Device Posture

Machine translated content

Disclaimer

Contents

新機能

October 21, 2024

29 May 2024

- テストモードでのデバイス姿勢サービスの可用性

  デバイス ポスチャ サービスはテスト モードでも利用可能で、管理者はデバイス ポスチャ サービスを本番環境で有効にする前にテストできます。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、実稼働環境で有効にする前にそれに応じてアクションを計画できるようになります。詳細については、テスト モードのデバイス ポスチャ サービスを参照してください。

- ** デバイスの定期スキャン

  設定されたチェックに対して、30 分ごとに Windows デバイスの定期的なスキャンを有効にできるようになりました。詳細については、「デバイスの定期的なスキャン」を参照してください。

14 May 2024

- デバイスの姿勢チェックをスキップする

  管理者は、エンドユーザーがデバイス上のデバイス 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、「デバイスの状態チェックをスキップする」を参照してください。

- デバイス姿勢ダッシュボード

  デバイス ポスチャ サービス ポータルに、ログの監視とトラブルシューティングを行うためのダッシュボードが追加されました。管理者は、監視とトラブルシューティングの目的でこのダッシュボードを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

  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、「デバイス姿勢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

  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されたメッセージ」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

デバイス ポスチャ サービスでカスタム ワークスペース URL が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 URL に加えて、自分が所有する 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 ドメインを構成する」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 サービスでは、ブラウザーとウイルス対策のチェックがサポートされるようになりました。詳細については、「デバイス姿勢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開始

  Device Posture サービスによるデバイス証明書チェックが一般提供されました。詳細については、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 サービスでは、次のチェックが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 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 サービスでは、地理位置情報とネットワーク ロケーションのチェックがサポートされるようになりました。

  詳細については、「デバイスの状態」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提供開始

  Microsoft Intune とのデバイス ポスチャ統合が一般提供されました。詳細については、「Microsoft Intune と Device Posture 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 サービス用の **Citrix** エンドポイント分析クライアントを管理する

  EPA クライアントは、NetScaler および Device Posture と併用できます。NetScaler および Device Posture 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構成変更が必要です。詳細については、「Citrix Endpoint Analysis Client for Device Posture サービスの管理」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。詳細については、「デバイスの状態」を参照してください。

2023 年 8 月 22 日

- **Citrix Device Posture** サービスによるデバイス証明書のチェック - プレビュー

  Citrix Device Posture サービスでは、エンド デバイスの証明書を企業の証明機関と照合してエンド デバイスが信頼できるかどうかを判断することにより、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) を有効にできるようになりました。詳細については、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が DaaS モニターで検索できるようになりました。詳細については、「Citrix DaaS Monitor 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

- デバイス姿勢サービス

  Citrix Device Posture サービスは、Citrix DaaS (仮想アプリとデスクトップ) または Citrix Secure Private Access リソース (SaaS、Web アプリ、TCP、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がある特定の要件を管理者が強制するのに役立つクラウド ベースのソリューションです。詳細については、「デバイスの状態」を参照してください。

  [AAUTH-90]

- **Microsoft Endpoint Manager** と **Device Posture** 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。Device Posture は、Windows および macOS 上の Microsoft Endpoint Manager (MEM) と統合されています。詳細については、「Microsoft Endpoint Manager と Device Posture 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姿勢サービス

