



Device Posture

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Cloud Software Group 文档内容采用了机器翻译，仅供您参考。Cloud Software Group 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Cloud Software Group 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Cloud Software Group 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Cloud Software Group 不承担任何责任。

Contents

新增功能	2
设备状态服务处于测试模式	4
监视和故障排除	7
Device Posture 日志	9
管理设备状态服务的 Citrix Endpoint Analysis 客户端	10
数据治理	13

新增功能

October 21, 2024

29 May 2024

- 测试模式下设备状态服务的可用性

Device Posture 服务在测试模式下也可用，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态势扫描对最终用户设备的影响，然后在生产环境中启用设备之前相应地规划其操作过程。有关详细信息，请参阅 [测试模式下的设备状态服务](#)。

- ** 定期扫描设备

现在，您可以启用每 30 分钟对 Windows 设备进行一次定期扫描配置的检查。有关详细信息，请参阅 [定期扫描设备](#)。

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](#)。

- 设备状态控制面板

Device Posture 服务门户现在有一个控制面板，用于监控日志和排查日志问题。管理员现在可以使用此控制面板进行监控和故障排除。有关详细信息，请参阅 [设备状态日志](#)。

- 浏览器和防病毒检查的正式发布

浏览器和防病毒检查现已正式发布。有关详细信息，请参阅 [设备状态支持的扫描](#)。

- 自定义消息的正式发布

在访问被拒绝时添加自定义消息的选项现已正式发布。有关详细信息，请参阅 [针对拒绝访问场景的自定义消息](#)。

26 三月 2024

- 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 之外，您还可以使用您拥有的 URL 来访问 workspace。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](#)。

12 二月 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 [设备状态支持的扫描](#)。

23 一月 2024

- 使用 **Device Posture** 服务进行设备证书检查的正式发布

使用 Device Posture 服务进行设备证书检查功能现已正式发布。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：

- IGEL 平台现在支持 Device Posture 服务。
- 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 [设备状态](#)。

11 九月 2023

- **Device Posture** 与 **Microsoft Intune** 的集成正式发布

Device Posture 与 Microsoft Intune 的集成现已正式发布。有关详细信息，请参阅 [Microsoft Intune 与 Device Posture 集成](#)。

30 八月 2023

- 管理适用于设备状态服务的 **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来管理 EPA 客户端。有关详细信息，请参阅 [管理适用于设备状态服务的 Citrix Endpoint Analysis 客户端](#)。

28 八月 2023

- **iOS** 平台上的设备状态服务支持 - 预览版

Device Posture 服务现在在 iOS 平台上受支持。有关详细信息，请参阅 [设备状态](#)。

22 八月 2023

- 使用 **Citrix Device Posture** 服务进行设备证书检查 - 预览版

Citrix Device Posture 服务现在可以启用对 Citrix DaaS 和 Secure Private Access 资源的上下文访问（智能访问），方法是根据公司证书颁发机构检查终端设备的证书，以确定终端设备是否可信。有关详细信息，请参阅 [设备证书检查](#)。

17 八月 2023

- **Citrix DaaS Monitor** 上的设备状态事件

现在可以在 DaaS Monitor 上搜索设备状态服务事件和监控日志。有关详细信息，请参阅 [Citrix DaaS Monitor 上的设备状态事件](#)。

23 一月 2023

- 设备状态服务

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 [设备状态](#)。

[AAUTH-90]

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

除了 Device Posture 服务提供的本机扫描之外，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。有关详细信息，请参阅 [Microsoft Endpoint Manager 与 Device Posture 集成](#)。

[ACS-1399]

设备状态服务处于测试模式

October 21, 2024


Device Posture 服务在测试模式下也可用，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态势扫描对最终用户设备的影响，然后在生产环境中启用设备之前相应地规划其操作过程。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，此分类不会对最终用户设备强制实施任何操作。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 控制面板上查看此数据。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。如果终端设备未安装 EPA 客户端，Device Posture 服务会向最终用户提供一个下载页面，用于下载和安装客户端，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 设备状态 Tab 键，然后单击 管理。
3. 滑动 设备状态已禁用 切换开关 ON。
4. 在确认窗口中，选中两个复选框。

**Enabling device posture will impact the subscriber experience**

Device posture scans all user devices before allowing users to log in. Users who have already logged in must have to relogin to enable device posture service to scan the subscriber devices.

