Gerätestatus

Machine translated content

Disclaimer

Contents

Was ist neu

June 19, 2024

29 May 2024

- **Verfügbarkeit des Device Posture Service im Testmodus —Vorschau**

  Der Device Posture Service ist auch im Testmodus verfügbar, in dem Administratoren den Device Posture Service testen können, bevor sie ihn in ihrer Produktionsumgebung aktivieren. Auf diese Weise können die Administratoren die Auswirkungen der Gerätezustandsscans auf die Geräte der Endbenutzer analysieren und dann ihre Vorgehensweise entsprechend planen, bevor sie sie in der Produktion aktivieren. Einzelheiten finden Sie unter Device Posture Service im Testmodus —Vorschau.

- **Regelmäßiges Scannen von Geräten —Vorschau**

  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 —Vorschau.

14 May 2024

- **Überspringen Sie die Haltungsprüfungen des Geräts**

  Administratoren können den Endbenutzern erlauben, die Gerätezustandsprüfungen auf ihren Geräten zu überspringen. Einzelheiten finden Sie unter Überspringen der Körperhaltung von Geräten.

- **Dashboard zur Gerätehaltung**

  Das Device Posture Service Portal verfügt jetzt über ein Dashboard für Überwachungs- und Fehlerbehebungsprotokolle. Administratoren können dieses Dashboard jetzt für Überwachungs- und Fehlerbehebungszwecke verwenden. Einzelheiten finden Sie unter Gerätezustands-Logs.

- **Allgemeine Verfügbarkeit von Browser- und Antiviren-Checks**

  Die Browser- und Antiviren-Checks sind jetzt allgemein verfügbar. Einzelheiten finden Sie unter Scans, die je nach Geräteposition unterstützt werden.

- **Allgemeine Verfügbarkeit von benutzerdefinierten Nachrichten**

Die Option, benutzerdefinierte Nachrichten hinzuzufügen, wenn ein Zugriff verweigert wird, ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Benutzerdefinierte Nachrichten für Szenarien mit Zugriffsverweigerungen.

26. März 2024

- **Unterstützung für benutzerdefinierte Workspace-URLs**

  Benutzerdefinierte Workspace-URLs werden jetzt vom Device Posture Service unterstützt. Du kannst zusätzlich zu deiner cloud.com-URL eine URL verwenden, die dir gehört, um auf Workspace zuzugreifen. Stellen Sie sicher, dass Sie den Zugriff auf citrix.com von Ihrem Netzwerk aus zulassen. Einzelheiten zu benutzerdefinierten Domänen finden Sie unter Eine benutzerdefinierte Domain konfigurieren.

12. Februar 2024

- **Unterstützung für Browser- und Antiviren-Checks —Vorschau**

  Der Device Posture Service unterstützt jetzt Browser- und Antivirenprüfungen. Einzelheiten finden Sie unter Scans, die je nach Geräteposition unterstützt werden.

23. Januar 2024

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

  Die Überprüfung von Gerätezertifikaten mit dem Device Posture Service ist jetzt allgemein verfügbar. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats mit dem Device Posture Service.

- **Vorschaufunktionen des Device Posture Service**

  Der Device Posture Service unterstützt jetzt die folgenden Prüfungen:

  - Der Device Posture Service wird jetzt auf den IGEL-Plattformen unterstützt.
  - Der Device Posture Service unterstützt jetzt Geolocation- und Netzwerkstandortprüfungen.

  Einzelheiten finden Sie unter Gerätestatus.

11. September 2023

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

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

30. August 2023

- **Citrix Endpoint Analysis Client für Device Posture Service verwalten**

  Der EPA-Client kann zusammen mit NetScaler und Device Posture verwendet werden. Einige Konfigurationsänderungen sind erforderlich, um den EPA-Client zu verwalten, wenn er mit NetScaler und Device Posture verwendet wird. Einzelheiten finden Sie unter Verwalten des Citrix Endpoint Analysis Client für den Device Posture Service.

28. August 2023

- **Unterstützung des Device Posture Service auf iOS-Plattformen —Vorschau**

  Der Device Posture Service wird jetzt auf iOS-Plattformen unterstützt. Einzelheiten finden Sie unter Gerätestatus.

22. August 2023

- **Überprüfung des Gerätezertifikats mit dem Citrix Device Posture Service —Vorschau**

  Der Citrix Device Posture Service kann jetzt den kontextuellen Zugriff (Smart Access) auf Citrix DaaS- und Secure Private Access-Ressourcen ermöglichen, indem das Zertifikat des Endgeräts mit einer Unternehmenszertifizierungsstelle verglichen wird, um festzustellen, ob dem Endgerät vertraut werden kann. Einzelheiten finden Sie unter Überprüfung des Gerätezertifikats mit dem Device Posture Service.

17. August 2023

- **Gerätezustandsereignisse auf Citrix DaaS Monitor**

  Device Posture Service-Ereignisse und Überwachungsprotokolle können jetzt auf DaaS Monitor durchsucht werden. Einzelheiten finden Sie unter Gerätezustandsereignisse auf Citrix DaaS Monitor.

23. Januar 2023

- **Device Posture Service**

Der Citrix Device Posture Service ist eine cloudbasierte Lösung, mit der Administratoren bestimmte Anforderungen durchsetzen können, 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 Gerätestatus.

[AAUTH-90]

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

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

  [ACS-1399]

Device Posture Service im Testmodus —Vorschau

June 19, 2024

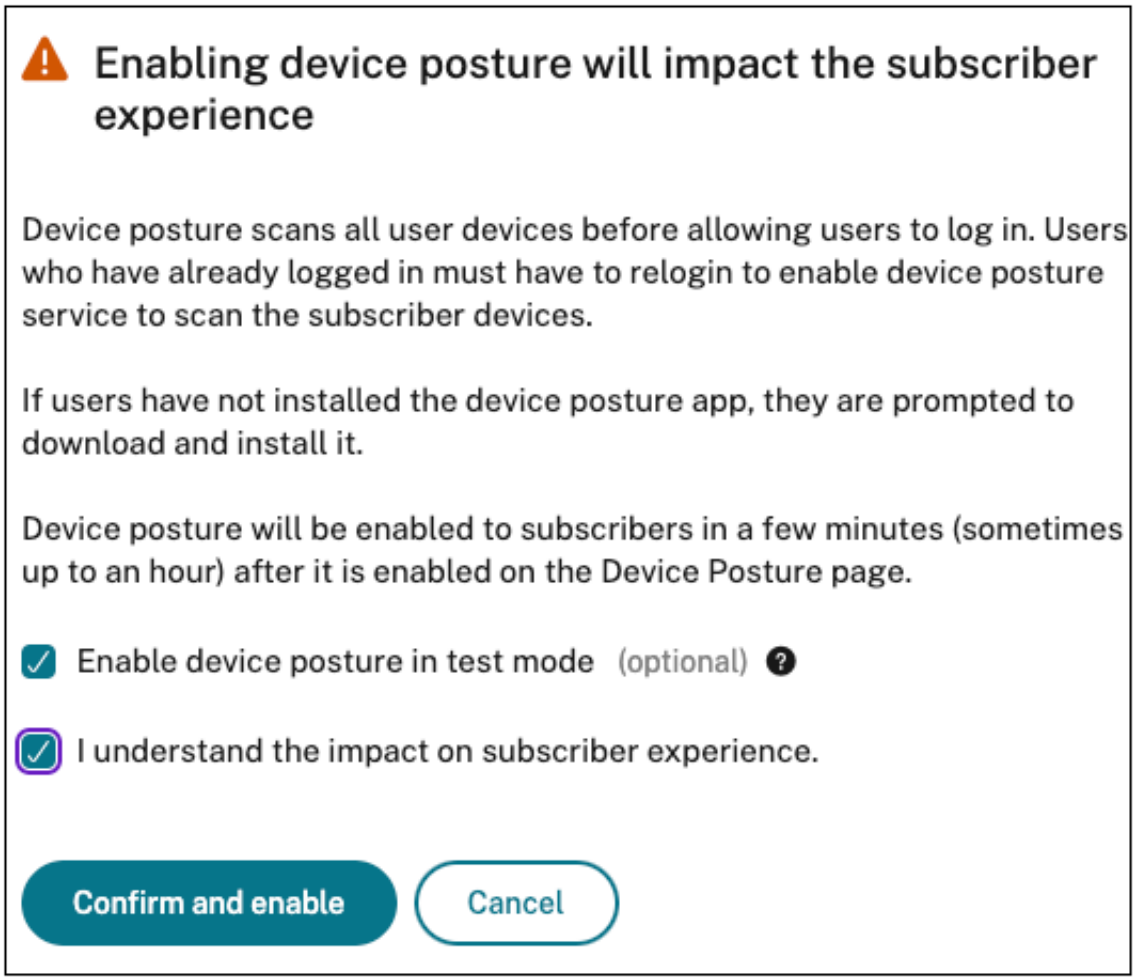
Der Device Posture Service ist auch im Testmodus verfügbar, in dem Administratoren den Device Posture Service testen können, bevor sie ihn in ihrer Produktionsumgebung aktivieren. Auf diese Weise können die Administratoren die Auswirkungen der Gerätezustandsscans auf die Geräte der Endbenutzer analysieren und dann ihre Vorgehensweise entsprechend planen, bevor sie sie in der Produktion aktivieren. Der Device Posture Service sammelt im Testmodus Daten der Endbenutzergeräte und klassifiziert die Geräte in die drei Kategorien "konform", "nicht konform"und "verweigert". Diese Klassifizierung erzwingt jedoch keine Aktionen auf den Endbenutzergeräten. Stattdessen ermöglicht es Administratoren, ihre Umgebungen zu bewerten und die Sicherheit zu erhöhen. Administratoren können diese Daten im Device Posture Dashboard einsehen. Admins können den Testmodus bei Bedarf 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 Service dem Endbenutzer eine Download-Seite zum Herunterladen und Installieren des Clients, ohne die sich der Endbenutzer nicht anmelden kann.

