Device Posture

Machine translated content

Disclaimer

Contents

新增功能

June 19, 2024

29 May 2024

- 测试模式下 **Device Posture** 服务的可用性 **-** 预览版

  Device Posture 服务也可在测试模式下使用，在该模式下，管理员可以在生产环境中启用 Device Posture 服务之前对其进行测试。这使管理员能够分析设备状态扫描对最终用户设备的影响，然后在将其启用到生产环境之前相应地规划操作方案。有关详细信息，请参阅测试模式下的 Device Posture 服务 - 预览版。

- 定期扫描设备 **-** 预览版

  现在，您可以启用 Windows 设备的定期扫描，每隔 30 分钟扫描一次已配置的检查。有关详细信息，请参阅定期扫描设备 - 预览版。

14 May 2024

- 跳过设备状态检查

  管理员可以允许最终用户跳过其设备上的设备状态检查。有关详细信息，请参阅跳过设备状态检查。

- **Device Posture** 控制板

  Device Posture 服务门户现在有一个控制板，用于监视和故障排除日志。管理员现在可以使用此控制板进行监视和故障排除。有关详细信息，请参阅 Device Posture 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正式推出。有关详细信息，请参阅 Device Posture 支持的扫描。

- 自定义消息的普遍可用性

  访问被拒绝时添加自定义消息的选项现已正式可用。有关详细信息，请参阅访问被拒绝场景的自定义消息。

2024 年 3 月 26 日

- 自定义工作区 **URL** 支持

  Device Posture 服务现在支持自定义工作区 URL。除了 cloud.com URL 外，您还可以使用自己拥有的 URL 来访问工作区。确保您允许从您的网络访问 citrix.com。有关自定义域的详细信息，请参阅配置自定义域。

2024 年 2 月 12 日

- 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 Device Posture 支持的扫描。

2024 年 1 月 23 日

- 使用 **Device Posture** 服务进行设备证书检查的正式可用性

  使用 Device Posture 服务进行设备证书检查现已正式推出。有关详细信息，请参阅使用 Device Posture 服务检查设备证书。

- **Device Posture** 服务预览功能

  Device Posture 服务现在支持以下检查：

  - IGEL 平台现在支持 Device Posture 服务。
  - Device Posture 服务现在支持地理定位和网络位置检查。

  有关详细信息，请参阅 Device Posture。

2023 年 9 月 11 日

- **Device Posture** 与 **Microsoft Intune** 集成的正式发布版本

  Device Posture 与 Microsoft Intune 集成现已正式上市。有关详细信息，请参阅 Microsoft Intune 与 Device Posture 集成。

2023 年 8 月 30 日

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

  EPA 客户端可以与 NetScaler 和 Device Posture 一起使用。与 NetScaler 和 Device Posture 一起使用时，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 Device Posture 服务的 Citrix Endpoint Analysis 客户端。

2023 年 8 月 28 日

- **iOS** 平台上的 **Device Posture** 服务支持 - 预览版

  iOS 平台现在支持 Device Posture 服务。有关详细信息，请参阅 Device Posture。

2023 年 8 月 22 日

- 使用 **Citrix Device Posture** 服务检查设备证书 **-** 预览版

  Citrix Device Posture 服务现在可以通过对照公司证书颁发机构检查终端设备的证书来确定终端设备是否可信，从而启用对 Citrix DaaS 和 Secure Private Access 资源的情境访问（智能访问）。有关详细信息，请参阅使用 Device Posture 服务检查设备证书。

2023 年 8 月 17 日

- **Citrix DaaS Monitor** 上的 **Device Posture** 事件

  现在可以在 DaaS Monitor 上搜索 Device Posture 服务事件和监视日志。有关详细信息，请参阅 Citrix DaaS Monitor 上的 Device Posture 事件。

2023 年 1 月 23 日

- **Device Posture** 服务

  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。有关详细信息，请参阅 Device Posture。

  [AAUTH-90]

- **Microsoft Endpoint Manager** 与 **Device Posture** 集成

  除了 Device Posture 服务提供的本机扫描外，Device Posture 服务还可以与其他第三方解决方案集成。Device Posture 与 Windows 和 macOS 上的 Microsoft Endpoint Manager (MEM) 集成在一起。有关详细信息，请参阅 Microsoft Endpoint Manager 与 Device Posture 集成。

  [ACS-1399]