If users have not installed the device posture app, they are prompted to download and install it.

Device posture will be enabled to subscribers in a few minutes (sometimes up to an hour) after it is enabled on the Device Posture page.

☒ Enable device posture in test mode (optional) ?

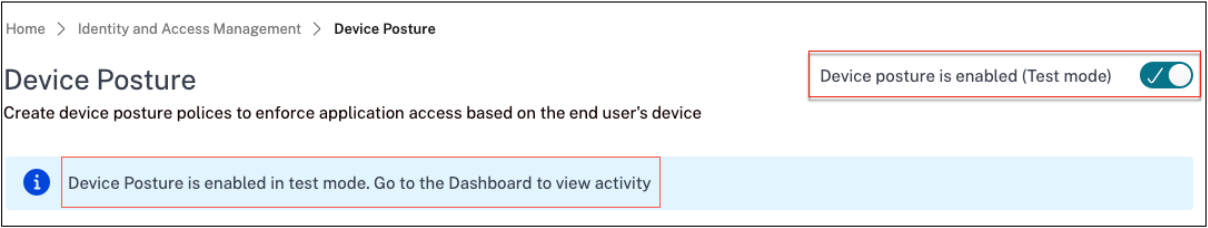
☒ I understand the impact on subscriber experience.

Confirm and enableCancel

5. 点击 确认并启用。

在测试模式下启用 Device Posture 服务时，Device Posture 主页会显示一条确认相同的注释。

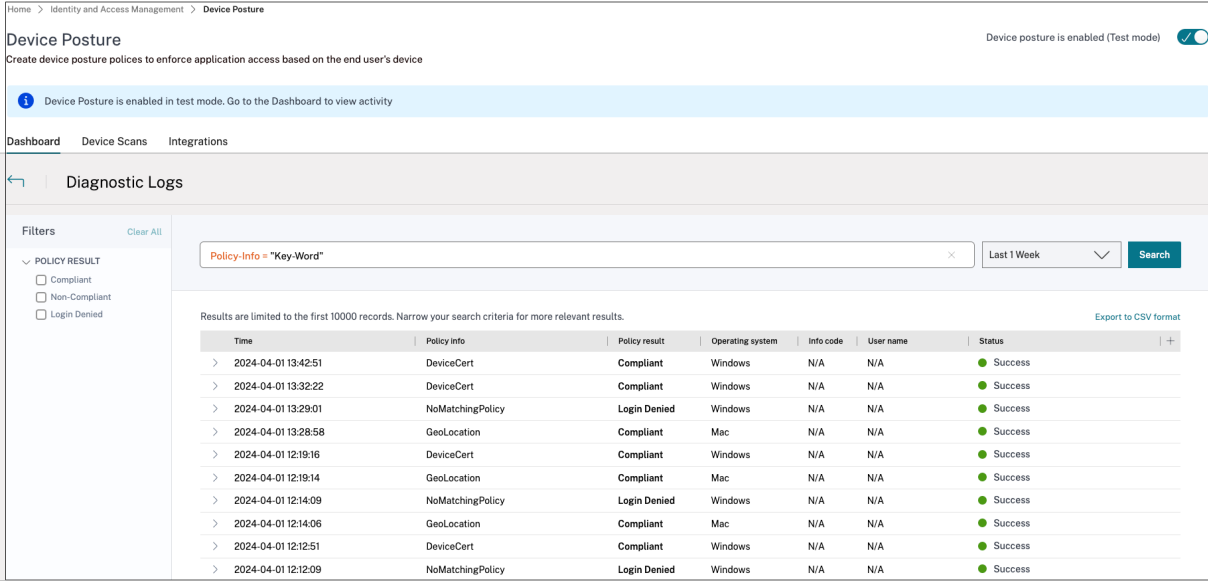
Device Posture



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，请参阅配置设备状态。根据扫描结果，最终用户设备分为 Compliant（合规）、Non-compliant（不合规）和 Denied（被拒绝）。管理员可以在控制面板上查看此数据。