Testmodus aktivieren

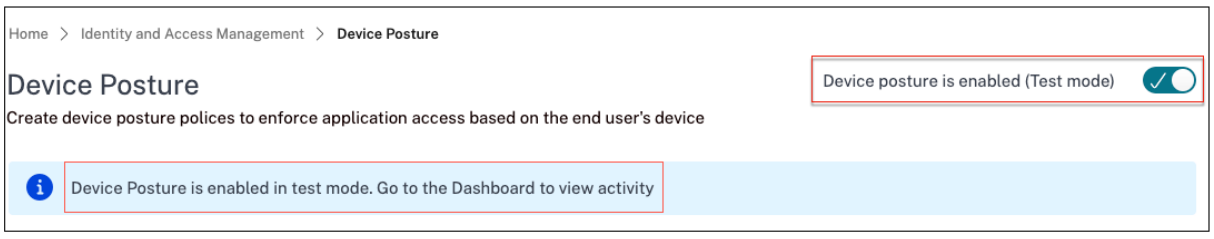
1. Melden Sie sich bei Citrix Cloud an und wählen Sie dann im Hamburger-Menü **Identitäts- und Zugriffsverwaltung** aus.

2. Klicken Sie auf die **Registerkarte Gerätestatus** und dann auf **Verwalten**.
3. Schieben Sie den Kippschalter auf "**Gerätehaltung ist deaktiviert** ".
4. Markieren Sie im Bestätigungsfenster beide Kontrollkästchen.



5. Klicken Sie auf **Bestätigen und aktivieren**.

Wenn der Device Posture Service im Testmodus aktiviert ist, wird auf der Device Posture Startseite ein Hinweis angezeigt, der dies bestätigt.



Administratoren können die Richtlinien und Regeln für Gerätezustandsscans konfigurieren. Einzelheiten finden Sie unter Gerätestatus konfigurieren. Basierend auf den Scanergebnissen werden die

Endbenutzergeräte als konform, nicht konform und verweigert eingestuft. Admins können diese Daten im Dashboard einsehen.

Sehen Sie sich die Aktivitäten im Testmodus auf dem Dashboard an

1. Klicken Sie auf der Seite Device Stature auf den Tab **Dashboard** .

   Das Diagramm mit den **Diagnoseprotokollen** zeigt die Anzahl der Geräte an, die als konform, nicht konform und Anmeldung verweigert eingestuft wurden.

2. Um die Details anzuzeigen, klicken Sie auf den Link **Mehr anzeigen** .

Diagnose im Testmodus

Administratoren können die Überwachungsprotokolle von der Benutzeroberfläche herunterladen.

Testmodus in der Produktion aktivieren

Wenn der Device Posture Service bereits in der Produktion aktiviert ist, gehen Sie wie folgt vor, um den Testmodus zu aktivieren:

1. Schieben Sie auf der Startseite den Kippschalter **Device Posture is enabled (Gerätehaltung ist aktiviert**) auf OFF.
2. Wählen Sie **Ich verstehe, dass alle Gerätehalterungsprüfungen deaktiviert werden**.
3. Klicken Sie auf **Bestätigen und deaktivieren**.
4. Aktivieren Sie nun die Gerätehaltung, indem Sie den Schalter **Gerätehaltung ist deaktiviert** auf ON schieben.
5. Wählen Sie im Bestätigungsfenster die beiden folgenden Optionen aus.
   - **Gerätehaltung im Testmodus aktivieren**
   - **Ich verstehe die Auswirkungen auf das Abonnentenerlebnis**
6. Klicken Sie auf **Bestätigen und aktivieren**.

CrowdStrike-Integration mit Device Posture

June 19, 2024

CrowdStrike Zero Trust Assessment (ZTA) bewertet den Sicherheitsstatus, indem für jedes Endgerät ein ZTA-Sicherheitswert von 1 bis 100 berechnet wird. Ein höherer ZTA-Score bedeutet, dass die Körperhaltung des Endgeräts besser ist.

Citrix Device Posture Service kann den kontextuellen Zugriff (Smart Access) auf Ressourcen von Citrix Desktop as a Service (DaaS) und Citrix Secure Private Access (SPA) mithilfe des ZTA-Scores eines Endgeräts ermöglichen.

Gerätestatus-Administratoren können den ZTA-Score als Teil von Richtlinien verwenden und die Endgeräte als konform, nicht konform (teilweiser Zugriff) oder sogar den Zugriff verweigern einstufen. Diese Klassifizierung kann wiederum von Organisationen verwendet werden, um kontextuellen Zugriff (Smart Access) auf virtuelle Apps und Desktops sowie SaaS- und Web-Apps bereitzustellen. ZTA-Score-Richtlinien werden für Windows- und macOS-Plattformen unterstützt.

CrowdStrike-Integration konfigurieren

Die Konfiguration der CrowdStrike-Integration erfolgt in zwei Schritten.

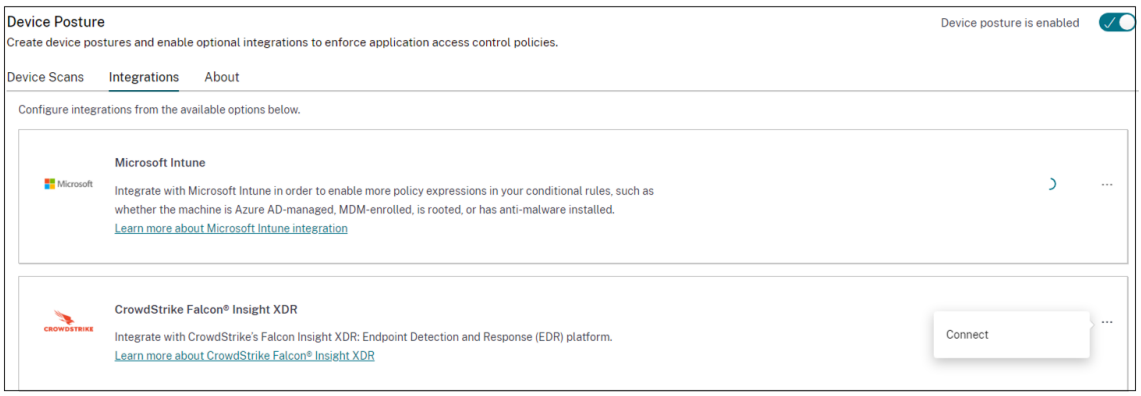
Schritt 1: Stellen Sie eine Vertrauensstellung zwischen dem Citrix Device Posture Service und dem CrowdStrike ZTA-Dienst her. Dies ist eine einmalige Aktivität.

Schritt 2: Konfigurieren Sie Richtlinien so, dass der CrowdStrike ZTA-Score in der Regel verwendet wird, um intelligenten Zugriff auf Citrix DaaS- und Citrix Secure Private Access-Ressourcen zu ermöglichen.

Schritt 1: Stellen Sie eine Vertrauensstellung zwischen dem Citrix Device Posture Service und dem CrowdStrike ZTA-Dienst her

Gehen Sie wie folgt vor, um eine Vertrauensstellung zwischen dem Citrix Device Posture Service und dem CrowdStrike ZTA-Dienst herzustellen.

1. Melden Sie sich bei Citrix Cloud an und wählen Sie dann **Identity and Access Management** aus dem Hamburger-Menü aus.
2. Klicken Sie auf **die Registerkarte Gerätestatus** und dann auf **Verwalten**.
3. Klicken Sie auf die Registerkarte **Integrationen**.



> **Hinweis:**
>
> Alternativ können Kunden im linken Navigationsbereich der Secure Private Access Service-GUI zur Option **Gerätestatus** navigieren und dann auf die Registerkarte **Integrationen** klicken.

4. Klicken Sie im CrowdStrike-Feld auf die Ellipsenschaltfläche und dann auf **Verbinden.** Der CrowdStrike Falcon Insight XDR-Integrationsbereich wird angezeigt.
5. Geben Sie die Client-ID und das Client-Geheimnis ein und klicken Sie dann auf **Speichern**.

> **Hinweis:**
>
> - Sie können die ZTA-API-Client-ID und das Client-Geheimnis im CrowdStrike-Portal (**Support und Ressourcen > API-Clients und Schlüssel**) abrufen.
> - Stellen Sie sicher, dass Sie die Bereiche **Zero Trust Assessment** und **Host** mit Leseberechtigungen für die Einrichtung des Vertrauens auswählen.

