Device Posture

Machine translated content

Disclaimer

Contents

Device Posture

February 20, 2024

Citrix Device Posture サービスは、管理者が Citrix DaaS（仮想アプリおよびデスクトップ）または Citrix Secure Private Access リソース（SaaS、Web アプリ、TCP、および UDP アプリ）にアクセスするためにエンドデバイスが満たす必要のある特定の要件を管理者が適用できるようにするクラウドベースのソリューションです。ゼロトラストベースのアクセスを実装するには、デバイスの状態を確認してデバイスの信頼を確立することが重要です。Device Posture サービスは、エンドユーザのログインを許可する前に、エンドデバイスのコンプライアンス（マネージド/BYOD とセキュリティ態勢）をチェックすることで、ネットワークにゼロトラストの原則を適用します。

前提条件

- ライセンス要件：Citrix Device Posture サービスの利用資格は、Citrix DaaS プレミアム、Citrix DaaS Premium Plus、および Citrix Secure Private Access Advanced ライセンスの一部です。他のライセンスをお持ちのお客様は、Device Posture サービスの利用権をアドオンとして購入できます。アドオンの場合、お客様はスタンドアロンのアダプティブ認証 SKU を購入する必要がありますが、Device Posture サービスを使用するために必ずしも導入する必要はありません。
- サポートされるプラットフォームは、以下のとおりです。
  - Windows（10 および 11）
  - macOS 13 Ventura
  - macOS 12 Monterey
  - iOS
  - IGEL

> 注：
>
> - サポートされていないプラットフォームで実行されているデバイスは、デフォルトで非対応としてマークされます。**Device Posture** ページの **[** 設定]** タブで、分類を [非対応] から [拒否 **] に変更できます。
> - サポートされているプラットフォームで実行されているが、事前に定義されている Device Posture ポリシーに一致しないデバイスは、デフォルトで非準拠としてマークされます。**Device Posture** ページの **[** 設定]** タブで、分類を [非対応] から [拒否 **] に変更できます。
> - Device Posture サービスでの iOS サポートについては、EPA クライアントが iOS 向け Citrix Workspace アプリの一部として組み込まれています。バージョンについて詳しくは、「iOS 向け Citrix Workspace アプリ」を参照してください。
> - Device Posture サービスでの IGEL OS サポートでは、EPA クライアントが IGEL OS の一部として組み込まれています。IGEL デバイスに EPA クライアントをインストールするには、IGEL サ

> ポートチームにお問い合わせください。

- Citrix Device Posture クライアント（EPA クライアント）: Device Posture スキャンを実行するにはエンドポイントデバイスにインストールする必要がある軽量アプリケーション。このアプリケーションをエンドポイントにダウンロードしてインストールするには、ローカル管理者権限は必要ありません。

  > **注:**
  >
  > デバイス証明書チェックを使用している場合は、管理者権限で EPA クライアントをインストールする必要があります。

- 対応ブラウザ: Chrome、Edge、Firefox。
- ファイアウォール設定: Device Posture サービスがエンドデバイス上の EPA クライアントを更新できるようにするには、ファイアウォール/プロキシを次のドメインを許可するように設定する必要があります。
  - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
  - `https://productioniconstorage.blob.core.windows.net`
  - *.netscalergateway.net
  - *.nssvc.net
  - *.cloud.com
  - *.pendo.io
  - *.citrixworkspacesapi.net

プレビュー機能

- IGEL による Device Posture サービス。https://podio.com/webforms/29062020/2362942を使用してプレビューにサインアップしてください。
- iOS での Device Posture サービス。https://podio.com/webforms/28888524/2338366を使用してプレビューにサインアップしてください。
- 位置情報チェックとネットワークロケーションチェック。https://podio.com/webforms/29051759/2362665を使用してプレビューにサインアップしてください。
- CrowdStrike と Device Posture サービスの統合。詳細については、「CrowdStrike と Device Posture の統合-プレビュー」を参照してください。

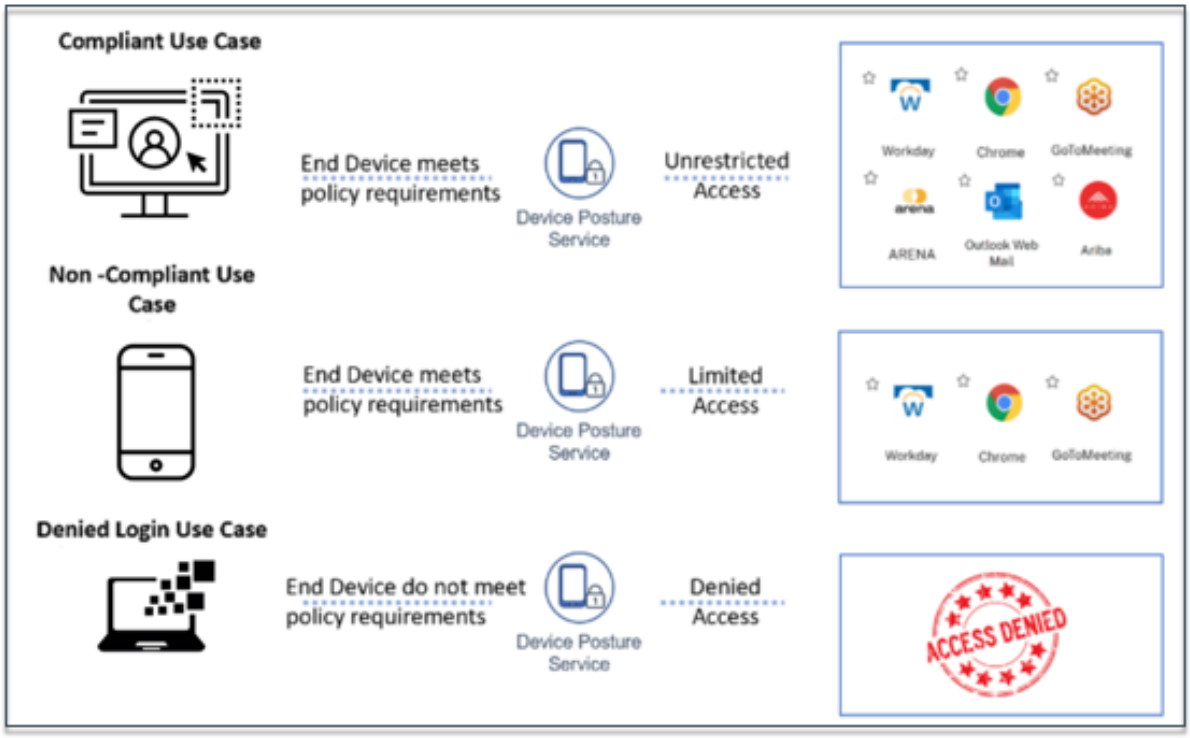
機能

管理者は Device Posture ポリシーを作成して、エンドポイントデバイスのポスチャをチェックし、エンドポイントデバイスのログインを許可するか拒否するかを判断できます。ログインが許可されているデバイスは、さらに準拠または非準拠に分類されます。ユーザーはブラウザまたは Citrix Workspace アプリからログインできます。

デバイスを「準拠」、「非準拠」、「ログイン拒否」に分類する際に使用される大まかな条件は次のとおりです。

- 準拠デバイス - 事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへのフルアクセスまたは無制限アクセスで会社のネットワークにログインできるデバイス。-
- 非準拠デバイス -事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへの部分的または制限されたアクセスで会社のネットワークにログインできるデバイス。
- ログイン拒否**:** - ポリシー要件を満たさないデバイスはログインを拒否されます。

デバイスを準拠、**** 非準拠、**** およびログイン拒否として分類すると、Citrix DaaS および Citrix Secure Private Access サービスに渡され、サービスはそのデバイス分類を使用してスマートアクセス機能を提供します。



> 注:
>
> - Device Posture ポリシーは、プラットフォームごとに個別に設定する必要があります。たとえば、macOS の場合、管理者は特定の OS バージョンを搭載したデバイスへのアクセスを許可できます。同様に、Windows の場合、管理者は特定の認証ファイルやレジストリ設定などを含むようにポリシーを設定できます。
> - Device Posture スキャンは、事前認証中またはログイン前にのみ実行されます。
> - 「準拠」と「非準拠」の定義については、定義を参照してください。

デバイスポスチャによるスキャンのサポート

Citrix Device Posture サービスでは、次のスキャンがサポートされています。

Windows	macOS	iOS	IGEL
Citrix Workspace アプリのバージョン	Citrix Workspace アプリのバージョン	Citrix Workspace アプリのバージョン	-
オペレーティングシステムのバージョン	オペレーティングシステムのバージョン	オペレーティングシステムのバージョン	-
ファイル (存在、ファイル名、パス)	ファイル (存在、ファイル名、パス)	-	ファイル (存在、ファイル名、パス)
ジオロケーション	ジオロケーション	-	-
ネットワークロケーション	ネットワークロケーション	-	-
MAC アドレス	MAC アドレス	-	-
プロセス (存在する)	プロセス (存在する)	-	-
Microsoft Endpoint Manager	Microsoft Endpoint Manager	-	-
クラウドストライク	クラウドストライク	-	-
デバイス証明書	デバイス証明書	-	-
ブラウザー	ブラウザー	-	-
アンチウイルス	アンチウイルス	-	-
非数値レジストリ (32 ビット)	-	-	-
非数値レジストリ (64 ビット)	-	-	-
数値レジストリ (32 ビット)	-	-	-
数値レジストリ (64 ビット)	-	-	-
Windows 更新プログラムのインストールタイプ	-	-	-
Windows Update のインストール最終更新プログラムの確認	-	-	-

> 注:
>
> - Device Posture サービスでの iOS サポートについては、EPA クライアントが iOS 向け Citrix Workspace アプリの一部として組み込まれています。バージョンについて詳しくは、「iOS 向け Citrix Workspace アプリ」を参照してください。

デバイスポスチャとのサードパーティ統合

Device Posture サービスが提供するネイティブスキャンに加えて、このサービスは Windows および macOS 上の以下のサードパーティソリューションと統合することもできます。

- Microsoft Intune。詳しくは、「Microsoft Intune と Device Posture の統合」を参照してください。
- クラウドストライク。詳細については、「CrowdStrike と Device Posture の統合-プレビュー」を参照してください。

デバイスの姿勢を設定

Device Posture は、デバイスがリソースにアクセスするために満たさなければならないポリシーとルールを組み合わせたものです。各ポリシーには、[準拠]、[非準拠]、[ログイン拒否] のいずれかのアクションが添付されています。さらに、各ポリシーには優先順位が関連付けられており、ポリシーが true と評価され、関連するアクションが実行されると、ポリシー評価は停止します。

1. Citrix Cloud にサインインし、ハンバーガーメニューから［**ID** とアクセス管理］を選択します。
2. [**Device Posture]** タブをクリックし、 [管理] をクリックします。

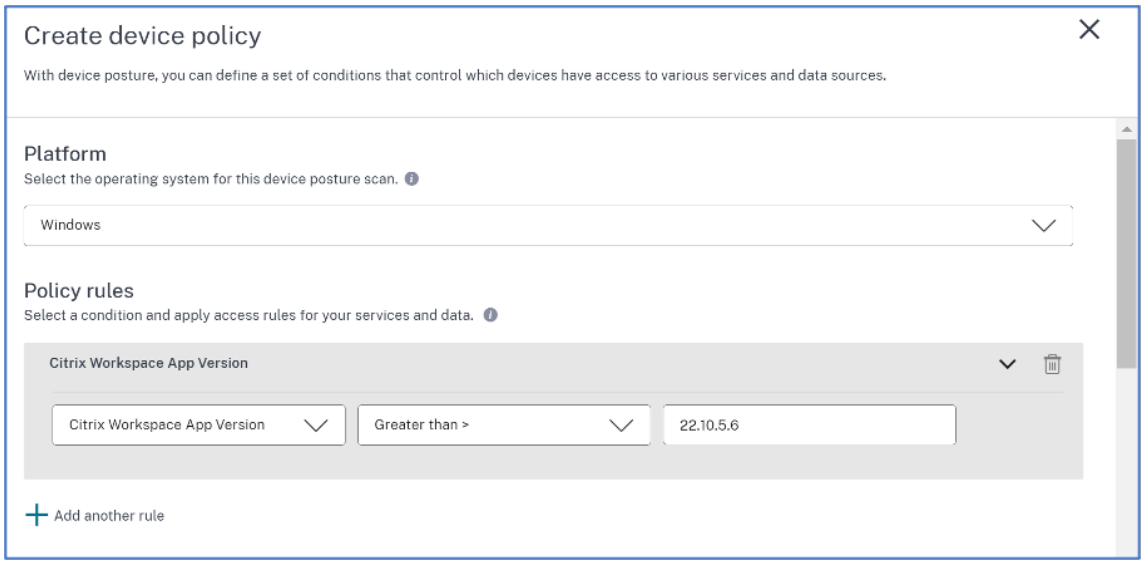
   > 注:
   >
   > - Secure Private Access サービスのお客様は、管理ユーザー・インターフェースの左側のナビゲーションにある「**Device Posture** 」を直接クリックできます。
   > - 初めて使用するユーザーには、Device Posture のランディングページに、Device Posture ポリシーを作成するように求められます。Device Posture ポリシーは、プラットフォームごとに個別に設定する必要があります。Device Posture ポリシーを作成すると、適切なプラットフォームに一覧表示されます。
   > - ポリシーは、Device Posture が有効になった後にのみ有効になります。デバイスポスチャを有効にするには、右上隅にある［デバイスポスチャを無効］にスライドさせて［オン］に切り替えます。

