8.25 到 18.10.6 (Android) 不包含任何已知问题。Secure Hub 中已修复以下问题。此列表包括影响 Secure Hub 的 MDX 问题。

安全中心 18.10.0

Secure Hub 18.10.0 中已修复的问题

- 如果在 EMS 控制台中关闭了 MVPN 策略，则 Secure Hub 在尝试打开 Intune 托管应用程序时会显示空白屏幕。

安全中心 10.8.60

Secure Hub 10.8.60 中已修复的问题

- 在 Samsung Galaxy Tab Active 2 SM-T395 设备上，当管理员在 XenMobile 中设置“禁用恢复出厂设置”限制时，Secure Hub for Android 的“完全擦除”安全操作会失败。
- 当配置了 VPN 策略且设备上未安装 Citrix SSO 应用程序时，Secure Hub for Android 在设备注册期间会无响应。如果您点击“返回”按钮或重新启动应用程序，它会恢复响应。
- Secure Hub for Android 在 Android Enterprise 环境中以设备所有者模式注册期间崩溃。
- 用户为 Secure Hub for iOS 输入有效 PIN 后，Secure Hub 会反复提示用户输入 PIN。

- Secure Hub for Android 在 Android Enterprise 环境中以配置文件所有者模式注册期间崩溃。
- 当在 Secure Hub for Android 中使用 Android Enterprise 时，它会默认安装 Google Chrome。
- 将 Secure Hub for iOS 升级到版本 10.8.55 后，不允许现有或新的 iOS 设备注册。

安全中心 10.8.55

Secure Hub 10.8.55 中已修复的问题

- 当 G Suite 凭据与 Endpoint Management 中的凭据不同时，用户无法登录 Secure Hub 以注册 Android for Work 帐户。

版本 10.8.55 中与 MDX 相关的已修复问题

- 当首选 VPN 模式设置为 SecureBrowse 时，企业应用程序可能会遇到与内部资源的连接问题。
- 将 `android.support.multidex.MultiDexApplication` 或 `android.app.Application` 指定为其应用程序类的应用程序无法在隧道式 - Web SSO 模式下连接到内部网络。
- 在 Android 设备上，会生成多个证书，并且证书会在其到期日期之前被吊销。

安全中心 10.8.55

Secure Hub 10.8.55 中的已知问题

- 从设备中删除 Secure Hub 帐户后，MDM 重新注册失败。

安全中心 10.8.50

Secure Hub 10.8.50 中的已知问题

- 在 Android 版 Secure Hub 上，用户无法添加 Web 链接快捷方式。

安全中心 10.8.35

Secure Hub 10.8.35 中已修复的问题

- 在 Android O 上，策略创建的快捷方式不会显示在设备主屏幕上。此行为在 Android O 中是设计使然。
- 在 Android 上，Secure Hub 在一段时间不活动后无法在三星平板电脑上打开。
- 在 Android 版 Secure Hub 中，您无法在 Samsung Knox 设备上部署推送策略。

- 在 iOS 版 Secure Hub 中，偶尔会出现以下问题：用户更改其 Active Directory 密码后，必须循环输入其 PIN。

安全中心 10.8.25

Secure Hub 10.8.25 中已修复的问题

- 对于使用 MDX Toolkit 10.7.20 版打包的第三方 iOS Cordova 应用程序，启用模糊屏幕内容策略后，将显示黑屏而不是 PIN 屏幕。
- 在运行 Android 7 的 Zebra T51 设备上，用户无法安装 Citrix Launcher 应用程序。

安全中心 10.8.20

Secure Hub 10.8.20 中已修复的问题

- 用户将其 Android 设备更新到版本 8 (Oreo) 后：他们无法从您从 Endpoint Management 部署的应用商店安装企业或 .apk 应用。即使他们启用了第三方应用的安装，问题仍然存在。此问题不限于三星设备。

安全中心 10.8.15

Secure Hub 10.8.15 中已修复的问题

- Secure Hub for Android 在运行 Android O 的设备上获取位置详细信息时崩溃。

安全中心 10.8.10

Secure Hub 10.8.10 中已修复的问题

- 在 Android 设备上，当多个应用未自动安装或用户未自行单击“安装”时，应用会持续下载。因此，会导致高数据使用量。
- 在运行 Android 7 或更高版本的设备上：当您从 XenMobile Server 向设备发送带密码的锁定安全操作时，设备会锁定。但是，如果用户已有锁屏密码，则设备密码不会更改。用户可以使用原始密码解锁设备。

Secure Hub for iOS 于 March 19, 2018 更新： Secure Hub for iOS 10.8.6 版已发布，用于修复 VPP 应用策略的问题。

