

デバイスポスチャ

Contents

デバイスポスチャの概要	9
前提条件	9
定義	11
仕組み	11
Device Postureサービスでサポートされているスキャン	13
Windows Update 最終更新チェック	14
Device Postureサービスとのサードパーティ統合	15
既知の制限事項	16
サービス品質	16
クローム エンタープライズ プレミアムとの統合	16
新機能	18
09 September 2026	18
22 June 2026	18
15 June 2026	18
05 June 2026	18
01 June 2026	19
09 April 2026	20
17 March 2026	20
21 January 2026	21
26 September 2025	21
09 July 2025	22
21 Feb 2025	23
04 Dec 2024	24
29 May 2024	24
14 May 2024	25
26 March 2024	25

12 February 2024	26
23 January 2024	26
11 September 2023	26
30 August 2023	26
28 August 2023	27
22 August 2023	27
17 August 2023	27
23 January 2023	27
エンドポイント分析リリースノート	28
V26.07.20 for macOS (18 September 2026)	28
V26.7.1.15 for Windows (11 September 2026)	28
新機能	28
修正された問題	32
V26.6.1.4 for Windows (24 August 2026)	33
新機能	33
修正された問題	33
V26.5.1.7 for Windows (08 Jul 2026)	34
修正された問題	34
V26.03.31 for macOS (14 May 2026)	34
新機能	34
デバイスポスチャポリシーを構成する	36
デバイスポスチャを使用してコンテキストアクセス（スマートアクセス）を構成する	38
デバイスポスチャによるCitrix DaaSの構成	38
デバイスポスチャを使用したCitrix Secure Private Access の構成	41
デバイスポスチャポリシーを編集する	42
デバイスポスチャのグローバル設定を構成する	43
イベント駆動型ポスチャチェックによるデバイスコンプライアンス	43
デバイスの定期スキャン	45

アクセス拒否のシナリオ向けカスタマイズメッセージ	46
デバイスポスチャチェックをスキップする	47
デバイスポスチャチェックのスキップを有効にする	48
カスタムワークスペースURLのサポート	49
Device Postureによるセッションレコーディングの構成	49
デバイス証明書チェック	49
デバイス証明書のアップロード	50
インポートされた証明書の表示	51
デバイス証明書チェックのスキャンを設定する	51
エンドデバイスにデバイス証明書をインストールする	52
許可されたドメインのリストを構成する	52
Device Posture サービスと Chrome Enterprise デバイス信頼コネクタの統合	54
サポートされるプラットフォームと展開	54
前提条件	55
構成	55
Chrome Enterprise Premium と Device Posture サービスを構成する	55
Citrix Device Posture サービスを Chrome デバイス信頼コネクタと統合する	55
Citrixシグナル用のコンテキストアウェアなルールを定義する	57
Citrixシグナルキー	57
Citrix 向け 共通式言語 (CEL) の例	58
ルールを適用するには	60
統合を検証する	60
トラブルシューティング	61
トラブルシューティングのための Citrix-DeviceId と Citrix-TransactionId の使用	61
制限事項	62
Device Postureサービスとのサードパーティ統合	63
Microsoft Entra IDとDevice Postureサービスの統合	63
システム要件	63

マイクロソフト Entra ID API 権限	63
Entra ID連携を構成する	64
Citrix Device PostureサービスとMicrosoft Entra ID間の信頼を確立する	64
Microsoft Entra ID連携のためのデバイスポスチャポリシーを構成する	65
Jamf Proとデバイスポスチャサービスの連携	66
Jamf Pro連携を構成する	66
Citrix Device PostureサービスとJamf Proサービス間の信頼を確立する	66
Jamf Pro統合のデバイスポスチャポリシーを構成する	68
Jamf ProポータルからiOSデバイスにCitrix Workspaceアプリをプッシュする	68
Microsoft IntuneとDevice Postureサービスの統合	69
複数のMicrosoft IntuneアカウントとDevice Postureの統合	69
Microsoft Intune統合を構成する	70
デバイスポスチャをMicrosoft Intuneと統合する	70
複数のMicrosoft IntuneアカウントをDevice Postureと統合する	71
Microsoft Intune API の権限	73
Intune 統合のためのデバイスポスチャポリシーを構成する	74
CrowdStrike と Device Posture サービスの統合	74
CrowdStrike 統合を構成する	74
Citrix Device PostureサービスとCrowdStrike ZTAサービス間の信頼を確立する	75
CrowdStrike統合のデバイスポスチャポリシーを構成する	76
サードパーティ統合障害通知	76
ユースケース	77
前提条件	78
デバイスポスチャサービス管理コンソールで通知を設定する	78
エンドユーザーフロー	79
ブラウザアクセスによるエンドユーザーフロー	79
Citrix Workspaceアプリケーションによるエンドユーザーフロー	80
エンドユーザーフロー - デバイスポスチャの結果	80

テストモードでのデバイスポスチャサービス	82
テストモードを有効にする	82
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	83
本番環境でテストモードを有効にする	84
テストモードから本番環境への移行	84
Citrix Secure Access Endpoint Analysis (EPA) クライアントバージョンを、サポートされる最小バージョンを設定して管理する	86
仕組み	86
EPAクライアントのバージョン管理オプションを設定する	88
EPAクライアントの配布とバージョン管理に関する考慮事項	89
複数のクラウドストアのサポート	90
重要な考慮事項	90
前提条件	91
ストアURLを構成する	91
Device Posture ユーザーイベントの SIEM システムへのエクスポート	94
DaaS Monitor を使用したデバイスポスチャの問題のトラブルシューティング	95
Citrix DaaS™ Monitorでのデバイスポスチャイベント	95
デバイスポスチャのログとイベント	97
Identity and Access Managementコンソールのデバイスポスチャダッシュボード	97
ログの場所	99
Secure Private Accessダッシュボード	99
デバイスポスチャのエラーログ	100
デバイスポスチャデータの書き出し	100
デバイスポスチャサービス トランザクションの診断	100
デバイスポスチャサービス評価フローの理解	101
Citrix Monitorにおけるトラブルシューティングの強化	101
ITチームがトラブルシューティングの強化をどのように活用できるか	101
デバイスポスチャの問題のトリアージ	102

ポリシーベースのアクセスブロックの調査	102
精密検索による大規模なポリシーセットのデバッグ	103
トランザクションの失敗とエラーの処理	104
Device Postureサービス取引を診断する手順	105
トランザクションの概要	106
設定済みポリシーの検証	106
エラーコード	107
Citrix Secure Access Endpoint Analysis (EPA) クライアントの配布とアップグレード	109
Citrix Secure Access Endpoint Analysis (EPA) クライアントの配布およびアップグレード方法	109
詳細な構成手順	114
Citrix Workspaceアプリリリースにバンドルされています	114
Citrix Workspaceアプリの自動更新（クライアントアプリ管理）	115
SCCM、Intune、Jamf、またはその他のエンドポイント管理ツールを使用してインストーラーをプッシュする	115
デバイスポスチャサービスコンソールで最小EPAクライアントバージョンを設定する	116
プラグインをNetScaler Gatewayポータルにアップロードする	117
EPAクライアントをNetScalerおよびDevice Postureサービスと併用する場合の考慮事項	117
Device PostureサービスとdeviceTRUST - より良い連携	119
Device PostureサービスとdeviceTRUSTの連携方法	120
認証前: ログイン前の信頼確立	120
列挙: アプリケーションへのコンテキストに応じたアクセス	121
セッション中: 継続的なコンテキストに応じたアクセス評価	122
Device PostureサービスとdeviceTRUST連携のユースケース	122
バージョンコンプライアンス	123
ジオフェンシング	123
デバイスのセキュリティ状態の監視	123
データガバナンス	124
データレジデンシー	124

データ収集	125
データ送信	125
データ制御	125
データ保持	126
データエクスポート	126
定義	126

デバイスポスチャの概要

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

前提条件

- ライセンス要件: Device Postureサービスは、Universal Hybrid Multi Cloud License (UHMC) およびPlatform License (CPL) の一部として利用可能です。詳細については、「[ライセンス](#)」を参照してください。
- サポートされているプラットフォーム:
 - Windows (10 および 11)
 - macOS 26 タホ
 - macOS 15 セコイア
 - macOS 14 ソノマ
 - iOS
 - Linux (Ubuntu 22.04/24.04 および eLux 7)

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、デフォルトで非準拠としてマークされます。分類は、Device Postureページの**設定**タブから**非準拠**から**ログイン拒否**に変更できます。「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。
 - 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、事前定義されたデバイスポスチャポリシーのいずれにも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。分類は、Device Postureページの**設定**タブから**非準拠**から**ログイン拒否**に変更できます。
 - iOSでのDevice Postureサービスのサポートについては、EPAクライアントはCitrix Workspaceアプリ for iOSの一部として組み込まれています。バージョンに関する詳細については、「[Citrix Workspaceアプリ for iOS](#)」を参照してください。
- Citrix Device Postureクライアント (EPAクライアント): デバイスポスチャスキャンを実行するために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です。このアプリケーションは、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を必要としません。

注:

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

- サポートされているブラウザ: Chrome、Edge、Firefox。
- ファイアウォールの構成: Device Postureサービスを使用するには、ファイアウォールまたはプロキシが以下のドメインを許可するように構成されていることを確認してください。
 - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
 - `https://productioniconstorage.blob.core.windows.net`
 - `*.netscalergateway.net`
 - `*.nssvc.net`
 - `*.cloud.com`
 - `*.pendo.io`

- *.citrix.com
- *.citrixworkspacesapi.net

定義

Device Postureサービスにおける「準拠 (compliant)」および「非準拠 (non-compliant)」という用語は、次のように定義されます。

- **準拠デバイス** – 事前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リソースへの完全または無制限のアクセス権を持って会社のネットワークにログインすることを許可されているデバイス。
- **非準拠デバイス** - 事前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権を持って会社のネットワークにログインすることを許可されているデバイス。

仕組み

管理者は、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が許可されるか拒否されるかを判断するために、デバイスポスチャポリシーを作成できます。ログインが許可されたデバイスは、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。

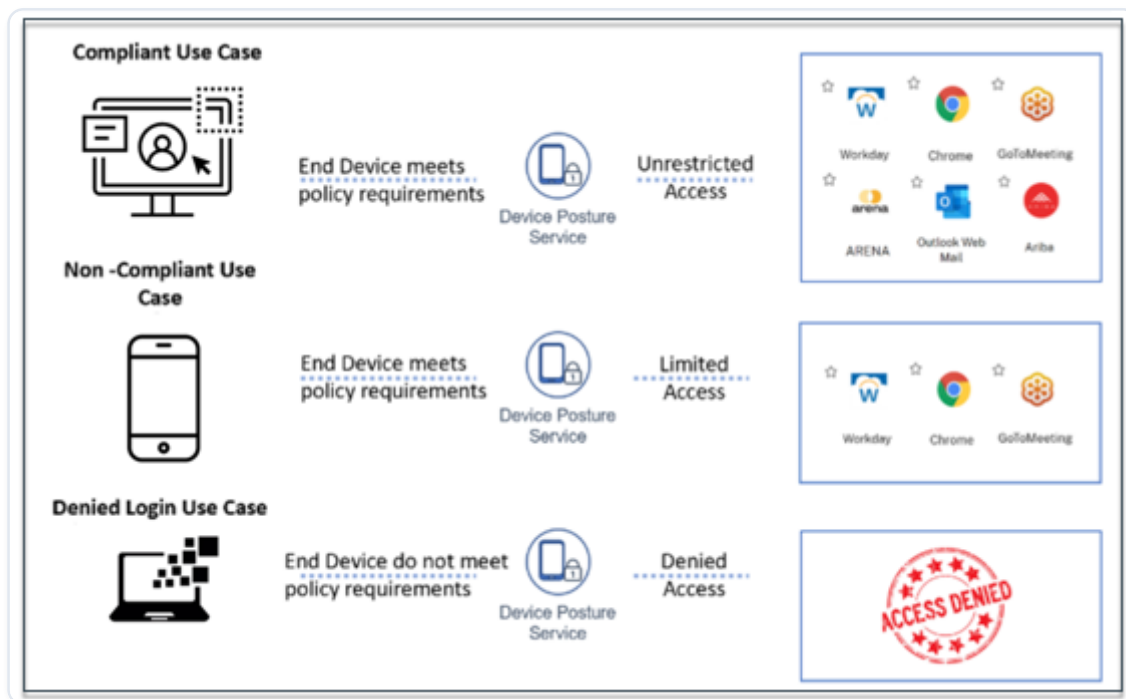
デバイスを準拠、非準拠、およびログイン拒否に分類するために使用される上位レベルの条件は次のとおりです。

- **準拠デバイス** – 事前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リソースへの完全または無制限のアクセス権を持って会社のネットワークにログインすることを許可されているデバイス。
- **非準拠デバイス** - 事前設定されたポリシー要件を満たし、Device PostureのDaaSおよびSecure Private Accessの構成に基づいて、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権を持って会社のネットワークにログインすることを許可されているデバイス。
 - DaaS: 管理者は、非準拠デバイスのアクセスを制限するデリバリーグループを指定できます。デリバリーグループへのアクセス制限の構成方法の詳細については、[Citrix DaaS configuration with Device Posture](#)を参照してください。
 - Secure Private Access: 管理者は、これらのデバイスのアクセスを制限する特定のアプリケーションを選択できます。特定のアプリケーションへのアクセス制限の構成方法の詳細

については、[Citrix Secure Private Access configuration with Device Posture](#)を参照してください。

- **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。

デバイスの**準拠**、**非準拠**、および**ログイン拒否**の分類は、Citrix DaaSおよびCitrix Secure Private Accessサービスに渡され、これらのサービスは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:

- デバイスポスチャポリシーは、プラットフォームごとに具体的に構成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バージョンを持つ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、レジストリ設定などを含むポリシーを構成できます。
- Linuxユーザーはフローでデバイスポスチャスキャンを確認できますが、ポスチャは管理者ポリシーでLinuxスキャンが構成されている場合にのみ評価されます。Linuxルールが構成されていない場合、ポスチャ評価はデフォルトの結果にフォールバックします。
- デバイスポスチャスキャンは、認証前/ログイン前だけに実行されます。
- 「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。

Device Postureサービスでサポートされているスキャン

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

ウィンドウズ	MACOS	IOS	リナックス
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	-
OSバージョン	OSバージョン	OSバージョン	OSバージョン
ファイル (存在、最終更新日時、MD5)	ファイル (存在、最終更新日時、MD5)	-	ファイル (存在、最終更新日時、MD5)
地理的位置	地理的位置	-	-
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、MD5、SHA1)	プロセス (存在、MD5、SHA1)	-	プロセス (存在、MD5、SHA1)
マイクロソフト エンドポイント マネージャー	マイクロソフト エンドポイント マネージャー	-	-
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	-	-
ウェブブラウザ	ウェブブラウザ	-	-
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)	-	-	-

ウィンドウズ	MACOS	IOS	リナックス
数値レジストリ (64ビット)	-	-	-
Windows Update インストールタイプ	-	-	-
Windows Update 最終更新チェック	-	-	-
外部デバイス接続済み	-	-	-
ネットワーク設定	-	-	-
-	-	-	マウントポイント

