Device Posture

Machine translated content

Disclaimer

Contents

Device Posture **2**

CrowdStrike 与 **Device Posture** 集成 **-** 预览版 **17**

Microsoft Intune 与 **Device Posture** 集成 **20**

使用 **Device Posture** 服务检查设备证书 **24**

使用 **Device Posture** 对 **DaaS** 实施智能控制 **26**

Device Posture 日志 **29**

管理 **Device Posture** 服务的 **Citrix Endpoint Analysis** 客户端 **29**

数据治理 **31**

Device Posture

February 20, 2024

Citrix Device Posture 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获得 Citrix DaaS (Virtual Apps and Desktops) 或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）的访问权限。通过检查设备的状态来建立设备信任对于实现基于零信任的访问至关重要。Device Posture 服务在允许最终用户登录之前检查终端设备的合规性（托管/BYOD 和安全状态），从而在您的网络中强制执行零信任原则。

必备条件

- 许可要求：Citrix Device Posture 服务的权利是 Citrix DaaS Premium、Citrix DaaS Premium Plus 和 Citrix Secure Private Access Advanced 许可证的一部分。拥有其他许可证的客户可以购买 Device Posture 服务授权作为附加组件。对于附加组件，客户必须购买独立的自适应身份验证 SKU，但不一定要部署它才能使用 Device Posture 服务。
- 支持的平台：
  - Windows（10 和 11）
  - macOS 13 Ventura
  - macOS 12 Monterey
  - iOS
  - IGEL

  > 注意：
  >
  > - 默认情况下，在不支持的平台上运行的设备被标记为不合规。您可以从“Device Posture”页面上的“设置”选项卡将分类从“不合规”更改为已拒绝登录。
  > - 默认情况下，在支持的平台上运行但不匹配任何预定义的 Device Posture 策略的设备被标记为不合规。您可以从“Device Posture”页面上的“设置”选项卡将分类从“不合规”更改为已拒绝登录。
  > - 为了在 Device Posture 服务中支持 iOS，EPA 客户端是作为适用于 iOS 的 Citrix Workspace 应用程序的一部分内置的。有关版本的详细信息，请参阅适用于 iOS 的 Citrix Workspace 应用程序。
  > - 为了在 Device Posture 服务上支持 IGEL 操作系统，EPA 客户端是作为 IGEL 操作系统的一部分内置的。如需在 IGEL 设备上安装 EPA 客户端，请联系 IGEL 支持团队。

- Citrix Device Posture 客户端（EPA 客户端）：一种轻量级应用程序，必须安装在端点设备上才能运行 Device Posture 扫描。此应用程序不需要本地管理员权限即可在端点上下载和安装。

> 注意：
>
> 如果您使用设备证书检查，则必须安装具有管理权限的 EPA 客户端。

- 支持的浏览器：Chrome、Edge 和 Firefox。
- 防火墙配置：要允许 Device Posture 服务更新终端设备上的 EPA 客户端，必须将防火墙/代理配置为允许以下域：
  - https://swa-ui-cdn-endpoint-prod.azureedge.net
  - https://productioniconstorage.blob.core.windows.net
  - *.netscalergateway.net
  - *.nssvc.net
  - *.cloud.com
  - *.pendo.io
  - *.citrixworkspacesapi.net

预览版功能

- 使用 IGEL 提供的 Device Posture 服务。使用 https://podio.com/webforms/29062020/2362942 注册预览版。
- iOS Device Posture 服务。使用 https://podio.com/webforms/28888524/2338366 注册预览版。
- 地理位置检查和网络位置检查。使用 https://podio.com/webforms/29051759/2362665 注册预览版。
- CrowdStrike 与 Device Posture 服务集成。有关详细信息，请参阅 CrowdStrike 与 Device Posture 集成 - 预览版。

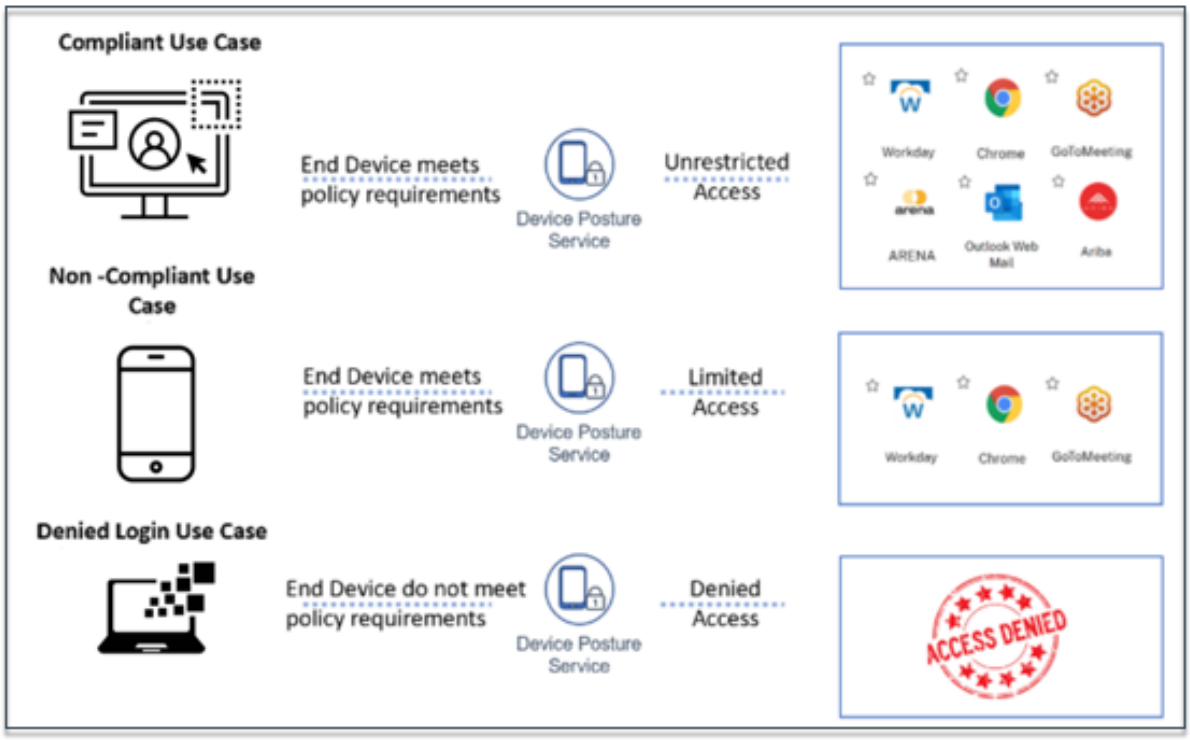
工作原理

管理员可以创建 Device Posture 策略来检查端点设备的状态并确定终端设备是被允许还是被拒绝登录。允许登录的设备被进一步归类为合规或不合规。用户可以从浏览器或 Citrix Workspace 应用程序登录。

以下是用于将设备归类为合规、不合规和拒绝登录的高级条件。

- 合规设备—符合预先配置的策略要求且允许登录公司网络的设备，同时可以完全或不受限制地访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源。
- 不合规设备 - 符合预先配置的策略要求且允许通过部分或限制访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源来登录公司网络的设备。
- 拒绝登录： - 不符合策略要求的设备将被拒绝登录。

将设备分为合规、不合规和拒绝登录的设备将传递给 Citrix DaaS 和 Citrix Secure Private Access 服务，后者反过来使用设备分类来提供智能访问功能。



注意：

- 必须专门为每个平台配置 Device Posture 策略。例如，对于 macOS，管理员可以允许访问具有特定操作系统版本的设备。同样，对于 Windows，管理员可以配置策略以包括特定的授权文件、注册表设置等。
- Device Posture 扫描仅在身份验证前/登录之前进行。
- 有关“合规”和“不合规”的定义，请参阅 定义。

Device Posture 支持的扫描

Citrix Device Posture 服务支持以下扫描：

Windows	macOS	iOS	IGEL
Citrix Workspace 应用程序版本 操作系统版本	Citrix Workspace 应用程序版本 操作系统版本	Citrix Workspace 应用程序版本 操作系统版本	- -
文件（存在、文件名和路径）	文件（存在、文件名和路径）	-	文件（存在、文件名和路径）
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）	进程（存在）	-	-

Windows	macOS	iOS	IGEL
Microsoft Endpoint Manager	Microsoft Endpoint Manager	-	-
CrowdStrike	CrowdStrike	-	-
设备证书	设备证书	-	-
浏览器	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 更新安装上次更新检查	-	-	-

> 注意：
>
> - 为了在 Device Posture 服务中支持 iOS，EPA 客户端是作为适用于 iOS 的 Citrix Workspace 应用程序的一部分内置的。有关版本的详细信息，请参阅适用于 iOS 的 Citrix Workspace 应用程序。

与 **Device Posture** 的第三方集成

除了 Device Posture 服务提供的本机扫描外，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 Device Posture 集成。
- CrowdStrike。有关详细信息，请参阅 CrowdStrike 与 Device Posture 集成 - 预览版。

配置 **Device Posture**

Device Posture 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。每项策略都附有一项操作，即合规、不合规和拒绝登录。此外，每项策略都与优先级相关联，如果策略评估结果为真并采取相关操作，则策略评估将停止。

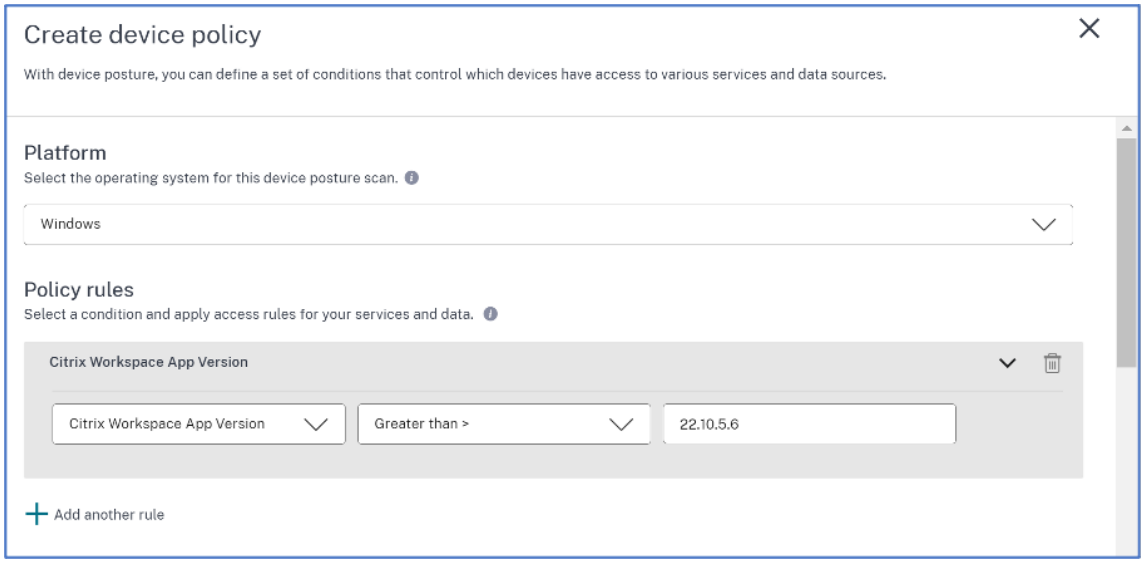
1. 登录 Citrix Cloud，然后从汉堡菜单中选择“身份和访问管理”。
2. 单击“**Device Posture**”选项卡，然后单击“管理”。