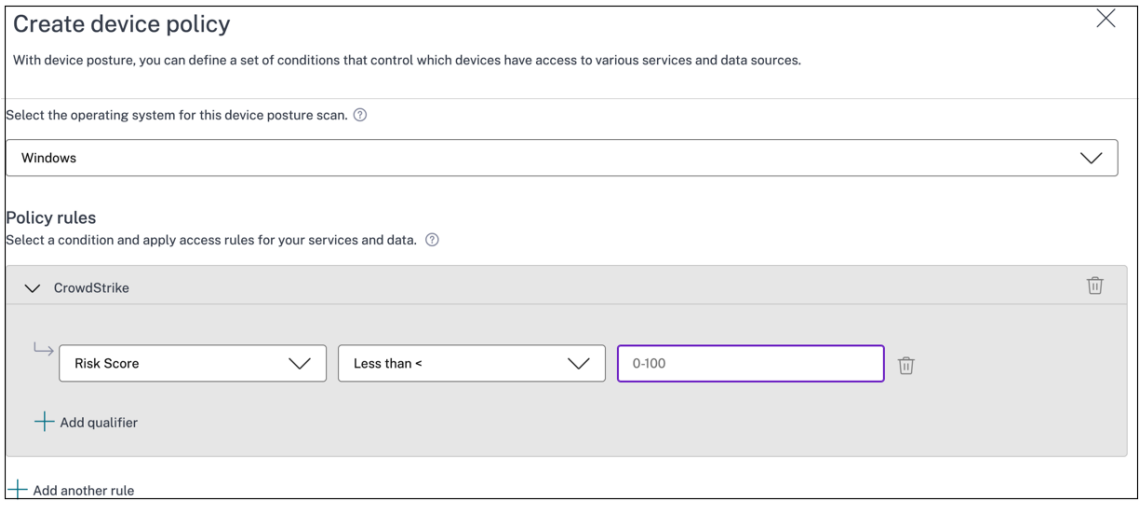
Die Integration gilt als erfolgreich, nachdem der Status von **Nicht konfiguriert** in **Konfiguriert** geändert wurde.

Wenn die Integration nicht erfolgreich ist, wird der Status als **Pending** angezeigt. Sie müssen auf die Ellipsenschaltfläche und dann auf **Erneut verbinden** klicken.

Schritt 2: Richtlinien für den Gerätestatus konfigurieren

Gehen Sie wie folgt vor, um Richtlinien so zu konfigurieren, dass der CrowdStrike ZTA-Score in der Regel verwendet wird, um intelligenten Zugriff auf Citrix DaaS- und Citrix Secure Private Access-Ressourcen zu ermöglichen.

1. Klicken Sie auf die Registerkarte **Gerätescans** und dann auf **Geräterichtlinie erstellen**.

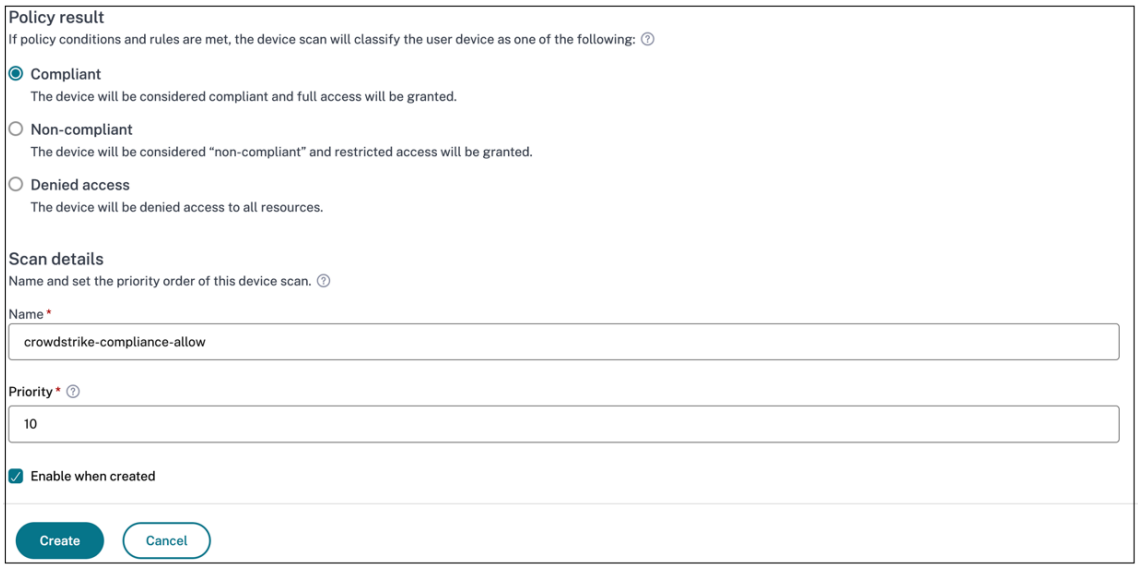


2. Wählen Sie die Plattform aus, für die diese Richtlinie erstellt wurde.
3. Wählen Sie unter **Policy Rule** die Option **CrowdStrike** aus.
4. Wählen Sie als Qualifizierer für die **Risc Score** die Bedingung aus, und geben Sie dann die Risikobewertung ein.
5. Klicken Sie auf **+**, um einen Qualifier hinzuzufügen, der überprüft, ob der CrowdStrike Falcon-Sensor läuft.

   > **Hinweis:**
   >
   > Sie können diese Regel zusammen mit anderen Regeln verwenden, die Sie für den Gerätestatus konfigurieren.

6. Wählen Sie unter **Richtlinienergebnis** basierend auf den von Ihnen konfigurierten Bedingungen eine der folgenden Optionen aus.

   - **Konform**
   - **Nicht konform**
   - **Anmeldung verweigert**



7. Geben Sie den Namen für die Richtlinie ein und legen Sie die Priorität fest.
8. Klicken Sie auf **Erstellen**.

Definitionen

Die Begriffe konform und nicht konform in Bezug auf den Device Posture Service sind wie folgt definiert.

- Kompatible Geräte —Ein Gerät, das die vorkonfigurierten Richtlinienanforderungen erfüllt und sich mit vollem oder uneingeschränktem Zugriff auf Citrix Secure Private Access-Ressourcen oder Citrix DaaS-Ressourcen im Unternehmensnetzwerk anmelden darf.
- Nicht konforme Geräte —Ein Gerät, das die vorkonfigurierten Richtlinienanforderungen erfüllt und sich mit teilweisem oder eingeschränktem Zugriff auf Citrix Secure Private Access-Ressourcen oder Citrix DaaS-Ressourcen im Unternehmensnetzwerk anmelden darf.

Referenzen

Gerätestatusdienst

Integration von Microsoft Intune mit Device Posture

June 19, 2024

Microsoft Intune klassifiziert das Gerät eines Benutzers auf der Grundlage seiner Richtlinienkonfiguration als konform oder registriert. Während der Benutzeranmeldung bei Citrix Workspace kann Device Posture bei Microsoft Intune den Gerätestatus des Benutzers abfragen und anhand dieser Informationen die Geräte in Citrix Cloud als konform, nicht konform (teilweiser Zugriff) klassifizieren oder sogar den Zugriff auf die Benutzeranmeldeseite verweigern. Dienste wie Citrix DaaS und Citrix Secure Private Access nutzen wiederum die Gerätestatusklassifizierung der Geräte, um kontextuellen Zugriff (Smart Access) auf virtuelle Apps und Desktops sowie SaaS- und Web-Apps zu ermöglichen.

So konfigurieren Sie die Microsoft Intune-Integration

Die Konfiguration der Intune-Integration erfolgt in zwei Schritten.

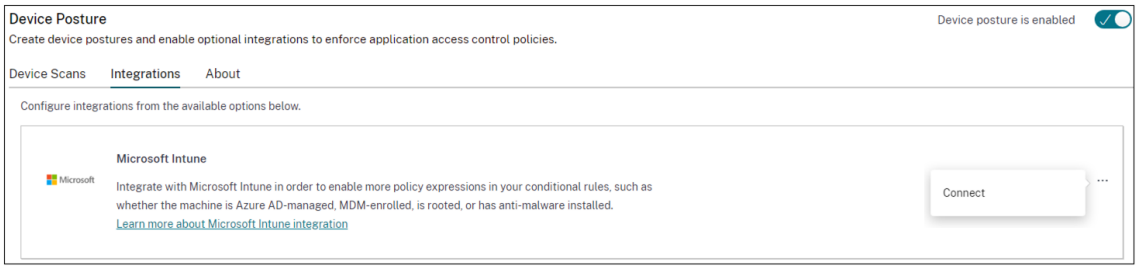
Schritt 1: Integrieren Sie die Geräteposition in den Microsoft Intune-Dienst. Dies ist eine einmalige Aktivität, die Sie ausführen, um eine Vertrauensstellung zwischen Device Posture und Microsoft Intune herzustellen.

Schritt 2: Konfigurieren Sie Richtlinien für die Verwendung Microsoft Intune-Informationen.