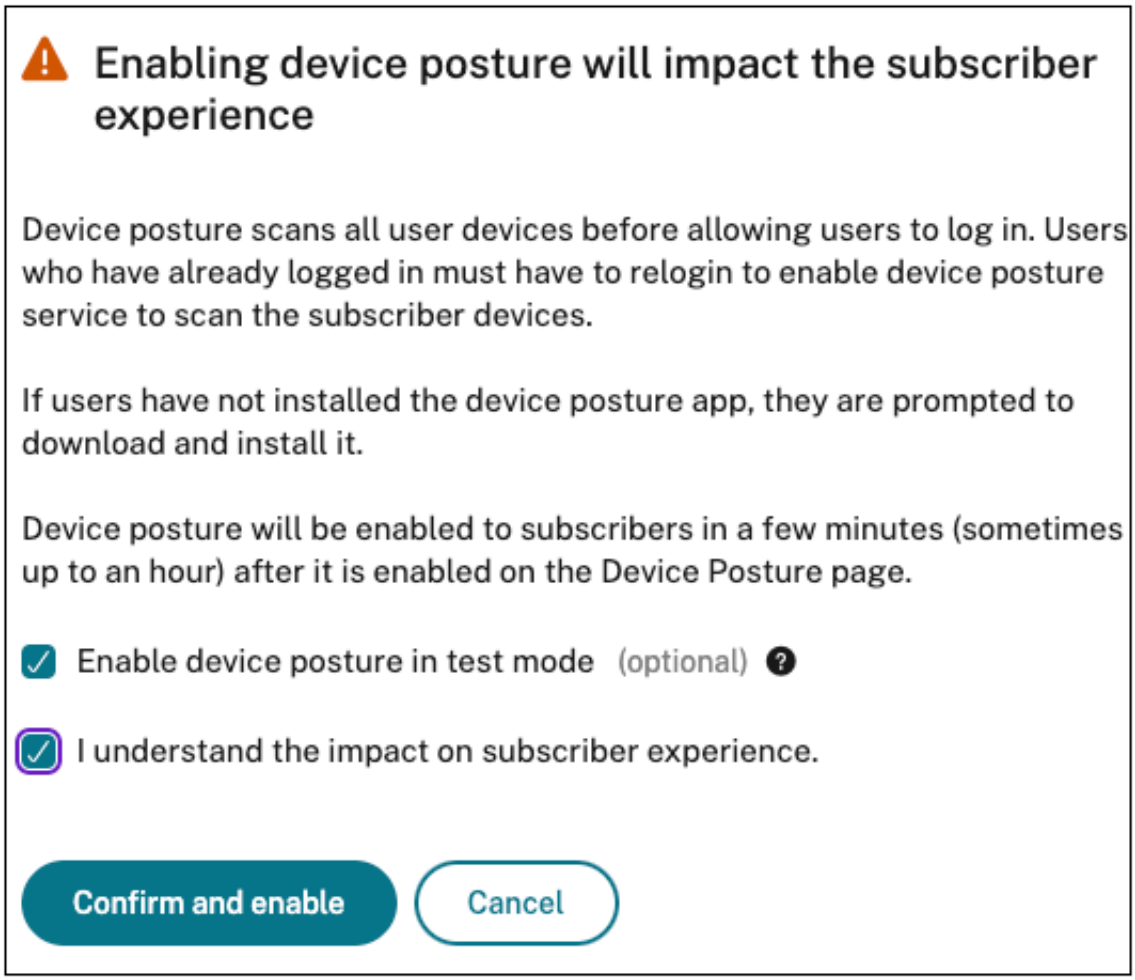
October 21, 2024

デバイス ポスチャ サービスはテスト モードでも利用可能で、管理者はデバイス ポスチャ サービスを本番環境で有効にする前にテストできます。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、実稼働環境で有効にする前にそれに応じてアクションを計画できるようになります。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して何らかのアクションが強制されるわけではありません。代わりに、管理者が環境を評価し、セキュリティを強化できるようになります。管理者は、デバイス ポスチャ ダッシュボードでこのデータを表示できます。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。

> 注意**:**
>
> 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 サービスはエンド ユーザーに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 ページを提示します。クライアントがないと、エンド ユーザーはログオンできません。

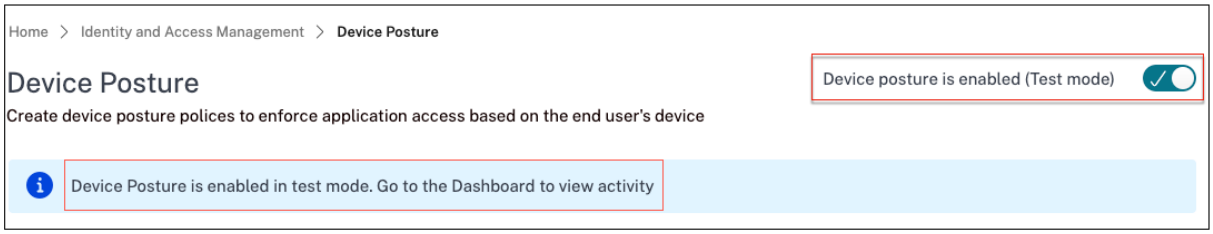
テストモードを有効にする

1. Citrix Cloud にサインインし、ハンバーガー メニューから **Identity and Access Management** を選択します。
2. **[**デバイスの状態] タブをクリックし、次に **[**管理] をクリックします。
3. デバイスの姿勢が無効になります トグル スイッチをオンにスライドします。
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. をクリックして確認し、を有効にします。