> 注意：
>
> - Secure Private Access 服务客户可以直接在管理员用户界面左侧导航栏中单击“**Device Posture**”。
> - 对于首次使用的用户，Device Posture 登录页面会提示您创建 Device Posture 策略。必须为每个平台单独配置 Device Posture 策略。创建 Device Posture 策略后，它将在相应的平台下列出。
> - 策略只有在启用 Device Posture 后才会生效。要启用 Device Posture，请将右上角的“**Device Posture** 已禁用”开关滑至“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“Device Posture”主页上选择了哪个选项卡，您都可以将平台从 Windows 更改为 macOS，反之亦然。
5. 在策略规则中，选择要作为 Device Posture 的一部分执行的检查，然后选择必须匹配的条件。

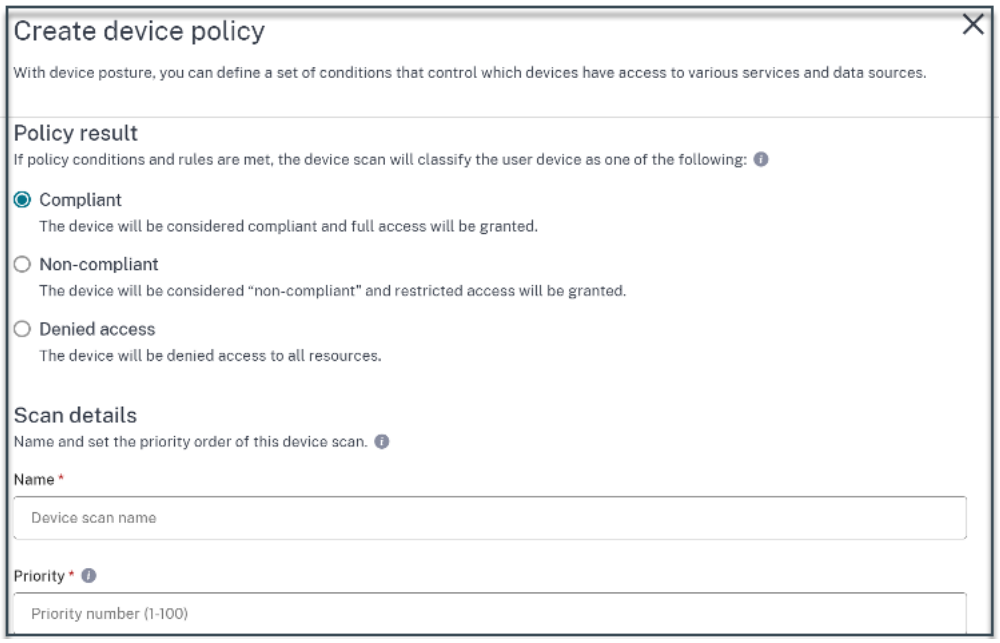
> 注意：
>
> - 要检查设备证书，请确保设备上存在颁发者证书。否则，您可以在创建 Device Posture 策略时导入设备证书，或者从 Device Posture 主页的设置上载证书。有关详细信息，请参阅在创建设备证书策略时导入设备证书和上载设备证书。
> - 要检查设备证书，必须使用管理权限安装终端设备上的 EPA 客户端。
> - 使用 Device Posture 服务进行的设备证书检查不支持证书吊销检查。

6. 单击“添加其他规则”以创建多个规则。AND 条件应用于多个规则。



7. 在基于您配置的条件的 策略结果 中，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
   - 访问被拒绝

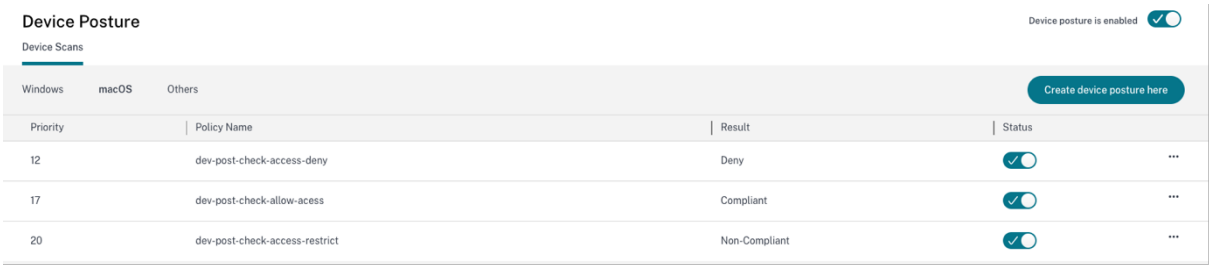
8. 输入策略的名称。
9. 在 优先级中，输入必须评估策略的顺序。
    - 可以输入 1 到 100 之间的值。建议您配置优先级更高的拒绝策略，然后是不合规，最后是合规。
    - 值较低的优先级优先级最高。
    - 只有已启用的策略才会根据优先级进行评估。
10. 单击创建。



> 重要提示：
>
> 您必须将“创建时启用”切换开关设置为“开”，Device Posture 策略才能生效。在启用策略之前，建议您确保策略配置正确，并在测试设置中执行这些任务。

编辑 **Device Posture** 策略

配置的 Device Posture 策略列在“设备扫描”页面的特定平台下。您可以从此页面搜索要编辑的策略。您也可以从此页面启用、禁用或删除策略。



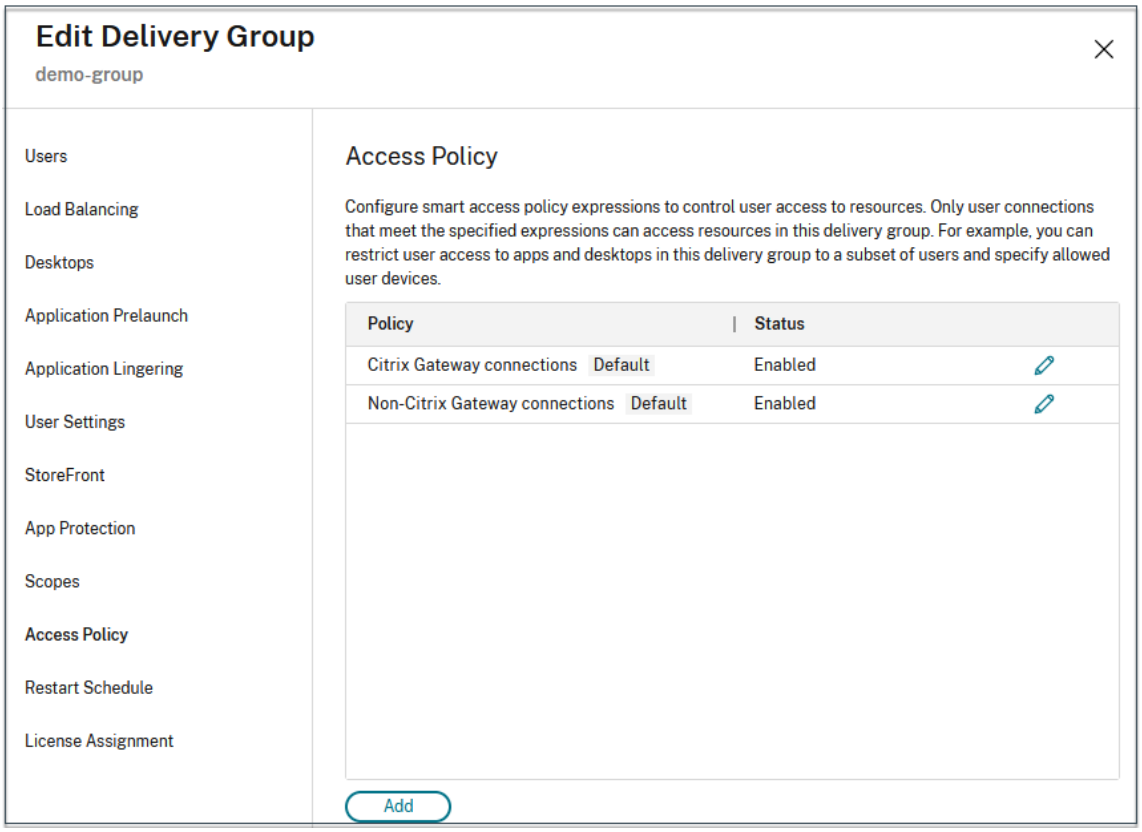
使用 **Device Posture** 配置上下文访问（智能接入）

Device Posture 验证后，允许设备登录并归类为合规或不合规。此信息可用作 Citrix DaaS 服务和 Citrix Secure Private Access 服务的标签，用于根据 Device Posture 提供上下文访问权限。因此，必须将 Citrix DaaS 和 Citrix Secure Private Access 配置为使用 Device Posture 标签强制执行访问控制。

