Gerätestatus

Machine translated content

Disclaimer

Contents

Was ist neu

October 21, 2024

29 May 2024

- **Verfügbarkeit des Device Posture-Dienstes im Testmodus**

  Der Device Posture-Dienst ist auch im Testmodus verfügbar, in dem Administratoren den Device Posture-Dienst testen können, bevor sie ihn in ihrer Produktionsumgebung aktivieren. Auf diese Weise können die Administratoren die Auswirkungen der Gerätestatus-Scans auf die Endbenutzergeräte analysieren und dann ihre Vorgehensweise entsprechend planen, bevor sie diese in der Produktion aktivieren. Einzelheiten finden Sie unter Device Posture-Dienst im Testmodus.

- **Regelmäßiges Scannen von Geräten

  Sie können jetzt das regelmäßige Scannen von Windows-Geräten für die konfigurierten Prüfungen alle 30 Minuten aktivieren. Einzelheiten finden Sie unter Regelmäßiges Scannen von Geräten.

14 May 2024

- **Gerätestatusprüfungen überspringen**

  Administratoren können Endbenutzern erlauben, die Gerätestatusprüfungen auf ihren Geräten zu überspringen. Einzelheiten finden Sie unter Gerätehaltungsprüfungen überspringen.

- **Dashboard zur Gerätehaltung**

  Das Device Posture-Serviceportal verfügt jetzt über ein Dashboard zur Überwachung und Fehlerbehebung von Protokollen. Administratoren können dieses Dashboard jetzt zu Überwachungs- und Fehlerbehebungszwecken verwenden. Einzelheiten finden Sie unter Gerätestatusprotokolle.

- **Generelle Verfügbarkeit von Browser- und Antivirus-Checks**

  Die Browser- und Antivirus-Prüfungen sind nun allgemein verfügbar. Einzelheiten finden Sie unter Durch die Gerätehaltung unterstützte Scans.

- **Allgemeine Verfügbarkeit von benutzerdefinierten Nachrichten**

  Die Option zum Hinzufügen benutzerdefinierter Nachrichten bei verweigertem Zugriff ist jetzt allgemein verfügbar. Weitere Einzelheiten finden Sie unter Benutzerdefinierte Meldungen für Szenarien mit verweigertem Zugriff.

26. März 2024

- **Unterstützung für benutzerdefinierte Arbeitsbereich-URLs**

  Benutzerdefinierte Arbeitsbereichs-URLs werden jetzt mit dem Device Posture-Dienst unterstützt. Sie können zusätzlich zu Ihrer cloud.com-URL eine URL verwenden, deren Eigentümer Sie sind, um auf den Arbeitsbereich zuzugreifen. Stellen Sie sicher, dass Sie den Zugriff auf citrix.com von Ihrem Netzwerk aus zulassen. Einzelheiten zu benutzerdefinierten Domänen finden Sie unter Konfigurieren einer benutzerdefinierten Domäne.

12. Februar 2024

- **Unterstützung für Browser- und Antivirusprüfungen –Vorschau**

  Der Device Posture-Dienst unterstützt jetzt Browser- und Antivirenprüfungen. Einzelheiten finden Sie unter Durch die Gerätehaltung unterstützte Scans.

23. Januar 2024

- **Allgemeine Verfügbarkeit der Gerätezertifikatsprüfung mit dem Device Posture-Dienst**

  Die Gerätezertifikatsprüfung mit dem Device Posture-Dienst ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Gerätezertifikatsprüfung.

- **Vorschaufunktionen des Device Posture-Dienstes**

  Der Device Posture-Dienst unterstützt jetzt die folgenden Prüfungen:

  - Der Device Posture-Dienst wird jetzt auf den IGEL-Plattformen unterstützt.
  - Der Device Posture-Dienst unterstützt jetzt Geolokalisierungs- und Netzwerkstandortprüfungen.

  Einzelheiten finden Sie unter Gerätehaltung.

11. September 2023

- **Allgemeine Verfügbarkeit der Device Posture-Integration mit Microsoft Intune**

  Die Device Posture-Integration mit Microsoft Intune ist jetzt allgemein verfügbar. Weitere Einzelheiten finden Sie unter Microsoft Intune-Integration mit Device Posture.

30. August 2023

- **Verwalten des Citrix Endpoint Analysis Client für den Device Posture-Dienst**

  Der EPA-Client kann zusammen mit NetScaler und Device Posture verwendet werden. Bei Verwendung mit NetScaler und Device Posture sind einige Konfigurationsänderungen erforderlich, um den EPA-Client zu verwalten. Einzelheiten finden Sie unter Citrix Endpoint Analysis Client für den Device Posture-Dienst verwalten.

28. August 2023

- **Unterstützung des Device Posture-Dienstes auf iOS-Plattformen –Vorschau**

  Der Device Posture-Dienst wird jetzt auf iOS-Plattformen unterstützt. Einzelheiten finden Sie unter Gerätehaltung.