3. [デバイスポリシーの作成] をクリックします。
4. 「プラットフォーム」で、ポリシーを適用するプラットフォームを選択します。Device Posture のホームページで選択したタブに関係なく、プラットフォームを Windows から macOS に、またはその逆に変更できます。
5. ポリシールールで、Device Posture の一部として実行するチェックを選択し、一致させる必要がある条件を選択します。

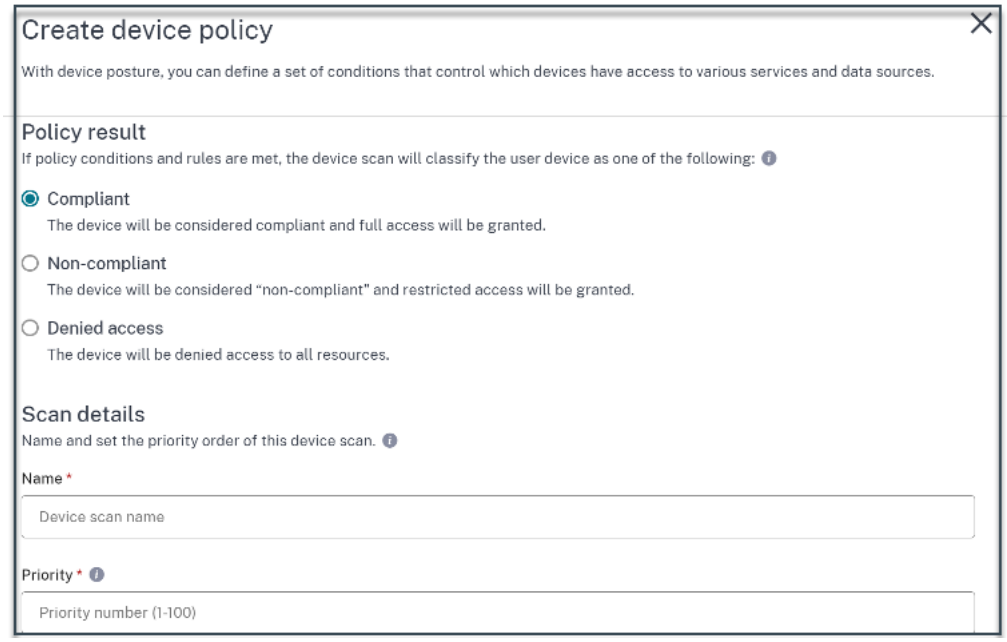
   > 注:
   >
   > - デバイス証明書をチェックするには、発行者証明書がデバイスに存在することを確認してください。それ以外の場合は、Device Posture ポリシーの作成時にデバイス証明書をインポートするか、Device Posture ホームページの **[設定]** から証明書をアップロードできます。詳しくは、「デバイ

> ス証明書のポリシー作成時のデバイス証明書のインポート」と「デバイス証明書のアップロード」を参照してください。
> - デバイス証明書をチェックするには、エンドデバイスに EPA クライアントが管理者権限でインストールされている必要があります。
> - Device Posture サービスによるデバイス証明書チェックは、証明書失効チェックをサポートしていません。

6. 複数のルールを作成するには、[別のルールを追加] をクリックします。AND 条件は複数のルールに適用されます。



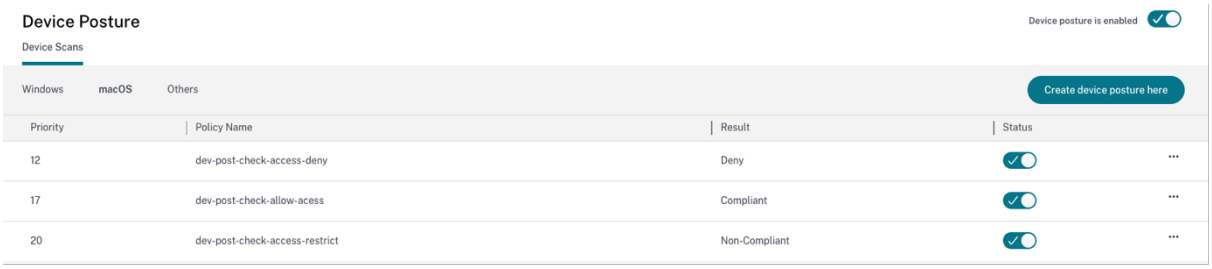
7. 設定した条件に基づくポリシー結果で、デバイススキャンでユーザーデバイスを分類するタイプを選択します。
   - 準拠
   - 非準拠
   - アクセス拒否
8. ポリシーの名前を入力します。
9. [優先度] に、ポリシーを評価する順序を入力します。
   - 1 から 100 までの値を入力できます。拒否ポリシーを優先度が高く、その後に非準拠、最後に準拠するように構成することをお勧めします。
   - 値が小さい優先度が最も高くなります。
   - 有効になっているポリシーのみが優先度に基づいて評価されます。
10. ［作成］をクリックします。



> 重要：
>
> **Device Posture** ポリシーを有効にするには、「作成時に有効にする」トグルスイッチを「オン」に切り替える必要があります。ポリシーを有効にする前に、ポリシーが正しく構成され、テスト設定でこれらのタスクを実行していることを確認することをお勧めします。

Device Posture ポリシーを編集する

設定された Device Posture ポリシーは、Device **Scans** ページの特定のプラットフォームの下に一覧表示されます。このページから、編集するポリシーを検索できます。このページからポリシーを有効化、無効化、または削除することもできます。



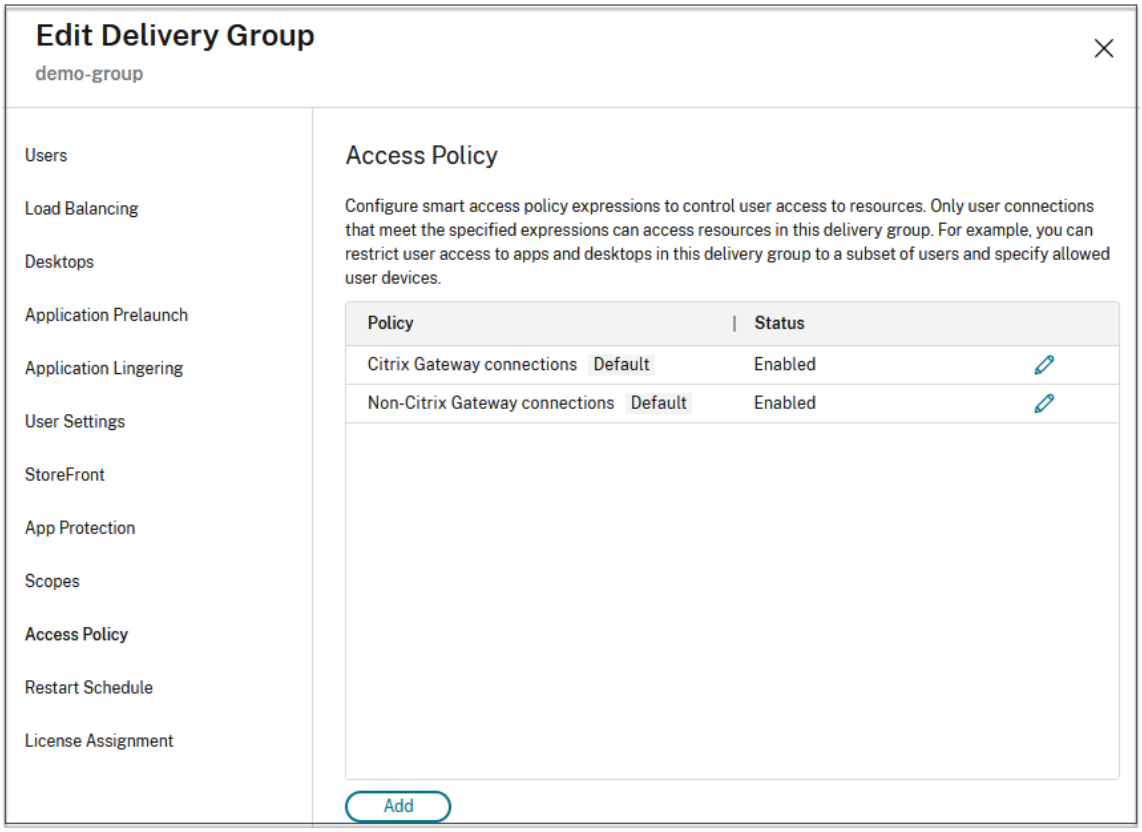
Device Posture を使用してコンテキストアクセス (スマートアクセス) を設定

デバイスのポスチャの検証後、デバイスのログインが許可され、準拠または非準拠として分類できます。この情報は、Citrix DaaS サービスおよび Citrix Secure Private Access サービスにタグとして提供され、デバイスの状態に基づいてコンテキストアクセスを提供するために使用されます。そのため、Citrix DaaS と Citrix Secure Private Access は、Device Posture タグを使用してアクセス制御を実施するように構成する必要があります。

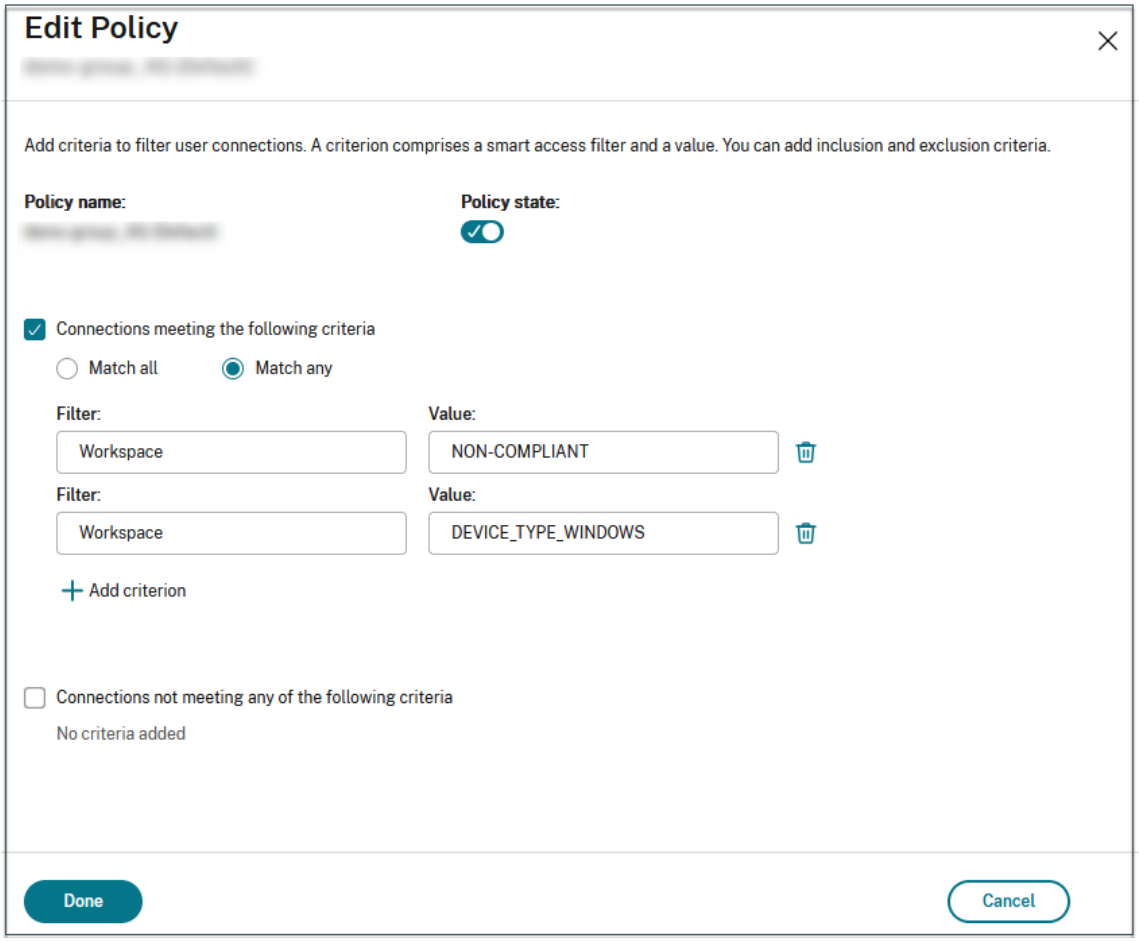
新しい **Studio UI** を使用した **Device Posture** による **Citrix DaaS** 構成 **(**プレビュー**)**