使用新的 **Studio** 用户界面使用设备状态进行 **Citrix DaaS** 配置（预览版）

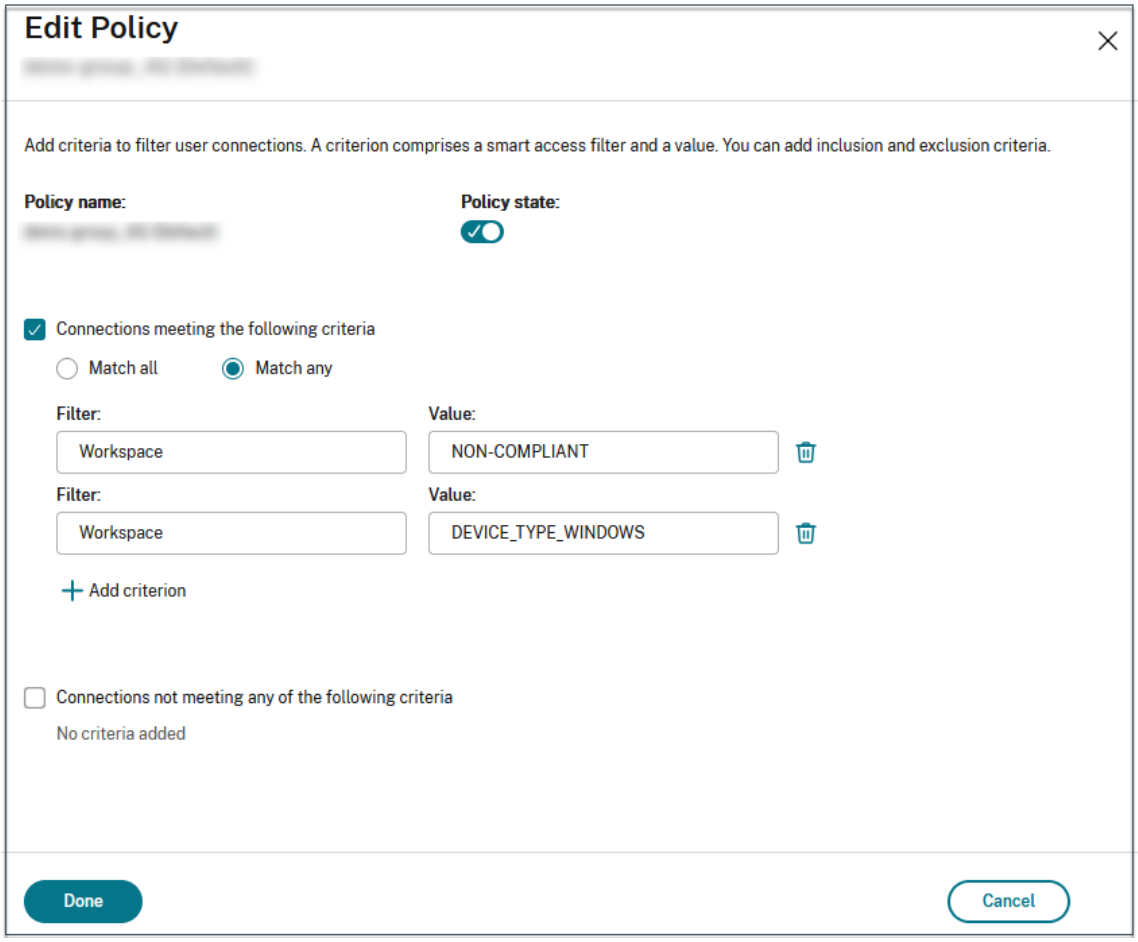
注册预览。

1. 登录 Citrix Cloud。
2. 在 **DaaS** 磁贴上，单击“管理”。
3. 从左侧菜单转到 交付组 部分。
4. 选择要根据 Device Posture 配置访问控制的交付组，然后单击“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) 选择任意匹配，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标准：在过滤器中键入 **Workspace**，在值中键入 **COMPLIANT** 或 **NON-COMPLIANT**。



注意：

设备分类标签的输入方式必须与之前捕获的语法相同，即全部使用大写（**COMPLIANT** 和 **NON-COMPLIANT**）。否则，Device Posture 策略将无法按预期运行。

除设备分类标签外，Device Posture 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只能以大写形式输入。

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

带有 **Device Posture** 的 **Citrix Secure Private Access** 配置

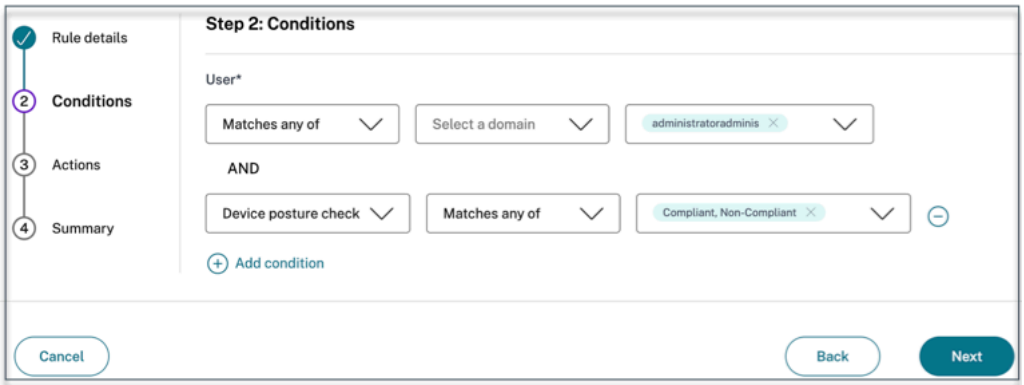
1. 登录 Citrix Cloud。
2. 在 Secure Private Access 图块上，单击管理。

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一组应用程序。
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. 选择用户的条件。用户条件是向用户授予应用程序访问权限时必须满足的强制性条件。
9. 单击 **+** 添加 Device Posture 条件。
10. 从下拉菜单中选择 **Device Posture** 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 - 适用于不兼容的设备
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”。

    摘要页面显示策略的详细信息。
14. 您可以验证详细信息，然后单击“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：
>
> 任何未在访问策略中标记为合规或不合规的 Secure Private Access 应用程序都被视为默认应用程序，无论 Device Posture 如何，都可以在所有端点上进行访问。



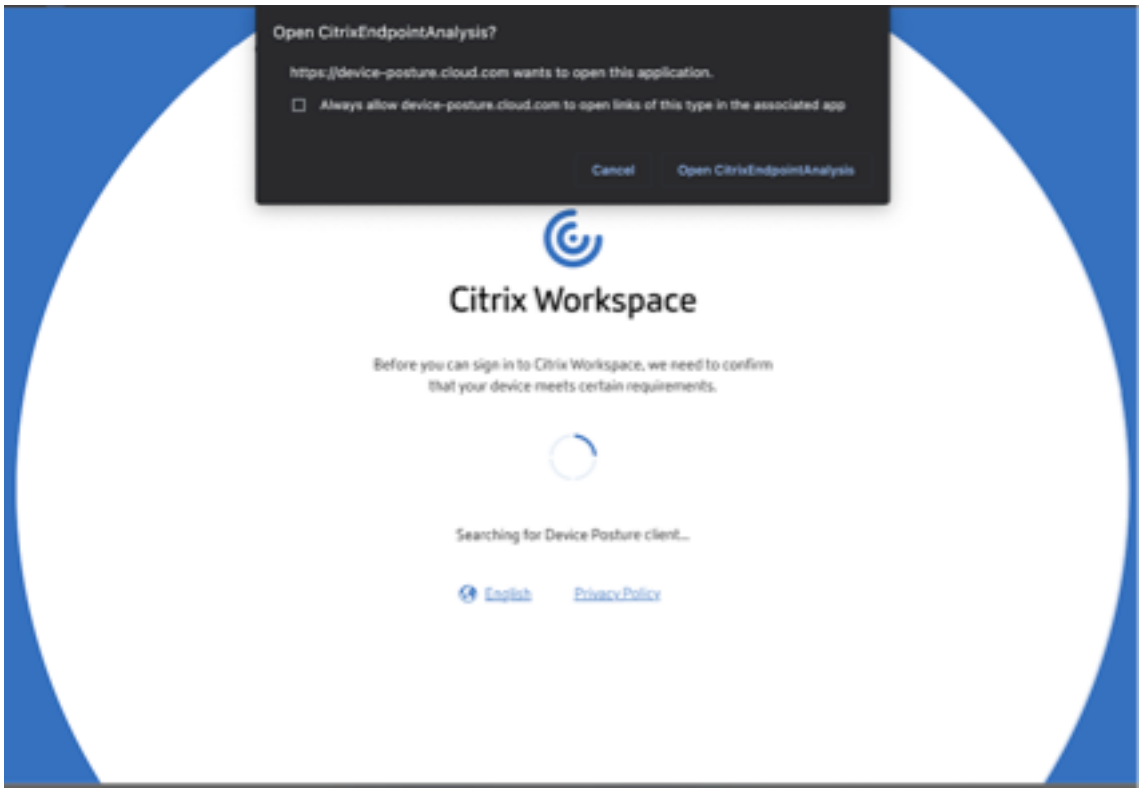
最终用户流程

设置 Device Posture 策略并启用 Device Posture 后，以下是基于最终用户登录 Citrix Workspace 的方式的最终用户流程。

最终用户通过浏览器访问流量

> 注意：
>
> macOS 客户机和 Chrome 浏览器作为示例，仅供参考。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 Citrix Workspace URL `https://<your-workspace-URL` 时，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，Device Posture 客户端会根据 Device Posture 策略要求运行并扫描端点参数。
- 如果端点设备上未安装最新的 Device Posture 客户端，则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”。
- 如果端点上已经安装了最新的 Device Posture 客户端，则用户必须再次单击“检查”。

通过 **Citrix Workspace** 应用程序进行的最终用户流程

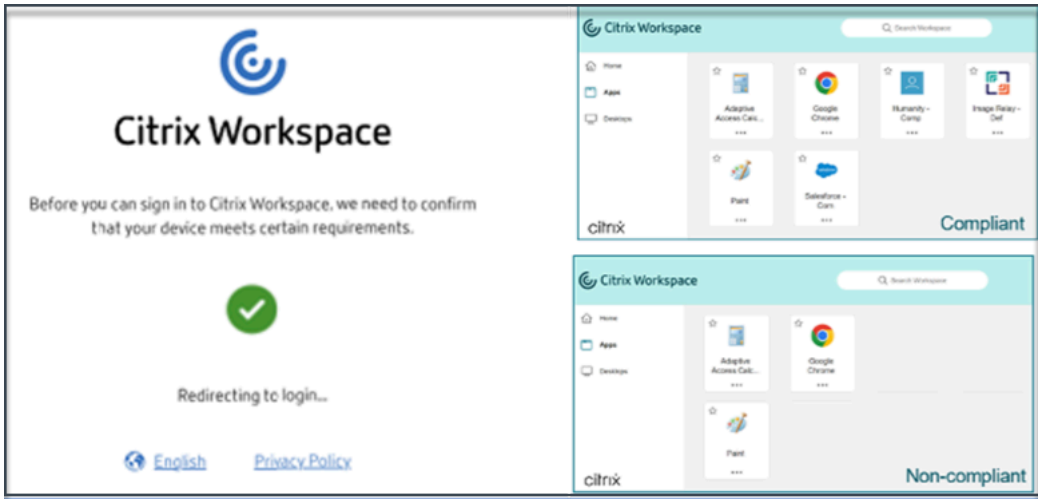
- 当最终用户通过 Citrix Workspace 应用程序登录 Citrix Workspace URL `https://your-workspace-url` 时，安装在终端上的 Device Posture 客户端会根据 Device Posture 策略要求运行并扫描端点参数。
- 如果端点设备上未安装最新的 Device Posture 客户端，则用户将被重定向到显示“再次检查”和“下载客户端”选项的页面。用户必须单击“下载客户端”。
- 如果端点上已经安装了最新的 Device Posture 客户端，则用户必须再次单击“检查”。

最终用户流程 **- Device Posture** 结果

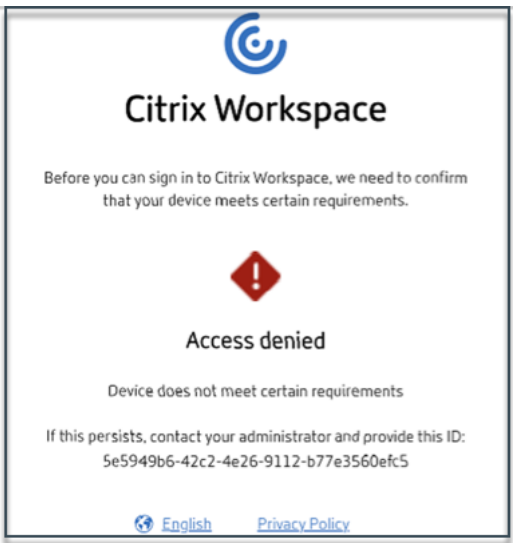
根据 Device Posture 策略条件，可能会出现三种可能性。

如果终端符合策略条件，则该设备被归类为；

- 合规 -允许最终用户使用 Secure Private Access 或 Citrix DaaS 资源不受限制的访问权限登录。
- 不合规 -允许最终用户以 Secure Private Access 或 Citrix DaaS 资源的受限访问权限登录。



