デバイスポスチャ

Machine translated content

Disclaimer

Contents

新機能

June 19, 2024

2024 年 **5** 月 **29** 日

- テストモードでのデバイスポスチャサービスの可用性-プレビュー

  デバイスポスチャ サービスはテストモードでも利用でき、管理者は本番環境で有効にする前にデバイスポスチャサービスをテストできます。これにより、管理者はデバイスポスチャスキャンがエンドユーザーのデバイスに与える影響を分析し、本番環境で有効にする前にそれに応じてアクションプランを立てることができます。詳細については、「テストモードのデバイスポスチャサービス-プレビュー」を参照してください。

- デバイスの定期スキャン-プレビュー

  Windows デバイスの定期スキャンで、設定したチェックを 30 分ごとに実行できるようになりました。詳細については、「デバイスの定期スキャン-プレビュー」を参照してください。

2024 年 **5** 月 **14** 日

- デバイスポスチャチェックを省略

  管理者は、エンドユーザーがデバイスのデバイスポスチャチェックをスキップできるようにすることができます。詳細については、「デバイスポスチャチェックをスキップする」を参照してください。

- デバイスポスチャダッシュボード

  デバイスポスチャ サービスポータルに、ログを監視およびトラブルシューティングするためのダッシュボードが追加されました。これで、管理者はこのダッシュボードを監視やトラブルシューティングに使用できるようになりました。詳細については、デバイスポスチャログを参照してください。

- ブラウザとウイルス対策チェックの一般提供状況

  ブラウザとウイルス対策のチェックが一般公開されました。詳細については、「デバイスポスチャでサポートされるスキャン」を参照してください。

- カスタムメッセージの一般提供状況

  アクセスが拒否されたときにカスタマイズされたメッセージを追加するオプションが一般提供されました。詳細については、「アクセス拒否シナリオのカスタマイズメッセージ」を参照してください。

2024 年 **3** 月 **26** 日

- カスタムワークスペース **URL** のサポート

カスタムワークスペース URL が デバイスポスチャ サービスでサポートされるようになりました。ワークスペースにアクセスするには、cloud.com の URL に加えて所有している URL を使用できます。ネットワークから citrix.com へのアクセスを許可していることを確認してください。カスタムドメインの詳細については、「カスタムドメインの設定」を参照してください。

2024 年 2 月 12 日

- ブラウザとウイルス対策チェックのサポート-プレビュー

  デバイスポスチャ サービスがブラウザとウイルス対策チェックをサポートするようになりました。詳細については、「デバイスポスチャでサポートされるスキャン」を参照してください。

2024 年 1 月 23 日

- デバイスポスチャサービスによるデバイス証明書チェックの一般提供

  デバイスポスチャ サービスによるデバイス証明書チェックが一般利用できるようになりました。詳しくは、「デバイスポスチャサービスによるデバイス証明書チェック」を参照してください。

- デバイスポスチャサービスのプレビュー機能

  デバイスポスチャサービスは次のチェックをサポートするようになりました:

  - デバイスポスチャサービスが IGEL プラットフォームでサポートされるようになりました。
  - デバイスポスチャ サービスがジオロケーションとネットワークロケーションのチェックをサポートするようになりました。

  詳細については、「デバイスポスチャ」を参照してください。

2023 年 9 月 11 日

- **Microsoft Intune** とのデバイスポスチャ統合の一般公開

  Microsoft Intune とのデバイスポスチャ統合が一般公開されました。詳しくは、「Microsoft Intune とデバイスポスチャの統合」を参照してください。

2023 年 8 月 30 日

- デバイスポスチャサービス用 **Citrix Endpoint Analysis** クライアントの管理

  EPA クライアントは NetScaler およびデバイスポスチャと一緒に使用できます。NetScaler とデバイスポスチャと併用する場合、EPA クライアントを管理するにはいくつかの設定変更が必要です。詳しくは、「デバイスポスチャサービス用 Citrix Endpoint Analysis クライアントの管理」を参照してください。

2023 年 8 月 28 日

- **iOS** プラットフォームでのデバイスポスチャサービスのサポート-プレビュー

  デバイスポスチャサービスが iOS プラットフォームでサポートされるようになりました。詳しくは、「デバイスポスチャ」を参照してください。

2023 年 8 月 22 日

- **Citrix** デバイスポスチャサービスによるデバイス証明書チェック-プレビュー

  Citrix デバイスポスチャサービスでは、エンドデバイスの証明書を企業の認証局と照合してエンドデバイスが信頼できるかどうかを判断することで、Citrix DaaS および Secure Private Access リソースへのコンテキストアクセス（スマートアクセス）が可能になりました。詳しくは、「デバイスポスチャサービスによるデバイス証明書チェック」を参照してください。

2023 年 8 月 17 日

- **Citrix DaaS** モニターのデバイスポスチャイベント

  デバイスポスチャサービスのイベントと監視ログを DaaS Monitor で検索できるようになりました。詳しくは、「Citrix DaaS モニターのデバイスポスチャイベント」を参照してください。

2023 年 1 月 23 日

- デバイスポスチャサービス

  Citrix デバイスポスチャサービスは、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。詳細については、「デバイスポスチャ」を参照してください。

  [AAUTH-90]

- **Microsoft** エンドポイントマネージャーとデバイスポスチャの統合

  デバイスポスチャサービスが提供するネイティブスキャンに加えて、デバイスポスチャサービスは他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。デバイスポスチャは Windows および macOS 上の Microsoft エンドポイントマネージャ (MEM) と統合されています。詳細については、「Microsoft Endpoint Manager とデバイスポスチャの統合」を参照してください。

  [ACS-1399]