22. August 2023

- **Gerätezertifikatsprüfung mit dem Citrix Device Posture Service –Vorschau**

  Der Citrix Device Posture-Dienst kann jetzt den kontextbezogenen Zugriff (Smart Access) auf Citrix DaaS- und Secure Private Access-Ressourcen ermöglichen, indem er das Zertifikat des Endgeräts mit einer Unternehmenszertifizierungsstelle vergleicht, um festzustellen, ob das Endgerät vertrauenswürdig ist. Einzelheiten finden Sie unter Gerätezertifikatsprüfung.

17. August 2023

- **Device Posture-Ereignisse im Citrix DaaS Monitor**

  Device Posture-Dienstereignisse und Überwachungsprotokolle können jetzt im DaaS Monitor durchsucht werden. Weitere Einzelheiten finden Sie unter Gerätestatusereignisse im Citrix DaaS Monitor.

23. Januar 2023

- **Gerätehaltungsdienst**

  Der Citrix Device Posture-Dienst ist eine Cloud-basierte Lösung, die Administratoren dabei hilft, bestimmte Anforderungen durchzusetzen, die die Endgeräte erfüllen müssen, um Zugriff auf Citrix DaaS (virtuelle Apps und Desktops) oder Citrix Secure Private Access-Ressourcen (SaaS, Web-Apps, TCP- und UDP-Apps) zu erhalten. Einzelheiten finden Sie unter Gerätehaltung.

  [AAUTH-90]

- **Microsoft Endpoint Manager-Integration mit Device Posture**

  Zusätzlich zu den nativen Scans, die der Device Posture-Dienst bietet, kann der Device Posture-Dienst auch in andere Lösungen von Drittanbietern integriert werden. Device Posture ist in Microsoft Endpoint Manager (MEM) unter Windows und macOS integriert. Weitere Einzelheiten finden Sie unter Microsoft Endpoint Manager-Integration mit Device Posture.

  [ACS-1399]