测试模式下的 **Device Posture** 服务 **-** 预览版

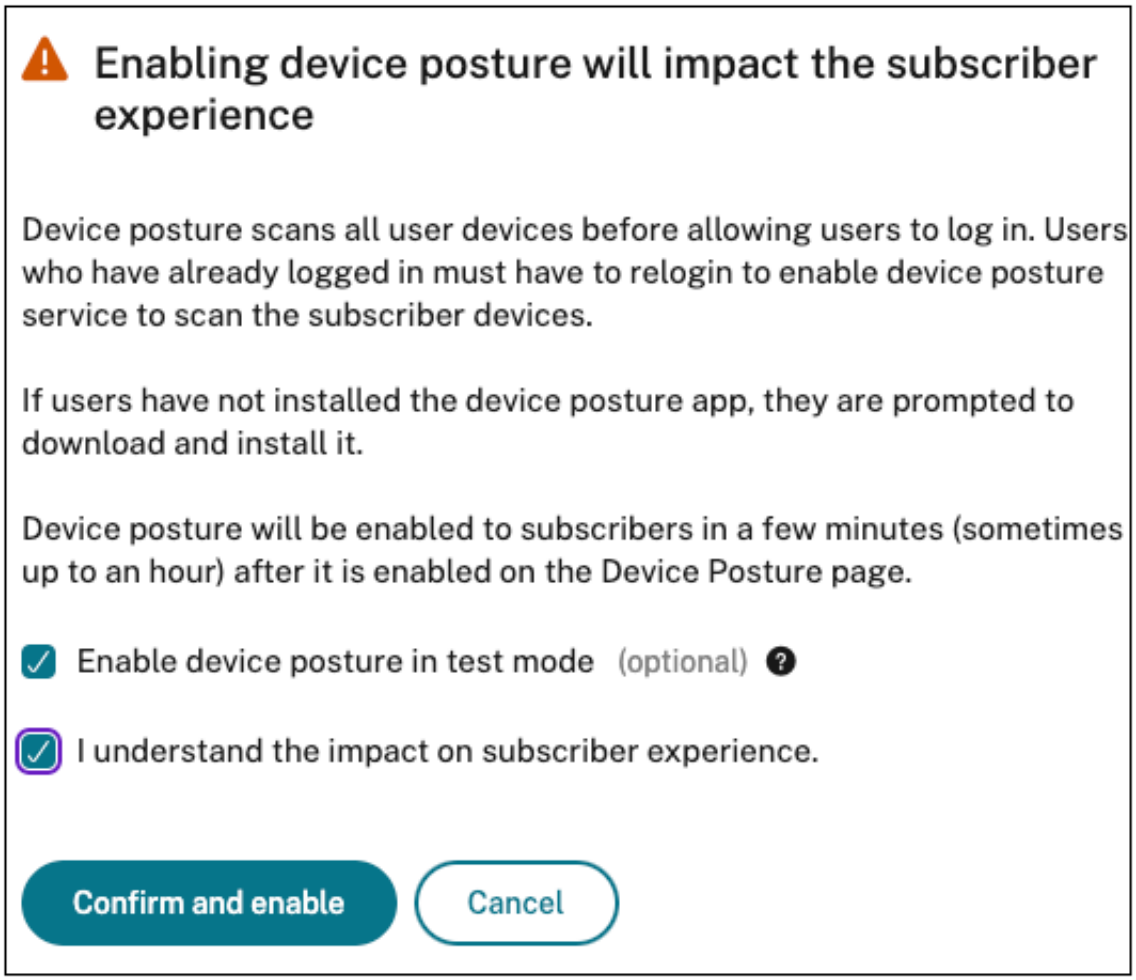
June 19, 2024

Device Posture 服务也可在测试模式下使用，在该模式下，管理员可以在生产环境中启用 Device Posture 服务之前对其进行测试。这使管理员能够分析设备状态扫描对最终用户设备的影响，然后在将其启用到生产环境之前相应地规划操作方案。测试模式下的 Device Posture 服务收集最终用户设备的数据，并将设备分为三类，即合规、不合规和拒绝。但是，这种分类不强制对最终用户设备执行任何操作。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 Device Posture 控制板上查看这些数据。如果需要，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。如果终端设备未安装 EPA 客户端，Device Posture 服务会向最终用户显示一个下载页面，供其下载和安装客户端，否则最终用户无法登录。

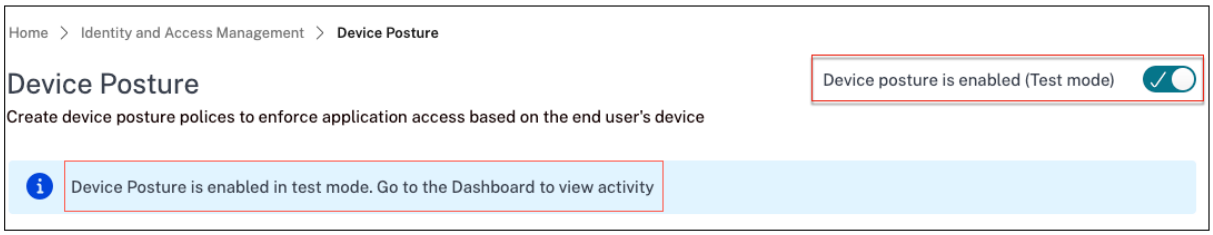
启用测试模式

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 **Device Posture** 选项卡，然后单击管理。
3. 滑动 **Device Posture** 已禁用切换开关打开。
4. 在确认窗口中，选中两个复选框。



5. 单击确认并启用。

在测试模式下启用 Device Posture 服务时，Device Posture 主页会显示一条注释来确认这一点。



管理员可以配置设备状态扫描的策略和规则。有关详细信息，请参阅“配置 Device Posture”。根据扫描结果，最终用户设备被分为合规、不合规和拒绝。管理员可以在控制板上查看这些数据。

在控制板上查看测试模式活动

1. 单击“Device Posture”页面上的“控制面板”选项卡。

   诊断日志图表显示归类为合规、不合规和登录被拒绝的设备数量。

2. 要查看详细信息，请单击“查看更多”链接。

测试模式诊断

管理员可以从用户界面下载监视日志。

在生产环境中启用测试模式

如果 Device Posture 服务已在生产环境中启用，请执行以下步骤以启用测试模式：

1. 在主页上，滑动“**Device Posture** 已启用”切换开关。
2. 选择“我知道所有设备状态检查都将被禁用”。
3. 单击确认并禁用。
4. 现在，通过滑动“**Device Posture** 已禁用”切换开关“打开”来启用设备状态。
5. 在确认窗口中，选择以下两个选项。

   - 在测试模式下启用 **Device Posture**
   - 我了解对订阅者体验的影响

6. 单击确认并启用。

CrowdStrike 与 Device Posture 集成

June 19, 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。

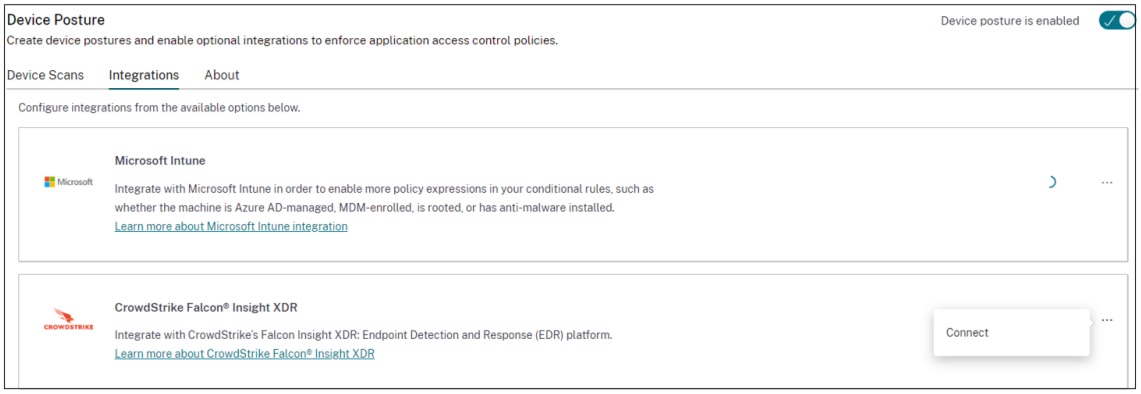
步骤 **1**：在 Citrix Device Posture 服务和 CrowdStrike ZTA 服务之间建立信任。这是一次性操作。