テストモードのデバイスポスチャサービス-プレビュー

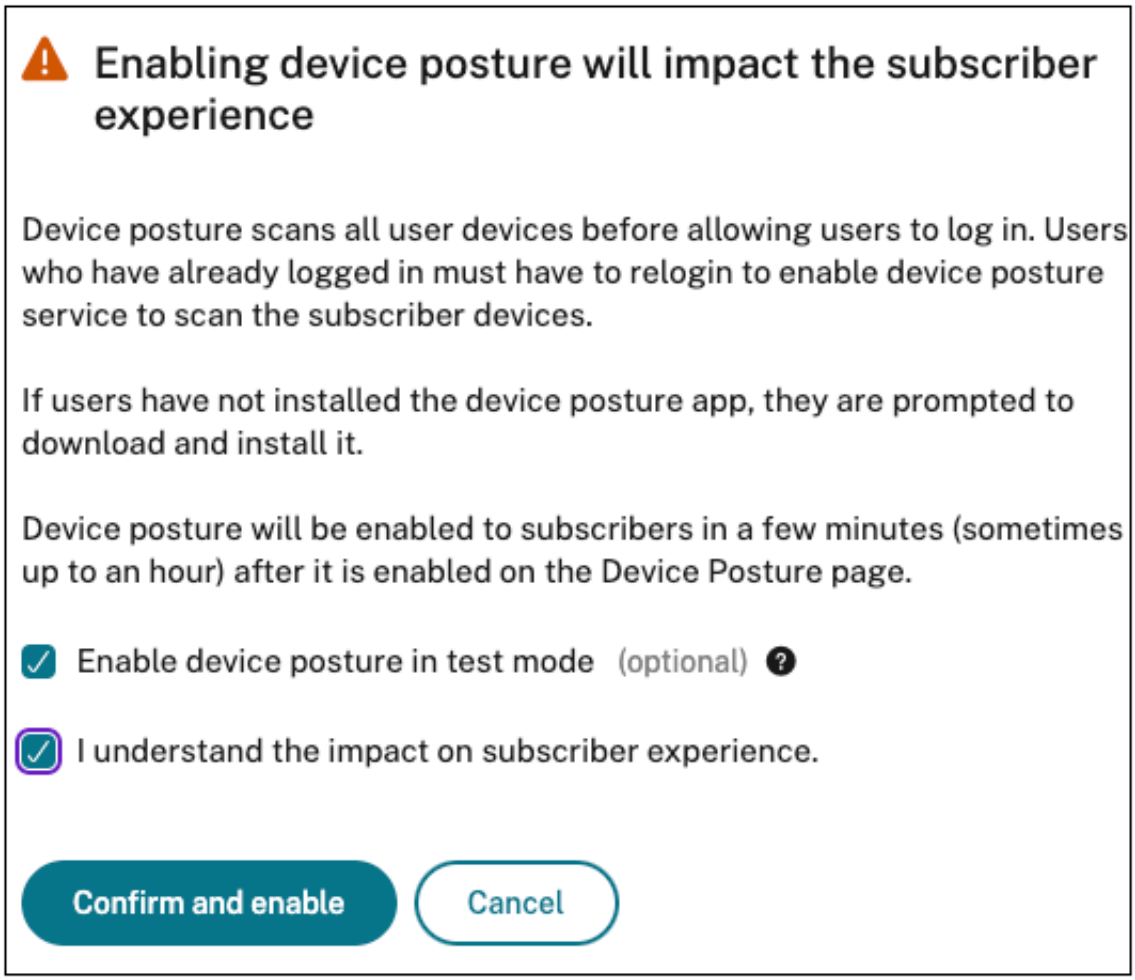
June 19, 2024

デバイスポスチャ サービスはテストモードでも利用でき、管理者は本番環境で有効にする前にデバイスポスチャサービスをテストできます。これにより、管理者はデバイスポスチャスキャンがエンドユーザーのデバイスに与える影響を分析し、本番環境で有効にする前にそれに応じてアクションプランを立てることができます。テストモードのデバイスポスチャサービスは、エンドユーザーデバイスのデータを収集し、デバイスを準拠、非準拠、拒否の 3 つのカテゴリに分類します。ただし、この分類ではエンドユーザーのデバイスに対するアクションは強制されません。代わりに、管理者が環境を評価してセキュリティを強化できるようになります。管理者はこのデータをデバイスポスチャダッシュボードで確認できます。管理者は必要に応じてテストモードを無効にすることもできます。

> 注**:**
>
> EPA クライアントをデバイスにインストールする必要があります。エンドデバイスに EPA クライアントがインストールされていない場合、デバイスポスチャ サービスはクライアントをダウンロードしてインストールするためのダウンロードページをエンドユーザーに表示します。これがないと、エンドユーザーはログオンできません。

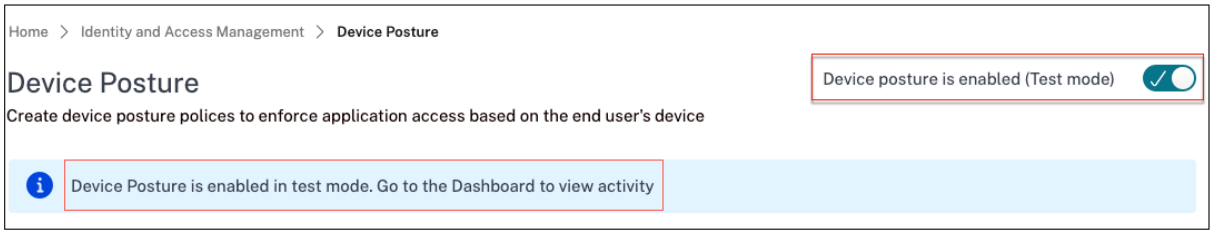
テストモードを有効にする

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. [デバイスポスチャ] タブをクリックし、[管理] をクリックします。
3. デバイスポスチャをスライドさせると無効になり、スイッチがオンになります。
4. 確認ウィンドウで、両方のチェックボックスを選択します。



5. [確認して有効にする] をクリックします。

デバイスポスチャ サービスがテストモードで有効になっている場合、デバイスポスチャ ホームページに同じことを確認するメモが表示されます。



管理者はデバイスポスチャスキャンのポリシーとルールを設定できます。詳細については、「デバイスポスチャの設定」を参照してください。スキャン結果に基づいて、エンドユーザーデバイスは準拠、非準拠、および拒否に分類されます。管理者はこのデータをダッシュボードで見ることができます。

テストモードのアクティビティをダッシュボードに表示する

1. デバイスポスチャページのダッシュボードタブをクリックします。

診断ロググラフには、準拠、非準拠、ログイン拒否に分類されたデバイスの数が表示されます。

2. 詳細を表示するには、「もっと見る」リンクをクリックします。

テストモード診断

管理者は UI から監視ログをダウンロードできます。

本番環境でテストモードを有効にする

デバイスポスチャ サービスが本番環境ですでに有効になっている場合は、次の手順を実行してテストモードを有効にします:

1. ホームページで、[デバイスポスチャが有効になっています] をスライドさせ、スイッチをオフに切り替えます。
2. [すべてのデバイスポスチャチェックが無効になることを理解しています] を選択します。
3. [確認して無効にする] をクリックします。
4. 次に、デバイスポスチャをスライドさせてデバイスポスチャを有効にします。デバイスポスチャが無効になり、スイッチがオンになります。
5. 確認ウィンドウで、次のオプションを両方選択します。
   - テストモードでデバイスポスチャを有効にする
   - サブスクライバーエクスペリエンスへの影響を理解しています
6. [確認して有効にする] をクリックします。

CrowdStrike とデバイスポスチャの統合

June 19, 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 デバイスポスチャサービスは、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。

デバイスポスチャ管理者は、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。

CrowdStrike 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。

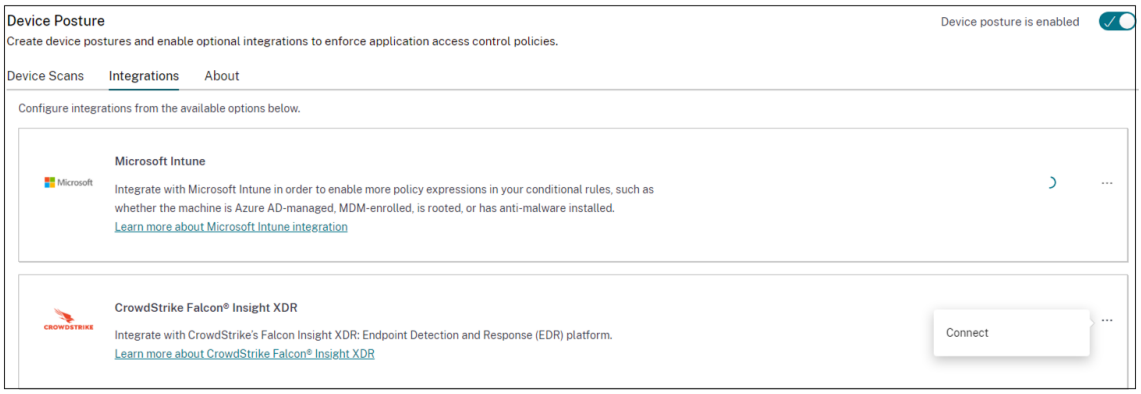
ステップ **1:** Citrix デバイスポスチャサービスと CrowdStrike ZTA サービス間の信頼を確立します。これは 1 回限りのアクティビティです。