适用于 Android 和 iOS 的 Secure Hub - 预览版

敬请期待即将发布的版本中的新功能和已解决的问题。

有关当前版本的更多信息，请参阅 [Secure Hub 中的新增功能](#)。

功能标志管理

管理员可以管理功能标志，以访问预览功能并动态控制生产环境中的功能。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。有关详细信息，请参阅[功能标志管理](#)。

身份验证提示场景

各种场景会提示用户通过在其设备上输入凭据来使用 Secure Hub 进行身份验证。

这些场景会根据以下因素而变化：

- Endpoint Management 控制台设置中的 MDX 应用程序策略和客户端属性配置。
- 身份验证是在离线还是在线状态下进行（设备需要网络连接到 Endpoint Management）。

此外，用户输入的凭据类型（例如 Active Directory 密码、Citrix PIN 或密码、一次性密码、指纹身份验证（在 iOS 中称为触控 ID））也会根据身份验证类型和身份验证频率而变化。

我们从导致身份验证提示的场景开始。

- **设备重启**：当用户重启设备时，他们必须重新使用 Secure Hub 进行身份验证。
- **离线不活动（超时）**：启用应用程序密码 MDX 策略（默认情况下）后，名为“不活动计时器”的 Endpoint Management 客户端属性将发挥作用。“不活动计时器”限制了在使用安全容器的任何应用程序中，在没有用户活动的情况下可以经过的时间长度。

当不活动计时器到期时，用户必须重新对设备上的安全容器进行身份验证。例如，当用户放下设备并离开，并且不活动计时器已到期时，其他人无法拿起设备并访问容器中的敏感数据。您可以在 Endpoint Management 控制台中设置**不活动计时器客户端属性**。默认值为 15 分钟。将应用程序密码设置为**开**和不活动计时器客户端属性的组合可能是最常见的身份验证提示场景。

- **从 Secure Hub 注销**：当用户从 Secure Hub 注销时，下次他们访问 Secure Hub 或任何 MDX 应用程序时，如果应用程序需要密码（由应用程序密码 MDX 策略和不活动计时器状态决定），他们必须重新进行身份验证。
- **最长离线时间**：此场景特定于单个应用程序，因为它由每个应用程序的 MDX 策略驱动。“最长离线时间”MDX 策略的默认设置为 3 天。如果应用程序在没有 Secure Hub 在线身份验证的情况下运行的时间段到期，则需要与 Endpoint Management 进行签入以确认应用程序授权并刷新策略。当发生此签入时，应用程序会触发 Secure Hub 进行在线身份验证。用户必须重新进行身份验证才能访问 MDX 应用程序。

请注意“最长离线时间”和“活动轮询周期”MDX 策略之间的关系：

- 活动轮询周期是应用程序与 Endpoint Management 签入以执行安全操作（例如应用程序锁定和应用程序擦除）的时间间隔。此外，应用程序还会检查更新的应用程序策略。

- 通过“活动轮询周期”策略成功检查策略后，“最长离线时间”计时器将重置并重新开始倒计时。

与 Endpoint Management 的两次签入（针对活动轮询周期和最长离线周期到期）都需要设备上有一个有效的 Citrix Gateway 令牌。如果设备具有有效的 Citrix Gateway 令牌，应用程序将从 Endpoint Management 检索新策略，而不会中断用户。如果应用程序需要 Citrix Gateway 令牌，则会切换到 Secure Hub，用户会在 Secure Hub 中看到身份验证提示。

在 Android 设备上，Secure Hub 活动屏幕直接在当前应用程序屏幕上方打开。然而，在 iOS 设备上，Secure Hub 必须切换到前台，这会暂时取代当前应用程序。

用户输入凭据后，Secure Hub 会切换回原始应用程序。在这种情况下，如果您允许缓存 Active Directory 凭据或已配置客户端证书，用户可以输入 PIN、密码或指纹进行身份验证。如果您不允许，用户必须输入完整的 Active Directory 凭据。

Citrix ADC 令牌可能因 Citrix Gateway 会话不活动或强制会话超时策略而失效，如下面的 Citrix Gateway 策略列表所述。当用户再次登录 Secure Hub 时，他们可以继续运行应用程序。

- **Citrix Gateway 会话策略：**两个 Citrix Gateway 策略也会影响何时提示用户进行身份验证。在这些情况下，他们通过身份验证来创建与 Citrix ADC 的在线会话，以便连接到 Endpoint Management。
 - **会话超时：**如果在设定的时间内没有网络活动，则 Endpoint Management 的 Citrix ADC 会话将断开连接。默认值为 30 分钟。但是，如果您使用 Citrix Gateway 向导配置策略，则默认值为 1440 分钟。用户会看到身份验证提示，要求重新连接到其公司网络。
 - **强制超时：**如果设置为 **On**，则在强制超时期限结束后，Endpoint Management 的 Citrix ADC 会话将断开连接。强制超时使在设定时间后重新进行身份验证成为强制性要求。用户将在下次使用时看到身份验证提示，要求重新连接到其公司网络。默认值为 **Off**。但是，如果您使用 Citrix Gateway 向导配置策略，则默认值为 1440 分钟。