注:

- EPAライブラリバージョン24.9.1.1以降、**Windows Update 最終更新チェック** スキャンには、Windows Auto Upgradeサービスを介してインストールされた更新プログラムに加えて、BigFix、Microsoft Intune、およびその他のサードパーティツールを介してインストールされた更新プログラムも含まれます。
- Device PostureサービスでのiOSサポートの場合、EPAクライアントはiOS版Citrix Workspaceアプリの一部として組み込まれています。バージョンの詳細については、[iOS版Citrix Workspaceアプリ](#)を参照してください。

Windows Update 最終更新チェック

Windows Update 最終更新チェック の機能強化は、EPAライブラリバージョン24.9.1.1から適用されます。バージョン24.9.1.1以降、このスキャンには、Windows Auto Upgradeサービスを介してインストールされた更新プログラムに加えて、BigFix、Intune、およびその他のサードパーティツールを介してインストールされた更新プログラムが含まれます。

EPAライブラリバージョン24.11.1.1以降、**Windows Update 最終更新チェック** スキャンは、Windows更新プログラムを次のカテゴリに分類して表示します。

- **汎用更新プログラム:** このカテゴリには、Windows Update、Microsoft Update、または自動更新機能を使用してインストールされた更新プログラムが含まれます。
- **セキュリティ更新プログラム:** このカテゴリには、セキュリティ関連の脆弱性に対するパッチが含まれます。セキュリティ更新プログラムは、毎月第2火曜日に公開されます。
- **緊急更新プログラム:** このカテゴリには、緊急のセキュリティ関連ではないバグに対するパッチが含まれます。緊急更新プログラムは、必要に応じて公開されます。
- **定義更新プログラム:** このカテゴリには、製品の定義データベースへの追加を含む更新プログラムが含まれます。定義更新プログラムが公開されると、最新の更新プログラムと現在インストールされている更新プログラムとの差分のみがダウンロードされ、デバイスに適用されます。
- **更新プログラムのロールアップ:** このカテゴリには、テスト済みの累積的な修正プログラム、セキュリティ更新プログラム、緊急更新プログラム、および展開を容易にするためにまとめたパッケージ化された更新プログラムが含まれます。更新プログラムのロールアップは、毎月第2火曜日に公開されます。

注:

- 「**Windows Update Last Update Check**」 スキャンを設定する際、各カテゴリの更新が設定された期間内にスケジュールされていることを確認してください。この期間内に更新がインストールされない場合、スキャンは失敗します。
- 「**Windows Update Last Update Check**」 スキャンは、ユーザーが更新パッチをダウンロードして手動でインストールした更新には適用されません。

Device Postureサービス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も統合できます。

- Microsoft Intune。詳細については、「[Microsoft IntuneとDevice Postureの統合](#)」を参照してください。
- CrowdStrike。詳細については、「[CrowdStrikeとDevice Postureの統合](#)」を参照してください。

既知の制限事項

- **Device Posture** トグルボタンをオンまたはオフにした後、デバイスポスチャ機能が有効または無効になるまでには、数分から1時間かかる場合があります。
- デバイスポスチャ構成の変更はすぐに反映されません。変更が有効になるまで約10分かかる場合があります。
- Citrix WorkspaceでService Continuityオプションを有効にしている、Device Postureサービスがダウンしている場合、ユーザーはWorkspaceにサインインできない可能性があります。これは、Citrix Workspaceがユーザーデバイス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で長期間有効なトークンとパスワードを設定している場合、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は最大10個のポリシーを持つことができ、各ポリシーは最大10個のルールを持つことができます。
- Device Postureサービスでは、ロールベースアクセスはサポートされていません。
- Device Postureサービスは、Citrix Cloud™ Japan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サービスはログイン時に2秒の追加遅延を発生させます。この遅延は、Microsoft Intuneなどのサードパーティ統合といった追加構成によって増加する可能性があります。
- 復元性: デバイスポスチャサービスは、複数のPOPを備え、ダウンタイムがないことを保証する高い回復力を持っています。

クローム エンタープライズ プレミアムとの統合

デバイスポスチャサービスをGoogle Chrome Enterprise Premiumと統合することで、デバイスコンプライアンスチェックをChromeブラウザベースのアクセスシナリオに拡張できます。この統合により、ユーザーがChrome Enterprise Premiumで管理されているブラウザを介してアプリケーションにアクセスする際に、組織はデバイスポスチャポリシーを適用できるようになります。

デバイスポスチャサービスとChrome Enterprise Premium間の統合を有効にするには、OpenID Connect (OIDC) 認証をプライマリ認証方法として構成する必要があります。

詳細については、以下のトピックを参照してください。

- [Google Chrome Enterpriseとの統合](#)
- [シトリックス ワークスペースとのオープンIDコネクト \(OIDC\)](#)

新機能

このトピックでは、Device Postureサービスにおける強化と新機能について詳しく説明します。

09 September 2026

- 複数クラウドストアサポートの一般提供開始

複数クラウドストアのサポートが一般提供されるようになりました。詳細については、「[複数クラウドストアのサポート](#)」を参照してください。

22 June 2026

- Device PostureサービスとMicrosoft Entra IDの統合

Device PostureとMicrosoft Entra IDの統合が、Windowsプラットフォーム向けに一般提供されるようになりました。

詳細については、「[Device PostureサービスとMicrosoft Entra IDの統合](#)」を参照してください。

15 June 2026

- Device PostureサービスとChrome Enterpriseデバイス信頼コネクタの統合

Device PostureサービスがChrome Enterpriseデバイス信頼コネクタと統合されました。この統合により、Citrix®管理者はデバイスのポスチャ結果をGoogle Workspaceと共有し、Chromeが管理対象デバイスのポスチャに基づいてコンテキストウェアアクセスおよびデータ損失防止（DLP）ポリシーを適用できるようになります。詳細については、「[Device PostureサービスとChrome Enterpriseデバイス信頼コネクタの統合](#)」を参照してください。

05 June 2026

- Device Postureサービスを介したEndpoint Analysis (EPA) クライアントバージョンの管理

管理者は、サポートされるEPAの最小バージョンを維持することで、Device Postureサービスを介してEPAクライアントバージョンを管理できます。管理者は、すべてのユーザーが準拠す

る必要がある最小バージョンを設定する必要があります。この最小バージョン以上のユーザーは、Device Postureスキャンを実行できます。詳細については、「[Device Postureサービスを介したEPAクライアントバージョンの管理](#)」を参照してください。

01 June 2026

• Linux向けデバイスポスチャサービスの一般提供開始

デバイスポスチャサービスがLinuxプラットフォームで一般提供されるようになりました。以前はテクニカルプレビューとして提供されていましたが、現在では、サポートされているLinuxディストリビューションを実行しているエンドポイントに対して、完全なポリシー構成と適用をサポートしています。

このリリースにより、デバイスポスチャサービスは、ユーザーがサインインする前に、管理対象またはBYODステータス、および全体的なセキュリティポスチャを含むLinuxエンドポイントのコンプライアンスを評価します。これにより、ゼロトラストアクセスモデルが強化されます。

この統合により、以下の利点が提供されます。

- 包括的なアクセス適用: Linuxエンドポイントのスキャン結果に基づいて、Citrix DaaS (仮想アプリおよびデスクトップ) およびCitrix Secure Private Accessリソース (SaaS、Webアプリ、TCP、UDPアプリ) へのアクセスを動的に許可、制限、または拒否します。
- 合理化されたセキュリティチェック: Linuxエンドポイントでの認証前コンテキストスキャンは、Windows、macOS、およびiOSの既存のポリシーとシームレスに統合されるようになりました。

管理者は、以下のサポートされているスキャンを使用して、Linuxデバイスのデバイスポスチャポリシーを構成できます。

- OSバージョン
- ファイル (存在、最終変更時刻、MD5)
- プロセス (存在、MD5、SHA1)
- マウントポイント

注:

Linuxユーザーはフロー内でデバイスポスチャスキャンを確認できますが、ポスチャは、管理者ポリシーでLinuxスキャンが構成されている場合にのみ評価されます。Linuxルールが構成されていない場合、ポスチャ評価はデフォルトの結果にフォールバックします。

エンドポイントデバイスのポスチャポリシーの構成の詳細については、「[デバイスポスチャポリシーの構成](#)」を参照してください。

09 April 2026

• Windows Citrix Endpoint Analysis (EPA) クライアントバージョン 26.3.1.10 の提供開始

Citrix Endpoint Analysis (EPA) クライアントのこのアップデートでは、Windows環境全体でスキャンの信頼性とポリシー処理を向上させるために設計された、大幅なパフォーマンス最適化と重要なバグ修正が導入されています。

入手方法: [Citrix Downloads](#)。

主な機能強化と修正:

- ポリシーのスケラビリティの向上: EPAクライアントは、複雑なエンタープライズ環境を処理するように最適化され、効率的なデータ処理と安定性の向上を実現します。
- Windows Updateスキャンの改善: 正確なパッチ検出を確実にするため、自動UpdateSearcherフォールバックメカニズムが追加されました。
- User-Agentの最新化: 従来のIE7ベースのUser-Agent文字列を、現在のWebゲートウェイおよびセキュリティフィルターとの互換性を向上させるための、最新の製品固有の形式に置き換えました。

17 March 2026

• サードパーティ統合の失敗に関するメール通知

管理者は、サードパーティ統合の失敗が発生した場合にメール通知を受け取るようになりました。これらのエラーは、Secure Private AccessおよびDevice Postureサービスダッシュボードでも確認でき、関連するエラー詳細を添えてサードパーティサービスサポートに直接連絡し、解決時間を最小限に抑えることができます。詳細については、「[サードパーティ統合の失敗通知](#)」を参照してください。

21 January 2026

- **Device PostureサービスとdeviceTRUST - より良い連携**

エンタープライズアプリケーションとデータへのアクセスを保護するには、静的なポリシーだけでは不十分です。ユーザーのジャーニー全体で継続的に適応する、リアルタイムでコンテキストを認識した制御が必要です。CitrixのDevice Posture Service (DPS) とdeviceTRUST (dT) は、認証前、列挙、セッション中のあらゆるフェーズで包括的なコンテキストアクセス範囲を提供するために連携することで、この機能を実現します。詳細については、「[Device Posture サービスとdeviceTRUST - より良い連携](#)」を参照してください。

26 September 2025

- **複数のレジストリキー値を評価するためのスキャン**

Device Postureサービスに、Windowsデバイス用の新しいスキャンが追加されました。管理者は、**複数値非数値レジストリスキャン**を設定して、複数のレジストリキー値を評価し、デバイスの管理対象ステータスを判断できます。複数値非数値レジストリスキャンを含むデバイスポスチャポリシーの設定の詳細については、「[Device Postureポリシーの設定](#)」を参照してください。

- **Citrix Monitor を使用した Device Posture サービス トランザクションのトラブルシューティング**

管理者は、Citrix Monitor ダッシュボードに統合された包括的な監視機能を通じて、Device Posture サービス トランザクションを効果的に診断およびトラブルシューティングできるようになりました。この機能強化により、Device Posture ポリシーの評価、コンプライアンスチェック、エラー診断に関する詳細なインサイトが得られます。詳細については、「[Citrix Monitor を使用した Device Posture サービス トランザクションのトラブルシューティング](#)」(/ja-jp/citrix-daas/monitor/troubleshoot-deployments/user-issues/diagnose-device-posture-service-transactions.html)を参照してください。

- **ポスチャチェックの自動スキップ**

Device Posture サービスは、エンドユーザーデバイスで EPA クライアントが検出されない場合に、ポスチャチェックの自動スキップをサポートするようになりました。自動スキップが構成されている場合、システムはリアルタイム検出を実行して、エンドユーザーのデバイスに EPA クライアントが存在するかどうかを判断します。クライアントが検出されない場合、ポスチャチェックプロセスはユーザーの操作を必要とせずに自動的にバイパスされ、ログインプロセスが効率化されます。

管理者は、EPA クライアントがマシンにインストールされていない場合や EPA クライアントのバージョンが古い場合に、エンドユーザーがログイン試行ごとに手動で をクリックできるよ

うに設定を構成することもできます。詳細については、「」(</ja-jp/device-posture/device-posture-global-settings.html#skip-device-posture-checks>)を参照してください。

- **複数の Microsoft Intune アカウントと Device Posture の統合**

Device Posture サービスは、複数の Microsoft Intune アカウントとの統合をサポートするようになりました。これにより、複数の Intune テナントを持つ組織（多くの場合、合併、買収、部門分割の結果）は、すべての環境でデバイスポスチャをシームレスに管理できます。詳細については、「」(</ja-jp/device-posture/device-posture-third-party-integrations.html#microsoft-intune-integration-with-device-posture>)を参照してください。

- **Secure Private Access ハイブリッド展開での Device Posture のサポート**

Device Posture は Secure Private Access ハイブリッド展開でサポートされていますが、リクエストに応じてのみ利用可能です。この機能を有効にするには、Citrix サポートまたは ATS にお問い合わせください。Device Posture サービスは、Citrix Virtual Apps and Desktops のゲートウェイではまだサポートされていません。

- NetScaler Gateway で Device Posture チェックを有効にする方法の詳細については、[NetScaler Gateway での Device Posture チェック](#)を参照してください。
- NetScaler Gateway で Device Posture 機能を有効にするだけでなく、StoreFront™ にアクセスする NetScaler Gateway の URL を Device Posture 設定ページに追加する必要があります。詳細については、「」(</ja-jp/citrix-secure-private-access/hybrid/spa-hybrid-dps-integration.html#enable-device-posture-for-secure-private-access-hybrid-solutions>)を参照してください。

09 July 2025

- **マルチワークスペース URL のサポート**

管理者は、異なる Citrix Workspace™ アクセス URL に個別のデバイスポスチャポリシーを適用できるようになり、きめ細かな制御と簡素化されたセキュリティ管理が可能になりました。以前は、Device Posture サービスはすべてのワークスペース URL でグローバルに有効になっていたため、管理者は URL ごとに特定の要件を適用できませんでした。

マルチワークスペース URL のサポートにより、次のことができるようになりました。

- 特定のワークスペースURLに対して、個別のデバイスポスチャチェックを適用します。
- ユーザーがアクセスするワークスペースURLに基づいて、デバイスコンプライアンスの異なるレベルを適用します。

- 。本番URLに展開する前に、テストワークスペースURLでデバイスポスチャチェックを作成し、テストします。

詳細については、[複数ワークスペースURLのサポート](#)を参照してください。

注:

この機能はプレビュー版です。

21 Feb 2025

- ・ **イベント駆動型ポスチャチェックによるデバイスコンプライアンス**

EPA Libraryバージョン24.11.1.1以降、Device Postureはデバイスのコンプライアンスを評価するための強化されたチェックを導入しました。

デバイスコンプライアンスをより詳細に制御するために、以下の2つのスキャンが追加されました。

- 。 **外部デバイス接続済み:** このスキャンは、外部USBストレージデバイスがエンドポイントに接続されているかどうかを検出します。
- 。 **ネットワーク設定:** このスキャンは、デバイスが保護されたWi-Fiネットワークに接続されているかどうかを判断します。