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** デバイスポスチャサービスと **CrowdStrike ZTA** サービス間の信頼を確立する

Citrix デバイスポスチャサービスと 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. [デバイスポスチャ] 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・ペインにあるデバイスポスチャ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。

> 注記:
>
> - 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 **。

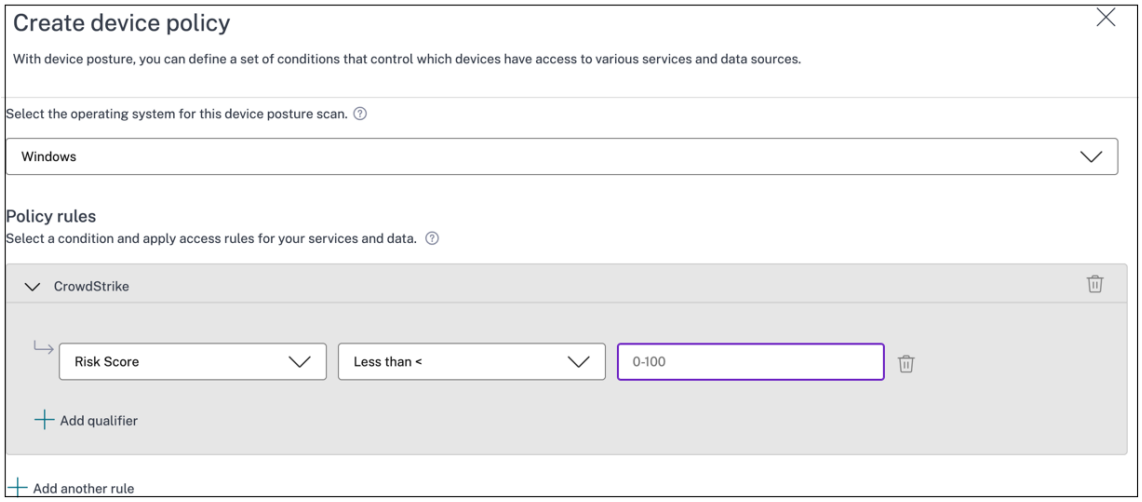
ステータスが [未構成] から [構成済み] に変わると、** 統合は成功したとみなされます **。

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:** デバイスポスチャポリシーの設定

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。

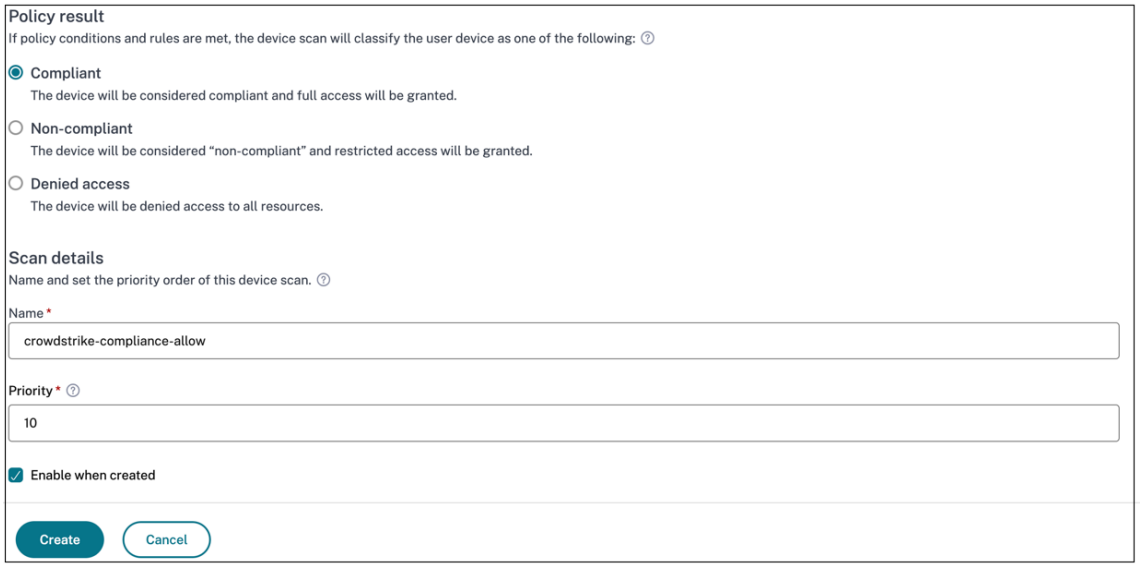
1. [デバイススキャン] タブをクリックし、[デバイスポリシーの作成] をクリックします。



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「**CrowdStrike**」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、デバイスポスチャ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. [**Create**] をクリックします。

定義

デバイスポスチャ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

デバイスポスチャサービス

Microsoft Intune とデバイスポスチャの統合

June 19, 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、デバイスポスチャ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、デバイスポスチャ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

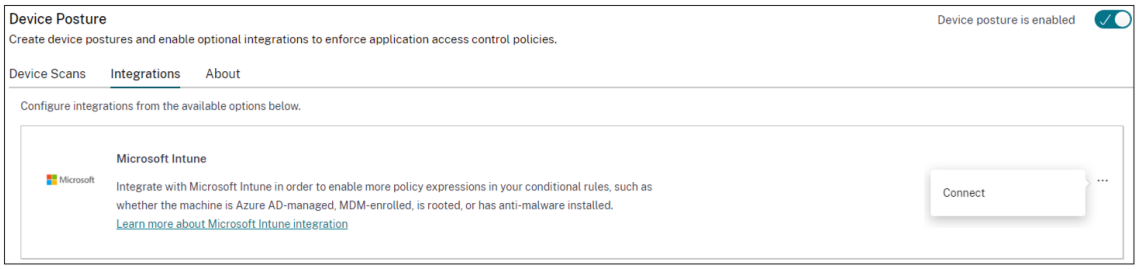
Intune 統合構成は 2 段階のプロセスです。

ステップ **1:** デバイスポスチャを Microsoft Intune サービスと統合します。これは、デバイスポスチャと 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。