凭据类型

上一节讨论了何时提示用户进行身份验证。本节讨论他们必须输入的凭据类型。通过各种身份验证方法进行身份验证是访问设备上加密数据所必需的。要最初解锁设备，您需要解锁**主容器**。在此之后，如果容器再次被保护，要再次访问，您需要解锁**辅助容器**。

注意：

*托管应用程序*一词是指由 MDX Toolkit 封装的应用程序，其中您已默认启用应用程序密码 MDX 策略并正在使用不活动计时器客户端属性。

决定凭据类型的情况如下：

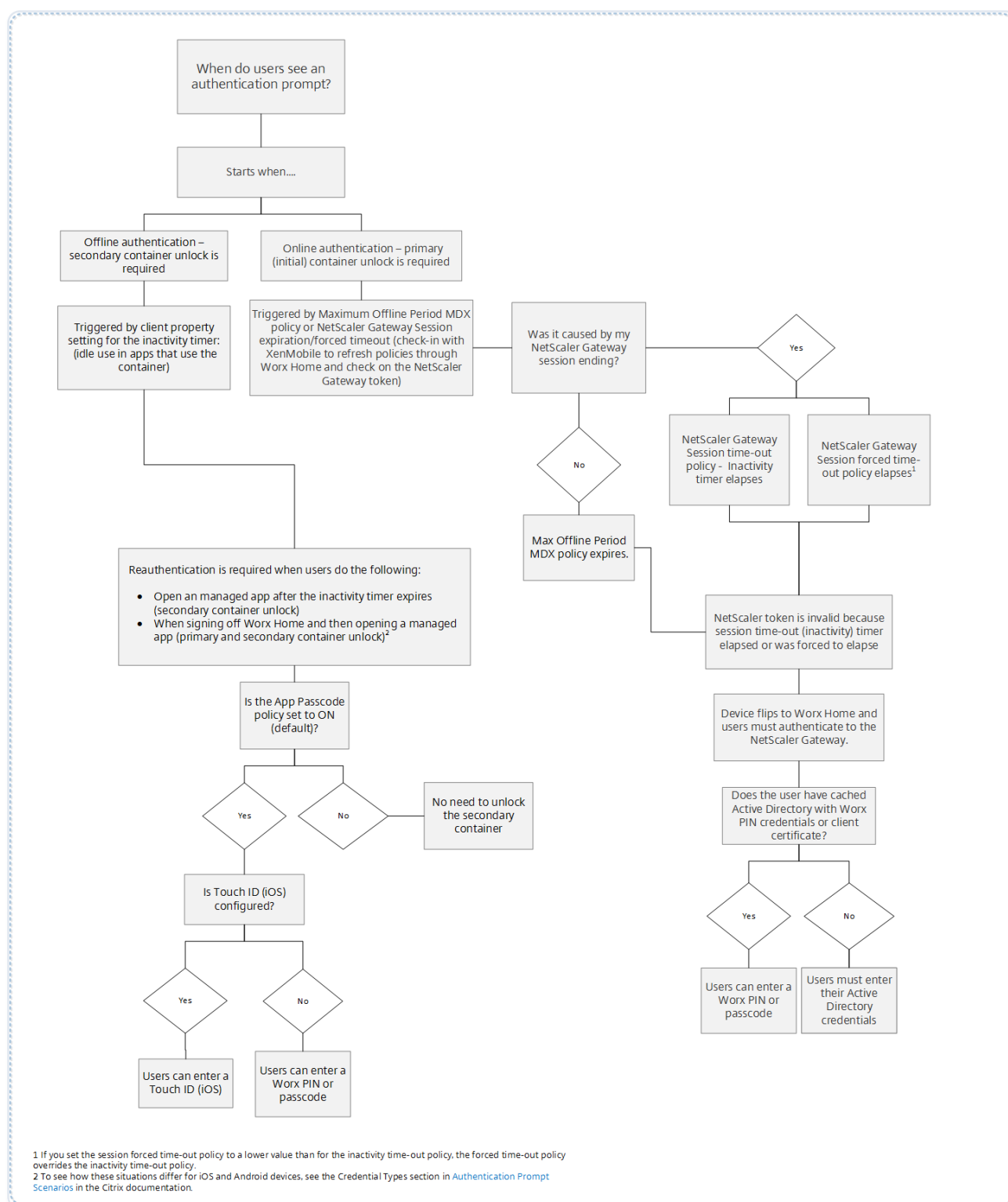
- **主容器解锁：** 解锁主容器需要 Active Directory 密码、Citrix PIN 或密码、一次性密码、触控 ID 或指纹 ID。
 - 在 iOS 上，当用户在设备上安装应用程序后首次打开 Secure Hub 或托管应用程序时。
 - 在 iOS 上，当用户重启设备然后打开 Secure Hub 时。
 - 在 Android 上，当用户打开托管应用程序而 Secure Hub 未运行时。
 - 在 Android 上，当用户因任何原因（包括设备重启）重新启动 Secure Hub 时。
- **辅助容器解锁：** 指纹身份验证（如果已配置）、Citrix PIN 或密码，或 Active Directory 凭据，用于解锁辅助容器。
 - 当用户在不活动计时器到期后打开托管应用程序时。
 - 当用户从 Secure Hub 注销然后打开托管应用程序时。