步骤 **2**：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。

步骤 **1**：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。

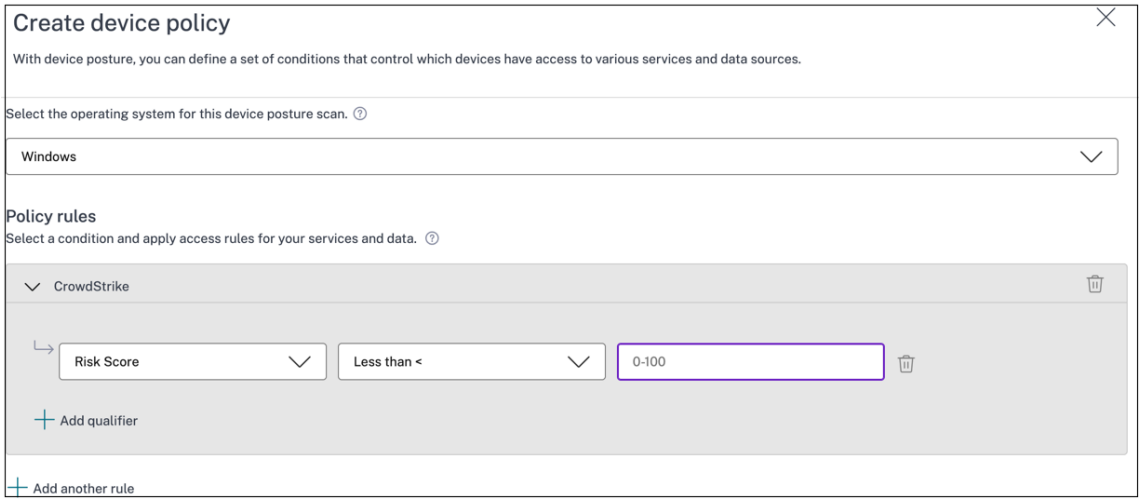
状态从“未配置”变为“已配置”后，即认为集成成功。

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”。

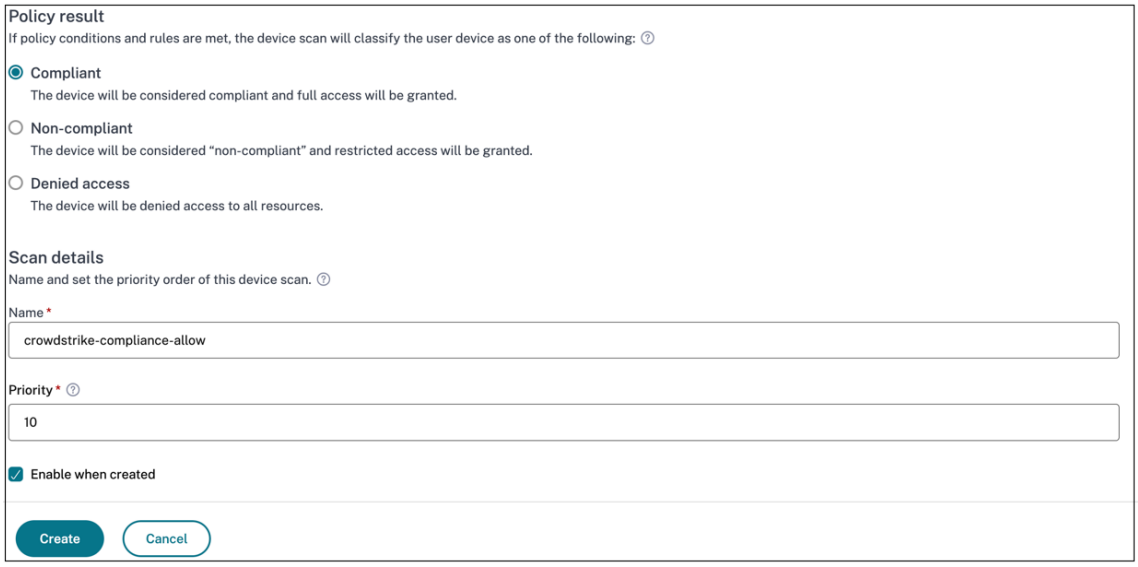


2. 选择创建此策略的平台。
3. 在“策略规则”中，选择 **CrowdStrike**。
4. 对于 风险评分 限定词，选择条件，然后输入风险分数。
5. 单击 **+** 添加一个限定符，用于检查 CrowdStrike Falcon 传感器是否在运行。

