

设备姿态

Contents

设备姿态概述	9
先决条件	9
定义	10
工作原理	11
设备姿态服务支持的扫描	12
Windows 更新上次检查	14
与设备姿态服务的第三方集成	14
已知限制	15
服务质量	15
与 Chrome Enterprise 高级版集成	15
最新功能	16
09 September 2026	16
22 June 2026	16
15 June 2026	16
05 June 2026	16
01 June 2026	17
09 April 2026	17
17 March 2026	18
21 January 2026	18
26 September 2025	18
09 July 2025	19
21 Feb 2025	20
04 Dec 2024	21
29 May 2024	21
14 May 2024	21
26 March 2024	22

12 February 2024	22
23 January 2024	22
11 September 2023	22
30 August 2023	22
28 August 2023	23
22 August 2023	23
17 August 2023	23
23 January 2023	23
端点分析发行说明	24
V26.07.20 适用于 macOS (18 September 2026)	24
V26.7.1.15 适用于 Windows (11 September 2026)	24
新增功能	24
已修复的问题	27
适用于 Windows 的 V26.6.1.4 (24 August 2026)	28
新增功能	28
已修复的问题	28
适用于 Windows 的 V26.5.1.7 (08 Jul 2026)	28
已修复的问题	29
V26.03.31 适用于 macOS (14 May 2026)	29
新增功能	29
配置设备姿态策略	30
使用设备姿态配置上下文访问（智能访问）	32
Citrix DaaS 与设备姿态配置	32
使用设备姿态配置 Citrix Secure Private Access	34
编辑设备体态策略	36
配置设备姿态全局设置	37
通过事件驱动的姿态检查实现设备合规性	37
设备的定期扫描	38

访问被拒绝场景的自定义消息	39
跳过设备姿态检查	41
启用跳过设备姿态检查	41
自定义工作区 URL 支持	42
会话录制与设备状态配置	42
设备证书检查	42
上传设备证书	43
查看已导入的证书	44
配置设备证书检查扫描	44
在终端设备上安装设备证书	45
配置允许的域列表	46
设备姿态服务与 Chrome Enterprise 设备信任连接器集成	48
支持的平台和部署	48
先决条件	48
配置	49
配置 Chrome Enterprise Premium 和设备姿态服务	49
将 Citrix 设备姿态服务与 Chrome 设备信任连接器集成	49
为 Citrix 信号定义上下文感知规则	51
Citrix 信号密钥	51
Citrix 的通用表达式语言 (CEL) 示例	52
应用规则	53
验证集成	54
故障排除	54
使用 Citrix-DeviceId 和 Citrix-TransactionId 进行故障排除	55
限制	55
设备姿态服务第三方集成	56
Microsoft Entra ID 与设备姿态服务的集成	56
系统要求	56

微软 Entra ID API 权限	56
配置 Entra ID 集成	57
在 Citrix Device Posture 服务和 Microsoft Entra ID 之间建立信任	57
为 Microsoft Entra ID 集成配置设备姿态策略	58
Jamf Pro 与设备姿态服务的集成	59
配置 Jamf Pro 集成	59
在 Citrix Device Posture 服务和 Jamf Pro 服务之间建立信任	59
为 Jamf Pro 集成配置设备姿态策略	60
将 Citrix Workspace 应用程序从 Jamf Pro 门户推送到 iOS 设备	61
Microsoft Intune 与设备姿态服务的集成	62
多个 Microsoft Intune 帐户与设备姿态的集成	62
配置 Microsoft Intune 集成	62
将设备姿态与 Microsoft Intune 集成	62
将多个 Microsoft Intune 帐户与设备姿态集成	63
Microsoft Intune 应用程序接口权限	65
配置用于 Intune 集成的设备姿态策略	65
CrowdStrike 与设备姿态服务的集成	66
配置 CrowdStrike 集成	66
在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任	66
为 CrowdStrike 集成配置设备姿态策略	67
第三方集成失败通知	68
用例	68
先决条件	68
在设备姿态服务管理控制台中配置通知	69
最终用户流程	70
通过浏览器访问的最终用户流程	70
通过 Citrix Workspace 应用程序的最终用户流程	71
最终用户流程 - 设备姿态结果	72

设备姿态服务测试模式	74
启用测试模式	74
在控制板上查看测试模式活动	74
在生产环境中启用测试模式	75
从测试模式过渡到生产模式	75
通过设置最低支持版本来管理 Citrix Secure Access Endpoint Analysis (EPA) 客户端版本	77
工作原理	77
设置 EPA 客户端版本管理选项	79
EPA 客户端分发和版本管理注意事项	79
多云商店支持	81
重要注意事项	81
先决条件	81
配置应用商店 URL	82
将设备姿态用户事件导出到 SIEM 系统	84
使用 DaaS Monitor 排除设备姿态问题	85
Citrix DaaS™ Monitor 上的设备姿态事件	85
设备姿态日志和事件	86
Identity and Access Management 控制台中的设备姿态仪表板	86
日志位置	88
安全私有访问仪表板	88
设备姿态错误日志	89
设备姿态数据导出	89
诊断设备姿态服务事务	89
了解设备姿态服务评估流程	90
Citrix Monitor 中的故障排除增强功能	90
IT 团队如何使用故障排除增强功能	90
分类处理设备姿态问题	90
调查基于策略的访问阻止	91

使用精确搜索调试大型策略集	91
处理事务故障和错误	93
诊断设备姿态服务事务的步骤	93
事务摘要	95
验证已配置的策略	95
错误代码	96
Citrix Secure Access 端点分析 (EPA) 客户端分发和升级	97
Citrix Secure Access 端点分析 (EPA) 客户端分发和升级方法	97
详细配置步骤	100
与 Citrix Workspace 应用程序版本捆绑	100
Citrix Workspace 应用程序自动更新（客户端应用程序管理）	101
使用 SCCM、Intune、Jamf 或其他端点管理工具推送安装程序	101
在设备状态服务控制台中设置最低 EPA 客户端版本	101
将插件上传到 NetScaler Gateway 门户	102
将 EPA 客户端与 NetScaler 和设备状态服务结合使用时的注意事项	102
设备姿态服务和 deviceTRUST - 强强联合	104
设备姿态服务和 deviceTRUST 如何协同工作	104
预身份验证：在登录前建立信任	105
枚举：对应用程序的上下文访问	105
会话内：持续的上下文访问评估	106
设备姿态服务与 deviceTRUST 集成的用例	107
版本合规性	107
地理围栏	108
监控设备安全状态	108
数据治理	109
数据驻留	109
数据收集	109
数据传输	110

数据控制	110
数据保留	110
数据导出	111
定义	111

设备姿态概述

Citrix 设备姿态服务是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求，才能访问 Citrix DaaS（虚拟应用和桌面）或 Citrix Secure Private Access 资源（SaaS、Web 应用、TCP 和 UDP 应用）。通过检查设备姿态来建立设备信任对于实施基于零信任的访问至关重要。设备姿态服务通过在允许最终用户登录之前检查终端设备的合规性（托管/BYOD 和安全姿态），从而在您的网络中强制执行零信任原则。

先决条件

- 许可要求：设备姿态服务作为通用混合多云许可证 (UHMC) 和平台许可证 (CPL) 的一部分提供。有关详细信息，请参阅 [许可](#)。
- 支持的平台：
 - Windows（10 和 11 版本）
 - macOS 26 塔霍
 - macOS 15 塞阔亚
 - macOS 14 索诺玛
 - iOS
 - Linux 操作系统（Ubuntu 22.04/24.04 版本和 eLux 7 版本）

注意：

- 默认情况下，在不受支持的平台上运行的设备会被标记为不合规。您可以从设备姿态页面上的“**设置**”选项卡中，将分类从“**不合规**”更改为“**拒绝登录**”。有关“合规”和“不合规”的定义，请参阅 [定义](#)。
 - 默认情况下，在受支持的平台上运行但与任何预定义设备姿态策略不匹配的设备会被标记为不合规。您可以从设备姿态页面上的“**设置**”选项卡中，将分类从“**不合规**”更改为“**拒绝登录**”。
 - 对于 iOS 上的设备姿态服务支持，EPA 客户端已作为 Citrix Workspace 应用程序 for iOS 的一部分内置。有关版本详细信息，请参阅 [适用于 iOS 的 Citrix Workspace 应用程序](#)。
- Citrix Device Posture 客户端 (EPA 客户端)：一个轻量级应用程序，必须安装在端点设备上才能运行设备状态扫描。此应用程序无需本地管理员权限即可在端点上下载和安装。

注意：

如果您正在使用设备证书检查，则必须以管理员权限安装 EPA 客户端。

- 支持的浏览器：Chrome、Edge 和 Firefox。
- 防火墙配置：要使用设备状态服务，请确保防火墙或代理已配置为允许以下域：
 - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
 - `https://productioniconstorage.blob.core.windows.net`
 - `*.netscalergateway.net`
 - `*.nssvc.net`
 - `*.cloud.com`
 - `*.pendo.io`
 - `*.citrix.com`
 - `*.citrixworkspacesapi.net`

定义

与设备状态服务相关的术语“合规”和“不合规”定义如下：

- **合规设备** – 满足预配置策略要求并允许登录公司网络，对 Citrix Secure Private Access 资源或 Citrix DaaS 资源具有完全或无限制访问权限的设备。
- **不合规设备** - 满足预配置策略要求并允许登录公司网络，对 Citrix Secure Private Access 资源或 Citrix DaaS 资源具有部分或受限访问权限的设备。

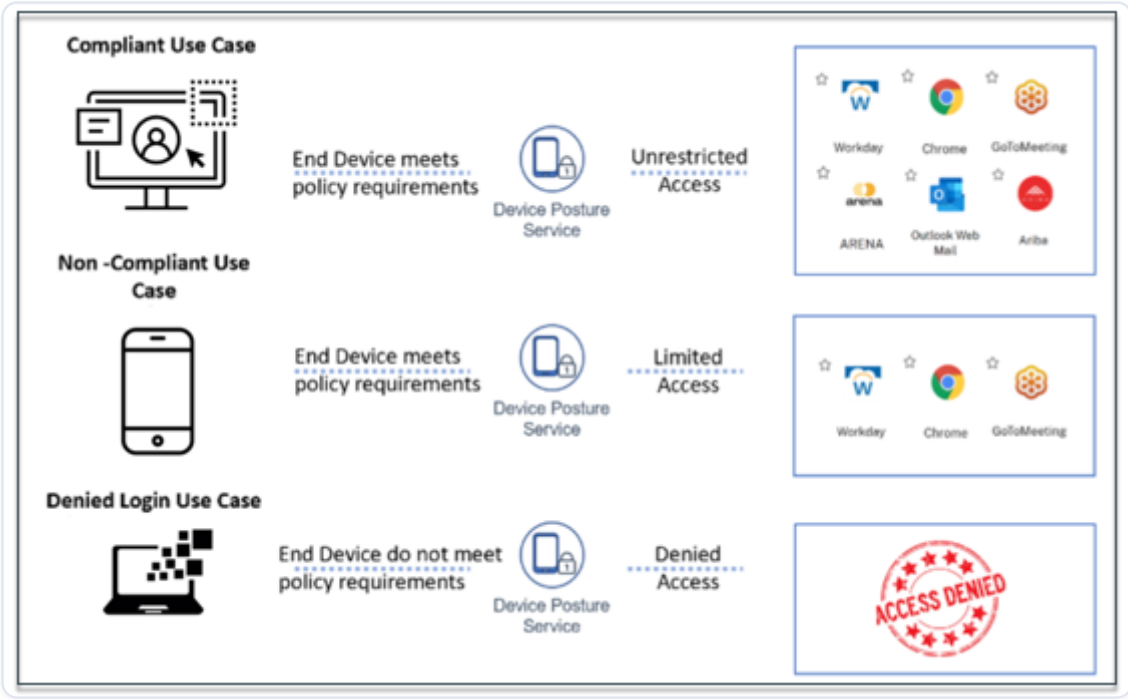
工作原理

管理员可以创建设备姿态策略，以检查端点设备的姿态并确定是否允许或拒绝端点设备登录。允许登录的设备进一步分类为合规或不合规。用户可以通过浏览器或 Citrix Workspace™ 应用程序登录。

将设备分类为合规、不合规和拒绝登录的高级条件如下：

- **合规设备** – 满足预配置策略要求并允许登录公司网络，对 Citrix Secure Private Access™ 资源或 Citrix DaaS 资源具有完全或无限制访问权限的设备。
- **不合规设备** - 满足预配置策略要求并允许登录公司网络，根据您为设备姿态配置的 DaaS 和 Secure Private Access，对 Citrix Secure Private Access 资源或 Citrix DaaS 资源具有部分或受限访问权限的设备。
 - DaaS：管理员可以指定交付组以限制不合规设备的访问。有关如何配置对交付组的受限访问的详细信息，请参阅 [Citrix DaaS configuration with Device Posture](#)。
 - Secure Private Access：管理员可以选择特定的应用程序来限制这些设备的访问。有关如何限制对特定应用程序的访问的详细信息，请参阅 [Citrix Secure Private Access configuration with Device Posture](#)。
- **拒绝登录**：- 未能满足策略要求的设备将被拒绝登录。

将设备分类为**合规**、**不合规**和**拒绝登录**的结果将传递给 Citrix DaaS 和 Citrix Secure Private Access 服务，该服务反过来利用设备分类提供智能访问功能。



注意：

- 设备姿态策略必须针对每个平台进行特定配置。例如，对于 macOS，管理员可以允许具有特定操作系统版本的设备访问。同样，对于 Windows，管理员可以配置策略以包含特定的授权文件、注册表设置等。
- Linux 用户会在流程中看到设备姿态扫描，但只有在管理员策略中配置了 Linux 扫描时，才会评估姿态。如果未配置 Linux 规则，姿态评估将回退到默认结果。
- 设备姿态扫描仅在预身份验证/登录前进行。
- 有关“合规”和“不合规”的定义，请参阅[定义](#)。

设备姿态服务支持的扫描

Citrix 设备姿态服务支持以下扫描：

WINDOWS 操作系统	MACOS	IOS	LINUX 操作系统
Citrix Workspace 应用程序版本	Citrix Workspace 应用程序版本	Citrix Workspace 应用程序版本	-
操作系统版本	操作系统版本	操作系统版本	操作系统版本

WINDOWS 操作系统	MACOS	IOS	LINUX 操作系统
文件（存在、上次修改时间、MD5）	文件（存在、上次修改时间、MD5）	-	文件（存在、上次修改时间、MD5）
地理位置	地理位置	-	-
网络位置	网络位置	-	-
MAC 地址	MAC 地址	-	-
进程 (存在、MD5、SHA1)	进程 (存在、MD5、SHA1)	-	进程 (存在、MD5、SHA1)
微软端点管理器	微软端点管理器	-	-
CrowdStrike	CrowdStrike	-	-
设备证书	设备证书	-	-
Web 浏览器	Web 浏览器	-	-
防病毒	防病毒	-	-
非数字注册表 (32 位)	-	-	-
非数字注册表 (64 位)	-	-	-
数字注册表 (32 位)	-	-	-
数字注册表 (64 位)	-	-	-
Windows 更新安装类型	-	-	-
Windows 更新上次检查	-	-	-
外部设备已连接	-	-	-
网络设置	-	-	-
-	-	-	挂载点

注意：

- 从 EPA 库版本 24.9.1.1 开始，**Windows 更新上次检查**扫描还包括通过 BigFix、Microsoft Intune 和其他第三方工具安装的更新，以及通过 Windows 自动升级服务安装的更新。
- 对于设备姿态服务上的 iOS 支持，EPA 客户端作为适用于 iOS 的 Citrix Workspace 应用程序的一部分内置。有关版本详细信息，请参阅 [适用于 iOS 的 Citrix Workspace 应用程序](#)。

Windows 更新上次检查

Windows 更新上次检查增强功能适用于 EPA 库版本 24.9.1.1。从版本 24.9.1.1 开始，此扫描包括通过 BigFix、Intune 和其他第三方工具安装的更新，以及通过 Windows 自动升级服务安装的更新。

从 EPA 库版本 24.11.1.1 开始，**Windows 更新上次检查**扫描将 Windows 更新列为以下类别：

- **通用更新**：此类别包括使用 Windows 更新、Microsoft 更新或自动更新功能安装的更新。
- **安全更新**：此类别包括针对安全相关漏洞的修补程序。安全更新在每个月的第二个星期二发布。
- **关键更新**：此类别包括针对关键和非安全相关错误的修补程序。关键更新根据需要发布。
- **定义更新**：此类别包括包含产品定义数据库新增内容的更新。发布定义更新时，仅下载最新更新与当前安装的更新之间的差异并将其应用于设备。
- **更新汇总**：此类别包括经过测试的累积修补程序、安全更新、关键更新和打包在一起以便于部署的更新。更新汇总在每个月的第二个星期二发布。

注意：

- 配置**Windows 更新上次检查**扫描时，请确保在每个类别的配置期限内安排更新。如果未在此时间范围内安装更新，则扫描将失败。
- 在用户手动下载和安装更新补丁的情况下，**Windows Update 上次更新检查**扫描不适用。

与设备姿态服务的第三方集成

除了设备姿态服务提供的原生扫描外，该服务还可以与 Windows 和 macOS 上的以下第三方解决方案集成。

- Microsoft Intune。有关详细信息，请参阅[Microsoft Intune 与设备姿态集成](#)。

- CrowdStrike。有关详细信息，请参阅[CrowdStrike 与设备姿态集成](#)。

已知限制

- 在打开或关闭**设备姿态**切换按钮后，启用或禁用设备姿态功能所需的时间可能需要几分钟到一小时。
- 设备姿态配置中的任何更改都不会立即生效。更改可能需要大约 10 分钟才能生效。
- 如果您在 Citrix Workspace 中启用了服务连续性选项，并且设备姿态服务已关闭，用户可能无法登录 Workspace。这是因为 Citrix Workspace 根据用户设备上的本地缓存枚举应用程序和桌面。
- 如果您在 Citrix Workspace 上配置了长期令牌和密码，则设备姿态扫描不适用于此配置。仅当用户登录 Citrix Workspace 时才会扫描设备。
- 每个平台最多可以有 10 个策略，每个策略最多可以有 10 条规则。
- 设备姿态服务不支持基于角色的访问。
- Citrix Cloud™ Japan 不支持设备姿态服务。

服务质量

- 性能：在理想条件下，设备姿态服务会在登录期间增加 2 秒的额外延迟。此延迟可能会根据其他配置（例如 Microsoft Intune 等第三方集成）而增加。
- 弹性：设备姿态服务具有高弹性，拥有多个POP点，以确保没有停机时间。

与 Chrome Enterprise 高级版集成

通过将设备姿态服务与 Google Chrome Enterprise Premium 集成，您可以将设备合规性检查扩展到基于 Chrome 浏览器的访问场景。此集成使组织能够在用户通过 Chrome Enterprise Premium 管理的浏览器访问应用程序时强制执行设备姿态策略。

要在设备姿态服务和 Chrome Enterprise Premium 之间启用集成，您必须将 OpenID Connect (OIDC) 身份验证配置为主要身份验证方法。

有关更多详细信息，请参阅以下主题：

- [与 Google Chrome 企业版集成](#)
- [开放身份连接 \(OIDC\) 与 Citrix Workspace 的集成](#)

最新功能

本主题介绍了设备姿态服务中的增强功能和新特性。

09 September 2026

- **多云存储支持正式发布**

多云存储支持现已正式发布。有关详细信息，请参阅[多云存储支持](#)。

22 June 2026

- **Microsoft Entra ID 与设备姿态服务集成**

设备姿态与 Microsoft Entra ID 的集成现已在 Windows 平台正式发布。

有关详细信息，请参阅[Microsoft Entra ID 与设备姿态服务集成](#)。

15 June 2026

- **设备姿态服务与 Chrome Enterprise 设备信任连接器集成**

设备姿态服务现已与 Chrome Enterprise 设备信任连接器集成。通过此集成，Citrix® 管理员可以将设备姿态结果共享给 Google Workspace，从而使 Chrome 能够根据受管设备的姿态强制执行上下文感知访问和数据丢失防护 (DLP) 策略。有关详细信息，请参阅[设备姿态服务与 Chrome Enterprise 设备信任连接器集成](#)。

05 June 2026

- **通过设备姿态服务管理 Endpoint Analysis (EPA) 客户端版本**

管理员可以通过设备姿态服务管理 EPA 客户端版本，方法是维护一个最低支持的 EPA 版本。管理员必须设置所有用户都必须遵守的最低版本。使用此最低版本或更高版本的用户可以执行设备姿态扫描。有关详细信息，请参阅[通过设备姿态服务管理 EPA 客户端版本](#)。

01 June 2026

• Linux 设备姿态服务的全面上市

设备姿态服务现已全面支持 Linux 平台。该服务此前作为技术预览版提供，现在支持对运行受支持 Linux 发行版的端点进行完整的策略配置和强制执行。

通过此版本，设备姿态服务在允许用户登录之前，会评估 Linux 端点的合规性，包括托管或 BYOD 状态以及整体安全姿态。这增强了零信任访问模型。

此集成提供以下优势：

- 全面的访问强制执行：根据 Linux 端点扫描结果，动态授予、限制或拒绝访问 Citrix DaaS（虚拟应用和桌面）和 Citrix Secure Private Access 资源（SaaS、Web 应用、TCP 和 UDP 应用）。
- 简化的安全检查：Linux 端点上的预身份验证上下文扫描现已与 Windows、macOS 和 iOS 的现有策略无缝集成。

管理员可以使用以下受支持的扫描为 Linux 设备配置设备姿态策略：

- 操作系统版本
- 文件（存在、上次修改时间、MD5）
- 进程（存在、MD5、SHA1）
- 挂载点

注意：

Linux 用户会在流程中看到设备姿态扫描，但只有在管理员策略中配置了 Linux 扫描时，才会评估姿态。如果未配置 Linux 规则，姿态评估将回退到默认结果。

有关为端点设备配置姿态策略的详细信息，请参阅[配置设备姿态策略](#)。

09 April 2026

• Windows Citrix Endpoint Analysis (EPA) 客户端版本 26.3.1.10 可用

此 Citrix Endpoint Analysis (EPA) 客户端更新引入了显著的性能优化和关键错误修复，旨在提高 Windows 环境中的扫描可靠性和策略处理能力。

可用性：[Citrix 下载](#)。

主要增强功能和修复：

- 改进的策略可扩展性：EPA 客户端现已优化，可处理复杂的企业环境，提供高效的数据处理和更高的稳定性。
- 改进的 Windows 更新扫描：添加了自动 UpdateSearcher 回退机制，以确保准确的补丁检测。
- User-Agent 现代化：将基于旧版 IE7 的 User-Agent 字符串替换为现代的、特定于产品的格式，以提高与当前 Web 网关和安全过滤器的兼容性。

17 March 2026

• 第三方集成失败的电子邮件通知

现在，当发生第三方集成失败时，管理员会收到电子邮件通知。这些错误也会显示在 Secure Private Access 和 Device Posture 服务仪表板中，从而能够直接联系第三方服务支持并提供相关的错误详细信息，最大限度地缩短解决时间。有关更多信息，请参阅 [第三方集成失败通知](#)。

21 January 2026

• Device Posture 服务和 deviceTRUST - 强强联合

现在，保护对企业应用程序和数据的访问不仅需要静态策略。它需要实时、上下文感知的控制，这些控制在整个用户旅程中持续适应。Citrix 的 Device Posture Service (DPS) 和 deviceTRUST (dT) 通过协作在每个阶段（预身份验证、枚举和会话内）提供全面的上下文访问覆盖，从而实现此功能。有关详细信息，请参阅 [Device Posture 服务和 deviceTRUST - 强强联合](#)。

26 September 2025

• 扫描以评估多个注册表项值

设备状态服务现在包含针对 Windows 设备的新扫描。管理员可以配置**多值非数字注册表**扫描，以评估多个注册表项值，然后确定设备的托管状态。有关使用多值非数字注册表扫描配置设备状态策略的详细信息，请参阅[配置设备状态策略](#)。

• 使用 Citrix Monitor 排除设备状态服务事务故障

管理员现在可以通过集成到 Citrix Monitor 控制板中的全面监控功能，有效诊断和排除设备状态服务事务故障。此增强功能提供了有关设备状态策略评估、合规性检查和错误诊断的详细见解。有关详细信息，请参阅[诊断设备状态服务事务](#)。

• 自动跳过状态检查

如果未在最终用户设备上检测到 EPA 客户端，设备状态服务现在支持自动跳过状态检查。配置为自动跳过时，系统会执行实时检测以确定 EPA 客户端是否存在于最终用户的设备上。如果未检测到客户端，则会自动绕过状态检查过程，无需任何用户交互，从而简化了登录过程。

如果 EPA 客户端未安装在其计算机上或 EPA 客户端版本已过时，管理员还可以配置设置，以允许最终用户在每次登录尝试时手动单击[跳过状态检查](#)。有关详细信息，请参阅[跳过设备状态检查](#)。

- **将多个 Microsoft Intune 帐户与设备状态集成**

设备状态服务现在支持与多个 Microsoft Intune 帐户集成。这使得拥有多个 Intune 租户（通常是合并、收购或部门细分的结果）的组织能够在其所有环境中无缝管理设备状态。有关详细信息，请参阅[Microsoft Intune 与设备状态集成](#)。

- **设备状态支持安全私有访问混合部署**

设备状态支持安全私有访问混合部署，但仅应要求提供。请联系 Citrix 支持或 ATS 以后用此功能。Citrix Virtual Apps and Desktops 的网关尚不支持设备状态服务。