Device Posture-Dienst im Testmodus

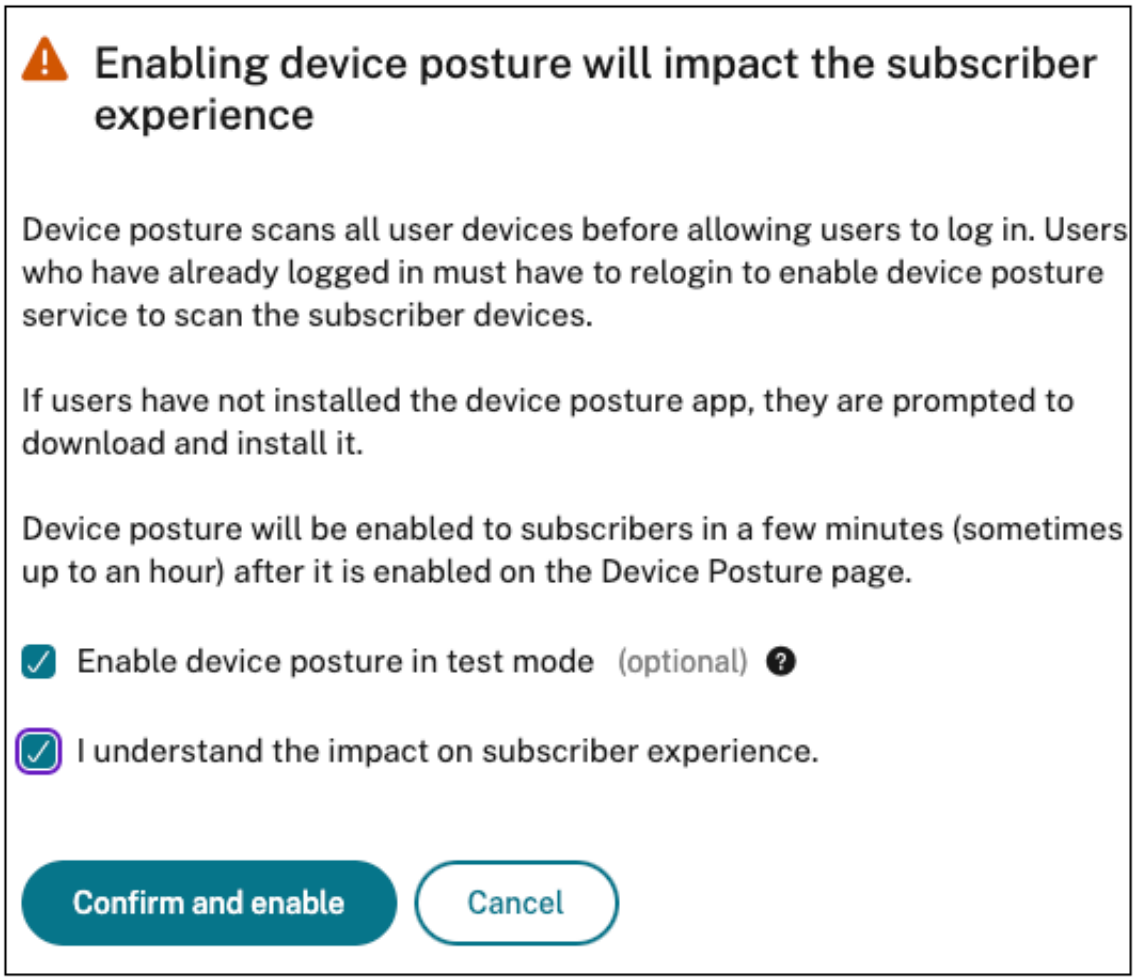
October 21, 2024

Der Device Posture-Dienst ist auch im Testmodus verfügbar, in dem Administratoren den Device Posture-Dienst testen können, bevor sie ihn in ihrer Produktionsumgebung aktivieren. Auf diese Weise können die Administratoren die Auswirkungen der Gerätestatus-Scans auf die Endbenutzergeräte analysieren und dann ihre Vorgehensweise entsprechend planen, bevor sie diese in der Produktion aktivieren. Der Device Posture-Dienst sammelt im Testmodus Daten der Endbenutzergeräte und klassifiziert die Geräte in die drei Kategorien konform, nicht konform und abgelehnt. Diese Klassifizierung erzwingt jedoch keine Aktionen auf den Endbenutzergeräten. Stattdessen werden Administratoren in die Lage versetzt, ihre Umgebungen zu bewerten und die Sicherheit zu verbessern. Administratoren können diese Daten auf dem Device Posture-Dashboard anzeigen. Bei Bedarf können Administratoren den Testmodus auch deaktivieren.

> **Hinweis:**
>
> Der EPA-Client muss auf den Geräten installiert sein. Falls auf einem Endgerät der EPA-Client nicht installiert ist, präsentiert der Device Posture-Dienst dem Endbenutzer eine Download-Seite zum Herunterladen und Installieren des Clients, ohne den sich der Endbenutzer nicht anmelden kann.

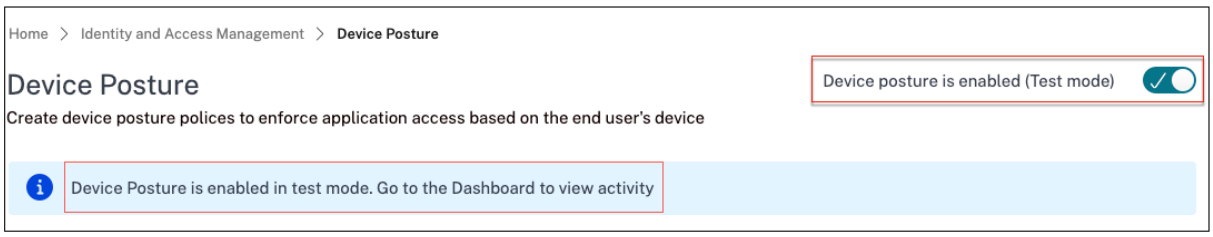
Testmodus aktivieren

1. Melden Sie sich bei Citrix Cloud an und wählen Sie dann **Identity and Access Management** aus dem Hamburger-Menü.
2. Klicken Sie auf die Registerkarte **Gerätehaltung** und dann auf **Verwalten**.
3. Schieben Sie den Kippschalter **„Gerätehaltung ist deaktiviert“** auf EIN.
4. Aktivieren Sie im Bestätigungsfenster beide Kontrollkästchen.



5. Klicken Sie auf **, bestätigen und aktivieren Sie**.

Wenn der Device Posture-Dienst im Testmodus aktiviert ist, wird auf der Device Posture-Startseite ein entsprechender Hinweis angezeigt.



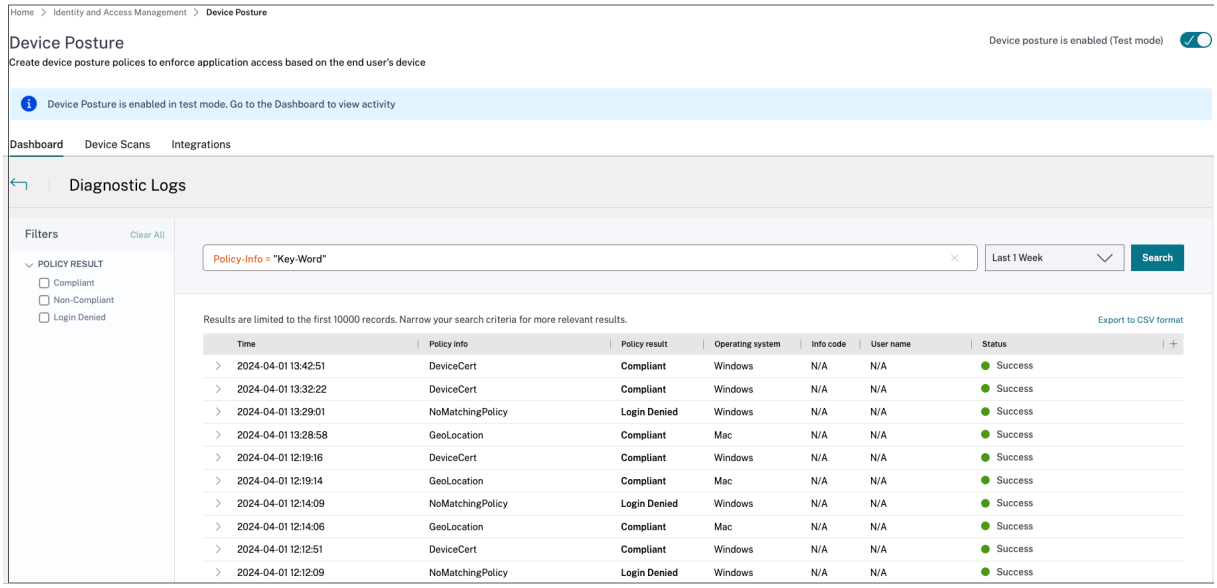
Administratoren können die Richtlinien und Regeln für Gerätestatus-Scans konfigurieren. Weitere Einzelheiten finden Sie unter „Gerätehaltung konfigurieren“. Basierend auf den Scan-Ergebnissen werden die Endbenutzergeräte als konform, nicht konform und abgelehnt klassifiziert. Administratoren können diese Daten auf dem Dashboard anzeigen.