プレビューにサインアップしてください。

1. Citrix Cloud にサインインします。
2. **DaaS** タイルで [管理] をクリックします。
3. 左側のメニューから「デリバリーグループ」セクションに移動します。
4. デバイスの状態に基づいてアクセス制御を構成するデリバリーグループを選択し、[編集] をクリックします。
5. 「デリバリーグループの編集」ページで、「アクセスポリシー」をクリックします。
6. **Citrix Gateway** 接続行の編集アイコンをクリックして、ゲートウェイ接続ポリシーを編集します。



a) [ポリシーの編集] ページで、次の条件を満たす接続を選択します。
b) [任意に一致] を選択し、[条件を追加] をクリックします。
c) 「ネットワークロケーションの設定」で設定したすべてのロケーションタグに条件を追加します。「フィルター」には「ワークスペース」、「値」には「準拠」または「非準拠」と入力します。



> 注:
>
> デバイス分類タグの構文は、先ほど説明したのと同じ方法で入力する必要があります。つまり、すべて大文字 (COMPLIANT と NON COMPLIANT) です。そうしないと、デバイスのセキュリティ態勢ポリシーが意図したとおりに機能しません。
>
> デバイス分類タグに加えて、Device Posture サービスはデバイスに関連するオペレーティングシステムタグとアクセスポリシータグも返します。オペレーティングシステムタグとアクセスポリシータグは大文字のみで入力する必要があります。
>
> - DEVICE_TYPE_WINDOWS
> - DEVICE_TYPE_MAC
> - 正確なポリシー名 (大文字)

Device Posture による **Citrix Secure Private Access** 構成

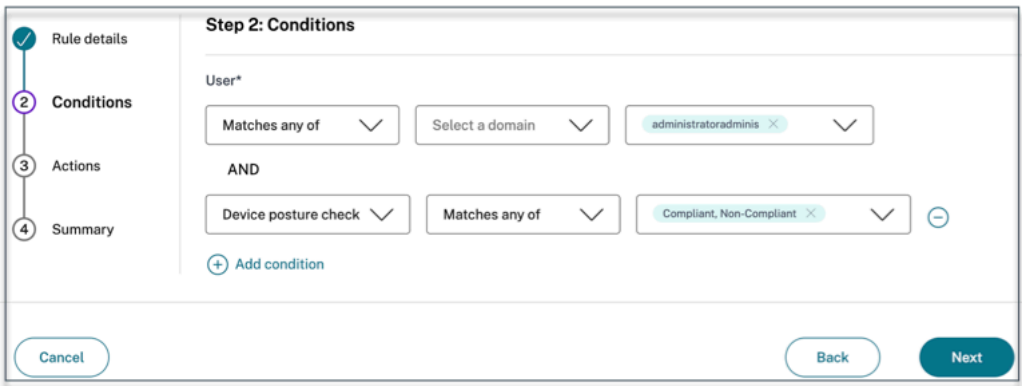
1. Citrix Cloud にサインインします。
2. 「Secure Private Access」タイルで、「管理」をクリックします。

3. 左側のナビゲーションで [アクセスポリシー] をクリックし、[ポリシーの作成] をクリックします。
4. ポリシー名とポリシーの説明を入力します。
5. 「アプリケーション」で、このポリシーを適用する必要があるアプリまたはアプリのセットを選択します。
6. 「**Create Rule** 」をクリックして、ポリシーのルールを作成します。
7. ルール名とルールの簡単な説明を入力して、[次へ] をクリックします。
8. ユーザーの条件を選択します。ユーザー条件は、ユーザーにアプリケーションへのアクセスを許可するための必須条件です。
9. **+** をクリックして、デバイスポスチャ条件を追加します。
10. ドロップダウンメニューから [デバイスポスチャチェック] と [論理式] を選択します。
11. カスタムタグに次のいずれかの値を入力します:
    - 準拠-準拠デバイス用
    - 非準拠-非準拠デバイス用
12. ［次へ］をクリックします。
13. 条件評価に基づいて適用する必要があるアクションを選択し、「次へ」をクリックします。

    「概要」ページには、ポリシーの詳細が表示されます。
14. 詳細を確認して [完了] をクリックします。

    アクセスポリシーの作成の詳細については、「複数のルールを含むアクセスポリシーの設定」を参照してください。

> 注:
>
> アクセスポリシーで準拠または非準拠のタグが付いていない Secure Private Access アプリケーションはデフォルトアプリケーションとして扱われ、デバイスの状態に関係なくすべてのエンドポイントからアクセスできます。



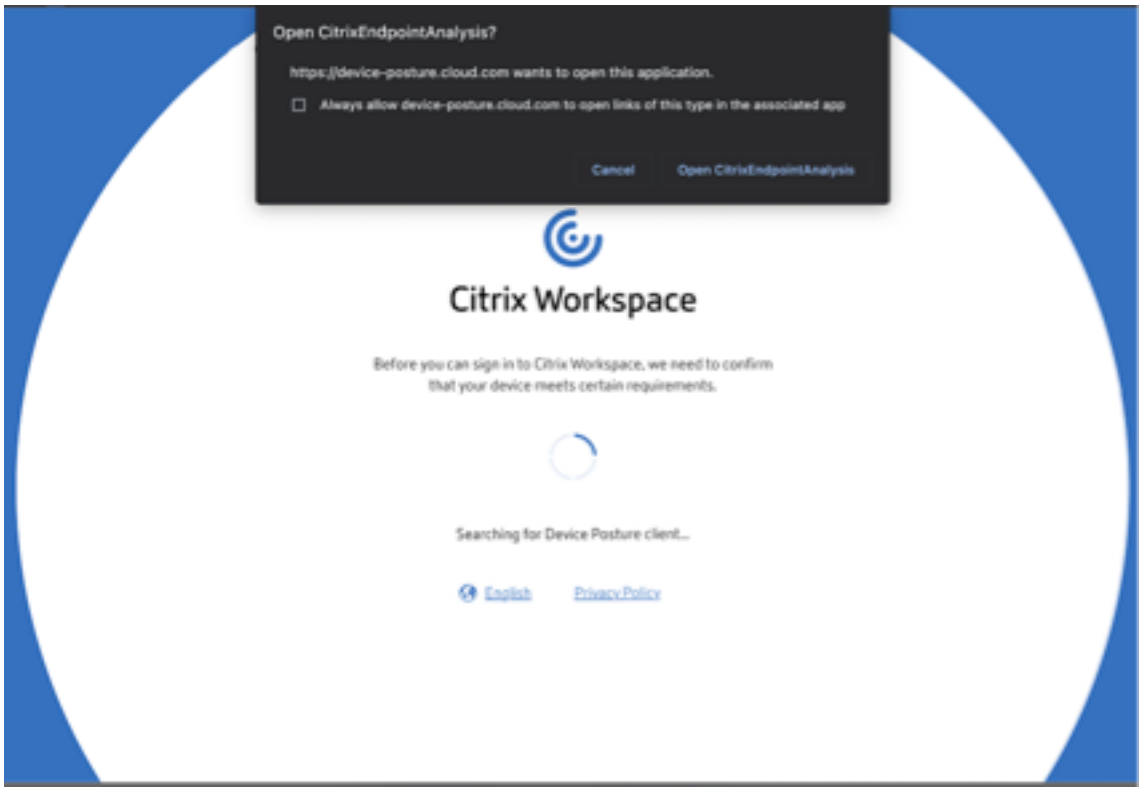
エンドユーザーフロー

Device Posture ポリシーを設定して Device Posture を有効にすると、エンドユーザーの Citrix Workspace へのログイン方法に基づくエンドユーザーフローが次のようになります。

ブラウザアクセスによるエンドユーザーフロー

> 注:
>
> macOS クライアントと Chrome ブラウザを例として使用しています。画面と通知は、Citrix Workspace URL へのアクセスに使用するクライアントとブラウザによって異なります。

- エンドユーザーがブラウザを介して Citrix Workspace URL`https://<your-workspace-URL`にログオンすると、エンドユーザーは Citrix EndpointAnalysis アプリケーションを実行するように求められます。



- エンドユーザーが「**Open Citrix End Point Analysis**」をクリックすると、Device Posture クライアントが実行され、Device Posture ポリシー要件に基づいてエンドポイントパラメータがスキャンされます。
- 最新の Device Posture クライアントがエンドポイントにインストールされていない場合、ユーザーは [再確認]、[クライアントのダウンロード] のオプションを表示するページにリダイレクトされます。ユーザーは [クライアントをダウンロード] をクリックする必要があります。
- 最新の Device Posture クライアントがエンドポイントにすでにインストールされている場合、ユーザーは再度 **[**確認] をクリックする必要があります。

Citrix Workspace アプリケーション経由のエンドユーザーフロー

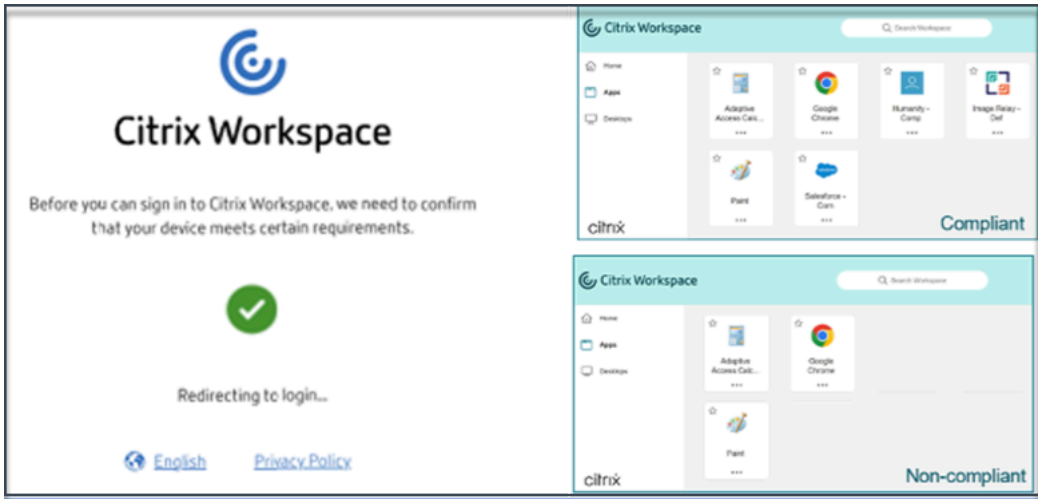
- エンドユーザーが Citrix Workspace アプリケーションを介して Citrix Workspace URL`https://your-workspace-url`にログオンすると、エンドポイントにインストールされた Device Posture クライアントが実行され、Device Posture ーポリシー要件に基づいてエンドポイントパラメータがスキャンされます。
- 最新の Device Posture クライアントがエンドポイントにインストールされていない場合、ユーザーは [再確認]、[クライアントのダウンロード] のオプションを表示するページにリダイレクトされます。ユーザーは [クライアントをダウンロード] をクリックする必要があります。
- 最新の Device Posture クライアントがエンドポイントにすでにインストールされている場合、ユーザーは再度 **[**確認] をクリックする必要があります。