- 有关在 NetScaler Gateway 上启用设备状态检查的详细信息，请参阅[NetScaler Gateway 上的设备状态检查](#)。
- 除了在 NetScaler Gateway 上启用设备状态功能外，您还必须在“设备状态设置”页面中添加访问 StoreFront™ 的 NetScaler Gateway 的 URL。有关详细信息，请参阅[为安全私有访问混合解决方案启用设备状态](#)。

09 July 2025

- **支持多工作区 URL**

管理员现在可以将不同的设备姿态策略应用于不同的 Citrix Workspace™ 访问 URL，从而提供精细控制并简化安全管理。以前，设备姿态服务是在所有工作区 URL 上全局启用的，这使得管理员无法根据每个 URL 应用特定要求。

借助多工作区 URL 支持，您现在可以执行以下操作：

- 为特定的工作区 URL 应用不同的设备姿态检查。
- 根据用户访问的工作区 URL，强制执行不同级别的设备合规性。
- 在部署到生产 URL 之前，在测试工作区 URL 上创建并测试设备姿态检查。

有关详细信息，请参阅 [多工作区 URL 支持](#)。

注意：

此功能处于预览阶段。

21 Feb 2025

- **通过事件驱动的姿态检查实现设备合规性**

从 EPA Library 版本 24.11.1.1 开始，设备姿态引入了增强型检查，以评估设备的合规性。

新增了以下两项扫描，以提供对设备合规性的更多控制：

- **外部设备已连接：** 此扫描检测外部 USB 存储设备是否连接到端点。
- **网络设置：** 此扫描确定设备是否连接到受保护的 Wi-Fi 网络。

当发生以下任何事件时，设备姿态会重新评估设备的合规性状态：

- 已配置**外部设备连接**扫描，并且插入或移除了外部 USB 存储设备。
- 已配置**网络设置**扫描，并且检测到开放网络和受保护网络之间的切换。
- 已配置**Windows Defender 防火墙**扫描，并且已启用或禁用它。

资源的访问权限会根据新的合规性状态进行更新。这确保了根据设备的实时合规性状态授予或撤销对资源的访问权限。

有关详细信息，请参阅[设备合规性与事件驱动的姿态检查](#)。

注意：

此功能仅在 Windows 平台上受支持。

- **降级后终止 TCP/UDP 活动会话**

对于从 Citrix Secure Access 客户端启动的 TCP/UDP 应用程序，如果设备姿态扫描导致降级（例如从**合规**到**不合规**或**拒绝访问**），用户将收到通知，并在 5 分钟后终止活动会话。有关详细信息，请参阅[设备的定期扫描](#)。

注意：

此功能仅在 Windows 平台上受支持，并且从 End Point Analysis (EPA) 客户端版本 24.8.1.19 和库版本 24.9.1.1 开始可用。

- **Windows 更新上次更新扫描的增强功能**

从 EPA 库版本 24.9.1.1 开始，**Windows 更新上次更新扫描**除了通过 Windows 自动升级服务安装的更新外，还包括通过 BigFix、Microsoft Intune 和其他第三方工具安装的更新。

04 Dec 2024

- **Jamf Pro 与设备姿态集成**

除了设备姿态服务提供的原生扫描之外，设备姿态服务还与 Jamf Pro 集成。有关详细信息，请参阅 [Jamf Pro 与设备姿态集成](#)。

29 May 2024

- **设备姿态服务在测试模式下的可用性**

设备姿态服务也提供测试模式，管理员可以在生产环境中启用该服务之前对其进行测试。这使管理员能够分析设备姿态扫描对最终用户设备的影响，然后相应地规划其行动方案，再在生产环境中启用。有关详细信息，请参阅 [测试模式下的设备姿态服务](#)。

- ****设备的定期扫描**

您现在可以为配置的检查启用 Windows 设备的定期扫描，每 30 分钟一次。有关详细信息，请参阅 [设备的定期扫描](#)。

14 May 2024

- **跳过设备姿态检查**

管理员可以允许最终用户跳过其设备上的设备姿态检查。有关详细信息，请参阅 [跳过设备姿态检查](#)。

- **设备姿态仪表板**

设备姿态服务门户现在有一个用于监控和故障排除日志的仪表板。管理员现在可以使用此仪表板进行监控和故障排除。有关详细信息，请参阅 [设备姿态日志](#)。

- **浏览器和防病毒检查的普遍可用性**

浏览器和防病毒检查现已普遍可用。有关详细信息，请参阅 [设备姿态支持的扫描](#)。

- **自定义消息的普遍可用性**

在拒绝访问时添加自定义消息的选项现已普遍可用。有关详细信息，请参阅 [访问被拒绝场景的自定义消息](#)。

26 March 2024

- **支持自定义工作区 URL**

Device Posture 服务现在支持自定义工作区 URL。除了 cloud.com URL 之外，您还可以使用自己拥有的 URL 来访问工作区。请确保允许您的网络访问 citrix.com。有关自定义域的详细信息，请参阅[配置自定义域](#)。

12 February 2024

- **支持浏览器和防病毒检查 - 预览版**

Device Posture 服务现在支持浏览器和防病毒检查。有关详细信息，请参阅[设备姿态支持的扫描](#)。

23 January 2024

- **Device Posture 服务设备证书检查正式发布**

Device Posture 服务的设备证书检查现已正式发布。有关详细信息，请参阅[设备证书检查](#)。

- **Device Posture 服务预览功能**

Device Posture 服务现在支持以下检查：

- Device Posture 服务现在支持 IGEL 平台。
- Device Posture 服务现在支持地理位置和网络位置检查。

有关详细信息，请参阅[设备姿态](#)。

11 September 2023

- **设备姿态与 Microsoft Intune 集成正式发布**

设备姿态与 Microsoft Intune 集成现已正式发布。有关详细信息，请参阅[Microsoft Intune 与设备姿态集成](#)。

30 August 2023

- **管理用于设备姿态服务的 Citrix Endpoint Analysis 客户端**

EPA 客户端可与 NetScaler 和设备姿态结合使用。与 NetScaler 和设备姿态结合使用时，需要进行一些配置更改才能管理 EPA 客户端。有关详细信息，请参阅 [管理用于设备姿态服务的 Citrix Endpoint Analysis 客户端](#)。

28 August 2023

- **iOS 平台上的设备姿态服务支持 - 预览版**

设备姿态服务现已在 iOS 平台上受支持。有关详细信息，请参阅 [设备姿态](#)。

22 August 2023

- **通过 Citrix 设备姿态服务进行设备证书检查 - 预览版**

Citrix 设备姿态服务现在可以通过检查终端设备的证书与企业证书颁发机构进行比对，从而确定终端设备是否可信，进而为 Citrix DaaS 和 Secure Private Access 资源启用上下文访问（智能访问）。有关详细信息，请参阅 [设备证书检查](#)。

17 August 2023

- **Citrix DaaS™ Monitor 上的设备姿态事件**

设备姿态服务事件和监控日志现已可在 DaaS Monitor 上搜索。有关详细信息，请参阅 [Citrix DaaS Monitor 上的设备姿态事件](#)。

23 January 2023

- **设备姿态服务**

Citrix 设备姿态服务是一种基于云的解决方案，可帮助管理员强制执行最终设备必须满足的某些要求，才能访问 Citrix DaaS（虚拟应用程序和桌面）或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）。有关详细信息，请参阅 [设备姿态](#)。

- **Microsoft Endpoint Manager 与设备姿态集成**

除了设备姿态服务提供的本机扫描之外，设备姿态服务还可以与其他第三方解决方案集成。设备姿态已与 Windows 和 macOS 上的 Microsoft Endpoint Manager (MEM) 集成。有关详细信息，请参阅 [Microsoft Endpoint Manager 与设备姿态集成](#)。

端点分析发行说明

端点分析 (EPA) 发行说明记录了适用于各种平台的 EPA 客户端的增强功能、新功能、已修复问题和已知问题。

V26.07.20 适用于 macOS (18 September 2026)

- **macOS 持续扫描支持**

Mac 版端点分析现在支持持续扫描。以前，macOS 上的设备姿态仅在用户连接时进行评估，因此登录后的更改（例如禁用防火墙或停止防病毒保护）直到下次连接尝试时才会被检测到。通过持续扫描，端点分析在整个会话期间持续重新评估设备姿态并报告其当前状态，从而使上下文访问策略能够响应设备的实时姿态，而不是一次性快照。此功能使 macOS 与 Windows 的持续扫描保持一致，从而增强了 Mac 用户的条件访问。

注意：

- 此功能正在分阶段推出，并将逐步向客户提供。
- 无需进行客户端配置更改。

V26.7.1.15 适用于 Windows (11 September 2026)

新增功能

- **Windows 上端点分析的原生 ARM64 支持**

端点分析现在支持在 ARM64 Windows 设备上原生安装。除了 x64 客户端之外，还提供了单独的 epasetup_ARM64.exe 软件包，从而无需通过 x64 仿真运行客户端。

部署与设备架构匹配的软件包：x64 设备使用 epasetup.exe，ARM64 设备使用 epasetup_ARM64.exe。原生 ARM64 支持提高了 ARM64 设备上的性能。

限制：

- ARM64 不支持键盘记录器检测。
- ARM64 客户端需要全新安装，因此在安装之前请卸载所有现有的 Endpoint Analysis 客户端。

- **Endpoint Analysis 中的键盘记录器检测（预览版）**

Endpoint Analysis 现在可以检测在端点上运行的键盘记录软件，并在 Monitor 中报告检测详细信息，以便管理员查看。

此功能可帮助管理员识别托管端点上的键盘记录风险。它仅用于可见性，不影响姿态评估或访问决策。启用它不能阻止用户访问资源。

注意：

- 此功能目前处于预览阶段，可根据请求为每个客户启用。
- ARM64 设备不支持此功能。

- **Endpoint Analysis 的捆绑扫描引擎**

扫描引擎及其库现在已包含在 Endpoint Analysis 客户端软件包中，并与客户端一起安装。将客户端和扫描引擎打包为单个版本可确保版本一致性，并消除了在下载扫描引擎组件的依赖性。客户端应用程序升级过程保持不变。

- **Endpoint Analysis 现仅支持 64 位**

Endpoint Analysis 现在仅提供 64 位客户端。不再生成或支持 32 位 (Win32/x86) 二进制文件和安装程序，并且安装程序无法在 32 位版本的 Windows 上运行。

- 更新任何引用 32 位 Endpoint Analysis 软件包的部署脚本或软件分发包。
- 两种支持的 64 位架构均可用：`epasetup.exe` 适用于 x64 设备，`epasetup_ARM64.exe` 适用于 ARM64 设备。

- **Endpoint Analysis 使用专用安装路径**

Endpoint Analysis 现在安装在产品特定的文件夹和注册表位置，而不是使用共享的 Secure Access Client 位置。

安装路径为：

- 每台计算机: C:\Program Files\Citrix\安全访问端点分析
- 每用户: %LocalAppData%\Citrix\安全访问端点分析
- 产品注册表键：HKLM\SOFTWARE\Citrix\Secure Access Endpoint Analysis

- **卸载期间的 Endpoint Analysis 保留**

当另一个已安装的 Citrix 产品仍依赖于 Endpoint Analysis 时，卸载 Citrix 产品不再会移除 Endpoint Analysis。这适用于 Endpoint Analysis 在同一设备上由多个 Citrix 产品（例如 Citrix Workspace 应用程序、Citrix Enterprise Browser 和 Citrix Secure Access）共享的情况。以前，卸载一个产品可能会移除 Endpoint Analysis，导致其他产品没有姿态客户端。

当交互式卸载会移除仍需的客户端时，维护页面会列出保持 Endpoint Analysis 安装的依赖应用程序。

注意：

- 对于脚本化移除，正确保留 Endpoint Analysis 的静默卸载将返回退出代码 `1000`。在您的部署系统中将 `1000` 配置为成功代码。
- 若要尽管存在依赖项仍移除 Endpoint Analysis，请从具有 `/SkipConsumerCheck` 的提升权限提示符下重新运行卸载命令。

• Endpoint Analysis 支持无人值守部署

Endpoint Analysis 安装程序现在支持通过 Configuration Manager 和 Intune 等软件分发工具进行无人值守安装和卸载。在安装和卸载时，使用 `/quiet` 进行静默操作，并使用 `/log <path>` 指定日志位置。

注意：

- 这些选项适用于集中管理部署。如果安装程序无法写入指定的日志路径，它将停止并显示退出代码 `1622`，而不是静默地将日志写入其他位置。
- 在卸载期间，即使有其他 Citrix 产品依赖于 Endpoint Analysis，也可以使用仅限提升权限的 `/SkipConsumerCheck` 选项将其删除。
- 在部署工具中将退出代码 `1000` 配置为成功代码。此代码表示 Endpoint Analysis 被有意保留，因为另一个 Citrix 产品仍需要它。

• 现代化 Endpoint Analysis 安装程序

Endpoint Analysis 安装程序界面现在已针对安装、修复和维护进行了增强。当用户以交互方式安装、修复或删除客户端时（例如从下载页面或维护页面），将显示增强的界面。

注意：

静默部署和脚本部署仍然受支持。由于不再支持基于 MSI 的部署，请根据需要使用以下 `epasetup.exe` 命令行开关。

- `/quiet`、`/silent`、`/q` - 无用户界面的静默安装。
- `/passive` - 仅显示进度，无交互式提示。
- `/uninstall` - 卸载产品。
- `/repair` - 修复现有安装。
- `/log "<file>"` - 将安装程序日志写入指定路径。
- `/norestart` - 禁止在安装或卸载后自动重启。
- `/?`、`/h`、`/help` - 显示安装程序帮助信息。

已修复的问题

- Windows Update 姿态从错误来源报告：热补丁机器显示了已取代基线的年龄，补丁年龄基于不相关的安装，并且报告了无法测量的值，而不是将其识别为不可用。
- 在 Windows Update 服务启动时，来自第三方扫描引擎的姿态信号会间歇性地不可用。
- 扫描引擎故障被报告为设备上未安装任何安全产品，这使得引擎故障与真正未受保护的设备无法区分，从而导致相同的访问拒绝。
- 签名验证现在要求签名者链接到机器信任存储中的根证书。仅在每个用户存储中受信任的根证书不再被接受。使用自定义受信任签名证书的管理员必须将其部署到整个机器。
- `devicePostureNativeBridge.exe` 进程可以清除 `config.js`，从而删除已保存的连接。结果，已保存的连接会从客户端消失。
- 重复扫描可能导致内存和句柄泄漏。
- 用户无法重试卸载或移除损坏的安装。

通过此修复，维护页面现在提供与静默路径相同的深度清理选项，允许在损坏的安装上卸载失败时进行恢复。

- 卸载 Endpoint Analysis 会留下孤立的服务注册表项。

- 当 NetScaler Gateway 上同时启用全局服务器负载均衡、HSTS、httpOnly cookie 和内容安全策略时，浏览器 Endpoint Analysis 流程会失败。
- 用户可能会无限期地停留在“正在检查您的设备...”屏幕上，因为大型服务响应可能会被截断或过度读取，从而阻止设备检查完成。
- 浏览器原生消息主机以前接受来自非验证浏览器的进程连接，因为它只检查连接的一端。通过此修复，它现在验证两端都属于同一个浏览器进程。
- 当接收器进程关闭时，与代理的剪贴板握手失败。

适用于 Windows 的 V26.6.1.4 (24 August 2026)

以下部分提供了有关适用于 Windows 的 V26.6.1.4 版本发布的更多信息。

新增功能

- **更新了 OPSWAT 库，解决了设备状态扫描期间的内存泄漏问题**

EPA 客户端现在包含更新的 OPSWAT (OESIS) 库，可解决第三方产品检测期间的内存泄漏问题。执行频繁或连续设备状态扫描的设备在扫描过程中不再出现内存逐渐累积的情况。此次更新还扩展了对第三方安全产品的检测支持，包括 ALYac、WatchGuard Endpoint Security Prime 和 Trellix EDRF。

已修复的问题

- 当在“客户端选择”页面上选择“完整隧道”时，从浏览器启动 Citrix Secure Access 可能会无法加载主页。出现此问题的原因是 EPA 发送了不正确终止的 HTTP 标头，该标头被 NetScaler Gateway 拒绝。
- 设备状态扫描可能无法完成，导致客户端停留在“正在检查您的设备...”消息。当设备状态服务返回的扫描配置超出客户端容量时（例如管理员启用注册表扫描策略时），就会出现此问题。
- 在每个扫描周期中，用户可能会被拒绝访问资源。当本地设备状态管理服务在定期扫描期间保存和读取上下文时无法持续解析已登录用户时，就会出现此问题。

适用于 Windows 的 V26.5.1.7 (08 Jul 2026)

以下部分提供了有关适用于 Windows 的 V26.5.1.7 版本发布的更多信息。

已修复的问题

- 在某些设备上，EPA 客户端错误地报告了 Windows 版本。例如，Windows 11 设备被报告为较旧的 Windows 版本，导致基于操作系统的扫描检查评估不正确。此问题影响某些 Windows 10 和 Windows 11 设备上的 EPA v1（经典、本地）扫描流程。
- 在管理模式部署中，设备证书姿态检查可能会失败，因为 EPA 管理服务在评估期间不会自动选择设备证书。在受影响的设置中，这会导致定期（连续）设备证书检查反复失败。
- 对于某些安全产品，例如 CrowdStrike Falcon 和基于 OPSWAT 的产品，扫描未能正确应用“忽略互联网检查”设置。结果，诸如病毒定义上次更新时间之类的检查可能会失败，即使产品运行正常。

此问题发生在受影响产品的基于 OPSWAT 的防病毒和定义扫描中。

- 用户可能会遇到设备姿态上下文读取失败。例如，浏览器扩展可能会报告无法获取设备姿态上下文，因为存储的 EPA 上下文文件未被可靠地解密和读取。当设备姿态服务写入并随后重新读取加密的姿态上下文和定期扫描文件时，会出现此问题。

V26.03.31 适用于 macOS (14 May 2026)

以下部分提供了有关适用于 macOS 的 V26.03.31 版本的更多信息。

新增功能

- **独立库更新的弃用**

从本版本开始，不再支持依赖运行时的库更新。这些组件的所有未来更新将仅通过新版本的 CitrixEndpointAnalysis 应用程序提供。

- **静态库与 EPA 应用程序集成**

系统扫描所需的核心库现在直接捆绑在 CitrixEndpointAnalysis 应用程序中，适用于云部署和本地部署。

这种集成提供了以下优势：

- 集成的库现在在应用程序启动期间会经过严格的签名验证。
- 通过捆绑这些资产，应用程序不再需要在运行时下载和提取库，从而实现更快的初始化和更可靠的启动。

配置设备姿态策略

设备姿态是策略和规则的组合，设备必须满足这些策略和规则才能访问资源。每个策略都附带以下操作之一：合规、不合规和拒绝登录。此外，每个策略都与一个优先级相关联，如果策略评估为 true，则策略评估将停止并执行关联的操作。

1. 登录 Citrix Cloud™，然后从汉堡菜单中选择“身份和访问管理”。
2. 单击“设备姿态”选项卡，然后单击“管理”。

注意：

- Secure Private Access 服务客户可以直接在管理员用户界面的左侧导航中单击“设备姿态”。
- 对于首次使用的用户，“设备姿态”登录页面会提示您创建设备姿态策略。必须为每个平台单独配置设备姿态策略。创建设备姿态策略后，它将列在相应的平台下。
- 策略仅在启用设备姿态后生效。要启用设备姿态，请将右上角的“设备姿态已禁用”切换开关滑动到“开”。

3. 单击“创建设备策略”。
4. 在“平台”中，选择要应用策略的平台。无论您在“设备姿态”主页上选择了哪个选项卡，都可以将平台从 Windows 更改为 macOS，反之亦然。
5. 在“策略规则”中，选择要作为设备姿态一部分执行的检查，然后选择必须匹配的条件。

请注意有关“设备证书”检查的以下几点：

- 确保颁发者证书存在于设备上。否则，您可以在创建设备姿态策略时导入设备证书，或从“设备姿态”主页上的“设置”上传证书。有关详细信息，请参阅[设备证书检查](#)。
- 在多个设备证书共享通用颁发者名称的环境中，“设备姿态”服务可能会评估错误的证书。为确保服务识别特定策略的确切证书，您必须明确启用“检查指纹”选项。有关详细信息，请参阅[配置设备证书检查扫描](#)。
- 终端设备上的 EPA 客户端必须以管理员权限安装。
- 设备证书检查与设备姿态服务不支持证书吊销检查。

注意：

- **多值非数字注册表扫描**允许管理员确定设备是托管还是非托管。这是通过评估多个注册表项值来实现的。
- 为网络位置检查创建策略规则时，您可以直接从设备姿态服务控制台添加网络位置。但是，要修改网络位置，您必须使用 Citrix Cloud 上的网络位置配置。

6. 单击**添加另一个规则**以创建多个规则。多个规则之间应用 AND 条件。

配置设备姿态(/en-us/device-posture/media/device-posture-configuration1.png)

7. 在**策略结果**中，根据您配置的条件，选择设备扫描必须对用户设备进行分类的类型。

- 合规
- 不合规
- 拒绝访问

8. 输入策略名称。

9. 在**优先级**中，输入评估策略的顺序。

- 您可以输入 1 到 100 之间的值。建议您将拒绝策略配置为更高优先级，其次是不合规策略，最后是合规策略。
- 值越低的优先级越高。
- 只有启用的策略才会根据优先级进行评估。

10. 单击**创建**。

Create device policy

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

Policy result

If policy conditions and rules are met, the device scan will classify the user device as one of the following:

☒ Compliant

The device will be considered compliant and full access will be granted.

☐ Non-compliant

The device will be considered "non-compliant" and restricted access will be granted.

☐ Denied access

The device will be denied access to all resources.

Scan details

Name and set the priority order of this device scan.

Name

Device scan name

Priority

Priority number (1-100)

重要提示：

- 您必须将“创建时启用”切换开关设置为“开”，以使设备姿态策略生效。在启用策略之前，建议您确保策略已正确配置，并且您正在测试设置中执行这些任务。
- Linux 用户会在流程中看到设备姿态扫描，但只有在管理员策略中配置了 Linux 扫描时，才会评估姿态。如果未配置 Linux 规则，姿态评估将回退到默认结果。

使用设备姿态配置上下文访问（智能访问）

设备姿态验证后，设备将被允许登录并分类为合规或不合规。此信息作为标签提供给 Citrix DaaS 服务和 Citrix Secure Private Access™ 服务，并用于根据设备姿态提供上下文访问。因此，必须配置 Citrix DaaS 和 Citrix Secure Private Access 以使用设备姿态标签强制执行访问控制。

Citrix DaaS 与设备姿态配置

要限制对 DaaS 资源的访问，您可以指定必须强制执行访问限制的交付组，并使用设备姿态标签配置访问控制限制。

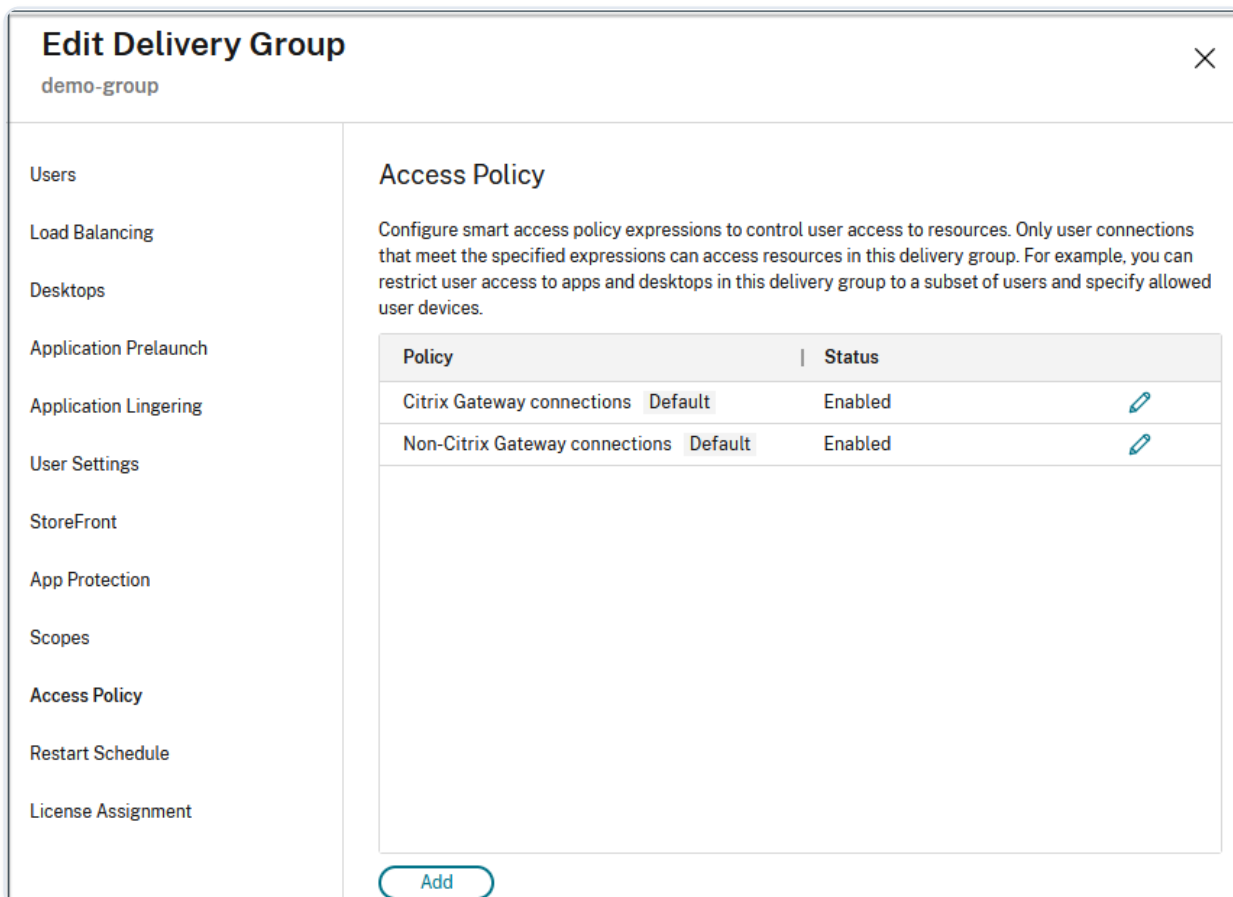
先决条件：

确保已启用自适应访问功能（**Citrix Workspace > 访问 > 自适应访问**）。有关详细信息，请参阅[启用自适应访问功能](#)。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

32

1. 登录 Citrix Cloud。
2. 在“DaaS”磁贴上，点击“管理”。
3. 从左侧菜单转到“交付组”部分。
4. 选择要为其配置基于设备姿态的访问控制的交付组，然后点击“编辑”。
5. 在“编辑交付组”页面中，单击“访问策略”。
6. 单击“Citrix Gateway 连接”行上的编辑图标以编辑网关连接策略。



- a. 在“编辑策略”页面上，选择“符合以下条件的连接”。
- b. 选择“匹配任意”，然后单击“添加条件”。
- c. 为您在“配置网络位置”中配置的所有位置标签添加条件：为“筛选器”键入“Workspace”，为“值”键入“COMPLIANT”或“NON-COMPLIANT”。

Edit Policy

Add criteria to filter user connections. A criterion comprises a smart access filter and a value. You can add inclusion and exclusion criteria.