> 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

June 19, 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

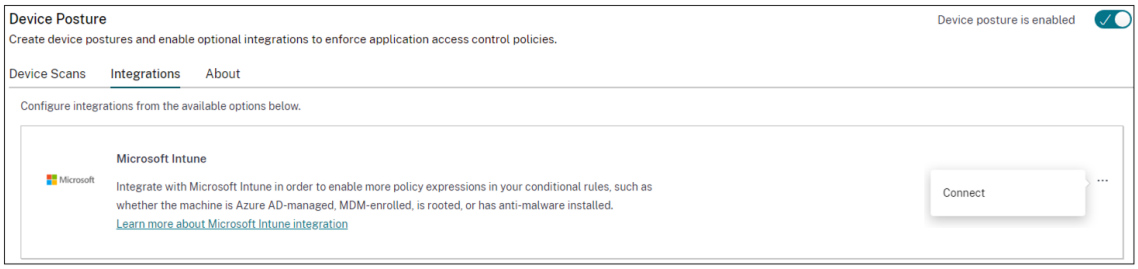
Intune 集成配置是一个分为两个步骤的过程。

步骤 **1**：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。

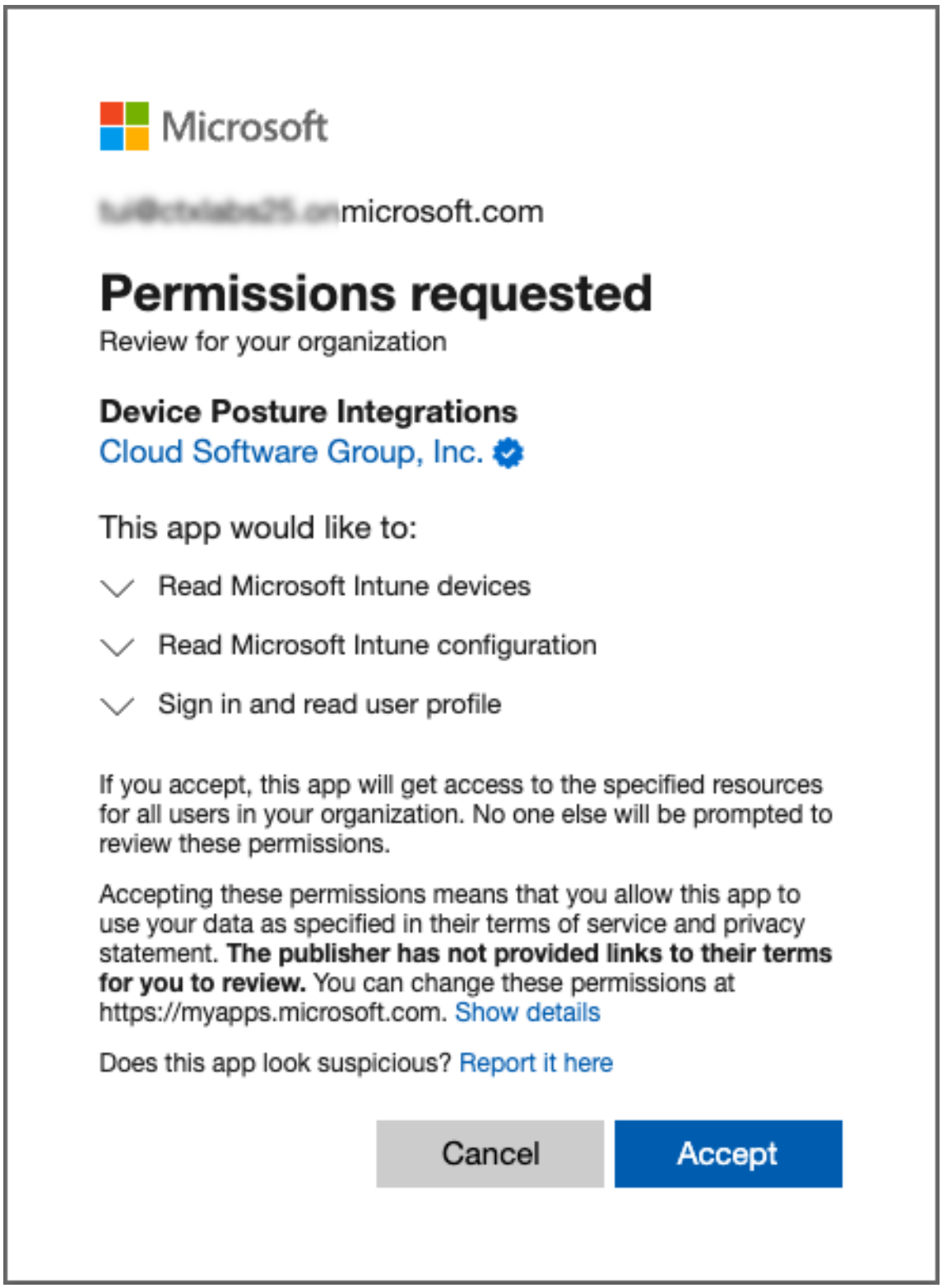
步骤 **2**：配置策略以使用 Microsoft Intune 信息。

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。



下表列出了与 Device Posture 服务集成的 Microsoft Intune API 权限。

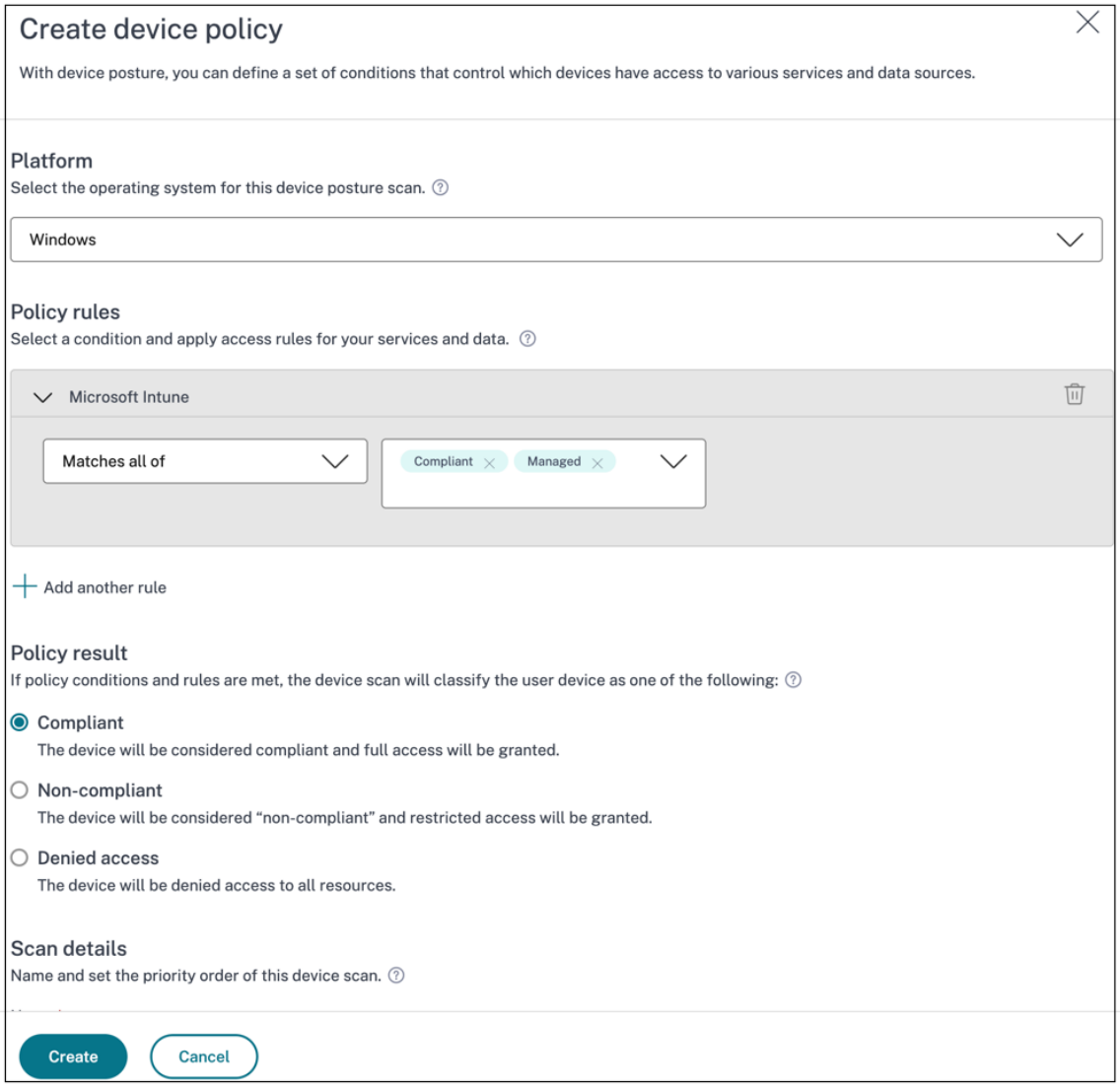
API 名称	声明值	权限名称	类型
Microsoft Graph	DeviceManagementManagedDevices.ReadWrite.All	读取和写入 Microsoft Intune 设备	应用程序
Microsoft Graph	DeviceManagementServiceConfig.ReadWrite.All	读取和写入 Microsoft Intune 设备	应用程序