エンドユーザーフロー**-Device Posture** ー結果

Device Posture ポリシーの条件によっては、3 つの可能性が考えられます。

エンドポイントがポリシー条件を満たしている場合、そのデバイスは次のように分類されます。

- 準拠 -エンドユーザーは、Secure Private Access または Citrix DaaS リソースに無制限にアクセスしてログインできます。
- 非準拠 -エンドユーザーは、Secure Private Access または Citrix DaaS リソースへのアクセスを制限してログインできます。



エンドポイントがポリシー条件を満たし、デバイスがアクセス拒否に分類される場合、「アクセス拒否 ** 」メッセージが表示されます。

アクセス拒否シナリオのカスタマイズメッセージ **(**プレビュー**)**　管理者は、アクセスが拒否されたときにエンドデバイスに表示されるメッセージをカスタマイズできます。

この機能はプレビュー中です。https://podio.com/webforms/29219975/2385710を使用してプレビューにサインアップしてください。

カスタマイズしたメッセージを追加するには、次の手順を実行します。

1. [Device Posture] **> [**デバイススキャン] ページに移動します。
2. [設定] をクリックします。
3. 「編集」をクリックし、「メッセージ」ボックスに、アクセス拒否シナリオで表示する必要があるメッセージを入力します。最大 256 文字を入力できます。

4. [保存時にカスタムメッセージを有効にする] をクリックして、カスタムメッセージを表示するオプションを適用します。このチェックボックスを選択しない場合、カスタムメッセージは作成されますが、アクセス拒否シナリオではデバイスに表示されません。

   または、設定ページのカスタムメッセージ切り替えスイッチを有効にして、デバイスにメッセージを表示することもできます。

5.「保存」をクリックします。

入力したメッセージは、エンドデバイスへのアクセスが拒否されるたびに表示されます。

Device Posture イベントの監視とトラブルシューティング

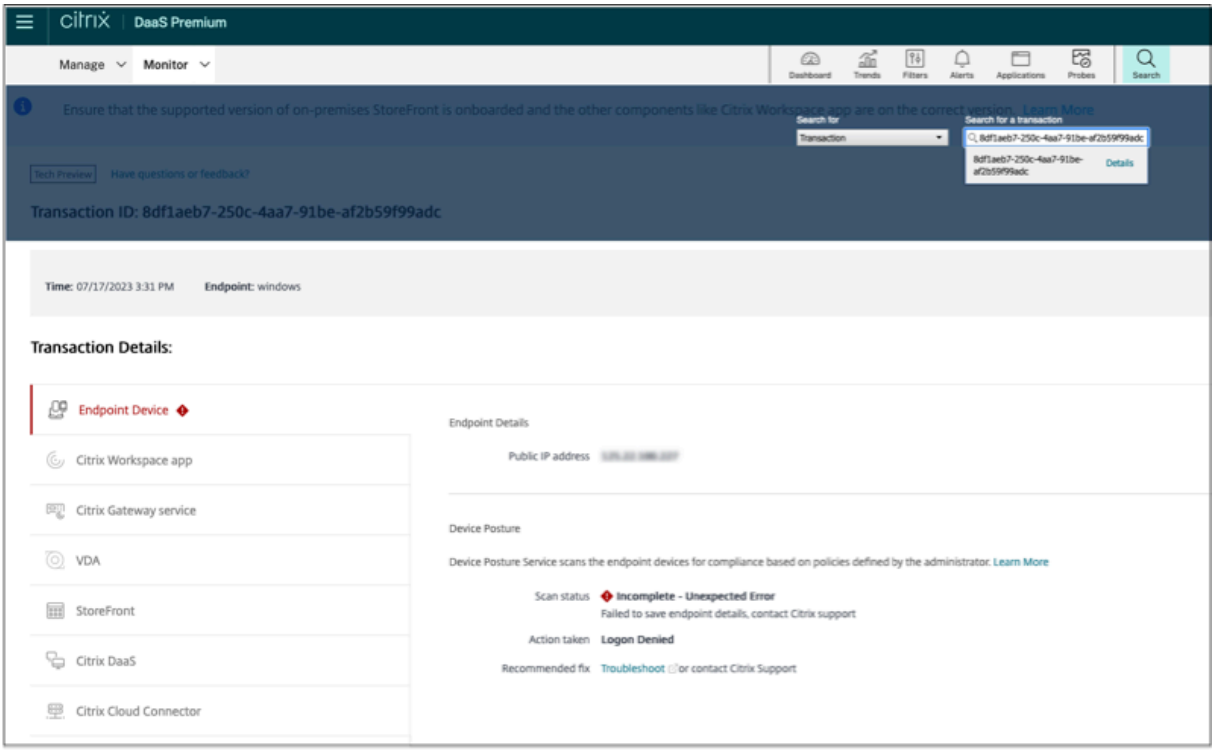
Device Posture イベントログは、次の 2 つの場所で表示できます。

- Citrix DaaS モニター
- Citrix Secure Private Access ダッシュボード

Citrix DaaS モニターの **Device Posture** イベント

Device Posture サービスのイベントログを表示するには、次の手順を実行します。

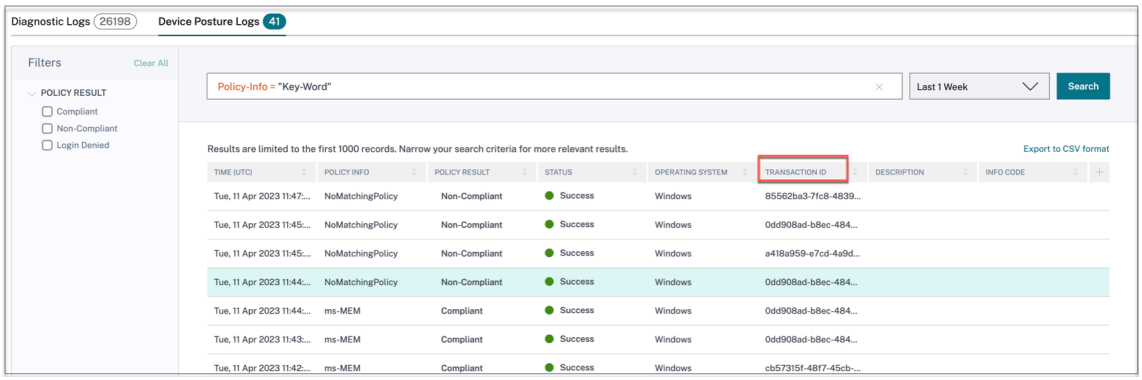
1. 失敗したセッションまたはアクセス拒否されたセッションのトランザクション ID をエンドユーザーデバイスからコピーします。
2. Citrix Cloud にサインインします。
3. DaaS タイルで **[**管理**]** をクリックし、**[**監視**]** タブをクリックします。
4. Monitor UI で、32 桁のトランザクション ID を検索し、［詳細］をクリックします。



Secure Private Access ダッシュボードの **Device Posture** イベント

Device Posture サービスのイベントログを表示するには、次の手順を実行します。

1. Citrix Cloud にサインインします。
2. 「Secure Private Access」タイルで、「管理」をクリックします。
3. 左側のメニューから [ダッシュボード] セクションに移動します。
4. 診断ログチャートの「さらに表示」リンクをクリックすると、Device Posture イベントログが表示されます。



- 管理者は、診断ログチャートのトランザクション **ID** に基づいてログをフィルタリングできます。トランザクション ID は、アクセスが拒否されるたびにエンドユーザーにも表示されます。

- エラーまたはスキャンが失敗した場合、Device Posture サービスはトランザクション ID を表示します。このトランザクション ID は、Secure Private Access サービスのダッシュボードで確認できます。ログが問題の解決に役立たない場合、エンドユーザーはトランザクション ID を Citrix サポートと共有して問題を解決できます。

- Windows クライアントログは次の場所にあります。
  - %localappdata%\Citrix\EPA\dpaCitrix.txt
  - %localappdata%\Citrix\EPA\epalib.txt
- macOS クライアントログは次の場所にあります。
  - ~/ライブラリ/アプリケーション Support/Citrix/EPAPlugin/EpaCloud.log
  - ~/ライブラリ/アプリケーション Support/Citrix/EPAPlugin/epaplugin.log

Device Posture のエラーログ

Device Posture サービスに関連する以下のログは、Citrix Monitor と Secure Private Access ダッシュボードで表示できます。これらすべてのログについては、Citrix サポートに連絡して解決してもらうことをお勧めします。

- 設定済みのポリシーの読み取りに失敗しました
- エンドポイントスキャンの評価に失敗しました
- ポリシー/式を処理できませんでした
- エンドポイントの詳細を保存できませんでした
- エンドポイントからのスキャン結果を処理できませんでした

既知の制限事項

- カスタムワークスペース URL は Device Posture サービスではサポートされていません。
- Device Posture 切り替えボタンがオンまたはオフになってから Device Posture が有効または無効になるまで、数分から 1 時間かかる場合があります。
- Device Posture 設定を変更しても、すぐには有効になりません。変更が反映されるまでに約 10 分かかる場合があります。
- Citrix Workspace でサービス継続性オプションを有効にしていて、Device Posture サービスが停止していると、ユーザーが Workspace にサインインできないことがあります。これは、Citrix Workspace がユーザーデバイス上のローカルキャッシュに基づいてアプリとデスクトップを列挙するためです。
- Citrix Workspace で有効期限の長いトークンとパスワードを設定した場合、この構成では Device Posture スキャンは機能しません。デバイスは、ユーザーが Citrix Workspace にログインしたときにのみスキャンされます。
- 各プラットフォームには最大 10 個のポリシーを設定でき、各ポリシーには最大 10 個のルールを設定できます。
- ロールベースのアクセスは、Device Posture サービスではサポートされていません。

サービス品質

- パフォーマンス: 理想的な条件下では、Device Posture サービスによりログイン中にさらに 2 秒の遅延が発生します。この遅延は、Microsoft Intune などのサードパーティ統合などの追加構成によっては増加する可能性があります。
- 耐障害性:Device Posture サービスは複数の POP による高い耐障害性を備えているため、ダウンタイムが発生しません。

定義

Device Posture サービスに関連する「準拠」と「非準拠」という用語は、次のように定義されています。

- 準拠デバイス - 事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへのフルアクセスまたは無制限アクセスで会社のネットワークにログインできるデバイス。-
- 非準拠デバイス -事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへの部分的または制限されたアクセスで会社のネットワークにログインできるデバイス。

CrowdStrike と **Device Posture** の統合**-**プレビュー

February 20, 2024

CrowdStrike ゼロトラストアセスメント (ZTA) は、各エンドデバイスの ZTA セキュリティスコアを 1 〜100 の範囲で計算することにより、セキュリティ態勢評価を行います。ZTA スコアが高いほど、エンドデバイスのセキュリティ態勢が良好であることを意味します。

Citrix Device Posture サービスは、エンドデバイスの ZTA スコアを使用して、Citrix Desktop as a Service（DaaS）および Citrix Secure Private Access（SPA）リソースへのコンテキストアクセス（スマートアクセス）を可能にします。

Device Posture 管理者は、ZTA スコアをポリシーの一部として使用し、エンドデバイスを準拠、非準拠（部分アクセス）、またはアクセス拒否に分類できます。この分類は、組織が仮想アプリやデスクトップ、SaaS、Web アプリへのコンテキストアクセス（スマートアクセス）を提供するためにも使用できます。ZTA スコアポリシーは Windows および macOS プラットフォームでサポートされています。

クラウドストライク統合の設定

CrowdStrike インテグレーションの設定は 2 段階のプロセスです。

ステップ **1:** Citrix Device Posture サービスと CrowdStrike ZTA サービス間の信頼を確立します。これは 1 回限りのアクティビティです。