在以下条件为真时，任一容器解锁情况都需要 Active Directory 凭据：

- 当用户更改与其公司帐户关联的密码时。
- 当您未在 Endpoint Management 控制台中设置客户端属性以启用 Citrix PIN 时：
ENABLE_PASSCODE_AUTH 和 ENABLE_PASSWORD_CACHING。
- 当 NetScaler® Gateway 会话结束时，这会在以下情况下发生：会话超时或强制超时策略计时器到期，如果设备未缓存凭据或没有客户端证书。

启用指纹身份验证后，当由于应用程序不活动而需要离线身份验证时，用户可以使用指纹登录。用户首次登录 Secure Hub 和重启设备时仍需输入 PIN。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](#)。

以下流程图总结了在提示进行身份验证时，确定用户必须输入哪些凭据的决策流程。



关于 Secure Hub 屏幕翻转

另一个需要注意的情况是，当需要从应用程序翻转到 Secure Hub 然后再翻转回应用程序时。翻转会显示一个通知，用户必须确认。发生这种情况时不需要身份验证。这种情况发生在 Endpoint Management 完成签入后，由“最大离线周期”和“活动轮询周期”MDX 策略指定，并且 Endpoint Management 检测到需要通过 Secure Hub 推送到设备的更新策略。

设备密码的密码复杂性 (Android 12+)

密码复杂性优于自定义密码要求。密码复杂性级别是预定义级别之一。因此，最终用户无法设置较低复杂性级别的密码。

Android 12+ 设备上的密码复杂性如下：

- **应用密码复杂性：**要求密码具有平台定义的复杂性级别，而不是自定义密码要求。仅适用于 Android 12+ 设备和使用 Secure Hub 22.9 或更高版本。
- **复杂性级别：**预定义的密码复杂性级别。
 - **无：**无需密码。
 - **低：**密码可以是：
 - 图案
 - 至少包含四个数字的 PIN
 - **中：**密码可以是：
 - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含四个数字的 PIN
 - 至少包含四个字符的字母密码
 - 至少包含四个字符的字母数字密码
 - **高：**密码可以是：
 - 不包含重复序列 (4444) 或有序序列 (1234) 且至少包含八个数字的 PIN
 - 至少包含六个字符的字母密码
 - 字母数字，最少六个字符

注意：

- 对于 BYOD 设备，密码设置（例如最小长度、所需字符、生物识别和高级规则）不适用于 Android 12+。请改用密码复杂性。
- 如果工作资料的密码复杂性已启用，则设备端的密码复杂性也必须启用。

有关详细信息，请参阅 Citrix Endpoint Management 文档中的 [Android Enterprise 设置](#)。

使用派生凭据注册设备

派生凭据为移动设备提供强身份验证。这些凭据从智能卡派生而来，驻留在移动设备中，而不是卡中。智能卡可以是个人身份验证 (PIV) 卡或通用访问卡 (CAC)。

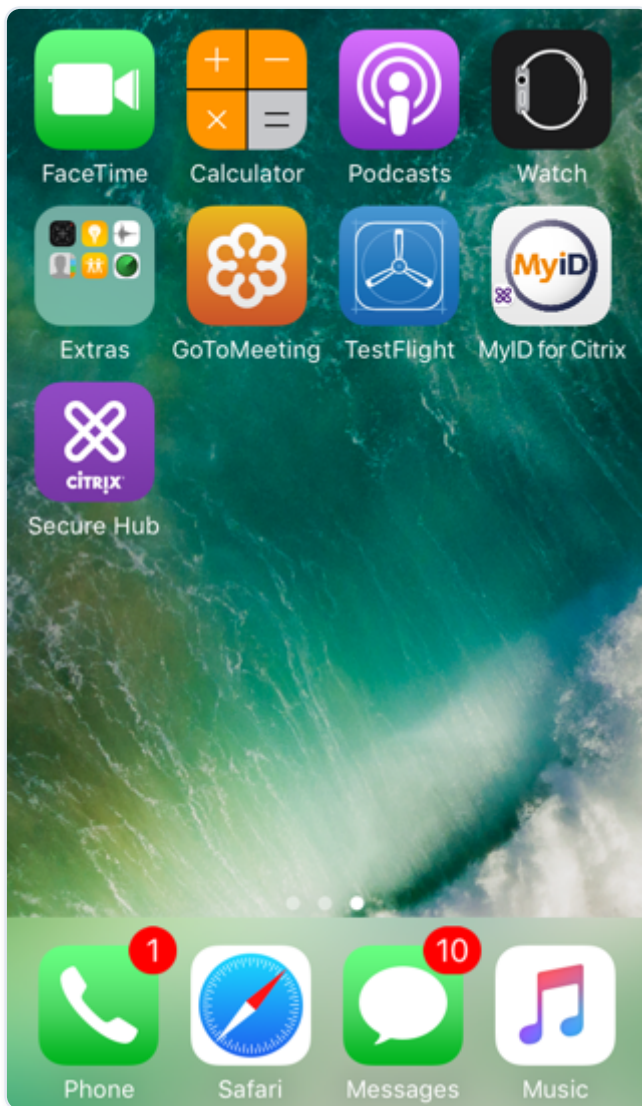
派生凭据是注册证书，其中包含用户标识符（例如 UPN）。Endpoint Management 将从凭据提供程序获取的凭据存储在设备上的安全保管库中。