在控制面板上查看测试模式活动

- 1. 单击 挡泥板 选项卡。
这 诊断日志 图表显示分类为合规、不合规和登录被拒绝的设备数量。
- 2. 要查看详细信息，请单击 查看更多 链接。



管理员可以从 UI 下载监控日志。

在生产环境中启用测试模式

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

- 1. 在主页上，滑动 已启用设备状态 切换开关 OFF。
- 2. 选择 我了解所有设备状态检查都将被禁用。
- 3. 单击 确认和禁用。
- 4. 现在，通过滑动 设备状态已禁用 切换开关 ON。

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状态
- 我了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下禁用 Device Posture，然后再次启用 Device Posture（设备状态），而不选择该选项 在测试模式下启用设备状态。

重要提示：

- 在从测试模式过渡到生产模式之前，请务必全面查看您的策略。在测试模式下设置的策略在生产中实施时的行为可能会有所不同，从而可能会特别影响用户访问 拒绝访问。在测试模式下，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。但是，在生产环境中，此结果会直接阻止访问，从而可能影响用户体验和运营。
- 此外，从测试模式过渡到生产模式时，可能会出现停机。建议仔细规划您的过渡，以最大限度地减少中断。

监视和故障排除

June 19, 2024

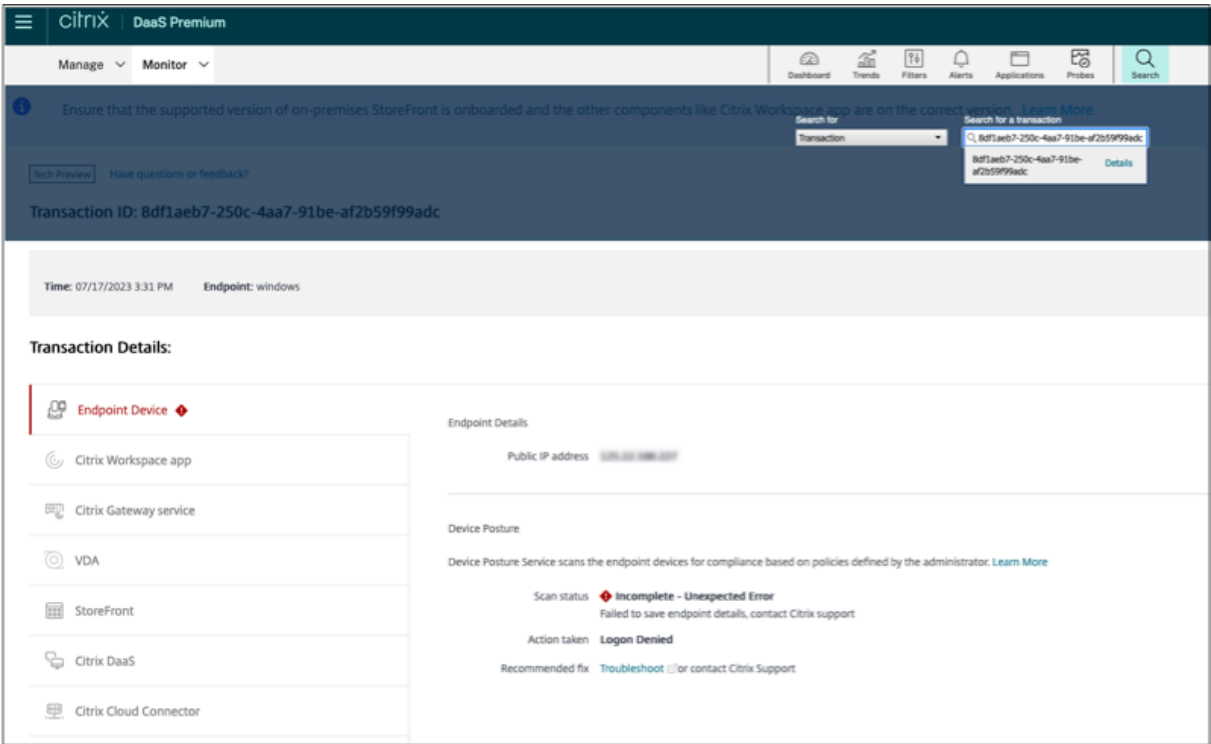
可以在两个位置查看 Device Posture 事件日志：

- 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。

Diagnostic Logs (26198) Device Posture Logs (41)									
Filters		Policy-Info = "Key-Word" Last 1 Week Search							
POLICY RESULT		Results are limited to the first 1000 records. Narrow your search criteria for more relevant results. Export to CSV format							