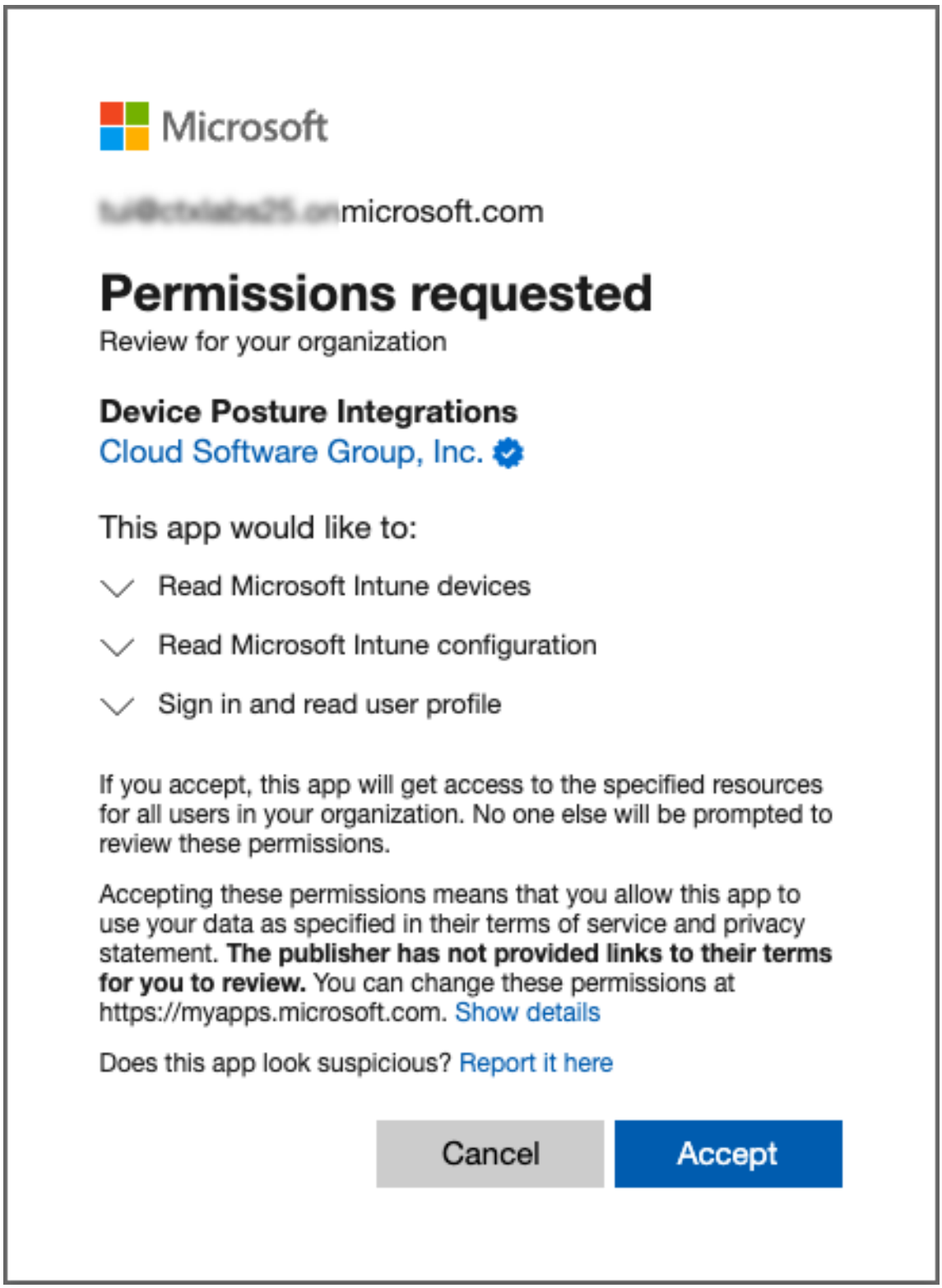
ステップ **2:** Microsoft Intune の情報を使用するようにポリシーを設定します。

ステップ **1:** デバイスポスチャを **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。



次の表は、デバイスポスチャサービスと統合するための Microsoft Intune API の権限を示しています。

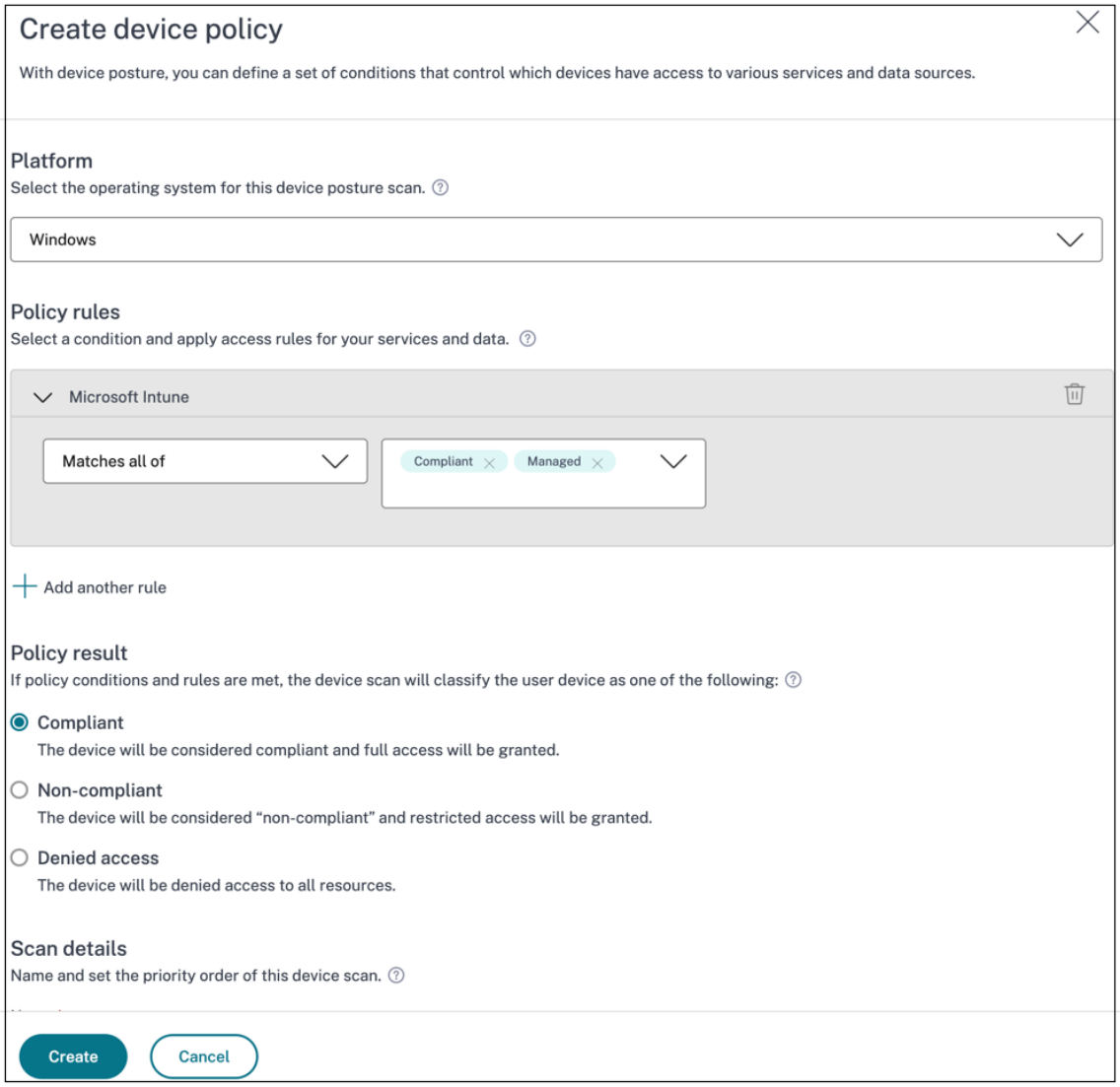
API 名	クレーム価値	権限名	種類
Microsoft Graph	DeviceManagementManagedDevices.Read.All	Microsoft Intune デバイスを読む	アプリケーション
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Microsoft Intune デバイスを読む	アプリケーション