Policy name:

Policy state: ☒

☒ Connections meeting the following criteria

☐ Match all ☒ Match any

Filter:	Value:	
<input type="text" value="Workspace"/>	<input type="text" value="NON-COMPLIANT"/>	
<input type="text" value="Workspace"/>	<input type="text" value="DEVICE_TYPE_WINDOWS"/>	

[+ Add criterion](#)

☐ Connections not meeting any of the following criteria

No criteria added

[Done](#) [Cancel](#)

注意：

设备分类标签的语法必须与之前捕获的完全一致，即全部大写（**COMPLIANT** 和 **NON-COMPLIANT**）。否则，设备姿态策略将无法按预期工作。

除了设备分类标签外，设备姿态服务还会返回与设备关联的操作系统标签和访问策略标签。操作系统标签和访问策略标签必须仅以大写形式输入。

- DEVICE_TYPE_WINDOWS
- DEVICE_TYPE_MAC
- 确切的策略名称（大写）

使用设备姿态配置 Citrix Secure Private Access

要限制对 Secure Private Access 资源的访问，您可以选择必须强制执行访问限制的应用程序，并使用设备姿态标签配置访问控制限制。

1. 登录 Citrix Cloud。

2. 在 Secure Private Access 磁贴上，单击 **管理**。
3. 在左侧导航栏中单击 **访问策略**，然后单击 **创建策略**。
4. 输入策略名称和策略描述。
5. 在 **应用程序** 中，选择必须强制执行此策略的应用程序或应用程序集。
6. 单击 **创建规则** 为策略创建规则。
7. 输入规则名称和规则的简要描述，然后单击 **下一步**。
8. 选择用户条件。**用户** 条件是授予用户访问应用程序的强制性条件。
9. 单击 **+** 添加设备姿态条件。
10. 从下拉菜单中选择 **设备姿态检查** 和逻辑表达式。
11. 在自定义标签中输入以下值之一：

- **合规** - 适用于合规设备
- **不合规** - 适用于不合规设备

注意：

标签必须与前面捕获的完全一致，使用首字母大写（**合规** 和 **不合规**）。否则，设备姿态策略将无法按预期运行。

12. 单击 **下一步**。
13. 根据条件评估选择必须应用的操作，然后单击 **下一步**。

“摘要”页面显示策略详细信息。

14. 您可以验证详细信息并单击 **完成**。

有关创建访问策略的更多详细信息，请参阅 [配置具有多个规则的访问策略](#)。

注意：

任何在访问策略中未标记为合规或不合规的 Secure Private Access 应用程序都将被视为默认应用程序，并且无论设备状态如何，都可在所有端点上访问。

✓ Rule details

2 Conditions

3 Actions

4 Summary

Step 2: Conditions

User*

Matches any of

Select a domain

administratoradminis

AND

Device posture check

Matches any of

Compliant, Non-Compliant

+ Add condition

Cancel

Back

Next

编辑设备体态策略

配置的设备体态策略列在“设备扫描”页面中特定平台下。您可以从此页面搜索要编辑的策略。您还可以从此页面启用、禁用或删除策略。

Device Posture

Device posture is enabled

Device Scans

WindowsmacOSOthers

Create device posture here

Priority	Policy Name	Result	Status
12	dev-post-check-access-deny	Deny	<div>✓</div>
17	dev-post-check-allow-access	Compliant	<div>✓</div>
20	dev-post-check-access-restrict	Non-Compliant	<div>✓</div>

配置设备姿态全局设置

以下是一些您可以根据需要进行配置的全局设备姿态设置。

- 通过事件驱动的姿态检查实现设备合规性(/zh-cn/device-posture/device-posture-global-settings.html#device-compliance-with-event-driven-posture-checks)
- 定期扫描设备(/zh-cn/device-posture/device-posture-global-settings.html#periodic-scanning-of-devices)
- 用于访问被拒绝场景的自定义消息(/zh-cn/device-posture/device-posture-global-settings.html#customized-messages-for-access-denied-scenarios)
- 跳过设备姿态检查(/zh-cn/device-posture/device-posture-global-settings.html#skip-device-posture-checks)
- 自定义工作区 URL 支持(/zh-cn/device-posture/device-posture-global-settings.html#custom-workspace-urls-support)
- 结合设备姿态的会话录制配置(/zh-cn/device-posture/device-posture-global-settings.html#session-recording-configuration-with-device-posture)
- 设备证书检查(/zh-cn/device-posture/device-posture-global-settings.html#device-certificate-check)
- 配置允许的域列表(/zh-cn/device-posture/device-posture-global-settings.html#configure-the-list-of-allowed-domains)

通过事件驱动的姿态检查实现设备合规性

从 EPA Library 版本 24.11.1.1 开始，设备姿态引入了增强的检查，以评估设备的合规性。

添加了以下两种扫描，以提供对设备合规性更强的控制：

- **外部设备已连接**：此扫描检测外部 USB 存储设备是否连接到端点。
- **网络设置**：此扫描确定设备是否连接到受保护的 Wi-Fi 网络。

当发生以下任何事件时，设备姿态会重新评估设备的合规性状态：

- 配置了**外部设备连接**扫描，并且插入或移除了外部 USB 存储设备。
- 配置了**网络设置**扫描，并且检测到开放网络和受保护网络之间的切换。

- 配置了**Windows Defender 防火墙**扫描，并且它已启用或禁用。

资源的访问权限会根据新的合规性状态进行更新。这确保了根据设备的实时合规性状态授予或撤销对资源的访问权限。

注意：

- 事件驱动的姿态检查目前仅在适用于 Windows 版本 24.8.1.19 及更高版本的 Citrix Secure Access 客户端上受支持。
- 尽管用户和管理员安装都可以利用姿态扫描，但基于事件的设备合规性实时重新评估需要管理员权限。

下图显示了在设备姿态管理控制台中配置的外部设备连接和网络设置扫描。

Create device policy

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

Platform

Select the operating system for this device posture scan. ?

Windows

Policy rules

Select a condition and apply access rules for your services and data. ?

External Device Connected

USB Storage

Equal to ==

false

+ Add qualifier

AND

Network Settings

Password Protected WiFi

Equal to ==

true

设备的定期扫描

您可以为配置的检查启用 Windows 设备每 30 分钟进行一次定期扫描。终端设备上的 EPA 客户端必须以管理员权限安装才能启用设备的定期扫描。要启用定期扫描，请执行以下操作：

1. 导航到**设备姿态 > 设备扫描**，然后单击**设置**。
2. 在**定期设备姿态扫描**部分中，将切换开关滑动到“开”以启用设备的定期扫描。

Periodic device posture scans

Check the end user's device posture, every 30 minutes. Currently supported only on windows end devices.



- 对于 HTTP/HTTPS 应用程序，如果设备姿态扫描结果从 **合规** 变为 **不合规** 或 **拒绝访问**，则对资源的访问将根据新的合规状态进行更新。
- 对于从 Citrix Secure Access 客户端启动的 TCP/UDP 应用程序，如果设备姿态扫描导致降级（例如从 **合规** 变为 **不合规** 或 **拒绝访问**），用户将收到通知，并在 5 分钟后终止活动会话。



访问被拒绝场景的自定义消息

管理员可以自定义在访问被拒绝时显示在终端设备上的消息。

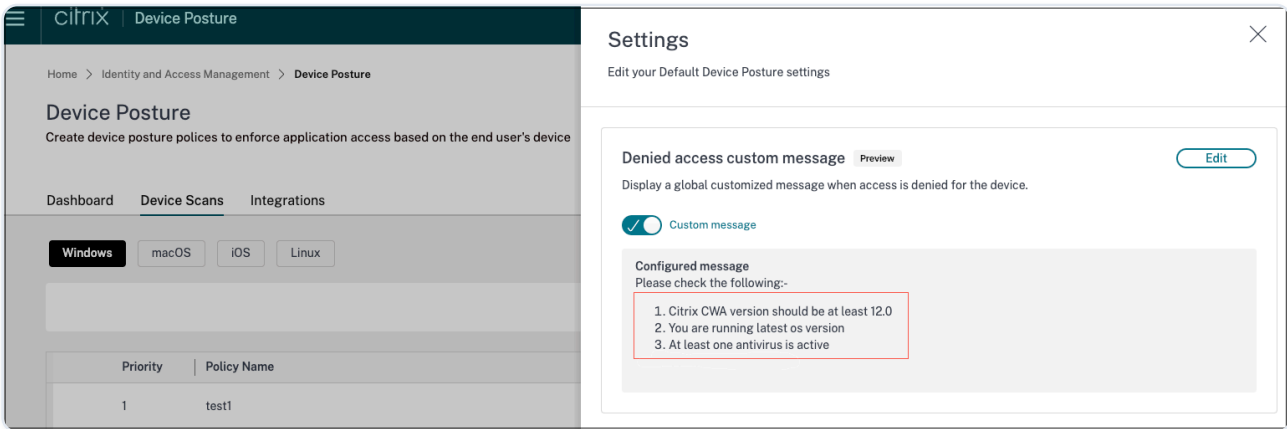
执行以下步骤以添加自定义消息：

1. 导航到 **设备姿态 > 设备扫描** 页面。
2. 单击 **设置**。
3. 单击 **编辑**，然后在 **消息** 框中，输入在访问被拒绝场景中必须显示的消息。您最多可以输入 256 个字符。
4. 单击 **保存时启用自定义消息** 以强制执行显示自定义消息的选项。如果您未选中此复选框，则会创建自定义消息，但不会在访问被拒绝场景中显示在设备上。

或者，您可以在 **设置** 页面上启用 **自定义消息** 切换开关以在设备上显示消息。

5. 单击 **保存**。

下图显示了管理员添加的示例消息。



下图显示了当访问被拒绝时，最终用户设备上显示的自定义消息。



当终端设备访问被拒绝时，您输入的消息将显示出来。

跳过设备姿态检查

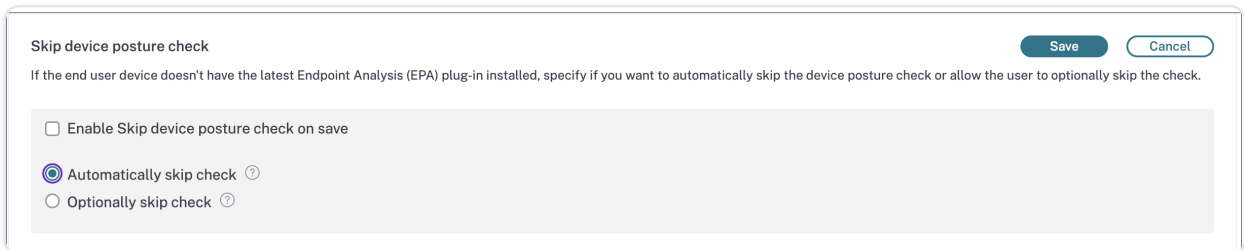
管理员可以配置设备姿态检查自动跳过，或者允许最终用户在以下场景中跳过检查：

- 设备上未安装 EPA 客户端。
- 设备上安装的 EPA 客户端已过时。

启用跳过检查功能后，将强制执行默认策略结果（不合规），并将设备归类为不合规。最终用户将获得对 Citrix Secure Private Access™ 或 Citrix DaaS 资源的有限或受限访问权限。

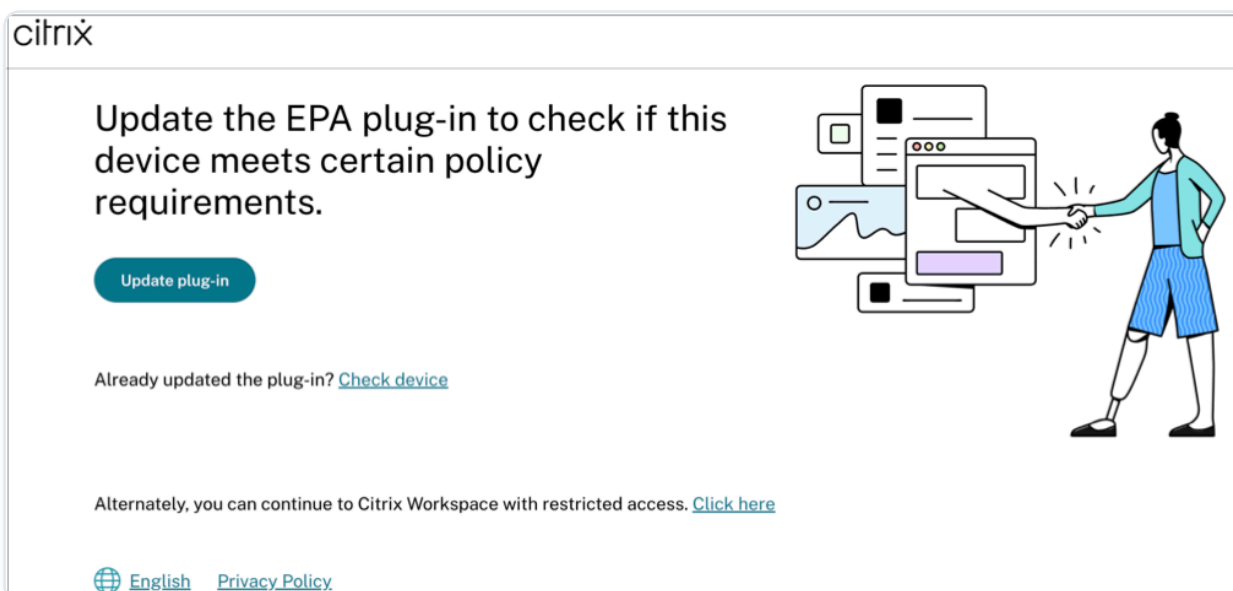
启用跳过设备姿态检查

1. 导航到 **设备姿态 > 设备扫描**。
2. 单击 **设置**。
3. 在 **跳过设备姿态检查** 部分，将切换开关滑动到“开”以启用跳过设备姿态检查，然后单击 **编辑**。



4. 选择以下选项之一：
- **自动跳过检查** - 当 EPA 客户端缺失或过时，系统会自动绕过姿态检查，从而简化了从没有 EPA 客户端的设备访问 Citrix Workspace 的用户的登录过程。
 - **可选跳过检查** - 当从没有 EPA 客户端的设备登录 Citrix Workspace 时，系统会提示用户通过单击 **跳过姿态检查** 来手动跳过姿态检查。

当启用**可选跳过检查**选项且最终用户登录到 Citrix Workspace 时，当最终用户尝试下载客户端或升级 EPA 版本时，将显示以下消息。



5. 单击**保存**。

自定义工作区 URL 支持

设备状态服务支持自定义工作区 URL。除了您的 cloud.com URL 之外，您还可以使用您拥有的 URL 来访问工作区。确保您允许您的网络访问 citrix.com。有关自定义域的详细信息，请参阅[配置自定义域](#)。

会话录制与设备状态配置

会话录制允许组织录制虚拟会话中的屏幕用户活动。您可以在创建自定义会话录制策略、事件检测策略或事件响应策略时指定标签。有关示例，请参阅[创建自定义录制策略](#)。

设备证书检查

要使用设备状态服务配置设备证书检查，管理员必须从其设备导入颁发者证书。一旦设备状态服务中存在有效的颁发者证书，管理员就可以将设备证书检查用作设备状态策略的一部分。

注意事项：

- 设备状态服务仅支持 PEM 颁发者证书类型。
- 对于 Windows 上的设备证书检查，最终设备上的 EPA 客户端必须以管理员权限安装。对于其他检查，您不需要本地管理员权限。有关支持的扫描的详细信息，请参阅[设备状态支持的扫描](#)。
- 要在 Windows 上以管理员权限安装 Endpoint Analysis 客户端，请在客户端下载的文件夹中，从提升的命令提示符运行命令 `epasetup.exe /quiet`。在 ARM64 设备上，请改为运行 `epasetup_ARM64.exe /quiet`。
- 使用设备状态服务的设备证书检查不支持证书吊销检查。
- 如果设备证书由中间证书签名，则必须将包含根证书和中间证书的完整链上传到单个 PEM 文件中。

Example: chain.pem

```
-----BEGIN CERTIFICATE-----
```

```
*****
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
*****
```

```
-----END CERTIFICATE
```

上传设备证书

1. 在设备姿态主页上，点击**设置**。
2. 点击**管理**，然后点击**导入颁发证书**。
3. 在**证书类型**中，选择证书类型。仅支持 PEM 类型。
4. 在**证书文件**中，点击**选择证书**以选择颁发者证书。
5. 点击**打开**，然后点击**导入**。

Import Issuer Certificate

Issuer certificate will be added to the Endpoint. View certificate details in certificate table once created.

Certificate Type *

PEM (Privacy Enhanced Mail)

Certificate File *

cgwsanitydc.pem

+ Choose Certificate

Import

Cancel

所选证书列在**设置 > 颁发者证书**中。您可以导入多个证书。

查看已导入的证书

1. 在设备姿态主页上，点击**设置**。
2. 在**颁发者证书**中，点击**管理**。
3. 颁发者证书页面列出了已导入的颁发者证书。

Issuer Certificates

Issuer Certificates will be used to validate the device certificates as per the configured policies.

Import Issuer Certificate

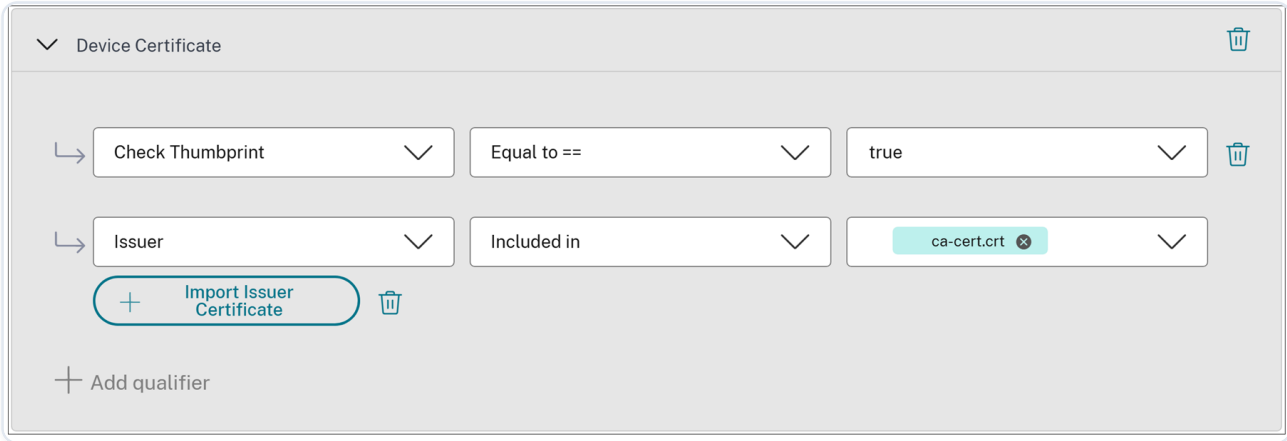
Issuer	Certificates	Policies	Status	
cgwsanity-DC-CA	cgwsanitydc.pem	NA	Valid	↓ 🗑️
int-CA	combinedchain.pem	NA	Valid	↓ 🗑️

配置设备证书检查扫描

1. 配置设备姿态策略。有关详细信息，请参阅[配置设备姿态策略](#)。
2. 添加设备证书检查的策略规则时，请同时指定“**检查指纹**”和“**颁发者**”条件。

重要提示：

如果您的环境中存在多个设备证书共享相同的颁发者名称，您必须启用“**检查指纹**”选项，以防止服务匹配错误的证书。如果未启用此选项，服务将仅按颁发者名称匹配证书，这可能会在存在重复颁发者名称时导致策略冲突。



在终端设备上安装设备证书

视窗：

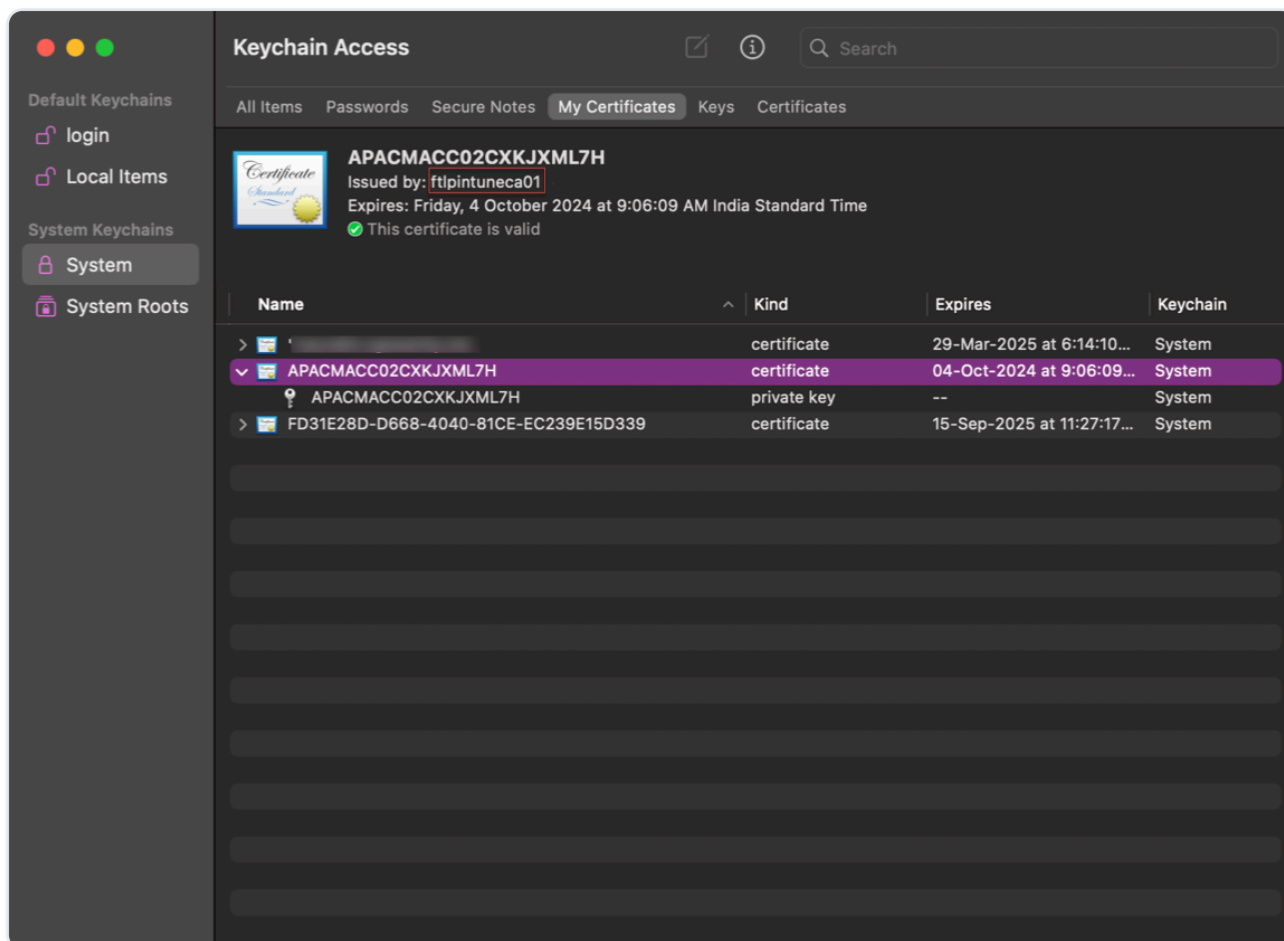
1. 从“开始”菜单，打开“计算机证书管理器”。
2. 确保证书已安装在 `Certificates - Local Computer\Personal\Certificates` 。
 - “预期用途”必须包括“客户端身份验证”。
 - “颁发者”列必须与管理 GUI 上配置的颁发者名称匹配。