如果终端满足策略条件，使该设备被归类为拒绝访问，则会出现“访问被拒绝”消息。



针对访问被拒绝场景的自定义消息（预览版）　管理员可以选择自定义访问被拒绝时显示在终端设备上的消息。

此功能正在预览中。使用 https://podio.com/webforms/29219975/2385710 注册预览版。

执行以下步骤以添加自定义消息：

1. 导航到设备状态 **>** 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访问被拒绝情况下必须显示的消息。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显示自定义消息的选项。如果未选中此复选框，则会创建自定义消息，但不会在访问被拒绝的情况下显示在设备上。

   或者，您可以启用设置页面上的自定义消息切换开关，以便在设备上显示消息。

5. 单击“保存”。

每当终端设备访问被拒绝时，就会显示您输入的消息。

监视 **Device Posture** 事件并对其进行故障排除

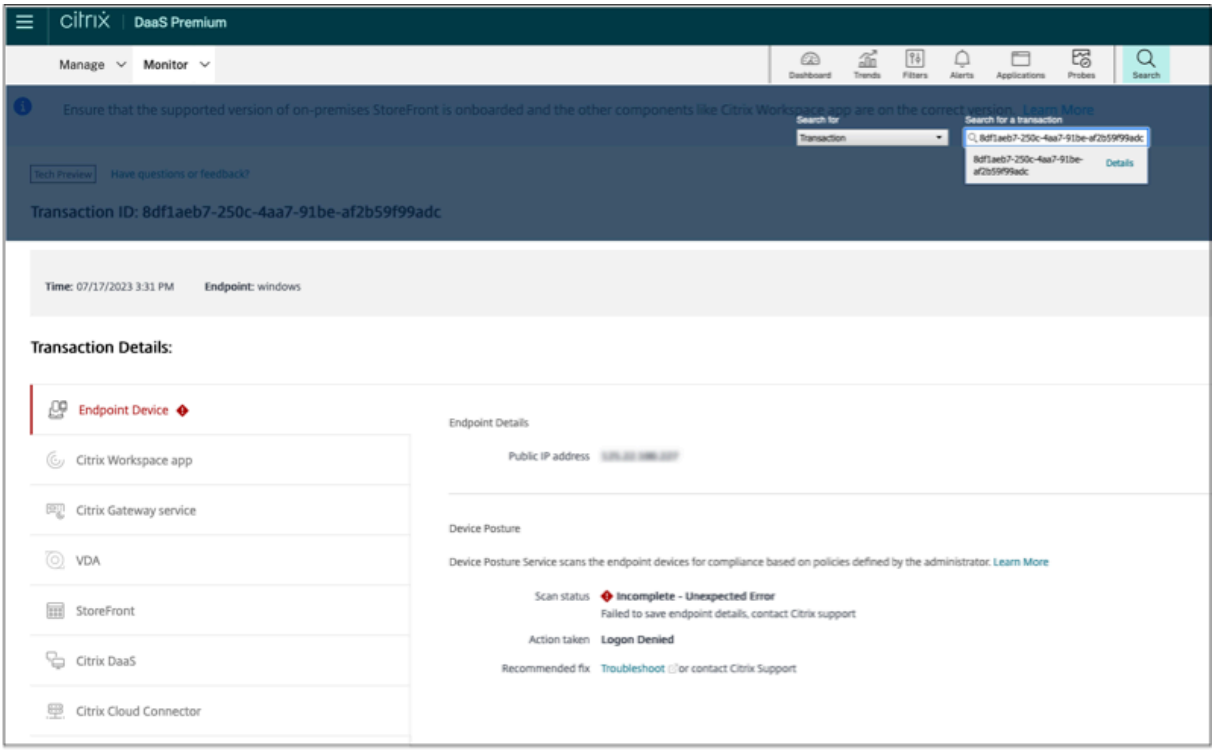
可以在两个位置查看 Device Posture 事件日志：

- Citrix DaaS Monitor
- Citrix Secure Private Access 控制面板

Citrix DaaS Monitor 上的 **Device Posture** 事件

执行以下步骤查看 Device Posture 服务的事件日志。

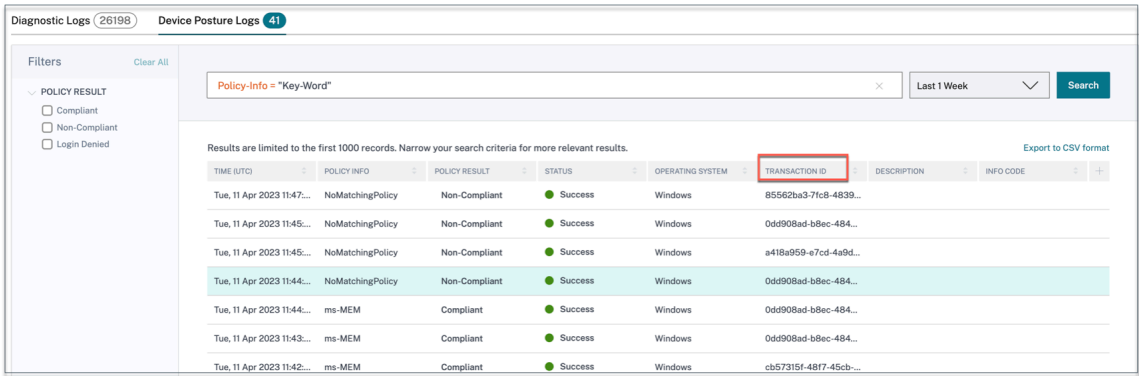
1. 从最终用户设备复制失败或访问被拒绝的会话的交易 ID。
2. 登录 Citrix Cloud。
3. 在 DaaS 磁贴上，单击“管理”，然后单击“监视”选项卡。
4. 在 Monitor UI 中中，搜索 32 位事务 ID，然后单击“详细信息”。



Secure Private Access 控制面板上的 **Device Posture** 事件

执行以下步骤查看 Device Posture 服务的事件日志。

1. 登录 Citrix Cloud。
2. 在 Secure Private Access 图块上，单击管理。
3. 从左侧菜单转到控制板部分。
4. 单击“诊断日志”图表中的“查看更多”链接以查看 Device Posture 事件日志。



- 管理员可以根据诊断日志图表中的交易 ID 筛选日志。每当访问被拒绝时，也会向最终用户显示交易 ID。

- 如果出现错误或扫描失败，Device Posture 服务会显示交易 ID。此交易 ID 可在 Secure Private Access 服务控制面板中找到。如果日志无法帮助解决问题，则最终用户可以与 Citrix 支持部门共享事务 ID 以解决问题。

- Windows 客户端日志可以在以下网址找到：
  - %localappdata%\Citrix\EPA\dpaCitrix.txt
  - %localappdata%\Citrix\EPA\epalib.txt
- macOS 客户端日志可以在以下网址找到：
  - ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
  - ~/ 库/应用程序 Support/Citrix/EPAPlugin/epaplugin.log

Device Posture 错误日志

可以在 Citrix Monitor 和 Secure Private Access 控制面板上查看以下与 Device Posture 服务相关的日志。对于所有这些日志，建议您联系 Citrix 支持部门寻求解决方案。

- 读取配置的策略失败
- 无法评估端点扫描
- 无法处理策略/表达式
- 保存终端节点详细信息失败
- 无法处理来自端点的扫描结果

已知限制

- Device Posture 服务不支持自定义 Workspace URL。
- 开启或关闭 Device Posture 切换按钮后，启用或禁用 Device Posture 功能所花费的时间可能需要几分钟到一个小时。
- Device Posture 配置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 Device Posture 服务已关闭，则用户可能无法登录 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 上配置了长期有效的令牌和密码，则 Device Posture 扫描不适用于此配置。只有在用户登录 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 个规则。
- Device Posture 服务不支持基于角色的访问。

服务质量

- 性能：在理想条件下，Device Posture 服务会在登录期间额外增加 2 秒的延迟。这种延迟可能会增加，具体取决于其他配置，例如 Microsoft Intune 等第三方集成。
- 灵活性：Device Posture 服务具有很强的弹性，具有多个 PoP，可确保没有停机。

定义

与 Device Posture 服务相关的合规和不合规术语定义如下。

- 合规设备—符合预先配置的策略要求且允许登录公司网络的设备，同时可以完全或不受限制地访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源。
- 不合规设备 - 符合预先配置的策略要求且允许通过部分或限制访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源来登录公司网络的设备。

CrowdStrike 与 **Device Posture** 集成 **-** 预览版

February 20, 2024

CrowdStrike Zero Trust Assessment (ZTA) 通过计算每台终端设备的 ZTA 安全分数从 1 到 100 来提供安全态势评估。ZTA 分数越高意味着终端设备的状况越好。

Citrix Device Posture 服务可以使用终端设备的 ZTA 分数来启用对 Citrix 桌面即服务 (DaaS) 和 Citrix Secure Private Access (SPA) 资源的情境访问（智能访问）。

Device Posture 管理员可以将 ZTA 分数用作策略的一部分，并将终端设备归类为合规、不合规（部分访问），甚至拒绝访问。反过来，组织可以使用这种分类来提供对虚拟应用程序和桌面以及 SaaS 和 Web 应用程序的情境访问（智能访问）。Windows 和 macOS 平台支持 ZTA 分数策略。

配置 **CrowdStrike** 集成

CrowdStrike 集成配置过程分为两步。

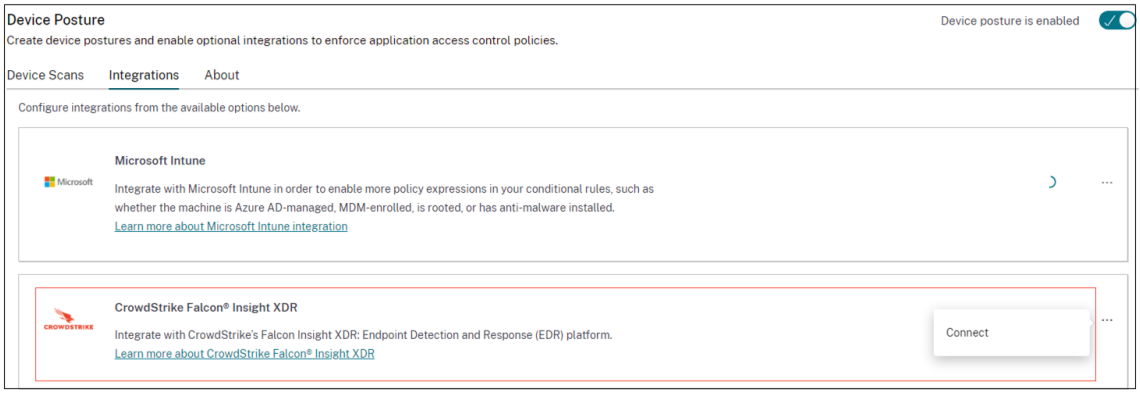
第 **1** 步：在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任。这是一次性操作。