統合ステータスが [未設定**]** から **[**** 構成済み ******] に変わったら、管理者はデバイスポスチャ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:** デバイスポスチャポリシーの設定

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、デバイスポスチャ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、「デバイスポスチャポリシーの設定」を参照してください。

デバイスポスチャサービスによるデバイス証明書チェック

June 19, 2024

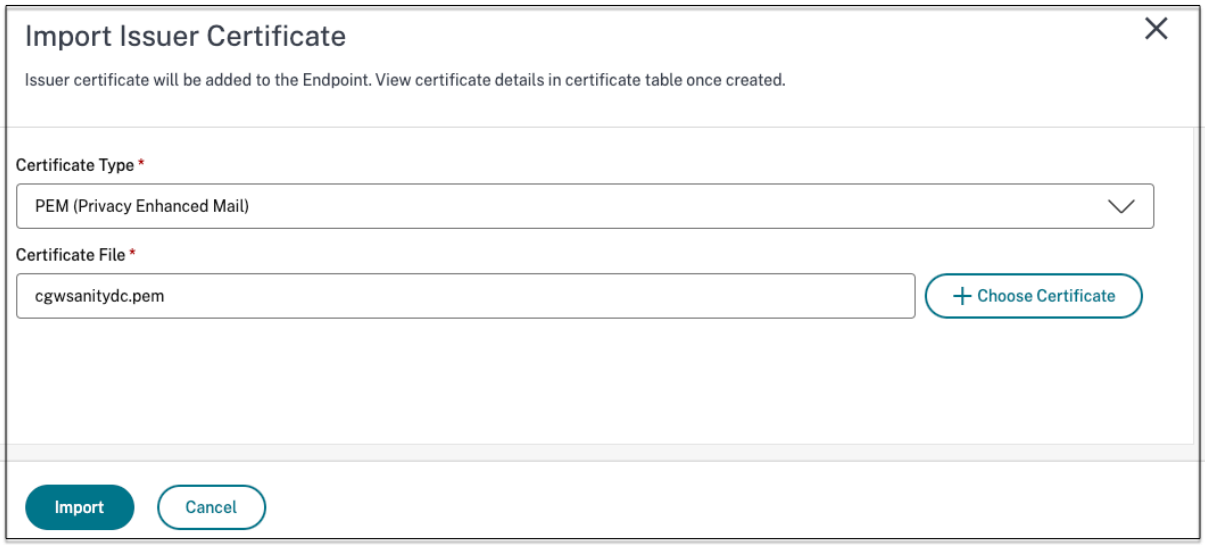
デバイスポスチャ サービスでデバイス証明書チェックを設定するには、管理者はデバイスから発行者証明書をインポートする必要があります。デバイスポスチャ サービスに有効な発行者証明書が存在すると、管理者はデバイスポスチャポリシーの一部としてデバイス証明書チェックを使用できます。

> 注意事項
>
> - デバイスポスチャサービスは 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、「デバイスポスチャ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
>   ```
>
> - デバイスポスチャ 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. デバイスポスチャのホームページで [設定] をクリックします。

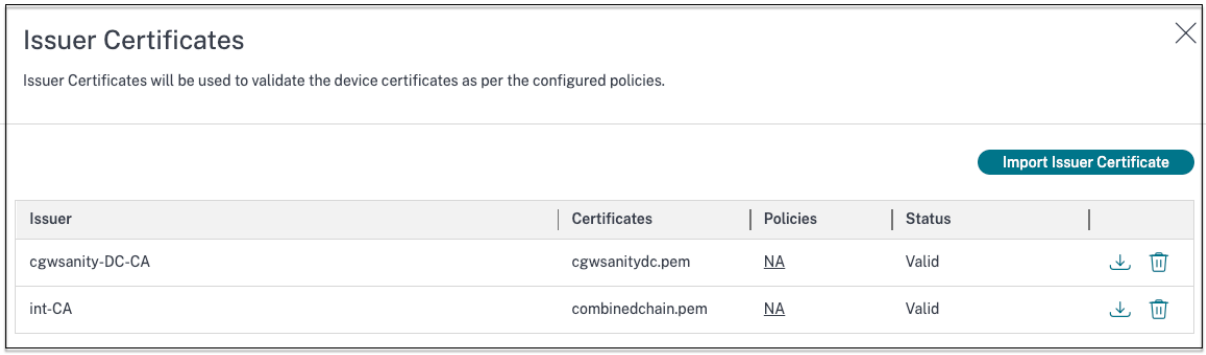
2. [管理] をクリックし、[発行証明書のインポート] をクリックします。
3. [証明書の種類] で、証明書のタイプを選択します。PEM タイプのみがサポートされます。
4. [証明書ファイル] で、**[**証明書を選択**]** をクリックして発行者証明書を選択します。
5. [開く] をクリックし、**[**インポート**]** をクリックします。



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. デバイスポスチャのホームページで [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。