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
34c6b0a3-e753-4009-b4b1-95d1...	Microsoft Intune MDM Device CA	17-10-2024	Client Authentication	<None>
APACENGW4UMJMN.citrite.net	ftlpintuneca01	18-10-2024	Client Authentication	<None>
APACENGW4UMJMN.citrite.net	ftlissuingca01	18-10-2024	Client Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-P2P-Access [2023]	24-10-2023	Server Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-Access	19-10-2033	Client Authentication	<None>

macOS：

1. 打开“钥匙串访问”，然后选择“系统”。
2. 单击“文件 > 导入项目”以导入证书。

“颁发者”字段必须显示证书颁发者名称。



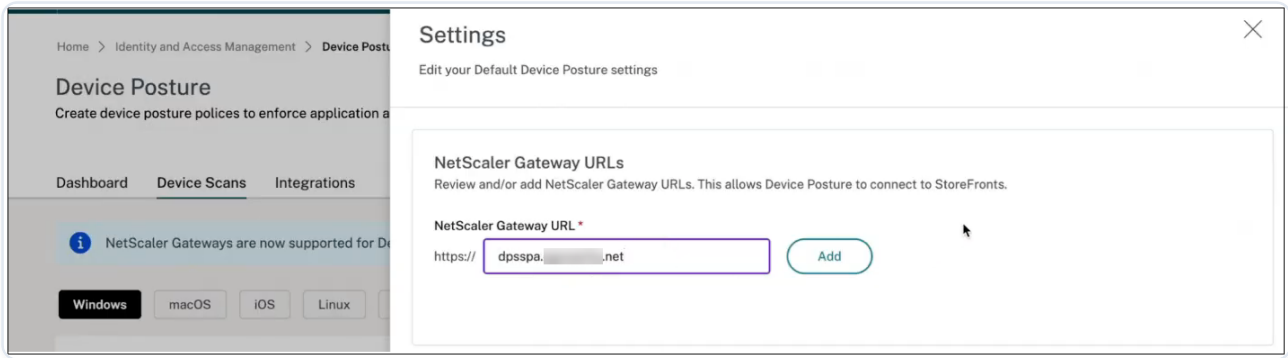
配置允许的域列表

您可以配置 NetScaler Gateway 虚拟服务器的 FQDN，从中可以启动设备姿态服务扫描。

注意：

- 此功能仅适用于 Secure Private Access 部署。
- 要为您的 Secure Private Access 部署启用此功能，请联系 Citrix 支持。

1. 导航到 **设备姿态 > 设备扫描**，然后单击 **设置**。
2. 在 **NetScaler Gateway URL** 中，输入必须为其启用设备姿态检查的虚拟服务器的 FQDN。例如， `https://gw.example.net`。



有关此功能的示例用例，请参阅 [为 Secure Private Access 混合解决方案启用设备姿态](#)。

要在 NetScaler 上配置设备姿态扫描，请参阅 [NetScaler Gateway 上的设备姿态检查](#)。

设备姿态服务与 Chrome Enterprise 设备信任连接器集成

设备姿态服务与 Chrome Enterprise 设备信任连接器集成。通过此集成，Citrix® 管理员可以将设备姿态结果共享给 Google Workspace，使 Chrome 能够根据受管设备的姿态强制执行上下文感知访问和数据丢失防护 (DLP) 策略。

Citrix 共享的姿态信号可由 Chrome 使用，以对以下各项做出访问决策：

- 受管 Chrome 浏览器
- 受管 Chrome 配置文件

有关 Chrome 可以从第三方连接器接收的信号列表，请参阅 [Google 的端点验证文档](#)。

注意：

仅当设备姿态服务处于全局模式时，才支持与 Chrome Enterprise 设备信任连接器集成。

支持的平台和部署

项目	支持
支持的平台	Windows，EPA 客户端版本 26.5.1.7 或更高版本
部署	带有 Citrix Enterprise Premium 的安全私有访问服务
	安全私有访问混合

先决条件

- 一个具有设备姿态服务授权并已配置的 Citrix Cloud 租户。
- 一个具有 Chrome Enterprise Premium (CEP) 许可证和访问 Google 管理控制台的超级管理员权限的 Google Workspace 租户。
- Chrome Enterprise Premium 已为客户部署。

- 在 Google 管理控制台中，[上下文感知访问](#)访问级别设置为“开”。有关详细信息，请参阅[应用推荐的访问级别](#)。

配置

Citrix 设备姿态服务与 Chrome Enterprise 设备信任连接器的集成涉及以下高级步骤：

1. [配置 Chrome Enterprise Premium 和设备姿态服务](#)
2. [将 Citrix 设备姿态服务与 Chrome 设备信任连接器集成](#)
3. [为 Citrix 信号定义上下文感知规则](#)

配置 Chrome Enterprise Premium 和设备姿态服务

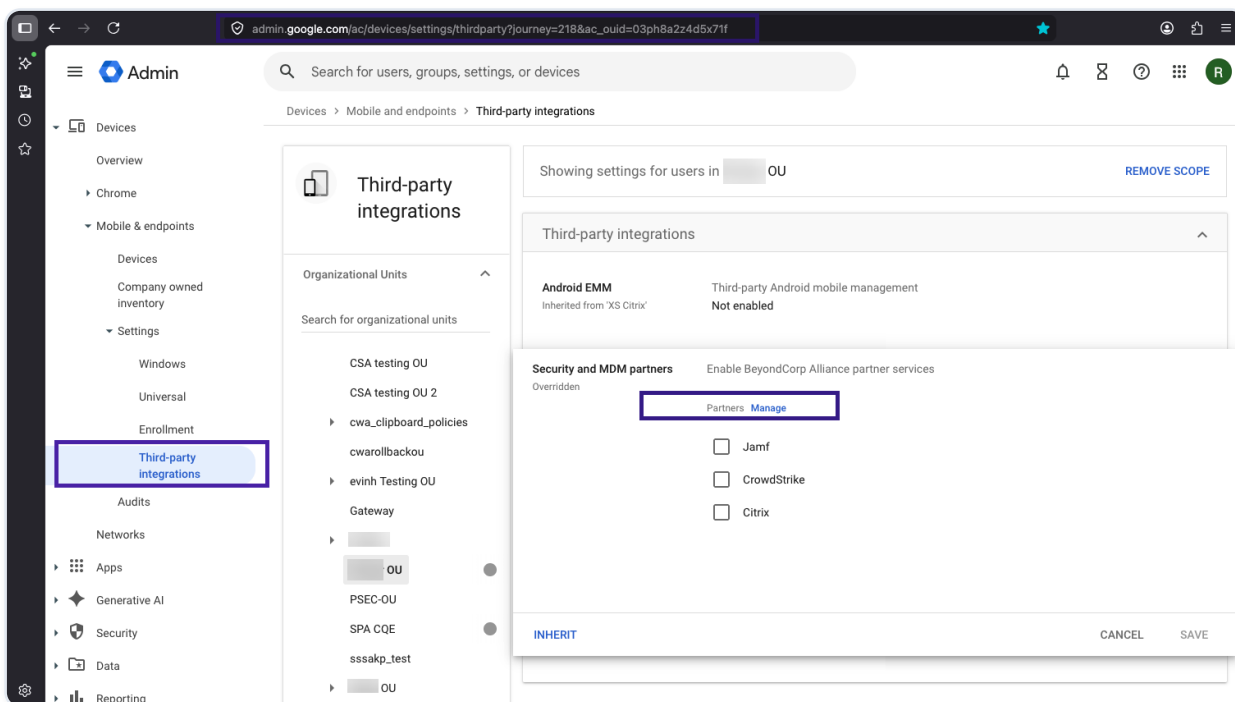
在与 Chrome 集成之前，请确保已完成以下配置：

1. 在托管的 Windows 端点上部署和配置 Chrome Enterprise Premium (CEP)。有关详细信息，请参阅[与 Google Chrome Enterprise Premium 集成](#)。
2. 配置设备姿态服务策略，以生成您打算与 Chrome 共享的信号（例如，操作系统版本、防病毒状态、地理位置或授权国家/地区、自定义检查）。有关详细信息，请参阅[配置设备姿态策略](#)。
3. 确认您的 Google Workspace 租户拥有 Chrome Enterprise Premium (CEP) 许可，这是使用设备信任连接器和上下文感知访问规则所必需的。有关详细信息，请参阅[许可证](#)、[应用版本和扩展](#)。

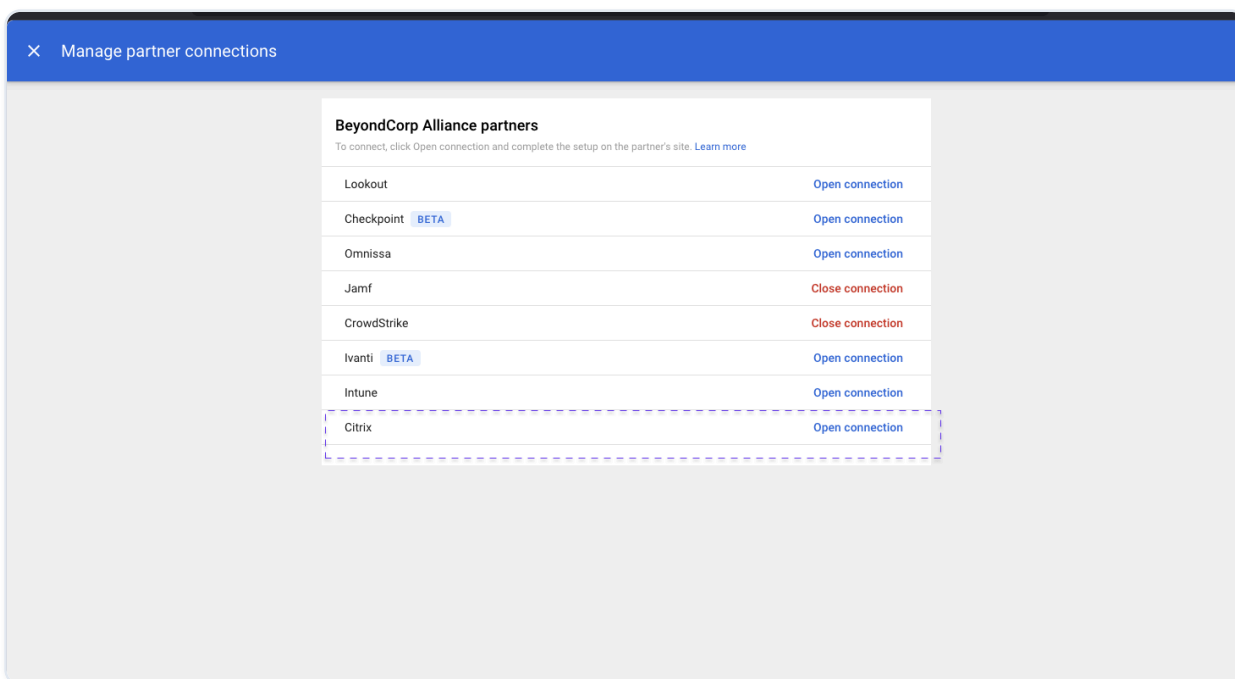
将 Citrix 设备姿态服务与 Chrome 设备信任连接器集成

要将 Citrix 设备姿态服务与 Chrome 设备信任连接器集成，您必须在 Google 管理控制台中启用第三方连接器。

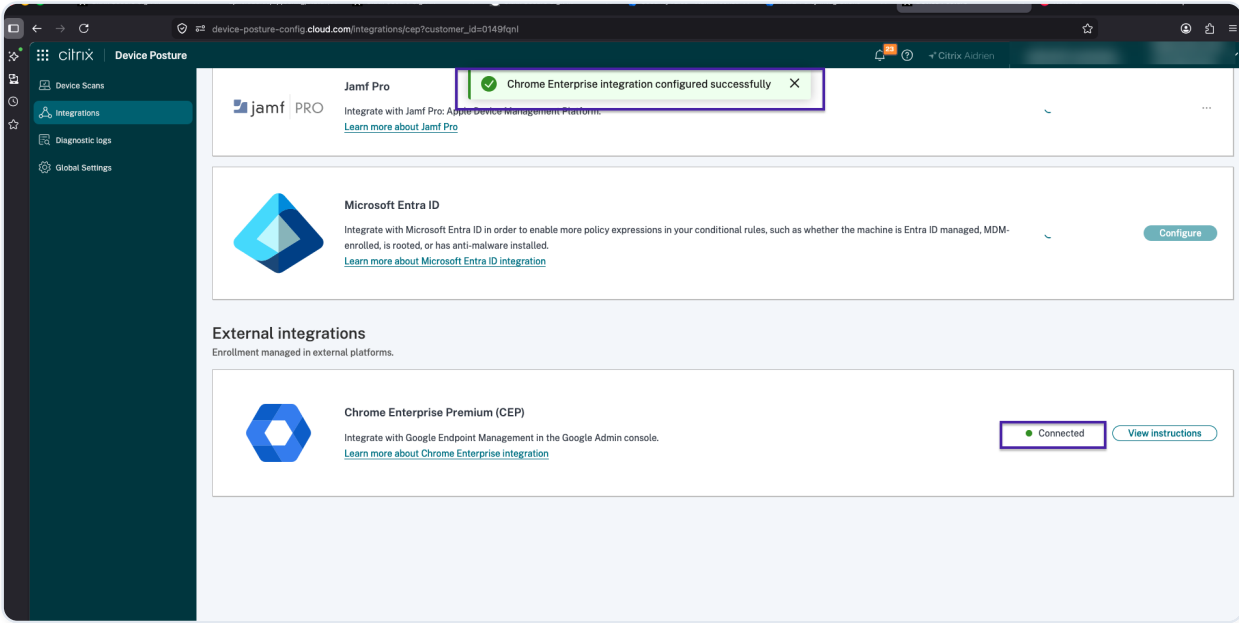
1. 以超级管理员身份登录 Google 管理控制台。
2. 导航到[设备 > 移动设备和端点 > 设置 > 第三方集成](#)。



3. 在合作伙伴列表中找到 **Citrix**，然后单击**管理**。
4. 按照屏幕上的提示授权您的 Citrix Cloud 租户与 Google Workspace 之间的连接。



握手成功后，Citrix 的集成状态将变为**已连接**。



有关详细信息，请参阅[设置第三方合作伙伴集成](#)。

为 Citrix 信号定义上下文感知规则

Google Workspace 中的上下文感知访问和 DLP 规则是使用通用表达式语言 (CEL) 编写的。Citrix 姿态数据在 `device.vendors["Citrix"].data[...]` 命名空间下公开。

有关详细信息，请参阅以下主题：

- [设置第三方合作伙伴集成](#)
- [将 DLP 规则与上下文感知访问条件结合](#)

Citrix 信号密钥

以下密钥由 Citrix 设备姿态服务发布到 Chrome 设备信任连接器：

密钥	描述	示例值
OVERALL_OUTCOME	设备姿态服务为端点返回的聚合姿态结果。	合规、不合规、拒绝
∧	∧	注意： 值区分大小写。请完全按照上面列出的内容输入。
OVERALL_OUTCOME_CON TEXT_NAME	驱动整体结果的设备姿态服务策略或上下文的名称。	AUTHORIZED_COUNTRY, AV_STATUS, OS_VERSION, Google-DTC-Demo-Deny, (自定义策略名称)

密钥	描述	示例值
思杰-设备ID	在 Citrix Device Posture 服务中注册的端点的唯一标识符。	6c813458-c27b-4299-87c6-55832a95ae7e
思杰-事务ID	生成信号的姿态评估事务的唯一标识符。	75b1e3f6-4224-484a-8c47-9a35c4e5eabd

注意：

- 确切的上下文名称取决于您在 [步骤 1](#) 中在 Device Posture 服务中定义的策略。
- Citrix-DeviceId 和 Citrix-TransactionId 是关联标识符。它们不用于策略决策。在 Citrix Device Posture 控制面板上进行故障排除时，可以使用它们来查找产生给定结果的确切扫描。

Citrix 的通用表达式语言 (CEL) 示例

示例 1 — 当 Citrix 报告不合规时阻止访问：

当 Citrix 总体结果为“不合规”时，拒绝访问 Google Workspace 应用。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

在上下文感知访问级别中使用此表达式，并将操作设置为“阻止”。

示例 2 — 仅当违规由未经授权的国家/地区引起时才阻止：

将结果与上下文名称结合，将规则范围限定为地理违规。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant" &&
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] ==
"AUTHORIZED_COUNTRY"
```

示例 3 — 仅当 Citrix 报告合规时才允许访问：

仅当设备姿态服务明确返回合规结果时才授予访问权限（故障关闭）。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant"
```

示例 4 — DLP：阻止不合规设备上的文件下载：

在 Google Drive 的 DLP 规则中，将以下条件附加到“下载/打印/复制”触发器，以阻止不合规端点的数据外泄：

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

示例 5 — 具有多个 Citrix 上下文的分层策略：

当姿态因防病毒或操作系统版本失败时阻止，但允许其他不合规原因由单独的、限制较少的规则处理。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant" &&  
( device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "AV_STATUS" ||  
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "OS_VERSION" )
```

示例 6 — 阻止来自指定设备姿态服务策略的明确拒绝结果：

匹配特定设备姿态服务策略产生的精确拒绝结果（例如，概念验证期间使用的 `Google-DTC-Demo-Deny` 策略）：

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Deny" &&  
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "Google-DTC-  
Demo-Deny"
```

