Gerätestatus

Machine translated content

Disclaimer

Contents

Gerätestatus

February 16, 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 einen Zero-Trust-basierten Zugriff zu implementieren, ist es wichtig, das Vertrauen zwischen Geräten herzustellen, indem der Status des Geräts überprüft wird. Der Device Posture Service setzt die Zero-Trust-Prinzipien in Ihrem Netzwerk durch, indem er die Endgeräte auf Konformität (verwaltet/BYOD und Sicherheitsstatus) überprüft, bevor ein Endbenutzer sich anmelden kann.

Voraussetzungen

- Lizenzanforderungen: Die Berechtigung für den Citrix Device Posture Service ist Teil der Lizenzen Citrix DaaS Premium, Citrix DaaS Premium Plus und Citrix Secure Private Access Advanced. Kunden mit anderen Lizenzen können eine Device Posture Service-Lizenz als Add-on erwerben. Für ein Add-on müssen Kunden eine eigenständige Adaptive Authentication-SKU erwerben, müssen diese aber nicht unbedingt bereitstellen, um den Device Posture Service nutzen zu können.
- Unterstützte Plattformen:
  - Windows (10 und 11)
  - macOS 13 Ventura
  - macOS 12 Monterey
  - iOS
  - IGEL

> **Hinweis:**
>
> - Ein Gerät, das auf einer Plattform läuft, die nicht unterstützt wird, ist standardmäßig als nicht konform gekennzeichnet. Sie können die Klassifizierung auf der Seite "Gerätestatus"auf der Registerkarte **Einstellungen** von **Nicht konform** in **Anmeldung verweigert** ändern.
> - Ein Gerät, das auf einer unterstützten Plattform läuft, aber keiner vordefinierten Gerätezustandsrichtlinie entspricht, wird standardmäßig als nicht konform markiert. Sie können die Klassifizierung auf der Seite "Gerätestatus"auf der Registerkarte **Einstellungen** von **Nicht konform** in **Anmeldung verweigert** ändern.

> - Für die iOS-Unterstützung im Device Posture Service ist der EPA-Client als Teil der Citrix Workspace-App für iOS integriert. Einzelheiten zu den Versionen finden Sie unter Citrix Workspace-App für iOS.
> - Für die Unterstützung von IGEL OS im Device Posture Service ist der EPA-Client als Teil des IGEL OS integriert. Wenden Sie sich an das IGEL-Supportteam, um den EPA-Client auf den IGEL-Geräten zu installieren.

- Citrix Device Posture Client (EPA-Client): Eine einfache Anwendung, die auf dem Endgerät installiert werden muss, um Gerätestatusscans auszuführen. Diese Anwendung benötigt keine lokalen Administratorrechte, um sie herunterzuladen und auf einem Endpunkt zu installieren.

  > **Hinweis:**
  >
  > Wenn Sie eine Gerätezertifikatsprüfung verwenden, müssen Sie den EPA-Client mit Administratorrechten installieren.

- Unterstützte Browser: Chrome, Edge und Firefox.
- Firewall-Konfiguration: Damit der Device Posture Service die EPA-Clients auf einem Endgerät aktualisieren kann, muss die Firewall/der Proxy so konfiguriert sein, dass die folgenden Domänen zugelassen werden:
  - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
  - `https://productioniconstorage.blob.core.windows.net`
  - *.netscalergateway.net
  - *.nssvc.net
  - *.cloud.com
  - *.pendo.io
  - *.citrixworkspacesapi.net

Preview-Features

- Device Posture Service mit IGEL. Melden Sie sich für die Vorschau an mit https://podio.com/webforms/29062020/2362942.
- Device Posture Service mit iOS. Melden Sie sich für die Vorschau an mit https://podio.com/webforms/28888524/2338366.
- Geolocationprüfung und Netzwerkstandortprüfung. Melden Sie sich für die Vorschau an mit https://podio.com/webforms/29051759/2362665.
- CrowdStrike-Integration mit dem Device Posture Service. Einzelheiten finden Sie unter CrowdStrike-Integration mit Device Posture —Vorschau.

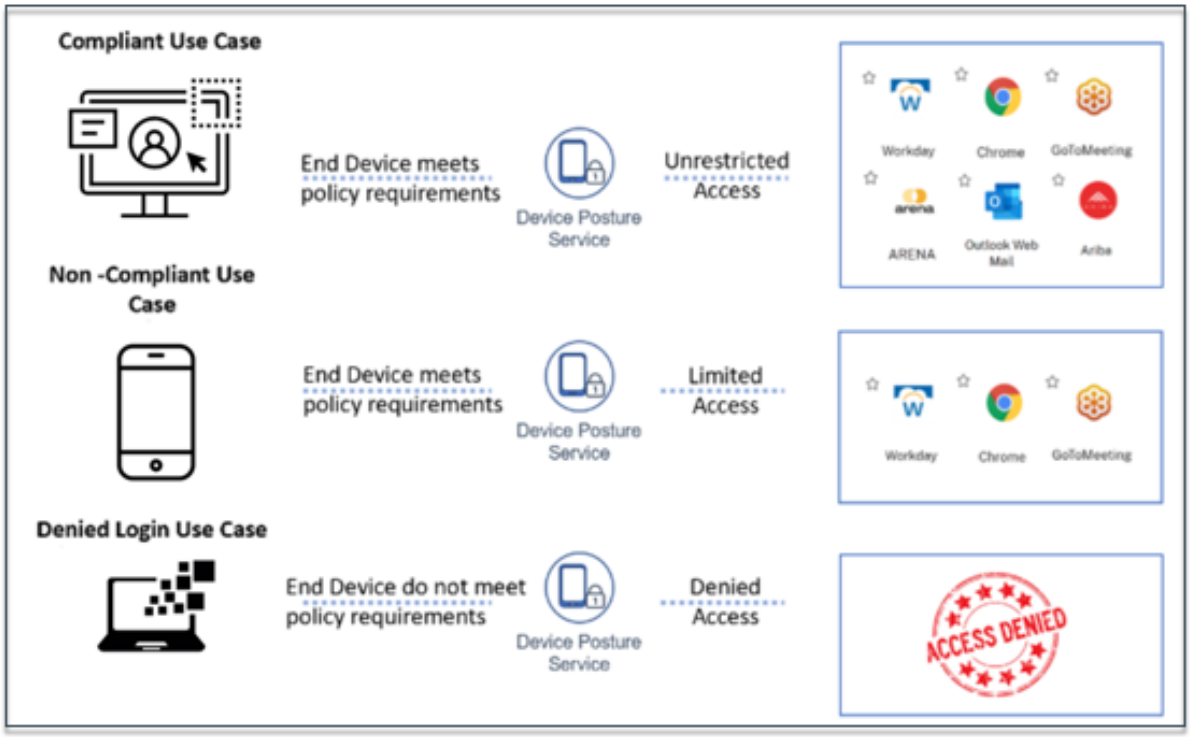
Funktionsweise

Die Administratoren können Richtlinien für den Gerätestatus erstellen, um den Status der Endgeräte zu überprüfen und festzustellen, ob die Anmeldung für ein Endgerät zulässig ist oder verweigert wird. Die Geräte, die sich anmelden dürfen, werden außerdem als konform oder nicht konform eingestuft. Benutzer können sich über einen Browser oder die Citrix Workspace-App anmelden.

Im Folgenden sind die allgemeinen Bedingungen aufgeführt, anhand derer ein Gerät als konform, nicht konform und als verweigerte Anmeldung eingestuft wird.

- **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.
- **Anmeldung verweigert:** - Einem Gerät, das die Richtlinienanforderungen nicht erfüllt, wird die Anmeldung verweigert.

Die Klassifizierung von Geräten als **konform**, **nicht konform**und **verweigerte Anmeldung** wird an den Citrix DaaS- und Citrix Secure Private Access-Dienst weitergegeben, der wiederum die Geräteklassifizierung verwendet, um intelligente Zugriffsfunktionen bereitzustellen.



> **Hinweis:**
>
> - Die Richtlinien zum Gerätestatus müssen für jede Plattform spezifisch konfiguriert werden. Für macOS kann ein Administrator beispielsweise den Zugriff für Geräte mit einer bestimmten Betriebssystemversion gewähren. In ähnlicher Weise kann der Administrator für Windows Richtlinien so konfigurieren, dass sie eine bestimmte Autorisierungsdatei, Registrierungseinstellungen usw. enthalten.
> - Scans der Geräteposition werden nur während der Vorauthentifizierung/vor der Anmeldung durchgeführt.
> - Definitionen von “konform”und “nicht konform”finden Sie unter Definitionen.

Vom Gerätestatus unterstützte Scans

Die folgenden Scans werden vom Citrix Device Posture Service unterstützt:

Windows	macOS	iOS	IGEL
Citrix Workspace-App	Citrix Workspace-App	Citrix Workspace-App	-
Betriebssystemversion	Betriebssystemversion	Betriebssystemversion	-
Datei (existiert, Dateiname und Pfad)	Datei (existiert, Dateiname und Pfad)	-	Datei (existiert, Dateiname und Pfad)
Geolocation	Geolocation	-	-
Standort im Netzwerk	Standort im Netzwerk	-	-
MAC-Adresse	MAC-Adresse	-	-
Prozess (vorhanden)	Prozess (vorhanden)	-	-
Microsoft Endpoint Manager	Microsoft Endpoint Manager	-	-
CrowdStrike	CrowdStrike	-	-
Gerätezertifikat	Gerätezertifikat	-	-
Browser	Browser	-	-
Antivirus	Antivirus	-	-
Nichtnumerische Registrierung (32 Bit)	-	-	-
Nichtnumerische Registrierung (64 Bit)	-	-	-
Numerische Registrierung (32 Bit)	-	-	-

Windows	macOS	iOS	IGEL
Numerische Registrierung (64 Bit)	-	-	-
Windows Update-Installationstyp	-	-	-
Windows Update-Installation — Überprüfung des letzten Updates	-	-	-

> **Hinweis:**
>
> - Für die iOS-Unterstützung im Device Posture Service ist der EPA-Client als Teil der Citrix Workspace-App für iOS integriert. Einzelheiten zu den Versionen finden Sie unter Citrix Workspace-App für iOS.

Integration von Drittanbietern in Device Posture

Zusätzlich zu den vom Device Posture Service angebotenen nativen Scans kann der Dienst auch in die folgenden Drittanbieterlösungen unter Windows und macOS integriert werden.