以下のいずれかのイベントが発生した場合、Device Postureはデバイスのコンプライアンスステータスを再評価します。

- 。 **外部デバイス接続済み**スキャンが構成されており、外部USBストレージデバイスが挿入または削除された場合。
- 。 **ネットワーク設定**スキャンが構成されており、オープンネットワークと保護されたネットワーク間の切り替えが検出された場合。
- 。 **Windows Defender ファイアウォール**スキャンが構成されており、それが有効または無効にされた場合。

リソースへのアクセスは、新しいコンプライアンスステータスに従って更新されます。これにより、デバイスのリアルタイムのコンプライアンスステータスに基づいて、リソースへのアクセスが許可または取り消されることが保証されます。

詳細については、[イベント駆動型ポスチャチェックによるデバイスコンプライアンス](#)を参照してください。

注:

この機能はWindowsプラットフォームでのみサポートされています。

- ダウングレード後に終了するTCP/UDPアクティブセッション

Citrix Secure Accessクライアントから起動されたTCP/UDPアプリケーションの場合、デバイスポスチャスキャンがダウングレード（例えば、[準拠](#)から[非準拠](#)または[アクセス拒否](#)へ）になった場合、ユーザーは通知を受け取り、5分後にアクティブセッションは終了します。詳細については、[デバイスの定期スキャン](#)を参照してください。

注:

この機能はWindowsプラットフォームでのみサポートされており、エンドポイント分析（EPA）クライアントバージョン24.8.1.19およびライブラリバージョン24.9.1.1から利用可能です。

- Windows Update最終更新スキャンの機能強化

EPAライブラリバージョン24.9.1.1以降、**Windows Update最終更新スキャン**には、Windows 自動アップグレードサービスを通じてインストールされた更新プログラムに加えて、BigFix、Microsoft Intune、およびその他のサードパーティツールを通じてインストールされた更新プログラムも含まれるようになりました。

04 Dec 2024

- Jamf Pro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Jamf Proとも統合されています。詳細については、[Jamf Proとデバイスポスチャの統合](#)を参照してください。

29 May 2024

- テストモードでのデバイスポスチャサービスの利用可能性

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

じた行動計画を立てることができます。詳細については、[テストモードで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**

Windowsデバイスに対して、設定されたチェックを30分ごとに定期的にスキャン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](#)を参照してください。

14 May 2024

- **デバイスポスチャチェックをスキップ**

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設定できます。詳細については、「[デバイスポスチャチェックをスキップ](#)」を参照してください。

- **デバイスポスチャダッシュボード**

Device Posture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用のダッシュボードが追加されました。管理者はこのダッシュボードを使用して、監視とトラブルシューティングを行うことができます。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。

- **ブラウザおよびウイルス対策チェックの一般提供**

ブラウザおよびウイルス対策チェックが一般提供され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。

- **カスタムメッセージの一般提供**

アクセスが拒否された場合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るようになりました。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。

26 March 2024

- **カスタムワークスペースURLのサポート**

Device Posture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。cloud.com URLに加えて、所有するURLを使用してワークスペースにアクセスできます。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構成](#)」を参照してください。

12 February 2024

- **ブラウザおよびウイルス対策チェックのサポート - プレビュー**

Device Postureサービスでブラウザおよびウイルス対策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。

23 January 2024

- **Device Posture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。

- **Device Postureサービスのプレビュー機能**

Device Posture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。

- Device Postureサービスは、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。
- Device Postureサービスは、地理位置情報およびネットワーク位置情報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、[Device Posture](#)を参照してください。

11 September 2023

- **Microsoft IntuneとのDevice Posture統合の一般提供開始**

Microsoft IntuneとのDevice Posture統合が一般提供されるようになりました。詳細については、[Microsoft IntuneとDevice Postureの統合](#)を参照してください。

30 August 2023

- **Device Postureサービス向けCitrix Endpoint Analysisクライアントの管理**

EPAクライアントは、NetScalerおよびDevice Postureと組み合わせて使用できます。

NetScalerおよびDevice Postureと組み合わせて使用する場合、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、[Device Postureサービス向けCitrix Endpoint Analysisクライアントの管理](#)を参照してください。

28 August 2023

- **iOSプラットフォームでのDevice Postureサービスのサポート - プレビュー**

Device Postureサービスは、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、[Device Posture](#)を参照してください。

22 August 2023

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

Citrix Device Postureサービスは、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（Smart Access）を有効にできるようになりました。詳細については、[Device certificate check](#)を参照してください。

17 August 2023

- **Citrix DaaS™ MonitorでのDevice Postureイベント**

Device Postureサービスのイベントと監視ログは、DaaS Monitorで検索できるようになりました。詳細については、[Device posture events on Citrix DaaS Monitor](#)を参照してください。

23 January 2023

- **Device Postureサービス**

Citrix Device Postureサービスは、エンドデバイスが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満たす必要がある特定の要件を管理者が適用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、[Device Posture](#)を参照してください。

- **マイクロソフト 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**

Device Postureサービスが提供するネイティブスキャンに加えて、Device Postureサービスは他のサードパーティソリューションとも統合できます。Device Postureは、WindowsおよびmacOSでMicrosoft Endpoint Manager（MEM）と統合されています。詳細については、[Microsoft Endpoint Manager integration with Device Posture](#)を参照してください。

エンドポイント分析リリースノート

エンドポイント分析 (EPA) リリースノートには、さまざまなプラットフォーム向け EPA クライアントの機能強化、新機能、修正された問題、および既知の問題が記載されています。

V26.07.20 for macOS (18 September 2026)

• macOS の継続スキャン対応

Mac 用エンドポイント分析が継続スキャンに対応しました。以前は、macOS のデバイスポスチャはユーザーが接続したときにのみ評価されていたため、サインイン後にファイアウォールを無効にしたり、ウイルス対策保護を停止したりするなどの変更は、次の接続試行まで検出されませんでした。継続スキャンにより、エンドポイント分析はセッション全体でデバイスポスチャを継続的に再評価し、その現在の状態を報告します。これにより、コンテキストアクセスポリシーは、一度のスナップショットではなく、デバイスのライブポスチャに対応できるようになります。この機能により、macOS は Windows の継続スキャンと連携し、Mac ユーザーの条件付きアクセスを強化します。

注記:

- 。この機能は段階的に展開されており、お客様には順次提供されます。
- 。クライアント側の設定変更は不要です。

V26.7.1.15 for Windows (11 September 2026)

新機能

• Windows 上のエンドポイント分析のネイティブ ARM64 サポート

エンドポイント分析は、ARM64 Windows デバイスへのネイティブインストールをサポートするようになりました。x64 クライアントと並行して、個別の epasetup_ARM64.exe パッケージが提供されるため、x64 エミュレーションを介してクライアントを実行する必要がなくなります。

デバイスアーキテクチャに一致するパッケージを展開してください。x64 デバイスの場合は epasetup.exe、ARM64 デバイスの場合は epasetup_ARM64.exe です。ネイティブ ARM64 サポートにより、ARM64 デバイスでのパフォーマンスが向上します。

制限事項:

- Keylogger 検出は ARM64 ではサポートされていません。
- ARM64クライアントはクリーンインストールが必要なため、既存のEndpoint Analysisクライアントをアンインストールしてからインストールしてください。

• Endpoint Analysisにおけるキーロガー検出（プレビュー）

Endpoint Analysisは、エンドポイントで実行されているキーロギングソフトウェアを検出できるようになり、検出の詳細をMonitorで報告して管理者が確認できるようにします。

この機能は、管理者が管理対象エンドポイント上のキーロギングのリスクを特定するのに役立ちます。これは可視性のみを目的としており、ポスチャ評価やアクセス決定には影響しません。これを有効にしても、ユーザーがリソースにアクセスするのをブロックすることはできません。

注記：

- この機能は現在プレビュー段階であり、お客様からのリクエストに応じて有効になります。
- この機能はARM64デバイスではサポートされていません。

• Endpoint Analysis用のバンドルされたスキャンエンジン

スキャンエンジンとそのライブラリは、Endpoint Analysisクライアントパッケージに同梱され、クライアントと一緒にインストールされるようになりました。クライアントとスキャンエンジンを単一のリリースとしてパッケージ化することで、バージョンの一貫性が確保され、実行時にスキャンエンジンコンポーネントをダウンロードする必要がなくなります。クライアントアプリケーションのアップグレードプロセスは変更されません。

• Endpoint Analysisは64ビットのみになりました

Endpoint Analysis は、64ビットクライアントとしてのみ利用可能になりました。32ビット (Win32/x86) のバイナリおよびインストーラーは、製造もサポートもされなくなり、インストーラーは32ビット版のWindowsでは実行されません。

- 32ビットのEndpoint Analysisパッケージを参照しているデプロイスクリプトまたはソフトウェア配布パッケージを更新してください。
- サポートされている両方の64ビットアーキテクチャが利用可能です。x64デバイス向け `epasetup.exe` とARM64デバイス向け `epasetup_ARM64.exe` です。

- **Endpoint Analysisは専用のインストールパスを使用します**

Endpoint Analysisは、共有のSecure Access Clientの場所を使用する代わりに、製品固有のフォルダーとレジストリの場所にインストールされるようになりました。

インストールパスは次のとおりです。

- マシンごと: C:\Program Files\Citrix\Secure Access Endpoint Analysis
- ユーザーごと: %LocalAppData%\Citrix\Secure Access Endpoint Analysis
- 製品レジストリキー: HKLM\SOFTWARE\Citrix\Secure Access Endpoint Analysis

- **アンインストール中のEndpoint Analysisの保持**

Citrix製品をアンインストールしても、他のインストール済みCitrix製品がそれに依存している場合、Endpoint Analysisは削除されなくなりました。これは、Citrix Workspaceアプリ、Citrix Enterprise Browser、Citrix Secure Accessなど、同じデバイス上の複数のCitrix製品でEndpoint Analysisが共有されている場合に適用されます。以前は、1つの製品をアンインストールするとEndpoint Analysisが削除され、他の製品にポスチャクライアントが残らない可能性がありました。

対話型アンインストールでまだ必要なクライアントが削除される場合、メンテナンスページには、Endpoint Analysisのインストールを維持している依存アプリケーションが一覧表示されません。

注:

- スクリプトによる削除の場合、Endpoint Analysisを正しく保持するサイレントアンインストールは終了コード `1000` を返します。展開システムで `1000` を成功コードとして構成してください。
- 依存関係があるにもかかわらずEndpoint Analysisを削除するには、昇格されたプロンプトからアンインストールコマンドを `/SkipConsumerCheck` で再実行してください。

- **Endpoint Analysis はサイレント展開をサポートします**

Endpoint Analysis のセットアップは、Configuration Manager や Intune などのソフトウェア配布ツールを介したサイレントインストールとアンインストールをサポートするようになりました。

た。サイレント操作には `/quiet` を使用し、インストールとアンインストールの両方でログの場所を指定するには `/log <path>` を使用します。

注:

- 。これらのオプションは、集中管理された展開を対象としています。セットアップが指定されたログパスに書き込めない場合、ログを他の場所にサイレントで書き込む代わりに、終了コード `1622` で停止します。
- 。アンインストール中に、昇格された権限のみの `/SkipConsumerCheck` オプションを使用して、他の Citrix 製品がそれに依存している場合でも Endpoint Analysis を削除します。
- 。展開ツールで、終了コード `1000` を成功コードとして構成します。このコードは、別の Citrix 製品がまだそれを必要としているため、Endpoint Analysis が意図的に保持されたことを示します。

• 最新化された Endpoint Analysis インストーラー

Endpoint Analysis インストーラーのインターフェースは、インストール、修復、およびメンテナンスのために強化されました。強化されたインターフェースは、ユーザーがダウンロードページやメンテナンスページからなど、クライアントを対話的にインストール、修復、または削除するときに表示されます。

注:

サイレント展開とスクリプトによる展開は引き続きサポートされます。MSI ベースの展開はサポートされなくなったため、必要に応じて、以下の `epasetup.exe` コマンドラインスイッチを使用してください。

- 。 `/quiet, /silent, /q` - ユーザーインターフェースなしのサイレントインストール。
- 。 `/passive` - 進行状況のみを表示し、対話型プロンプトはありません。
- 。 `/uninstall` - 製品をアンインストールします。
- 。 `/repair` - 既存のインストールを修復します。
- 。 `/log "<file>"` - インストーラーログを指定されたパスに書き込みます。
- 。 `/norestart` - インストールまたはアンインストール後の自動再起動を抑制します。
- 。 `/? , /h, /help` - インストーラーのヘルプ情報を表示します。

修正された問題

- Windows Updateのポスチャが誤ったソースから報告されていました。ホットパッチが適用されたマシンでは、置き換えられたベースラインの経過時間が表示され、パッチの経過時間は無関係なインストールに基づいており、測定不能な値は利用不可として識別される代わりに報告されていました。
- Windows Updateサービスが起動している間、サードパーティのスキャンエンジンからのポスチャングナルが断続的に利用できなくなります。
- スキャンエンジンの障害が、デバイスにセキュリティ製品がインストールされていないかのよう報告され、エンジンの障害と、実際に保護されていないデバイスとの区別がつかなくなり、同じアクセス拒否が発生していました。
- 署名検証では、署名者がマシンの信頼ストア内のルート証明書にチェーンすることが必要になりました。ユーザーごとのストアでのみ信頼されているルートは、もはや受け入れられません。カスタムの信頼された署名証明書を使用する管理者は、それをマシン全体に展開する必要があります。
- `devicePostureNativeBridge.exe` プロセスはconfig.jsをクリアし、保存された接続を消去する可能性があります。その結果、保存された接続がクライアントから消えてしまいます。
- 繰り返しスキャンすると、メモリリークやハンドルリークが発生する可能性があります。
- ユーザーはアンインストールを再試行したり、破損したインストールを削除したりできません。

この修正により、メンテナンスページでサイレントパスと同じディープクリーンオプションが提供されるようになり、破損したインストールでアンインストールが失敗した場合に回復できるようになります。

- Endpoint Analysis をアンインストールすると、孤立したサービスレジストリキーが残ります。
- NetScaler Gateway でグローバルサーバー負荷分散、HSTS、httpOnly クッキー、コンテンツセキュリティポリシーがすべて有効になっている場合、ブラウザの Endpoint Analysis フローが失敗します。
- 大量のサービス応答が切り捨てられたり、過剰に読み取られたりする可能性があるため、デバイスチェックが完了せず、ユーザーは「デバイスを確認中…」画面に無期限に留まる可能性があります。

- 以前は、ブラウザのネイティブメッセージングホストは、接続の一端のみをチェックしていたため、検証済みのブラウザ以外のプロセスからの接続を受け入れていました。この修正により、接続の両端が同じブラウザプロセスに属していることを検証するようになりました。
- レシーバープロセスが閉じられると、ブローカーとのクリップボードハンドシェイクが失敗します。

V26.6.1.4 for Windows (24 August 2026)