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 ポスチャのホームページにそのことを確認するメモが表示されます。



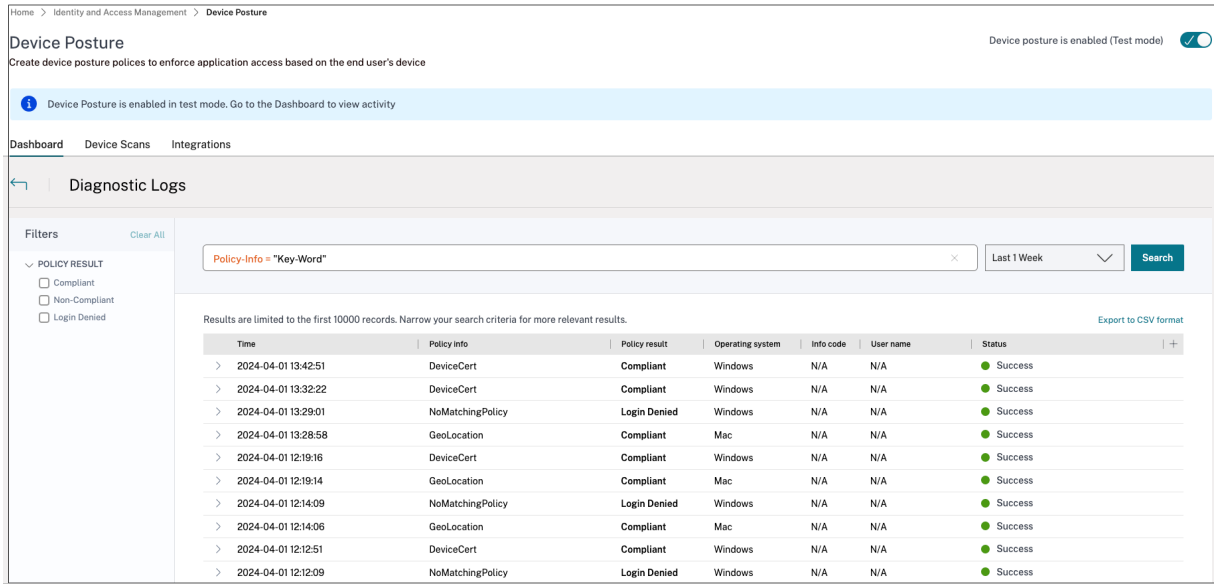
管理者は、デバイスの姿勢スキャンのポリシーとルールを設定できます。詳細については、「デバイスの状態を構成する」を参照してください。スキャン結果に基づいて、エンドユーザー デバイスは準拠、非準拠、拒否に分類されます。管理者はダッシュボードでこのデータを表示できます。

ダッシュボードでテストモードのアクティビティを表示する

1. [デバイス ポスチャ] ページで、[ダッシュボード] タブをクリックします。

診断ログ チャートには、準拠、非準拠、ログイン拒否として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てください。



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 サービスがすでに本番環境で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、デバイス姿勢が有効 トグルスイッチをオフにスライドします。
2. すべてのデバイス姿勢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. をクリックして確認し、を無効にします。
4. 次に、デバイスの姿勢が無効 トグル スイッチをオンにスライドして、デバイスの姿勢を有効にします。
5. 確認ウィンドウで、次の両方のオプションを選択します。
   - テストモードでデバイスの姿勢を有効にする
   - 加入者体験への影響を理解している
6. をクリックして確認し、を有効にします。

テストモードから本番環境への移行

テスト モードから本番環境に移行するには、まずテスト モードでデバイス ポスチャを無効にし、次にオプション テスト モードでデバイス ポスチャを有効にするを選択せずにデバイス ポスチャを再度有効にする必要があります。