- Microsoft Intune. Einzelheiten finden Sie unter Microsoft Intune-Integration mit Device Posture.
- CrowdStrike. Einzelheiten finden Sie unter CrowdStrike-Integration mit Device Posture — Vorschau.

Gerätestatus konfigurieren

Der Gerätestatus ist eine Kombination aus Richtlinien und Regeln, die ein Gerät erfüllen muss, um Zugriff auf die Ressourcen zu erhalten. Jeder Richtlinie ist eine der Aktionen zugeordnet, nämlich konform, nicht konform und Anmeldung verweigert. Darüber hinaus ist jede Richtlinie mit einer Priorität verknüpft, und die Bewertung der Richtlinie wird beendet, wenn eine Richtlinie als wahr bewertet wird und die zugehörigen Maßnahmen ergriffen werden.

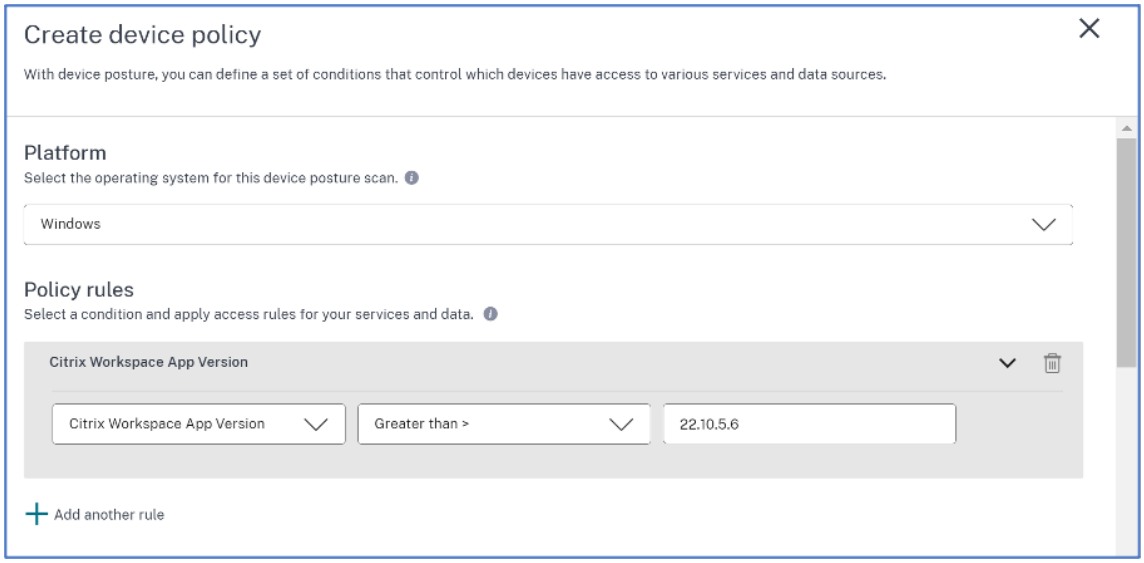
1. Melden Sie sich bei Citrix Cloud an und wählen Sie dann im Hamburger-Menü **Identitäts- und Zugriffsverwaltung** aus.
2. Klicken Sie auf die Registerkarte **Gerätestatus** und dann auf **Verwalten**.

> **Hinweis:**
>
> - Kunden des Secure Private Access Service können in der Admin-Benutzeroberfläche in der linken Navigationsleiste direkt auf **Device Posture** klicken.
> - Erstbenutzer werden auf der Landingpage des Gerätestatus aufgefordert, eine Gerätestatusrichtlinie zu erstellen. Die Gerätestatusrichtlinie muss für jede Plattform individuell konfiguriert werden. Sobald Sie eine Gerätestatusrichtlinie erstellt haben, wird diese unter den entsprechenden Plattformen aufgeführt.
> - Eine Richtlinie tritt erst in Kraft, nachdem der Gerätestatus aktiviert wurde. Um den Gerätestatus zu aktivieren, stellen Sie den Schalter **Gerätestatus ist deaktiviert** in der rechten oberen Ecke auf **ON**.

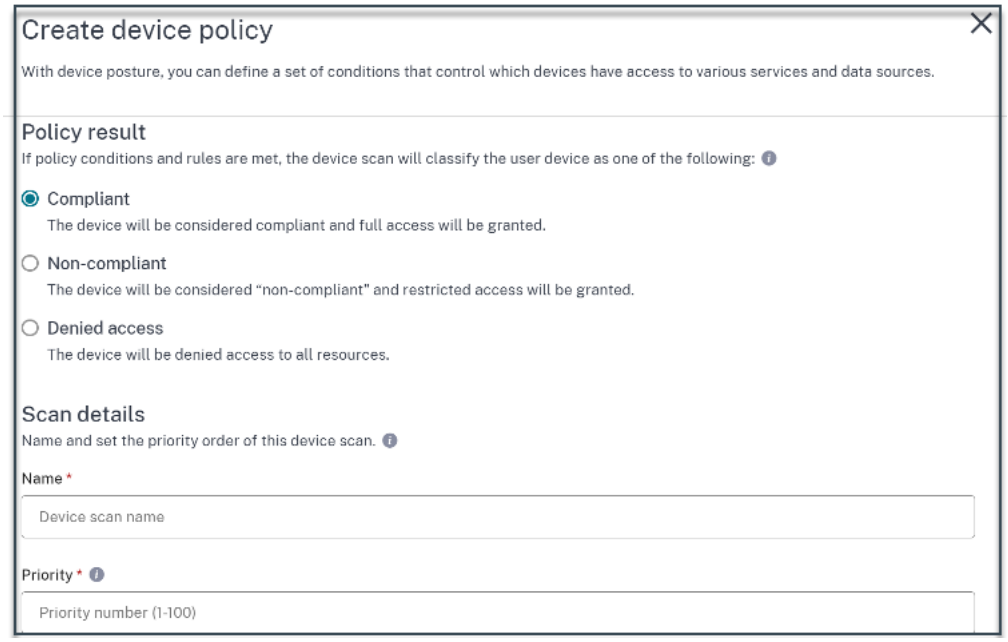
3. Klicken Sie auf **Geräterichtlinie erstellen**.
4. Wählen Sie unter **Plattform**die Plattform aus, für die Sie eine Richtlinie anwenden möchten. Sie können die Plattform von Windows auf macOS oder umgekehrt ändern, unabhängig von der Registerkarte, die Sie auf der Device Posture Homepage ausgewählt haben.
5. Wählen Sie unter **Richtlinienregeln**die Prüfung aus, die Sie im Rahmen des Gerätestatus durchführen möchten, und wählen Sie die Bedingungen aus, die erfüllt werden müssen.

> **Hinweis:**
>
> - Stellen Sie bei der Überprüfung des Gerätezertifikats sicher, dass das Ausstellerzertifikat auf dem Gerät vorhanden ist. Andernfalls können Sie bei der Erstellung der Device Posture-Richtlinie ein Gerätezertifikat importieren oder das Zertifikat über die **Einstellungen** auf der Device Posture-Startseite hochladen. Einzelheiten finden Sie unter Gerätezertifikat importieren beim Erstellen der Richtlinie für das Gerätezertifikat und Gerätezertifikat hochladen.
> - Für die Prüfung des Gerätezertifikats muss der EPA-Client auf dem Endgerät mit Administratorrechten installiert sein.
> - Die Überprüfung von Gerätezertifikaten mit dem Device Posture Service unterstützt die Überprüfung des Zertifikatswiderrufs nicht.

6. Klicken Sie auf **Weitere Regel hinzufügen**, um mehrere Regeln zu erstellen. Eine UND-Bedingung wird auf mehrere Regeln angewendet.



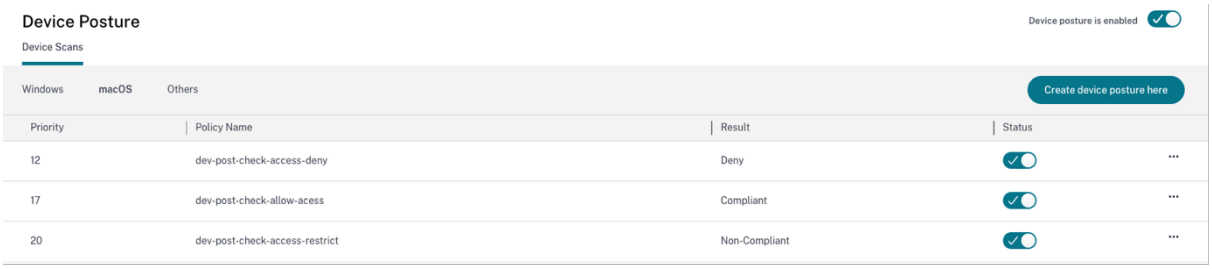
7. Wählen Sie unter **Richtlinienergebnis** basierend auf den von Ihnen konfigurierten Bedingungen den Typ aus, unter dem der Gerätescan das Benutzergerät klassifizieren muss.
   - Konform
   - Nicht konform
   - Zugriff verweigert
8. Geben Sie einen Namen für die Richtlinie ein.
9. Geben Sie im Feld **Priorität**die Reihenfolge ein, in der die Richtlinien bewertet werden müssen.
   - Sie können einen Wert zwischen 1 und 100 eingeben. Es wird empfohlen, Ablehnungsrichtlinien mit einer höheren Priorität zu konfigurieren, gefolgt von „Nicht konform“und schließlich „konform“.
   - Die Priorität mit dem niedrigeren Wert hat die höchste Präferenz.
   - Nur die aktivierten Richtlinien werden anhand der Priorität bewertet.
10. Klicken Sie auf **Erstellen**.



> **Wichtig:**
>
> Sie müssen den Schalter **Bei Erstellung aktivieren** auf **ON** stellen, damit die Richtlinien zum Gerätestatus wirksam werden. Bevor Sie die Richtlinien aktivieren, sollten Sie sicherstellen, dass die Richtlinien korrekt konfiguriert sind und dass Sie diese Aufgaben in Ihrem Test-Setup ausführen.

Gerätestatusrichtlinie bearbeiten

Die konfigurierten Gerätestatusrichtlinien sind unter der jeweiligen Plattform auf der Seite **Gerätescans** aufgeführt. Auf dieser Seite können Sie nach der Richtlinie suchen, die Sie bearbeiten möchten. Sie können auf dieser Seite auch eine Richtlinie aktivieren, deaktivieren oder löschen.