以下のセクションでは、Windows用 V26.6.1.4 リリースに関する詳細情報を提供します。

新機能

- **デバイスポスチャスキャン中のメモリリークを解決するOPSWATライブラリの更新**

EPAクライアントには、サードパーティ製品の検出中にメモリリークを解決する更新された OPSWAT (OESIS) ライブラリが含まれるようになりました。頻繁または継続的にデバイスポスチャスキャンを実行するデバイスでは、スキャンプロセスにおける段階的なメモリ蓄積が発生しなくなりました。このアップデートにより、ALYac、WatchGuard Endpoint Security Prime、Trellix EDRFなどのサードパーティ製セキュリティ製品の検出サポートも拡張されます。

修正された問題

- クライアント選択ページで「フルトンネル」が選択されている場合、ブラウザからCitrix Secure Accessを起動すると、ホームページの読み込みに失敗することがあります。この問題は、EPAがNetScaler Gatewayによって拒否される、誤って終了されたHTTPヘッダーを送信するために発生します。
- デバイスポスチャスキャンが完了せず、クライアントが「デバイスを確認中…」というメッセージで停止したままになることがあります。この問題は、デバイスポスチャサービスから返されるスキャン構成がクライアントの容量を超えている場合（管理者がレジストリスキャンポリシーを有効にした場合など）に発生します。
- 各スキャンサイクル中に、ユーザーがリソースへのアクセスを拒否されることがあります。この問題は、定期的なスキャン中にローカルのデバイスポスチャ管理サービスがコンテキストの保存と読み取りを行う際に、サインインしているユーザーを一貫して解決できない場合に発生します。

V26.5.1.7 for Windows (08 Jul 2026)

以下のセクションでは、Windows用 V26.5.1.7 リリースに関する詳細情報を提供します。

修正された問題

- 一部のデバイスで、EPAクライアントがWindowsのバージョンを誤って報告します。例えば、Windows 11デバイスが古いWindowsバージョンとして報告され、OSベースのスキャンチェックが誤って評価される原因となります。この問題は、特定のWindows 10およびWindows 11デバイス上のEPA v1（クラシック、オンプレミス）スキャンフローに影響します。
- 管理者モードの展開では、EPA管理サービスが評価中にデバイス証明書を自動的に選択しないため、デバイス証明書のポスチャチェックが失敗する可能性があります。影響を受けるセットアップでは、これにより定期的な（継続的な）デバイス証明書チェックが繰り返し失敗します。
- CrowdStrike FalconやOPSWATベースの製品など、特定のセキュリティ製品では、スキャンが「インターネットチェックを無視」設定を正しく適用しません。その結果、製品が正常な状態であっても、ウイルス定義の最終更新時刻などのチェックが失敗する可能性があります。

この問題は、影響を受ける製品のOPSWATベースのアンチウイルスおよび定義スキャンで発生します。

- ユーザーはデバイスポスチャコンテキストの読み取り失敗を経験する可能性があります。例えば、ブラウザ拡張機能が、保存されたEPAコンテキストファイルが復号化されて確実に読み戻されないため、デバイスポスチャコンテキストを取得できないと報告する場合があります。この問題は、デバイスポスチャサービスが暗号化されたポスチャコンテキストと定期スキャンファイルを書き込み、後で再読み取りする際に発生します。

V26.03.31 for macOS (14 May 2026)

以下のセクションでは、macOS用V26.03.31リリースに関する詳細情報を提供します。

新機能

- 独立したライブラリ更新の非推奨化

このリリース以降、ランタイムに依存するライブラリの更新はサポートされなくなります。これらのコンポーネントに対する今後のすべての更新は、CitrixEndpointAnalysisアプリケーションの新しいバージョンを通じてのみ提供されます。

- EPAアプリケーションとの静的ライブラリ統合

システムスキャンに必要なコアライブラリは、クラウドおよびオンプレミス展開の両方で CitrixEndpointAnalysis アプリケーションに直接バンドルされるようになりました。

この統合により、以下の利点が得られます。

- 。統合されたライブラリは、アプリケーションの起動時に厳格な署名検証の対象となります。
- 。これらのアセットをバンドルすることで、アプリケーションは実行時にライブラリをダウンロードして抽出する必要がなくなり、初期化の高速化と起動の信頼性向上につながります。

デバイスポスチャポリシーを構成する

デバイスポスチャは、デバイスがリソースにアクセスするために満たす必要があるポリシーとルールとの組み合わせです。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関連付けられています。さらに、各ポリシーには優先度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 を選択します。
2. タブをクリックし、 をクリックします。

注:

- Secure Private Access サービスのお客様は、管理者ユーザーインターフェイスの左側のナビゲーションで を直接クリックできます。
- 初めて使用する場合、デバイスポスチャのランディングページでデバイスポスチャポリシーの作成を求められます。デバイスポスチャポリシーは、プラットフォームごとに個別に構成する必要があります。デバイスポスチャポリシーを作成すると、適切なプラットフォームの下に一覧表示されます。
- ポリシーは、デバイスポスチャ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、右上の トグルを にスライドします。

3. をクリックします。
4. で、ポリシーを適用するプラットフォームを選択します。デバイスポスチャ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. で、デバイスポスチャの一部として実行するチェックを選択し、一致する必要がある条件を選択します。

チェックに関する次の点に注意してください。

- 発行者証明書がデバイスに存在することを確認します。そうでない場合は、デバイスポスチャポリシーの作成中にデバイス証明書をインポートするか、デバイスポスチャのホーム

ページの から証明書をアップロードできます。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。

- 複数のデバイス証明書が共通の発行者名を共有する環境では、デバイスポスチャサービスが誤った証明書を評価する可能性があります。サービスが特定のポリシーの正確な証明書を識別できるようにするには、オプションを明示的に有効にする必要があります。詳細については、「[デバイス証明書チェックのスキャンを構成する](#)」を参照してください。
- エンドデバイスのEPAクライアントは、管理者権限で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によるデバイス証明書チェックは、チェックをサポートしていません。

注:

- 「**Multi-Value Non Numeric Registry**」スキャンを使用すると、管理者はデバイスが管理対象か非管理対象かを判断できます。これは、いくつかのレジストリキー値を評価することによって実現されます。
- ネットワークロケーションチェックのポリシー規則を作成する際、Device Posture サービスコンソールから直接ネットワークロケーションを追加できます。ただし、ネットワークロケーションを変更するには、Citrix Cloudのネットワークロケーション設定を使用する必要があります。

6. 複数の規則を作成するには、 をクリックします。複数の規則にはAND条件が適用されます。

デバイスポスチャの構成(/en-us/device-posture/media/device-posture-configuration1.png)

7. 構成した条件に基づいて、 で、デバイススキャンがユーザーデバイスを分類する必要があ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. に、ポリシーが評価される順序を入力します。

- 1から100までの値を入力できます。拒否ポリシーをより高い優先度で構成し、次に非準拠、最後に準拠と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。

デバイスポスチャの構成(/en-us/device-posture/media/device-posture-configuration2.png)

重要：

- デバイスポスチャポリシーを有効にするには、トグルスイッチを にする必要があります。ポリシーを有効にする前に、ポリシーが正しく構成されており、テスト環境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。
- Linuxユーザーはフロー内でデバイスポスチャスキャンを確認できますが、ポスチャは管理者ポリシーでLinuxスキャンが構成されている場合にのみ評価されます。Linuxルールが構成されていない場合、ポスチャ評価はデフォルトの結果にフォールバックします。

デバイスポスチャを使用してコンテキストアクセス（スマートアクセス）を構成する

デバイスポスチャの検証後、デバイスはログインを許可され、準拠または非準拠として分類されます。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利用可能であり、デバイスポスチャ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。したがって、Citrix DaaSとCitrix Secure Private Accessは、デバイスポスチャタグを使用してアクセス制御を適用するように構成する必要があります。

デバイスポスチャによるCitrix DaaSの構成

DaaSリソースへのアクセスを制限するには、アクセス制限を適用する必要があるデリバリーグループを指定し、デバイスポスチャタグを使用してアクセス制御制限を構成できます。

前提条件:

アダプティブアクセス機能が有効になっていることを確認します（**Citrix Workspace > アクセス > アダプティブアクセス**）。詳細については、「[アダプティブアクセス機能を有効にする](#)」を参照してください。

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. デバイスポスチャ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。

Edit Delivery Group

demo-group

- Users
- Load Balancing
- Desktops
- Application Prelaunch
- Application Linging
- User Settings
- StoreFront
- App Protection
- Scopes
- Access Policy**
- Restart Schedule
- License Assignment

Access Policy

Configure smart access policy expressions to control user access to resources. Only user connections that meet the specified expressions can access resources in this delivery group. For example, you can restrict user access to apps and desktops in this delivery group to a subset of users and specify allowed user devices.

Policy		Status	
Citrix Gateway connections	Default	Enabled	
Non-Citrix Gateway connections	Default	Enabled	

Add

- 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. **いずれかに一致**を選択し、**条件の追加**をクリックします。
- c. 「ネットワークロケーションの構成」で構成したすべてのロケーションタグの基準を追加します。「Filter」に「Workspace」と入力し、「Value」に「COMPLIANT」または「NON-COMPLIANT」と入力します。

Edit Policy

Add criteria to filter user connections. A criterion comprises a smart access filter and a value. You can add inclusion and exclusion criteria.

Policy name:

Policy state: ☒

☒ Connections meeting the following criteria

☐ Match all ☒ Match any

Filter:	Value:	
<input type="text" value="Workspace"/>	<input type="text" value="NON-COMPLIANT"/>	
<input type="text" value="Workspace"/>	<input type="text" value="DEVICE_TYPE_WINDOWS"/>	

[+ Add criterion](#)

☐ Connections not meeting any of the following criteria

No criteria added

[Done](#) [Cancel](#)

注:

デバイス分類タグの構文は、以前にキャプチャしたとおり、すべて大文字で入力する必要があります (**COMPLIANT** および **NON-COMPLIANT**)。そうしないと、デバイスポスチャポリシーは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、デバイスポスチャサービスは、デバイスに関連付けられた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、大文字でのみ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)

デバイスポスチャを使用したCitrix Secure Private Access の構成

Secure Private Access リソースへのアクセスを制限するには、アクセス制限を適用する必要があるアプリケーションを選択し、デバイスポスチャタグを使用してアクセス制御制限を構成できます。

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. 左側のナビゲーションで「**アクセスポリシー**」をクリックし、その後「**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ケーションまたはアプリケーションセットを選択します。
6. 「**ルールの作成**」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、その後「**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、ユーザーがアプリケーションにアクセスすることを許可するために満たすべき必須条件です。
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。

- **Compliant** - 準拠デバイスの場合
- **Non-Compliant** - 非準拠デバイスの場合

注:

タグは、以前にキャプチャされたとおりに、大文字で入力する必要があります
(**Compliant** および **Non-Compliant**)。そうしないと、デバイスポスチャポリシーは意図したとおりに機能しません。

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。

概要ページにポリシーの詳細が表示されます。

14. 詳細を確認し、**完了** をクリックします。

アクセスポリシーの作成に関する詳細については、「[複数のルールを持つアクセスポリシーを構成する](#)」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としてタグ付けされていないSecure Private Accessアプリケーションは、デフォルトのアプリケーションとして扱われ、デバイスポスチャに関係なくすべてのエンドポイントでアクセス可能です。

Step 2: Conditions

User*

Matches any of ▼ Select a domain ▼ administratoradminis X ▼

AND

Device posture check ▼ Matches any of ▼ Compliant, Non-Compliant X ▼ -

+ Add condition

Cancel Back Next

デバイスポスチャポリシーを編集する

構成されたデバイスポスチャポリシーは、**デバイススキャン** 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したい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。

デバイスポスチャポリシー1を編集(/en-us/device-posture/media/device-posture-edit-policy.png)

デバイスポスチャのグローバル設定を構成する

以下は、必要に応じて構成できるデバイスポスチャのグローバル設定の一部です。

- イベント駆動型ポスチャチェックによるデバイスコンプライアンス(/ja-jp/device-posture/device-posture-global-settings.html#device-compliance-with-event-driven-posture-checks)
- デバイスの定期スキャン(/ja-jp/device-posture/device-posture-global-settings.html#periodic-scanning-of-devices)
- 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(/ja-jp/device-posture/device-posture-global-settings.html#customized-messages-for-access-denied-scenarios)
- デバイスポスチャチェックをスキップ(/ja-jp/device-posture/device-posture-global-settings.html#skip-device-posture-checks)
- カスタムワークスペースURLのサポート(/ja-jp/device-posture/device-posture-global-settings.html#custom-workspace-urls-support)
- デバイスポスチャによるセッションレコーディングの構成(/ja-jp/device-posture/device-posture-global-settings.html#session-recording-configuration-with-device-posture)
- デバイス証明書チェック(/ja-jp/device-posture/device-posture-global-settings.html#device-certificate-check)
- 許可されたドメインのリストを構成する(/ja-jp/device-posture/device-posture-global-settings.html#configure-the-list-of-allowed-domains)

イベント駆動型ポスチャチェックによるデバイスコンプライアンス

EPAライブラリバージョン24.11.1.1以降、デバイスポスチャはデバイスのコンプライアンスを評価するための強化されたチェックを導入しています。

デバイスコンプライアンスをより詳細に制御するために、以下の2つのスキャンが追加されました。

- **外部デバイス接続済み:** このスキャンは、外部USBストレージデバイスがエンドポイントに接続されているかどうかを検出します。

- **ネットワーク設定:** このスキャンは、デバイスが保護されたWi-Fiネットワークに接続されているかどうかを判断します。

以下のいずれかのイベントが発生すると、Device Posture はデバイスのコンプライアンスステータスを再評価します。

- **外部デバイス接続**スキャンが構成されており、外部 USB ストレージデバイスが挿入または削除された場合。
- **ネットワーク設定**スキャンが構成されており、オープンネットワークと保護されたネットワーク間の切り替えが検出された場合。
- **Windows Defender ファイアウォール**スキャンが構成されており、それが有効または無効にされた場合。

リソースへのアクセスは、新しいコンプライアンスステータスに従って更新されます。これにより、リソースへのアクセスがデバイスのリアルタイムのコンプライアンスステータスに基づいて許可または取り消されることが保証されます。

注:

- イベント駆動型ポスチャチェックは現在、Windows 版 Citrix Secure Access クライアントバージョン 24.8.1.19 以降でのみサポートされています。
- ユーザーインストールと管理者インストールの両方でポスチャスキャンを利用できますが、イベントに基づくデバイスコンプライアンスのリアルタイム再評価には管理者権限が必要です。

次の図は、Device Posture 管理コンソールで構成された**外部デバイス接続**および**ネットワーク設定**スキャンを示しています。

Create device policy

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

Platform

Select the operating system for this device posture scan. [?](#)

Windows

Policy rules

Select a condition and apply access rules for your services and data. [?](#)

External Device Connected

→ USB Storage

Equal to ==

false

+ Add qualifier

AND

Network Settings

→ Password Protected WiFi

Equal to ==

true

デバイスの定期スキャン

構成されたチェックについて、Windows デバイスの定期スキャンを 30 分ごとに有効にできます。デバイスの定期スキャンを有効にするには、エンドデバイス上の 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。定期スキャンを有効にするには、次の手順を実行します。