Endpoint Management 可以使用派生凭据进行 iOS 设备注册。如果配置为使用派生凭据，Endpoint Management 不支持 iOS 设备的注册邀请或其他注册模式。但是，您可以使用相同的 Endpoint Management 服务器通过注册邀请和其他注册模式注册 Android 设备。

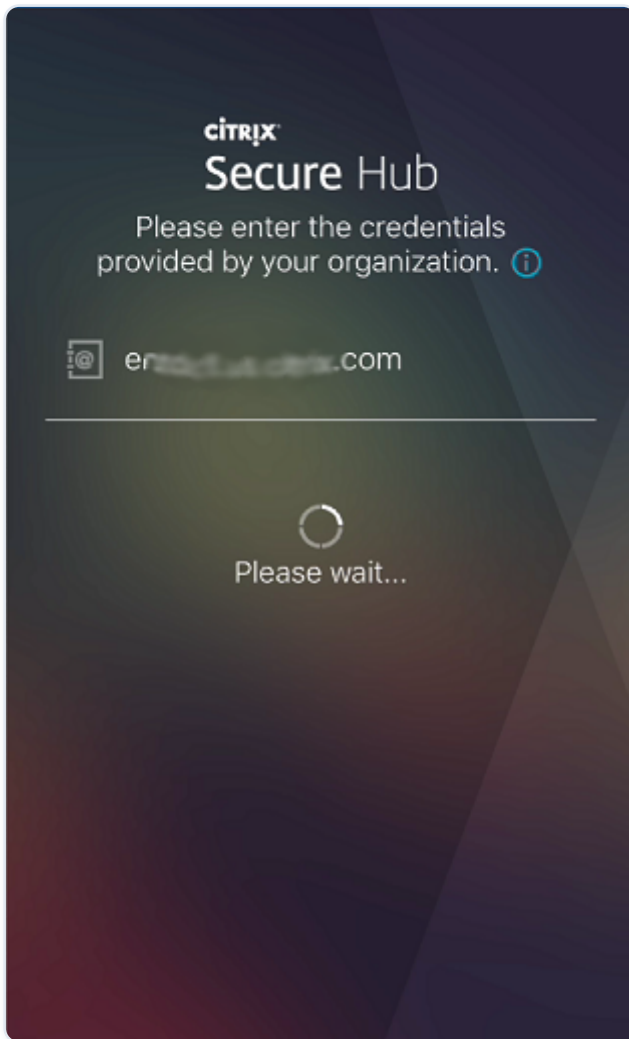