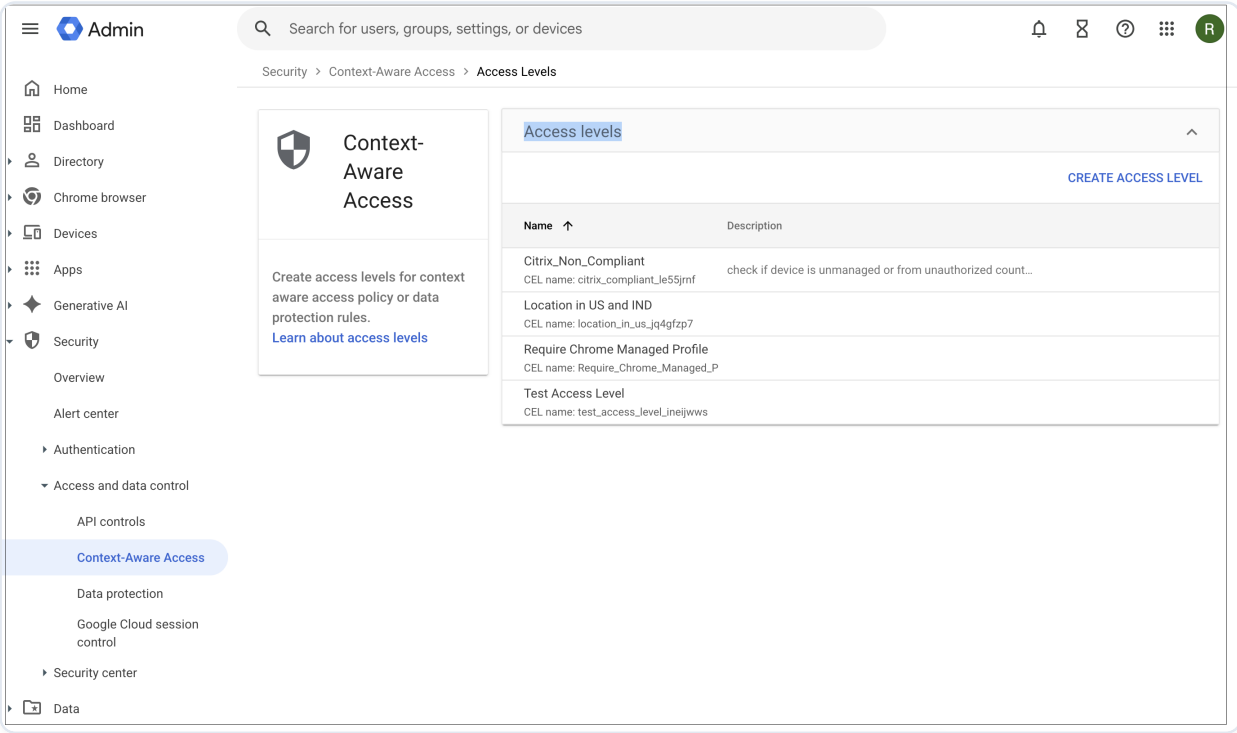
示例 7 — 将 Citrix 设备状态与 Google 原生信号结合：

Citrix 信号可以与内置的 Chrome / 端点验证属性结合使用。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant" &&  
device.encryption_status == ENCRYPTED && device.os_version.major >= 10
```

应用规则

1. 在 Google 管理控制台中，转到“安全 > 访问和数据控制 > 情境感知访问（或 DLP 的数据保护）”。
2. 创建“访问级别”（或“DLP 规则”），并将 CEL 表达式粘贴到“高级/条件”编辑器中。



3. 将访问级别分配给目标 Google Workspace 应用（例如 Drive、Gmail 等）以及相关的组织单位或群组。
4. 保存并推出。等待几分钟以完成传播。

验证集成

1. 从运行 CEP 的受管 Windows 端点，故意使设备状态服务扫描失败（例如，从未经授权的国家/地区登录或禁用防病毒软件）。
2. 尝试从该端点上的 Chrome 浏览器或配置文件访问受保护的 Google Workspace 应用。
3. 确认 Chrome 强制执行您的 CEL 规则定义的操作（阻止、警告或允许）。
4. 在“报告 > 审计和调查 > 访问透明度/规则日志事件”下查看审计日志，以确认 Citrix 信号已评估。

故障排除

症状	可能原因	解决方案
集成状态保持“未连接”	OAuth/管理员同意未完成	使用超级管理员帐户重新运行 步骤 2
规则不匹配	CEL 密钥名称拼写错误或设备姿态服务中未启用策略	在管理控制台规则日志事件中验证密钥。确认设备姿态服务中的策略处于活动状态

症状	可能原因	解决方案
端点上缺少信号	CEP 未安装或用户未登录	验证端点上的 CEP 部署和设备姿态服务注册
意外的不合规或拒绝	另一个设备姿态服务策略失败	检查 OVERALL_OUTCOME_CONTEXT_NAME 以识别失败的检查

注意：

如果您需要调查特定的访问决策，请从 Chrome / Workspace 审计日志中捕获 `Citrix-DeviceId` 和 `Citrix-TransactionId`，并在 Citrix Device Posture 控制面板上查找它们，以查看完整的扫描结果、策略命中和时间戳。

使用 Citrix-DeviceId 和 Citrix-TransactionId 进行故障排除

当 Chrome 访问或 DLP 决策需要调查时：

1. 打开 **Google 管理控制台 > 报告 > 审计和调查 > 规则日志事件（或访问透明度日志）** 并找到相关事件。
2. 复制事件负载中报告的 `Citrix-DeviceId` 和 `Citrix-TransactionId` 值。
3. 登录到 **Citrix Cloud > Device Posture > 控制面板**。
4. 按设备 ID 搜索以查看端点的注册、操作系统和最近的扫描历史记录。
5. 按事务 ID 搜索以查看确切的扫描实例 — 包括评估了哪些策略、收集了哪些信号以及发送到 Chrome 的最终 OVERALL_OUTCOME 和 OVERALL_OUTCOME_CONTEXT_NAME。

这种关联使您能够确认意外的 Chrome 决策是由 Citrix 姿态结果、CEL 表达式还是 Workspace 策略绑定引起的。

限制

每个主机最多可将 10 个 Google 资源 ID 从 Citrix Device Posture 服务推送到 Chrome 设备信任连接器。

要将设备姿态信号推送到每个主机超过 10 个 Google 资源 ID，请联系 Citrix 支持以请求扩展。

设备姿态服务第三方集成

除了设备姿态服务提供的本机扫描之外，设备姿态服务还可以与 Windows 和 macOS 上的以下第三方解决方案集成。

- [微软 Entra ID](#)
- [Jamf 专业版](#)
- [微软 Intune](#)
- [CrowdStrike](#)

Microsoft Entra ID 与设备姿态服务的集成

借助 Microsoft Entra ID 集成，Citrix® 支持统一的合规性工作流，该工作流在所有 Microsoft Entra ID 注册设备上保持一致，无论哪种移动设备管理 (MDM) 解决方案与 Microsoft Entra ID 集成。

系统要求

- 支持的平台：Windows
- 适用于 Windows 的支持的 EPA 客户端版本：26.3.1.10 或更高版本

微软 Entra ID API 权限

下表列出了用于与设备姿态服务集成的 Microsoft Entra ID API 权限。

API 名称	声明值	权限名称	类型
微软图形	Devices.Read.All	读取所有设备	应用程序
微软图形	User.Read	登录并读取用户配置 文件	委派

注意：

- 只有特权角色管理员和全局管理员才能授予应用程序权限。
- 虽然设备姿态服务仅需要应用程序权限来获取 Entra ID 设备详细信息，但初始管理员授权流程是由个人执行的交互式过程。
- Microsoft Entra ID 中默认包含的 `User.Read (Delegated)` 权限在授权流程中验证管理员的身份。这确保只有授权角色（全局管理员或特权角色管理员）才能授予设备姿态服务所需的应用程序级访问权限。

配置 Entra ID 集成

Entra ID 集成配置是一个两步过程。

1. 在 [Citrix Device Posture 服务](#) 和 [Microsoft Entra ID](#) 之间建立信任。这是一次性活动，用于在 Device Posture 和 Microsoft Entra ID 之间建立信任。
2. 配置策略以使用 [Microsoft Entra ID 合规性信息](#)。

在 Citrix Device Posture 服务和 Microsoft Entra ID 之间建立信任

执行以下步骤以在 Citrix Device Posture 服务和 Microsoft Entra ID 之间建立信任。

1. 登录 Citrix Cloud™，然后从菜单中选择 **Identity and Access Management**。
2. 单击“**Device Posture**”选项卡，然后单击“**Manage**”。
3. 单击“**Integrations**”选项卡。

Configure integrations from the available options below.



Microsoft Intune
Integrate with Microsoft Intune in order to enable more policy expressions in your conditional rules, such as whether the machine is Azure AD-managed, MDM-enrolled, is rooted, or has anti-malware installed.
[Learn more about Microsoft Intune integration](#)

● 2 accounts configured

Manage



CrowdStrike Falcon® Insight XDR
Integrate with CrowdStrike's Falcon Insight XDR: Endpoint Detection and Response (EDR) platform.
[Learn more about CrowdStrike Falcon® Insight XDR](#)

☐ Not Configured

Configure



Jamf Pro
Integrate with Jamf Pro: Apple Device Management Platform.
[Learn more about Jamf Pro](#)

☐ Not Configured

Configure



Microsoft Entra ID
Integrate with Microsoft Entra ID in order to enable more policy expressions in your conditional rules, such as whether the machine is Entra ID managed, MDM-enrolled, is rooted, or has anti-malware installed.
[Learn more about Microsoft Entra ID integration](#)

☐ Not Configured

Configure

注意：

或者，客户可以导航到 Secure Private Access 服务 GUI 左侧导航窗格中的“**Device Posture**”选项，然后单击“**Integrations**”选项卡。

- 单击 Microsoft Entra ID 框中的省略号按钮，然后单击“**Configure**”。此时将显示“**Microsoft Entra ID**”窗格。
- 输入配置文件名称，然后单击“**Connect account**”。
- 单击“**Done**”。

Microsoft Entra ID 部分显示成功配置的帐户数和存在问题的帐户数。要解决问题，请从“配置文件名称”下拉列表中选择受影响的配置文件，然后重新连接帐户。

为 Microsoft Entra ID 集成配置设备姿态策略

- 配置设备姿态策略。有关详细信息，请参阅[配置设备姿态策略](#)。
- 在**策略规则**中，选择 **Microsoft Entra ID**。
- 选择一个条件，然后选择要匹配的值。
 - **合规** - 检查设备是否符合 Microsoft Entra ID 中配置的合规性策略。
 - **受管** - 检查设备是否已在 Microsoft Entra ID 中注册。

注意：

您可以将此规则与为设备姿态配置的其他规则一起使用。

4. 完成策略配置，然后单击**创建**。

Jamf Pro 与设备姿态服务的集成

Jamf Pro 是一家 Apple 移动设备管理 (MDM) 软件和安全提供商，可帮助组织配置和保护其 Apple 设备。

重要提示：

- 适用于 macOS 版本 24.9.6 的 Citrix Secure Access 客户端支持 Jamf Pro 集成。
- 要使 Jamf Pro 与设备姿态集成在 iOS 设备上运行，管理员必须从 Jamf Pro 门户推送 Citrix Workspace™ 应用程序。有关详细信息，请参阅[从 Jamf Pro 门户推送 Citrix Workspace 应用程序](#)。

配置 Jamf Pro 集成

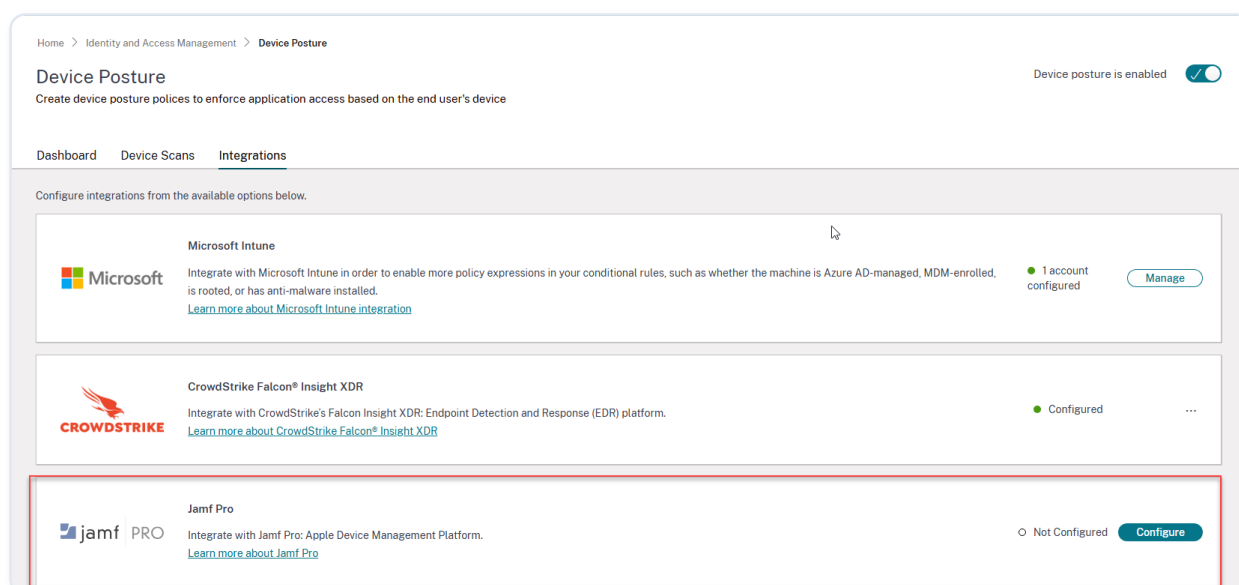
Jamf Pro 集成配置是一个两步过程。

1. 在 Citrix Device Posture 服务和 Jamf Pro 服务之间建立信任。
2. 配置策略以使用 Jamf Pro 信息。

在 Citrix Device Posture 服务和 Jamf Pro 服务之间建立信任

执行以下步骤以在 Citrix Device Posture 服务和 Jamf Pro 服务之间建立信任。

1. 登录 Citrix Cloud，然后从菜单中选择 **Identity and Access Management**。
2. 单击“**Device Posture**”选项卡，然后单击“**Manage**”。
3. 单击“**Integrations**”选项卡。

**注意：**

或者，客户可以导航到 Secure Private Access 服务 GUI 左侧导航窗格中的“**Device Posture**”选项，然后单击“**Integrations**”选项卡。

- 单击 Jamf Pro 框中的省略号按钮，然后单击“**Connect**”。此时将显示“**Configure Jamf Pro Integration**”窗格。
- 输入客户端 ID、客户端密钥和 Jamf Pro URL，然后单击“**Save**”。

注意：

- 您可以从 Jamf Pro 门户获取 API 客户端 ID。
- 确保您选择 **读取计算机** 和 **读取移动设备** 范围，并具有读取权限以建立信任。
- Jamf 为每个客户帐户提供 Jamf Pro URL。Jamf Pro URL 的格式为 `https://<organization name>.jamfcloud.com`。

当状态从 **未配置** 更改为 **已配置** 后，集成被视为成功。

如果集成不成功，状态将显示为 **待处理**。您必须单击省略号按钮，然后单击 **重新连接**。

为 Jamf Pro 集成配置设备姿态策略

- 配置设备姿态策略。有关详细信息，请参阅 [配置设备姿态策略](#)。
- 在 **策略规则** 中，选择 **Jamf Pro**。

3. 选择一个条件，然后选择要匹配的值。

- **自动注册** - 检查 Apple 设备是否在初始设置期间自动注册到 Jamf 系统。
- **已管理** - 检查设备是否由 Jamf Pro 管理。
- **上次联系时间** - 仅适用于 macOS。检查设备上上次与 Jamf Pro 服务器通信以来的时间（以分钟为单位）。
- **上次清单更新时间** - 仅适用于 iOS。检查设备上上次与 Jamf Pro 通信以更新其清单数据以来的时间（以分钟为单位）。

4. 单击 + 以添加其他限定符。

注意：

您可以将此规则与为设备姿态配置的其他规则一起使用。

5. 完成策略配置，然后点击**创建**。

将 Citrix Workspace 应用程序从 Jamf Pro 门户推送到 iOS 设备

为了支持 Jamf Pro 与 iOS 设备上的设备姿态集成，管理员必须将 Citrix Workspace 应用程序从 Jamf Pro 门户推送到 iOS 设备。执行以下步骤：

1. 登录到您的 Jamf Pro MDM。
2. 添加您要管理的 Citrix Workspace 应用程序。
3. 在 App Store 中链接该应用程序。
4. 为该应用程序创建应用程序配置策略。
5. 将以下 XML 添加到应用程序配置中。