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

June 19, 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。

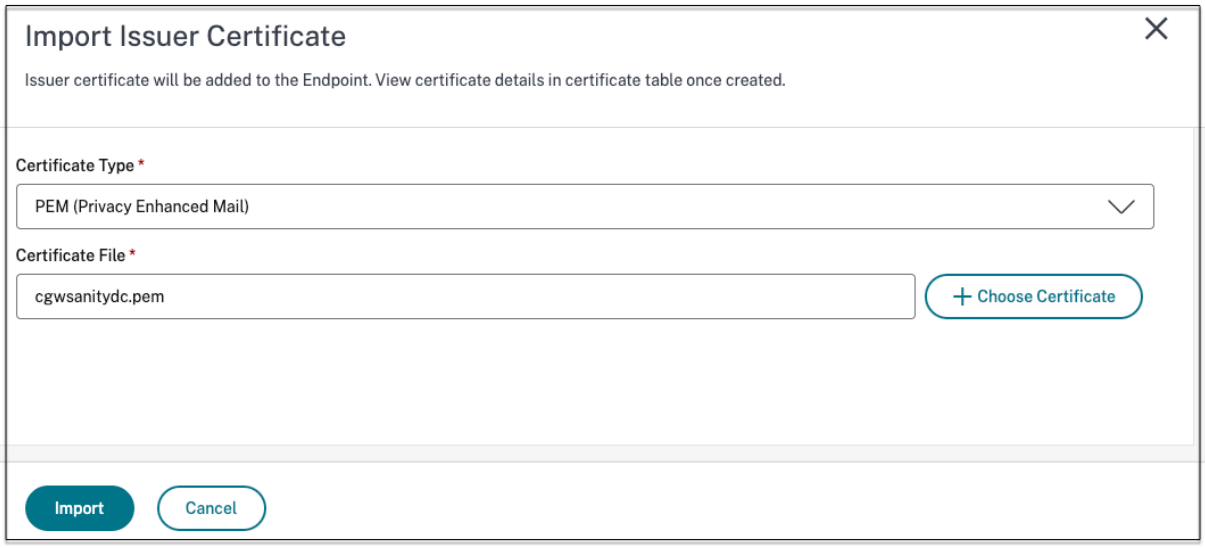
> 注意事项：
>
> - Device Posture 服务仅支持 PEM 颁发者证书类型。
> - 要在 Windows 上进行设备证书检查，必须使用管理权限安装终端设备上的 EPA 客户端。对于其他支票，您不需要本地管理权限。有关支持的扫描的详细信息，请参阅 Device Posture 支持的扫描。
> - 要在 Windows 上安装具有管理权限的 EPA 客户端，请在下载 EPA 客户端插件的位置运行以下命令。
>
>   ```
>   msiexec /i epasetup.msi
>   ```
>
> - 使用 Device Posture 服务进行的设备证书检查不支持证书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

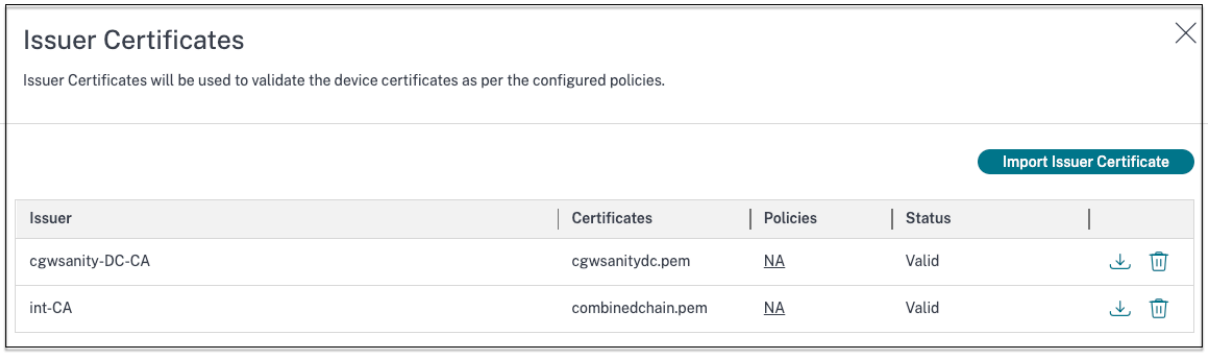
1. 在 Device Posture 主页上单击“设置”。
2. 单击“管理”，然后单击“导入颁发证书”。
3. 在 证书类型中，选择证书类型。仅支持 PEM 类型。
4. 在“证书文件”中，单击“选择证书”以选择颁发者证书。
5. 单击“打开”，然后单击“导入”。



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

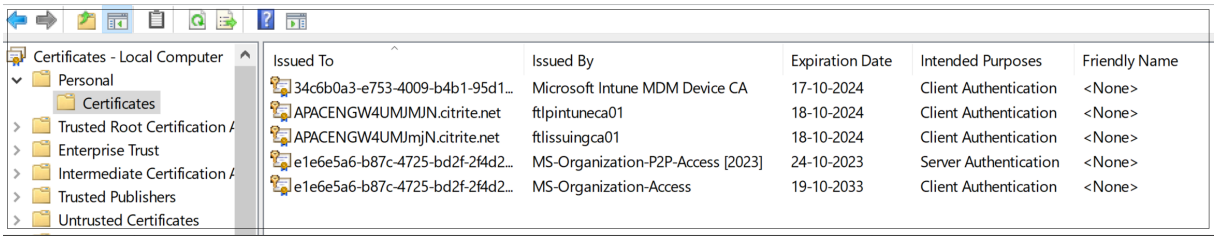
1. 在 Device Posture 主页上单击“设置”。
2. 在“颁发者证书”中，单击“管理”。
3. 颁发者证书页面列出了导入的颁发者证书。



在终端设备上安装设备证书

Windows:

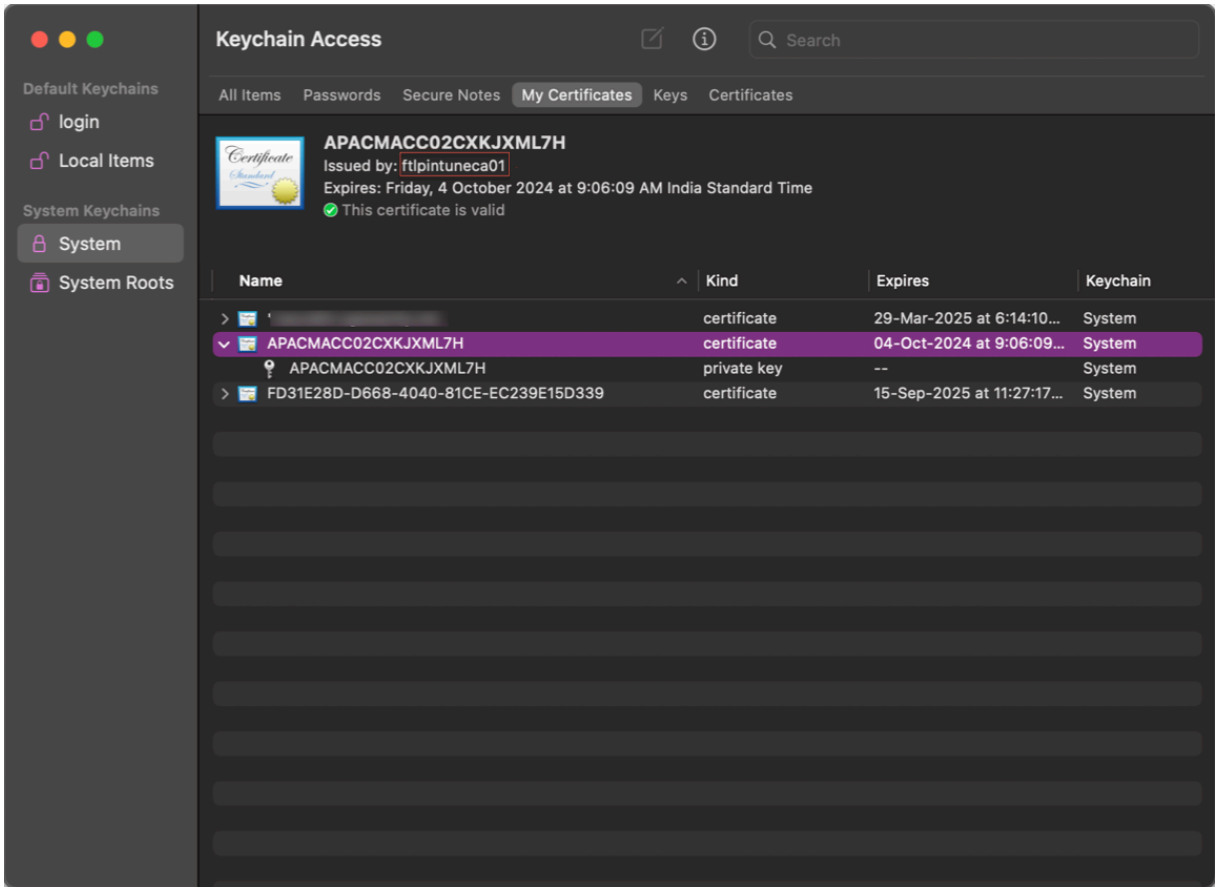
1. 从“开始”菜单中，打开“计算机证书管理器”。
2. 确保证书安装在 `Certificates - Local Computer\Personal\Certificates` 中。
   - 预期目的必须包括客户身份验证。
   - “发行者”列必须与管理员 GUI 上配置的发行者名称相匹配。



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。

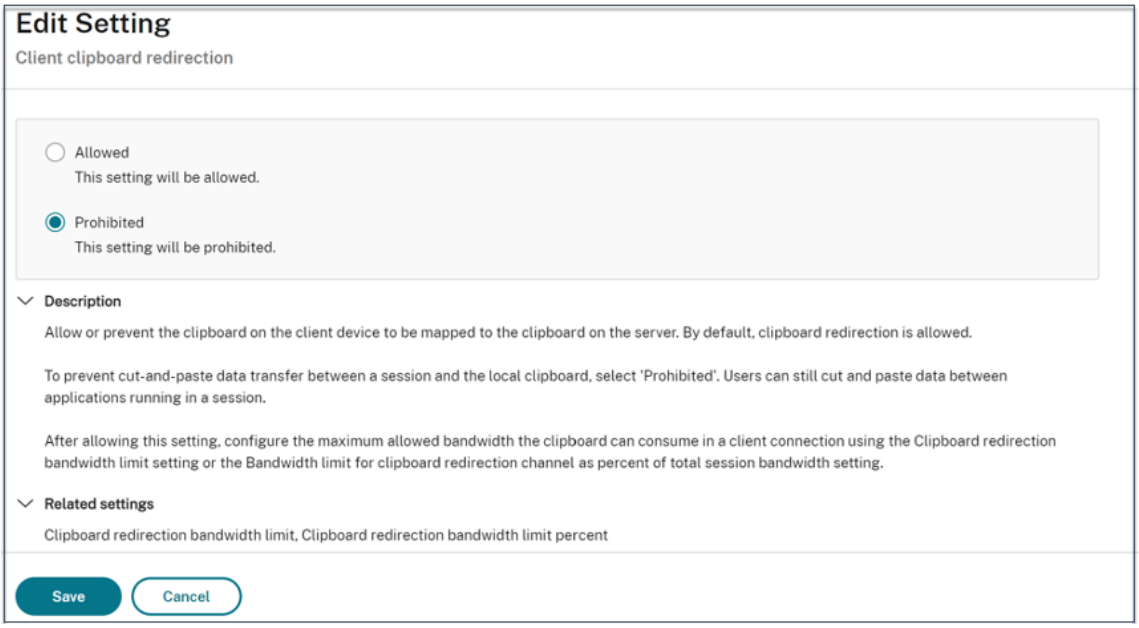
> 注意：
>
> 这不是详尽的配置，而是有关如何使用 Device Posture 配置 Studio 策略的示例。

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。

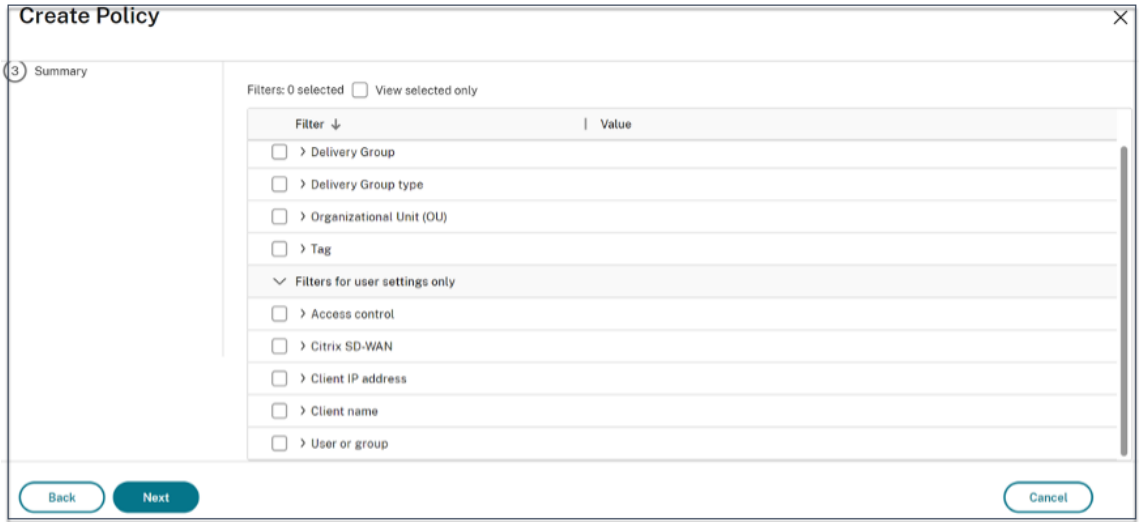
要在 Citrix DaaS 上为来自 NON-COMPLIANT 设备的用户禁用复制粘贴功能，请执行以下步骤：