> 重要:
>
> - テスト モードから本番環境に移行する前に、ポリシーを徹底的に確認することが重要です。テスト モードで設定されたポリシーは、運用環境で適用された場合に異なる動作をする可能性があり、特にユーザー アクセスに影響を及ぼす可能性があります アクセス拒否。テスト モードでは、アクセス拒否 は事実上 非準拠として扱われ、ユーザーは中断することなくシステムにアクセスし続けることができます。ただし、本番環境では、この結果によりアクセスが直接ブロックされ、ユーザー エクスペリエンスと操作に影響する可能性があります。
> - また、テスト モードから本番環境に移行する際には、ダウンタイムが発生する可能性があります。混乱を最小限に抑えるために、移行を慎重に計画することをお勧めします。

監視とトラブルシューティング

June 19, 2024

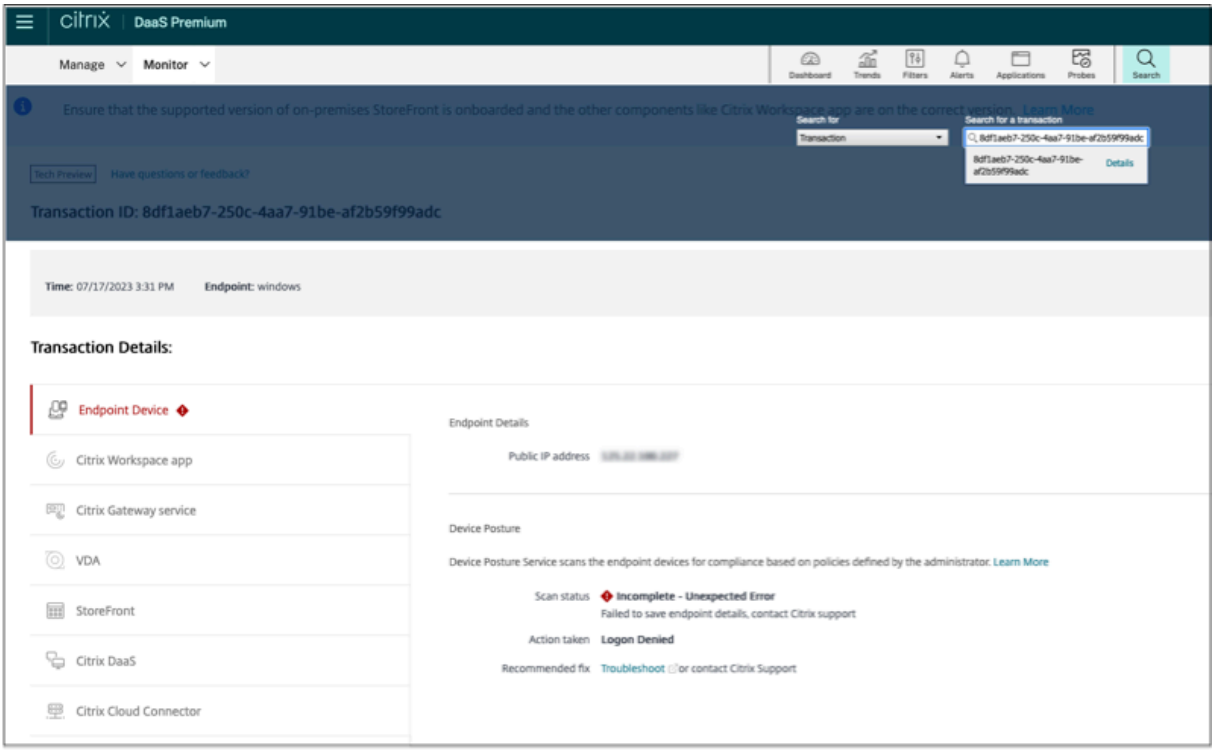
デバイスポスチャイベントログは、次の 2 つの場所で表示できます:

- 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。

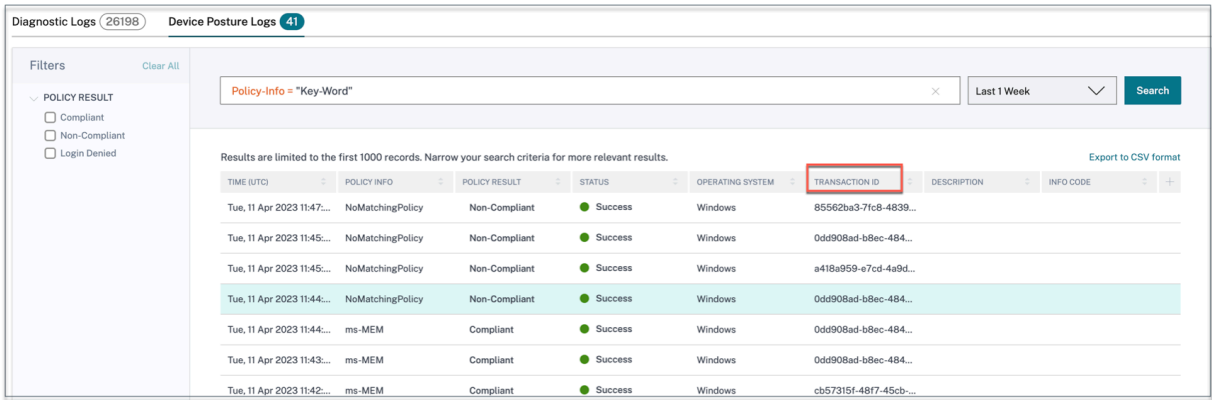
1. 失敗したセッションまたはアクセス拒否されたセッションのトランザクション ID をエンドユーザーデバイスからコピーします。
2. Citrix Cloud にサインインします。
3. DaaS タイルで **[管理]** をクリックし、**[監視]** タブをクリックします。
   モニター UI で 32 桁のトランザクション ID を検索し、［詳細］をクリックします。



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

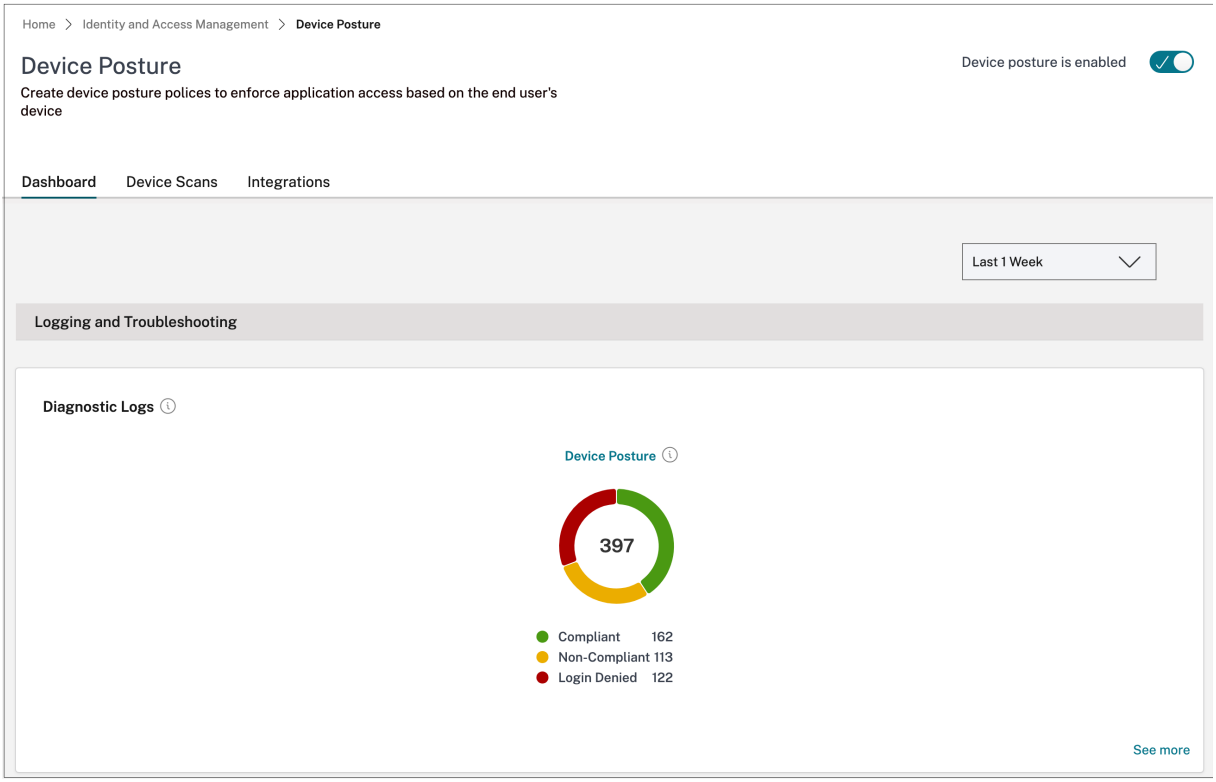
デバイスポスチャサービスに関連する以下のログは、Citrix Monitor と Secure Private Access ダッシュボードで表示できます。これらすべてのログについては、Citrix サポートに連絡して解決してもらうことをお勧めします。