```
<dict>

<key>UDID</key>

<string>$UDID</string>
```

</dict>

Microsoft Intune 与设备姿态服务的集成

Microsoft Intune 根据其策略配置将用户的设备分类为合规或已注册。在用户登录 Citrix Workspace 期间，设备姿态可以向 Microsoft Intune 查询用户的设备状态，并使用此信息将 Citrix Cloud 中的设备分类为合规、不合规（部分访问）甚至拒绝访问用户登录页面。Citrix DaaS™ 和 Citrix Secure Private Access™ 等服务反过来利用设备姿态对设备的分类，分别为虚拟应用程序和桌面以及 SaaS 和 Web 应用程序提供上下文访问（智能访问）。

多个 Microsoft Intune 帐户与设备姿态的集成

设备姿态服务支持最多集成五个 Microsoft Intune 帐户。这使得拥有多个 Intune 租户（通常是合并、收购或部门细分的结果）的组织能够在其所有环境中无缝管理设备姿态。

将多个 Intune 帐户与设备姿态服务集成的一些主要优势包括：

- 集中式设备姿态管理：从单个设备姿态控制台管理多个 Intune 租户中设备的姿态。
- 简化管理：无需在不同的设备姿态实例之间切换，也无需为每个 Intune 帐户管理单独的配置。
- 改进的可视性：无论设备由哪个 Intune 租户管理，都能获得所有设备安全状况的整合视图。
- 增强的灵活性：支持拥有复杂 IT 环境和多个 Intune 部署的组织。

配置 Microsoft Intune 集成

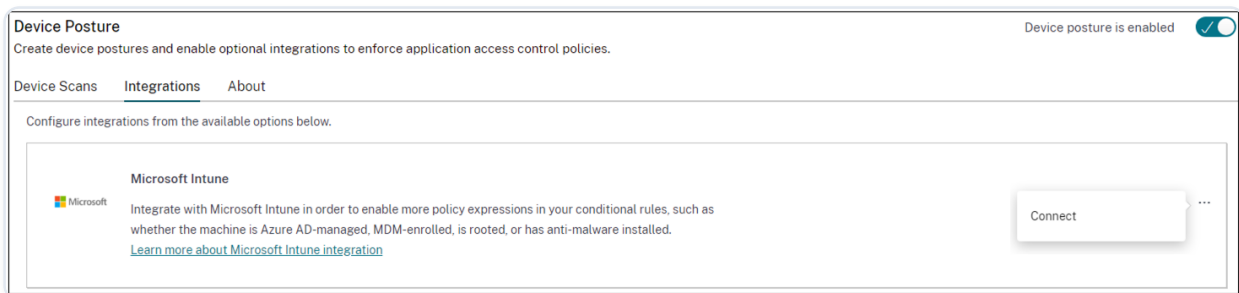
Intune 集成配置是一个两步过程。

1. 将设备姿态与 Microsoft Intune 服务集成。这是一次性活动，用于在设备姿态和 Microsoft Intune 之间建立信任。
2. 配置策略以使用 Microsoft Intune 信息。

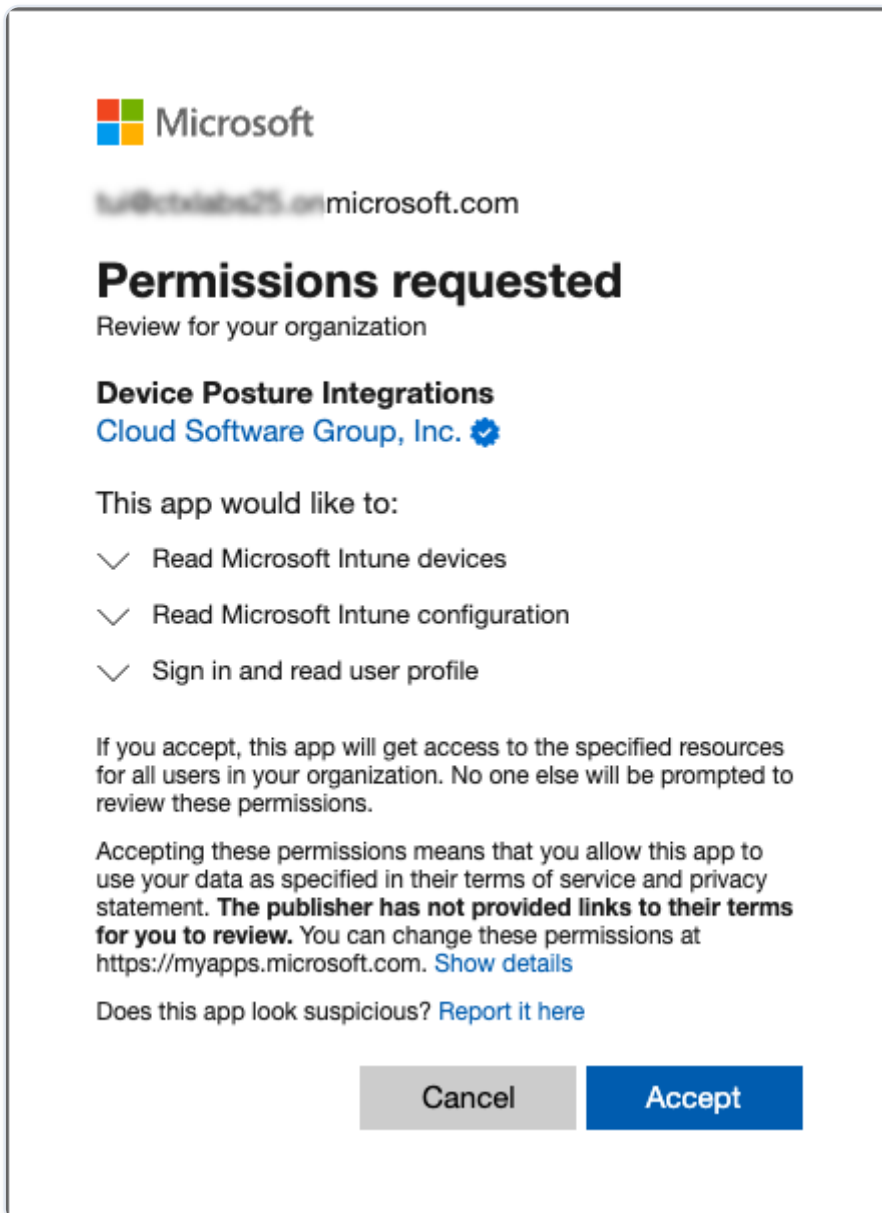
将设备姿态与 Microsoft Intune 集成

1. 要访问“集成”选项卡，请使用以下方法之一：

- 在浏览器中访问 URL `<https://device-posture-config.cloud.com>`，然后单击“集成”选项卡。
- Secure Private Access 客户 - 在 Secure Private Access GUI 的左侧导航窗格中，单击“设备姿态”，然后单击“集成”选项卡。



2. 单击“省略号”按钮，然后单击“连接”。管理员将被重定向到 Azure AD 进行身份验证。



将多个 Microsoft Intune 帐户与设备姿态集成

1. 在“集成”页面中，单击 Microsoft Intune 部分中的“管理”。
2. 在“配置文件名称”中，输入配置文件名称以连接到您的 Microsoft Intune 帐户。
3. 单击“连接帐户”。

Microsoft Intune

Create up to 5 Intune account profiles and connect to an account using your login credentials.

Profile name

Account2

Connect account

Account1

● Configured

Tenant ID xxxxxxxx-xxxx-xxxx-xxxx-e7fc8e4fe5f7

...

test

● Pending

Tenant ID N/A

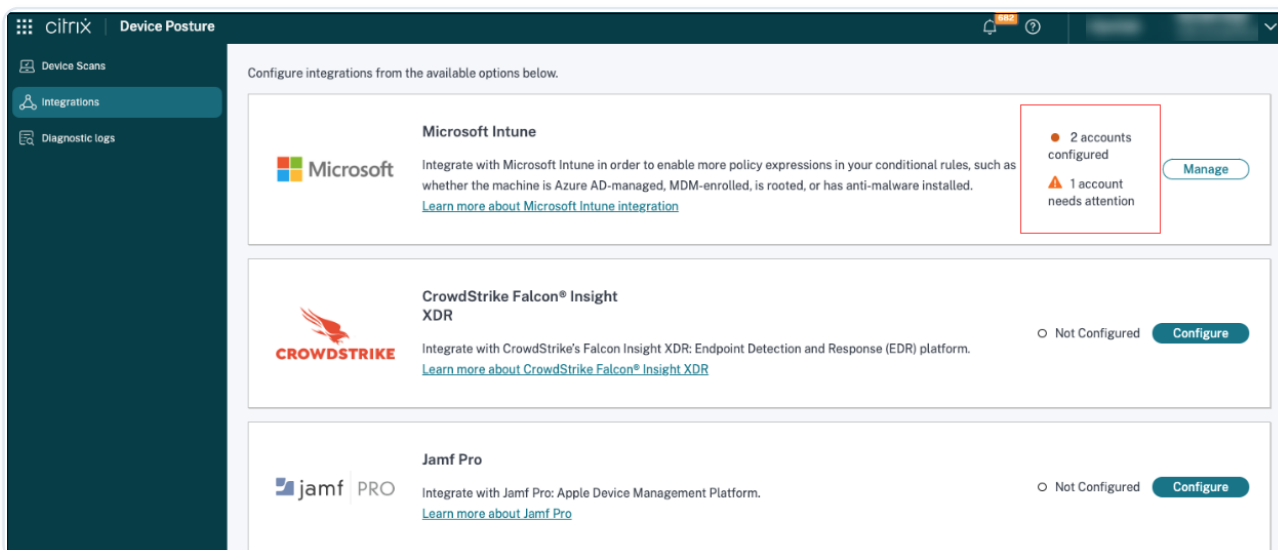
...

Done

连接建立后，状态显示为“已配置”，并显示与该帐户关联的租户 ID。

4. 单击“完成”。

Microsoft Intune 部分显示已成功配置的帐户数量以及存在问题的帐户数量。要解决问题，请从“配置文件名称”下拉列表中选择受影响的配置文件并重新连接帐户。



集成状态从“未配置”变为“已配置”后，管理员可以创建设备姿态策略。

如果集成不成功，状态显示为“待处理”。您必须单击“省略号”按钮，然后单击“重新连接”。

Microsoft Intune 应用程序接口权限

下表列出了用于与设备姿态服务集成的 Microsoft Intune API 权限。

API 名称	声明值	权限名称	类型
微软 Graph	DeviceManagement ManagedDevices.Read.All	读取 Microsoft Intune 设备	应用程序
微软 Graph	DeviceManagement ServiceConfig.Read.All	读取 Microsoft Intune 设备	应用程序
微软 Graph	User.Read	登录并读取用户配置文件	委派

注意：

- 只有特权角色管理员和全局管理员才能授予应用程序权限。
- 虽然设备姿态服务仅需要应用程序权限来获取 Entra ID 设备详细信息，但初始管理员授权流程是由个人执行的交互式过程。
- Microsoft Entra ID 中默认包含的 `User.Read (Delegated)` 权限在授予流程期间验证管理员的身份。这确保只有授权角色（全局管理员或特权角色管理员）才能授予设备姿态服务所需的应用程序级访问权限。

配置用于 Intune 集成的设备姿态策略

1. 配置设备姿态策略。有关详细信息，请参阅[配置设备姿态策略](#)。
2. 在策略规则中，选择**Microsoft Intune**。
3. 选择一个条件，然后选择要匹配的值。
 - **托管** - 表示设备已注册到 Intune。
 - **合规** - 表示设备符合 Intune 管理员在 Intune 管理中心设置的合规策略。

注意：

您可以将此规则与为设备姿态配置的其他规则一起使用。

4. 完成策略配置，然后单击**创建**。

CrowdStrike 与设备姿态服务的集成

CrowdStrike 零信任评估 (ZTA) 通过为每个终端设备计算 1 到 100 的 ZTA 安全分数来提供安全姿态评估。ZTA 分数越高，表示终端设备的姿态越好。

Citrix 设备姿态服务可以通过使用终端设备的 ZTA 分数，为 Citrix 桌面即服务 (DaaS) 和 Citrix 安全私有访问 (SPA) 资源启用上下文访问（智能访问）。

设备姿态管理员可以使用 ZTA 分数作为策略的一部分，并将终端设备分类为合规、不合规（部分访问）甚至拒绝访问。这种分类反过来可以被组织用于为虚拟应用和桌面以及 SaaS 和 Web 应用提供上下文访问（智能访问）。ZTA 分数策略支持 Windows 和 macOS 平台。

配置 CrowdStrike 集成

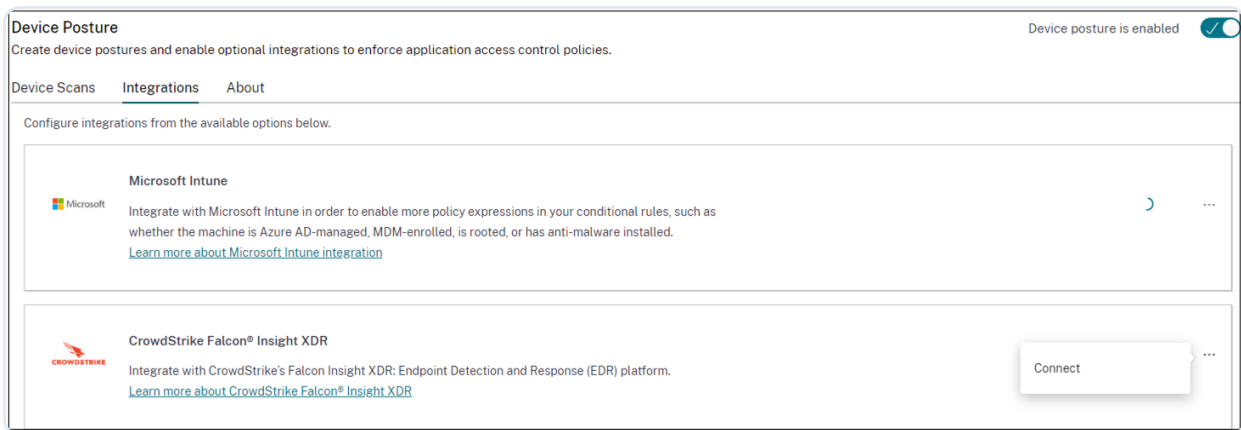
CrowdStrike 集成配置是一个两步过程。

1. 在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任(/zh-cn/device-posture/device-posture-third-party-integrations.html#establish-trust-between-citrix-device-posture-service-and-crowdstrike-zta-service)。这是一次性活动。
2. 配置访问策略(/zh-cn/device-posture/device-posture-third-party-integrations.html#configure-device-posture-policies-for-crowdstrike-integration)。访问策略使用 CrowdStrike ZTA 分数作为规则，为 Citrix DaaS 和 Citrix Secure Private Access 资源提供智能访问。

在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任

执行以下步骤以在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任。

1. 登录 Citrix Cloud，然后从汉堡菜单中选择 **Identity and Access Management**。
2. 单击“**Device Posture**”选项卡，然后单击“**Manage**”。
3. 单击“**Integrations**”选项卡。

**注意：**

或者，客户可以导航到 Secure Private Access 服务 GUI 左侧导航窗格中的“**Device Posture**”选项，然后单击“**Integrations**”选项卡。

- 单击 CrowdStrike 框中的省略号按钮，然后单击“**Connect**”。此时将显示 CrowdStrike Falcon Insight XDR 集成窗格。
- 输入客户端 ID 和客户端密钥，然后单击“**Save**”。

注意：

- 您可以从 CrowdStrike 门户（**Support and resources > API clients and keys**）获取 ZTA API 客户端 ID 和客户端密钥。
- 确保您选择具有读取权限的 **Zero Trust Assessment** 和 **Host** 范围以建立信任。

当状态从 **Not Configured** 变为 **Configured** 后，集成被视为成功。

如果集成不成功，状态将显示为 **Pending**。您必须单击省略号按钮，然后单击 **Reconnect**。

为 CrowdStrike 集成配置设备姿态策略

执行以下步骤来配置策略，以使用 CrowdStrike ZTA 分数作为规则，为 Citrix DaaS 和 Citrix Secure Private Access 资源提供智能访问。

- 配置设备姿态策略。有关详细信息，请参阅 [配置设备姿态策略](#)。
- 在 **Policy rules** 中，选择 **CrowdStrike**。
- 对于 **Risk Score** 限定符，选择条件，然后输入风险分数。
- 单击 **+** 以添加一个限定符，用于检查 CrowdStrike Falcon 传感器是否正在运行。

注意：

您可以将此规则与为设备姿态配置的其他规则一起使用。

5. 完成策略配置，然后单击 **Create**。

第三方集成失败通知

Device Posture 服务与 Microsoft Intune、CrowdStrike 和 Jamf Pro 等第三方解决方案集成。这些第三方云服务的停机或错误可能导致意外的设备姿态扫描结果。此功能在发生第三方集成失败时向管理员提供电子邮件通知。这些错误也会显示在 Secure Private Access 和 Device Posture 服务控制面板中。这允许客户直接联系第三方服务支持，提供相关的错误信息，从而绕过 Citrix 支持并减少停机时间。

用例

考虑一个客户，他已配置 CrowdStrike 扫描以将设备标记为合规。否则，设备将被标记为不合规。

如果发生 CrowdStrike 中断，Citrix Device Posture 服务无法联系 CrowdStrike 以检索设备合规性详细信息。结果是，最终用户设备会自动标记为不合规。

当此故障发生时，客户会收到电子邮件通知，并可以在 Device Posture 和 Secure Private Access 诊断控制面板中查看详细的错误信息。这种可见性使客户能够直接联系第三方支持团队解决问题，从而减少停机时间。

下图显示了一个示例电子邮件通知：

示例集成通知电子邮件(/en-us/device-posture/media/dps-integration-failure-email.png)

下图显示了控制面板上的通知：

控制面板中的示例集成通知失败(/en-us/device-posture/media/dps-integration-failure-on-dashboard.png)

先决条件

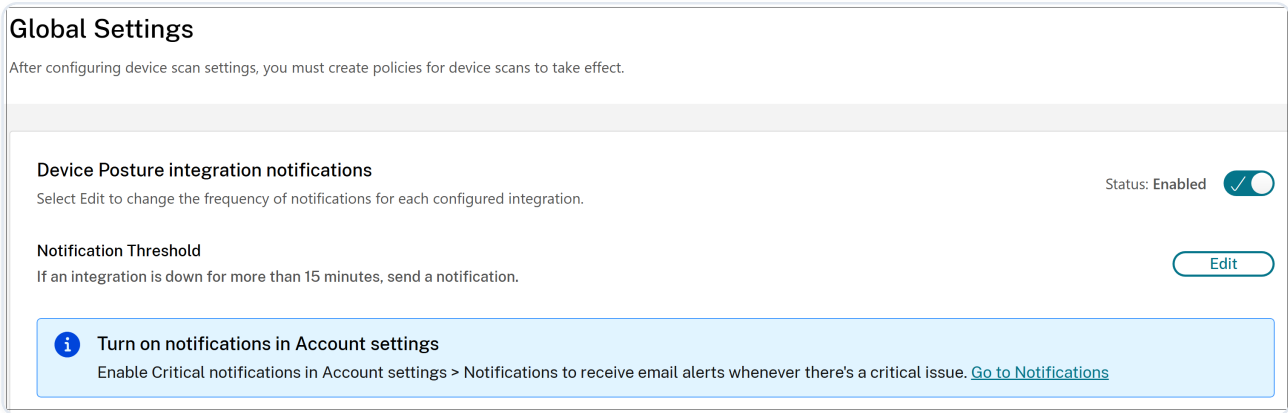
Citrix 管理员必须在 Citrix **帐户设置 > 通知**页面中启用以下功能，然后单击**应用**。

- 将**通过电子邮件通知我**切换开关设置为“开”。
- 选择**关键**通知设置。

通知切换开关(/en-us/device-posture/media/dps-integration-failure-email-setting.png)

在设备姿态服务管理控制台中配置通知

1. 导航到全局设置。
2. 在设备姿态集成通知框中，将切换开关启用为“开”。



默认情况下，如果集成中断，则会在 15 分钟后发送通知。您可以根据需要自定义通知频率。

要更改频率，请单击**编辑**，选择所需的频率，然后单击**保存**。

最终用户流程

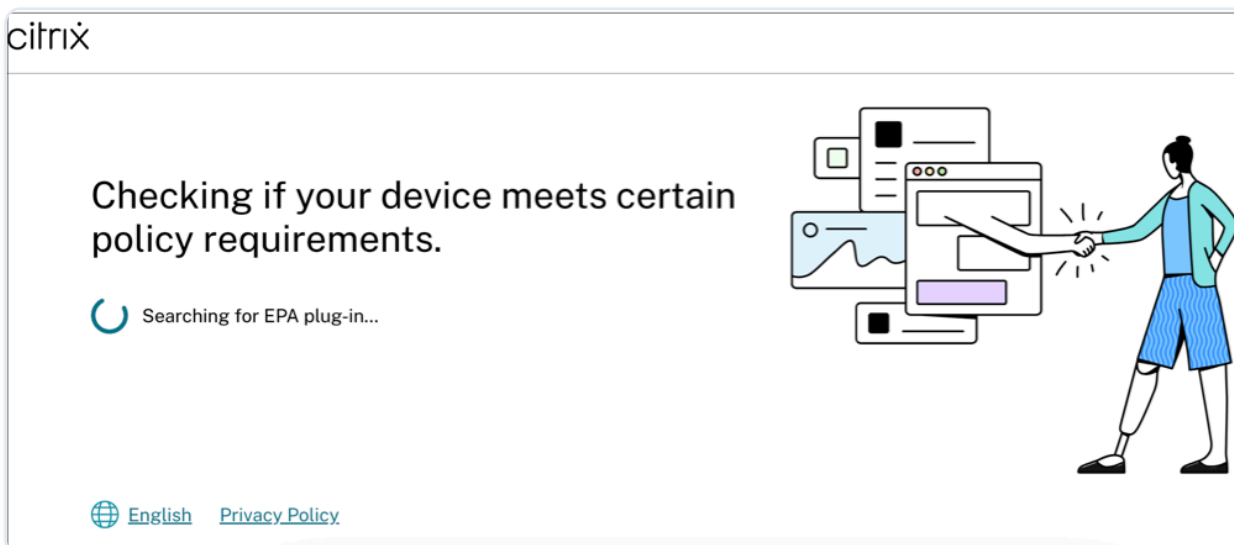
设置设备姿态策略并启用设备姿态后，以下是根据最终用户登录 Citrix Workspace 的方式而定的最终用户流程。

通过浏览器访问的最终用户流程

注意：

macOS 客户端和 Chrome 浏览器用作示例进行说明。屏幕和通知因您用于访问 Citrix Workspace URL 的客户端和浏览器而异。

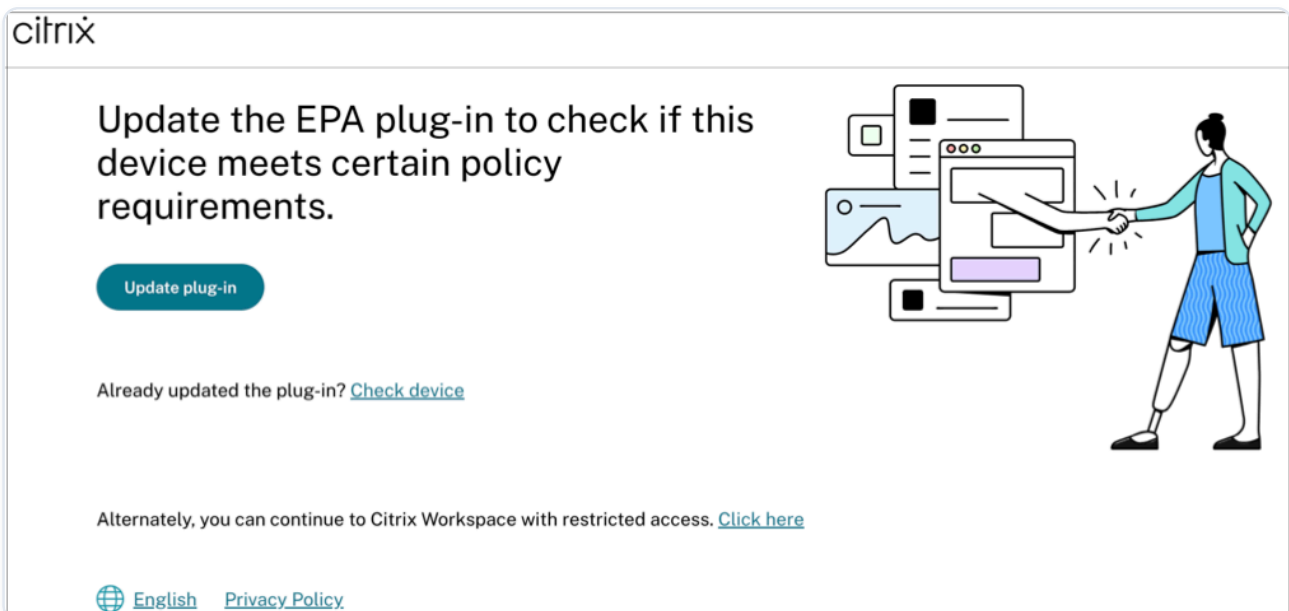
- 当最终用户通过浏览器登录到 Citrix Workspace URL `https://<your-workspace-URL>` 时，系统会提示最终用户运行 Citrix EndPointAnalysis 应用程序。



- 当最终用户单击“打开 Citrix End Point Analysis”时，设备姿态客户端将运行并根据设备姿态策略要求扫描端点参数。
- 如果设备上未安装设备姿态客户端，用户将被重定向到显示“下载插件”选项的页面。如果端点上已安装最新设备姿态客户端，用户必须单击“检查设备”以确认。同样，如果设备上安装的 EPA 不是最新版本，用户将被重定向到显示“更新插件”选项的页面。如果 EPA 客户端已更新，则用户必须单击“检查设备”以确认。



在这两种情况下，如果启用了跳过检查功能，则在“**下载插件**”或“**更新插件**”页面上会显示消息 或者，您可以继续访问 Citrix Workspace，但访问受限。



通过 Citrix Workspace 应用程序的最终用户流程

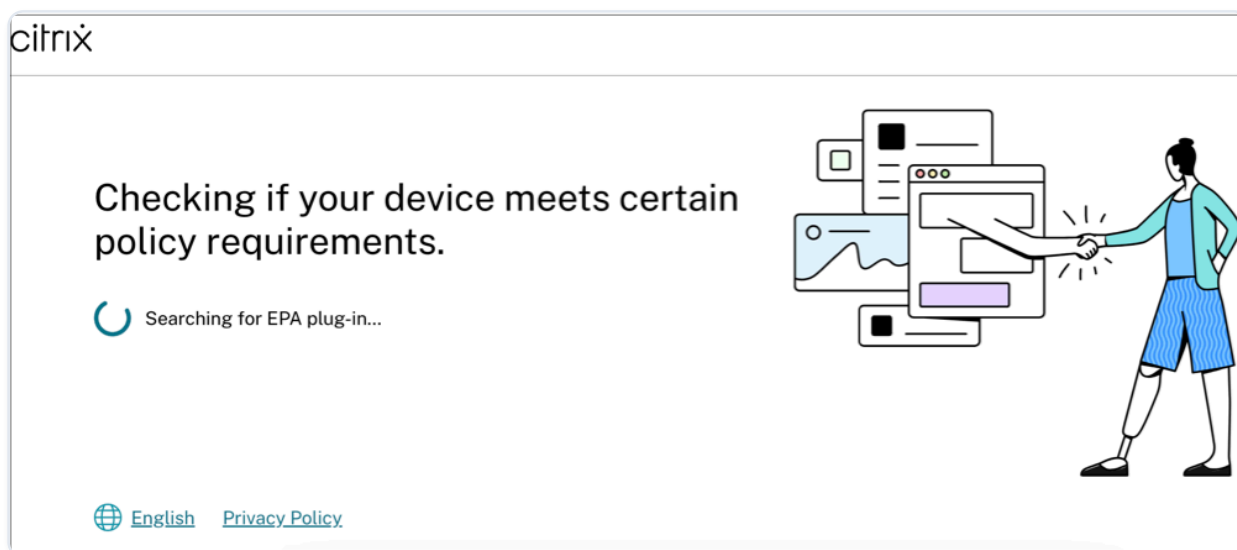
- 当最终用户通过 Citrix Workspace 应用程序登录到 Citrix Workspace URL `https://your-workspace-url` 时，安装在端点上的设备姿态客户端将运行并根据设备姿态策略要求扫描端点参数。
- 如果端点上未安装最新设备姿态客户端，用户将被重定向到显示“**再次检查**”和“**下载客户端**”选项的页面。用户必须单击“**下载客户端**”。
- 如果最新的设备姿态客户端已安装在端点上，用户必须单击 **再次检查**。

最终用户流程 - 设备姿态结果

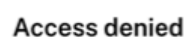
根据设备姿态策略条件，可能会出现三种情况。

如果端点满足策略条件，使得设备被归类为；

- **合规** - 最终用户被允许登录，并对 Secure Private Access 或 Citrix DaaS 资源拥有无限制访问权限。
- **不合规** - 最终用户被允许登录，但对 Secure Private Access 或 Citrix DaaS 资源拥有受限访问权限。



如果端点满足策略条件，使得设备被归类为 **拒绝访问**，则会显示 **访问被拒绝** 消息。



Check device again

 [English](#) [Privacy Policy](#)

设备姿态服务测试模式

设备姿态服务也提供测试模式，管理员可以在生产环境中启用设备姿态服务之前对其进行测试。这使管理员能够分析设备姿态扫描对最终用户设备的影响，然后相应地规划其操作方案，再在生产环境中启用它。测试模式下的设备姿态服务会收集最终用户设备的数据，并将设备分为合规、不合规和拒绝这三类。但是，此分类不会对最终用户设备强制执行任何操作。相反，它使管理员能够评估其环境并增强安全性。管理员可以在设备姿态控制板上查看此数据。如有必要，管理员还可以禁用测试模式。

注意：

必须在设备上安装 EPA 客户端。如果最终设备未安装 EPA 客户端，设备姿态服务会向最终用户显示一个下载页面，供其下载并安装客户端，否则最终用户无法登录。

启用测试模式

1. 登录 Citrix Cloud™，然后从汉堡菜单中选择**身份和访问管理**。
2. 单击**设备姿态**选项卡，然后单击**管理**。
3. 打开**设备姿态已禁用**切换开关。
4. 在确认窗口中，选中这两个复选框。

启用测试模式(/en-us/device-posture/media/dp-enable-test-mode.png)

5. 单击**确认并启用**。

当设备姿态服务在测试模式下启用时，设备姿态主页会显示一条说明以确认此情况。

测试模式(/en-us/device-posture/media/dp-enable-test-mode-banner.png)

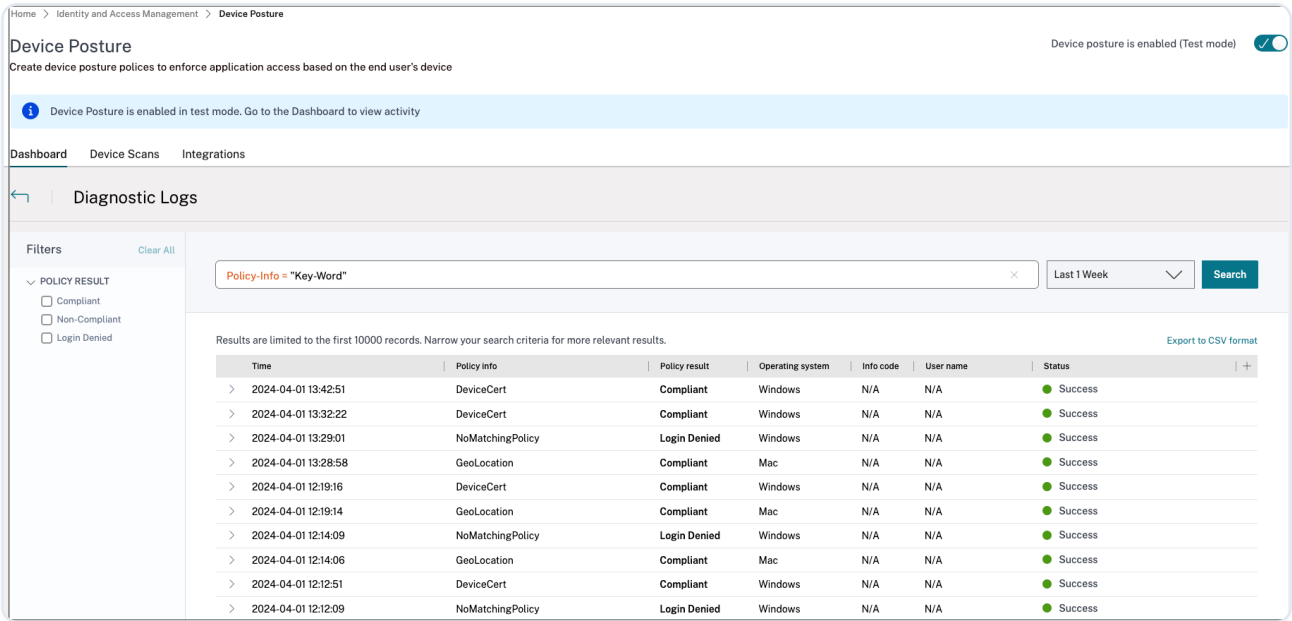
管理员可以配置设备姿态扫描的策略和规则。有关详细信息，请参阅配置设备姿态。根据扫描结果，最终用户设备被分类为合规、不合规和拒绝。管理员可以在控制板上查看此数据。

在控制板上查看测试模式活动

1. 在设备姿态页面上，单击**仪表盘**选项卡。

诊断日志图表显示被分类为合规、不合规和登录被拒绝的设备数量。

2. 要查看详细信息，点击[查看更多](#)链接。



管理员可以从用户界面下载监控日志。

在生产环境中启用测试模式

如果设备姿态服务已在生产环境中启用，请执行以下步骤以后启用测试模式：

1. 在主页上，将设备姿态已启用切换开关滑动到关闭。
2. 选择我理解所有设备姿态检查都将被禁用。
3. 点击确认并禁用。
4. 现在，通过将设备姿态已禁用切换开关滑动到开后来启用设备姿态。
5. 在确认窗口中，选择以下两个选项。
 - 在测试模式下启用设备姿态
 - 我理解对订阅者体验的影响
6. 点击确认并启用。

从测试模式过渡到生产模式

要从测试模式过渡到生产模式，您必须首先在测试模式中禁用设备姿态，然后再次启用设备姿态，但不选择 在测试模式下启用设备姿态 选项。

重要提示：

- 在从测试模式过渡到生产模式之前，务必彻底审查您的策略。在测试模式中设置的策略在生产环境中强制执行时可能会有不同的行为，这可能会影响用户访问，特别是 **拒绝访问**。在测试模式中，**拒绝访问** 实际上被视为 **不合规**，允许用户继续访问系统而不会中断。然而，在生产环境中，此结果会直接阻止访问，可能会影响用户体验和操作。
- 此外，从测试模式过渡到生产模式时，可能会出现潜在的停机时间。建议您仔细规划过渡，以最大程度地减少中断。

通过设置最低支持版本来管理 Citrix Secure Access Endpoint Analysis (EPA) 客户端版本

注意：

在本主题中，EPA 指的是 Citrix Secure Access Endpoint Analysis 客户端。这两个术语可互换使用。

管理员可以通过设备姿态服务，通过维护最低支持的 EPA 版本来管理 Citrix Secure Access Endpoint Analysis (EPA) 客户端版本。

以前，设备姿态服务要求所有端点使用单一固定的 EPA 客户端版本。

优点：

通过设备姿态服务解决方案进行 EPA 客户端版本管理具有以下优点：

- 简化版本控制
- 降低支持开销
- 确保端点符合设备姿态服务要求

工作原理

设备姿态服务会根据设备姿态管理控制台中特定于平台的设置，提示用户安装或升级客户端版本。

- **最低支持版本：** 当管理员设置最低支持版本时，设备姿态服务的行为如下：

客户端设备	设备姿态服务行为
未安装客户端的设备	系统会提示用户安装最新的 EPA 客户端。
客户端版本低于最低版本的设备	门户提供下载选项。最终用户手动安装或升级客户端。请使用管理员权限安装。否则，安装

客户端设备	设备姿态服务行为
	将在用户模式下运行，并且某些功能可能不可用。
版本等于或高于最低版本的设备	无更改。

- **始终使用最新版本：**当管理员设置“始终使用最新版本”选项时，所有端点都将运行最新可用的 EPA 客户端版本。

如果未安装 EPA 客户端或客户端已过时，设备状态服务将按如下方式运行：

客户端设备	设备状态服务行为
未安装客户端的设备	系统会提示用户安装最新的 EPA 客户端。
版本较旧的设备	门户提供下载选项。最终用户手动安装或升级客户端。请使用管理员权限安装。否则，安装将在用户模式下运行，并且某些功能可能不可用。

示例：

请考虑以下针对特定平台的示例，其中最低支持版本为 24.8，最新版本为 25.8。

下表总结了根据管理控制台中配置的设置，设备状态服务的行为：

客户端设备	最低支持版本选择为 24.8	始终使用最新版本
未安装 EPA 客户端	提示安装最新的 EPA 客户端。	提示安装最新的 EPA 客户端。
EPA 版本 < 24.8	提示升级到最新版本	提示升级到最新版本
EPA 版本 ≥ 24.8（但不是最新版本）	保持不变	提示升级到最新版本
EPA 版本 == 最新版本	保持不变	保持不变

注意：

当设备姿态服务引入需要更新 EPA 客户端的新功能时，管理员必须修改最低支持版本，以确保兼容性和最佳功能。

设置 EPA 客户端版本管理选项

1. 导航到 **设备姿态 > 设备扫描**，然后单击 **设置**。
2. 启用 EPA 客户端最低版本切换开关，然后单击 **编辑**。
3. 对于每个平台，选择以下客户端版本管理选项之一：

- 始终使用最新版本
- 列出的最低版本（例如，Windows 为 24.8.1.19）

4. 单击 **保存**。

Endpoint Analysis (EPA) client minimum version

SaveCancel

Select the minimum version of the EPA client that is required to be installed on endpoint devices.

☒ Enable EPA client minimum version check

Platform	Select Minimum Version	
Linux	Always use latest version	View Support Matrix
Mac	25.9.16	View Support Matrix
Windows	25.10.1.10	View Support Matrix

On mobile devices, the EPA client version is inherited from Citrix Workspace app.

重要提示：

- EPA 客户端版本管理支持下拉列表中列出的版本。我们建议您的最终用户使用这些版本或更高版本。下拉菜单中未列出的任何版本均不建议用于生产环境。
- 有关最新的客户端版本，请参阅 [Citrix Endpoint Analysis](#)。

EPA 客户端分发和版本管理注意事项

关于 EPA 客户端分发和版本管理，请考虑以下几点：

- **分发策略：** 使用标准端点管理工具（例如，适用于 Windows 的 SCCM、适用于 macOS 的 Jamf）来部署或修补 EPA 客户端。
- **标准化推出：** 通过设置与部署计划一致的最低支持版本来逐步推出客户端更新。
- **即时功能推出：** 确保启用“始终使用最新版本”设置，以便所有用户在发布时都能收到最新的 EPA 版本。
- **兼容性保证：** 每当发布新的设备姿态服务相关功能时，更新最低支持版本，以避免出现不受支持的客户端版本。

多云商店支持

管理员可以将不同的设备姿态策略应用于不同的云商店，从而提供精细控制并简化安全管理。

以前，设备姿态服务是在所有云商店中全局启用的，这阻止了管理员根据每个 URL 应用特定要求。

借助多商店支持，您现在可以执行以下操作：

- 为特定商店应用不同的设备姿态检查。
- 根据用户访问的商店强制执行不同级别的设备合规性。
- 在部署到商店之前，在测试商店上创建和测试设备姿态检查。

重要注意事项

在为每个商店实施不同规则之前，请注意以下事项：

- 多工作区 URL 支持不适用于 Chrome Extension Premium (CEP)。
- 多工作区 URL 不支持 NetScaler Gateway URL。
- 当您切换到多工作区模式时，现有的设备姿态配置将为每个工作区 URL 克隆。
- 现有客户可以设置一个测试 URL，然后为设备姿态服务启用多工作区 URL 支持。他们可以在测试 URL 上试用更改，同时保持设备姿态服务在其生产 URL 上处于活动状态。这种方法允许您验证姿态检查中的更改，而不会干扰更广泛的用户群。

注意：

设备姿态服务在多工作区部署中的服务连续性从 Delivery Controller™ (DDC) 26.03 版开始支持。

先决条件

- 支持的平台：Windows、macOS 和 iOS
- 以下 EPA 客户端支持多工作区 URL：
 - Windows：版本 25.7.1.11 及更高版本。[下载链接](#)。

- macOS：版本 25.11.19 及更高版本。[下载链接](#)。
- iOS：Citrix Workspace 应用程序 (CWA) 25.5.0 及更高版本（从 App Store 安装）。

注意：

- 从运行 Windows、macOS 或 iOS 以外平台的设备访问的用户被视为使用不受支持的设备，并遵循管理员在设备状态服务控制台中配置的默认行为。这仅在配置了[跳过检查](#)时适用。否则，系统会提示用户下载最新客户端。
- 不受支持平台上的设备默认标记为**不合规**。
- 您可以通过设备状态页面上的**设置**选项卡，将分类从**不合规**更改为**拒绝登录**。
- 有关“合规”和“不合规”的定义，请参阅“定义”。
- 端点上的 EPA 客户端必须使用先决条件部分中指定的版本。如果客户端使用旧版本，设备扫描将无法启动。对于 Windows 管理员，此要求已简化，因为 EPA 客户端与 Citrix Secure Access™ Client for Windows 2505 捆绑在一起。
- 您还可以跳过对不受支持设备的设备状态检查。有关详细信息，请参阅[跳过设备状态检查](#)。

配置应用商店 URL

1. 确保通过 **StoreFront Cloud > 访问**配置了工作区 URL。

配置工作区 URL(/en-us/device-posture/media/dps-workspace-access-urls.png)

2. 要访问设备姿态，请登录到 Citrix Cloud™ 并导航到设备姿态导航栏中的**身份和访问管理 > 设备姿态 > 全局设置**。

全局设置(/en-us/device-posture/media/dps-global-setting-multi-store-url.png)

3. 单击**配置设备姿态**，然后单击**设置**。
4. 选择**为每个工作区 URL 使用不同的设备扫描**。
5. 要修改设备姿态首选项，请单击**更改**。

修改设备姿态首选项(/en-us/device-posture/media/dps-change-scan-preference.png)

注意：

- 当为每个工作区 URL 使用不同的设备扫描选项启用时，您必须为每个工作区 URL 单独配置新的扫描。
- 配置新扫描后，系统会提示用户在 1-2 小时内重新进行身份验证，以确保使用新配置评估其登录会话。

将设备姿态用户事件导出到 SIEM 系统

设备姿态服务事件会导出到安全信息和事件管理 (SIEM) 系统。这使您可以在 SIEM 中查看与设备姿态服务相关的以下用户事件：

- 与设备姿态服务相关的所有事件类型。
- 设备姿态评估事件，提供有关根据已定义策略评估设备姿态的信息。

将事件导出到 SIEM 系统的好处如下：

- 使您的安全运营团队能够关联、分析和搜索来自不同日志的数据。
- 帮助您的安全运营团队识别并快速补救安全风险。
- 在一个集中位置查看安全警报。
- 集中式方法来检测潜在的安全威胁，以实现组织风险分析功能，例如风险指标、用户配置文件和风险评分。
- 能够将用户帐户的 Citrix Analytics 风险情报信息与 SIEM 中连接的外部数据源进行组合和关联。

有关详细信息，请参阅以下主题：

- [设备姿态服务事件](#)
- [诊断设备姿态服务事件故障](#)
- [安全信息和事件管理 \(SIEM\) 集成](#)

使用 DaaS Monitor 排除设备姿态问题

您可以使用为用户通过 Secure Private Access 或 DaaS 连接时为每个会话生成的事务 ID，在 DaaS Monitor 中排除设备姿态问题/错误。找到事务 ID 后，DaaS Monitor 会显示有关会话以及已应用的关联设备姿态策略的信息。Monitor 还会显示策略结果，包括设备是否通过了姿态检查。

Citrix DaaS™ Monitor 上的设备姿态事件

执行以下步骤以查看设备姿态服务的事件日志。

1. 从最终用户设备复制失败或拒绝访问的会话的事务 ID。
2. 登录 Citrix Cloud。
3. 在 DaaS 磁贴上，单击“管理”，然后单击“Monitor”选项卡。在 Monitor UI 中，搜索 32 位事务 ID，然后单击“详细信息”。

The screenshot displays the Citrix DaaS Monitor interface. On the left is a navigation sidebar with options like Dashboard, Trends, Filters, Alerts, Applications, Probes, Cost optimization, Infrastructure, Integrations and data exports, Analytics, Settings, and Secure Private Access. The main content area is titled 'DaaS > Monitor'. It shows a transaction summary for a specific Transaction ID, indicating a 'Success' status at 11/18/2024 8:04 PM for an endpoint named 'windows'. The summary notes that all device policy conditions were met. To the right, a 'Verify configured policies' section details three policies: 'CWA_OS_MeM_Check' (ID 3, Passed), 'MicrosoftEndpointManager' (match-none, Not found), and 'OSVersion' (ID 11, True). Each policy entry shows its type, condition criteria, expected and actual values, and the final condition result.

有关详细信息，请参阅以下主题：

- 使用 Monitor 排除设备姿态服务策略和事务故障
- 查看设备姿态事件的 SIEM 数据导出格式

设备姿态日志和事件

管理员可以通过设备姿态仪表板监控设备合规性。他们可以查看所有已配置的设备姿态策略，这些策略定义了访问组织资源的端点的合规性要求。他们还可以查看所有设备的实时合规性状态，包括按以下类别划分的详细评估结果：