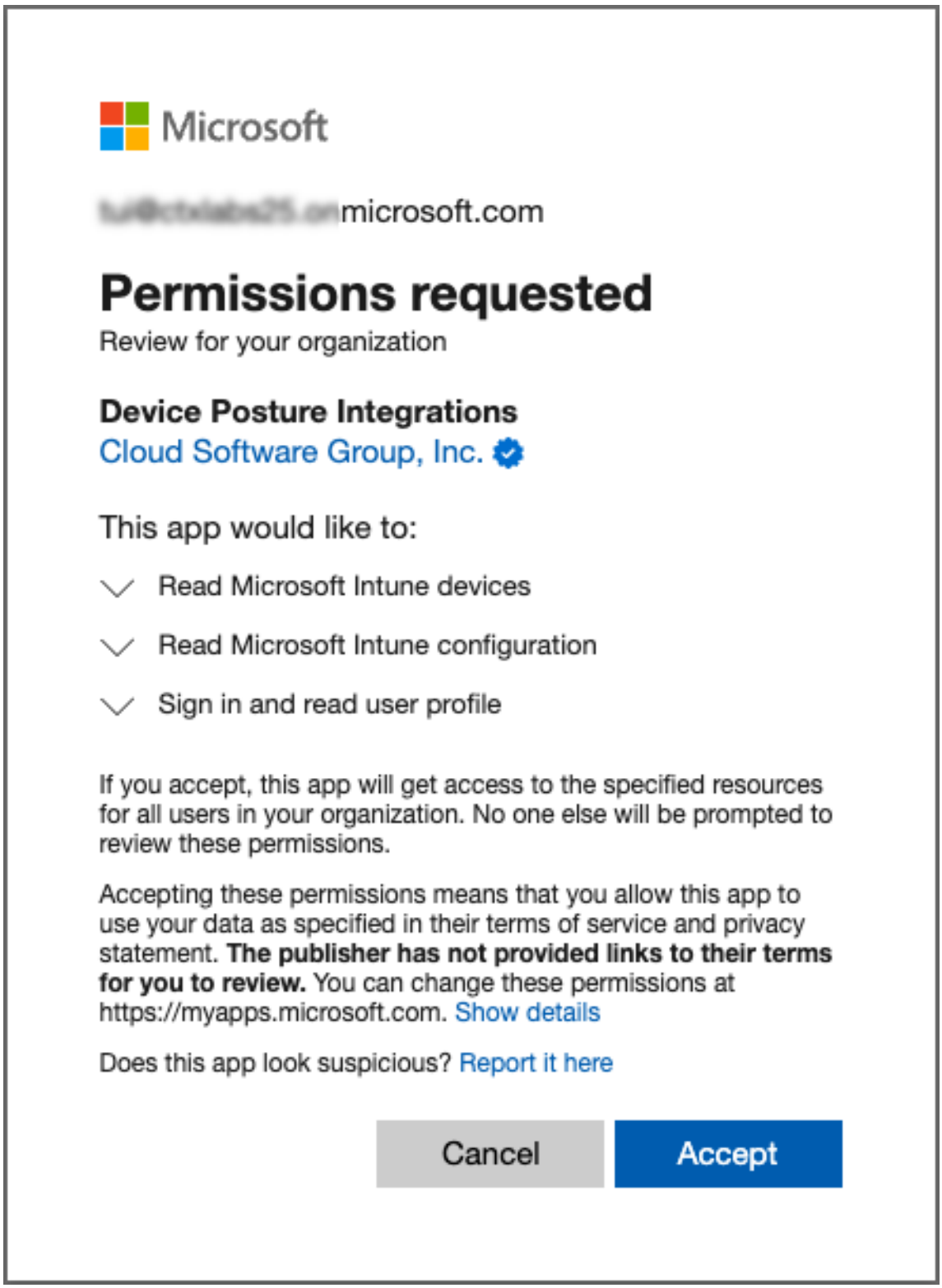
Schritt 1: Integrieren Sie die Geräteposition in Microsoft Intune

1. Verwenden Sie eine der folgenden Methoden, um auf die Registerkarte **Integrationen** zuzugreifen:
    - Greifen Sie in Ihrem Browser auf die URL https://device-posture-config.cloud.com zu und klicken Sie dann auf die Registerkarte **Integrationen**.

- Secure Private Access-Kunden - Klicken Sie auf der Benutzeroberfläche von Secure Private Access im linken Navigationsbereich auf **Gerätestatus** und dann auf die Registerkarte **Integrationen**.



2. Klicken Sie auf die **Ellipsenschaltfläche** und dann auf **Verbinden**. Der Administrator wird zur Authentifizierung zu Azure AD umgeleitet.



In der folgenden Tabelle sind die Microsoft Intune Intune-API-Berechtigungen für die Integration mit dem Device Posture-Dienst aufgeführt.

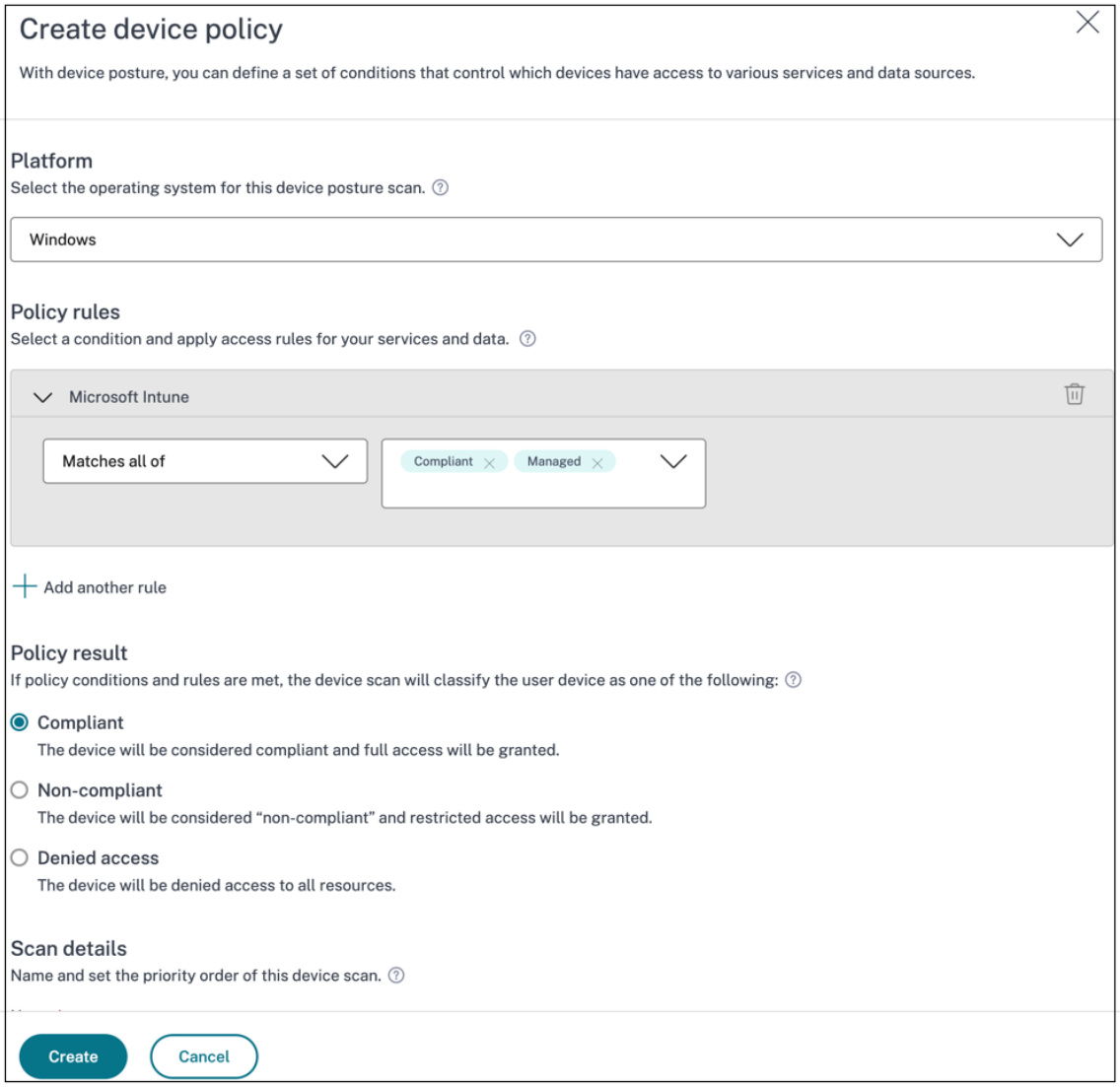
API-Name	Anspruchswert	Name der Erlaubnis	Typ
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Microsoft Intune-Geräte lesen	Anwendung
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Microsoft Intune-Geräte lesen	Anwendung

Nachdem sich der Integrationsstatus von **Nicht konfiguriert** in **Konfiguriert** geändert hat, können Administratoren eine Gerätestatusrichtlinie erstellen.

Wenn die Integration nicht erfolgreich ist, wird der Status als **Pending** angezeigt. Sie müssen auf die **Ellipsenschaltfläche** und dann auf **Erneut verbinden** klicken.