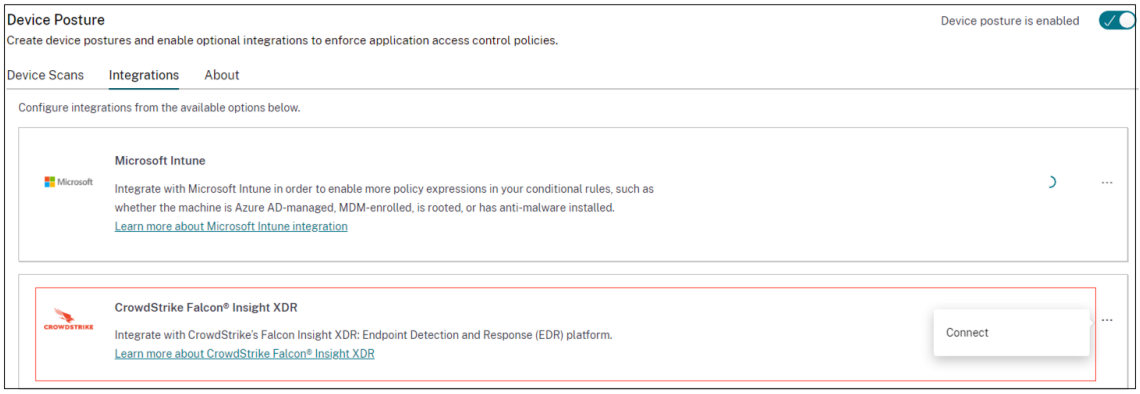
ステップ **2:** CrowdStrike ZTA スコアをルールとして使用して、Citrix DaaS および Citrix Secure Private Access リソースへのスマートアクセスを提供するようにポリシーを設定します。

ステップ **1: Citrix Device Posture** サービスと **CrowdStrike ZTA** サービス間の信頼を確立する

Citrix Device Posture サービスと CrowdStrike ZTA サービス間の信頼を確立するには、次の手順を実行します。

1. Citrix Cloud にサインインし、ハンバーガーメニューから［**ID** およびアクセス管理］を選択します。
2. [**Device Posture**] タブをクリックし、[管理] をクリックします。

3. [インテグレーション] タブをクリックします。



> 注:
>
> または、お客様は **Secure Private Access** サービス **GUI** の左側のナビゲーション・ペインにある **Device Posture** オプションに移動し、「統合」タブをクリックすることもできます。

4. **CrowdStrike** ボックスの省略記号ボタンをクリックし、「接続」をクリックします。CrowdStrike Falcon Insight XDR 統合ペインが表示されます。
5. クライアント ID とクライアントシークレットを入力し、[保存] をクリックします。

> 注:
>
> - ZTA API クライアント ID とクライアントシークレットは CrowdStrike ポータル ([サポートとリソース] **> [API** クライアントとキー**])** から取得できます。
> - 信頼を確立するには、必ず読み取り権限のあるゼロトラストアセスメントスコープとホストスコープを選択してください **。

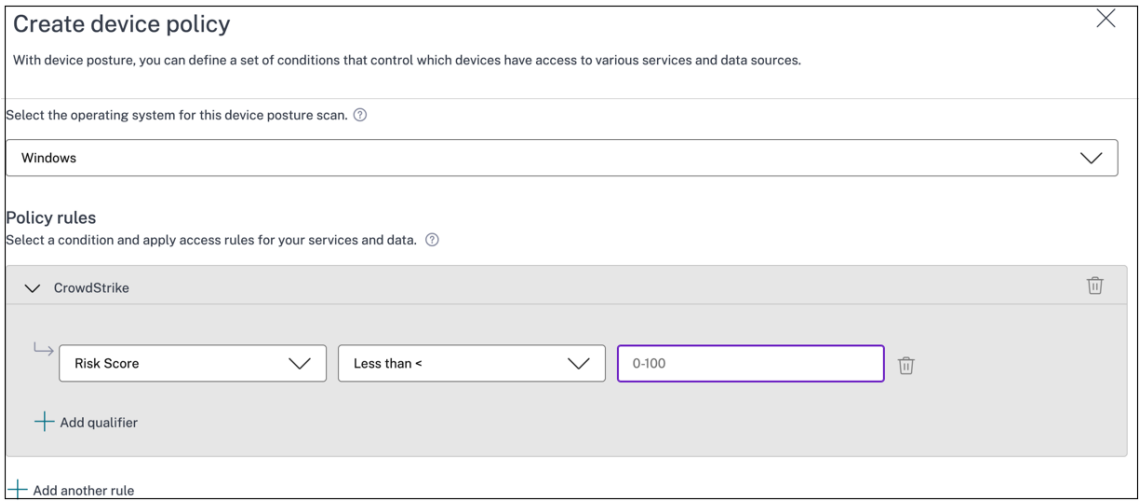
ステータスが [未構成] から [構成済み**]** に変わると、****** 統合は成功したとみなされます **。

統合が成功しなかった場合、ステータスは「保留中」と表示されます。省略記号ボタンをクリックし、**[**再接続**]** をクリックする必要があります。

ステップ **2: Device Posture** ポリシーの設定

以下を実行して、CrowdStrike ZTA スコアをルールとして使用して Citrix DaaS および Citrix Secure Private Access リソースへのスマートアクセスを提供するようにポリシーを構成します。

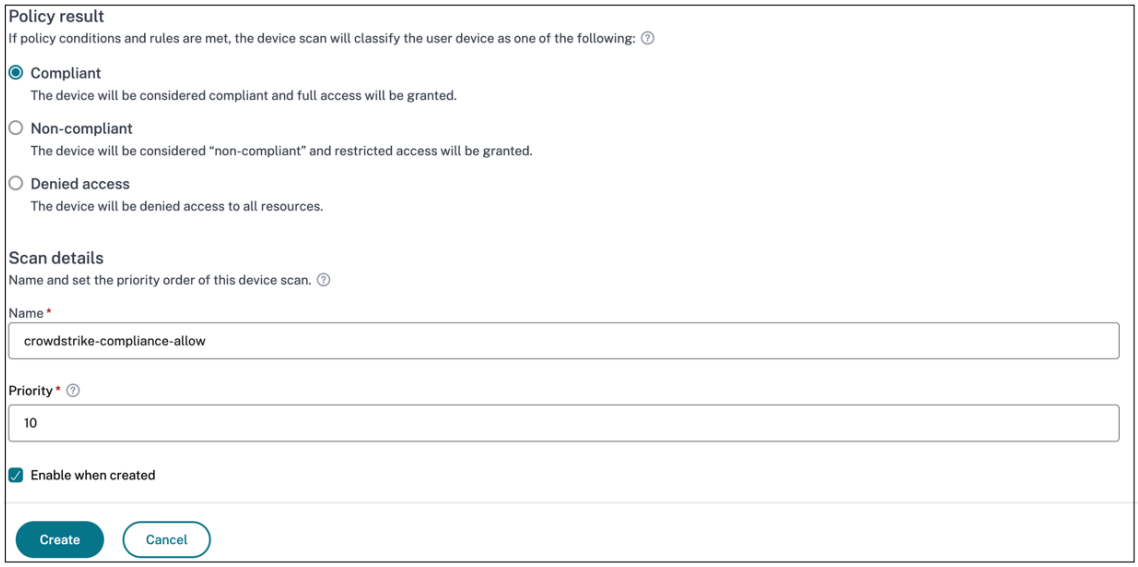
1. [デバイススキャン] タブをクリックし、[デバイスポリシーの作成] をクリックします。



2. このポリシーを作成するプラットフォームを選択してください。
3. 「ポリシールール」で「クラウドストライク」を選択します。
4. リスクスコア修飾子では、条件を選択し、リスクスコアを入力します。
5. **+** をクリックすると、CrowdStrike Falcon センサーが動作しているかどうかを確認する修飾子が追加されます。

> 注:
>
> このルールは、Device Posture に設定した他のルールと併用できます。

6. 設定した条件に基づくポリシー結果で、次のいずれかを選択します。
   - 準拠
   - 非準拠
   - ログイン拒否



7. ポリシーの名前を入力し、優先度を設定します。
8. ［作成］をクリックします。

定義

Device Posture サービスに関する準拠用語と非準拠用語の定義は次のとおりです。

- 準拠デバイス - 事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへのフルアクセスまたは無制限アクセスで会社のネットワークにログインできるデバイス。-
- 非準拠デバイス -事前に設定されたポリシー要件を満たし、Citrix Secure Private Access リソースまたは Citrix DaaS リソースへの部分的または制限されたアクセスで会社のネットワークにログインできるデバイス。

参照ドキュメント

Device Posture サービス

Microsoft Intune と Device Posture の統合

February 20, 2024

Microsoft Intune は、ポリシー構成に基づいて、ユーザーのデバイスを準拠デバイスまたは登録済みデバイスとして分類します。ユーザーが Citrix Workspace にログインしている間、Device Posture はユーザーのデバイスステータスを Microsoft Intune で確認し、この情報を使用して Citrix Cloud 内のデバイスを準拠しているか、準拠していないか（部分的なアクセス）に分類し、ユーザーログインページへのアクセスを拒否することもできます。Citrix DaaS や Citrix Secure Private Access などのサービスは、Device Posture によるデバイス分類を使用して、それぞれ仮想アプリやデスクトップ、SaaS や Web アプリへのコンテキストアクセス（スマートアクセス）を提供します。

Microsoft Intune 統合を構成するには

Intune 統合構成は 2 段階のプロセスです。

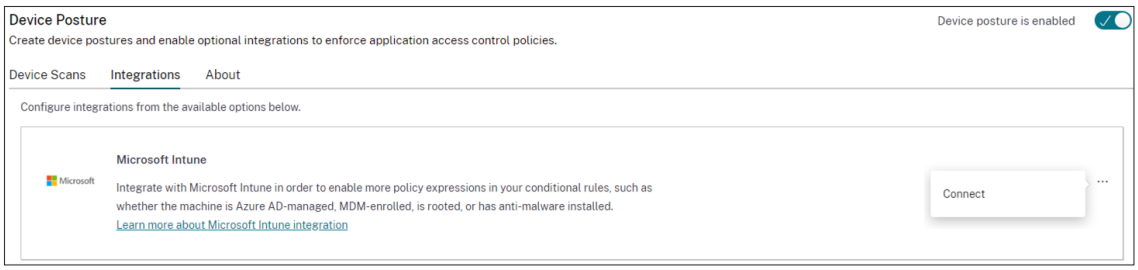
ステップ **1:** Device Posture を Microsoft Intune サービスと統合します。これは、Device Posture と Microsoft Intune 間の信頼を確立するために行う 1 回限りのアクティビティです。

ステップ **2:** Microsoft Intune の情報を使用するようにポリシーを設定します。

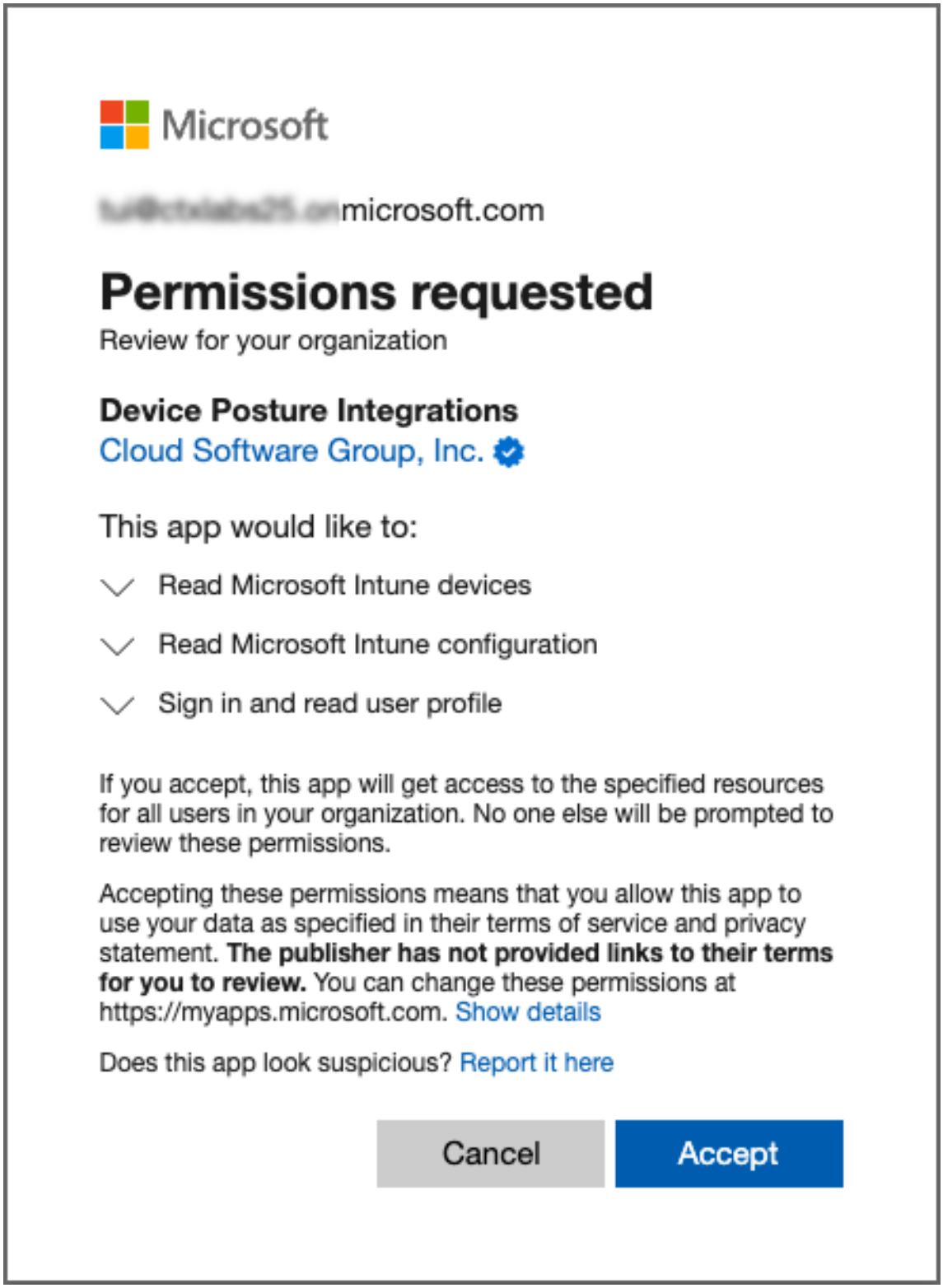
ステップ **1: Device Posture** を **Microsoft Intune** と統合します