第 **2** 步：配置策略以使用 CrowdStrike ZTA 分数作为规则，提供对 Citrix DaaS 和 Citrix Secure Private Access 资源的智能访问。

第 **1** 步：在 **Citrix Device Posture** 服务和 **CrowdStrike ZTA** 服务之间建立信任

执行以下操作以在 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“身份和访问管理”。
2. 单击“**Device Posture**”选项卡，然后单击“管理”。
3. 单击“集成”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“集成”选项卡。

4. 单击 CrowdStrike 框中的省略号按钮，然后单击“连接”。CrowdStrike Falcon Insight XDR 集成窗格出现。
5. 输入客户端 ID 和客户端密钥，然后单击“保存”。

> 注意：
>
> - 您可以从 CrowdStrike 门户（支持和资源 **> API** 客户端和密钥）获取 ZTA API 客户端 ID 和客户端密钥。
> - 确保选择零信任评估和具有读取权限的主机范围来建立信任。

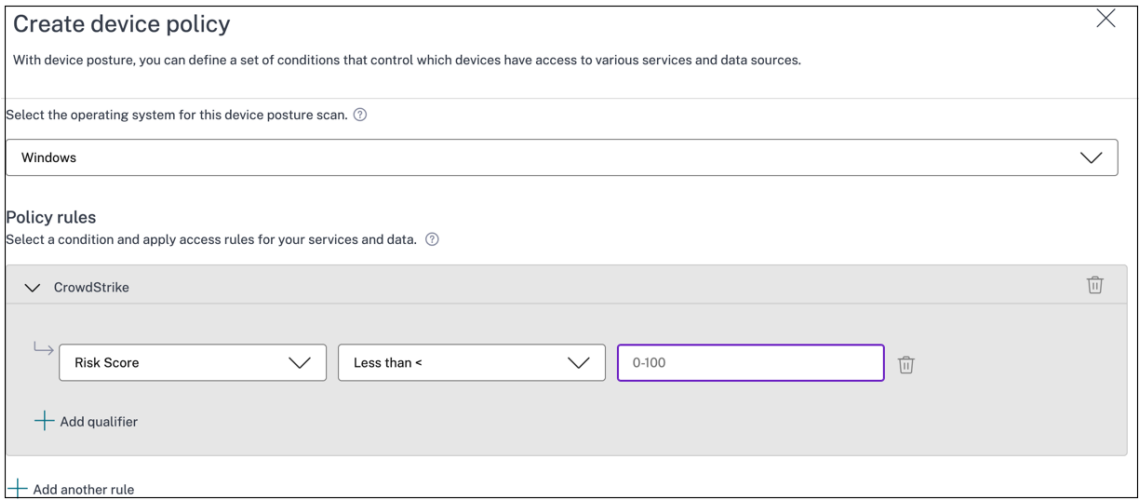
状态从“未配置”变为“已配置”后，即认为集成成功。

如果集成不成功，则状态显示为“待定”。必须单击省略号按钮，然后单击“重新连接”。

步骤 **2**：配置 **Device Posture** 策略

执行以下操作以配置策略，以使用 CrowdStrike ZTA 分数作为规则，提供对 Citrix DaaS 和 Citrix Secure Private Access 资源的智能访问。

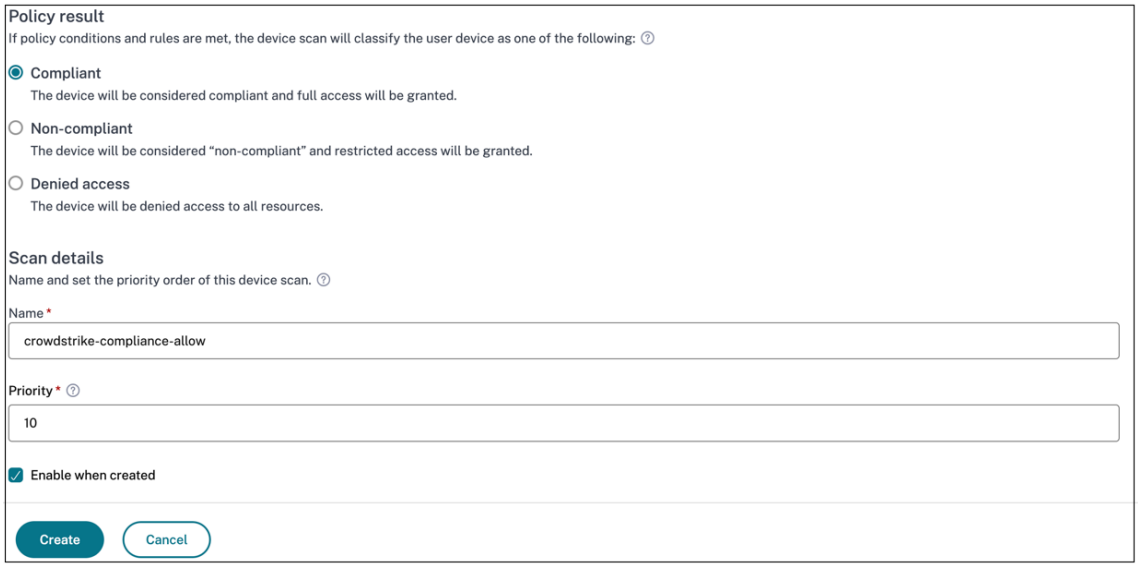
1. 单击“设备扫描”选项卡，然后单击“创建设备策略”。



2. 选择创建此策略的平台。
3. 在“策略规则”中，选择 **CrowdStrike**。
4. 对于 风险评分 限定词，选择条件，然后输入风险分数。
5. 单击 **+** 添加一个限定符，用于检查 CrowdStrike Falcon 传感器是否在运行。

> 注意：
>
> 您可以将此规则与为 Device Posture 配置的其他规则一起使用。

6. 在基于您配置的条件的 策略结果 中，选择以下选项之一。
   - 合规
   - 不合规
   - 拒绝登录



7. 输入策略的名称并设置优先级。
8. 单击创建。

定义

涉及 Device Posture 服务的合规和不合规术语定义如下。

- 合规设备—符合预先配置的策略要求且允许登录公司网络的设备，同时可以完全或不受限制地访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源。
- 不合规设备 - 符合预先配置的策略要求且允许通过部分或限制访问 Citrix Secure Private Access 资源或 Citrix DaaS 资源来登录公司网络的设备。

引用

Device Posture 服务

Microsoft Intune 与 Device Posture 集成

February 20, 2024

Microsoft Intune 根据其策略配置将用户的设备归类为合规设备或已注册设备。在用户登录 Citrix Workspace 期间，Device Posture 可以向 Microsoft Intune 检查用户的设备状态，并使用这些信息将 Citrix Cloud 中的设备归类为合规、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 等服务反过来使用设备状况的设备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）。

配置 **Microsoft Intune** 集成

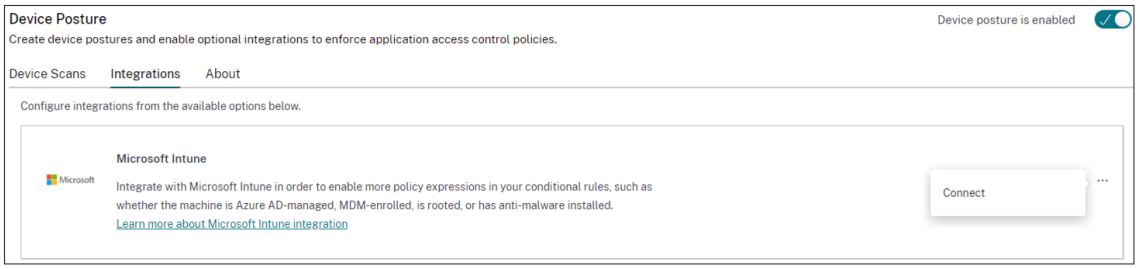
Intune 集成配置是一个分为两个步骤的过程。

第 **1** 步：将 Device Posture 与 Microsoft Intune 服务集成。这是您进行的一次性活动，目的是在 Device Posture 与 Microsoft Intune 之间建立信任。

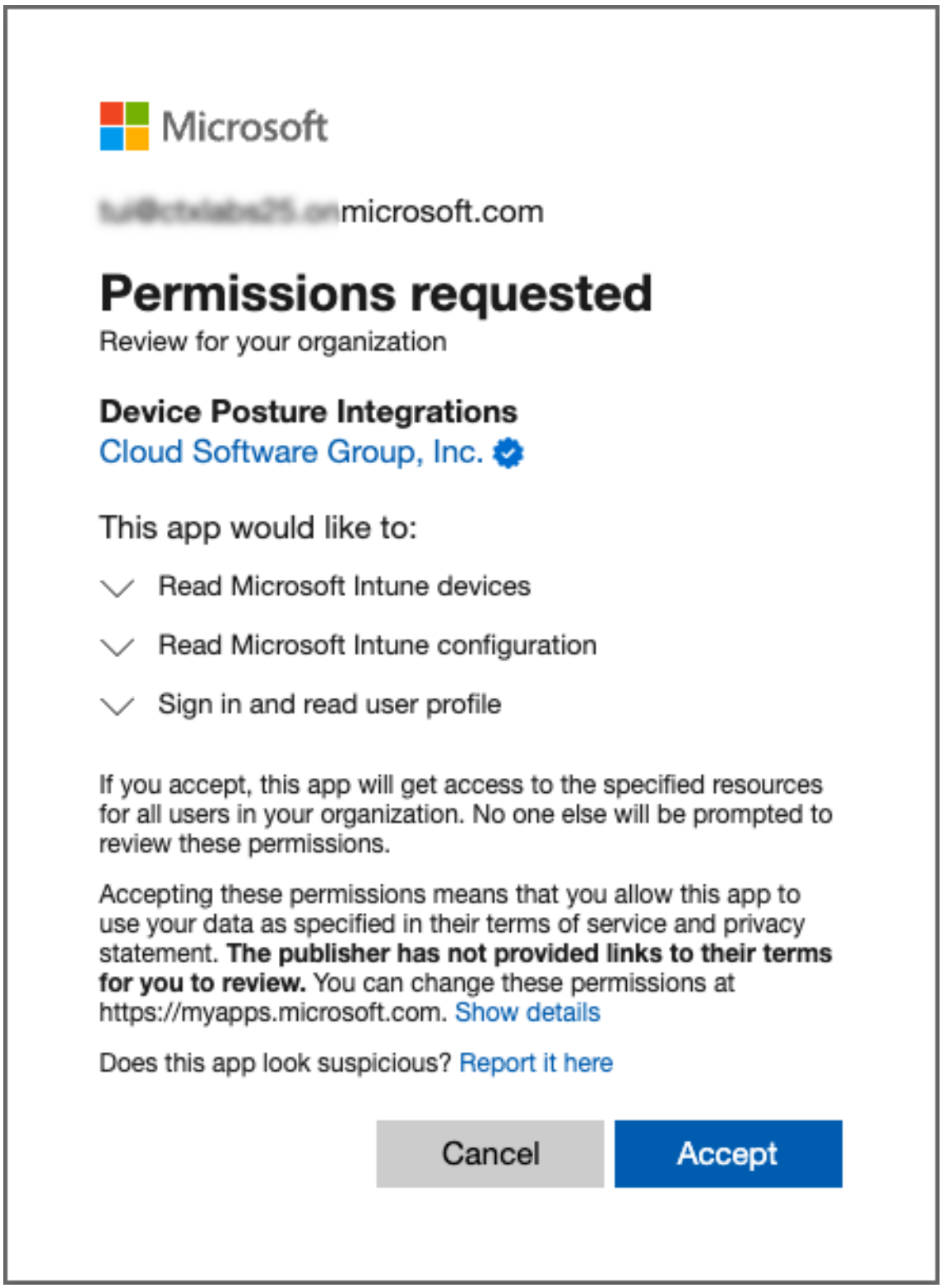
步骤 **2**：配置策略以使用 Microsoft Intune 信息。

步骤 **1**：将 **Device Posture** 与 **Microsoft Intune** 集成

1. 要访问“集成”选项卡，请使用以下方法之一：
   - 在您的浏览器上访问 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 上，在左侧导航窗格中，单击 **Device Posture**，然后单击“集成”选项卡。