Schritt 2: Richtlinien für den Gerätestatus konfigurieren

1. Klicken Sie auf die Registerkarte **Gerätescans** und dann auf **Geräterichtlinie erstellen**.



2. Geben Sie den Namen für die Richtlinie ein und legen Sie die Priorität fest.
3. Wählen Sie die Plattform aus, für die diese Richtlinie erstellt wurde.
4. Wählen Sie für **Select Rule** die Option **Microsoft Endpoint Manager** aus.
5. Wählen Sie eine Bedingung und dann die MEM-Tags aus, die abgeglichen werden sollen.

    - Für **Matches any of** wird eine ODER-Bedingung angewendet.
    - Für **Matches all of** wird eine UND-Bedingung angewendet.

    > **Hinweis:**
    >
    > Sie können diese Regel zusammen mit anderen Regeln verwenden, die Sie für den Gerätestatus konfigurieren.

6. Wählen Sie unter **Then the device is:** basierend auf den Bedingungen, die Sie konfiguriert

haben, eine der folgenden Optionen aus.

- **Konform (voller Zugriff wird gewährt)**
- **Nicht konform (Eingeschränkter Zugriff wird gewährt)**
- **Anmeldung verweigert**

Weitere Informationen zum Erstellen einer Richtlinie finden Sie unter Konfiguration der Gerätestatus-richtlinie.

Überprüfung des Gerätezertifikats mit dem Device Posture Service

June 19, 2024

Um Gerätezertifikatsprüfungen mit dem Device Posture Service zu konfigurieren, müssen Administratoren ein Ausstellerzertifikat von ihrem Gerät importieren. Sobald ein gültiges Ausstellerzertifikat im Device Posture Service vorhanden ist, können Administratoren Gerätezertifikatsprüfungen als Teil der Gerätestatus-Richtlinien verwenden.

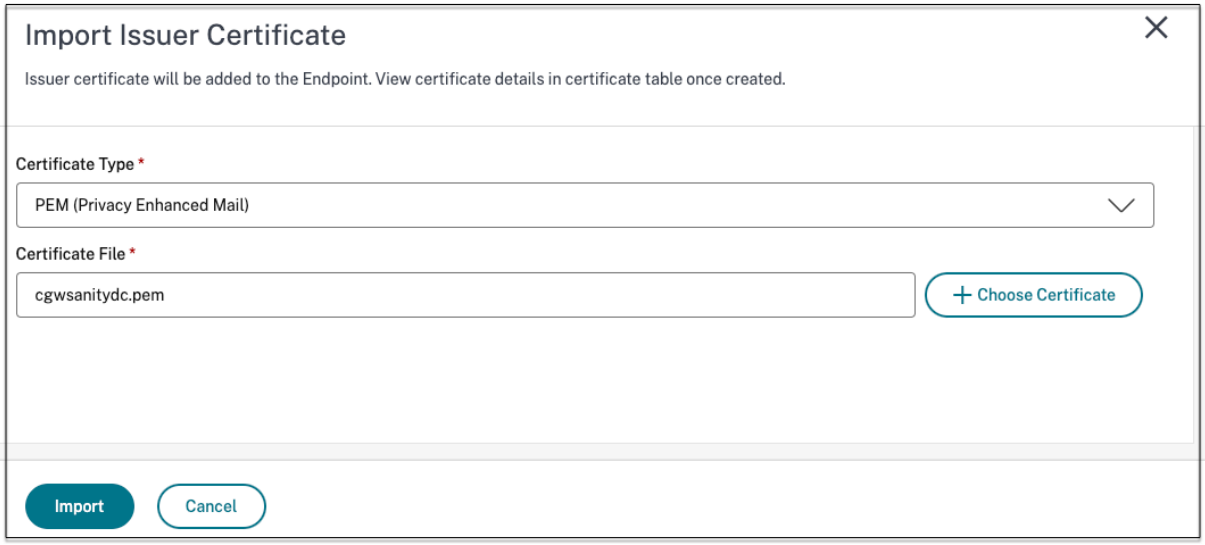
> **Zu beachtende Punkte:**
>
> - Der Device Posture Service unterstützt nur den Zertifikatstyp PEM-Aussteller.
> - Für die Gerätezertifikatsprüfung unter Windows muss der EPA-Client auf dem Endgerät mit Administratorrechten installiert sein. Für andere Prüfungen benötigen Sie keine lokalen Administratorrechte. Einzelheiten zu den unterstützten Scans finden Sie unter Unterstützte Scans nach Gerätestatus.
> - Um den EPA-Client mit Administratorrechten unter Windows zu installieren, führen Sie den folgenden Befehl an dem Ort aus, an dem das EPA-Client-Plug-In heruntergeladen wurde.
>
>   ```
>   msiexec /i epasetup.msi
>   ```
>
> - Die Überprüfung des Gerätezertifikats mit dem Device Posture Service unterstützt die Überprüfung des Zertifikatswiderrufs nicht.
> - Wenn ein Gerätezertifikat durch ein Zwischenzertifikat signiert ist, müssen Sie die komplette Kette mit den Stamm- und Zwischenzertifikaten in einer einzigen PEM-Datei hochladen.
>
>   ```
>   Example: chain.pem
>
>   -----BEGIN CERTIFICATE-----
>   ******************************
>   -----END CERTIFICATE-----
>   -----BEGIN CERTIFICATE-----
>   ```



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

Gerätezertifikat hochladen

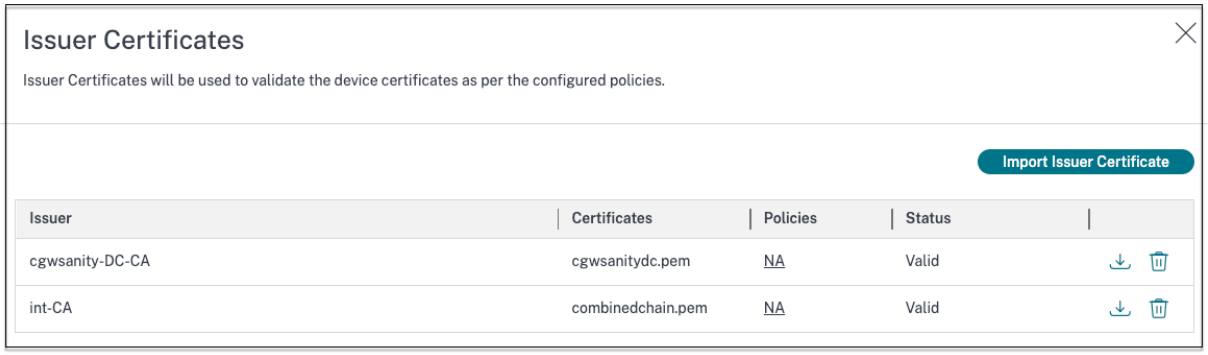
1. Klicken Sie auf der Device Posture-Startseite auf **Einstellungen** .
2. Klicken Sie auf **Verwalten**und dann auf **Zertifikat importieren**.
3. Wählen Sie **unter Zertifikatstyp**den Zertifikatstyp aus. Nur der PEM-Typ wird unterstützt.
4. Klicken Sie unter **Zertifikatsdatei**auf **Zertifikat auswählen**, um das Ausstellerzertifikat auszuwählen.
5. Klicken Sie auf **Öffnen**und dann auf **Importieren**.



Das ausgewählte Zertifikat ist **unter Einstellungen > Ausstellerzertifikate**aufgeführt. Sie können mehrere Zertifikate importieren.

Importierte Zertifikate anzeigen

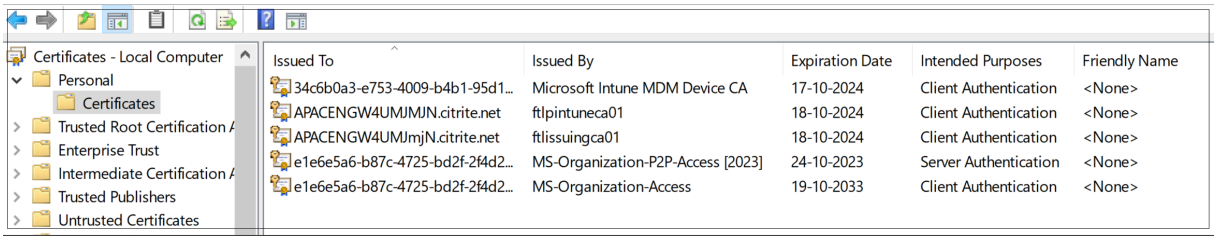
1. Klicken Sie auf der Device Posture-Startseite auf **Einstellungen** .
2. Klicken Sie unter **Issuer Certificates**auf **Manage**.
3. Auf der Seite Ausstellerzertifikate werden die importierten Ausstellerzertifikate aufgeführt.