使用派生凭据时的设备注册步骤

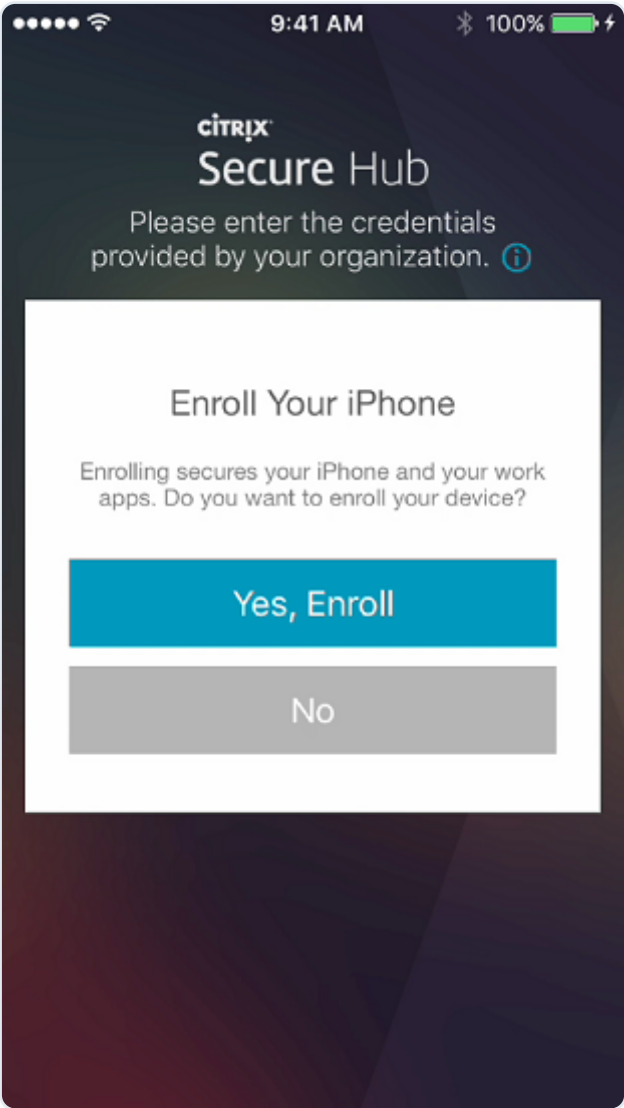
注册要求用户将其智能卡插入连接到其桌面的读卡器中。

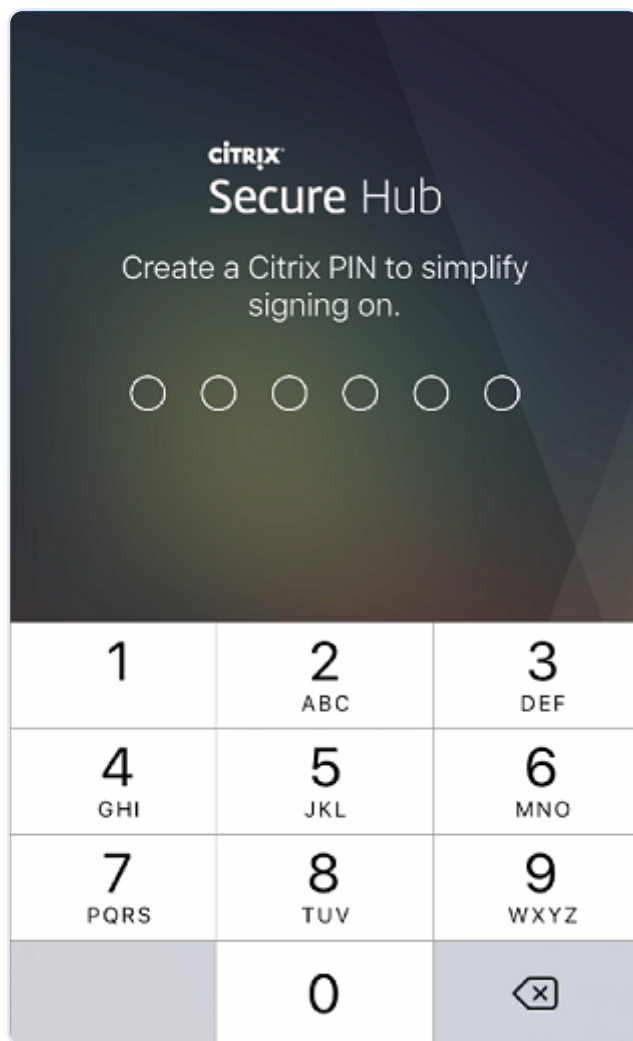
1. 用户安装 Secure Hub 和来自其派生凭据提供程序的应用程序。在此示例中，身份提供程序应用程序是 Intercede MyID Identity Agent。