<input type="checkbox"/> Compliant		TIME (UTC)	POLICY INFO	POLICY RESULT	STATUS	OPERATING SYSTEM	TRANSACTION ID	DESCRIPTION	INFO CODE
<input type="checkbox"/> Non-Compliant		Tue, 11 Apr 2023 11:47...	NoMatchingPolicy	Non-Compliant	Success	Windows	85562ba3-7fc8-4839...		
<input type="checkbox"/> Login Denied		Tue, 11 Apr 2023 11:45...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
		Tue, 11 Apr 2023 11:45...	NoMatchingPolicy	Non-Compliant	Success	Windows	a418a959-e7cd-4a9d...		
		Tue, 11 Apr 2023 11:44...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
		Tue, 11 Apr 2023 11:44...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
		Tue, 11 Apr 2023 11:43...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
		Tue, 11 Apr 2023 11:42...	ms-MEM	Compliant	Success	Windows	cb57315f-48f7-45cb...		

- 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

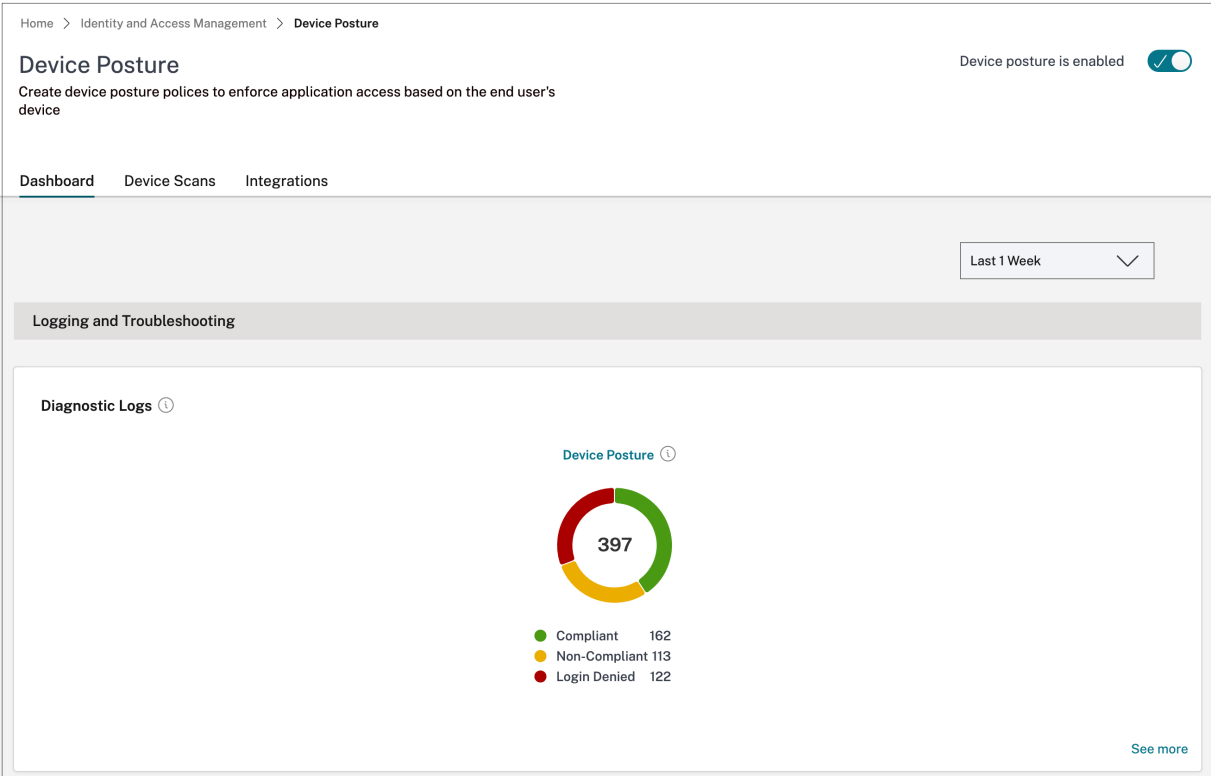
可以在 Citrix Monitor 和 Secure Private Access 控制面板上查看以下与 Device Posture 服务相关的日志。对于所有这些日志，建议您联系 Citrix 支持部门寻求解决方案。