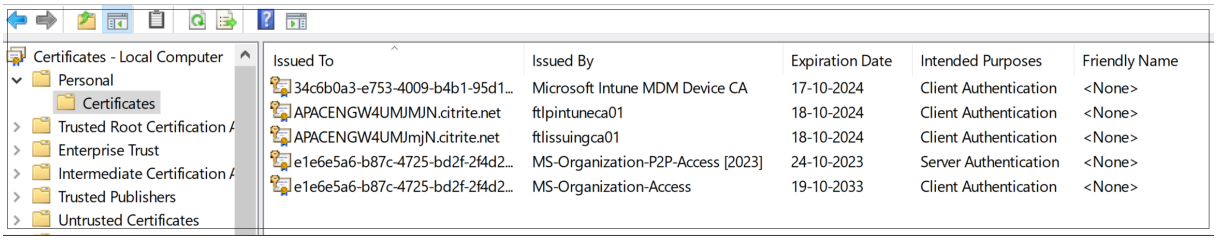
エンドデバイスにデバイス証明書をインストールします

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。

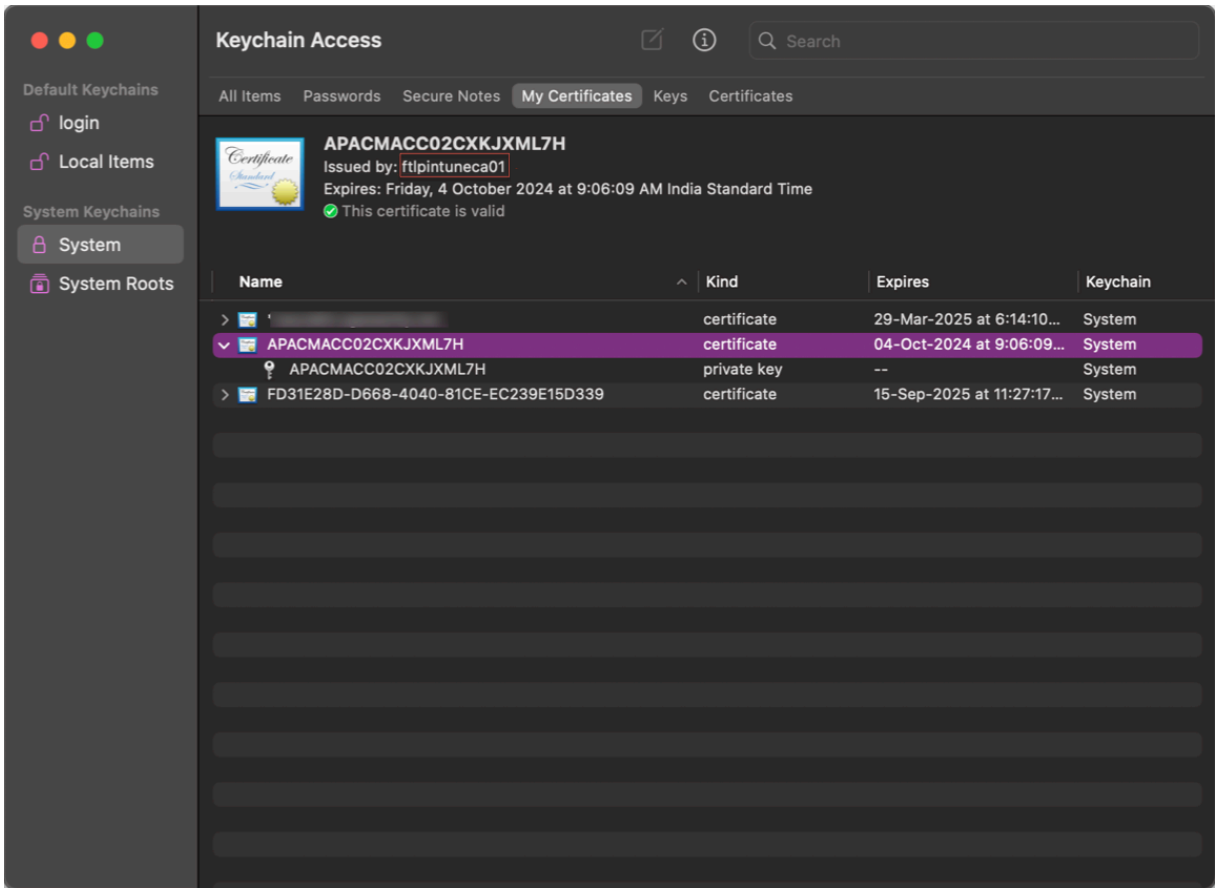
    - 意図された目的には、クライアント認証を含める必要があります。
    - 発行者列は、管理 GUI で設定された発行者名と一致する必要があります。



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

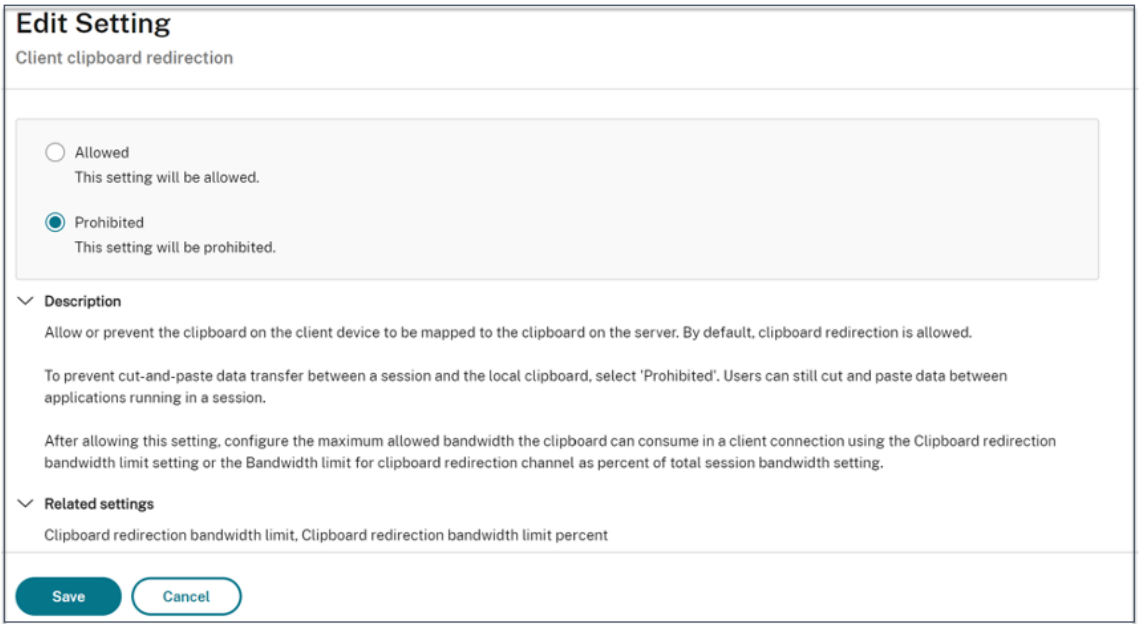
Citrix Device Posture サービスを介して Citrix Desktop as a Service（DaaS）リソースにアクセスしているときに、スマートコントロールを適用できます。

> 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。

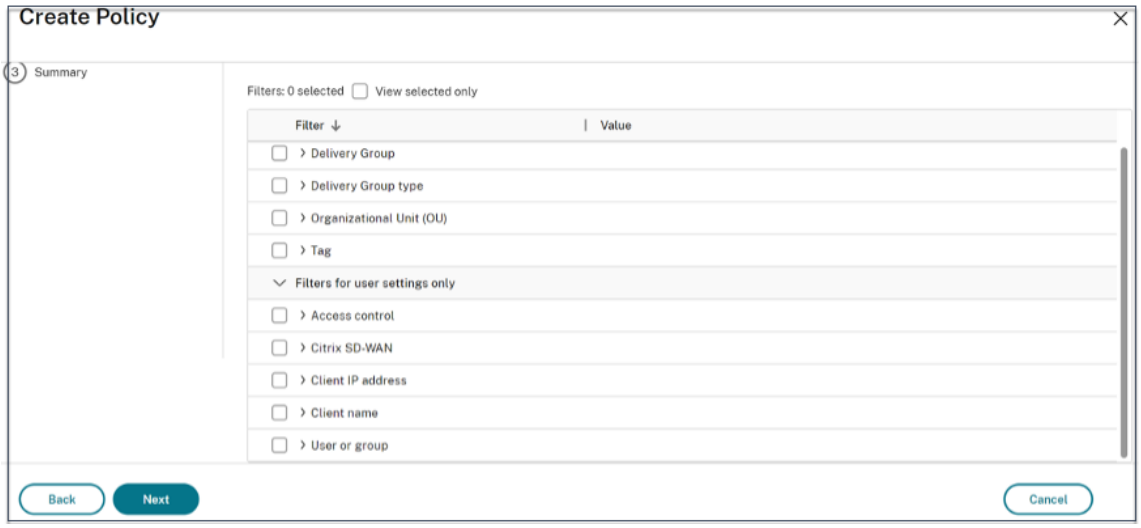
Citrix DaaS 上の非対応デバイスからアクセスするユーザーのコピー & ペースト機能を無効にするには、次の手順を実行します:

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。



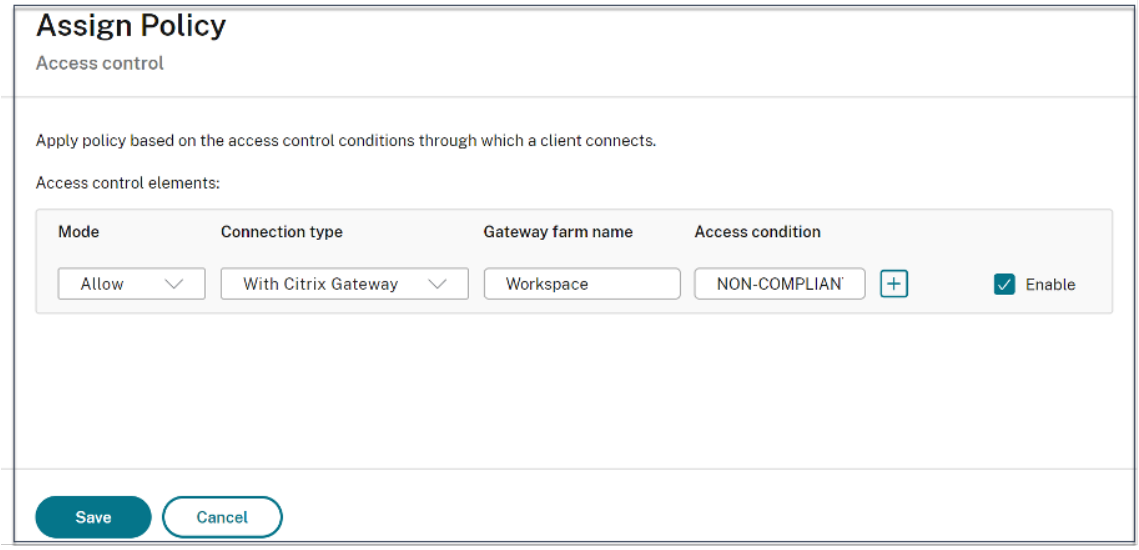
6. 「ユーザーとマシン」ページで、「フィルターされたユーザーとコンピュータ」をクリックし、このポリシーをアクセスコントロールに割り当てます。

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。

監視とトラブルシューティング

June 19, 2024

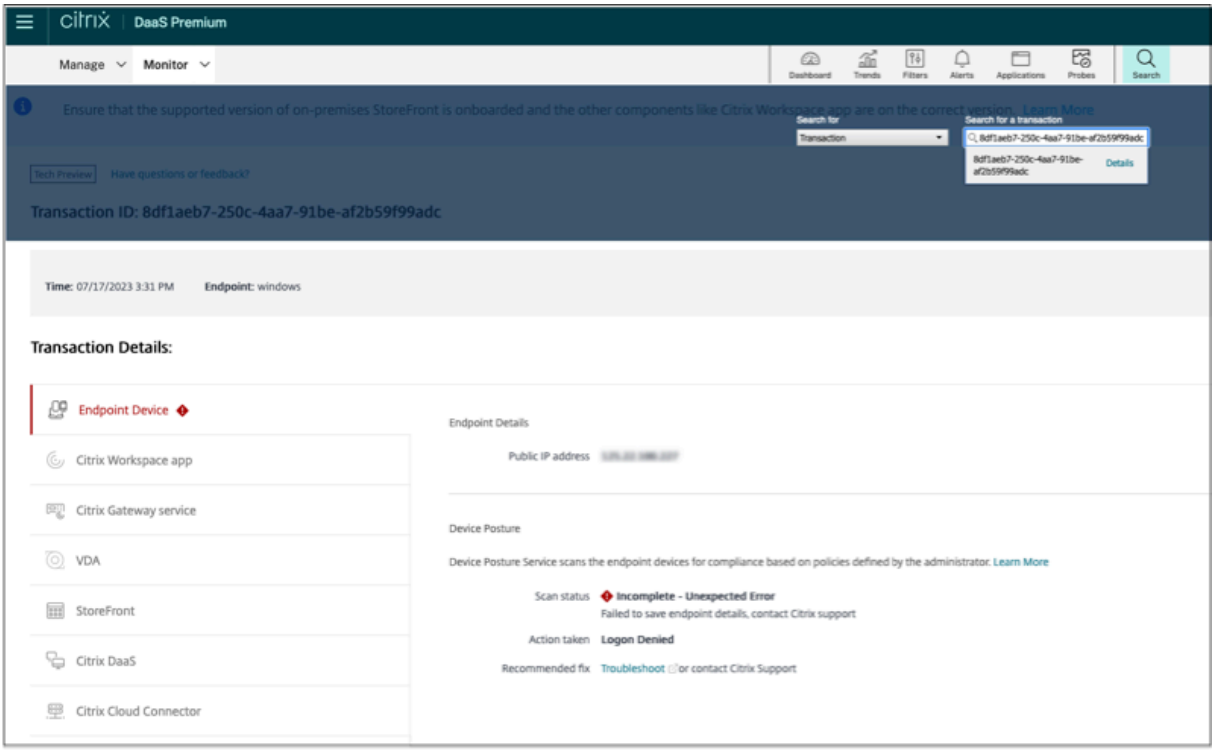
デバイスポスチャイベントログは、次の 2 つの場所で表示できます:

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

Citrix DaaS モニターのデバイスポスチャイベント

デバイスポスチャ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。

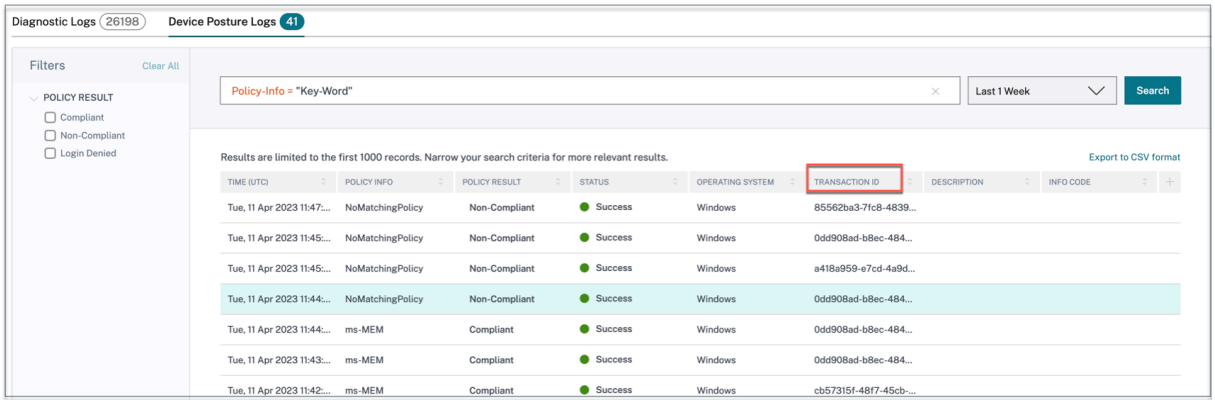
1. 失敗したセッションまたはアクセス拒否されたセッションのトランザクション ID をエンドユーザーデバイスからコピーします。
2. Citrix Cloud にサインインします。
3. DaaS タイルで **[管理]** をクリックし、**[監視]** タブをクリックします。
   モニター UI で 32 桁のトランザクション ID を検索し、［詳細］をクリックします。