- **合规：** 满足所有指定安全要求和策略条件的设备。
- **不合规：** 未能满足一项或多项安全要求但可能仍具有有限访问权限的设备。
- **拒绝访问：** 存在重大安全风险并被阻止访问资源的设备。

您可以在 [Secure Private Access 仪表板](#) 和 [Identity and Access Management 控制台](#) 中的设备姿态仪表板 中查看设备姿态日志和事件。

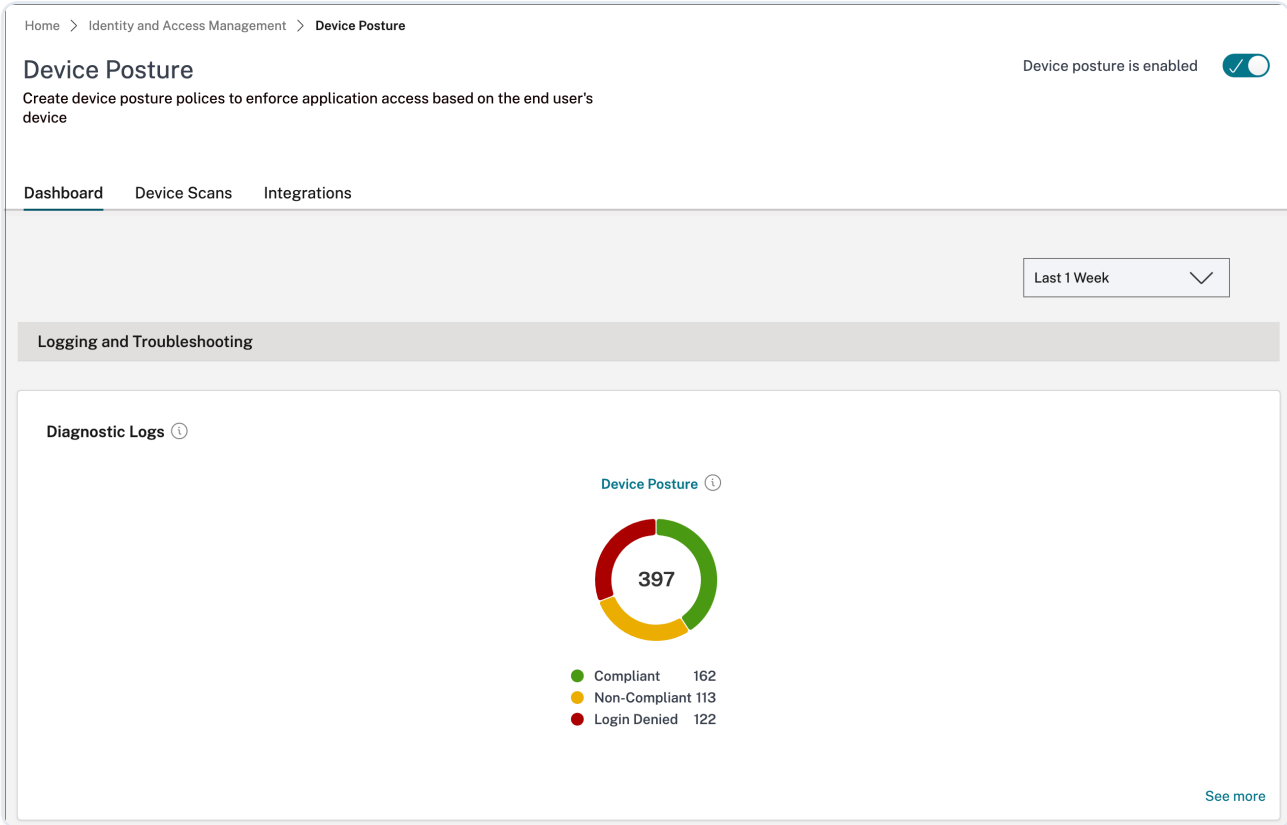
Identity and Access Management 控制台中的设备姿态仪表板

执行以下步骤以查看 Identity and Access Management 控制台中设备姿态仪表板的日志和事件。

1. 登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 **身份和访问管理**，
3. 单击 **Device Posture > Manage**，然后单击 **Dashboard**。

Logging and Troubleshooting（日志记录和故障排除）部分显示与设备姿态服务相关的诊断日志。

4. 单击**查看更多**链接以查看日志详细信息。您可以根据策略结果（**合规**、**不合规**和**登录被拒绝**）优化搜索。



您可以使用添加筛选器选项根据各种条件（例如策略信息、策略结果、操作系统、事务 ID、信息代码或设备 ID）优化搜索。例如，在搜索字段中，您可以单击 **Device-ID**，选择 **~ (包含某些值)**，然后输入 6273。将显示与包含 6273 的设备 ID 相关的所有日志。

点击每个日志条目旁边的展开图标，查看详细信息，例如扫描类型、客户端应用程序版本、客户端库版本和端点信息。

Diagnostic Logs

Last 1 Week Add filter

Results are limited to the first 10000 records. Narrow your search criteria for more relevant results. Export to CSV format

Time	Policy info	Policy result	Operating system	Info code	User name	Status
2025-10-07 15:20:11	Hard_Disk_Encryption_Scan_Windows	Compliant	Windows	N/A	spatext.corp\invernekar	Success

Time: 2025-10-07 15:20:11

Policy info: Hard_Disk_Encryption_Scan_Windows

Policy result: Compliant

Operating system: Windows

Transaction ID: d4441eff-ae9f-418e-bbfc-37f0148117c0

Public IP: 103.14.255.9

Info code: N/A

Description: N/A

Device ID: 52acfe3d-97c4-493b-81cd-a562556455c6

User name: spatext.corp\invernekar

Status: Success

ScanType: login

TestMode: false

SkipCheck: None

OriginDomainType: 0

ClientAppVersion: 24.8.1.19

ClientLibraryVersion: 25.6.1.2

Endpoint Information

Scan Configured	Endpoint Evidence
scanResultExpiryTime	2025-10-07T13:50:11Z
scanTime	2025-10-07T09:50:11Z
HD-ENC Microsoft Corporation BitLocker Drive Encryption VERSION	10.0.19041.1
HD-ENC Microsoft Corporation BitLocker Drive Encryption AUTHENTIC	true
HD-ENC Microsoft Corporation BitLocker Drive Encryption ENC-PATH	E:\-encrypted, C:\-unencrypted

注意：

- **ClientAppVersion** 和 **ClientLibraryVersion** 字段分别显示 EPA 客户端版本和库版本。
- 每当访问被拒绝时，事务 ID 也会显示给最终用户。
- 如果出现错误或扫描失败，设备姿态服务会显示一个事务 ID。此事务 ID 在 Secure Private Access 服务仪表板中可用。如果日志无法帮助解决问题，最终用户可以与 Citrix 支持部门共享事务 ID 以解决问题。

日志位置

Windows 客户端日志位于：

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

macOS 客户端日志位于：

- ~/Library/Application Support/Citrix/EPAPugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPugin/epapugin.log

安全私有访问仪表板

执行以下步骤以查看设备姿态服务的日志和事件。

1. 登录 Citrix Cloud。
2. 在 Secure Private Access 磁贴上，单击**管理**，然后单击**控制板**。

“**日志记录和故障排除**”部分显示与设备姿态服务相关的诊断日志。

3. 单击**查看更多**链接以查看日志详细信息。您可以根据策略结果（**合规**、**不合规**和**登录被拒绝**）优化搜索。

Secure Private Access > Dashboard > Diagnostic Logs

Diagnostic Logs 1947 Device Posture Logs 208

Last 1 Week + Add filter

Results are limited to 1000 rows. Export to CSV format

Device-ID ~ (contains some val... 6273

Apply Cancel Clear filters

Time	Device ID	User name	Status
> 2025-06-23 14...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows
> 2025-06-23 13...	NoMatchingPo...	Non-Compliant	Windows

设备姿态错误日志

可以在 Citrix Monitor 和 Secure Private Access 控制板上查看与设备姿态服务相关的以下日志。对于所有这些日志，建议您联系 Citrix 支持部门以获取解决方案。

- 未能读取已配置的策略
- 未能评估端点扫描
- 未能处理策略/表达式
- 未能保存端点详细信息
- 未能处理来自端点的扫描结果

设备姿态数据导出

设备姿态服务事件（例如设备姿态结果和事件类型）可以导出到安全信息和事件管理 (SIEM) 服务。当 Citrix Endpoint Analysis (EPA) 客户端对尝试访问 Citrix Virtual Apps and Desktops™ 或 Citrix Secure Private Access 资源的设备执行姿态检查时，会生成这些事件。

- 要了解如何设置、配置设备姿态服务日志并将其导出到 SIEM，请参阅[安全信息和事件管理 \(SIEM\) 集成](#)。
- 要详细了解可以从设备姿态服务导出的事件和日志，请参阅[设备姿态服务事件](#)。
- 要了解如何诊断和排查设备姿态服务事务，请参阅[诊断设备姿态服务事务](#)。

诊断设备姿态服务事务

管理员现在可以有效地诊断和排查设备姿态服务事务。此更新增强了 Citrix Monitor 中的故障排除功能，可提供有关设备姿态策略评估、合规性检查和错误诊断的详细见解。

了解设备姿态服务评估流程

典型的安全私有访问或 VDI 应用程序访问启动涉及以下三个阶段：

1. **预身份验证**：使用设备姿态服务执行基本的端点卫生检查。如果设备未能满足合规性策略，则在身份验证之前阻止访问。
2. **身份验证**：在此阶段对用户进行身份验证。如果存在凭据不匹配或身份提供程序错误，则身份验证失败。
3. **应用程序访问**：此阶段涉及以下两个子阶段：
 - **策略代理和枚举阶段**：当用户的设备上下文违反策略设置时，对应用程序的访问将受到限制。
 - **应用程序启动阶段**：最后一个阶段，应用程序事务使用 Citrix Enterprise Browser™、安全私有访问客户端或本机端点客户端完成。

Citrix Monitor 中的故障排除增强功能

通过此更新，Citrix Monitor 提供了基于搜索的设备姿态服务故障排除功能，使 IT 团队能够：

- 按用户 ID 或事务 ID 筛选事务，以进行有针对性的调试。
- 分析策略评估结果，例如设备是否合规、不合规或因策略违规而被阻止。
- 通过检查详细的合规性检查、预期值和实时上下文值来查明策略故障。
- 查看设备元数据、策略配置和日志，以进行更深入的诊断。
- 识别因系统错误导致的失败事务，错误消息链接到知识库文章以实现快速解决。

IT 团队如何使用故障排除增强功能

以下部分提供了有关故障排除问题的更多信息：

分类处理设备姿态问题

搜索用户报告的事务 ID，以快速定位相关的设备姿态服务日志。审查合规性检查是通过还是失败，并确定根本原因。

例如，在搜索事务 ID 时，您可以查看设备姿态检查策略的结果——无论是成功（合规或不合规）还是因错误而失败。系统提供设备姿态服务评估的完整上下文，包括客户端元数据、策略详细信息和其他事务详细信息。

DaaS > Monitor

Try unified search

Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427805

Product Documentation

Status: Success

Time: 11/13/2024 2:10 PM

User name: dps0929@citrix.com

Endpoint: windows

Transaction Summary

Details of the device policy where all conditions were met.

Policy name

CWACheckWithMonitorEvent

Evaluation result

Passed

Device Posture result

Compliant

Last scanned time

13 Nov 2024 at 2:10 PM

Verify configured policies

Details of each device policy for this transaction ID.

< Policy 3 of 4 >

Policy name

CWACheckWithMonitorEvent

ID

3

Evaluation result

Passed

Policy result

Compliant

Policy conditions

Type

CWAVersion

Condition criteria

>=

Expected value

10.0.0.0

Actual value

24.5.10.29

Condition result

True

调查基于策略的访问阻止

当设备不合规时，IT 部门可以检查失败的具体策略参数。系统提供配置的预期值与设备的实时数据的并排比较。

DaaS > Monitor

Try unified search

Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427783

Product Documentation

Status: Success

Time: 11/13/2024 1:26 PM

User name: dps0924@citrix.com

Endpoint: windows

Transaction Summary

Details of the device policy where all conditions were met.

Policy name

CWAVersion_Mem_Check

Evaluation result

Passed

Device Posture result

Non Compliant

Last scanned time

13 Nov 2024 at 1:26 PM

Verify configured policies

Details of each device policy for this transaction ID.

< Policy 2 of 3 >

Policy name

CWAVersion_Mem_Check

ID

3

Evaluation result

Passed

Policy result

Non Compliant

Policy conditions

Type

CWAVersion

Condition criteria

>

Expected value

22.11.0.67

Actual value

23.55.66.77

Condition result

True

AND

Type

MicrosoftEndpointManager

Condition criteria

Is

Expected value

[MicrosoftIsManaged MicrosoftIsCompliant]

Actual value

MicrosoftIsManaged

Condition result

True

使用精确搜索调试大型策略集

管理员可以在具有多个策略的复杂环境中搜索特定参数，并验证预期的用户上下文是否存在。如果发生参数值不匹配，系统会直观地突出显示失败条件，从而加速根本原因识别。此外，管理员可以浏览策略，查看哪些策略已评估以及哪些策略生成了当前的事务结果。

DaaS > Monitor

Try unified search

Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427791

Product Documentation

Status: Success

Time: 11/13/2024 1:26 PM

User name: dps0924@citrix.com

Endpoint: windows

Transaction Summary

Details of the device policy where all conditions were met.

Policy name

CWAVersion_Mem_Check

Evaluation result

Passed

Device Posture result

❌ Denied ⓘ

Last scanned time

13 Nov 2024 at 1:26 PM

Verify configured policies

Details of each device policy for this transaction ID.

Policy 1 of 3

Policy name

CWAVersion_CW_Check

ID

1

Evaluation result

Failed

Policy conditions

Type

CWAVersion

Condition criteria

>

Expected value

21.09.1.32

Actual value

20.55.66.77

Condition result

❌ False

AND

Type

CrowdStrikeRiskScore

Condition criteria

>

Expected value

50

Actual value

20

Condition result

❌ False

要排除大型策略参数工作集的故障，您可以搜索参数并查看所需的 用户上下文是否实时存在。

Verify configured policies

Details of each device policy for this transaction ID.

< Policy 1 of 4 >

Actual value

10.0.22621.4169

Condition result

● True

AND

Type

MACAddress

Condition criteria

in

Expected value

00-B0-D0-63-C2-26

12:34:56:78:9A:BC

12:34:56:78:9A:BC

DE:AD:BE:EF:00:11

01:23:45:67:89:AB

FE:DC:BA:98:76:54

12:34:56:78:9A:BC

12:34:56:78:9A:BC

+2 more

Actual value

00005e0053af

Condition result

❌ False

例如，在前面的屏幕截图中，突出显示的字段在搜索时没有结果（在下图中提及），这表明参数值不匹配。这种不匹配导致条件结果为假，进而导致整体策略结果被拒绝。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

92

OSDomainCheck

Policy condition: MACAddress in

Expected value (10)

处理事务故障和错误

如果策略评估因系统错误而失败，Citrix Monitor 中会显示以下详细信息：

- 包含上下文详细信息的错误描述。
- 指向故障排除文档的链接，可加快解决速度。

DaaS > Monitor

Try unified search Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427855

Product Documentation

Status: **Failed** Time: 09/26/2024 3:50 PM

Transaction Summary

 An internal error occurred during the device posture scan. Please use the provided error code to troubleshoot further.

Error Code [0x0050001](#)

Verify configured policies

Details of each device policy for this transaction ID.



Evaluation policies haven't been assessed yet because the device didn't meet the posture check requirements.

诊断设备姿态服务事务的步骤

1. 从最终用户设备复制失败或访问被拒绝会话的事务 ID。



Access denied

Device does not meet certain requirements

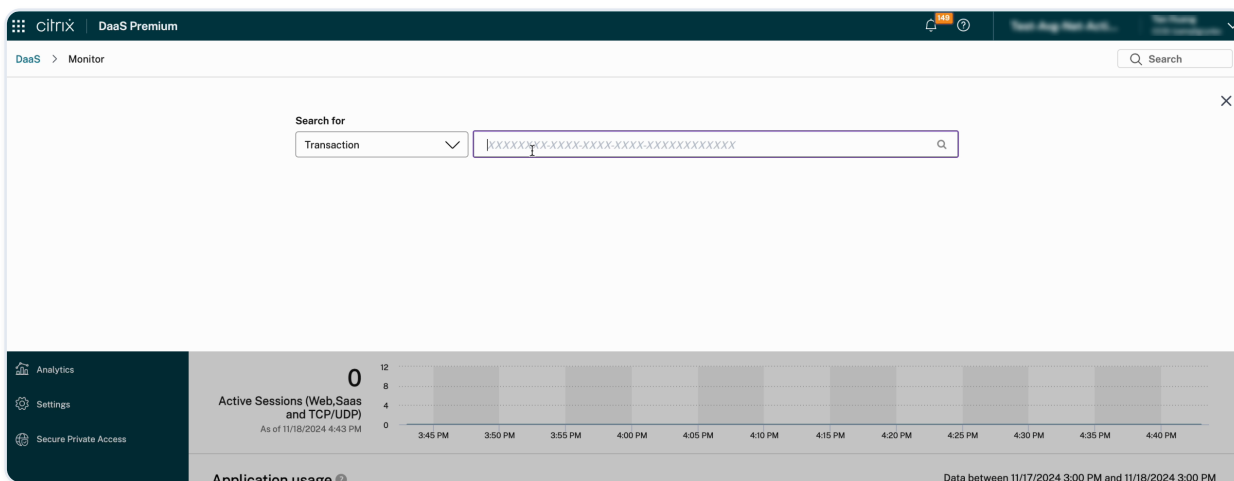
[Check device again](#)

If this persists **contact your administrator** and provide this ID:

0d05fbcc-1690-48d5-9fd0-09fa415c8575



2. 登录 Citrix Cloud。
3. 在 DaaS 磁贴上，单击 **管理**，然后单击 **监视器** 选项卡。
4. 在 **搜索** 字段中输入事务 ID，然后单击 **详细信息**。



您可以查看事务摘要和已配置设备姿态策略的验证详细信息。策略评估的不同值包括合规、不合规和拒绝。

事务摘要

“事务摘要”页面提供设备姿态策略的结果。对于合规、不合规和拒绝的结果，摘要包括：

- **平台**：客户端设备的操作系统。
- **策略名称**：设备姿态策略的名称。
- **评估结果**：指示设备姿态策略是通过还是失败。
- **设备姿态结果**：指示设备姿态结果是合规、不合规还是被拒绝。
- **上次扫描时间**：设备上上次扫描的时间。

验证已配置的策略

“验证已配置的策略”部分提供策略评估的详细信息，包括：

- 失败原因。
- 失败的具体规则。
- 收集到的证据。

此信息允许管理员根据策略详细信息进行故障排除并采取适当措施。

设备姿态策略评估过程

1. 策略失败和规则识别：

- 识别哪个规则失败了以及失败的原因。
- 收集与失败相关的证据。

2. 结果判定：

- 根据策略评估，结果可以是合规、不合规或拒绝。
- 如果没有策略匹配，结果是“无匹配策略”。

3. 查看策略详情：

- 管理员可以查看特定事务 ID 的每个设备策略的详细信息。
- 使用向后和向前箭头浏览不同的策略。

在合规、不合规和拒绝结果的情况下，“设备姿态”策略评估在“验证已配置策略”部分包含以下信息：

- **策略名称**：设备策略的名称。
- **ID**：策略的评估顺序。
- **评估结果**：指示设备姿态策略是通过还是失败。
- **策略结果**：指示设备姿态结果是合规、不合规还是拒绝。
- **策略条件**：
 - **类型**：设备扫描类型。
 - **条件标准**：用于评估策略规则的条件。
 - **预期值**：策略条件的配置值。
 - **实际值**：从端点收集的证据。
 - **条件结果**：指示条件是通过还是失败。

错误代码

当出现问题并且设备姿态未能评估策略时，将显示错误代码。

如果出现故障，请复制错误代码并联系 Citrix 支持。

策略详细信息和错误代码简化了用户问题的分类和故障排除。

下表提供了错误的错误代码、错误消息和解决方案：

# 序号	错误消息	错误代码	操作
1	未能读取配置的策略。	0x0050001	联系 Citrix 支持
2	无法评估端点扫描。	0x0050002	联系 Citrix 支持
3	无法处理策略或表达式。	0x0050003	联系 Citrix 支持
4	无法保存端点详细信息。	0x0050004	联系 Citrix 支持
5	无法处理来自端点的扫描结果。	0x0050005	联系 Citrix 支持
6	无法读取设备姿态模式配置。	0x0050006	联系 Citrix 支持

Citrix Secure Access 端点分析 (EPA) 客户端分发和升级

本主题介绍了分发和升级 Citrix Secure Access 端点分析客户端的受支持方法。此处捕获的信息适用于托管和非托管 Windows 设备，以及云（设备状态服务）和本地 (NetScaler® Gateway) 部署。

注意：

在本主题中，EPA 指的是 Citrix Secure Access 端点分析 (EPA) 客户端。这两个术语可互换使用。

Citrix Secure Access 端点分析 (EPA) 客户端分发和升级方法

方法	部署	托管	非托管	触发器	如何配置
与 Citrix Workspace™ 应用程序版本捆绑	云和本地	是	是	自动（随 Citrix Workspace 应用程序更新）	<p>Citrix Workspace 应用程序安装程序默认携带 Citrix Secure Access Endpoint Analysis 客户端，并与 Citrix Workspace 应用程序一起安装或升级它。</p> <p>请参阅 下载 Citrix Workspace 应用程序。</p>

方法	部署	托管	非托管	触发器	如何配置
					有关详细配置步骤，请参阅 与 Citrix Workspace 应用程序版本捆绑 。
Citrix Workspace 应用程序自动更新（客户端应用程序管理）	云和本地	是	是	自动 (Citrix Workspace 应用程序更新服务)	在客户端应用程序管理 (GACS) 控制台中启用 Citrix Endpoint Analysis 插件 以自动升级客户端。
					有关 GACS 设置的详细信息，请参阅 云：配置 GACS (云) 。
					本地部署： 配置 GACS (StoreFront) 。
					有关详细配置步骤，请参阅 Citrix Workspace 应用程序自动更新（客户端应用程序管理）
使用 SCCM、	云和本地部署	是	不适用	手动或管理员管理	管理员从 Citrix 下载

方法	部署	托管	非托管	触发器	如何配置
Intune、Jamf 或其他端点管理工具推送安装程序					下载安装程序。
					有关详细配置步骤，请参阅 使用 SCCM、Intune、Jamf 或其他端点管理工具推送安装程序 。
在设备姿态服务控制台中设置最低 EPA 客户端版本	仅限云	是	是	仅提示（不强制执行）	运行较低版本的客户端会在门户中看到下载选项。这不是静默或强制升级。最终用户手动安装或升级客户端。使用管理员权限安装。否则，安装将在用户模式下运行，并且某些功能可能不可用。
					有关详细配置步骤，请参阅 在设备状态服务控制台中设置最低 EPA 客户端版本 。

方法	部署	托管	非托管	触发器	如何配置
将插件上传到 NetScaler Gateway 门户	本地部署	是	是	仅提示（不强制执行）	<p>门户提供下载选项。最终用户手动安装或升级客户端。使用管理员权限安装。否则，安装将在用户模式下运行，并且某些功能可能不可用。</p> <p>有关详细配置步骤，请参阅将插件上传到 NetScaler Gateway 门户。</p>

详细配置步骤

以下部分包含详细的配置步骤：

与 Citrix Workspace 应用程序版本捆绑

Citrix Secure Access Endpoint Analysis 客户端与 Citrix Workspace 应用程序捆绑在一起。因此，安装或升级 Citrix Workspace 应用程序会自动安装或升级 EPA 客户端。

1. 在 Citrix Workspace 应用程序发行说明中跟踪 Citrix Workspace 应用程序的可用性。
2. 通过常用渠道分发 Citrix Workspace 应用程序：Citrix Workspace 应用程序自动更新、手动下载或移动设备管理 (MDM) 工具。

在安装过程中，捆绑的 Citrix Secure Access Endpoint Analysis 客户端将安装或升级。无需单独操作。

适用性： 云和本地。托管和非托管设备，最终用户自行安装或更新 Citrix Workspace 应用程序。

Citrix Workspace 应用程序自动更新（客户端应用程序管理）

当在客户端应用程序管理中启用 **Citrix Endpoint Analysis plug-in** 时，Citrix Workspace 应用程序自动更新服务会升级 Citrix Secure Access Endpoint Analysis 客户端。客户端应用程序管理控件名为 **Citrix Endpoint Analysis plug-in**，它升级的客户端在 Windows 控制面板中显示为 **Citrix Secure Access Endpoint Analysis**。

1. 打开客户端应用程序管理控制台。对于云，请参阅 [配置全局应用程序配置服务（云）](#)。对于本地，请参阅 [配置全局应用程序配置服务 \(StoreFront\)](#)。
2. 启用 **Citrix Endpoint Analysis plug-in** 以进行自动更新。
3. 确保配置的版本针对所需的 Citrix Secure Access Endpoint Analysis 版本。

Citrix Workspace 应用程序自动更新服务通过 Citrix Workspace 应用程序更新程序服务自动升级符合条件的端点上的 EPA 客户端。

配置的版本显示在门户的下载选项中，最终用户自行下载并安装或升级客户端。

适用性： 云和本地。托管和非托管设备。

使用 SCCM、Intune、Jamf 或其他端点管理工具推送安装程序

对于托管端点，管理员可以使用 SCCM、Intune、Jamf 或其他端点管理工具分发 Citrix Secure Access Endpoint Analysis 安装程序。

1. 从 [Citrix 下载](#) 下载 Citrix Secure Access Endpoint Analysis 安装程序。
2. 在您的端点管理平台中打包安装程序。
3. 使用您的标准软件分发流程将软件包部署到所需的托管 Windows 设备。
4. 从 Windows 控制面板或您的管理清单中验证已安装的版本。

适用性： 云和本地。仅限托管设备。

在设备状态服务控制台中设置最低 EPA 客户端版本

在设备状态服务控制台中，您可以设置最低 EPA 客户端版本。运行较低版本的客户端将在门户中看到下载选项，允许最终用户安装或升级客户端。

1. 在设备状态服务控制台中，将 Endpoint Analysis (EPA) 客户端最低版本设置为您的目标版本（例如，26.5.1.7）。有关详细信息，请参阅 [通过设备状态服务管理 EPA 客户端版本](#)。

在下一次状态评估时，运行较低版本的客户端将在门户中看到下载选项。

2. 最终用户下载并安装或升级客户端。

注意：

使用管理员权限安装。否则，安装将在用户模式下运行，并且某些功能可能不可用。

注意：

此方法会提示最终用户更新客户端。它不会强制执行静默或自动升级。

适用性： 仅限云。托管和非托管设备，其中最终用户通常是管理员。

将插件上传到 NetScaler Gateway 门户

您可以将 Citrix Secure Access Endpoint Analysis 插件上传到 NetScaler Gateway 门户。登录时，网关会提示用户下载或升级客户端。

有关配置步骤，请参阅 [用户如何通过 NetScaler Gateway 插件连接](#)。

注意：

此方法仅检测并提示。最终用户可以拒绝该操作，并且它不强制执行静默自安装。

使用管理员权限安装。否则，客户端将以用户模式安装，并且某些功能可能不可用。

适用性： 本地部署。托管和非托管设备，具有相同的检测和提示行为。

将 EPA 客户端与 NetScaler 和设备状态服务结合使用时的注意事项

当 EPA 客户端与设备状态服务和 NetScaler 一起使用时，可能会出现最终设备运行最新 EPA 客户端版本而 NetScaler 运行不同版本 EPA 客户端的情况。这种不匹配可能会导致 NetScaler 提示最终用户安装 NetScaler 上存在的 EPA 客户端版本。为避免此冲突，我们建议进行以下配置更改：

- 如果您已将 EPA 配置为自适应身份验证、本地身份验证或网关虚拟服务器，我们建议您在 NetScaler 上禁用 EPA 客户端的版本控制。这可确保客户端应用程序管理 (GACS) 或设备状态服务不会将最新版本的 EPA 客户端推送到最终设备。
- 您可以使用 CLI 或 GUI 将 EPA 版本控制设置为 **从不**。这些配置更改在 NetScaler 13.x 及更高版本上受支持。
 - CLI：对自适应身份验证和本地身份验证虚拟服务器使用 CLI 命令。

- GUI：对本地网关虚拟服务器使用 GUI。有关详细信息，请参阅 [控制 Citrix Secure Access 客户端的升级](#)。

示例 CLI 命令：