1. インテグレーションタブにアクセスするには、以下のいずれかの方法を使用します。

   - ブラウザで URL（https://device-posture-config.cloud.com）にアクセスし、「統合」タブをクリックします。
   - Secure Private Access のお客様-Secure Private Access GUI の左側のナビゲーション・ペインで、「デバイス・ポスチャ」をクリックし、「統合」タブをクリックします。



2. 省略記号ボタンをクリックし、[接続] をクリックします。管理者は Azure AD にリダイレクトされ、認証されます。



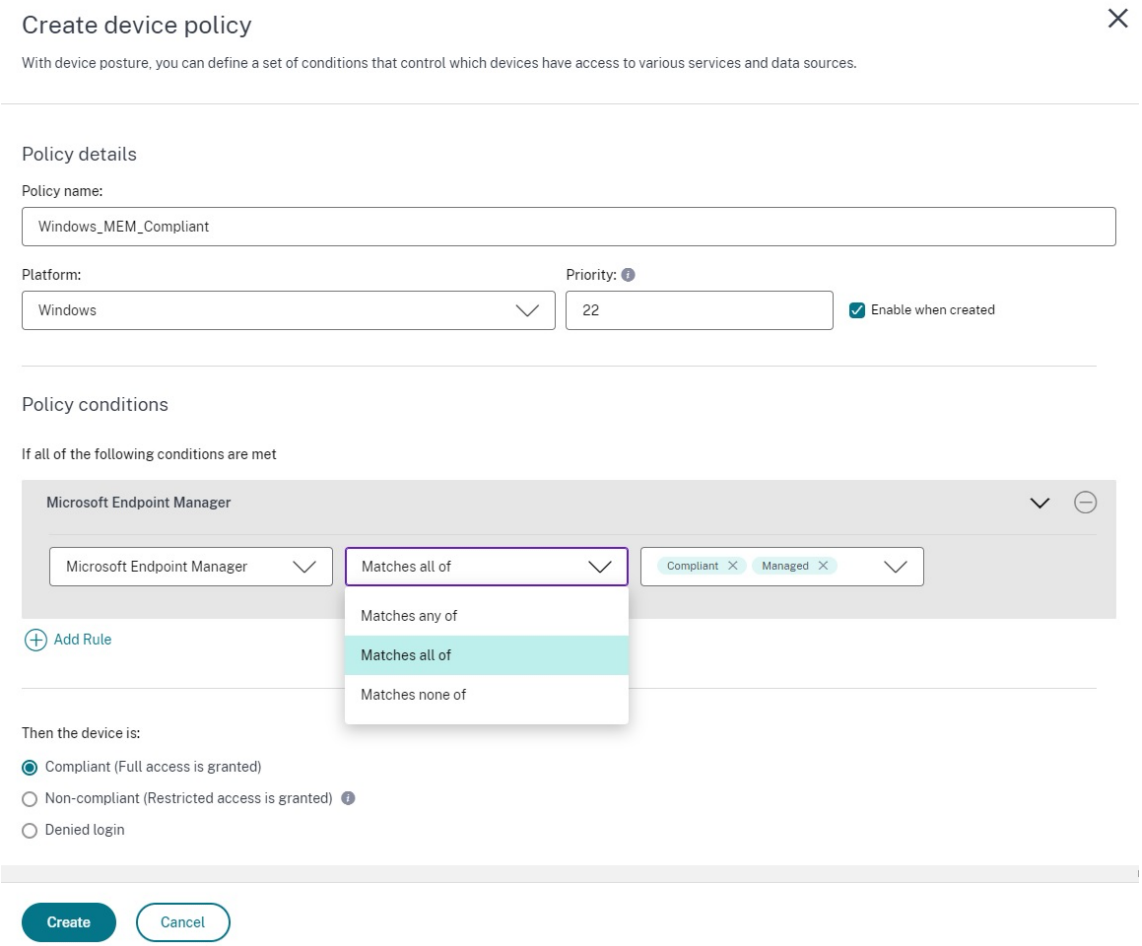
統合ステータスが [未設定] から **[**** 構成済み ****] に変わったら、管理者は Device Posture ポリシーを作成できます。

統合が成功しなかった場合、ステータスは「保留中」と表示されます。省略記号ボタンをクリックし、 [再接続] をク

リックする必要があります。

ステップ **2: Device Posture** ポリシーの設定

1. [デバイススキャン] タブをクリックし、[デバイスポリシーの作成] をクリックします。



2. ポリシーの名前を入力し、優先度を設定します。
3. このポリシーを作成するプラットフォームを選択してください。
4. 「ルールを選択」で「**Microsoft** エンドポイントマネージャー」を選択します。
5. 条件を選択し、一致させる MEM タグを選択します。

   - いずれかに一致する場合は、OR 条件が適用されます。
   - すべて一致する場合は、AND 条件が適用されます。

   > 注:
   >
   > このルールは、Device Posture に設定した他のルールと併用できます。

6. デバイスは次のようになります。設定した条件に基づいて、次のいずれかを選択します。

- 準拠 (フルアクセスが許可されている)
- 非準拠 (制限付きアクセスが許可されている)
- ログイン拒否

ポリシーの作成の詳細については、「Device Posture ポリシーの設定」を参照してください。

Device Posture サービスによるデバイス証明書チェック

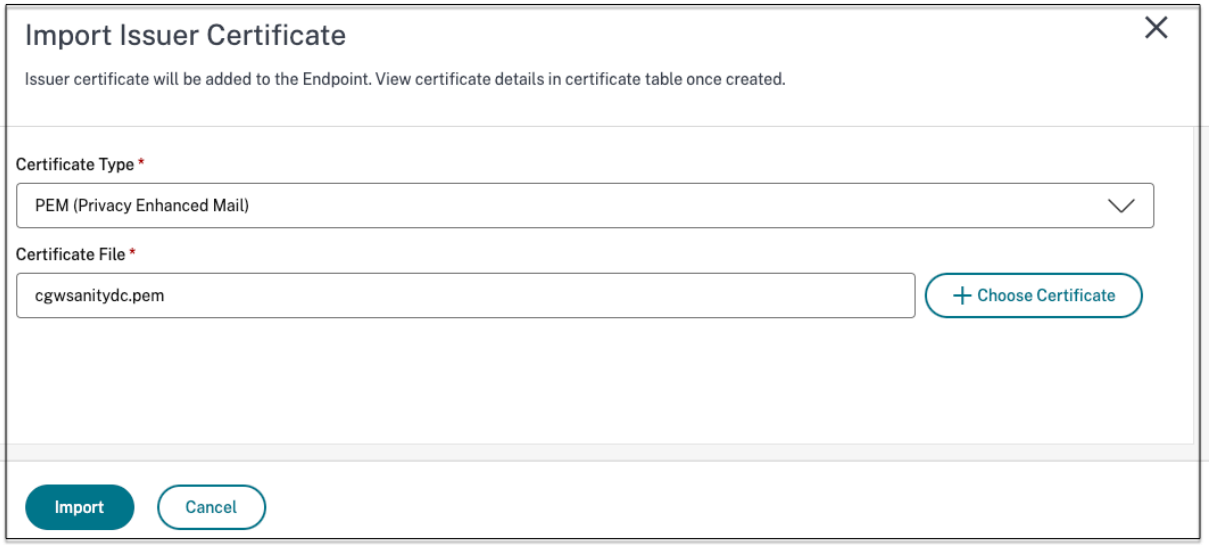
February 20, 2024

Device Posture サービスでデバイス証明書チェックを設定するには、管理者はデバイスから発行者証明書をインポートする必要があります。Device Posture サービスに有効な発行者証明書が存在すると、管理者は Device Posture ポリシーの一部としてデバイス証明書チェックを使用できます。

> 注意事項
>
> - Device Posture サービスは PEM 発行者証明書タイプのみをサポートします。
> - Windows でデバイス証明書をチェックするには、エンドデバイスの EPA クライアントを管理権限でインストールする必要があります。その他のチェックでは、ローカル管理者権限は必要ありません。サポートされているスキャンの詳細については、「Device Posture でサポートされるスキャン」を参照してください。
> - 管理者権限で EPA クライアントを Windows にインストールするには、EPA クライアントプラグインをダウンロードした場所で次のコマンドを実行します。
>
> ```
> msiexec /i epasetup.msi
> ```
>
> - Device Posture サービスによるデバイス証明書チェックは、証明書失効チェックをサポートしていません。
> - デバイス証明書が中間証明書によって署名されている場合は、ルート証明書と中間証明書を含むチェーン全体を 1 つの PEM ファイルにアップロードする必要があります。
>
> ```
> Example: chain.pem
>
> -----BEGIN CERTIFICATE-----
> ******************************
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
> ******************************
> -----END CERTIFICATE
> ```


デバイス証明書をアップロード

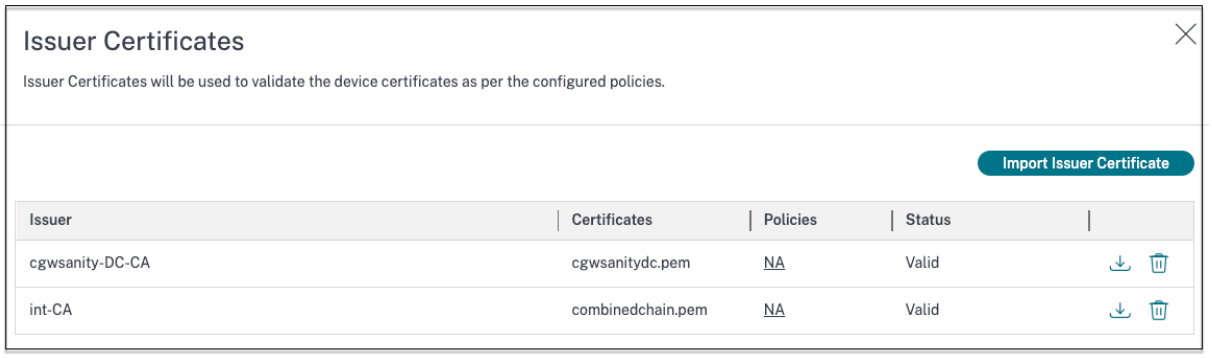
1. Device Posture のホームページで [設定] をクリックします。
2. [管理] をクリックし、[発行証明書のインポート] をクリックします。
3. [証明書の種類] で、証明書のタイプを選択します。PEM タイプのみがサポートされます。
4. [証明書ファイル] で、**[**証明書を選択**]** をクリックして発行者証明書を選択します。
5. [開く] をクリックし、**[**インポート**]** をクリックします。



選択した証明書は **[**設定**] > [**発行者証明書**]** に表示されます。複数の証明書をインポートできます。

インポートした証明書を表示する

1. Device Posture のホームページで [設定] をクリックします。
2. [発行者証明書**]** で、**[**管理**]** をクリックします。
3. [発行者証明書] ページには、インポートされた発行者証明書が一覧表示されます。