Installieren Sie das Gerätezertifikat auf dem Endgerät

Windows:

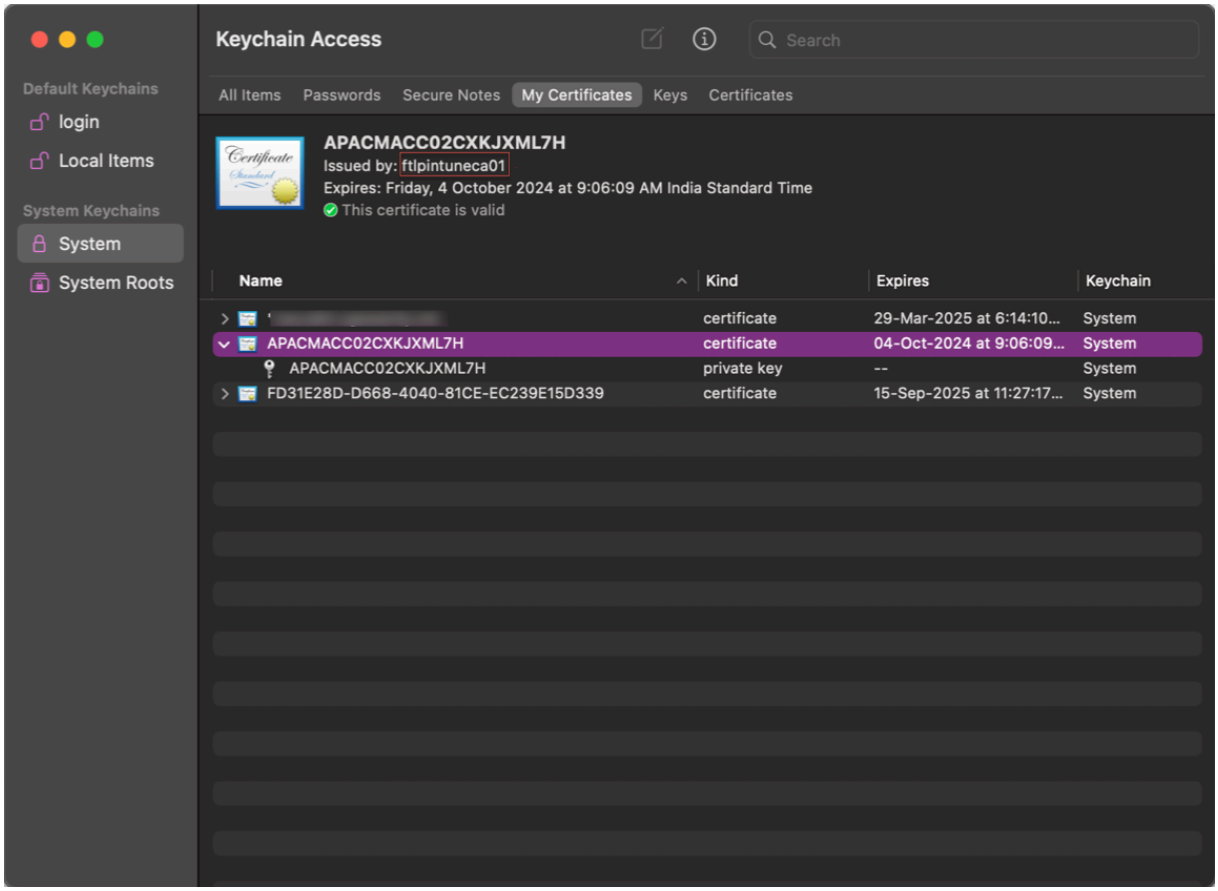
1. Öffnen Sie im **Startmenü** den **Computer Certificate Manager**.
2. Stellen Sie sicher, dass das Zertifikat in `Certificates - Local Computer\Personal\Certificates` installiert ist.
    - Zu den **beabsichtigten Zwecken** muss die **Kundenauthentifizierung** gehören.
    - Die Spalte **Ausgestellt von** muss mit dem Namen des Ausstellers übereinstimmen, der auf der Admin-GUI konfiguriert wurde.



macOS:

1. Öffnen Sie **Keychain Access** und wählen Sie dann **System** aus.
2. Klicken Sie auf **Datei > Elemente importieren**, um das Zertifikat zu importieren.

   Das Feld **Ausgestellt von** muss den Namen des Zertifikatsausstellers enthalten.



Erzwingen Sie intelligente Steuerungen auf DaaS mithilfe von Device Posture

February 16, 2024

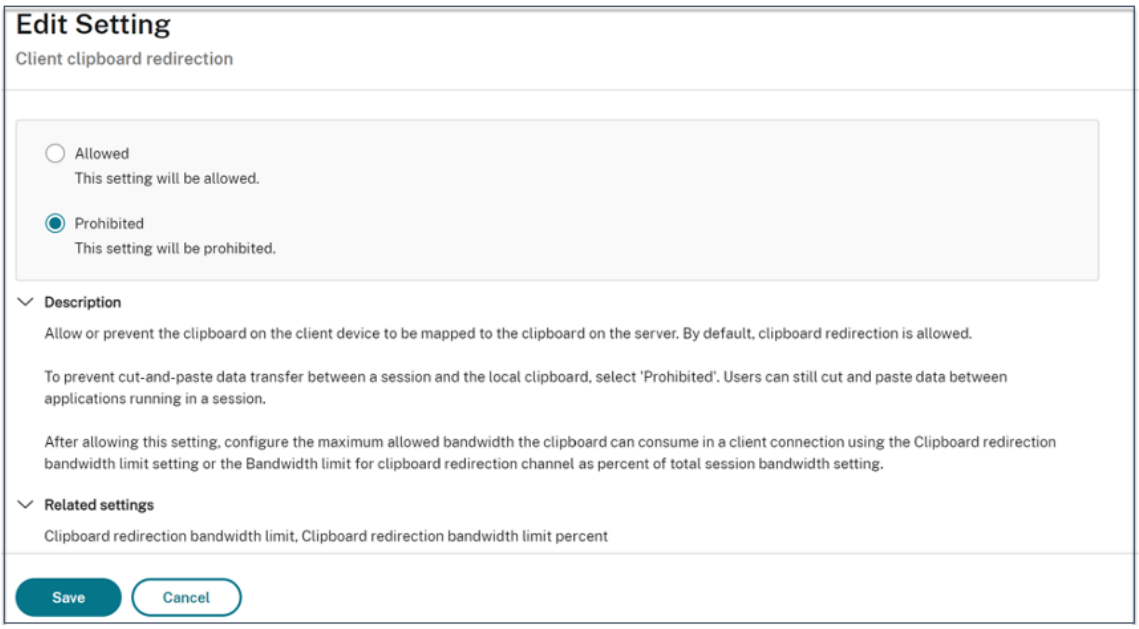
Sie können Smart Controls beim Zugriff auf die Citrix Desktop as a Service (DaaS) -Ressourcen über den Citrix Device Posture Service erzwingen.

> **Hinweis:**
>
> Dies ist keine vollständige Konfiguration, sondern ein Beispiel für die Verwendung von Device Posture zur Konfiguration von Studio-Richtlinien.

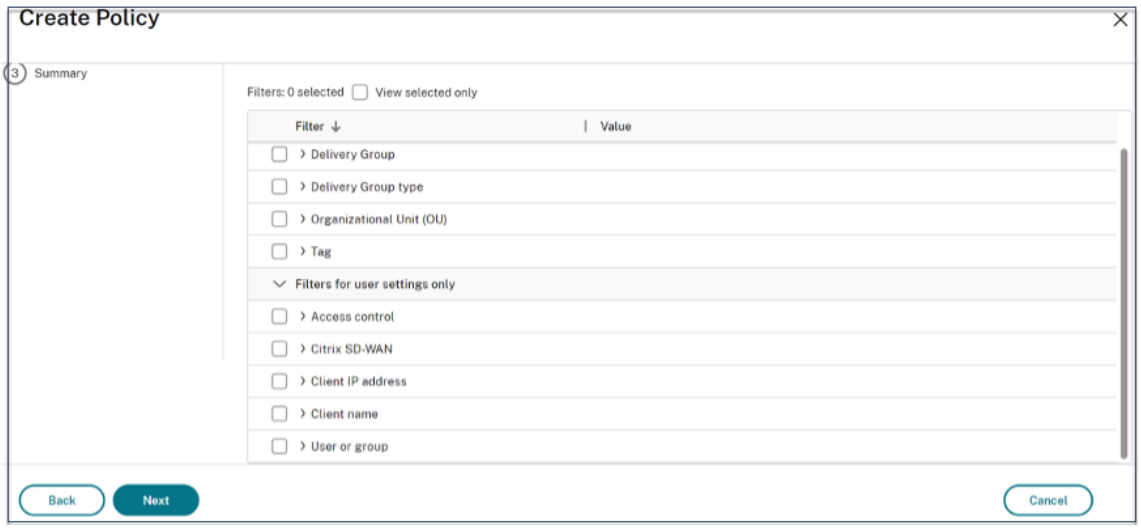
In diesem Beispiel wird eine Richtlinie erstellt, um die Funktion zum Kopieren und Einfügen auf Citrix DaaS-Ressourcen mithilfe der Device Posture Service-Tags (COMPLIANT und NON-COMPLIANT) zu deaktivieren.