1. **Device Posture > Device Scans** に移動し、**Settings** をクリックします。
2. **Periodic device posture scans** セクションで、トグルスイッチを「ON」にスライドして、デバイスの定期スキャンを有効にします。

Periodic device posture scans 

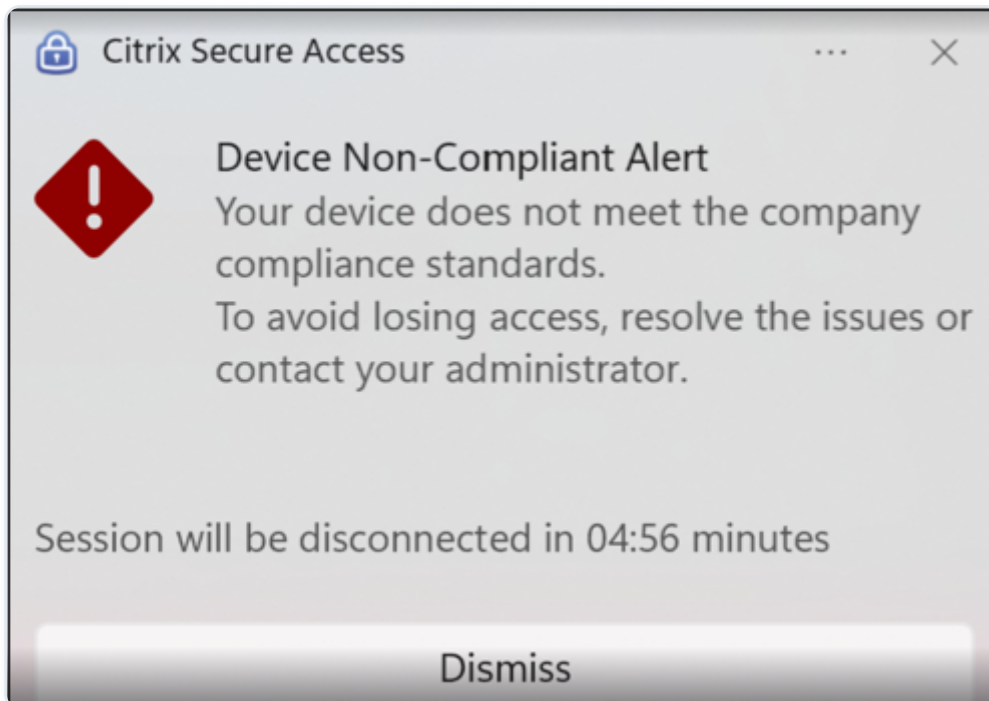
Check the end user's device posture, every 30 minutes. Currently supported only on windows end devices.

- HTTP/HTTPSアプリケーションの場合、デバイスポスチャスキャン結果が**準拠**から**非準拠**または**アクセス拒否**に変わると、リソースへのアクセスは新しいコンプライアンスステータスに従って更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

45

- Citrix Secure Accessクライアントから起動されたTCP/UDPアプリケーションの場合、デバイスポスチャスキャンでダウングレードが発生した場合（例えば、**準拠**から**非準拠**または**アクセス拒否**へ）、ユーザーは通知を受け取り、5分後にアクティブなセッションは終了します。



アクセス拒否のシナリオ向けカスタマイズメッセージ

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。

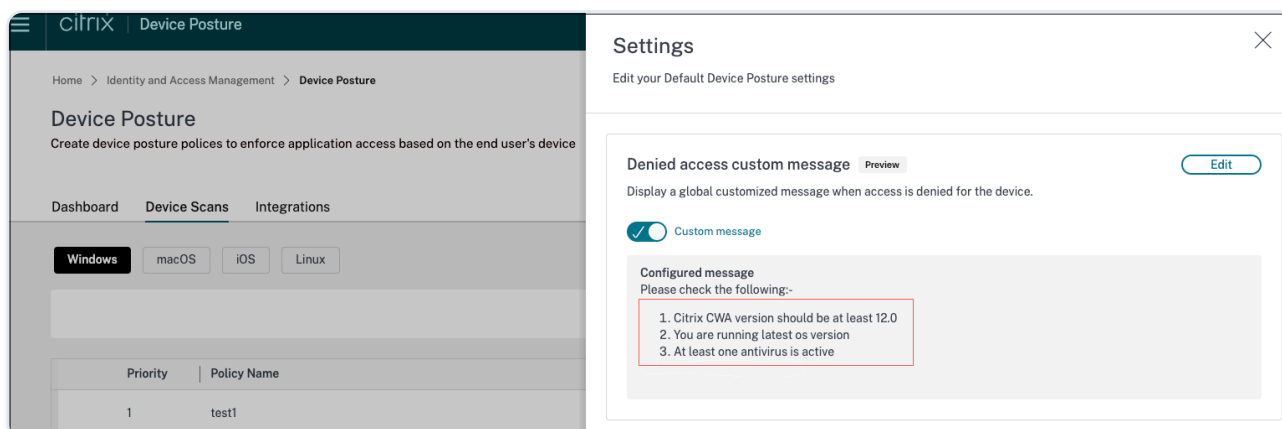
カスタマイズされたメッセージを追加するには、次の手順を実行します。

1. **Device Posture > Device Scans**ページに移動します。
2. **Settings**をクリックします。
3. **Edit**をクリックし、**Message**ボックスに、アクセス拒否のシナリオで表示されるべきメッセージを入力します。最大256文字まで入力できます。
4. **Enable custom message on save**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有効にします。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、アクセス拒否のシナリオでデバイスに表示されません。

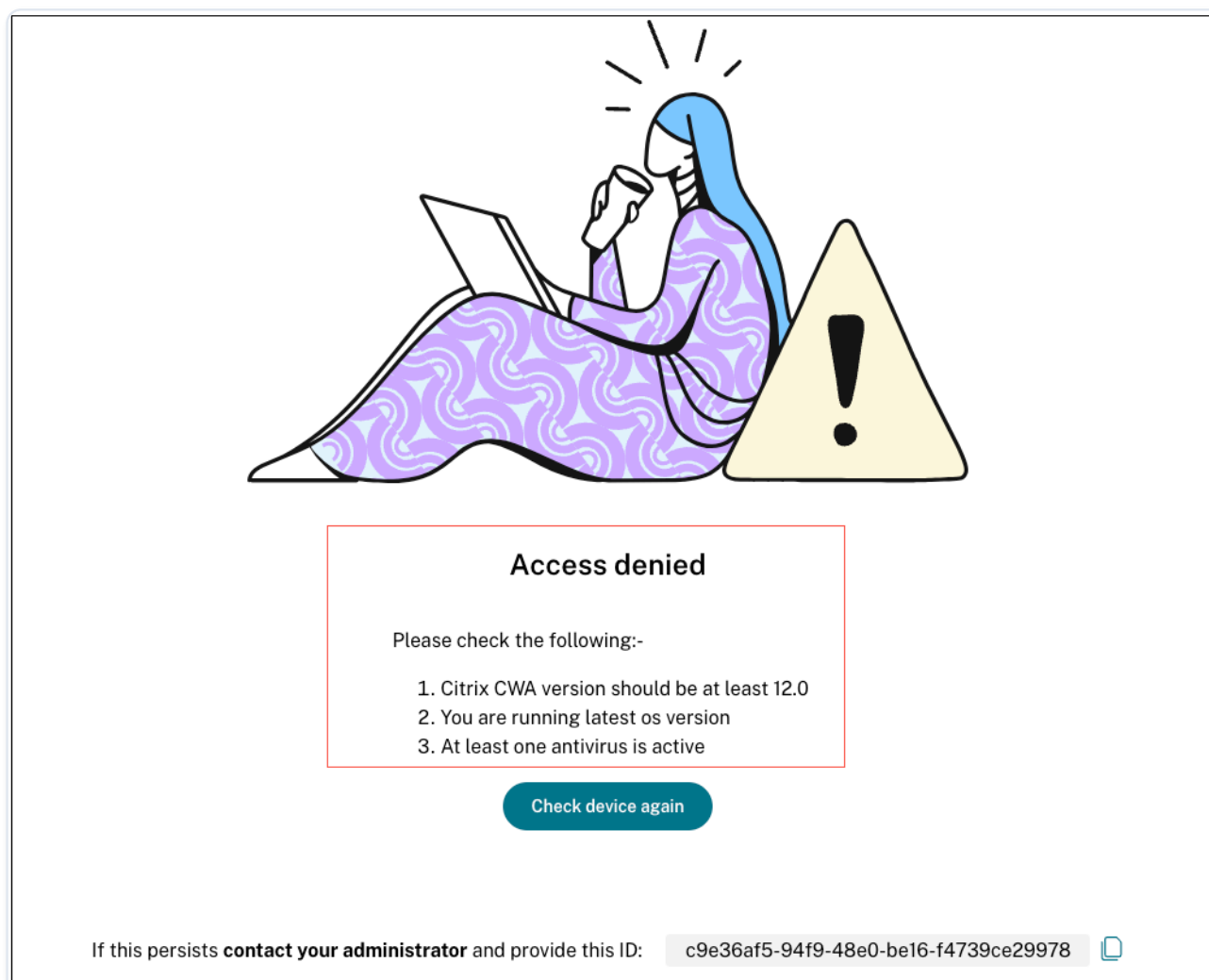
または、**Settings**ページで**Custom message**トグルスイッチを有効にして、デバイスにメッセージを表示することもできます。

5. **Save**をクリックします。

次の画像は、管理者によって追加されたサンプルメッセージを表示します。



次の画像は、アクセスが拒否されたときにエンドユーザーデバイスに表示されるカスタムメッセージを表示します。



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。

デバイスポスチャチェックをスキップする

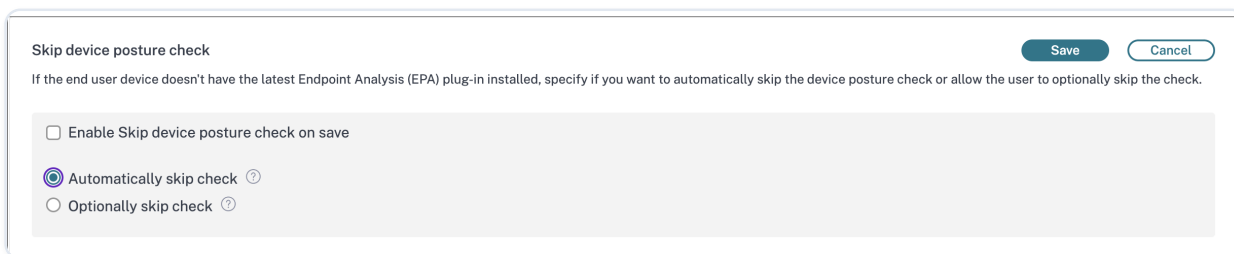
管理者は、デバイスポスチャチェックを自動的にスキップするように構成したり、以下のシナリオでエンドユーザーがスキップできるようにしたりできます。

- EPAクライアントがデバイスにインストールされていない。
- デバイスにインストールされているEPAクライアントが古くなっている。

スキップチェック機能が有効になっている場合、デフォルトのポリシー結果（非準拠）が適用され、デバイスは非準拠として分類されます。エンドユーザーには、Citrix Secure Private Access™ 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が提供されます。

デバイスポスチャチェックのスキップを有効にする

1. デバイスポスチャ > デバイススキャンに移動します。
2. **設定**をクリックします。
3. デバイスポスチャチェックをスキップセクションで、トグルスイッチを「ON」にスライドしてデバイスポスチャチェックのスキップを有効にし、**編集**をクリックします。



4. 次のいずれかのオプションを選択します。
 - **チェックを自動的にスキップ** - EPAクライアントがない、または古くなっている場合、システムはポスチャチェックを自動的にバイパスし、EPAクライアントのないデバイスからCitrix Workspaceにアクセスするユーザーのログインプロセスを効率化します。
 - **オプションでチェックをスキップ** - EPAクライアントのないデバイスからCitrix Workspaceにログインする際、ユーザーはポスチャチェックをスキップをクリックして、ポスチャチェックを手動でスキップするように求められます。

「**Optionally skip check**」オプションが有効で、エンドユーザーがCitrix Workspaceにログインしている場合、エンドユーザーがクライアントをダウンロードしようとしたり、EPAバージョンをアップグレードしようすると、次のメッセージが表示されます。

チェックをスキップするメッセージ(/en-us/device-posture/media/device-posture-end-user-flow4.png)

5. **保存**をクリックします。

カスタムワークスペースURLのサポート

Device Postureサービスでは、カスタムワークスペースURLがサポートされています。cloud.com URLに加えて、所有しているURLを使用してワークスペースにアクセスできます。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構成](#)」を参照してください。

Device Postureによるセッションレコーディングの構成

[セッションレコーディング](#)を使用すると、組織は仮想セッションでの画面上のユーザーアクティビティを記録できます。カスタムセッションレコーディングポリシー、イベント検出ポリシー、またはイベント応答ポリシーを作成する際にタグを指定できます。例については、「[カスタムレコーディングポリシーの作成](#)」を参照してください。

デバイス証明書チェック

Device Postureサービスでデバイス証明書チェックを構成するには、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。有効な発行者証明書がDevice Postureサービスに存在すると、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。

注意点:

- 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ています。
- Windowsでのデバイス証明書チェックの場合、エンドデバイスのEPAクライアントは管理者権限でインストールされている必要があります。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ているスキャン](#)」を参照してください。
- WindowsでEndpoint Analysisクライアントを管理者権限でインストールするには、クライアントがダウンロードされたフォルダーで、管理者として実行したコマンドプロンプトからコマンド `epasetup.exe /quiet` を実行します。ARM64デバイスでは、代わりに `epasetup_ARM64.exe /quiet` を実行します。
- 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。
- 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、ルート証明書と中間証明書を含む完全なチェーンを単一のPEMファイルで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

デバイス証明書のアップロード

1. Device Posture のホームページで、 をクリックします。
2. をクリックし、 をクリックします。

3. で、証明書タイプを選択します。PEM タイプのみがサポートされています。
4. で、 をクリックして発行者証明書を選択します。
5. をクリックし、 をクリックします。

Import Issuer Certificate

Issuer certificate will be added to the Endpoint. View certificate details in certificate table once created.

Certificate Type *

PEM (Privacy Enhanced Mail)

Certificate File *

cgwsanitydc.pem

+ Choose Certificate

Import

Cancel

選択した証明書は、 > に表示されます。複数の証明書をインポートできます。

インポートされた証明書の表示

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

Issuer Certificates

Issuer Certificates will be used to validate the device certificates as per the configured policies.