Kontextbezogenen Zugriff (Smart Access) mit Gerätestatus konfigurieren

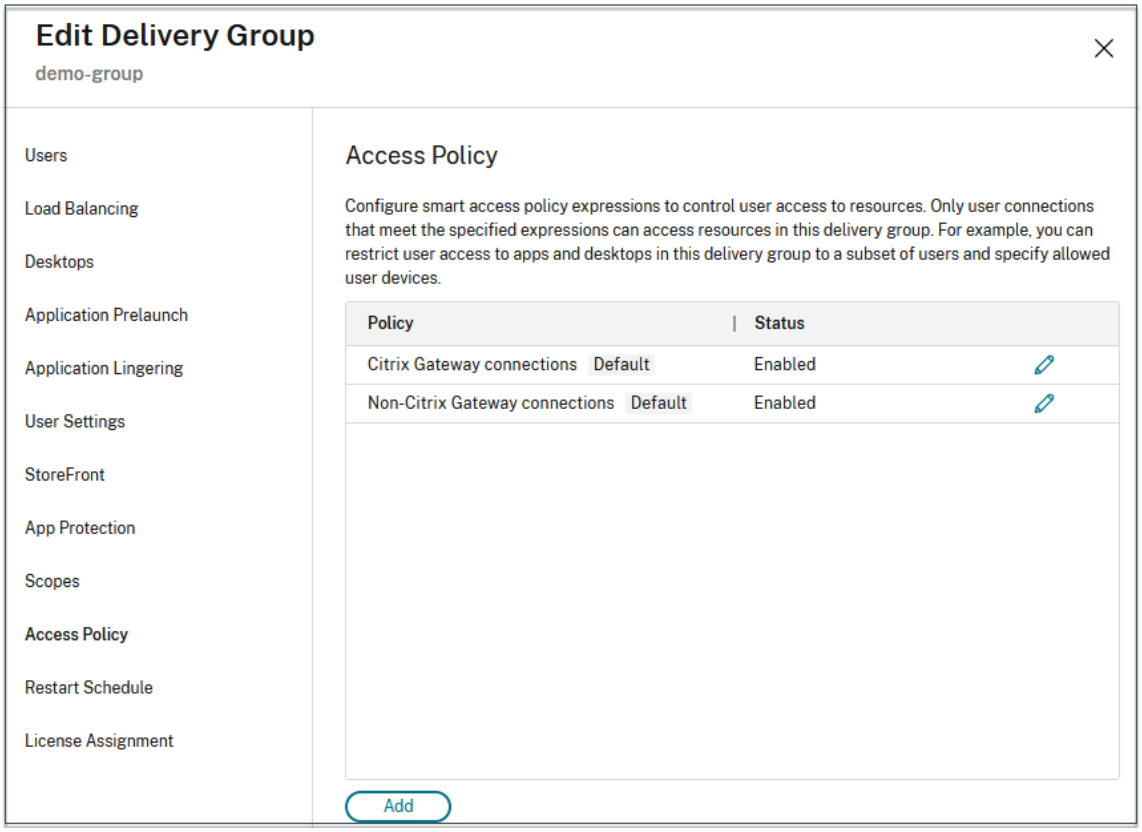
Nach der Überprüfung der Gerätehaltung darf sich das Gerät anmelden und wird als konform oder nicht konform eingestuft. Diese Informationen sind als Tags für den Citrix DaaS-Dienst und den Citrix Secure Private Access-Dienst verfügbar und werden verwendet, um den kontextbezogenen Zugriff auf

der Grundlage der Gerätehaltung bereitzustellen. Daher müssen Citrix DaaS und Citrix Secure Private Access so konfiguriert werden, dass die Zugriffskontrolle mithilfe von Device Posture Tags erzwungen wird.

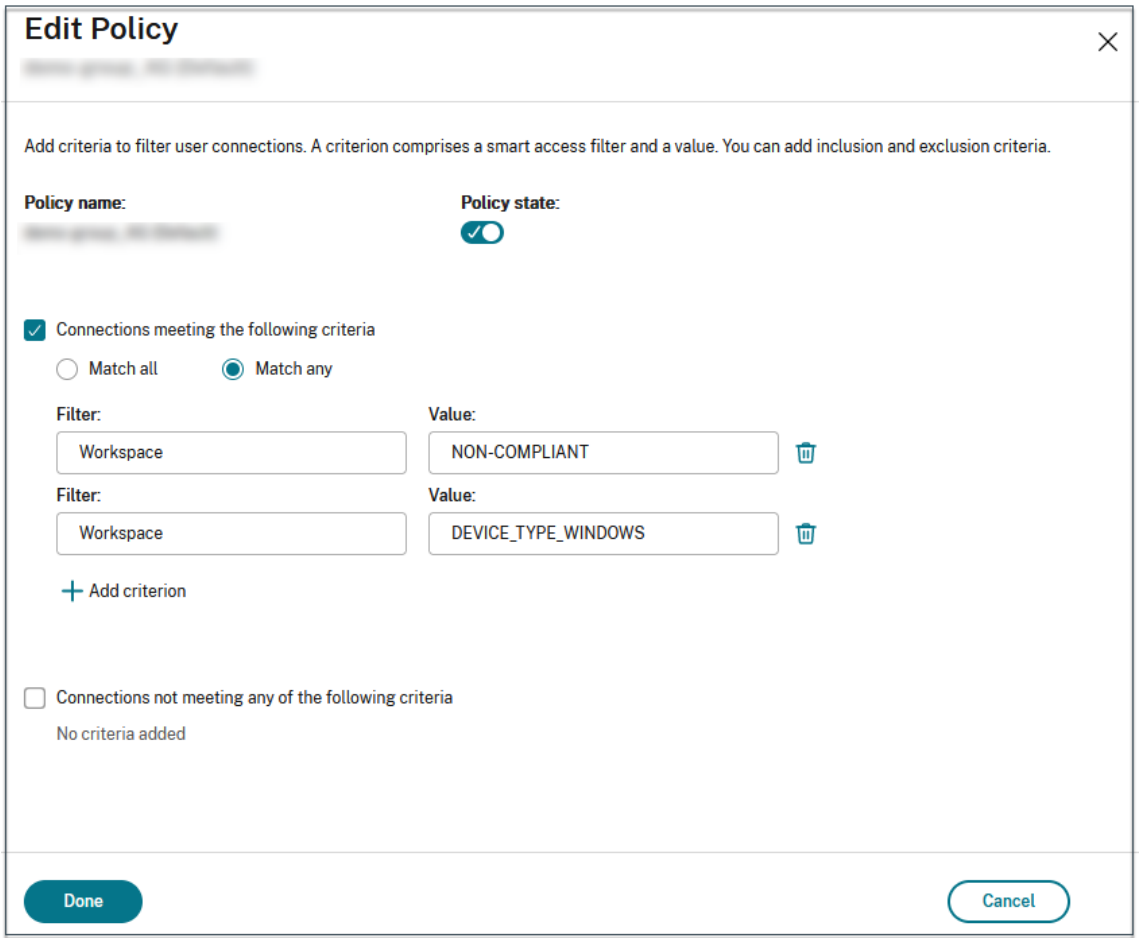
Citrix DaaS-Konfiguration mit Device Posture mithilfe der neuen Studio-Benutzeroberfläche (Vorschau)

Melde dich für die Vorschau an.

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der **DaaS-Kachel** auf **Verwalten**.
3. Gehen Sie im linken Menü zum Abschnitt **Delivery Group** .
4. Wählen Sie die Bereitstellungsgruppe aus, für die Sie die Zugriffskontrolle basierend auf dem Gerätestatus konfigurieren möchten, und klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf der Seite **Bereitstellungsgruppe bearbeiten** auf **Access Policy**.
6. Klicken Sie in der Zeile **Citrix Gateway-Verbindungen** auf das Bearbeitungssymbol, um die Gateway-Verbindungsrichtlinie zu bearbeiten.



a) Wählen Sie auf der Seite “Richtlinie bearbeiten”die Option **Verbindungen, die folgende Kriterien erfüllen**.
b) Wählen Sie **Mit beliebigem übereinstimmen** aus, und klicken Sie dann auf **Kriterium hinzufügen**.
c) Fügen Sie Kriterien für alle Standort-Tags hinzu, die Sie unter Netzwerkstandorte konfigurieren konfiguriert haben: Geben Sie **Workspace** für **Filter** und **COMPLIANT** oder **NON-COMPLIANT** für **Value** ein.



Hinweis:

Die Syntax für die Geräteklassifizierungs-Tags muss auf dieselbe Weise eingegeben werden, wie sie zuvor erfasst wurde, d. h. ausschließlich in Großbuchstaben (**COMPLIANT** und **NON-COMPLIANT**). Andernfalls funktionieren die Gerätestatusrichtlinien nicht wie vorgesehen.

Zusätzlich zu den Geräteklassifizierungs-Tags gibt der Device Posture Service auch das Betriebssystem-Tag und das dem Gerät zugeordnete Zugriffsrichtlinien-Tag zurück. Die Betriebssystem-Tags und die Zugriffsrichtlinien-Tags dürfen nur in Großbuchstaben eingegeben werden.