Gehen Sie wie folgt vor, um die Funktion zum Kopieren und Einfügen für Benutzer zu deaktivieren, die von einem NICHT KONFORMEN Gerät auf Citrix DaaS kommen:

1. Klicken Sie auf der Konfigurationsseite für Citrix DaaS auf die Registerkarte **Verwalten**.
2. Klicken Sie auf die Registerkarte **Richtlinien**.
3. Wählen Sie **Richtlinie erstellen**.
4. Wählen Sie unter **Einstellungen auswählen** die Option **Client-Zwischenablagenumleitung** aus.
5. Wählen Sie unter **Einstellung bearbeiten**die Option **Verboten**aus, und klicken Sie dann auf **Speichern**.

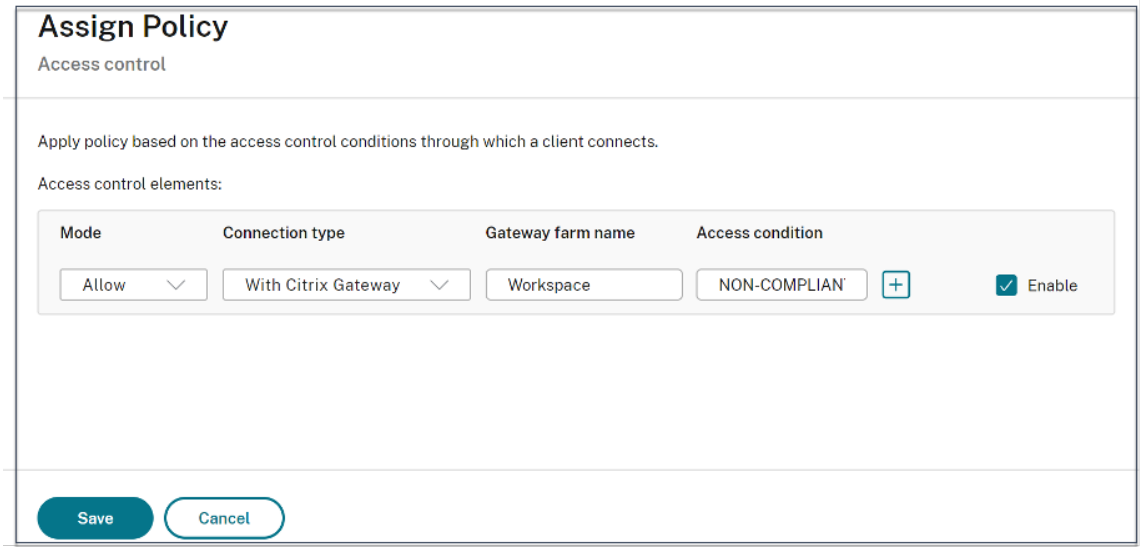


6. Klicken Sie auf der Seite **Benutzer und Maschinen** auf **Gefilterte Benutzer und Computer**, und weisen Sie diese Richtlinie dann der **Zugriffssteuerung**zu.
7. Gehen Sie zu **Nur für Benutzereinstellungen filtern** und wählen Sie **Zugriffskontrolle**aus.



8. Behalten Sie auf der Seite „ **Richtlinie zuweisen** “die Standardeinstellungen für **Modus** und **Verbindungstyp**bei.

   Geben Sie im Feld **Gateway-Farmname**den Wert **Workspace** und im Feld **Zugriffsbedingung**den Text **NON-COMPLIANT ein.**



9. Geben Sie einen Namen für die Richtlinie ein. Erwägen Sie, die Richtlinie danach zu benennen, auf wen oder was sie sich auswirkt, z. B. *eingeschränkter Zugriff auf die Zwischenablage für Geräte, die nicht den Richtlinien entsprechen*. Geben Sie optional eine Beschreibung ein.
10. Klicken Sie auf **Fertig stellen**.

> **Hinweis:**
>
> Die Richtlinie ist standardmäßig deaktiviert. Wenn Sie die Richtlinie aktivieren, kann sie sofort für die Benutzer angewendet werden, die sich anmelden. Deaktivieren der Richtlinie verhindert, dass sie angewendet wird. Wenn Sie die Priorität der Richtlinie ändern müssen oder später weitere Einstellungen hinzufügen möchten, können Sie die Richtlinie deaktivieren, bis Sie damit fertig sind, und die Richtlinie dann anwenden.

Validieren der Richtlinienkonfiguration

Überprüfen Sie Ihre Richtlinien, um sicherzustellen, dass sie wie vorgesehen funktionieren, bevor Sie diese Richtlinien umfassend implementieren. Im Konfigurationsbeispiel:

- Für Benutzer, die von einem KONFORMEN Endgerät kommen, müssen die Citrix DaaS-Ressourcen ohne die Einschränkungen beim Kopieren und Einfügen aufgelistet werden.
- Für Benutzer, die von einem NICHT KONFORMEN Endgerät kommen, müssen die Citrix DaaS-Ressourcen mit den Einschränkungen beim Kopieren und Einfügen aufgelistet werden.

Überwachen und Problembehandlung

June 19, 2024

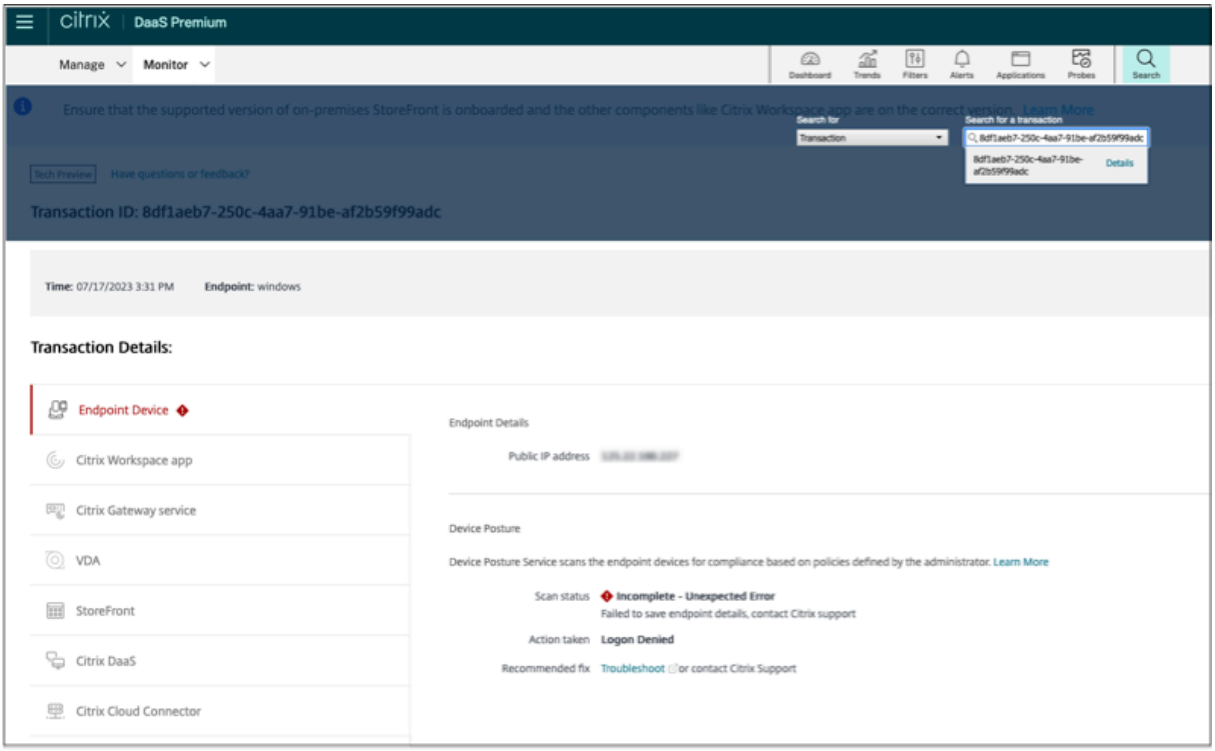
Die Ereignisprotokolle zur Gerätehaltung können an zwei Stellen eingesehen werden:

- 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.