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”。

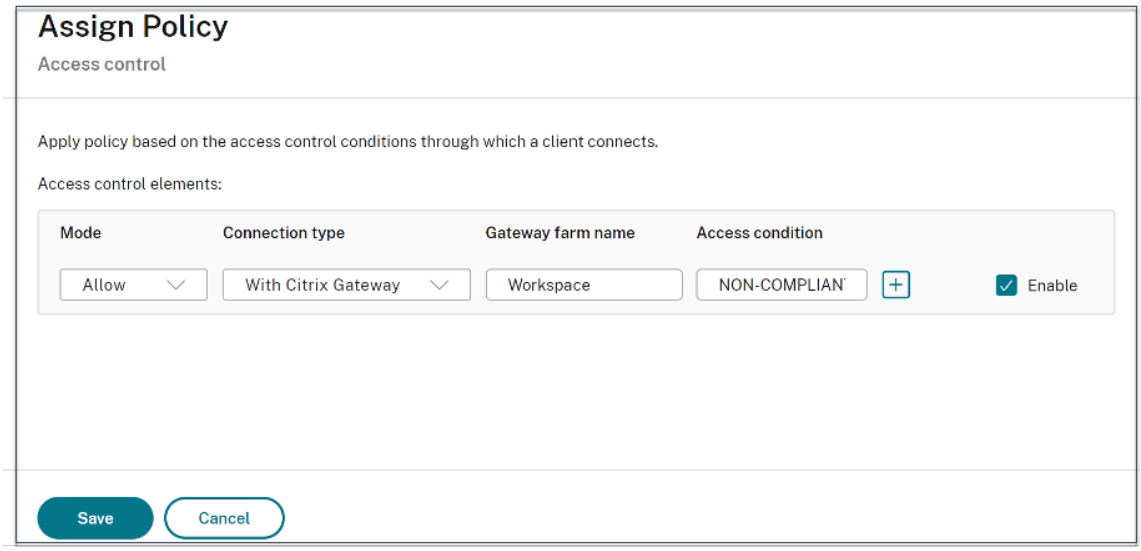


6. 在“用户和计算机”页面中，单击“筛选的用户和计算机”，然后将此策略分配给 访问控制。
7. 转到 仅限用户设置的过滤器，然后选择 访问控制。



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。

监视和故障排除

June 19, 2024

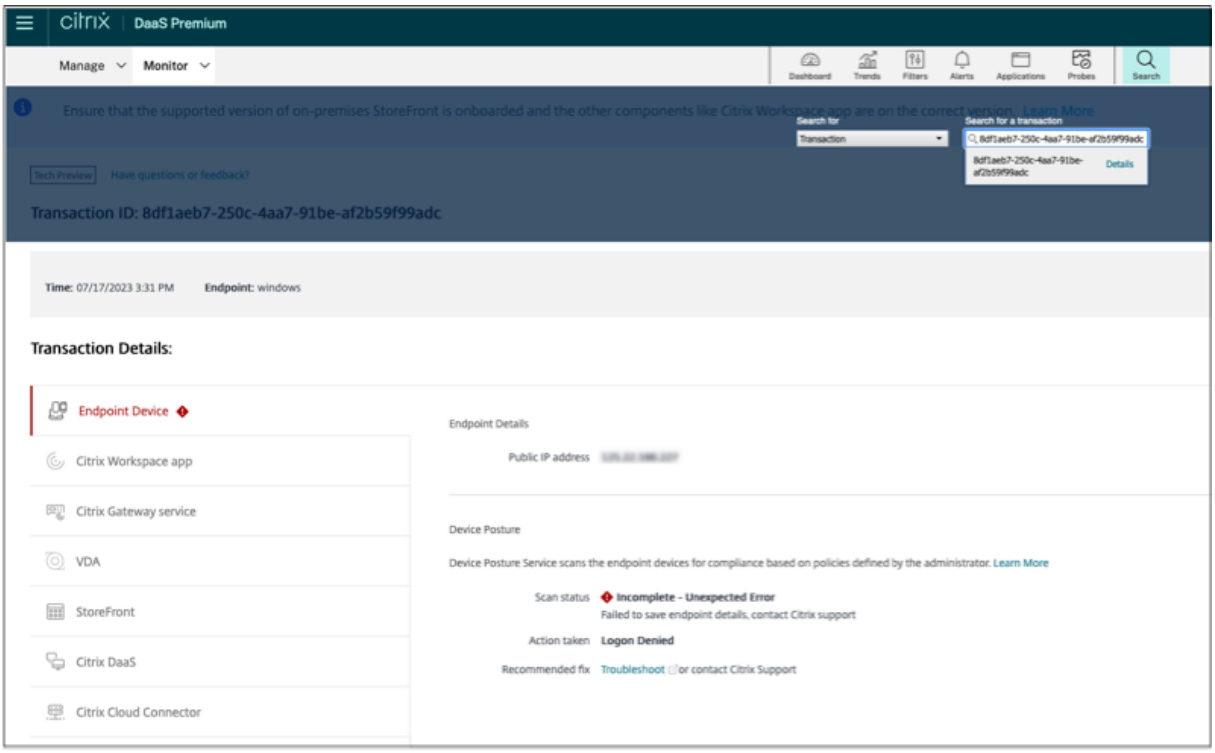
可以在两个位置查看 Device Posture 事件日志：

- 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。

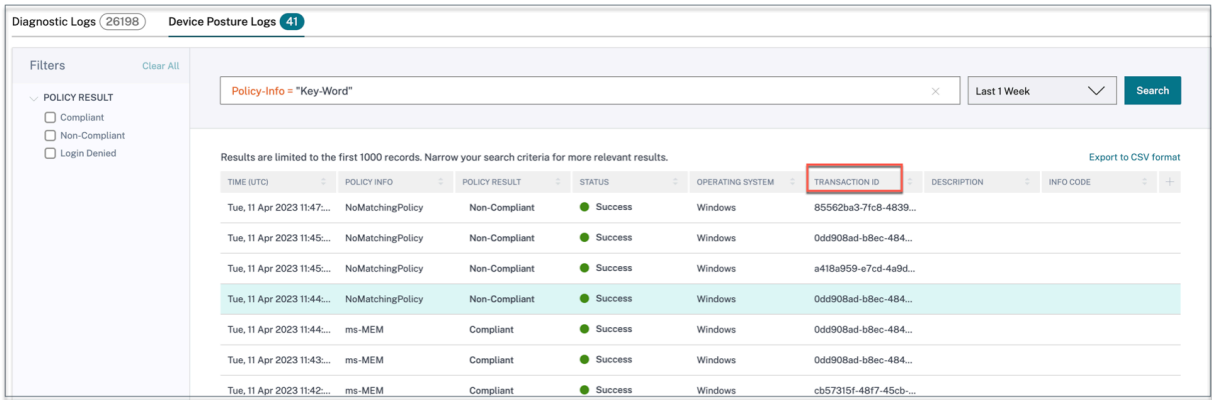
1. 从最终用户设备复制失败或访问被拒绝的会话的交易 ID。
2. 登录 Citrix Cloud。
3. 在 DaaS 磁贴上，单击“管理”，然后单击“监视”选项卡。
   在监视用户界面中，搜索 32 位事务 ID，然后单击“详细信息”。



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”，然后单击“控制面板”。
3. 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

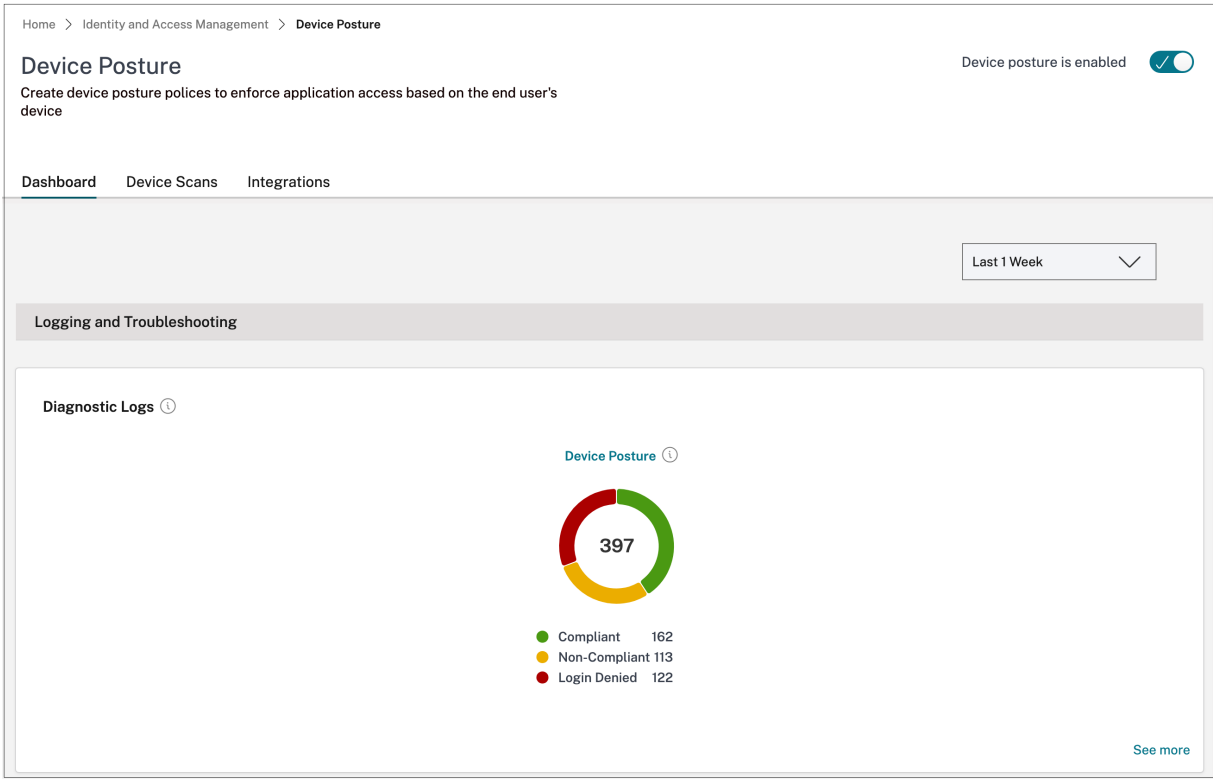
可以在 Citrix Monitor 和 Secure Private Access 控制面板上查看以下与 Device Posture 服务相关的日志。对于所有这些日志，建议您联系 Citrix 支持部门寻求解决方案。

- 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

Device Posture 日志

June 19, 2024

您可以使用 Device Posture 服务门户中的控制板进行监视和故障排除。要查看 Device Posture 服务控制板，请单击 Device Posture 主页上的控制板选项卡。日志记录和故障排除部分显示与 Device Posture 服务相关的诊断日志。您可以单击查看更多链接以查看日志的详细信息。您可以根据策略结果（合规、不合规和拒绝登录）细化搜索。



> 注意：
>