> - DEVICE_TYPE_WINDOWS
> - DEVICE_TYPE_MAC
> - Genauer Richtlinienname (Großbuchstaben)

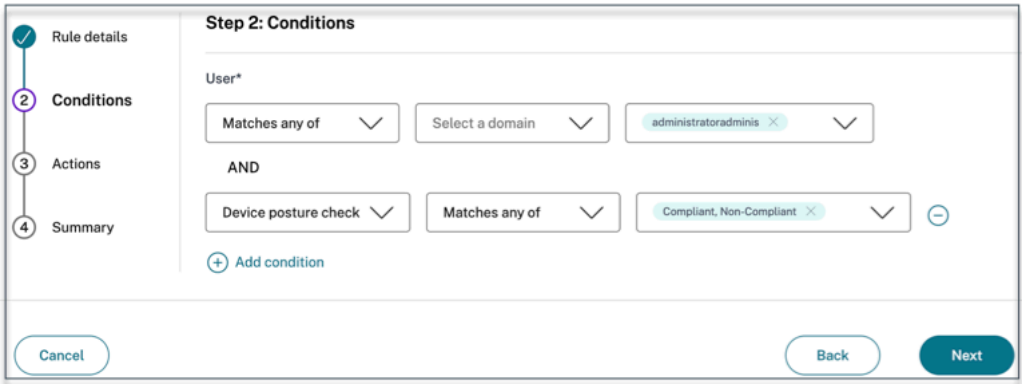
Citrix Secure Private Access-Konfiguration mit Device Posture

1. Melden Sie sich bei Citrix Cloud an.
2. Klicken Sie auf der Kachel Secure Private Access auf **Verwalten** .
3. Klicken Sie im linken Navigationsbereich auf **Richtlinien zugreifen** und dann auf **Richtlinie erstellen**.
4. Geben Sie den Richtliniennamen und die Beschreibung der Richtlinie ein.
5. Wählen Sie unter **Anwendungen** die App oder die Gruppe von Apps aus, für die diese Richtlinie durchgesetzt werden muss.
6. Klicken Sie auf **Regel erstellen**, um Regeln für die Richtlinie zu erstellen.
7. Geben Sie den Regelnamen und eine kurze Beschreibung der Regel ein, und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Bedingungen der Benutzer aus. Die **Benutzerbedingung** ist eine zwingende Voraussetzung, die erfüllt sein muss, um den Benutzern Zugriff auf die Anwendungen zu gewähren.
9. Klicken Sie auf **+**, um den Zustand der Gerätehaltung hinzuzufügen.
10. Wählen Sie **Device Posture Check** und den logischen Ausdruck aus dem Drop-down-Menü aus.
11. Geben Sie einen der folgenden Werte in benutzerdefinierte Tags ein:
    - Konform —Für konforme Geräte
    - Nicht konform —Für Geräte, die nicht konform sind
12. Klicken Sie auf **Weiter**.
13. Wählen Sie die Aktionen aus, die auf der Grundlage der Zustandsbewertung angewendet werden müssen, und klicken Sie dann auf **Weiter**.

    Auf der Übersichtsseite werden die Richtliniendetails angezeigt.
14. Sie können die Details überprüfen und auf **Fertig stellen**klicken.

    Weitere Informationen zum Erstellen von Zugriffsrichtlinien finden Sie unter Konfigurieren einer Zugriffsrichtlinie mit mehreren Regeln.

> **Hinweis:**
>
> Jede Secure Private Access-Anwendung, die in der Zugriffsrichtlinie nicht als konform oder nicht konform gekennzeichnet ist, wird als Standardanwendung behandelt und ist unabhängig vom Gerätestatus auf allen Endgeräten zugänglich.



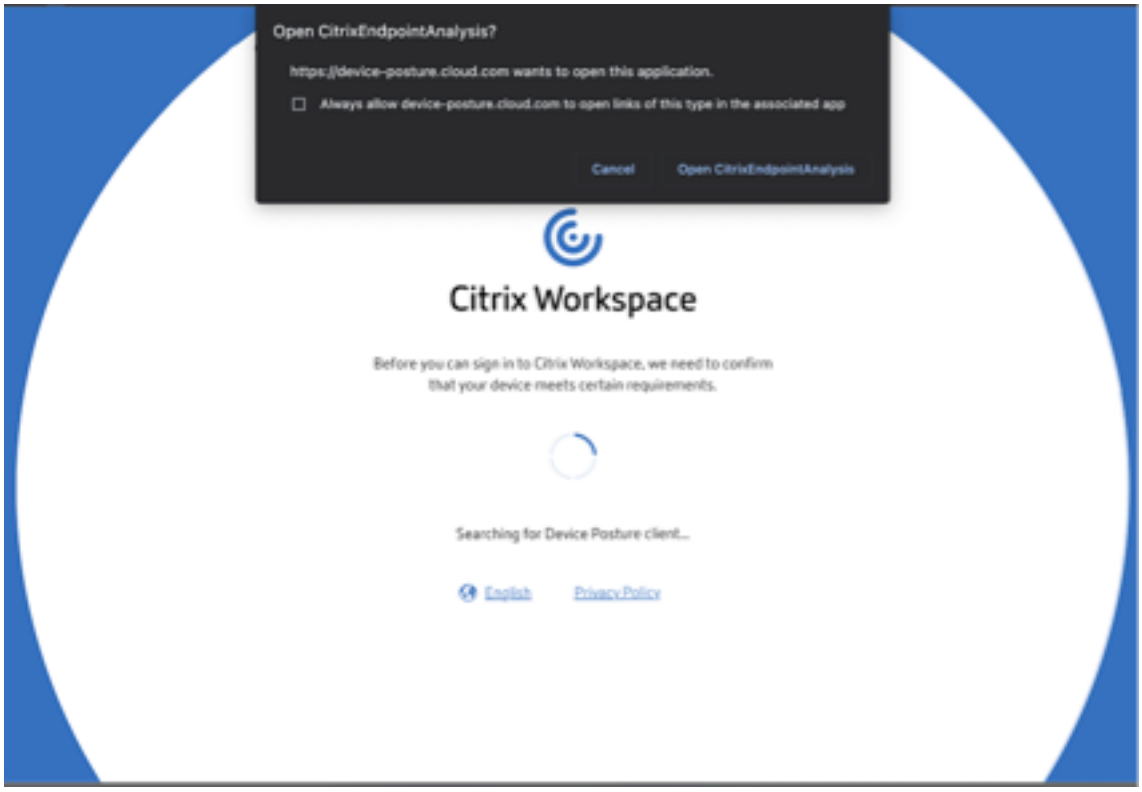
Ablauf für Endbenutzer

Sobald die Gerätestatusrichtlinien festgelegt und der Gerätestatus aktiviert ist, finden Sie im Folgenden die Endbenutzerabläufe, die darauf basieren, wie sich der Endbenutzer bei Citrix Workspace anmeldet.

Endbenutzerfluss per Browserzugriff

> **Hinweis:**
>
> Der macOS-Client und der Chrome-Browser werden als Beispiel zur Veranschaulichung verwendet. Die Bildschirme und Benachrichtigungen variieren je nach Client und Browser, den Sie für den Zugriff auf die Citrix Workspace-URL verwenden.

- Wenn sich ein Endbenutzer über einen Browser an der Citrix Workspace-URL `https://<your-workspace-URL` anmeldet, wird der Endbenutzer aufgefordert, die Citrix Endpoint Analysis-Anwendung auszuführen.



- Wenn der Endbenutzer auf **Citrix Endpoint Analysis öffnen** klickt, wird der Device Posture Client ausgeführt und scannt die Endpunktparameter auf der Grundlage der Anforderungen der Device Posture Policy.
- Wenn der neueste Device Posture Client nicht auf dem Endpunkt installiert ist, werden die Benutzer zu der Seite weitergeleitet, auf der die Optionen „ **Erneut prüfen** “und „ **Client herunterladen**“angezeigt werden. Der Benutzer muss auf **Client herunterladen** klicken.
- Wenn der neueste Device Posture Client bereits auf dem Endpunkt installiert ist, muss der Benutzer erneut auf **Erneut prüfen** klicken.

Endbenutzerfluss über die Citrix Workspace-Anwendung

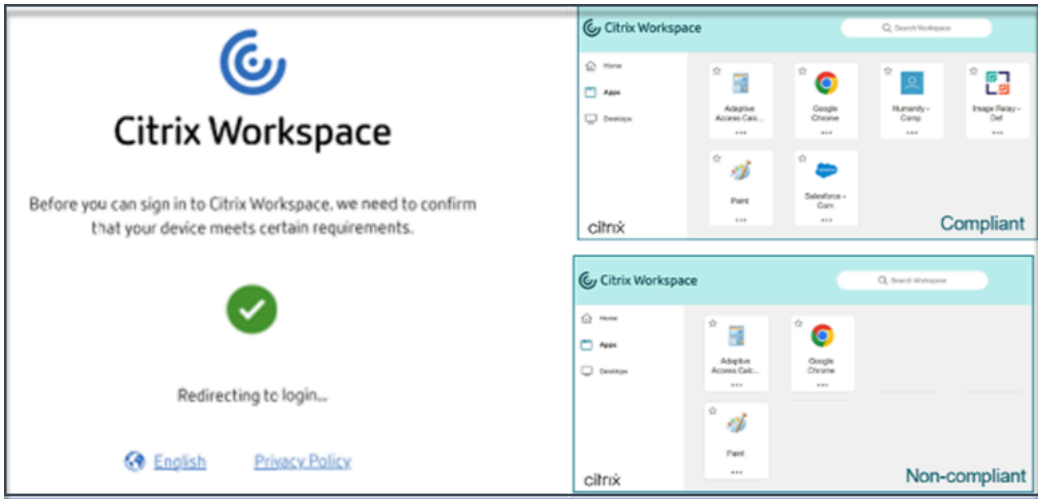
- Wenn sich ein Endbenutzer über die Citrix Workspace-Anwendung an der Citrix Workspace-URL `https://your-workspace-url` anmeldet, wird der auf dem Endpunkt installierte Device Posture Client ausgeführt und scannt die Endpunktparameter auf der Grundlage der Device Posture Policy-Anforderungen.
- Wenn der neueste Device Posture Client nicht auf dem Endpunkt installiert ist, werden die Benutzer zu der Seite weitergeleitet, auf der die Optionen „ **Erneut prüfen** “und „ **Client herunterladen**“angezeigt werden. Der Benutzer muss auf **Client herunterladen** klicken.
- Wenn der neueste Device Posture Client bereits auf dem Endpunkt installiert ist, muss der Benutzer erneut auf **Erneut prüfen** klicken.

Ablauf beim Endbenutzer —Gerätestatus - Ergebnisse

Basierend auf den Gerätestatusrichtlinien können drei Möglichkeiten auftreten.

Wenn ein Endpunkt die Policy-Bedingungen erfüllt, sodass das Gerät in folgende Kategorien unterteilt ist:

- **Konform** —Der Endbenutzer darf sich mit uneingeschränktem Zugriff auf Secure Private Access- oder Citrix DaaS-Ressourcen anmelden.
- **Nicht konform** —Der Endbenutzer darf sich mit eingeschränktem Zugriff auf Secure Private Access- oder Citrix DaaS-Ressourcen anmelden.



Wenn ein Endpunkt die Richtlinienbedingungen erfüllt, sodass das Gerät als **Zugriff verweigert**eingestuft wird, wird die Meldung **Zugriff verweigert** angezeigt.

Maßgeschneiderte Meldungen für Szenarien mit Zugriffsverweigerungen (Vorschau) Admins haben die Möglichkeit, die Meldung anzupassen, die auf dem Endgerät angezeigt wird, wenn ein Zugriff verweigert wird.

Diese Funktion befindet sich in der Vorschau. Melden Sie sich für die Vorschau an mit https://podio.com/webforms/29219975/2385710.