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

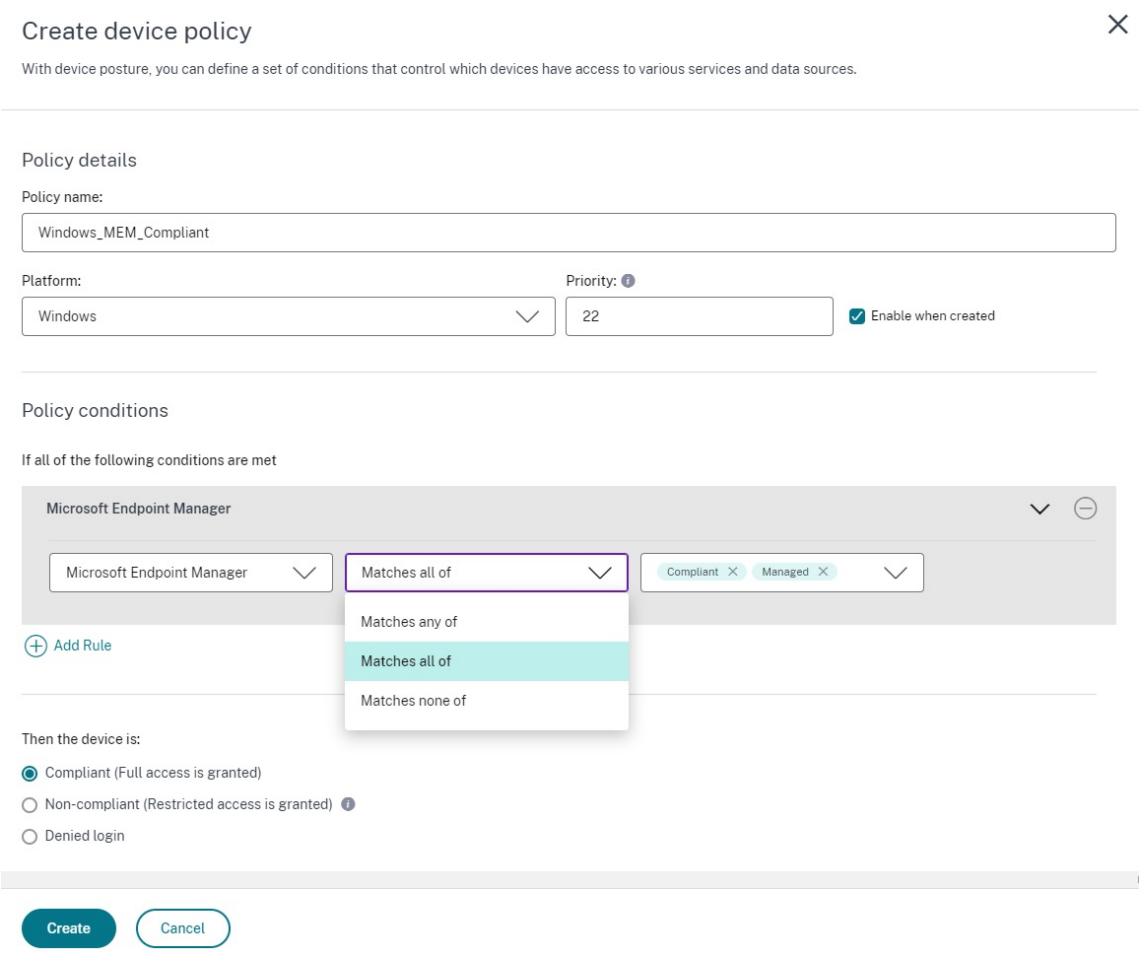


集成状况从“未配置”更改为“已配置”后，管理员可以创建设备状况策略。

如果集成不成功，则状态显示为“待定”。必须单击省略号按钮，然后单击“重新连接”。

步骤 **2**：配置 **Device Posture** 策略

1. 单击“设备扫描”选项卡，然后单击“创建设备策略”。



2. 输入策略的名称并设置优先级。
3. 选择创建此策略的平台。
4. 在“选择规则”中，选择“**Microsoft Endpoint Manager**”。
5. 选择一个条件，然后选择要匹配的 MEM 标记。
   - 对于任一匹配，将应用 OR 条件。
   - 对于“全部匹配”，则应用 AND 条件。

   > 注意：
   >
   > 您可以将此规则与为 Device Posture 配置的其他规则一起使用。

6. 在则设备为**:** 中，根据您配置的条件，选择以下选项之一。
   - 合规（已授予完全访问权限）

- 不合规（授予受限访问权限）
- 拒绝登录

有关创建策略的更多详细信息，请参阅配置设备状况策略。

使用 **Device Posture** 服务检查设备证书

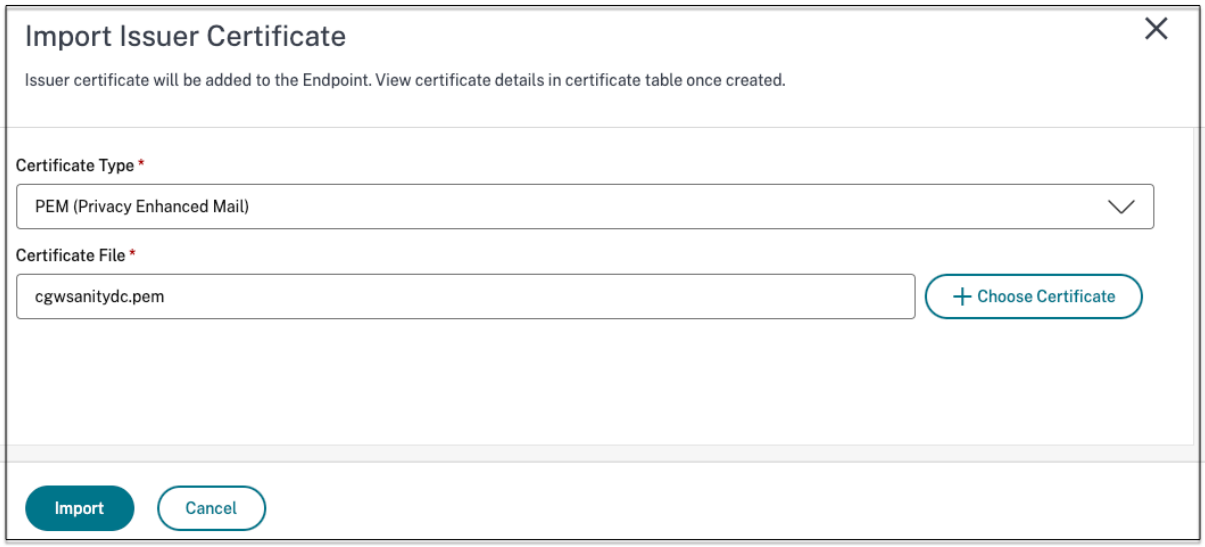
February 20, 2024

要使用 Device Posture 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 Device Posture 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作为 Device Posture 策略的一部分。

> 注意事项：
>
> - Device Posture 服务仅支持 PEM 颁发者证书类型。
> - 要在 Windows 上进行设备证书检查，必须使用管理权限安装终端设备上的 EPA 客户端。对于其他支票，您不需要本地管理权限。有关支持的扫描的详细信息，请参阅 Device Posture 支持的扫描。
> - 要在 Windows 上安装具有管理权限的 EPA 客户端，请在下载 EPA 客户端插件的位置运行以下命令。
>
>   ```
>   msiexec /i epasetup.msi
>   ```
>
> - 使用 Device Posture 服务进行的设备证书检查不支持证书撤消检查。
> - 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载到单个 PEM 文件中。
>
>   ```
>   Example: chain.pem
>
>   -----BEGIN CERTIFICATE-----
>   ******************************
>   -----END CERTIFICATE-----
>   -----BEGIN CERTIFICATE-----
>   ******************************
>   -----END CERTIFICATE
>   ```

上载设备证书

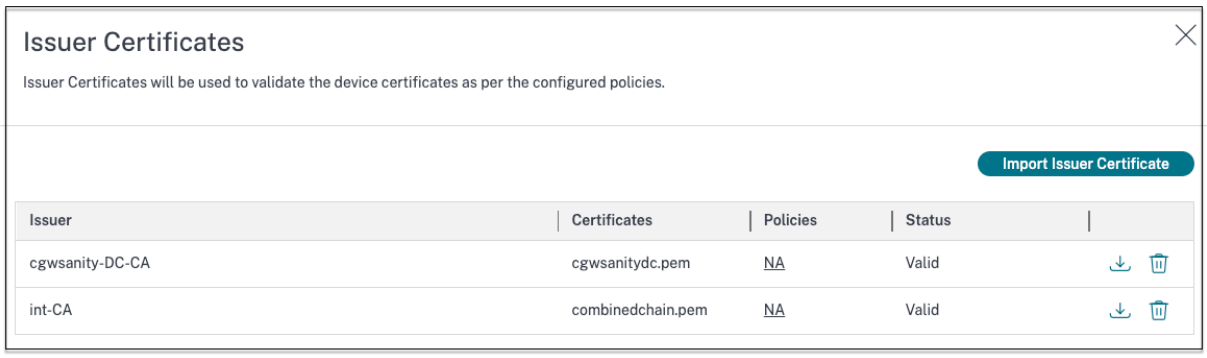
1. 在 Device Posture 主页上单击“设置”。
2. 单击“管理”，然后单击“导入颁发证书”。
3. 在 证书类型中，选择证书类型。仅支持 PEM 类型。
4. 在“证书文件”中，单击“选择证书”以选择颁发者证书。
5. 单击“打开”，然后单击“导入”。