> Device Posture 日志也可以在 Secure Private Access 服务控制板中捕获。要查看设备状态日志，请单击“**Device Posture** 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

June 19, 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。有关安装具有管理员访问权限的 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。

- **EPA** 客户端安装程序与 **Citrix Workspace** 应用程序集成： EPA 客户端安装程序与适用于 Windows 的 Citrix Workspace 应用程序 2402 LTSR 集成。这种集成使最终用户无需在安装 Citrix Workspace 应用程序后单独安装 EPA 客户端。

  要将 EPA 客户端作为 Citrix Workspace 应用程序的一部分进行安装，请使用命令行选项 `InstallEPAClient`。 例如，`./CitrixworkspaceApp.exe InstallEPAClient`。

  > 注意：
  >
  > - 默认情况下，作为 Citrix Workspace 应用程序一部分的 EPA 客户端安装处于禁用状态。必须使用命令行选项 `InstallEPAClient` 明确将其启用。
  > - 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，则现有 EPA 客户端将升级。
  > - 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。
  > - 与 Citrix Workspace 应用程序集成的 EPA 客户端安装程序也可以与 NetScaler 一起使用。有关详细信息，请参阅与 NetScaler 和 Device Posture 一起使用时管理 EPA 客户端。

- 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，请参阅如何使用全局应用程序配置服务。

> 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：


```
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;""

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
<!--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。