- 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](#)。

管理设备状态服务的 **Citrix Endpoint Analysis** 客户端

October 21, 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）。

要在终端设备上运行设备状态扫描，必须在该设备上安装 Citrix EndPoint Analysis（EPA）客户端，这是一个轻量级应用程序。设备终端安全评估服务始终与 Citrix 发布的最新版本的 EPA 客户端一起运行。

安装 **EPA** 客户端

在运行时，Device Posture 服务会提示最终用户在运行时下载并安装 EPA 客户端。有关详细信息，请参阅[最终用户流](#)。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

发布新版本的 EPA 客户端时，默认情况下，适用于 Windows 的 EPA 客户端将在首次安装后升级。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。对于自动升级，必须已安装具有管理员访问权限的 EPA 客户端。

EPA 客户端的分发

EPA 客户端可以使用 Global App Configuration Service (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进行分发。

- 与 **Citrix Workspace** 应用程序集成的 **EPA** 客户端安装程序：EPA 客户端安装程序与适用于 Windows 的 Citrix Workspace 应用程序 2402 LTSR 集成。通过此集成，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 `安装EPAClient`。例如 `./CitrixworkspaceApp.exe 安装 EPAClient`。

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 `安装EPAClient`。
- 如果终端设备已安装 EPA 客户端，并且最终用户安装了 Citrix Workspace 应用程序，则会升级现有 EPA 客户端。
- 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删除。但是，如果 EPA 客户端未作为集成 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 和设备状态一起使用时管理 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，而无需最终用户干预。有关 GACS 的更多信息，请参阅 [如何使用 Global App Configuration 服务](#)。

注意：

- GACS 在 Windows 设备上仅支持分发 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 **Software** 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** 和设备状态一起使用时管理 **EPA** 客户端

EPA 客户端可与 NetScaler 和 Device Posture 在以下部署中一起使用：

- 使用 EPA 的基于 NetScaler 的自适应身份验证
- 基于 NetScaler 的本地网关，具有 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：

- 总是：终端设备上的 EPA 客户端和 NetScaler 必须位于同一版本上。
- 基本：终端设备上的 EPA 客户端版本必须在 NetScaler 上配置的范围。
- 从不：终端设备可以具有任何版本的 EPA 客户端。

有关更多信息，请参阅 [插件行为](#)。

将 **EPA** 客户端与 **NetScaler** 和设备安全评估一起使用时的注意事项

当 EPA 客户端与 Device Posture Service 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 位于不同版本的 EPA 客户端上的情况。这可能会导致 NetScaler 上的“EPA 客户端版本”与终端设备不匹配。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。为避免此冲突，我们建议进行以下配置更改：

- 如果您已使用自适应身份验证或本地身份验证或网关虚拟服务器配置了 EPA，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。
- EPA 版本控制可以设置为 从不 通过使用 CLI 或 GUI。NetScaler 13.x 及更高版本支持这些配置更改。
 - CLI：将 CLI 命令用于自适应身份验证和本地身份验证虚拟服务器。
 - GUI：使用本地网关虚拟服务器的 GUI。有关详细信息，请参阅 [控制 Citrix Secure Access 客户端的升级](#)。

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
```

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。



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).