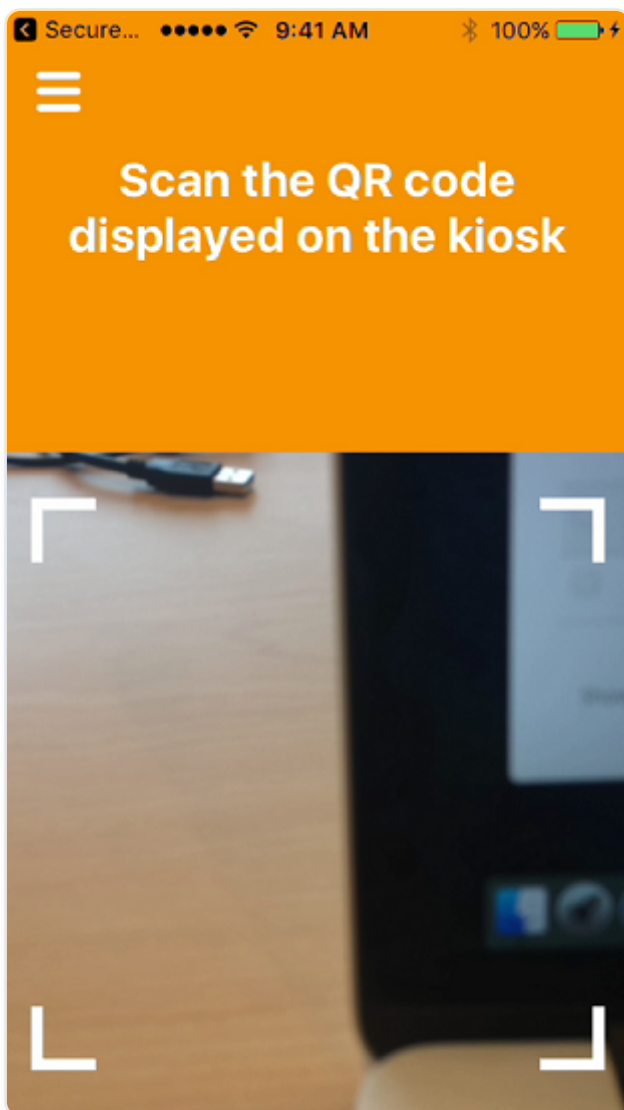
2. 用户启动 Secure Hub。出现提示时，用户键入 Endpoint Management 完全限定域名 (FQDN)，然后单击“下一步”。Secure Hub 中的注册开始。如果 Endpoint Management 支持派生凭据，Secure Hub 会提示用户创建 Citrix PIN。







3. 用户按照说明激活其智能凭据。此时将显示一个启动屏幕，然后提示扫描 QR 码。



4. 用户将其卡插入连接到其桌面的智能卡读卡器中。桌面应用程序随后会显示一个 QR 码，并提示用户使用其移动设备扫描该码。

扫描提示的图像(/en-us/mobile-productivity-apps/media/derived-credentials-kiosk2.png)

出现提示时，用户输入其 Secure Hub PIN。

PIN 提示的图像(/en-us/mobile-productivity-apps/media/derived-credentials-secure-hub-pin.png)

验证 PIN 后，Secure Hub 会下载证书。然后，用户按照提示完成注册。

要在 Endpoint Management 控制台中查看设备信息，请执行以下操作之一：

- 转至**管理 > 设备**，然后选择一个设备以显示命令框。单击**显示更多**。
- 转至**分析 > 控制板**。

通过 Citrix Endpoint Management™ 控制台配置提示

管理员可以为注册模式设置为 **双因素** 的设备在 Secure Hub 登录页面上配置提示。您可以通过以下方式之一配置提示：

- 将提示配置为文本
- 配置包含网页链接的提示文本

将提示配置为文本

要配置提示文本，请执行以下步骤：

1. 使用管理员凭据登录 Citrix Endpoint Management 控制台。
2. 导航到 **设置 > 客户端属性**，然后单击 **添加新客户端属性**。
3. 从 **密钥** 下拉列表中，选择 **自定义密钥**。
4. 在 **密钥** 字段中，输入 **enrollment.twofactor.token.hint**。
5. 在 **值** 字段中，您可以提供在登录页面上显示为提示的文本。该提示会引导用户找到双因素身份验证的 PIN。
6. 在 **名称** 字段中，输入 **enrollment.twofactor.token.hint**。
7. 在 **描述** 字段中，您可以提供有关您配置的提示的备注，这将有助于您将来参考。

配置提示为文本的图像(/en-us/mobile-productivity-apps/media/sh-config-hint-text-1.png)

8. 单击 **保存**。

配置完成后，提示文本将显示在登录页面上。

提示文本登录页面的图像(/en-us/mobile-productivity-apps/media/sh-config-hint-text-2.png)

配置带网页链接的提示文本

您可以配置一个网页，其中包含有关访问 PIN 的详细信息。稍后，将该网页链接作为超链接提供在提示文本中。当用户在登录页面上单击提示时，Secure Hub 将打开一个嵌入式浏览器并导航到您已配置的网页。

要配置带网页链接的提示文本，首先需要按照[将提示配置为文本](#)文章中的说明配置提示文本。完成后，请继续执行以下步骤：

1. 使用管理员凭据登录 Citrix Endpoint Management 控制台。
2. 导航到 **设置 > 客户端属性**，然后单击 **添加新客户端属性**。
3. 从 **密钥** 下拉列表中，选择 **自定义密钥**。
4. 在 **密钥** 字段中，输入 **enrollment.twofactor.token.hint.url**。
5. 在 **值** 字段中，输入您配置的网页 URL。
6. 在 **名称** 字段中，输入 **enrollment.twofactor.token.hint.url**。
7. 在 **描述** 字段中，您可以提供有关您配置的提示的备注，这将有助于您将来参考。

注意：

当用户单击提示链接时，网页将显示在嵌入式浏览器中。

配置提示链接的图像(/en-us/mobile-productivity-apps/media/sh-config-hint-link-1.png)