所选证书列在“设置”**>**“颁发者证书”中。您可以导入多个证书。

查看导入的证书

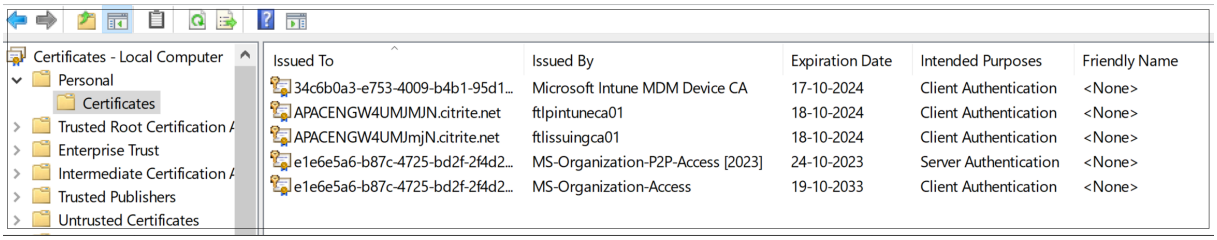
1. 在 Device Posture 主页上单击“设置”。
2. 在“颁发者证书”中，单击“管理”。
3. 颁发者证书页面列出了导入的颁发者证书。



在终端设备上安装设备证书

Windows:

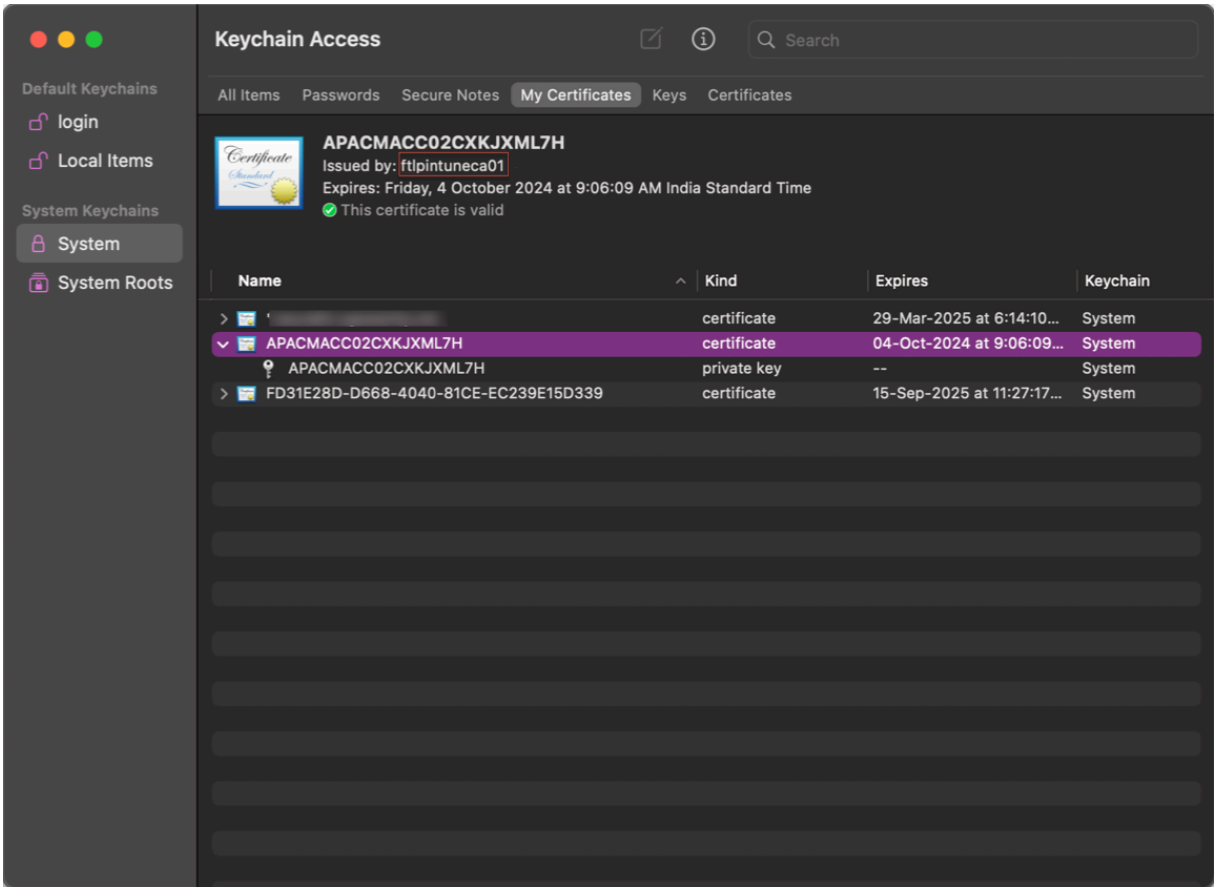
1. 从“开始”菜单中，打开“计算机证书管理器”。
2. 确保证书安装在 `Certificates - Local Computer\Personal\Certificates` 中。
    - 预期目的必须包括客户身份验证。
    - “发行者”列必须与管理员 GUI 上配置的发行者名称相匹配。



macOS:

1. 打开 **Keychain Access**，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。



使用 **Device Posture** 对 **DaaS** 实施智能控制

February 20, 2024

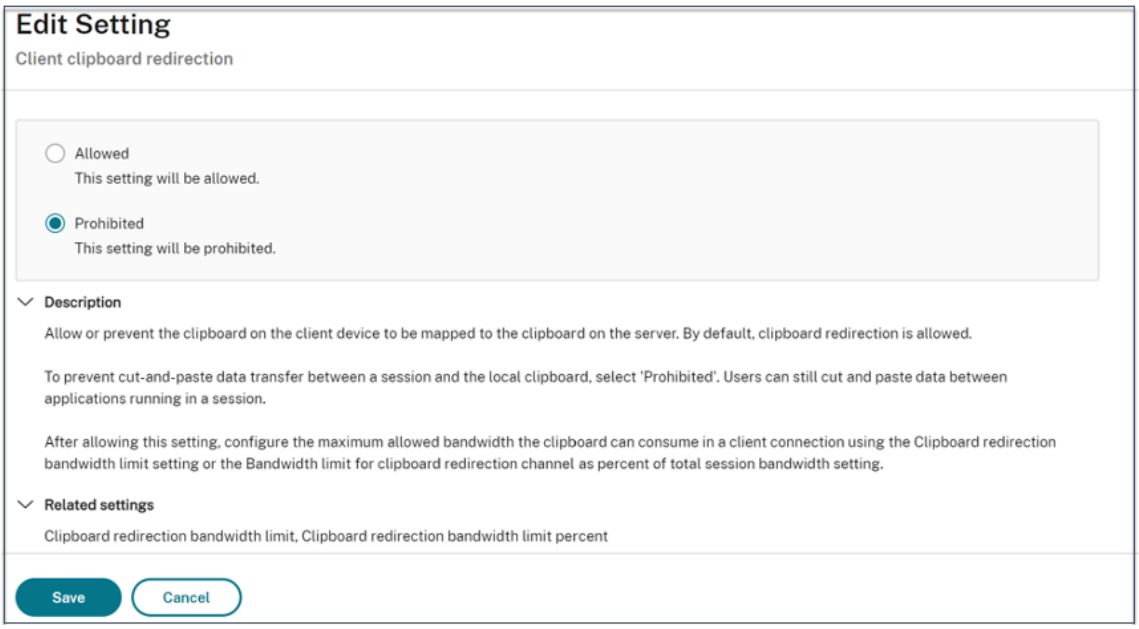
在通过 Citrix Device Posture 服务访问 Citrix 桌面即服务 (DaaS) 资源时，您可以强制执行智能控制。

> 注意：
>
> 这不是详尽的配置，而是有关如何使用 Device Posture 配置 Studio 策略的示例。

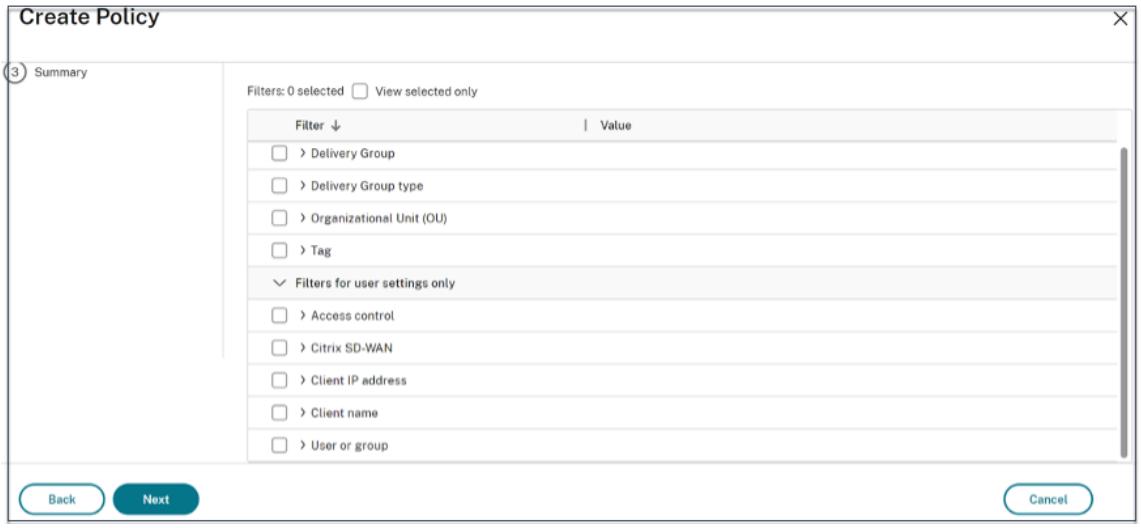
在此示例中，创建了一个使用 Device Posture 服务标签（COMPLIANT 和 NON-COMPLIAN）在 Citrix DaaS 资源上禁用复制粘贴功能的策略。

要在 Citrix DaaS 上为来自 NON-COMPLIANT 设备的用户禁用复制粘贴功能，请执行以下步骤：

1. 在“Citrix DaaS 配置”页面上，单击管理选项卡。
2. 单击策略选项卡。
3. 选择创建策略。
4. 在“选择设置”中，选择“客户端剪贴板重定向”。
5. 在“编辑设置”中，选择“禁止”，然后单击“保存”。