- 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 サービス用の **Citrix** エンドポイント分析クライアントを管理する

October 21, 2024

Citrix Device Posture サービスは、Citrix DaaS (仮想アプリとデスクトップ) または Citrix Secure Private Access リソース (SaaS、Web アプリ、TCP、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がある特定の要件を管理者が強制するのに役立つクラウド 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、Citrix がリリースした EPA クライアントの最新バージョンで常に実行されます。

EPA クライアントのインストール

実行時に、デバイス ポスチャ サービスは、エンド ユーザーに実行時に 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要求します。詳細については、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には、ローカル管理者権限は必要ありません。ただし、エンド デバイスでデバイス証明書チェック スキャンを実行するには、EPA クライアントを管理者アクセス権でインストールする必要があります。管理者アクセス権を持つ EPA クライアントのインストールの詳細については、「エンドデバイスにデバイス証明書をインストールする」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 用の 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、エンドユーザーのデバイスは常に、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実行されるようになります。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アクセス権でインストールされている必要があります。

EPA クライアントの配布

EPA クライアントは、Global App Configuration サービス (GACS) または Citrix Workspace アプリ インストーラーに統合された EPA、あるい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。

  Citrix Workspace アプリの一部として EPA クライアントを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。たとえば、`./CitrixworkspaceApp.exe InstallEPAClient`です。

> 注意**:**
>
> - 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、デフォルトでは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 EPA クライアントがすでにインストールされており、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 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なかった場合、既存の EPA クライアントはデバイスに保持されます。

> - Citrix Workspace アプリに統合された EPA クライアント インストーラーは、NetScaler でも使用できます。詳細については、「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」を参照してください。

- **GACS** を使用してクライアントを配布します: GACS は、クライアント側エージェント (プラグイン) の配布を管理するために Citrix が提供する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 バージョンに保たれます。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。

> 注意:
>
> - GACS は、EPA クライアントの配布用に Windows デバイスでのみサポートされます。
> - GACS を介して EPA クライアントを管理するには、エンド デバイスに Citrix Workspace Application (CWA) をインストールします。
> - CWA がエンド ユーザーのデバイスに管理者権限でインストールされる場合、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 デバイスにユーザー権限でインストールされる場合、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する: 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 と一緒に使用できます。

- EPA を使用した NetScaler ベースの適応型認証
- EPA を備えた 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上の 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: エンドデバイスと NetScaler 上の EPA クライアントは同じバージョンである必要があります。
- 必須: エンドデバイス上の EPA クライアント バージョンは、NetScaler で構成された範囲内である必要があります。
- なし: エンドデバイスには、EPA クライアントの任意のバージョンを含めることができます。

詳細については、「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 ポスチャで使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 と一緒に使用する場合、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、NetScaler では異なるバージョンの EPA クライアントが実

行されるというシナリオが発生する可能性があります。これにより、NetScaler とエンド デバイスの EPA クライアント 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 はエンドユーザーに対して、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要求する場合があります。この競合を回避するには、次の構成変更をお勧めします。

- EPA を Adaptive Authentication または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 上の 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 EPA クライアントの最新バージョンをエンド デバイスにプッシュしないようにするために行われます。
- EPA バージョン コントロールは、CLI または GUI を使用して **Never** 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ています。
  - CLI: Adaptive Authentication およびオンプレミス認証仮想サーバーの CLI コマンドを使用します。
  - GUI: オンプレミス ゲートウェイ仮想サーバーの GUI を使用します。詳細については、「Citrix Secure Access クライアントのアップグレードの制御」を参照してください。

サンプル **CLI** コマンド**:**

```
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
```

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。