8. 单击 **保存**。

完成配置后，带有网页链接的提示文本将显示在登录页面上。

提示链接登录页面的图像(/en-us/mobile-productivity-apps/media/sh-config-hint-link-2.png)

在 Android 设备上进行检查（技术预览版）

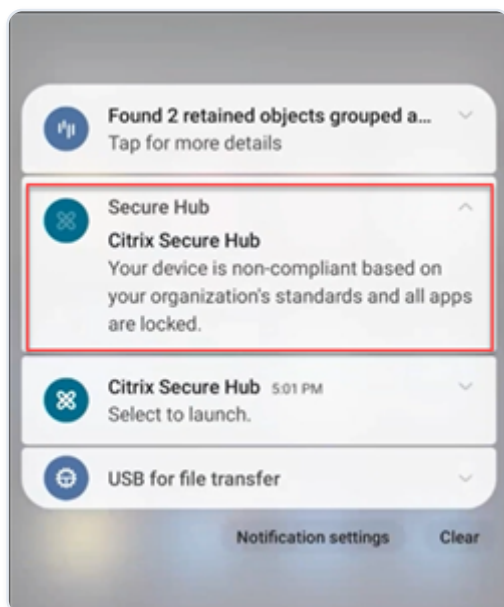
注意：

此功能适用于已注册到 *设备所有者* 模式的 Android 设备。

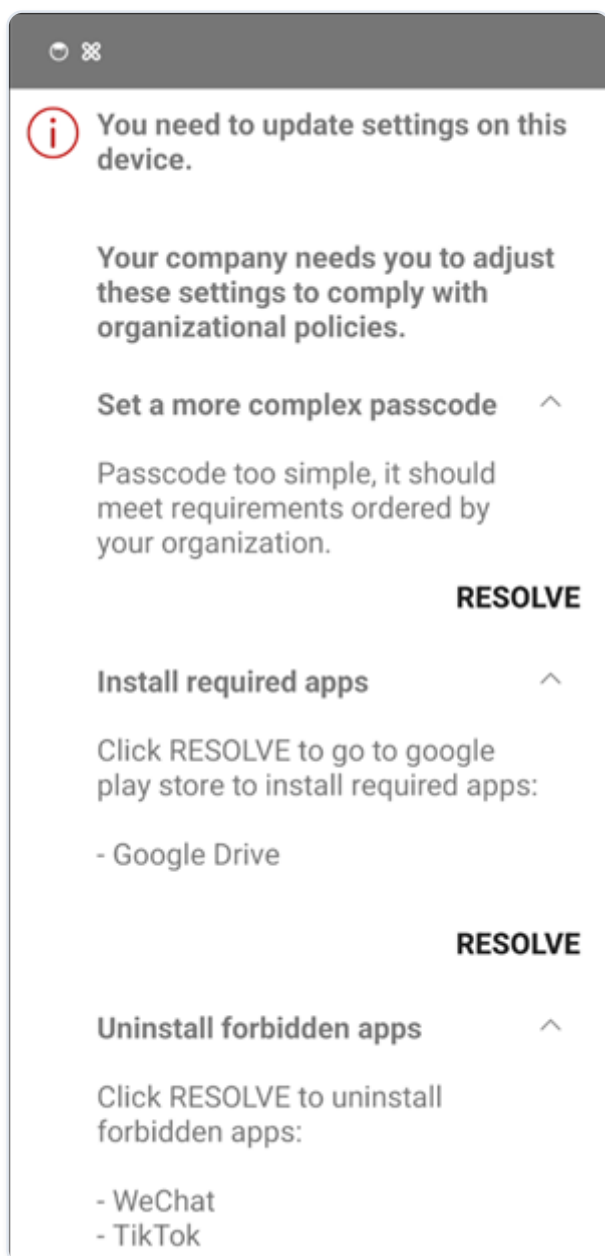
从 Secure Hub for Android 24.8.0 版本开始，Secure Hub 会验证 Android 设备的合规性是否符合管理员通过 Citrix Endpoint Management 配置的策略。这些合规性检查包括：

- 确保设备密码强度
- 验证强制性应用程序的安装
- 确认已删除禁用应用程序

当设备不合规时，用户设备上会显示以下通知。



当设备不合规时，用户打开 Secure Hub 时会看到以下消息。



用户可以单击“解决”按钮以解决相应问题。

注意：

- 应用程序将保持锁定状态，直到满足合规性要求。
- 您可以选择通过将特定应用程序添加到“解锁应用程序”列表来解锁它们。有关详细信息，请参阅 [Android 设备合规性强制执行（技术预览版）](#)。

有关配置策略和合规性检查的更多信息，请参阅 Citrix Endpoint Management 产品文档中的 [Android 设备合规性强制执行（技术预览版）](#)。