Gehen Sie wie folgt vor, um benutzerdefinierte Nachrichten hinzuzufügen:

1. **Navigieren Sie zur Seite Gerätestatus >** Gerätescans .
2. Klicken Sie auf **Einstellungen**.

3. Klicken Sie auf **Bearbeiten** und geben Sie im Feld **Meldung** die Meldung ein, die in Szenarien mit verweigertem Zugriff angezeigt werden muss. Sie können maximal 256 Zeichen eingeben.
4. Klicken Sie beim **Speichern auf Benutzerdefinierte Nachricht** aktivieren , um die Option zum Anzeigen der benutzerdefinierten Nachricht zu erzwingen. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die benutzerdefinierte Nachricht zwar erstellt, aber nicht auf den Geräten angezeigt, in denen der Zugriff verweigert wurde.

   Alternativ können Sie auf der Seite „ Einstellungen "den **Kippschalter**für benutzerdefinierte **Nachrichten** aktivieren, um die Nachricht auf den Geräten anzuzeigen.
5. Klicken Sie auf **Speichern**.

Die von Ihnen eingegebene Meldung erscheint immer dann, wenn dem Endgerät der Zugriff verweigert wird.

Device Posture Ereignisse überwachen und Fehler beheben

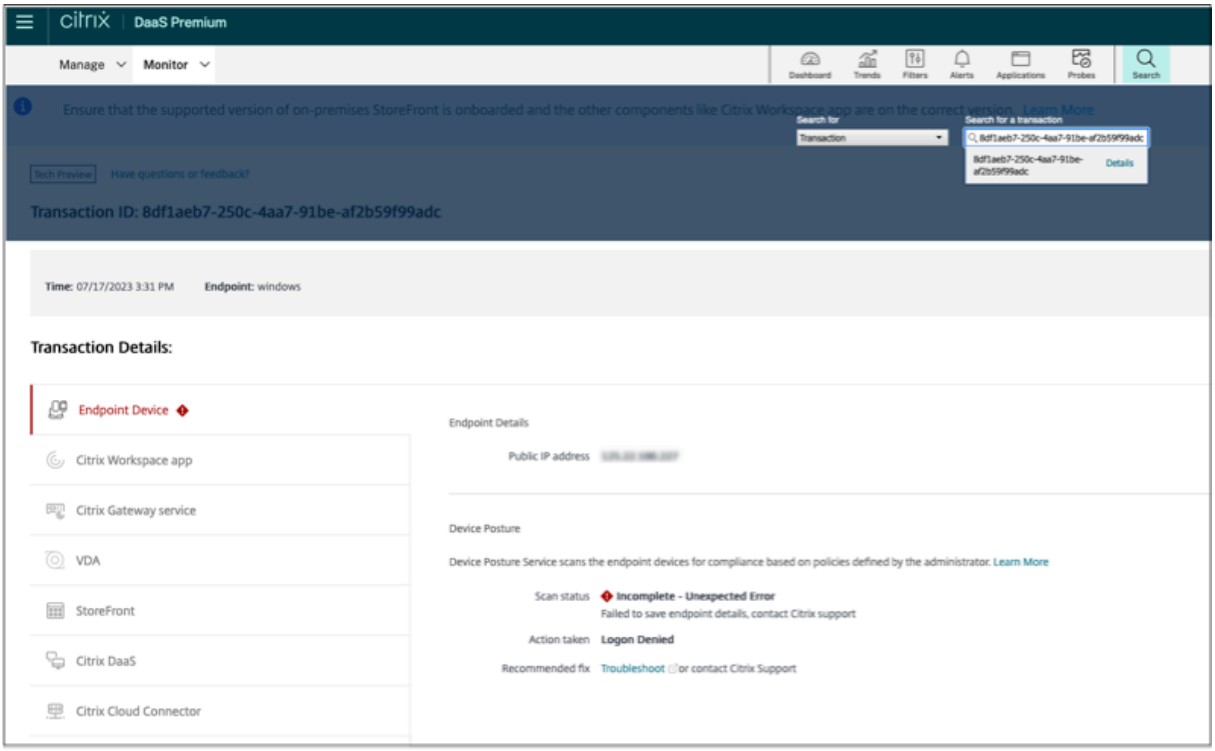
Die Ereignisprotokolle zur Gerätehaltung können an zwei Stellen eingesehen werden:

- 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.

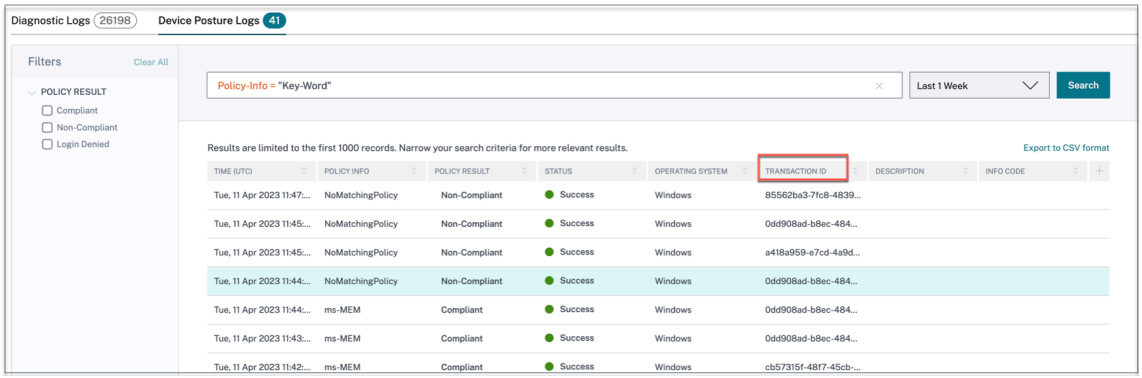
1. Kopieren Sie die Transaktions-ID der fehlgeschlagenen Sitzung oder der Sitzung mit verweigertem Zugriff vom Endbenutzergerät.
2. Melden Sie sich bei Citrix Cloud an.
3. Klicken Sie auf der DaaS-Kachel auf **Verwalten**und dann auf die Registerkarte **Überwachen** .
4. Suchen Sie in der Benutzeroberfläche "Überwachen"nach der 32-stelligen Transaktions-ID 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** .
3. Gehen Sie im Menü auf der linken Seite zum Abschnitt Dashboard.
4. 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

Bekannte Einschränkungen

- Benutzerdefinierte Workspace-URLs werden vom Device Posture Service nicht unterstützt.
- Es kann einige Minuten bis zu einer Stunde dauern, bis die Funktion zur Gerätehaltung aktiviert oder deaktiviert wird, nachdem die Taste zum Umschalten der Gerätehaltung ein- oder ausgeschaltet wurde.
- Änderungen an der Konfiguration des Gerätestatusservices werden nicht sofort wirksam. Es kann etwa 10 Minuten dauern, bis die Änderungen wirksam werden.
- Wenn Sie die Option Service Continuity in Citrix Workspace aktiviert haben und der Device Posture Service nicht verfügbar ist, können sich Benutzer möglicherweise nicht bei Workspace anmelden. Dies liegt daran, dass Citrix Workspace Apps und Desktops auf der Grundlage des lokalen Caches auf dem Benutzergerät auflistet.
- Wenn Sie in Citrix Workspace ein langlebiges Token und ein Kennwort konfiguriert haben, funktioniert der Gerätestatus-Scan für diese Konfiguration nicht. Die Geräte werden nur gescannt, wenn sich die Benutzer bei Citrix Workspace anmelden.
- Jede Plattform kann maximal 10 Richtlinien haben und jede Richtlinie kann maximal 10 Regeln haben.
- Rollenbasierter Zugriff wird vom Device Posture Service nicht unterstützt.

Qualität der Dienstleistung

- Leistung: Unter idealen Bedingungen verzögert der Device Posture Service die Anmeldung um weitere 2 Sekunden. Diese Verzögerung kann sich je nach zusätzlichen Konfigurationen wie Integrationen von Drittanbietern wie Microsoft Intune erhöhen.
- Resilienz: Der Device Posture Service ist äußerst widerstandsfähig und verfügt über mehrere POPs, um sicherzustellen, dass keine Ausfallzeiten auftreten.

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.

CrowdStrike-Integration mit Device Posture —Vorschau

February 16, 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.

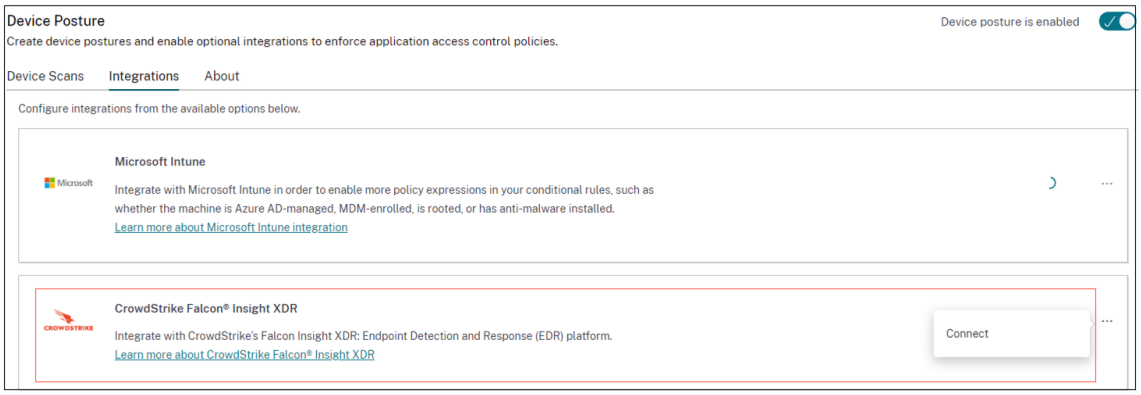
Schritt 1: Stellen Sie eine Vertrauensstellung zwischen dem Citrix Device Posture Service und dem CrowdStrike ZTA-Dienst her. Dies ist eine einmalige Aktivität.

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.