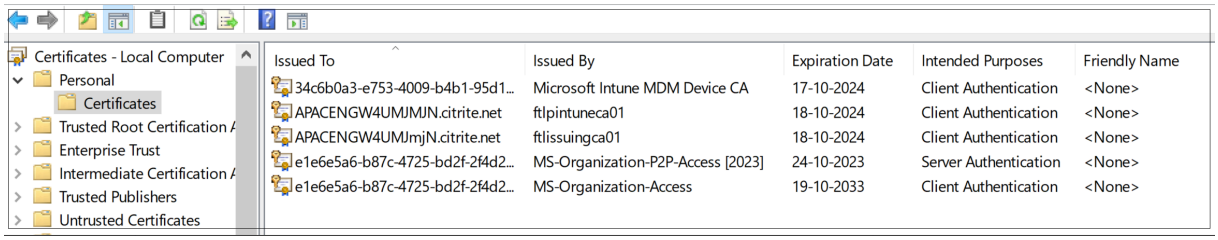


エンドデバイスにデバイス証明書をインストールします

Windows:

1. [スタート] メニューから、[コンピューター証明書マネージャー] を開きます。
2. 証明書が`Certificates - Local Computer\Personal\Certificates`にインストールされていることを確認します。

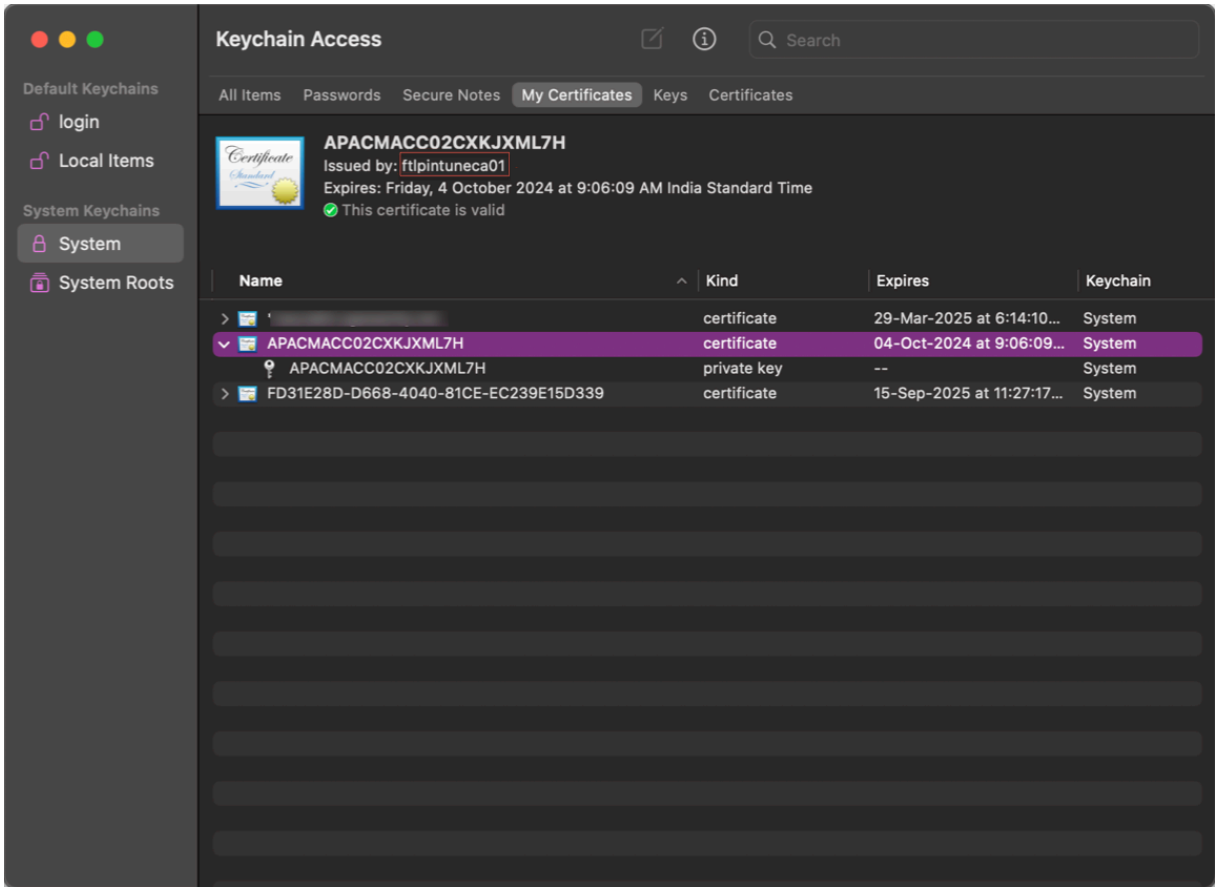
    - 意図された目的には、クライアント認証を含める必要があります。
    - 発行者列は、管理 GUI で設定された発行者名と一致する必要があります。



macOS:

1. 「キーチェーンアクセス」を開き、「システム」を選択します。
2. [ファイル**] > [**項目のインポート] をクリックして証明書をインポートします。

    発行者フィールドには、証明書の発行者名が表示されている必要があります。



Device Posture を使用して **DaaS** にスマートコントロールを適用

February 20, 2024

Citrix Device Posture サービスを介して Citrix Desktop as a Service（DaaS）リソースにアクセスしているときに、スマートコントロールを適用できます。

> 注:
>
> これは完全な構成ではなく、Device Posture を使用して Studio ポリシーを構成する方法のサンプルです。

この例では、Device Posture サービスタグ（準拠および非準拠）を使用して、Citrix DaaS リソースのコピーアンドペースト機能を無効にするポリシーが作成されます。

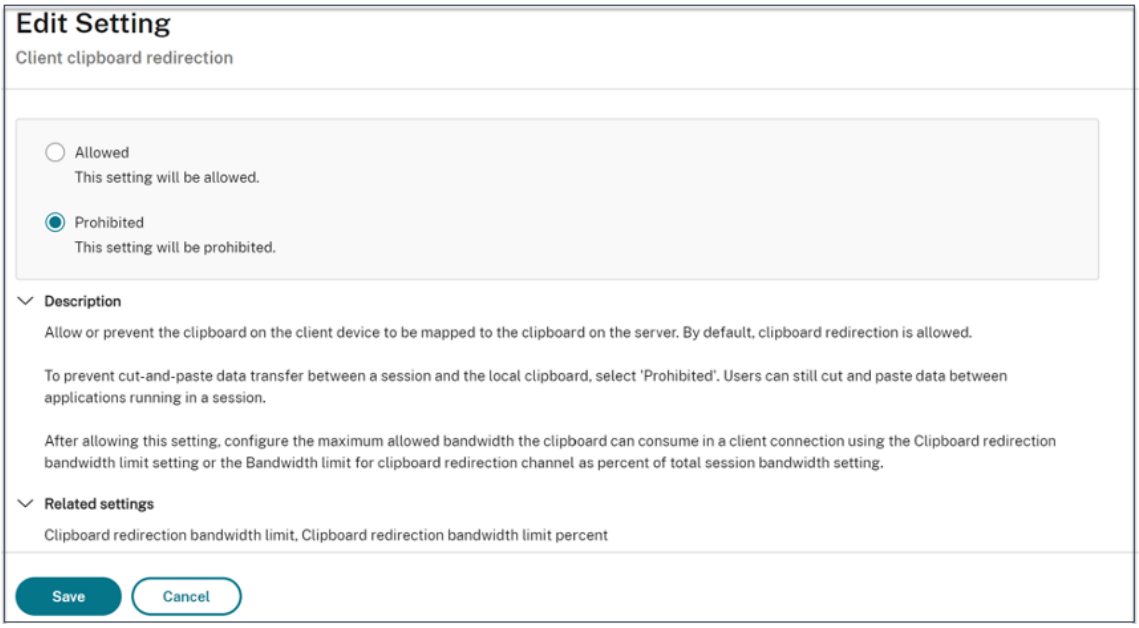
Citrix DaaS 上の非対応デバイスからアクセスするユーザーのコピー & ペースト機能を無効にするには、次の手順を実行します:

1. Citrix DaaS の構成ページで、［管理］タブをクリックします。
2. ［ポリシー］タブをクリックします。

3. ［ポリシーの作成］ を選択します。

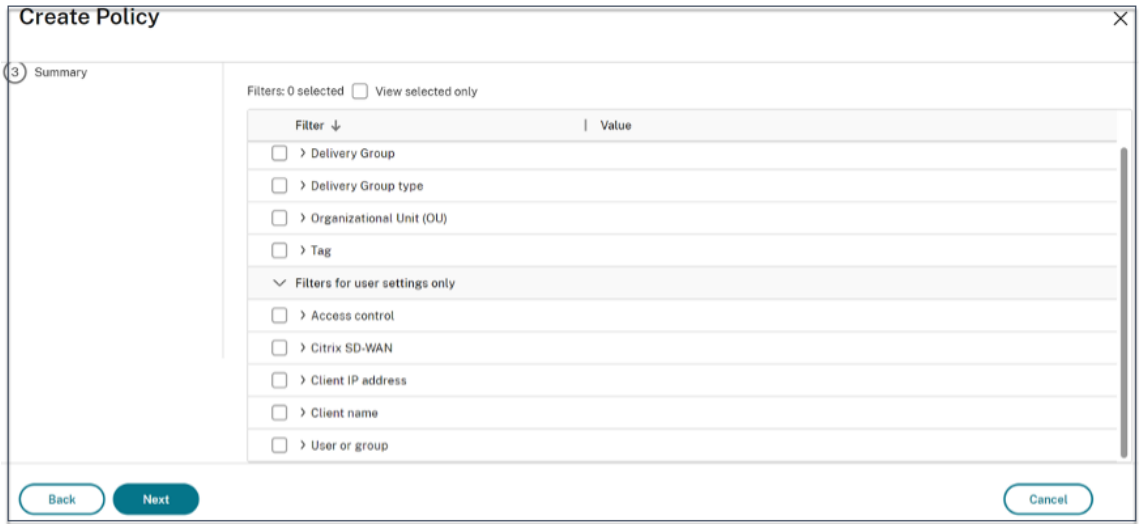
4. **[**設定の選択**]** で、[クライアントクリップボードリダイレクト] を選択します。

5. [設定の編集] で [禁止] を選択し、[保存] をクリックします。



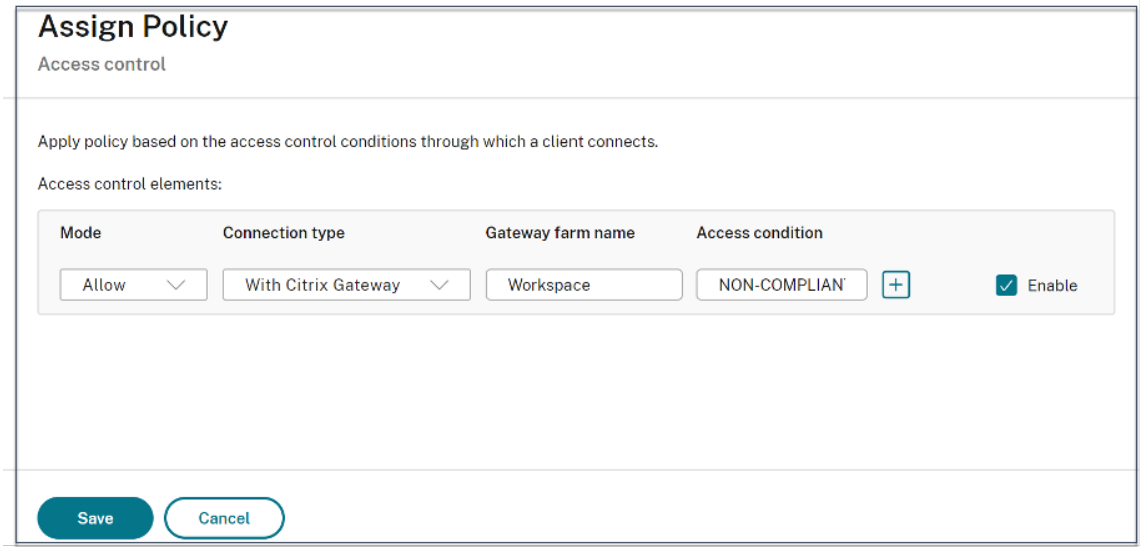
6.「ユーザーとマシン」ページで、「フィルターされたユーザーとコンピュータ」をクリックし、このポリシーをアクセスコントロールに割り当てます。