Zeigen Sie die Testmodusaktivitäten auf dem Dashboard an

1. Klicken Sie auf der Seite „Gerätehaltung“auf die Registerkarte **Dashboard** .

   Das Diagramm **Diagnoseprotokolle** zeigt die Anzahl der Geräte an, die als konform, nicht konform und Anmeldung verweigert klassifiziert sind.

2. Klicken Sie zum Anzeigen der Details auf den Link **Weitere Informationen** .



Administratoren können die Überwachungsprotokolle von der Benutzeroberfläche herunterladen.

Aktivieren des Testmodus in der Produktion

Wenn der Device Posture-Dienst in der Produktion bereits aktiviert ist, führen Sie die folgenden Schritte aus, um den Testmodus zu aktivieren:

1. Schieben Sie auf der Startseite den Kippschalter **Gerätehaltung ist aktiviert** auf AUS.
2. Wählen Sie **. Ich verstehe, dass alle Gerätehaltungsprüfungen deaktiviert werden**.
3. Klicken Sie auf **, bestätigen Sie und deaktivieren Sie**.
4. Aktivieren Sie nun die Gerätehaltung, indem Sie den Kippschalter **„Gerätehaltung ist deaktiviert“** auf EIN schieben.
5. Wählen Sie im Bestätigungsfenster beide der folgenden Optionen aus.

   - **Aktivieren der Gerätehaltung im Testmodus**
   - **Ich verstehe die Auswirkungen auf das Abonnentenerlebnis**

6. Klicken Sie auf **, bestätigen und aktivieren Sie**.

Übergang vom Testmodus zur Produktion

Um vom Testmodus in die Produktion zu wechseln, müssen Sie zunächst die Gerätehaltung im Testmodus deaktivieren und dann die Gerätehaltung wieder aktivieren, ohne die Option **Gerätehaltung im Testmodus aktivieren**auszuwählen.

> **Wichtig:**
>
> - Es ist wichtig, Ihre Richtlinien vor dem Übergang vom Testmodus zur Produktion gründlich zu überprüfen. Richtlinien, die im Testmodus eingerichtet wurden, verhalten sich möglicherweise anders, wenn sie in der Produktion durchgesetzt werden, und haben möglicherweise insbesondere Auswirkungen auf den Benutzerzugriff **Zugriff verweigern**. Im Testmodus wird **Zugriff verweigert** effektiv als **Nicht konform behandelt,** , sodass Benutzer weiterhin ohne Unterbrechung auf das System zugreifen können. In der Produktion blockiert dieses Ergebnis jedoch direkt den Zugriff und kann sich auf das Benutzererlebnis und den Betrieb auswirken.
> - Außerdem kann es beim Übergang vom Testmodus zur Produktion zu Ausfallzeiten kommen. Es wird empfohlen, den Übergang sorgfältig zu planen, um Störungen zu minimieren.

Überwachen und Problembehandlung

June 19, 2024

Die Ereignisprotokolle zur Gerätehaltung können an zwei Stellen eingesehen werden:

- Citrix DaaS-Monitor
- Citrix Secure Private Access-Dashboard

Gerätezustandsereignisse auf Citrix DaaS Monitor

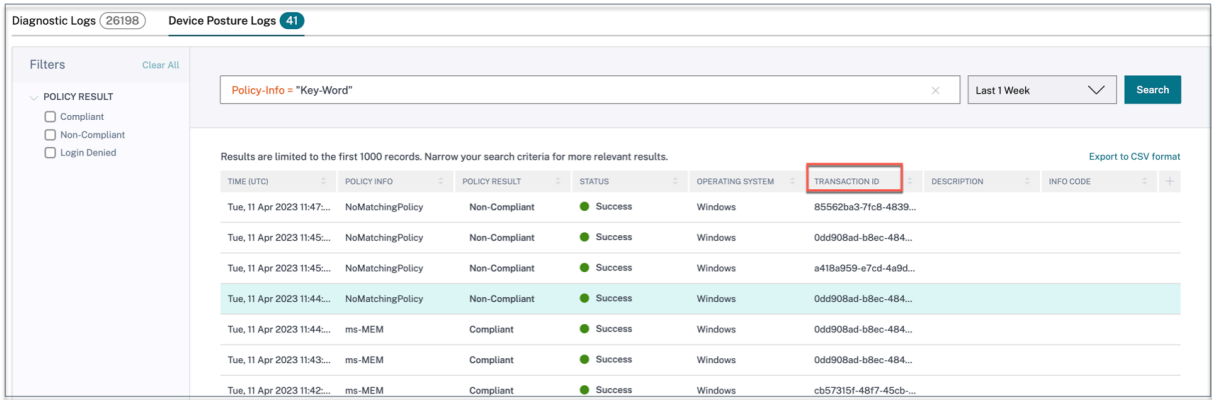
Gehen Sie wie folgt vor, um die Ereignisprotokolle für den Device Posture Service einzusehen.

1. Kopieren Sie die Transaktions-ID der fehlgeschlagenen Sitzung oder der Sitzung mit verweigertem Zugriff vom Endbenutzergerät.
2. Melden Sie sich bei Citrix Cloud an.
3. Klicken Sie auf der DaaS-Kachel auf **Verwalten**und dann auf die Registerkarte **Überwachen** . Suchen Sie in der Monitor-Benutzeroberfläche nach der 32-stelligen Transaktions-ID und klicken Sie auf **Details**.

Gerätezustandsereignisse im Secure Private Access-Dashboard

Gehen Sie wie folgt vor, um die Ereignisprotokolle für den Device Posture Service einzusehen.

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Kachel Secure Private Access auf **Verwalten** und dann auf **Dashboard**.
3. Klicken Sie im Diagramm mit den **Diagnoseprotokollen** auf den Link **Mehr anzeigen**, um die Ereignisprotokolle zum Gerätestatus einzusehen.



- Administratoren können die Protokolle anhand der Transaktions-ID in der Tabelle mit den Diagnoseprotokollen filtern. Die Transaktions-ID wird dem Endbenutzer auch angezeigt, wenn der Zugriff verweigert wird.
- Wenn ein Fehler oder ein Scanfehler auftritt, zeigt der Device Posture Service eine Transaktions-ID an. Diese Transaktions-ID ist im Secure Private Access Service Access-Dienst-Dashboard verfügbar. Wenn die Protokolle das Problem nicht lösen, können Endbenutzer die Transaktions-ID an den Citrix Support weitergeben, um das Problem zu lösen.
- Die Windows-Client-Logs finden Sie unter:
  - %localappdata%\Citrix\EPA\dpaCitrix.txt
  - %localappdata%\Citrix\EPA\epalib.txt
- Die macOS-Client-Logs finden Sie unter:
  - ~/Bibliothek/Anwendung Support/Citrix/EPAPlugin/EpaCloud.log
  - ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

Fehlerprotokolle zur Gerätehaltung

Die folgenden Protokolle zum Device Posture Service können auf dem Citrix Monitor- und Secure Private Access-Dashboard eingesehen werden. Für all diese Protokolle wird empfohlen, dass Sie sich an den Citrix Support wenden, um eine Lösung zu finden.

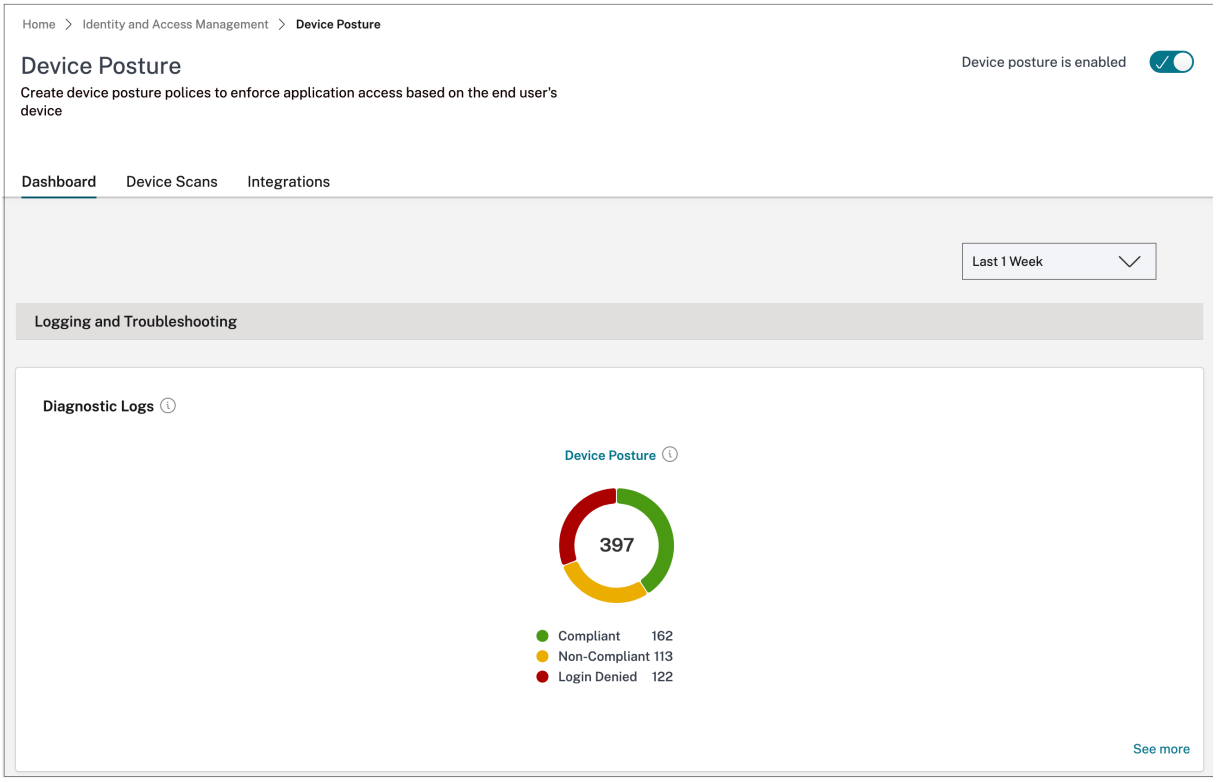
- Konnte konfigurierte Richtlinien nicht lesen