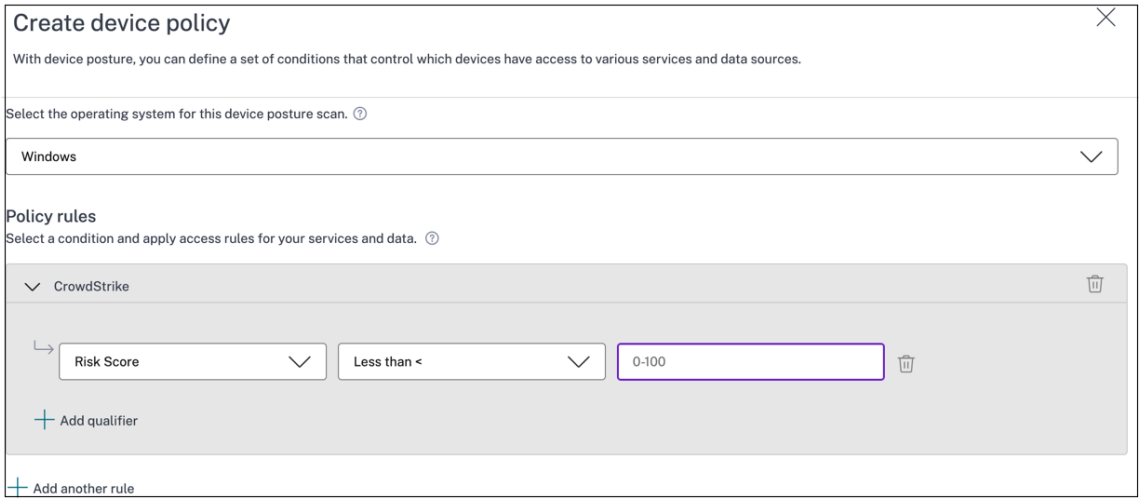
Die Integration gilt als erfolgreich, nachdem der Status von **Nicht konfiguriert** in **Konfiguriert** geändert wurde.

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**.

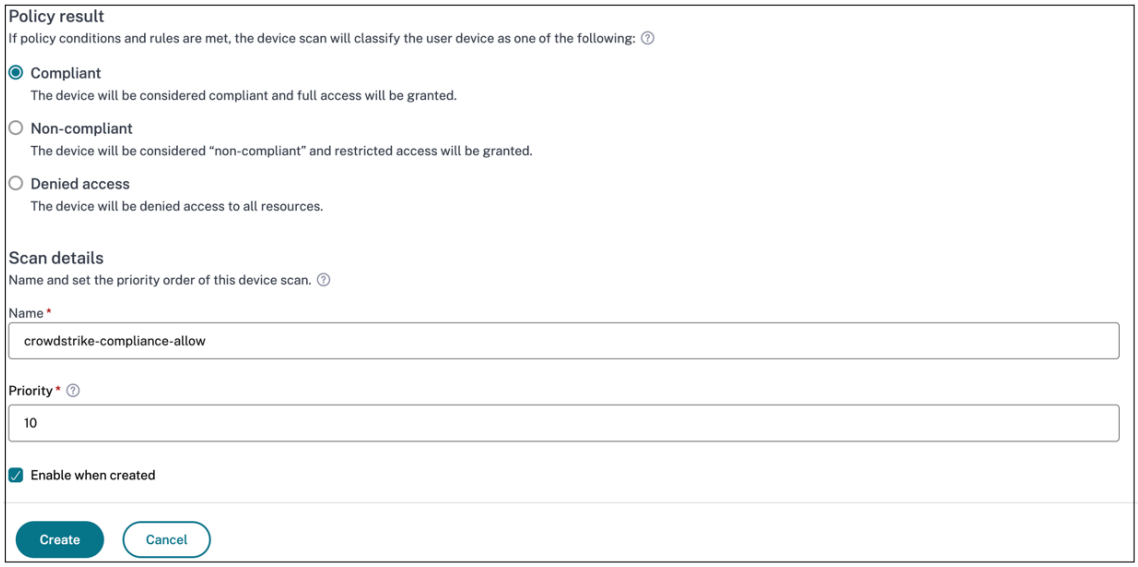


2. Wählen Sie die Plattform aus, für die diese Richtlinie erstellt wurde.
3. Wählen Sie unter **Policy Rule** die Option **CrowdStrike** aus.
4. Wählen Sie als Qualifizierer für die **Risc Score** die Bedingung aus, und geben Sie dann die Risikobewertung ein.
5. Klicken Sie auf **+**, um einen Qualifier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

Service zur Körperhaltung von Geräten

Integration von Microsoft Intune mit Device Posture

February 16, 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.

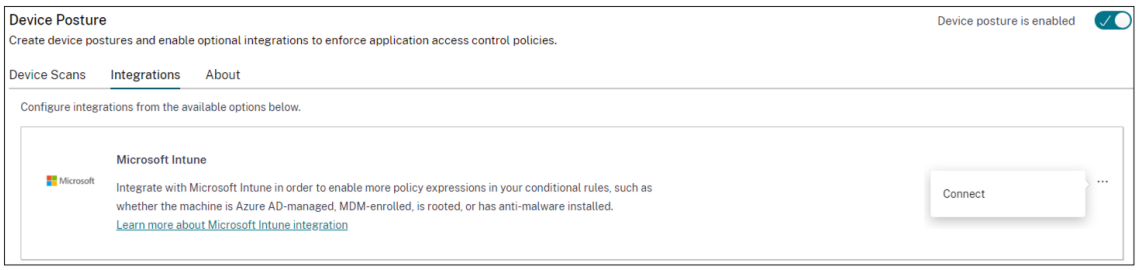
Schritt 1: Integrieren Sie die Geräteposition in den Microsoft Intune-Dienst. Dies ist eine einmalige Aktivität, die Sie ausführen, um eine Vertrauensstellung zwischen Device Posture und Microsoft Intune herzustellen.

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

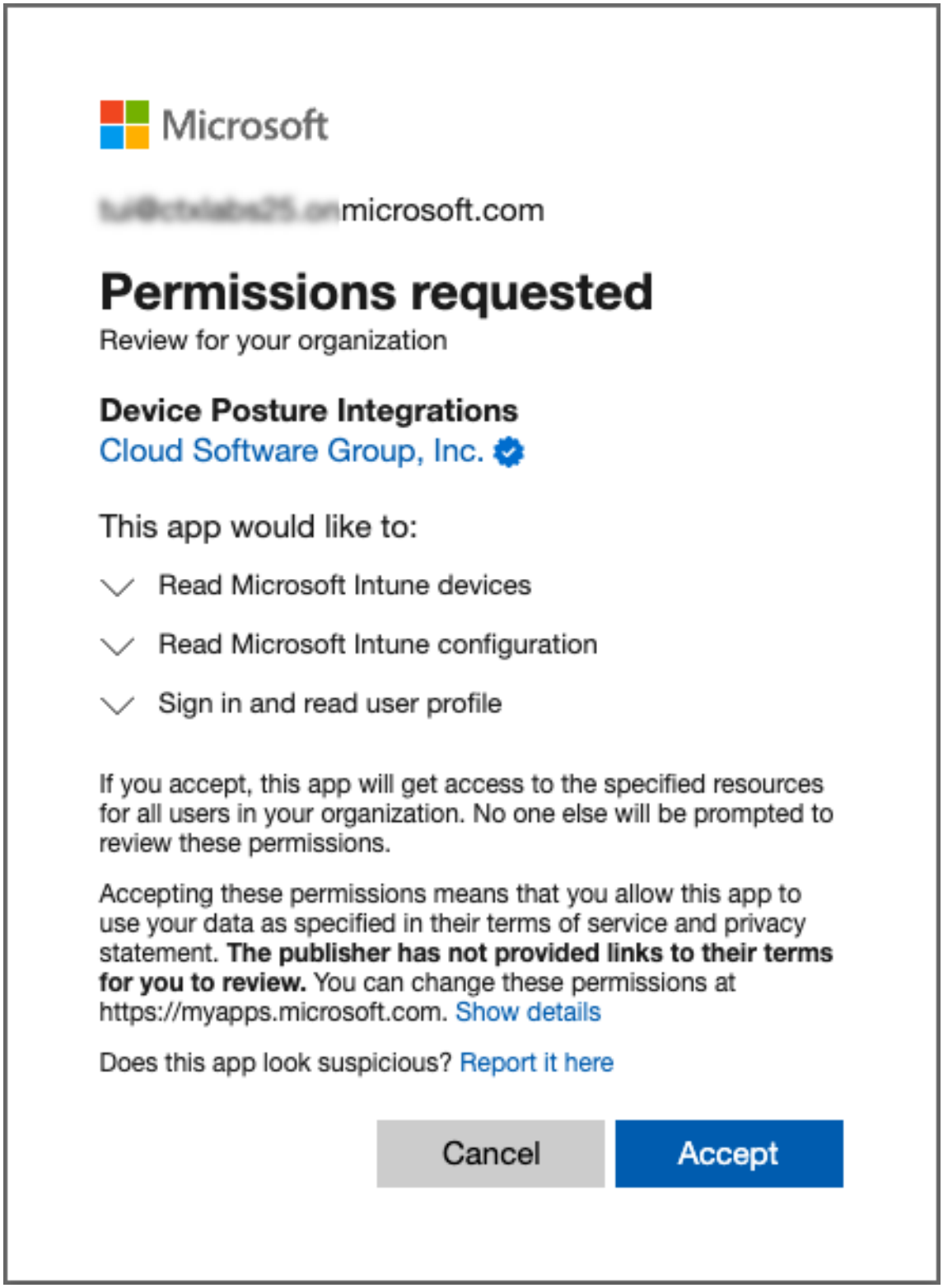
Schritt 1: Integrieren Sie die Geräteposition in Microsoft Intune

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.