Import Issuer Certificate

Issuer	Certificates	Policies	Status	
cgwsanity-DC-CA	cgwsanitydc.pem	NA	Valid	↓ 🗑️
int-CA	combinedchain.pem	NA	Valid	↓ 🗑️

デバイス証明書チェックのスキャンを設定する

1. デバイスポスチャポリシーを設定します。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。
2. デバイス証明書チェックのポリシー ルールを追加する際は、**サンプリントの確認と発行者の両方**の条件を指定します。

重要:

環境内で複数のデバイス証明書が同じ発行者名を共有している場合、サービスが誤った証明書と一致するのを防ぐために、**サムプリントの確認オプション**を有効にする必要があります。このオプションが有効になっていない場合、サービスは発行者名のみで証明書を照合するため、発行者名が重複している場合にポリシーの競合が発生する可能性があります。

サムプリントを確認する(/en-us/device-posture/media/check-thumbprint.png)

エンドデバイスにデバイス証明書をインストールする

ウィンドウズ:

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。

- 目的には**クライアント認証**が含まれている必要があります。
- **発行者列**は、管理GUIで設定された発行者名と一致している必要があります。

証明書をインストールする(/en-us/device-posture/media/device-posture-install-certificate.png)

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 > 項目を読み込む**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。

証明書をインストール macOS(/en-us/device-posture/media/device-posture-install-certificate-macos.png)

許可されたドメインのリストを構成する

Device Postureサービスのスキャンを開始できるNetScaler Gateway仮想サーバーのFQDNを構成できます。

注:

- この機能は、Secure Private Access展開にのみ適用されます。
- Secure Private Access展開でこの機能を有効にするには、Citrixサポートにお問い合わせください。

1. **Device Posture > Device Scans**に移動し、次に、**Settings**をクリックします。
2. **NetScaler Gateway URL**で、Device Postureチェックを有効にする必要がある仮想サーバーのFQDNを入力します。例: `https://gw.example.net`。

デバイスポスチャチェック(/en-us/device-posture/media/device-posture-gateway-url.png)

この機能のサンプルユースケースについては、[Secure Private AccessハイブリッドソリューションのDevice Postureを有効にする](#)を参照してください。

NetScalerでデバイスポスチャスキャンを構成するには、[NetScaler GatewayでのDevice Postureチェック](#)を参照してください。

Device Posture サービスと Chrome Enterprise デバイス信頼コネクタの統合

Device Posture サービスは、Chrome Enterprise デバイス信頼コネクタと統合されています。この統合により、Citrix® 管理者はデバイスのポスチャ結果を Google Workspace と共有し、Chrome が管理対象デバイスのポスチャに基づいてコンテキストアウェアアクセスおよびデータ損失防止 (DLP) ポリシーを適用できるようになります。

Citrix が共有するポスチャシグナルは、Chrome によって以下のアクセス決定のために利用されません。

- 管理対象の Chrome ブラウザ
- 管理対象の Chrome プロファイル

Chrome がサードパーティコネクタから受信できるシグナルのリストについては、[Google のエンドポイント検証ドキュメント](#)を参照してください。

注:

Chrome Enterprise デバイス信頼コネクタとの統合は、Device Posture サービスがグローバルモードの場合にのみサポートされます。

サポートされるプラットフォームと展開

項目	サポート
サポートされるプラットフォーム	EPA クライアントバージョン 26.5.1.7 以降の Windows
展開	Citrix Enterprise Premium を使用した Secure Private Access サービス
	Secure Private Access ハイブリッド

前提条件

- Device Posture サービスのエンタイトルメントがあり、構成されている Citrix Cloud テナント。
- Google Workspace テナントと、Chrome Enterprise Premium (CEP) ライセンス、および Google 管理コンソールへのスーパー管理者権限。
- Chrome Enterprise Premium が顧客向けに展開されていること。
- Google 管理コンソールで **コンテキストウェアアクセス** のアクセスレベルが ON に設定されていること。詳細については、[推奨アクセスレベルの適用](#) を参照してください。

構成

Citrix Device Posture サービスと Chrome Enterprise Device Trust Connector の統合には、次の大まかな手順が含まれます。

1. [Chrome Enterprise Premium と Device Posture サービスを構成する](#)
2. [Citrix Device Posture サービスを Chrome デバイス信頼コネクタと統合する](#)
3. [Citrix シグナルに対するコンテキストウェアなルールを定義する](#)

Chrome Enterprise Premium と Device Posture サービスを構成する

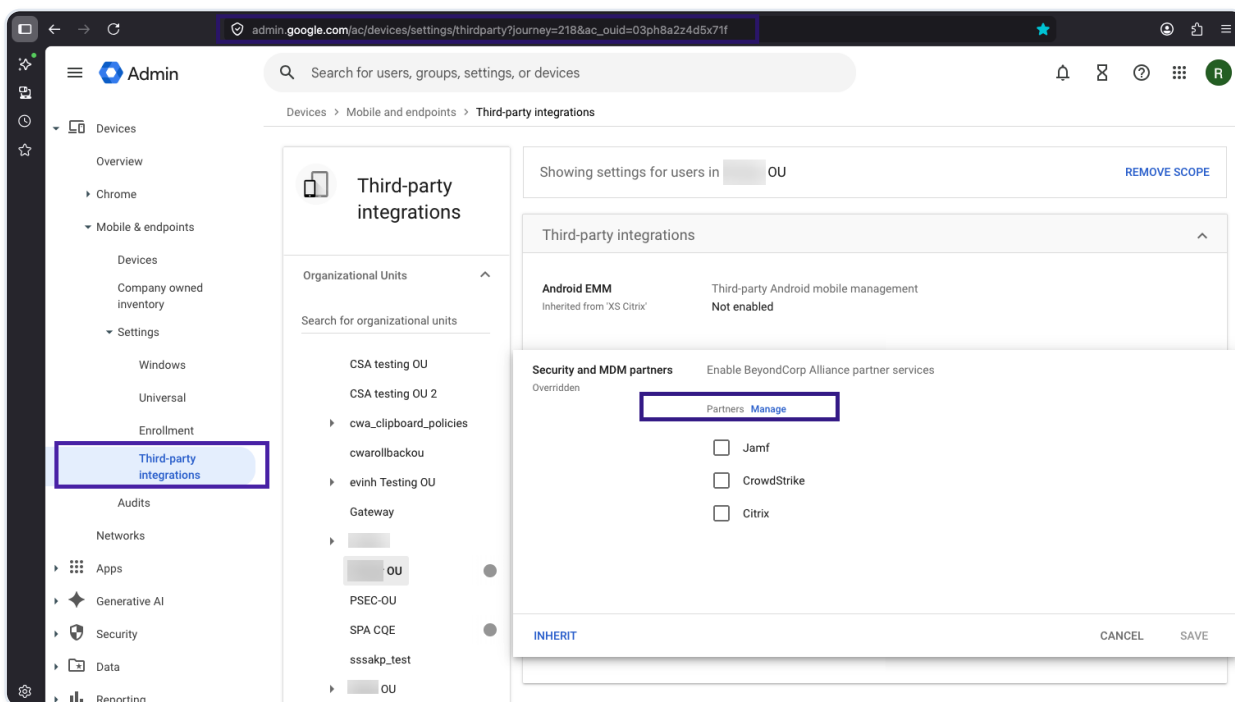
Chrome と統合する前に、以下の構成が完了していることを確認してください。

1. 管理対象の Windows エンドポイントに Chrome Enterprise Premium (CEP) を展開して構成します。詳細については、[Google Chrome Enterprise Premium との統合](#) を参照してください。
2. Chrome と共有する予定のシグナル (OS バージョン、ウイルス対策の状態、地理的または承認された国、カスタムチェックなど) を生成する Device Posture サービスポリシーを構成します。詳細については、[Device Posture ポリシーの構成](#) を参照してください。
3. Google Workspace テナントに Chrome Enterprise Premium (CEP) ライセンスがあることを確認します。これは、Device Trust Connector とコンテキストウェアアクセスルールを使用するために必要です。詳細については、[ライセンス、アプリのバージョン、拡張機能](#) を参照してください。

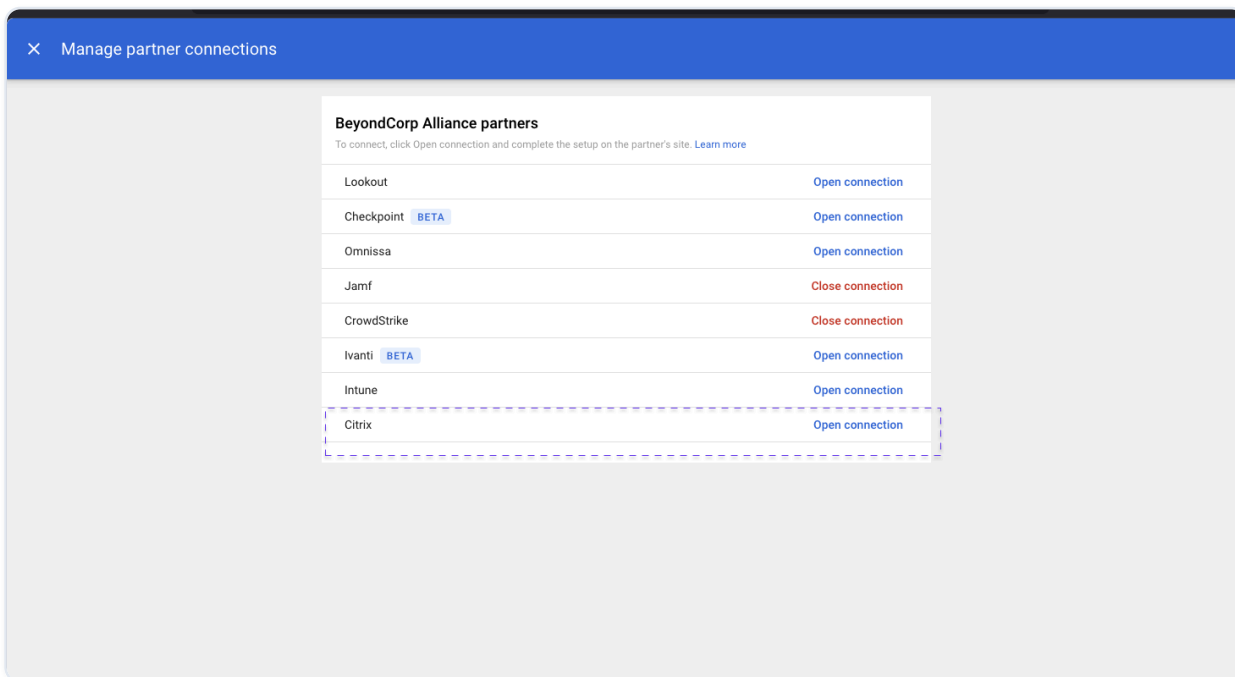
Citrix Device Posture サービスを Chrome デバイス信頼コネクタと統合する

Citrix Device Posture サービスを Chrome デバイス信頼コネクタと統合するには、Google 管理コンソールでサードパーティコネクタを有効にする必要があります。

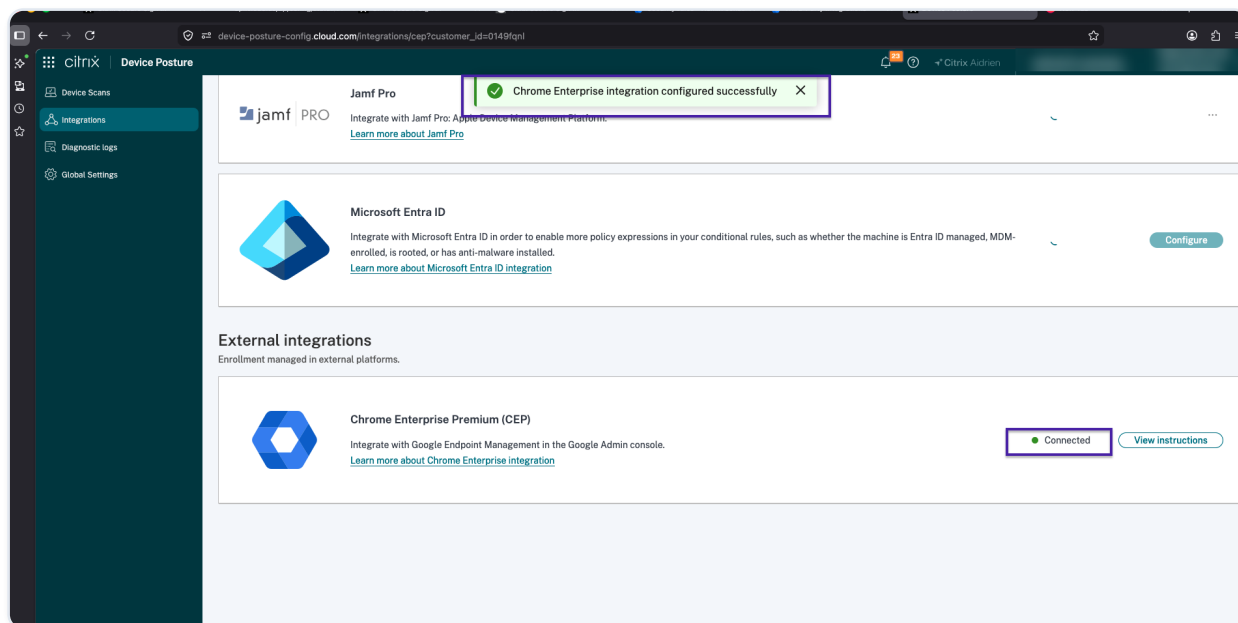
1. スーパー管理者として Google 管理コンソールにサインインします。
2. デバイス > モバイルとエンドポイント > 設定 > サードパーティ統合に移動します。



3. パートナリストで**Citrix**を見つけて、**管理**をクリックします。
4. 画面の指示に従って、Citrix CloudテナントとGoogle Workspace間の接続を承認します。



ハンドシェイクが成功すると、Citrixの統合ステータスが**接続済み**に変わります。



詳細については、「サードパーティパートナー統合のセットアップ」を参照してください。

Citrixシグナル用のコンテキストウェアナールールを定義する

Google WorkspaceのコンテキストウェアナアクセスおよびDLPルールは、Common Expression Language (CEL) を使用して記述されます。Citrixのポスチャデータは、

`device.vendors["Citrix"].data[...]` 名前空間の下で公開されます。

詳細については、以下のトピックを参照してください。

- サードパーティパートナー統合のセットアップ
- DLPルールとコンテキストウェアナアクセス条件を組み合わせる

Citrixシグナルキー

次のキーは、Citrix Device PostureサービスによってChromeデバイス信頼コネクタに公開されます。

キー	説明	例の値
OVERALL_OUTCOME	エンドポイントに対してDevice Postureサービスから返される集計ポスチャ結果。	準拠、非準拠、拒否
∧	∧	注: 値は大文字と小文字を区別します。上記のとおり正確に入力してください。

キー	説明	例の値
OVERALL_OUTCOME_CONTEXT_NAME	全体的な結果を導き出した Device Postureサービスのポリシーまたはコンテキストの名前。	AUTHORIZED_COUNTRY, AV_STATUS, OS_VERSION, Google-DTC-Demo-Deny, (カスタムポリシー名)
シトリックス-デバイスID	Citrix Device Postureサービスに登録されているエンドポイントの一意の識別子。	6c813458-c27b-4299-87c6-55832a95ae7e
Citrix-トランザクションID	シグナルを生成したポスチャ評価トランザクションの一意の識別子。	75b1e3f6-4224-484a-8c47-9a35c4e5eabd