- Endpunktscans konnten nicht ausgewertet werden
- Richtlinien/Ausdruck konnten nicht verarbeitet werden
- Endpunktdetails konnten nicht gespeichert werden
- Scanergebnisse von Endpunkten konnten nicht verarbeitet werden

Gerätestatusprotokolle

June 19, 2024

Sie können das Dashboard im Device Posture Service Portal für Überwachungs- und Fehlerbehebungszwecke verwenden. Um das Device Posture Service-Dashboard anzuzeigen, klicken Sie auf der Device Posture Startseite auf die Registerkarte **Dashboard** . Im Abschnitt **Protokollierung und Problembehandlung** werden die Diagnoseprotokolle für den Device Posture Service angezeigt. Sie können auf den Link **Weitere Informationen** klicken, um die Details der Protokolle anzuzeigen. Sie können Ihre Suche anhand der Richtlinienergebnisse (**konform**, **nicht konform**und **Anmeldung verweigert**) verfeinern.



> **Hinweis:**
>
> Gerätezustands-Logs werden auch im Secure Private Access Service Service-Dashboard erfasst.

> Um die Gerätezustands-Logs anzuzeigen, klicken Sie auf die Registerkarte **Device Stature Logs**. Sie können Ihre Suche anhand der Richtlinienergebnisse verfeinern (**Konform, Nicht konform und Anmeldung verweigert**). Weitere Informationen finden Sie unter Diagnoseprotokolle.

Verwalten des Citrix Endpoint Analysis-Clients für den Device Posture-Dienst

October 21, 2024

Der Citrix Device Posture-Dienst ist eine Cloud-basierte Lösung, die Administratoren dabei hilft, bestimmte Anforderungen durchzusetzen, die die Endgeräte erfüllen müssen, um Zugriff auf Citrix DaaS (virtuelle Apps und Desktops) oder Citrix Secure Private Access-Ressourcen (SaaS, Web-Apps, TCP- und UDP-Apps) zu erhalten.

Um Gerätestatus-Scans auf einem Endgerät auszuführen, müssen Sie den Citrix EndPoint Analysis (EPA)-Client, eine einfache Anwendung, auf diesem Gerät installieren. Der Device Posture-Dienst wird immer mit der neuesten von Citrix veröffentlichten Version des EPA-Clients ausgeführt.

Installation des EPA-Clients

Während der Laufzeit fordert der Device Posture-Dienst den Endbenutzer auf, den EPA-Client herunterzuladen und zu installieren. Einzelheiten finden Sie unter Endbenutzerablauf. Normalerweise erfordert der Download und die Installation eines EPA-Clients auf einem Endpunkt keine lokalen Administratorrechte. Um jedoch Gerätezertifikatsprüfungen auf einem Endgerät ausführen zu können, muss der EPA-Client mit Administratorzugriff installiert werden. Einzelheiten zur Installation eines EPA-Clients mit Administratorzugriff finden Sie unter Gerätezertifikat auf dem Endgerät installieren.

Upgrade des EPA-Clients für Windows

Wenn eine neue Version des EPA-Clients veröffentlicht wird, werden die EPA-Clients für Windows nach der ersten Installation standardmäßig aktualisiert. Durch das automatische Upgrade wird sichergestellt, dass auf den Endbenutzergeräten immer die neueste Version des EPA-Clients ausgeführt wird, die mit dem Device Posture-Dienst kompatibel ist. Für das Auto-Upgrade muss der EPA-Client mit Administratorrechten installiert worden sein.

Verteilung des EPA-Clients

EPA-Clients können mithilfe des Global App Configuration Service (GACS) oder EPA, das in das Citrix Workspace-App-Installationsprogramm integriert ist, oder mithilfe von Softwarebereitstellungstools verteilt werden.