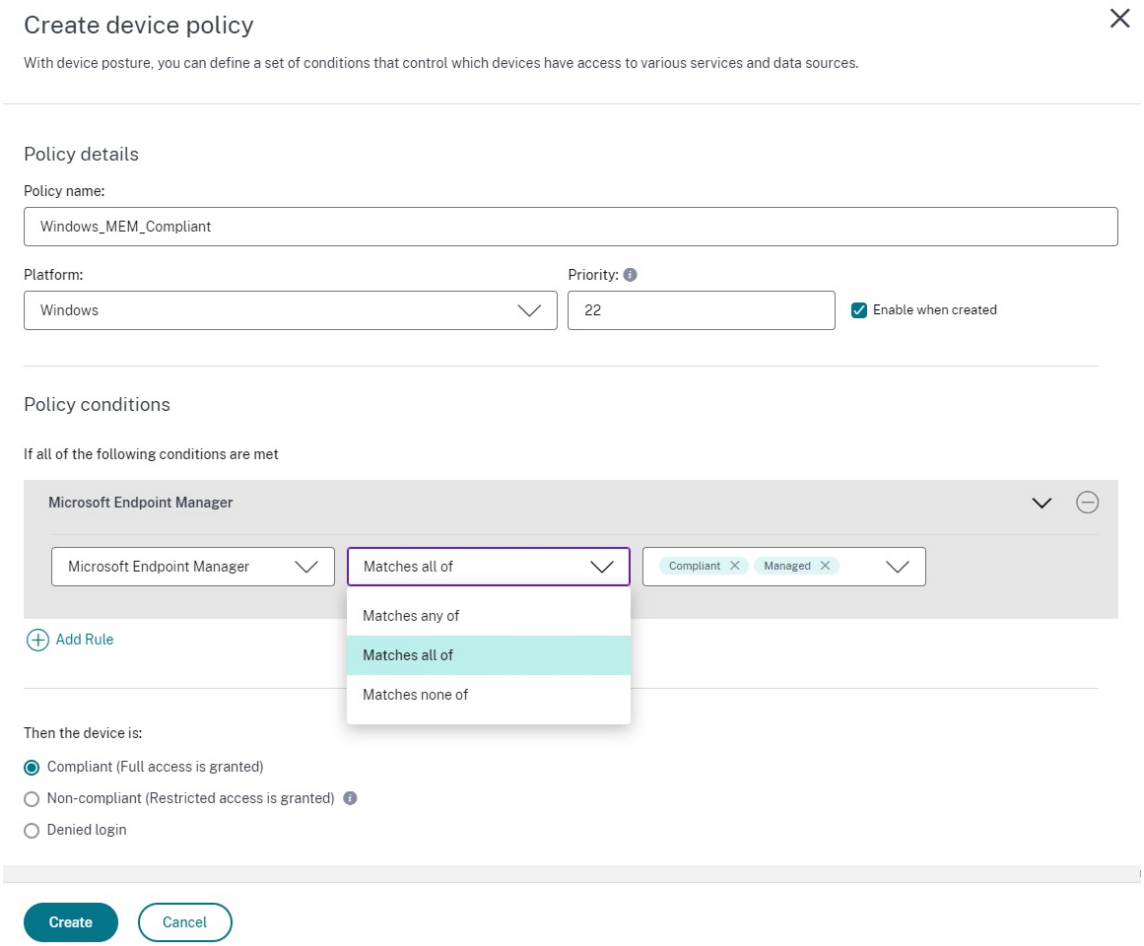
Nachdem sich der Integrationsstatus von **Nicht konfiguriert** in **Konfiguriert** geändert hat, können Administratoren eine Gerätestatusrichtlinie erstellen.

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 Gerätes-

> tatus 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 Gerätestatusrichtlinie.

Überprüfung des Gerätezertifikats mit dem Device Posture Service

February 16, 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.

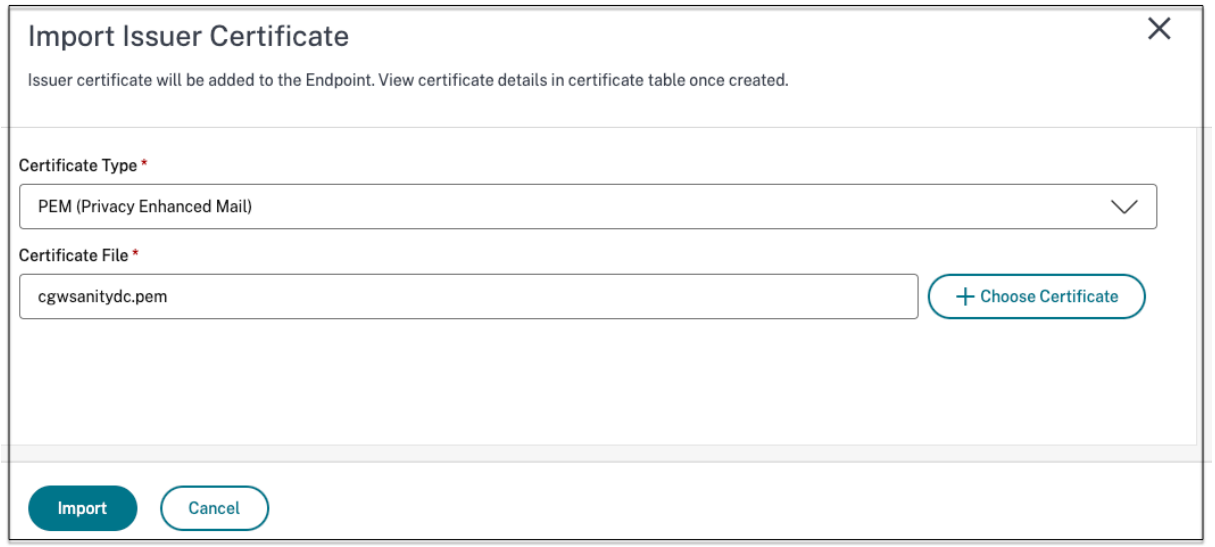
> **Zu beachtenswerte Punkte:**
>
> - Der Device Posture Service unterstützt nur den Zertifikatstyp PEM-Aussteller.
> - Für die Gerätezertifikatsprüfung unter Windows muss der EPA-Client auf dem Endgerät mit Administratorrechten installiert sein. Für andere Prüfungen benötigen Sie keine lokalen Administratorrechte. 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-----
>  ```



```
4  ******************************
5  -----END CERTIFICATE-----
6  -----BEGIN CERTIFICATE-----
7  ******************************
8  -----END CERTIFICATE
```

Gerätezertifikat hochladen

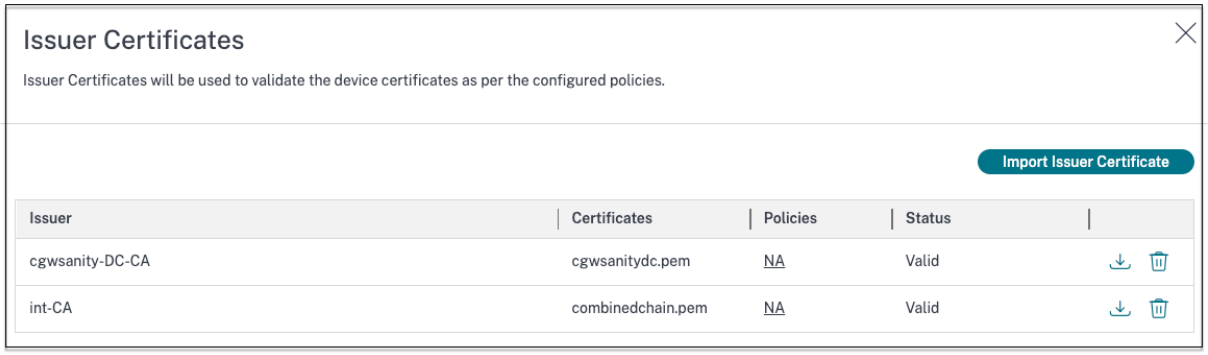
1. Klicken Sie auf der Device Posture-Startseite auf **Einstellungen** .
2. Klicken Sie auf **Verwalten**und dann auf **Zertifikat importieren**.
3. Wählen Sie **unter Zertifikatstyp**den Zertifikatstyp aus. Nur der PEM-Typ wird unterstützt.
4. Klicken Sie unter **Zertifikatsdatei**auf **Zertifikat auswählen**,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

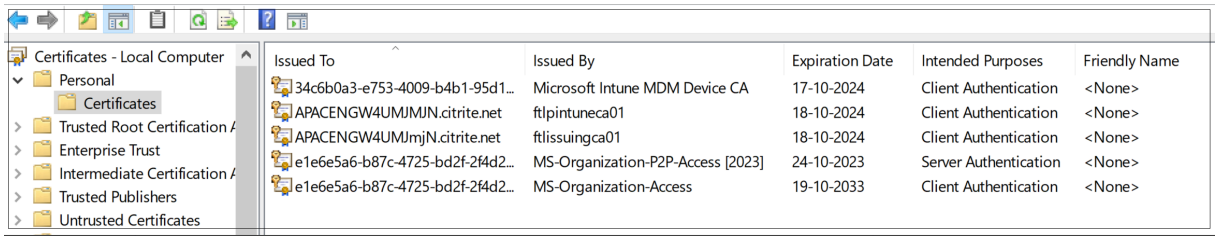
1. Klicken Sie auf der Device Posture-Startseite auf **Einstellungen** .
2. Klicken Sie unter **Issuer Certificates**auf **Manage**.
3. Auf der Seite Ausstellerzertifikate werden die importierten Ausstellerzertifikate aufgeführt.



Installieren Sie das Gerätezertifikat auf dem Endgerät

Windows:

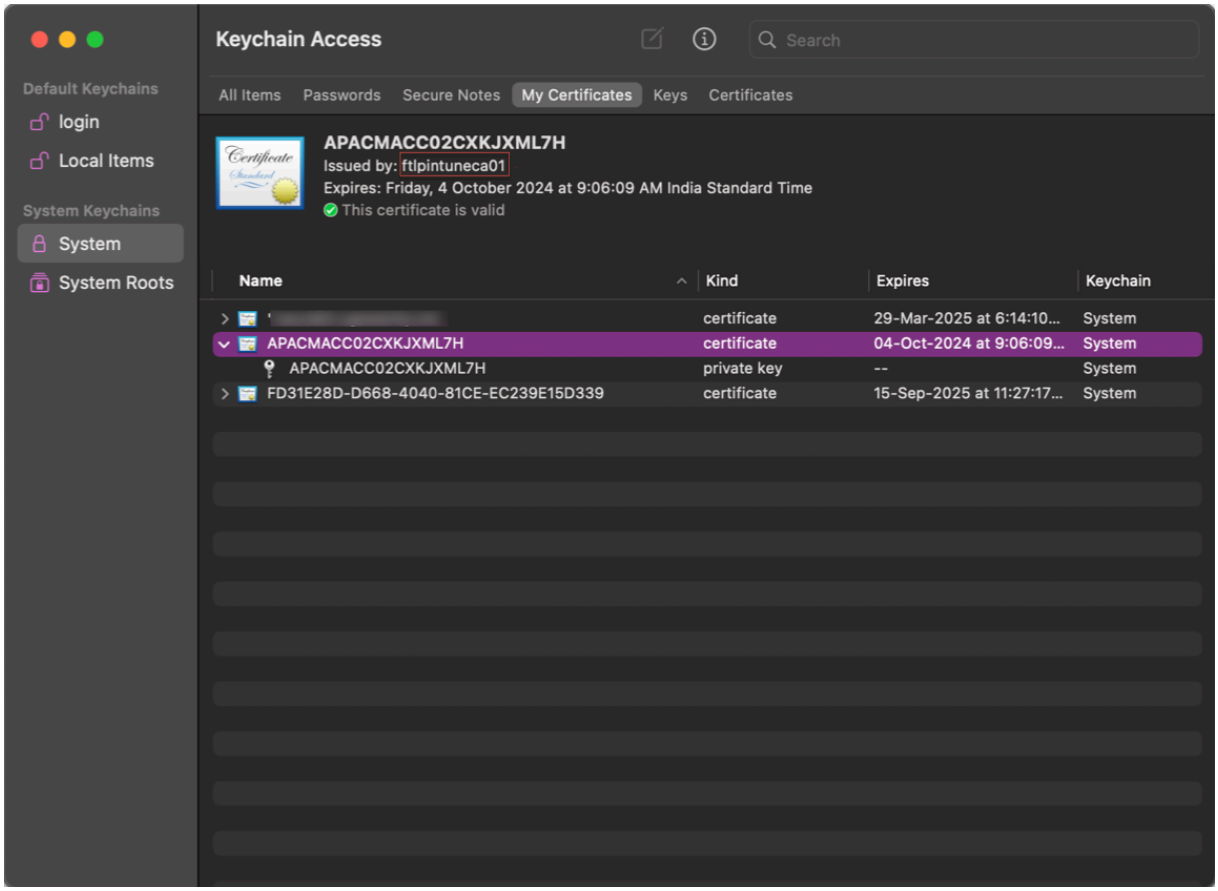
1. Öffnen Sie im **Startmenü** den **Computer Certificate Manager**.
2. Stellen Sie sicher, dass das Zertifikat in `Certificates - Local Computer\Personal\Certificates` installiert ist.
   - Zu den **beabsichtigten Zwecken** muss die **Kundenauthentifizierung** gehören.
   - Die Spalte **Ausgestellt 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

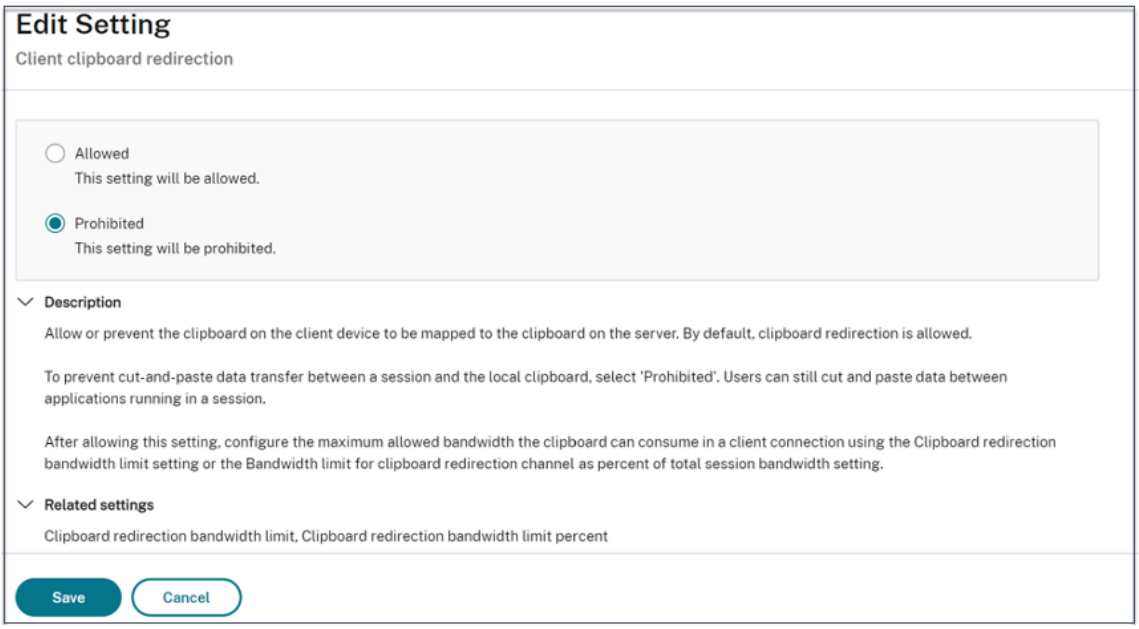
Sie können Smart Controls beim Zugriff auf die Citrix Desktop as a Service (DaaS) -Ressourcen über den Citrix Device Posture Service erzwingen.

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

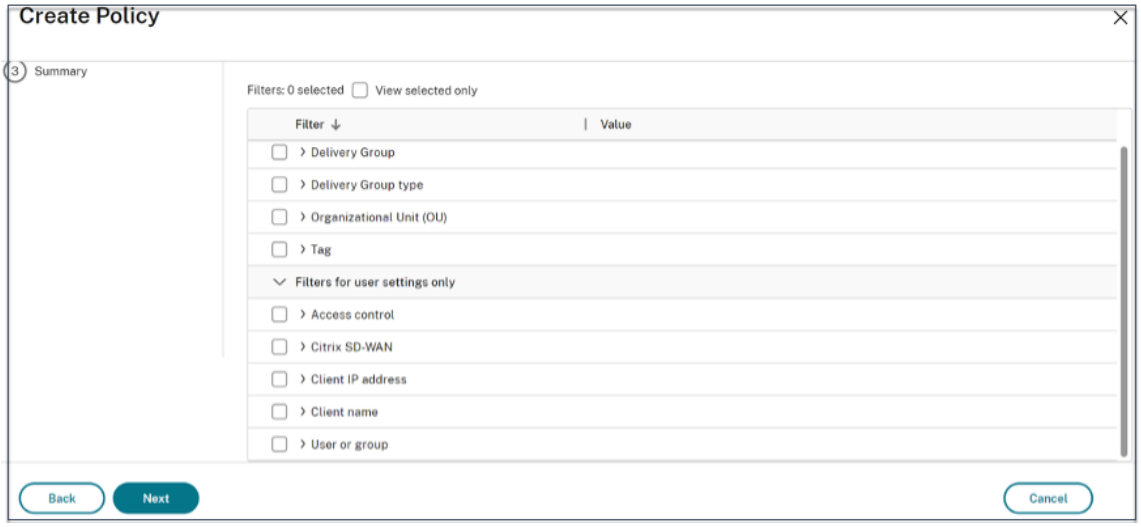
In diesem Beispiel wird eine Richtlinie erstellt, um die Funktion zum Kopieren und Einfügen auf Citrix DaaS-Ressourcen mithilfe der Device Posture Service-Tags (COMPLIANT und NON-COMPLIANT) zu deaktivieren.

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**.

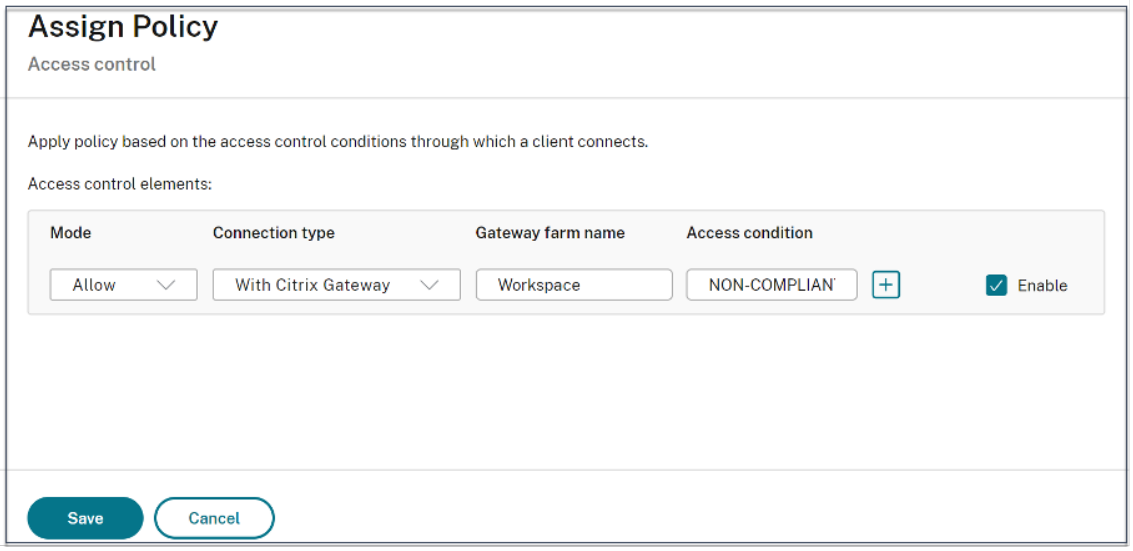


6. Klicken Sie auf der Seite **Benutzer und Maschinen** auf **Gefilterte Benutzer und Computer**, und weisen Sie diese Richtlinie dann der **Zugriffssteuerung**zu.
7. Gehen Sie zu **Nur für Benutzereinstellungen filtern** und wählen Sie **Zugriffskontrolle**aus.



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.

Gerätestatusprotokolle

February 16, 2024

Das Secure Private Access Service-Dashboard erfasst zusätzlich zu den Protokollen der SaaS/Web- und TCP/UDP-Apps die Gerätezustands-Protokolle.

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

February 16, 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 des 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 derzeit 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.

- **EPA-Client in die Citrix Workspace-App integriert (Vorschau):**Der EPA-Client ist auch in die Citrix Workspace-App integriert. Durch diese Integration müssen die Endbenutzer den EPA-Client nach der Installation der Citrix Workspace-App nicht mehr installieren.
  - Wenn auf einem Endgerät bereits ein EPA-Client installiert ist und der Endbenutzer die Citrix Workspace-App installiert, ist der integrierte EPA-Client nicht auf diesem Gerät installiert. Der bestehende EPA-Client wird für die Überprüfung der Gerätehaltung verwendet.
  - Ebenso wird der integrierte EPA-Client standardmäßig vom Gerät entfernt, wenn der Endbenutzer die Citrix Workspace-App deinstalliert. 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.

> **Hinweis:**
>
> - Die EPA-Clientintegration mit der Citrix Workspace-App wird nur auf der Windows-Plattform unterstützt und befindet sich in der Vorschauversion. Melden Sie sich für die Vorschau an mit https://podio.com/webforms/29219973/2385708.

- **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 Wie verwende ich 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.