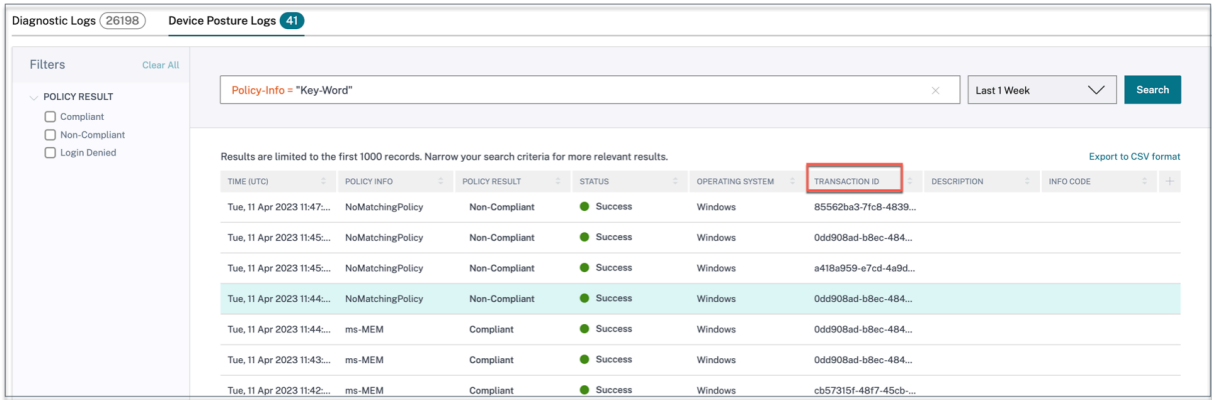
1. Kopieren Sie die Transaktions-ID der fehlgeschlagenen Sitzung oder der Sitzung mit verweigertem Zugriff vom Endbenutzergerät.
2. Melden Sie sich bei Citrix Cloud an.
3. Klicken Sie auf der DaaS-Kachel auf **Verwalten**und dann auf die Registerkarte **Überwachen** . Suchen Sie in der Monitor-Benutzeroberfläche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

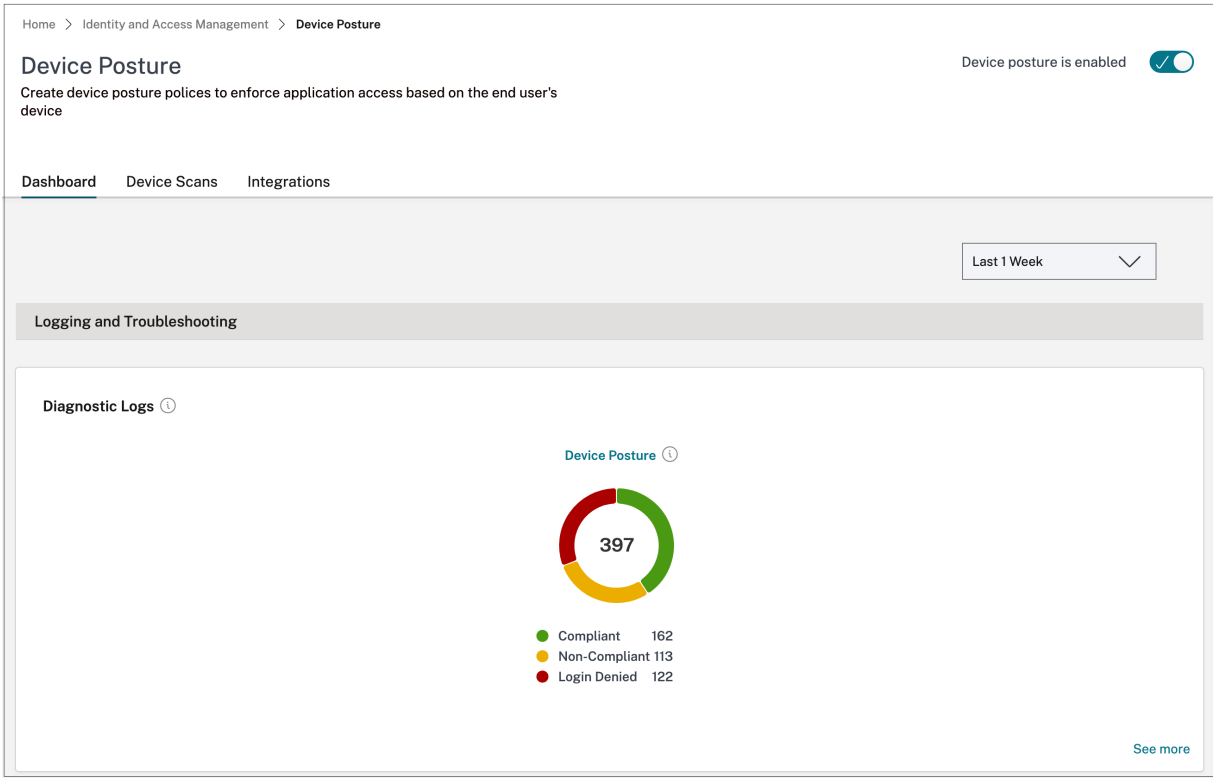
- Konnte konfigurierte Richtlinien nicht lesen

- 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.

Citrix Endpoint Analysis Client für Device Posture Service verwalten

June 19, 2024

Der Citrix Device Posture Service ist eine cloudbasierte Lösung, mit der Administratoren bestimmte Anforderungen durchsetzen können, 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 Device Posture Scans auf einem Endgerät auszuführen, müssen Sie den Citrix EndPoint Analysis (EPA) -Client, eine einfache Anwendung, auf diesem Gerät installieren. Der Device Posture Service wird immer mit der neuesten Version des von Citrix veröffentlichten EPA-Clients ausgeführt.

Installation des EPA-Clients

Während der Laufzeit fordert der Device Posture Service den Endbenutzer auf, den EPA-Client während der Laufzeit herunterzuladen und zu installieren. Einzelheiten finden Sie unter Endbenutzer-Flow.
Normalerweise benötigt ein EPA-Client keine lokalen Administratorrechte, um ihn herunterzuladen und auf einem Endpunkt zu installieren. Um Scans zur Überprüfung von Gerätezertifikaten auf einem Endgerät durchzuführen, muss der EPA-Client jedoch mit Administratorzugriff installiert sein. 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 standardmäßig nach der ersten Installation aktualisiert. Das automatische Upgrade stellt sicher, dass die Endbenutzergeräte immer auf der neuesten Version des EPA-Clients ausgeführt werden, die mit dem Device Posture Service kompatibel ist. Für das automatische Upgrade muss der EPA-Client mit Administratorzugriff installiert worden sein.

> **Hinweis:**
>
> Das automatische Upgrade befindet sich in der Vorschauversion. Melden Sie sich für die

> Vorschau an mit https://podio.com/webforms/29214695/2384946.

Vertrieb 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.

- Das**EPA-Clientinstallationsprogramm ist in die Citrix Workspace Workspace-App integriert:** Das EPA-Clientinstallationsprogramm ist in die Citrix Workspace Workspace-App 2402 LTSR für Windows integriert. Diese Integration macht es für Endbenutzer überflüssig, den EPA-Client nach der Installation der Citrix Workspace Workspace-App separat zu installieren.

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

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

- **Verteilen Sie den Client mithilfe von GACS**: GACS ist eine von Citrix bereitgestellte Lösung zur Verwaltung der Verteilung von clientseitigen Agenten (Plug-ins). Der in GACS verfügbare Auto Update Service stellt sicher, dass auf den Endgeräten die neuesten EPA-Versionen installiert sind, ohne dass der Endbenutzer eingreifen muss. Weitere Informationen zu GACS finden Sie unter So verwenden Sie den Global App Configuration Service.

> **Hinweis:**
>
> - GACS wird auf Windows-Geräten nur für die Verteilung des EPA-Clients unterstützt.

> - Um einen EPA-Client über GACS zu verwalten, installieren Sie die Citrix Workspace Application (CWA) auf den Endgeräten.
> - Wenn CWA mit Administratorrechten auf einem Endbenutzergerät installiert ist, installiert GACS den EPA-Client mit denselben Administratorrechten.
> - Wenn CWA mit Benutzerrechten auf einem Endbenutzergerät installiert ist, installiert GACS den EPA-Client mit denselben Benutzerrechten.

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

Verwaltung 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
- NetScaler-basiertes On-Premise-Gateway mit EPA

Der Device Posture Service überträgt die neueste Version des EPA-Clients auf die Endgeräte. Auf 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 dieselbe Version haben.
- **Unverzichtbar**: Die EPA-Client-Version auf dem Endgerät muss innerhalb des auf NetScaler konfigurierten Bereichs liegen.
- **Niemals**: Das Endgerät kann eine beliebige Version des EPA-Clients haben.

Weitere Informationen finden Sie unter Verhalten von Plug-ins.

Überlegungen bei der 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 EPA-Client-Version ausgeführt wird, während NetScaler auf einer anderen Version des EPA-Clients läuft. Dies kann dazu führen, dass die EPA-Client-Version auf NetScaler und dem Endgerät nicht übereinstimmt. Daher fordert NetScaler den Endbenutzer möglicherweise auf, die EPA-Clientversion zu installieren, die auf NetScaler vorhanden ist. Um diesen Konflikt zu vermeiden, empfehlen wir die folgenden Konfigurationsänderungen:

- Wenn Sie EPA mit adaptiver Authentifizierung oder on-premises Authentifizierung oder virtuellem Gateway-Server konfiguriert haben, wird empfohlen, die Versionskontrolle des EPA-Clients auf NetScaler zu deaktivieren. Dadurch wird sichergestellt, dass der GACS- oder Device Posture Service nicht die neueste Version des EPA-Clients auf die Endgeräte überträgt.

- Die EPA-Versionskontrolle kann mithilfe der CLI oder der GUI auf **Nie** gesetzt werden. Diese Konfigurationsänderungen werden auf NetScaler 13.x und späteren Versionen unterstützt.
  - CLI: Verwenden Sie die CLI-Befehle für adaptive Authentifizierung und virtuellen Authentifizierungsserver on-premises.
  - GUI: Verwenden Sie die GUI für den virtuellen Gateway-Server on-premises. Einzelheiten finden Sie unter Steuern des Upgrades 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
<!--NeedCopy-->
```

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.