- **In die Citrix Workspace-App integriertes EPA-Clientinstallationsprogramm:** Das EPA-Clientinstallationsprogramm ist in die Citrix Workspace-App 2402 LTSR für Windows integriert. Durch diese Integration ist es für Endbenutzer nicht mehr erforderlich, den EPA-Client nach der Installation der Citrix Workspace-App separat zu installieren.

  Um den EPA-Client als Teil der Citrix Workspace-App zu installieren, verwenden Sie die Befehlszeilenoption `InstallEPAClient`. Beispiel: `./CitrixworkspaceApp.exe InstallEPAClient`.

> **Hinweis:**
>
> - Die EPA-Clientinstallation als Teil der Citrix Workspace-App ist standardmäßig deaktiviert. Es muss explizit mit der Befehlszeilenoption `InstallEPAClient`aktiviert werden.
> - Wenn auf einem Endgerät bereits ein EPA-Client installiert ist und der Endbenutzer die Citrix Workspace-App installiert, wird der vorhandene EPA-Client aktualisiert.
> - Wenn ein Endbenutzer die Citrix Workspace-App deinstalliert, wird standardmäßig auch der integrierte EPA-Client vom Gerät entfernt. Wenn der EPA-Client jedoch nicht als Teil der integrierten Citrix Workspace-App-Installation installiert wurde, bleibt der vorhandene EPA-Client auf dem Gerät erhalten.
> - Das in die Citrix Workspace-App integrierte EPA-Client-Installationsprogramm kann auch mit NetScaler verwendet werden. Einzelheiten finden Sie unter Verwalten des EPA-Clients bei Verwendung mit NetScaler und Device Posture.

- **Verteilen Sie den Client mit GACS.**: GACS ist eine von Citrix bereitgestellte Lösung zum Verwalten der Verteilung clientseitiger Agenten (Plug-Ins). Der in GACS verfügbare automatische Update-Dienst stellt sicher, dass die Endgeräte ohne Eingreifen des Endbenutzers über die neusten EPA-Versionen verfügen. Weitere Informationen zu GACS finden Sie unter Verwenden des Global App Configuration-Dienstes.

> **Hinweis:**
>
> - GACS wird auf Windows-Geräten nur zur Verteilung des EPA-Clients unterstützt.
> - Um einen EPA-Client über GACS zu verwalten, installieren Sie Citrix Workspace Application (CWA) auf den Endgeräten.
> - Wenn CWA mit Administratorrechten auf einem Endbenutzergerät installiert wird, installiert GACS den EPA-Client mit denselben Administratorrechten.

> • Wenn CWA mit Benutzerrechten auf einem Endbenutzergerät installiert wird, installiert GACS den EPA-Client mit denselben Benutzerrechten.

Verteilen Sie den Client mithilfe von Softwarebereitstellungstools.: Der neueste EPA-Client kann von Administratoren mithilfe von Softwarebereitstellungstools wie Microsoft SCCM verteilt werden.

Verwalten des EPA-Clients bei Verwendung mit NetScaler und Device Posture

Der EPA-Client kann zusammen mit NetScaler und Device Posture in den folgenden Bereitstellungen verwendet werden:

- NetScaler-basierte adaptive Authentifizierung mit EPA
- Auf NetScaler basierendes On-Premise-Gateway mit EPA

Der Device Posture-Dienst überträgt die neueste Version des EPA-Clients auf die Endgeräte. Unter NetScaler können Administratoren jedoch die folgende Versionskontrolle für die EPA-Scans auf virtuellen Gateway-Servern konfigurieren:

- **Immer**: Der EPA-Client auf dem Endgerät und NetScaler müssen auf der gleichen Version sein.
- **Unbedingt erforderlich**: Die EPA-Client-Version auf dem Endgerät muss innerhalb des auf NetScaler konfigurierten Bereichs liegen.
- **Niemals**: Das Endgerät kann über jede beliebige Version des EPA-Clients verfügen.

Weitere Informationen finden Sie unter Plug-in-Verhalten.

Überlegungen zur Verwendung des EPA-Clients mit NetScaler und Device Posture

Wenn ein EPA-Client zusammen mit Device Posture Service und NetScaler verwendet wird, kann es Szenarien geben, in denen auf dem Endgerät die neueste Version des EPA-Clients läuft, NetScaler jedoch eine andere Version des EPA-Clients verwendet. Dies kann zu einer Nichtübereinstimmung der EPA-Clientversion auf NetScaler und dem Endgerät führen. Infolgedessen fordert NetScaler den Endbenutzer möglicherweise auf, die auf NetScaler vorhandene EPA-Clientversion zu installieren. Um diesen Konflikt zu vermeiden, empfehlen wir die folgenden Konfigurationsänderungen:

- Wenn Sie EPA mit adaptiver Authentifizierung, lokaler Authentifizierung oder einem virtuellen Gateway-Server konfiguriert haben, wird empfohlen, die Versionskontrolle des EPA-Clients auf NetScaler zu deaktivieren. Dies geschieht, um sicherzustellen, dass der GACS- oder Device Posture-Dienst nicht die neueste Version des EPA-Clients auf die Endgeräte überträgt.
- Die EPA-Versionskontrolle kann mithilfe der CLI oder der GUI auf **und niemals auf** eingestellt werden. Diese Konfigurationsänderungen werden auf NetScaler 13.x und späteren Versionen unterstützt.