7. [ユーザー設定のみ**]** の **[**フィルター] に移動し、[アクセス制御] を選択します。



8.「ポリシーの割り当て」ページでは、「モード」と「接続タイプ」はデフォルト設定のままにします。

「ゲートウェイファーム名」に「ワークスペース」と入力し、「アクセス条件」に「非準拠」と入力します。



9. ポリシーの名前を入力します。ポリシーには、適用対象者や対象に応じて名前を付けることを検討してください。たとえば、非準拠デバイスにはクリップボードアクセスが制限されます。また、必要に応じて説明を入力します。
10. 「完了」をクリックします。

> 注:
>
> このポリシーは、デフォルトでは無効になっています。ポリシーを有効にすると、ログオンしているユーザーにすぐに適用できます。無効にしたポリシーは適用されません。作成済みのポリシーに優先度を設定したり、設定項目を追加したりする必要がある場合は、そのポリシーを一時的に無効にすることを検討してください。

ポリシー構成を検証する方法

ポリシーを広く導入する前に、ポリシーを検証して、意図したとおりに機能していることを確認してください。設定例では以下のようになります:

- 準拠しているエンドデバイスからアクセスするユーザーの場合、Citrix DaaS リソースはコピーアンドペーストの制限なしで列挙する必要があります。
- 非準拠のエンドデバイスからアクセスするユーザーの場合、Citrix DaaS リソースをコピーアンドペーストの制限付きで列挙する必要があります。

デバイスポスチャログ

February 20, 2024

Secure Private Access サービスダッシュボードは、SaaS/Web および TCP/UDP アプリに関連するログに加えて、デバイスのポスチャログもキャプチャします。

Device Posture ログを表示するには、[Device Posture ログ（**Device Posture Logs**）] タブをクリックします。ポリシーの結果 ([準拠]、[非準拠]、[ログイン拒否]) に基づいて検索を絞り込むことができます。

詳細については、「診断ログ」を参照してください。

Device Posture サービス用 **Citrix** エンドポイント分析クライアントの管理

February 20, 2024

Citrix Device Posture サービスは、管理者が Citrix DaaS（仮想アプリおよびデスクトップ）または Citrix Secure Private Access リソース（SaaS、Web アプリ、TCP、および UDP アプリ）にアクセスするためにエンドデバイスが満たす必要のある特定の要件を管理者が適用できるようにするクラウドベースのソリューションです。

エンドデバイスで Device Posture スキャンを実行するには、軽量アプリケーションである Citrix EndPoint Analysis (EPA) クライアントをそのデバイスにインストールする必要があります。Device Posture サービスは、常に Citrix がリリースした最新バージョンの EPA クライアントで実行されます。

EPA クライアントのインストール

実行中、Device Posture サービスはエンドユーザに対し、実行時に EPA クライアントをダウンロードしてインストールするように求めます。詳しくは、「エンドユーザーフロー」を参照してください。
通常、EPA クライアントをエンドポイントにダウンロードしてインストールするためにローカル管理者権限は必要ありません。ただし、エンドデバイス上でデバイス証明書チェックスキャンを実行するには、管理者アクセス権で EPA クライアントをインストールする必要があります。管理者アクセスで EPA クライアントをインストールする方法の詳細については、「エンドデバイスへのデバイス証明書のインストール」を参照してください。

Windows 用 **EPA** クライアントのアップグレード

EPA クライアントの新しいバージョンがリリースされると、Windows 用 EPA クライアントは最初のインストール後にデフォルトでアップグレードされます。自動アップグレードにより、エンドユーザーデバイスは常に Device Posture サービスと互換性のある EPA クライアントの最新バージョンで動作するようになります。自動アップグレードを行うには、EPA クライアントが管理者権限でインストールされている必要があります。

> **注:**
>
> 自動アップグレードは現在プレビュー中です。https://podio.com/webforms/29214695/2384946を使用してプレビューにサインアップしてください。

EPA クライアントの配布

EPA クライアントは、グローバルアプリ構成サービス（GACS）または Citrix Workspace アプリインストーラーと統合された EPA、またはソフトウェア展開ツールを使用して配布できます。

- **Citrix Workspace** アプリと統合された **EPA** クライアント（プレビュー）: EPA クライアントは Citrix Workspace アプリとも統合されています。この統合により、エンドユーザーは Citrix Workspace アプリをインストールした後に EPA クライアントをインストールする必要がなくなります。
  - エンドデバイスにすでに EPA クライアントがインストールされていて、エンドユーザーが Citrix Workspace アプリをインストールした場合、統合された EPA クライアントはそのデバイスにインストールされません。既存の EPA クライアントはデバイスのポスチャチェックに使用されます。
  - 同様に、エンドユーザーが Citrix Workspace アプリをアンインストールすると、統合された EPA クライアントもデフォルトでデバイスから削除されます。ただし、EPA クライアントが統合された Citrix Workspace アプリのインストールの一部としてインストールされていない場合は、既存の EPA クライアントはデバイスに保持されます。

> 注:
>
> - EPA クライアントと Citrix Workspace アプリの統合は Windows プラットフォームでのみサポートされており、プレビュー段階です。https://podio.com/webforms/29219973/2385708を使用してプレビューにサインアップしてください。

- **GACS** を使用してクライアントを配布: GACS は、クライアント側のエージェント（プラグイン）の配布を管理するための Citrix 提供のソリューションです。GACS で利用可能な自動更新サービスにより、エンドユーザーの介入なしにエンドデバイスが最新の EPA バージョンになります。GACS について詳しくは、「グローバルアプリ構成サービスの使用方法」を参照してください。

> 注:
>
> - GACS は、EPA クライアントを配布する目的でのみ Windows デバイスでサポートされます。
> - GACS を使用して EPA クライアントを管理するには、エンドデバイスに Citrix Workspace アプリケーション (CWA) をインストールします。
> - CWA がエンドユーザーデバイスの管理者権限でインストールされている場合、GACS は同じ管理者権限で EPA クライアントをインストールします。
> - CWA がエンドユーザーデバイスのユーザー権限でインストールされている場合、GACS は同じユーザー権限で EPA クライアントをインストールします。

ソフトウェア展開ツールを使用してクライアントを配布: 最新の EPA クライアントは、管理者が Microsoft SCCM などのソフトウェア展開ツールを使用して配布できます。

NetScaler および **Device Posture** と併用する場合の **EPA** クライアントの管理

EPA クライアントは、次の展開で NetScaler および Device Posture と併用できます。

- EPA による NetScaler ベースのアダプティブ認証
- EPA による NetScaler ベースのオンプレミスゲートウェイ

Device Posture サービスは、最新バージョンの EPA クライアントをエンドデバイスにプッシュします。ただし、NetScaler では、管理者はゲートウェイ仮想サーバーでの EPA スキャンに対して次のバージョン管理を構成できます。

- 常に: エンドデバイス上の EPA クライアントと NetScaler は同じバージョンである必要があります。
- 必須: エンドデバイスの EPA クライアントバージョンは、NetScaler で設定されている範囲内である必要があります。
- なし: エンドデバイスには、どのバージョンの EPA クライアントでもかまいません。

詳しくは、「プラグインの動作」を参照してください。

EPA クライアントを NetScaler および Device Posture と併用する場合の考慮事項

EPA クライアントを Device Posture サービスおよび NetScaler と併用する場合、エンドデバイスでは最新の EPA クライアントバージョンが実行されているのに対し、NetScaler では異なるバージョンの EPA クライアントが実行されている場合があります。これにより、NetScaler とエンドデバイスの EPA クライアントのバージョンが一致しなくなる可能性があります。その結果、NetScaler は、NetScaler に存在する EPA クライアントバージョンをインストールするようにエンドユーザーに求める場合があります。この競合を避けるため、以下の構成変更をお勧めします。

- EPA をアダプティブ認証、オンプレミス認証、またはゲートウェイ仮想サーバーで構成している場合は、NetScaler での EPA クライアントのバージョン管理を無効にすることをお勧めします。これは、GACS または Device Posture サービスが最新バージョンの EPA クライアントをエンドデバイスにプッシュしないようにするためです。
- EPA バージョン管理は CLI または GUI を使用して **[なし]** に設定できます。これらの構成変更は、NetScaler 13.x 以降のバージョンでサポートされます。
  - CLI: アダプティブ認証およびオンプレミス認証仮想サーバーに CLI コマンドを使用します。
  - GUI: オンプレミスのゲートウェイ仮想サーバーに GUI を使用します。詳しくは、「Citrix Secure Access クライアントのアップグレードを制御」を参照してください。

CLI コマンドの例**:**

```
add rewrite action <rewrite_action_name> insert_http_header Plugin-Upgrade ""epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:Never;vpn_mac:Always;vpn_linux:Always;""

add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("pluginlist.xml")" <rewrite_action_name>

bind authentication vserver <Authentication_Vserver_Name> -policy <rewrite_action_policy> -priority 10 -type RESPONSE
```



```
<!--NeedCopy-->
```

データガバナンス

February 20, 2024

このトピックでは、Device Posture サービスによるログの収集、保存、および保持に関する情報を提供します。定義セクションで定義されていない大文字の用語は 、Citrix エンドユーザーサービス契約で指定された意味を持ちます。

データ所在地

Citrix の Device Posture の顧客コンテンツデータは、AWS と Azure のクラウドサービスにあります。可用性と冗長性のために以下のリージョンに複製されます。

- AWS
  - 米国東部
  - 西インド
  - ヨーロッパ (フランクフルト)
- Azure
  - 米国西部
  - 西ヨーロッパ
  - アジア (シンガポール)
  - 米国中南部

サービス設定、ランタイムログ、およびイベントのさまざまな宛先は次のとおりです。

- システム監視とデバッグログ用の Splunk サービス、米国内のみ。
- 診断ログとユーザーアクセスログについては、「Citrix Analytics サービスのデータガバナンス」を参照してください。
- 管理者監査ログ用の Citrix Cloud システムログサービス。詳しくは、「Citrix Cloud Services の顧客コンテンツとログの処理」および「地理的な考慮事項」を参照してください。

データ収集

Citrix の Device Posture サービスでは、顧客管理者が Device PostureUI を使用してサービスを構成できます。次の顧客コンテンツは、Device Posture ポリシー設定とプラットフォームに基づいて収集されます。

- オペレーティングシステムバージョン
- Citrix Workspace アプリのバージョン
- MAC アドレス
- 実行中のプロセス
- デバイス証明書
- レジストリの詳細
- Windows インストールアップデートの詳細
- 前回の Windows アップデートの詳細
- ファイルシステム—ファイル名、ファイルハッシュ、変更日時
- ドメイン名

サービスコンポーネントによって収集されたランタイムログの場合、重要な情報は次のもので構成されます。

- 顧客/テナント ID
- デバイス ID (Citrix が生成した一意の識別子)
- Device Posture スキャン出力
- エンドポイントデバイスのパブリック IP アドレス

データ送信

Citrix Device Posture サービスは、トランスポート層セキュリティで保護された宛先にログを送信します。

データ管理

Citrix Device Posture サービスでは、現在、ログの送信をオフにしたり、お客様のコンテンツがグローバルに複製されないようにしたりするオプションをお客様に提供していません。

データ保持

Citrix Cloud のデータ保持ポリシーに基づいて、顧客の構成データは、サブスクリプションの有効期限が切れてから 90 日後にサービスから削除されます。

ログの宛先は、サービス固有のデータ保持ポリシーを維持します。

- 詳しくは、Analytics ログ保持ポリシーの「データガバナンス」を参照してください。
- Splunk ログはアーカイブされ、最終的には 90 日後に削除されます。

データのエクスポート

ログの種類ごとに異なるデータエクスポートオプションがあります。

- 管理者監査ログには、Citrix Cloud システムログコンソールからアクセスできます。
- Device Posture サービスの診断ログは、Citrix Analytics サービスまたは Secure Private Access サービスのダッシュボードから CSV ファイルとしてエクスポートできます。

定義

- 「顧客コンテンツ」とは、Citrix がサービスを実行するためのアクセス権を与えられている顧客環境のストレージまたはデータを保存するために顧客アカウントにアップロードされたデータを指します。
- ログとは、パフォーマンス、安定性、使用状況、セキュリティ、およびサポートを測定する記録を含む、サービスに関連するイベントの記録を意味します。
- サービスとは、Citrix Analytics の目的で前述した Citrix Cloud サービスを意味します。