```
add rewrite action <rewrite_action_name> insert_http_header Plugin-Upgrade  
"\epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:Never;vpn_mac:Alw  
ays;vpn_linux:Always;"
```

```
add rewrite policy <rewrite_action_policy>  
"HTTP.REQ.URL.CONTAINS(\"pluginlist.xml\")" <rewrite_action_name>
```

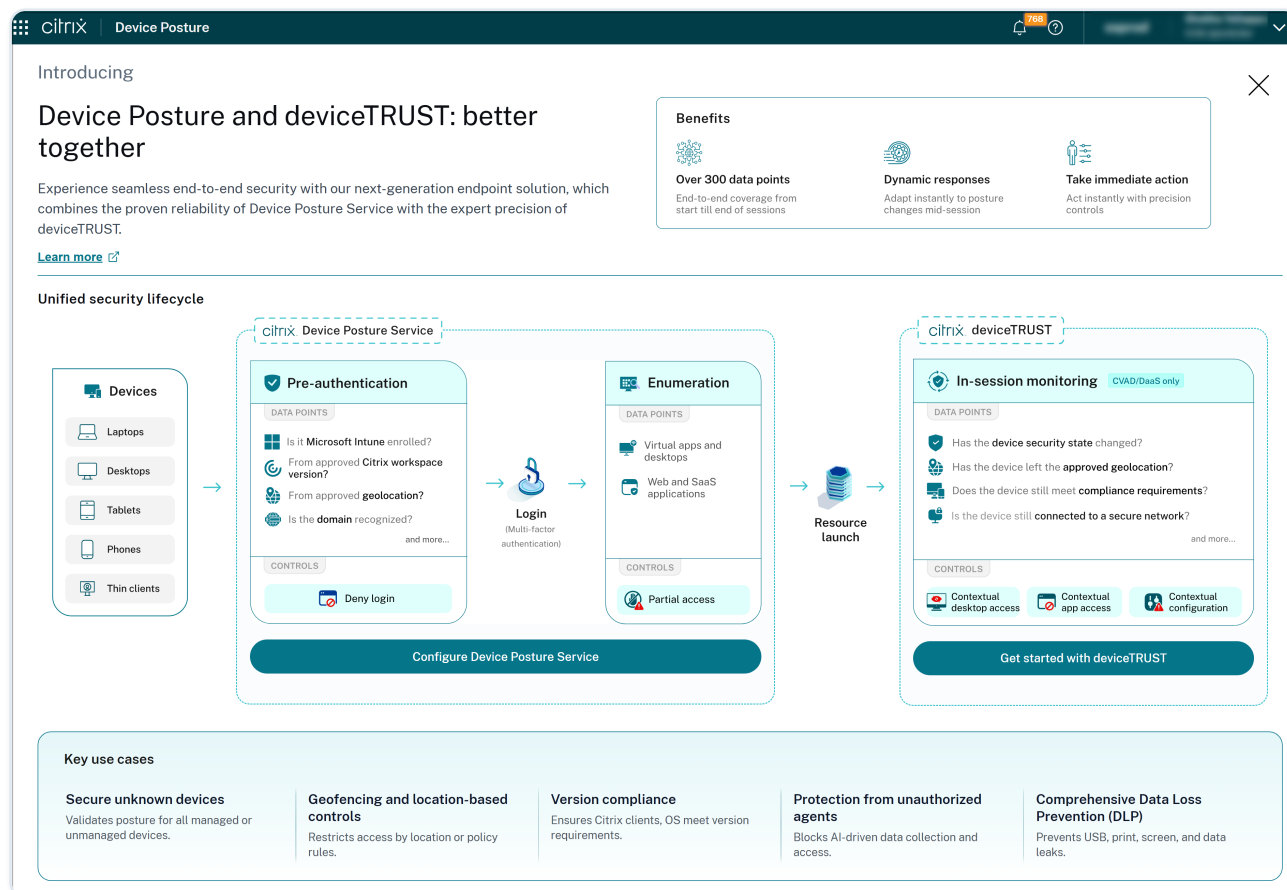
```
bind authentication vserver <Authentication_Vserver_Name> -policy  
<rewrite_action_policy> -priority 10 -type RESPONSE
```

设备姿态服务和 deviceTRUST - 强强联合

保护企业应用程序和数据的访问现在需要的不仅仅是静态策略。它们需要实时、上下文感知的控制，这些控制在用户旅程中持续适应。Citrix 设备姿态服务和 deviceTRUST 集成在每个阶段（预身份验证、枚举和会话内）提供全面的上下文访问覆盖。

要为您的特定环境配置设备姿态服务和 deviceTRUST，请参阅以下主题：

- [使用设备姿态配置上下文访问（智能访问）](#)
- [deviceTRUST 快速设置](#)



设备姿态服务和 deviceTRUST 如何协同工作

以下部分提供了有关设备姿态服务和 deviceTRUST 如何协同工作的信息。

预身份验证：在登录前建立信任

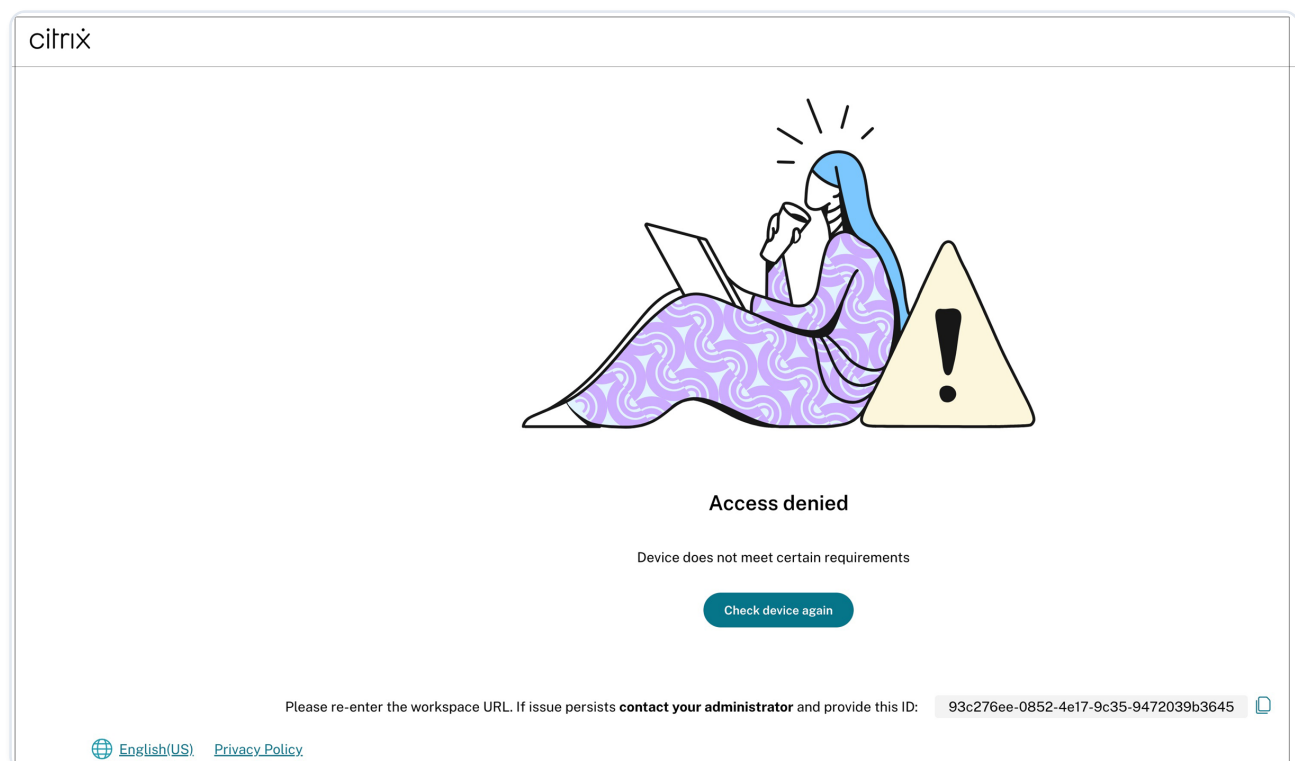
设备姿态服务充当第一道防线，在允许用户进行身份验证之前执行端点卫生检查。管理员可以定义策略来检查设备属性，例如：

- Citrix Workspace 应用程序版本
- 操作系统版本
- 安全软件状态（防病毒）
- 通过 MDM 解决方案进行企业注册
- 设备证书
- 符合企业标准

如果设备未能满足这些要求，则在身份验证开始之前就会阻止访问。

示例：

当用户尝试从个人设备登录时，设备姿态服务会验证防病毒软件是否已安装并正在运行。如果设备未能满足管理员创建的策略要求，则会拒绝登录，从而确保只有受信任的设备才能访问敏感资源。

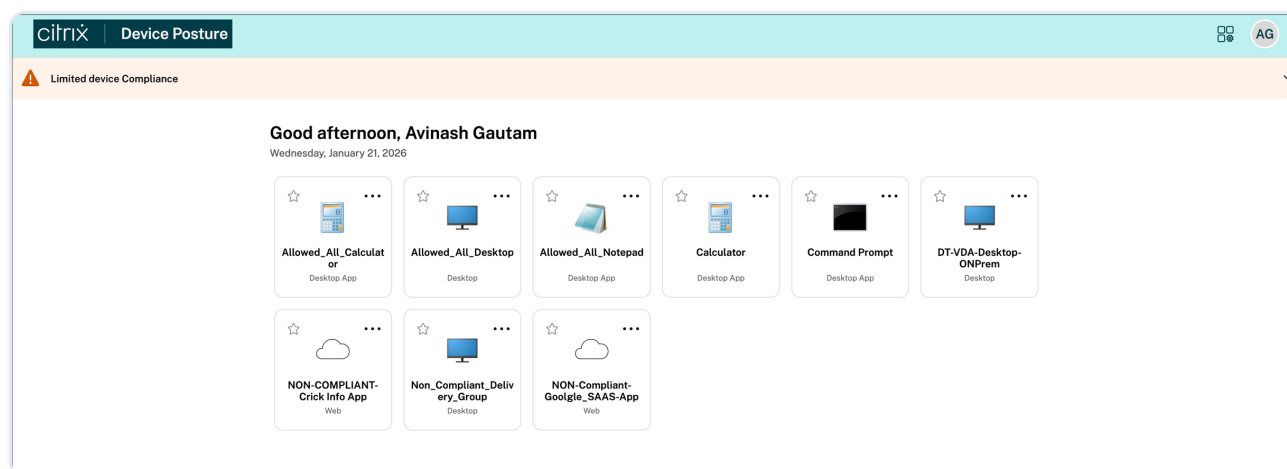


枚举：对应用程序的上下文访问

在枚举阶段，设备姿态服务通过在用户浏览或枚举商店中的应用程序时评估设备姿态来继续强制执行策略。管理员可以根据上下文限制哪些应用程序或桌面可见或可访问。

示例：

如果设备合规，用户将看到所有有权使用的应用程序。如果设备不合规，则某些应用程序可能会被隐藏，或者访问可能会受到限制，例如禁用剪贴板或文件传输功能。



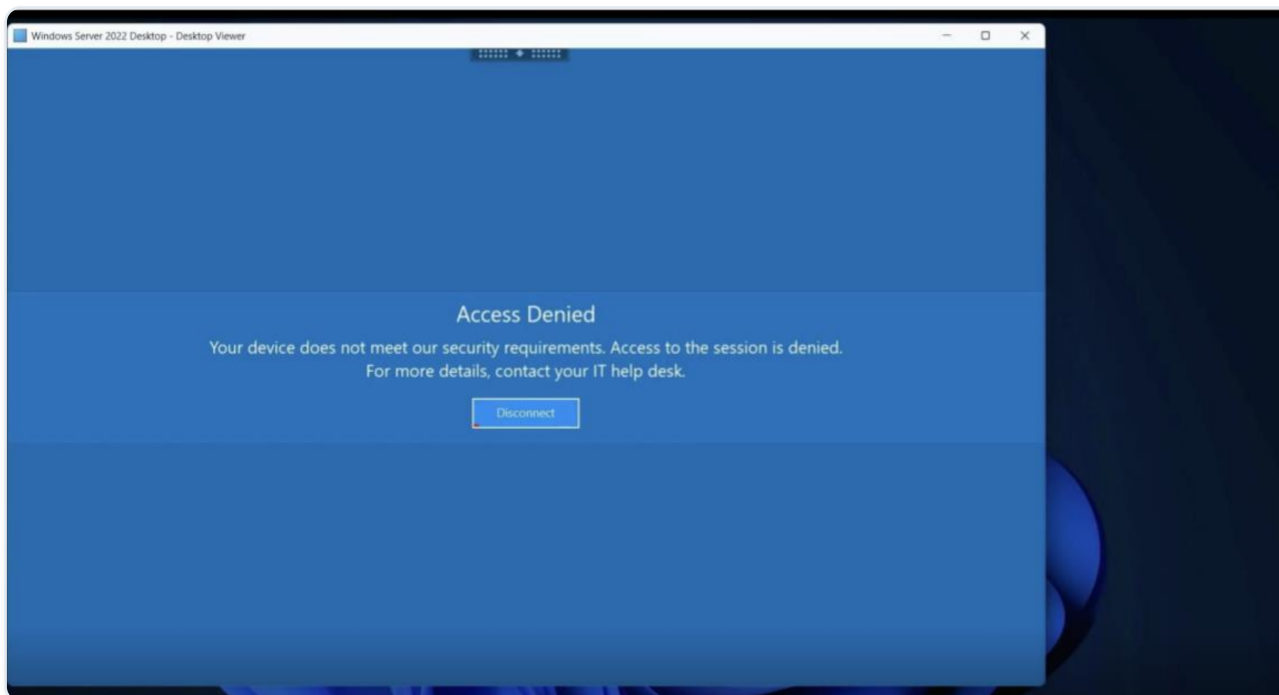
会话内：持续的上下文访问评估

会话建立后，deviceTRUST 接管以提供持续的会话内上下文访问控制。与仅在登录时检查设备姿态的传统解决方案不同，deviceTRUST 在整个会话期间监控设备上下文，从而在端点条件发生变化时动态强制执行策略。

精细控制：当设备上下文发生变化时（例如，插入未经授权的 USB 闪存盘、禁用防火墙、连接到未加密的 Wi-Fi、更改网络位置），管理员可以配置会话断开连接、弹出通知或审计等操作。

示例：

用户从合规设备启动会话。在会话期间，deviceTRUST 检测到更改——例如，设备连接到不安全的网络或连接了被禁止的外围设备。系统可以自动限制访问、断开会话或通知用户所需的操作，从而保持持续合规。



设备姿态服务与 deviceTRUST 集成的用例

设备姿态服务与 deviceTRUST 集成支持一系列关键用例，例如：

- 版本合规性（限制访问经批准的操作系统和应用程序版本）
- 地理围栏（根据设备位置控制访问）
- 持续监控安全状态，例如：
 - 防病毒状态
 - 防止未经授权的软件代理 - 通过动态限制剪贴板、文件传输和打印，实现全面的数据丢失防护 (DLP)
 - 在 BYOD 场景中保护未知或非托管设备。

这些功能使管理员能够在动态混合环境中保持持续合规性、降低风险并保护企业数据。

版本合规性

确保只有运行经批准的操作系统和 Citrix Workspace 应用程序 (CWA) 版本的设备才能访问资源。这可以防止过时或易受攻击的端点连接，从而降低未打补丁系统带来的风险。

有关详细的策略配置步骤，请参阅此[教程](#)。

地理围栏

根据设备的物理位置限制对应用程序和桌面的访问。例如，仅允许从经批准的国家或公司办公室访问，如果设备越过边界则撤销访问权限。

有关详细的策略配置步骤，请参阅此[教程](#)。

监控设备安全状态

杀毒软件检查：检查杀毒软件是一项基础安全措施，有助于确保只有受信任、受保护的设备才能在登录时和整个用户会话期间访问企业资源。这在动态、混合或BYOD环境中尤为重要，因为在这些环境中无法假定设备合规性。

有关详细的策略配置步骤，请参阅此[教程](#)。

数据治理

本主题提供有关设备姿态服务收集、存储和保留日志的信息。任何未在 [定义部分](#) 中定义的大写术语，均具有 [Citrix 最终用户服务协议](#) 中指定的含义。

数据驻留

Citrix 设备姿态客户内容数据驻留在 AWS 和 Azure 云服务中。这些数据会复制到以下区域以实现可用性和冗余：

- AWS
 - 美国东部
 - 印度西部
 - 欧洲（法兰克福）
- Azure 云
 - 美国西部
 - 欧洲西部
 - 亚洲（新加坡）
 - 美国中南部

以下是服务配置、运行时日志和事件的不同目标。

- Splunk 服务用于系统监控和调试日志，仅限美国地区。
- Citrix Analytics Service 用于诊断和用户访问日志，有关更多信息，请参阅 [Citrix Analytics Service Data Governance](#)。
- Citrix Cloud System Logs 服务用于管理员审计日志。有关详细信息，请参阅 [Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations](#)。

数据收集

Citrix Device Posture 服务允许客户管理员通过 Device Posture UI 配置服务。根据设备姿态策略配置和平台，收集以下客户内容：

- 操作系统版本
- Citrix Workspace™ 应用程序版本
- MAC 地址
- 正在运行的进程
- 设备证书
- 注册表详细信息
- Windows 安装更新详细信息
- 上次 Windows 更新详细信息
- 文件系统 – 文件名、文件哈希和修改时间
- 域名

对于服务组件收集的运行时日志，关键信息包括以下内容：

- 客户/租户 ID
- 设备 ID（Citrix 生成的唯一标识符）
- 设备姿态扫描输出
- 端点设备的公共 IP 地址

数据传输

Citrix Device Posture 服务将日志发送到受传输层安全保护的目标。

数据控制

Citrix Device Posture 服务目前不提供客户关闭日志发送或阻止客户内容在全球范围内复制的选项。

数据保留

根据 Citrix Cloud™ 数据保留策略，客户配置数据将在订阅到期 90 天后从服务中清除。

日志目标维护其服务特定的数据保留策略。

- 有关详细信息，请参阅 [数据治理](#)，了解分析日志的保留策略。
- Splunk 日志将在 90 天后存档并最终删除。

数据导出

针对不同类型的日志，有不同的数据导出选项。

- 管理员审计日志可从 Citrix Cloud 系统日志控制台访问。
- 设备姿态服务诊断日志可以从 Citrix Analytics Service 或 Secure Private Access 服务仪表板导出为 CSV 文件。

定义

- 客户内容 指上传到客户帐户进行存储的任何数据，或 Citrix 为执行服务而获得访问权限的客户环境中的数据。
- 日志 指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性以及支持的记录。
- 服务 指为 Citrix Analytics 目的而概述的 Citrix Cloud 服务。