- CLI: Verwenden Sie die CLI-Befehle für die adaptive Authentifizierung und den virtuellen Authentifizierungsserver vor Ort.
- GUI: Verwenden Sie die GUI für den virtuellen Gateway-Server vor Ort. Einzelheiten finden Sie unter Steuerungsupgrade von Citrix Secure Access-Clients.

Beispiele für CLI-Befehle:

```
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
```

Data Governance

February 16, 2024

Dieses Thema enthält Informationen zur Erfassung, Speicherung und Aufbewahrung von Protokollen durch den Device Posture Service. Begriffe mit Großbuchstaben, die nicht in denDefinitionsabschnitten definiert sind, haben die im Citrix Endbenutzerservicevertrag angegebene Bedeutung.

Datenresidenz

Die Kundeninhaltsdaten von Citrix Device Posture befinden sich in den AWS- und Azure Cloud Services. Sie werden aus Gründen der Verfügbarkeit und Redundanz in die folgenden Regionen repliziert:

- AWS
  - USA, Osten
  - Indien, Westen
  - Europa (Frankfurt)
- Azure
  - USA, Westen
  - Westeuropa
  - Asien (Singapur)
  - USA, Süden-Mitte

Im Folgenden sind die verschiedenen Ziele für die Dienstkonfiguration, Laufzeitprotokolle und Ereignisse aufgeführt.

- Splunk-Dienst für die Systemüberwachung und Debug-Protokolle, nur in den USA.
- Der Citrix Analytics-Dienst für die Diagnose und Benutzerzugriffsprotokolle finden Sie unter Citrix Analytics Service Data Governance für weitere Informationen.
- Citrix Cloud System Logs-Dienst für Administratorüberwachungsprotokolle. Einzelheiten finden Sie unter Umgang mit Kundeninhalten und Protokollen von Citrix Cloud Services sowie geografische Überlegungen.

Datensammlung

Der Citrix Device Posture Service ermöglicht es den Kundenadministratoren, den Dienst über die Device Posture UI zu konfigurieren. Die folgenden Kundeninhalte werden basierend auf der Konfiguration der Gerätestatusrichtlinie und der Plattform gesammelt:

- Betriebssystemversion
- Citrix Workspace-App
- MAC-Adressen
- Laufende Prozesse
- Gerätezertifikat
- Einzelheiten zur Registrierung
- Details zum Windows-Installationsupdate
- Details zum letzten Windows-Update
- Dateisystem —Dateinamen, Datei-Hashes und Änderungszeit
- Domänenname

Für Laufzeitprotokolle, die von den Servicekomponenten gesammelt werden, bestehen die wichtigsten Informationen aus den folgenden

- Kunden-/Mandanten-ID
- Geräte-ID (von Citrix generierte eindeutige Kennung)
- Ausgabe des Gerätestatusscans
- Öffentliche IP-Adresse des Endgeräts

Datenübertragung

Der Citrix Device Posture Service sendet Protokolle an Ziele, die durch die Transport Layer Security geschützt sind.

Steuerung von Daten

Der Citrix Device Posture Service bietet Kunden derzeit keine Optionen, um das Senden von Protokollen zu deaktivieren oder zu verhindern, dass Kundeninhalte global repliziert werden.

Datenaufbewahrung

Basierend auf der Citrix Cloud-Datenaufbewahrungsrichtlinie werden die Kundenkonfigurationsdaten 90 Tage nach Ablauf des Abonnements aus dem Dienst gelöscht.

Die Protokollziele behalten ihre dienstspezifische Datenaufbewahrungsrichtlinie bei.

- Einzelheiten finden Sie unter Data Governance für die Aufbewahrungsrichtlinie für die Analytics-Protokolle.
- Die Splunk-Protokolle werden archiviert und schließlich nach 90 Tagen entfernt.

Datenexport

Es gibt verschiedene Datenexportoptionen für verschiedene Arten von Protokollen.

- Auf die Administratorüberwachungsprotokolle kann über die Citrix Cloud System Log-Konsole zugegriffen werden.
- Die Diagnoseprotokolle des Device Posture Service können im Dashboard des Citrix Analytics Service oder des Secure Private Access Service als CSV-Datei exportiert werden.

Definitionen

- Kundeninhalt bezeichnet alle Daten, die zur Speicherung in ein Kundenkonto hochgeladen werden, oder Daten in einer Kundenumgebung, auf die Citrix Zugriff zur Erbringung von Diensten erhält.
- Protokoll ist eine Aufzeichnung von Ereignissen im Zusammenhang mit den Diensten, einschließlich Aufzeichnungen, die Leistung, Stabilität, Nutzung, Sicherheit und Support messen.
- Dienste bedeuten, dass die zuvor für Citrix Analytics beschriebenen Citrix Cloud-Dienste.