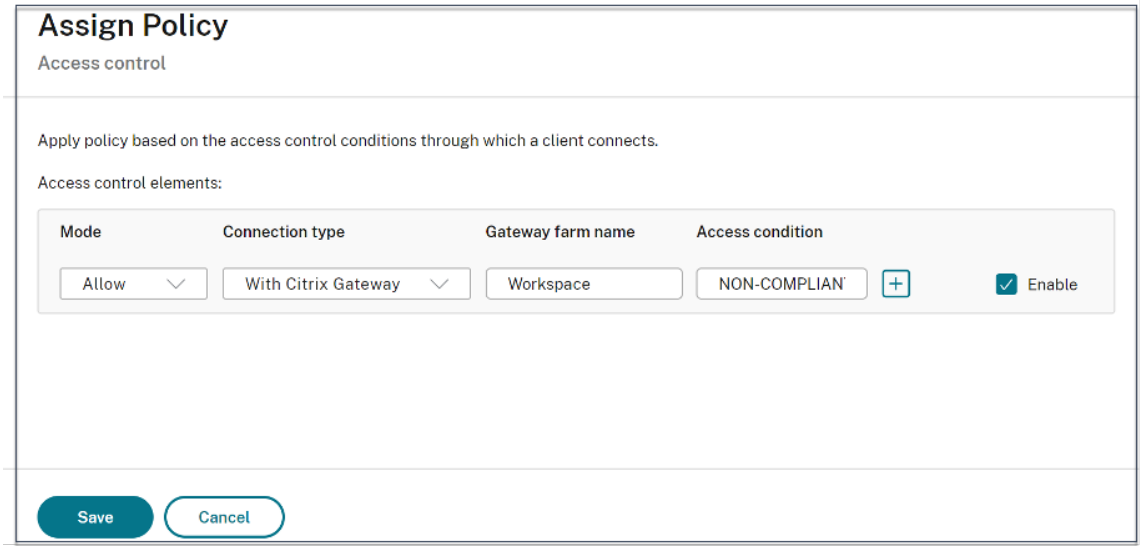


6. 在“用户和计算机”页面中，单击“筛选的用户和计算机”，然后将此策略分配给 访问控制。
7. 转到 仅限用户设置的过滤器，然后选择 访问控制。



8. 在“分配策略”页面中，保留“模式”和“连接类型”的默认设置。

   在 **Gateway** 服务器场名称中，输入 **NON-COMPLIANT**，然后在 访问条件中输入 **NON-COMPLIANT**。



9. 输入策略的名称。考虑根据策略的影响对象或内容来命名策略，例如，限制不合规设备的剪贴板访问权限。提供说明（可选）。
10. 单击“完成”。

> 注意：
>
> 默认情况下，该策略处于禁用状态。启用该策略可以立即将其应用于登录的用户。禁用策略可阻止应用策略。如果您过后必须设定策略的优先级或添加设置，请考虑禁用策略，直至准备好应用此策略。

如何验证策略配置

在广泛实施这些策略之前，请验证您的策略以确保它们按预期运行。在配置示例中：

- 对于来自 COMPLIANT 终端设备的用户，必须枚举 Citrix DaaS 资源，不受复制粘贴限制。
- 对于来自 NON-COMPLIAN 终端设备的用户，必须列举具有复制粘贴限制的 Citrix DaaS 资源。

Device Posture 日志

February 20, 2024

除了与 SaaS/Web 和 TCP/UDP 应用程序相关的日志外，Secure Private Access 服务控制板还会捕获设备状态日志。

要查看设备状态日志，请单击“设备状态日志”选项卡。您可以根据策略结果（合规、不合规和拒绝登录）细化搜索。

有关更多详细信息，请参阅诊断日志。

管理 **Device Posture** 服务的 **Citrix Endpoint Analysis** 客户端

February 20, 2024

Citrix Device Posture 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获得 Citrix DaaS (Virtual Apps and Desktops) 或 Citrix Secure Private Access 资源（SaaS、Web 应用程序、TCP 和 UDP 应用程序）的访问权限。

要在终端设备上运行 Device Posture 扫描，必须在该设备上安装 Citrix EndPoint Analysis (EPA) 客户端，这是一款轻量级应用程序。Device Posture 服务始终使用 Citrix 发布的最新版本的 EPA 客户端运行。

安装 **EPA** 客户端

在运行期间，Device Posture 服务会在运行时提示最终用户下载并安装 EPA 客户端。有关详细信息，请参阅 最终用户流程。
通常，EPA 客户端不需要本地管理员权限即可在端点上下载和安装。但是，要在终端设备上运行设备证书检查扫描，必须安装具有管理员访问权限的 EPA 客户端。有关使用管理员访问权限安装 EPA 客户端的详细信息，请参阅在终端设备上安装设备证书。

升级适用于 **Windows** 的 **EPA** 客户端

当新版本的 EPA 客户端发布时，Windows 版 EPA 客户端在首次安装后默认会升级。自动升级可确保最终用户设备始终在与 Device Posture 服务兼容的最新版本的 EPA 客户端上运行。要进行自动升级，必须以管理员访问权限安装 EPA 客户端。

> 注意：
>
> 自动升级目前处于预览阶段。使用 https://podio.com/webforms/29214695/2384946 注册预览版。

EPA 客户的分布

可以使用全球应用程序配置服务 (GACS) 或与 Citrix Workspace 应用程序安装程序集成的 EPA 进行分发，也可以使用软件部署工具分发 EPA 客户端。

- 与 **Citrix Workspace** 应用程序集成的 **EPA** 客户端（预览版）：EPA 客户端也与 Citrix Workspace 应用程序集成。这种集成使最终用户无需在安装 Citrix Workspace 应用程序后安装 EPA 客户端。
  - 如果终端设备已经安装了 EPA 客户端，并且最终用户安装了 Citrix Workspace 应用程序，则集成的 EPA 客户端不会安装在该设备上。现有的 EPA 客户端用于设备状态检查。
  - 同样，如果最终用户卸载 Citrix Workspace 应用程序，则默认情况下，集成的 EPA 客户端也会从设备中移除。但是，如果未将 EPA 客户端作为集成 Citrix Workspace 应用程序安装的一部分进行安装，则现有 EPA 客户端将保留在设备中。

> 注意：
>
> - 仅在 Windows 平台上支持 EPA 客户端与 Citrix Workspace 应用程序的集成，目前处于预览阶段。使用 https://podio.com/webforms/29219973/2385708 注册预览版。

- 使用 **GACS** 分发客户端：GACS 是 Citrix 提供的解决方案，用于管理客户端代理（插件）的分发。GACS 中提供的自动更新服务可确保终端设备使用最新的 EPA 版本，无需最终用户干预。有关 GACS 的更多信息，请参阅如何使用 Global App Configuration Service?。

> 注意：
>
> - Windows 设备仅支持 GACS，用于分发 EPA 客户端。
> - 要通过 GACS 管理 EPA 客户端，请在终端设备上安装 Citrix Workspace 应用程序 (CWA)。
> - 如果在最终用户设备上以管理员权限安装 CWA，则 GACS 将使用相同的管理员权限安装 EPA 客户端。
> - 如果在最终用户设备上以用户权限安装 CWA，则 GACS 将使用相同的用户权限安装 EPA 客户端。

使用软件部署工具分发客户端：管理员可以通过 Microsoft SCCM 等软件部署工具分发最新的 EPA 客户端。

与 NetScaler 和 Device Posture 一起使用时管理 EPA 客户端

在以下部署中，EPA 客户端可以与 NetScaler 和 Device Posture 一起使用：

- 使用 EPA 进行基于 NetScaler 的自适应身份验证
- 基于 NetScaler 的本地网关，带有 EPA

Device Posture 服务将最新版本的 EPA 客户端推送到终端设备。但是，在 NetScaler 上，管理员可以为网关虚拟服务器上的 EPA 扫描配置以下版本控制：

- 始终：终端设备上的 EPA 客户端和 NetScaler 必须使用相同的版本。
- 必备：终端设备上的 EPA 客户端版本必须在 NetScaler 上配置的范围内。
- 从不：终端设备可以安装任何版本的 EPA 客户端。

有关更多信息，请参阅插件行为。

将 **EPA** 客户端与 **NetScaler** 和 **Device Posture** 一起使用时的注意事项

当 EPA 客户端与 Device Posture 服务和 NetScaler 一起使用时，可能会出现终端设备运行最新的 EPA 客户端版本，而 NetScaler 在不同版本的 EPA 客户端上运行的情况。这可能会导致 NetScaler 和终端设备上的 EPA 客户端版本不匹配。因此，NetScaler 可能会提示最终用户安装 NetScaler 上存在的 EPA 客户端版本。为避免这种冲突，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，则建议您在 NetScaler 上禁用 EPA 客户端的版本控制。这样做是为了确保 GACS 或 Device Posture 服务不会将最新版本的 EPA 客户端推送到终端设备。
- 可以使用 CLI 或 GUI 将 EPA 版本控制设置为“从不”。NetScaler 13.x 及更高版本支持这些配置更改。
  - CLI：使用自适应身份验证和本地身份验证虚拟服务器的 CLI 命令。
  - GUI：使用本地网关虚拟服务器的 GUI。有关详细信息，请参阅 Citrix Secure Access 客户端的控制升级。

CLI 命令示例：

```
1 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:Always;vpn_linux:Always;""
2
3 add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("
     pluginlist.xml")" <rewrite_action_name>
4
5 bind authentication vserver <Authentication_Vserver_Name> -policy <
     rewrite_action_policy> -priority 10 -type RESPONSE
6 <!--NeedCopy-->
```

数据治理

February 20, 2024

本主题提供有关 Device Posture 服务收集、存储和保留日志的信息。定义部分 中未定义的任何大写术语均具有Citrix 最终用户服务协议中指定的含义。

数据驻留

Citrix Device Posture 客户内容数据位于 AWS 和 Azure 云服务中。为了实现可用性和冗余，它们被复制到以下区域：

- AWS
  - 美国东部
  - 印度西部
  - 欧洲（法兰克福）
- Azure
  - 美国西部
  - 西欧
  - 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的地。

- 用于系统监视和调试日志的 Splunk 服务，仅在美国提供。
- 有关诊断和用户访问日志的 Citrix Analytics Service，请参阅 Citrix Analytics 服务数据治理 了解更多信息。
- 用于管理员审核日志的 Citrix Cloud 系统日志服务。有关详细信息，请参阅 Citrix Cloud 服务客户内容和日志处理以及地理注意事项。

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。以下客户内容是根据 Device Posture 策略配置和平台收集的：

- 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
- 注册表详情
- Windows 安装更新详细信息
- 上次的 Windows 更新详细信息
- 文件系统 - 文件名、文件哈希值和修改时间
- 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）
- Device Posture 扫描输出
- 端点设备的公用 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的地。

数据控制

Citrix Device Posture 服务目前不为客户提供关闭发送日志或阻止全局复制客户内容的选项。

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。

日志目标维护其特定于服务的数据保留策略。

- 有关详细信息，请参阅 数据治理 ，了解 Analytics 日志的保留策略。
- Splunk 日志将被存档，并在 90 天后最终删除。

数据导出

不同类型的日志有不同的数据导出选项。

- 管理员审核日志可从 Citrix Cloud 系统日志控制台访问。
- Device Posture 服务诊断日志可以从 Citrix Analytics 服务或 Secure Private Access 服务控制板导出为 CSV 文件。

定义

- 客户内容是指上载到客户帐户以在客户环境中存储或数据的任何数据，Citrix 有权访问该客户环境以执行服务。
- 日志是指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性和支持的记录。
- 服务意味着前面为了 Citrix Analytics 的目的概述的 Citrix Cloud 服务。