注:

- 正確なコンテキスト名は、[ステップ 1](#)で Device Postureサービスに定義したポリシーによって異なります。
- Citrix-DeviceIdとCitrix-TransactionIdは関連識別子です。これらはポリシー決定での使用を意図していません。Citrix Device Postureダッシュボードでトラブルシューティングを行う際に、特定の結果を生成した正確なスキャンを検索するために使用します。

Citrix 向け 共通式言語 (CEL) の例

例 1 — Citrix が非準拠を報告した場合にアクセスをブロックする:

Citrix の全体的な結果が非準拠である場合、Google Workspace アプリへのアクセスを拒否します。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

この式を、アクションが**ブロック**に設定されたコンテキストアウェアアクセスレベルで使用します。

例 2 — 非準拠が不正な国によって引き起こされた場合にのみブロックする:

結果をコンテキスト名と組み合わせて、ルールを地理的違反に限定します。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant" &&  
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] ==  
"AUTHORIZED_COUNTRY"
```

例 3 — Citrix が準拠を報告した場合にのみアクセスを許可する:

Device Posture サービスが明示的に準拠結果を返す場合にのみアクセスを許可します (フェイルクローズ)。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant"
```

例 4 — DLP: 非準拠デバイスでのファイルダウンロードを防止する:

Google Drive の DLP ルールで、非準拠エンドポイントからのデータ流出をブロックするために、ダウンロード/印刷/コピー トリガーに次の条件を付加します。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant"
```

例 5 — 複数の Citrix コンテキストを持つ階層型ポリシー:

アンチウイルスまたは OS バージョンのいずれかでポスチャが失敗した場合はブロックしますが、その他の非準拠の理由は、別の制限の少ないルールで処理できるようにします。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Non-Compliant" &&  
( device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "AV_STATUS" ||  
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "OS_VERSION" )
```

例 6 — 指定された Device Posture サービスポリシーからの明示的な拒否結果をブロックする:

特定のデバイスポスチャサービスポリシーによって生成された正確な拒否結果と一致させます (例: 概念実証中に使用された Google-DTC-Demo-Deny ポリシー):

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Deny" &&  
device.vendors["Citrix"].data["OVERALL_OUTCOME_CONTEXT_NAME"] == "Google-DTC-  
Demo-Deny"
```

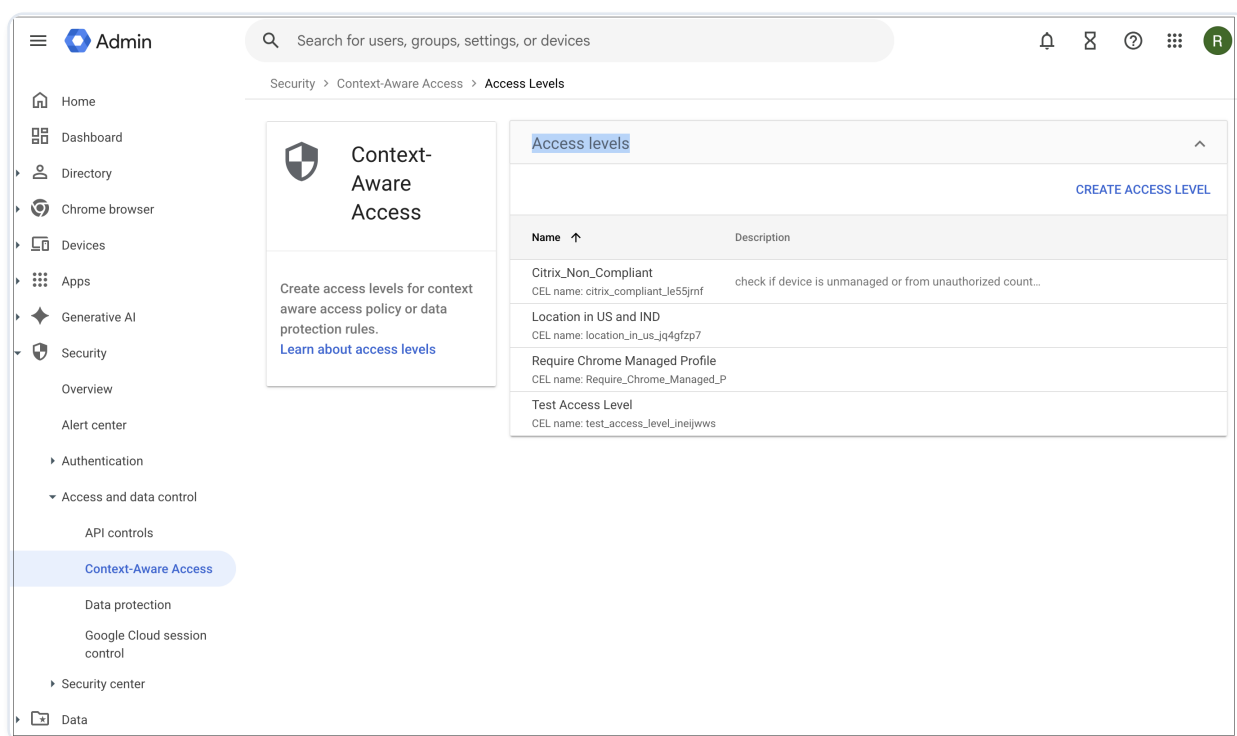
例 7 — CitrixポスチャとGoogleネイティブシグナルを組み合わせる:

Citrixシグナルは、組み込みのChrome / エンドポイント検証属性と組み合わせることができます。

```
device.vendors["Citrix"].data["OVERALL_OUTCOME"] == "Compliant" &&  
device.encryption_status == ENCRYPTED && device.os_version.major >= 10
```

ルールを適用するには

1. Google管理コンソールで、セキュリティ > アクセスとデータ制御 > コンテキストウェアアクセス (または DLP のデータ保護) に移動します。
2. アクセスレベル (または DLP ルール) を作成し、CEL式を詳細 / 条件エディターに貼り付けます。



3. アクセスレベルを対象のGoogle Workspaceアプリ (Drive、Gmailなど) および関連する組織部門またはグループに割り当てます。
4. 保存して展開します。伝播に数分かかります。

統合を検証する

1. CEPを実行している管理対象のWindowsエンドポイントから、意図的にデバイスポスチャサービスのスキャンを失敗させます (例: 許可されていない国からサインインするか、アンチウイルスを無効にする)。
2. そのエンドポイント上のChromeブラウザまたはプロファイルから、保護されたGoogle Workspaceアプリへのアクセスを試みます。
3. ChromeがCELルールで定義されたアクション (ブロック、警告、許可) を適用することを確認します。
4. レポート > 監査と調査 > アクセスの透明性 / ルールログイベント の監査ログを確認し、Citrix シグナルが評価されたことを確認します。

トラブルシューティング

症状	可能性のある原因	解決策
統合ステータスが「未接続」のままになる	OAuth/管理者による同意が完了していない	スーパー管理者アカウントで ステップ2 を再実行する
ルールが一致しない	CELキー名の入力ミス、またはDevice Postureサービスでポリシーが有効になっていない	管理コンソールのルールログイベントでキーを確認します。Device Postureサービスでポリシーがアクティブであることを確認します。
エンドポイントでシグナルが欠落している	CEPがインストールされていない、またはユーザーがサインインしていない	エンドポイントでのCEP展開とDevice Postureサービスへの登録を確認します。
予期しない非準拠または拒否	別のDevice Postureサービスポリシーが失敗している	失敗しているチェックを特定するために OVERALL_OUTCOME_CONTEXT_NAMEを検査します。

注:

特定のアクセス決定を調査する必要がある場合は、Chrome / Workspace監査ログから `Citrix-DeviceId` と `Citrix-TransactionId` をキャプチャし、Citrix Device Postureダッシュボードでそれらを検索して、完全なスキャン結果、ポリシーヒット、およびタイムスタンプを表示します。

トラブルシューティングのための Citrix-DeviceId と Citrix-TransactionId の使用

Chrome のアクセスまたは DLP の決定を調査する必要がある場合:

1. **Google 管理コンソール** > **レポート** > **監査と調査** > **ルールログイベント (またはアクセス透過性ログ)** を開き、関連するイベントを見つけます。
2. イベントペイロードで報告された `Citrix-DeviceId` と `Citrix-TransactionId` の値をコピーします。
3. **Citrix Cloud** > **Device Posture** > **ダッシュボード** にサインインします。

4. デバイス ID で検索して、エンドポイントの登録、OS、および最近のスキャン履歴を表示します。
5. トランザクション ID で検索して、正確なスキャンインスタンスを表示します。これには、評価されたポリシー、収集されたシグナル、および Chrome に送信された結果の OVERALL_OUTCOME と OVERALL_OUTCOME_CONTEXT_NAME が含まれます。

この関連付けにより、予期しない Chrome の決定が Citrix のポスチャ結果、CEL 式、または Workspace ポリシーバインディングのいずれによって引き起こされたかを確認できます。

制限事項

ホストあたり最大 10 個の Google リソース ID を、Citrix Device Posture サービスから Chrome デバイス信頼コネクタにプッシュできます。

ホストあたり 10 個を超える Google リソース ID にデバイスポスチャシグナルをプッシュするには、Citrix サポートに連絡して拡張をリクエストしてください。

Device Postureサービス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、Device Posture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も統合できます。

- [マイクロソフト エントラ ID](#)
- [ジャムフ プロ](#)
- [マイクロソフト Intune](#)
- [CrowdStrike](#)

Microsoft Entra IDとDevice Postureサービスの統合

Microsoft Entra ID統合により、Citrix®は、Microsoft Entra IDに統合されているモバイルデバイス管理 (MDM) ソリューションに関係なく、すべてのMicrosoft Entra ID登録デバイスで一貫して機能する統合コンプライアンスワークフローをサポートします。

システム要件

- サポートされているプラットフォーム: Windows
- WindowsでサポートされているEPAクライアントバージョン: 26.3.1.10以降

マイクロソフト Entra ID API 権限

次の表に、Device Postureサービスとの統合に必要なMicrosoft Entra ID API権限を示します。

API名	クレーム値	権限名	タイプ
マイクロソフト グラフ	Devices.Read.All	すべてのデバイスを 読み取る	アプリケーション
マイクロソフト グラフ	User.Read	サインインしてユー ザープロファイルを 読み取る	委任

注:

- 特権ロール管理者とグローバル管理者のみがアプリケーション権限を付与できます。
- Device PostureサービスはEntra IDデバイスの詳細を取得するためにアプリケーション権限のみを必要としますが、最初の管理者付与フローは個人によって実行される対話型プロセスです。
- Microsoft Entra IDにデフォルトで含まれている `User.Read (Delegated)` 権限は、付与フロー中に管理者のIDを検証します。これにより、Device Postureサービスに必要なアプリケーションレベルのアクセスを、承認されたロール（グローバル管理者または特権ロール管理者）のみが付与することが保証されます。

Entra ID連携を構成する

Entra ID 統合の設定は2段階のプロセスです。

1. Citrix Device PostureサービスとMicrosoft Entra ID間の信頼を確立する。これは、Device PostureとMicrosoft Entra ID間の信頼を確立するために一度だけ行うアクティビティです。
2. Microsoft Entra IDコンプライアンス情報を使用するようにポリシーを構成する。

Citrix Device PostureサービスとMicrosoft Entra ID間の信頼を確立する

Citrix Device PostureサービスとMicrosoft Entra ID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、メニューから**Identity and Access Management**を選択します。
2. **Device Posture**タブをクリックし、**Manage**をクリックします。
3. **Integrations**タブをクリックします。

Configure integrations from the available options below.



Microsoft Intune

Integrate with Microsoft Intune in order to enable more policy expressions in your conditional rules, such as whether the machine is Azure AD-managed, MDM-enrolled, is rooted, or has anti-malware installed.
[Learn more about Microsoft Intune integration](#)

● 2 accounts configured Manage



CrowdStrike Falcon® Insight XDR

Integrate with CrowdStrike's Falcon Insight XDR: Endpoint Detection and Response (EDR) platform.
[Learn more about CrowdStrike Falcon® Insight XDR](#)

○ Not Configured Configure



Jamf Pro

Integrate with Jamf Pro: Apple Device Management Platform.
[Learn more about Jamf Pro](#)

○ Not Configured Configure



Microsoft Entra ID

Integrate with Microsoft Entra ID in order to enable more policy expressions in your conditional rules, such as whether the machine is Entra ID managed, MDM-enrolled, is rooted, or has anti-malware installed.
[Learn more about Microsoft Entra ID integration](#)

○ Not Configured Configure

注:

または、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、**Integrations** タブをクリックすることもできます。

- Microsoft Entra IDボックス内の省略記号ボタンをクリックし、**Configure**をクリックします。**Microsoft Entra ID** ペインが表示されます。
- プロファイルの名前を入力し、**Connect account**をクリックします。
- Done**をクリックします。

Microsoft Entra IDセクションには、正常に構成されたアカウントの数と問題のあるアカウントの数が表示されます。問題を解決するには、プロファイル名ドロップダウンリストから影響を受けるプロファイルを選択し、アカウントを再接続します。

Microsoft Entra ID連携のためのデバイスポスチャポリシーを構成する

- デバイスポスチャポリシーを構成します。詳細については、「[デバイスポスチャポリシーの構成](#)」を参照してください。
- ポリシー規則で、**Microsoft Entra ID**を選択します。
- 条件を選択し、一致させる値を選択します。
 - **準拠** - デバイスがMicrosoft Entra IDで構成されたコンプライアンスポリシーを満たしているかを確認します。

- **管理対象** - デバイスがMicrosoft Entra IDに登録されているかを確認します。

注:

この規則は、デバイスポスチャ用に構成する他の規則と組み合わせて使用できます。

4. ポリシー構成を完了し、**作成**をクリックします。

Jamf Proとデバイスポスチャサービスの連携

Appleモバイルデバイス管理 (MDM) ソフトウェアおよびセキュリティプロバイダーであるJamf Proは、組織がAppleデバイスを構成および保護するのに役立ちます。

重要:

- macOS版Citrix Secure Accessクライアントバージョン24.9.6は、Jamf Pro連携をサポートしています。
- iOSデバイスでJamf Proとデバイスポスチャの連携を機能させるには、管理者はJamf ProポータルからCitrix Workspace™アプリをプッシュする必要があります。詳細については、「[Jamf ProポータルからCitrix Workspaceアプリをプッシュする](#)」を参照してください。

Jamf Pro連携を構成する

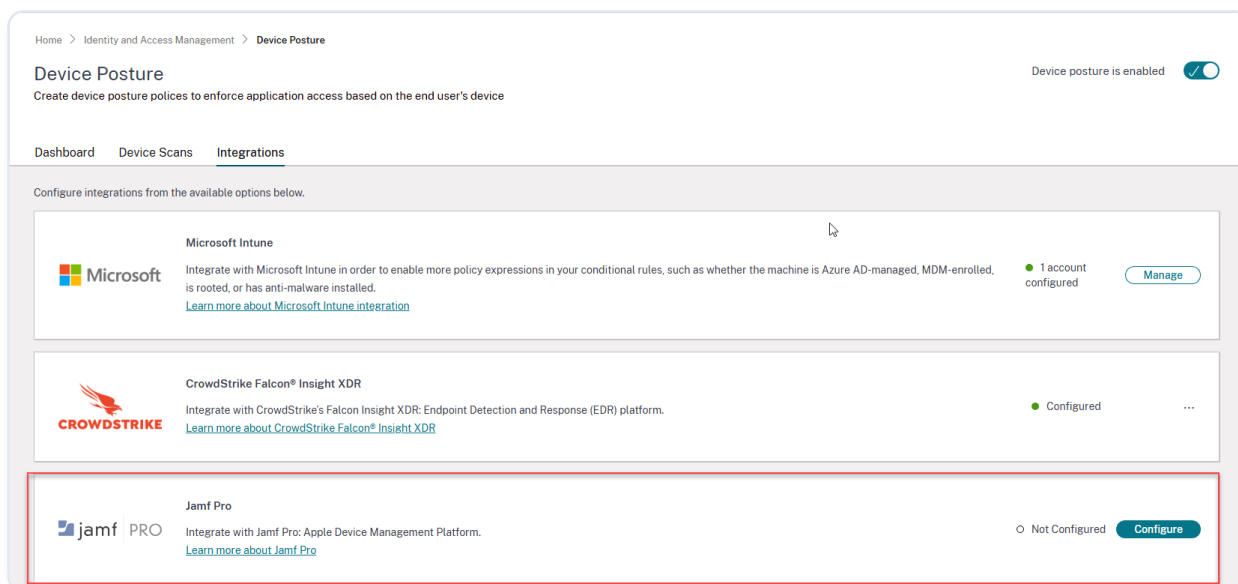
Jamf Pro連携の設定は2段階のプロセスです。

1. [Citrix Device PostureサービスとJamf Proサービス間の信頼を確立する](#)。
2. [Jamf Pro情報を使用するようにポリシーを構成する](#)。

Citrix Device PostureサービスとJamf Proサービス間の信頼を確立する

Citrix Device PostureサービスとJamf Pro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、メニューから**Identity and Access Management**を選択します。
2. **Device Posture**タブをクリックし、**Manage**をクリックします。
3. **Integrations**タブをクリックします。

**注:**

または、Secure Private Accessサービスの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、**Integrations** タブをクリックすることもできます。

4. Jamf Proボックスの省略記号ボタンをクリックし、**Connect**をクリックします。**Configure Jamf Pro Integration** ペインが表示されます。
5. クライアントID、クライアントシークレット、およびJamf Pro URLを入力し、**Save**をクリックします。

注:

- APIクライアントIDはJamf Proポータルから取得できます。
- 信頼を確立するために、読み取り権限を持つ**Read Computers**および**Read Mobile Devices** スコープを選択していることを確認してください。
- Jamf Pro URLは、各顧客アカウントに対してJamfによって提供されます。Jamf Pro URLは `https://<organization name>.jamfcloud.com` の形式です。

ステータスが**未設定**から**設定済み**に変わると、統合は成功したと見なされます。

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。

Jamf Pro統合のデバイスポスチャポリシーを構成する

1. デバイスポスチャポリシーを構成します。詳細については、[デバイスポスチャポリシーの構成](#)を参照してください。
2. **ポリシー規則**で、**Jamf Pro**を選択します。
3. 条件を選択し、一致させる値を選択します。
 - **自動登録済み** - 初期設定中にAppleデバイスがJamfシステムに自動的に登録されているかどうかを確認します。
 - **管理済み** - デバイスがJamf Proによって管理されているかどうかを確認します。
 - **最終連絡からの時間** - macOSのみに適用されます。デバイスがJamf Proサーバーと最後に通信してからの時間（分単位）を確認します。
 - **最終インベントリ更新からの時間** - iOSのみに適用されます。デバイスがJamf Proと最後に通信してインベントリデータを更新してからの時間（分単位）を確認します。
4. 追加の修飾子を追加するには、+をクリックします。

注:

このルールは、デバイスポスチャ用に構成する他のルールと組み合わせて使用できます。

5. ポリシー設定を完了し、**作成**をクリックします。

Jamf ProポータルからiOSデバイスにCitrix Workspaceアプリをプッシュする

iOSデバイスでのDevice PostureとJamf Proの統合をサポートするために、管理者はJamf ProポータルからiOSデバイスにCitrix Workspaceアプリをプッシュする必要があります。次の手順を実行します。

1. Jamf Pro MDMにサインインします。
2. 管理するCitrix Workspaceアプリを追加します。
3. App Storeでアプリをリンクします。
4. アプリのアプリ構成ポリシーを作成します。
5. 次のXMLをアプリ構成に追加します。