Secure Private Access ダッシュボードのデバイスポスチャイベント

デバイスポスチャ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、「ダッシュボード」をクリックします。
3. 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、デバイスポスチャ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、デバイスポスチャ 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

デバイスポスチャのエラーログ

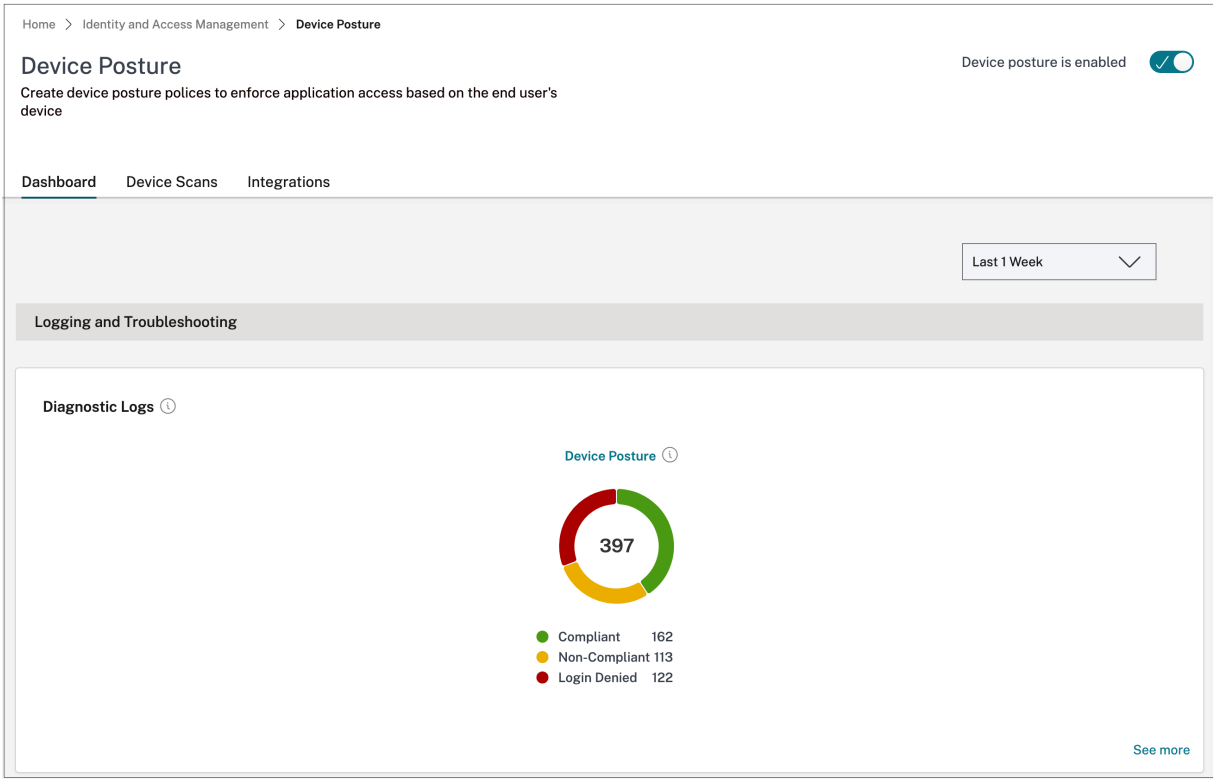
デバイスポスチャサービスに関連する以下のログは、Citrix Monitor と Secure Private Access ダッシュボードで表示できます。これらすべてのログについては、Citrix サポートに連絡して解決してもらうことをお勧めします。

- 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

デバイスポスチャログ

June 19, 2024

デバイスポスチャ サービスポータルのダッシュボードは、モニタリングやトラブルシューティングに使用できます。デバイスポスチャサービスダッシュボードを表示するには、デバイスポスチャホームページの「ダッシュボード」タブをクリックします。ロギングとトラブルシューティングセクションには、デバイスポスチャ サービスに関連する診断ログが表示されます。[**See more**] リンクをクリックすると、ログの詳細を表示できます。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。



> 注:
>
> デバイスポスチャログは、Secure Private Access サービスのダッシュボードにもキャプチャされます。デバイスポスチャログを表示するには、[デバイスポスチャログ（デバイスポスチャ **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。

デバイスポスチャサービス用 **Citrix Endpoint Analysis** クライアントの管理

June 19, 2024

Citrix デバイスポスチャサービスは、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。

エンドデバイスでデバイスポスチャ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。デバイスポスチャサービスは、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、デバイスポスチャ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。管理者アクセス権で 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 デバイスポスチャ 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プレビュー段階です。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** クライアントインストーラー： EPA クライアントインストーラーは、Windows 向け Citrix Workspace アプリ 2402 LTSR と統合されています。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 クライアントを個別にインストールする必要がなくなります。

  EPA クライアントを Citrix Workspace アプリの一部としてインストールするには、コマンドラインオプション`InstallEPAClient`を使用します。例: `./CitrixworkspaceApp.exe InstallEPAClient`。

  > 注記:
  >
  > - Citrix Workspace アプリの一部としての EPA クライアントのインストールは、デフォルトで無効になっています。コマンドラインオプション`InstallEPAClient`を使用して明示的に有効にする必要があります。
  > - 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すると、既存の EPA クライアントがアップグレードされます。

  - 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。
  - Citrix Workspace アプリと統合されている EPA クライアントインストーラーは、NetScaler でも使用できます。詳しくは、「NetScaler と併用した場合の EPA クライアントの管理」および「デバイスポスチャ」を参照してください。

- **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 の詳細については、「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。

> 注記:
>
> - 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 およびデバイスポスチャと併用する場合の EPA クライアントの管理

EPA クライアントは、次の展開で NetScaler およびデバイスポスチャと併用できます。

- 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

デバイスポスチャサービスは、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 およびデバイスポスチャと併用する場合の考慮事項

EPA クライアントをデバイスポスチャサービスおよび 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 またはデバイスポスチャ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**:**

```
1 add rewrite action <rewrite_action_name> insert_http_header Plugin-
    Upgrade ""epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:
    Never;vpn_mac:Always;vpn_linux:Always;""
2
3 add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("
    pluginlist.xml")" <rewrite_action_name>
4
5 bind authentication vserver <Authentication_Vserver_Name> -policy <
    rewrite_action_policy> -priority 10 -type RESPONSE
6 <!--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。