```
<dict>

<key>UDID</key>

<string>$UDID</string>

</dict>
```

Microsoft IntuneとDevice Postureサービスの統合

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または登録済みとして分類します。Citrix Workspaceへのユーザーログイン中に、デバイスポスチャはMicrosoft Intuneにユーザーのデバイスステータスを照会し、この情報を使用してCitrix Cloud内のデバイスを準拠、非準拠（部分アクセス）、またはユーザーログインページへのアクセス拒否として分類できます。Citrix DaaS™やCitrix Secure Private Access™などのサービスは、デバイスポスチャのデバイス分類を利用して、それぞれ仮想アプリとデスクトップ、SaaSおよびWebアプリへのコンテキストアクセス（Smart Access）を提供します。

複数のMicrosoft IntuneアカウントとDevice Postureの統合

Device Postureサービスは、最大5つのMicrosoft Intuneアカウントの統合をサポートしています。これにより、複数のIntuneテナントを持つ組織（多くの場合、合併、買収、または部門の細分化の結果）は、すべての環境でデバイスポスチャをシームレスに管理できます。

複数のIntuneアカウントをDevice Postureサービスと統合する主な利点は次のとおりです。

- 一元化されたデバイスポスチャ管理: 複数のIntuneテナントにわたるデバイスのポスチャを、単一のDevice Postureコンソールから管理します。
- 合理化された管理: 異なるDevice Postureインスタンス間を切り替えたり、各Intuneアカウントの個別の構成を管理したりする必要がなくなります。
- 視認性の向上: どのIntuneテナントによって管理されているかに関わらず、すべてのデバイスのセキュリティポスチャの統合されたビューを取得します。

- 柔軟性の向上: 複雑なIT環境と複数のIntune展開を持つ組織をサポートします。

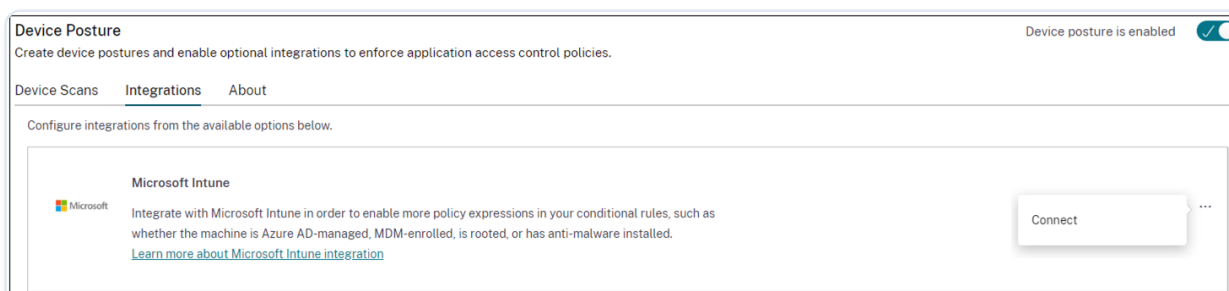
Microsoft Intune統合を構成する

Intune統合の構成は2段階のプロセスです。

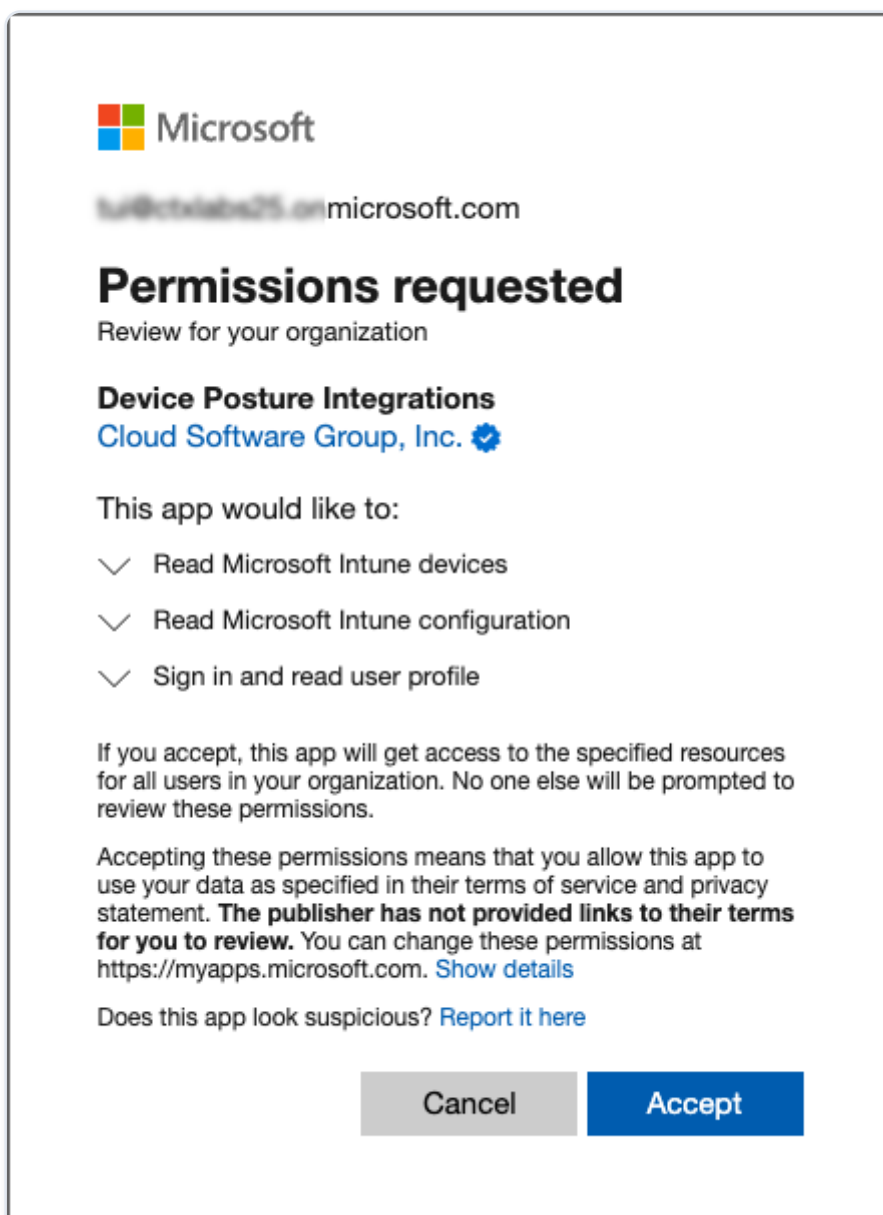
1. デバイスポスチャをMicrosoft Intuneサービスと統合する。これは、Device PostureとMicrosoft Intune間の信頼を確立するために一度だけ行うアクティビティです。
2. Microsoft Intune情報を使用するようにポリシーを構成する。

デバイスポスチャをMicrosoft Intuneと統合する

1. 統合タブにアクセスするには、次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、その後、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、その後、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、その後、接続をクリックします。管理者は認証のためにAzure ADにリダイレクトされます。



複数のMicrosoft IntuneアカウントをDevice Postureと統合する

1. 統合ページで、Microsoft Intuneセクションの**管理**をクリックします。
2. 「プロファイル名」に、Microsoft Intuneアカウントに接続するためのプロファイル名を入力します。
3. 「アカウントを接続」をクリックします。

Microsoft Intune

Create up to 5 Intune account profiles and connect to an account using your login credentials.

Profile name

Account2

Connect account

Account1

● Configured

Tenant ID xxxxxxxx-xxxx-xxxx-xxxx-e7fc8e4fe5f7

test

● Pending

Tenant ID N/A

Done

接続が確立されると、ステータスは「設定済み」と表示され、アカウントに関連付けられたテナントIDが表示されます。

4. 「完了」をクリックします。

Microsoft Intuneセクションには、正常に設定されたアカウントの数と、問題のあるアカウントの数が表示されます。問題を解決するには、「プロファイル名」ドロップダウンリストから影響を受けるプロファイルを選択し、アカウントを再接続します。

Citrix | Device Posture

Device Scans

Integrations

Diagnostic logs

Configure integrations from the available options below.

Microsoft

Microsoft Intune

Integrate with Microsoft Intune in order to enable more policy expressions in your conditional rules, such as whether the machine is Azure AD-managed, MDM-enrolled, is rooted, or has anti-malware installed.
[Learn more about Microsoft Intune integration](#)

2 accounts configured

1 account needs attention

Manage

CrowdStrike

CrowdStrike Falcon® Insight XDR

Integrate with CrowdStrike's Falcon Insight XDR: Endpoint Detection and Response (EDR) platform.
[Learn more about CrowdStrike Falcon® Insight XDR](#)

Not Configured

Configure

Jamf PRO

Jamf Pro

Integrate with Jamf Pro: Apple Device Management Platform.
[Learn more about Jamf Pro](#)

Not Configured

Configure

統合ステータスが「未設定」から「設定済み」に変わると、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、その後「再接続」をクリックする必要があります。

Microsoft Intune API の権限

次の表に、Device Postureサービスとの統合のためのMicrosoft Intune APIの権限を示します。

API名	クレーム値	権限名	タイプ
マイクロソフト グラフ	DeviceManagement ManagedDevices.Read.All	Microsoft Intune デバイスの読み取り	アプリケーション
マイクロソフト グラフ	DeviceManagement ServiceConfig.Read.All	Microsoft Intune デバイスの読み取り	アプリケーション
マイクロソフト グラフ	User.Read	サインインしてユーザープロファイルを読み取る	委任

注:

- アプリケーションのアクセス許可を付与できるのは、特権ロール管理者とグローバル管理者のみです。
- Device Posture サービスは Entra ID デバイスの詳細を取得するためにアプリケーションのアクセス許可のみを必要としますが、最初の管理者付与フローは個人によって実行される対話型プロセスです。
- Microsoft Entra ID にデフォルトで含まれている `User.Read (Delegated)` 権限は、付与フロー中に管理者のIDを検証します。これにより、承認された役割 (グローバル管理者または特権ロール管理者) のみが、Device Posture サービスに必要なアプリケーションレベルのアクセスを付与できるようになります。

Intune 統合のためのデバイスポスチャポリシーを構成する

1. デバイスポスチャポリシーを構成します。詳細については、「[デバイスポスチャポリシーの構成](#)」を参照してください。
2. **ポリシー規則**で、**Microsoft Intune**を選択します。
3. 条件を選択し、一致させる値を選択します。
 - **管理対象** - デバイスがIntuneに登録されていることを示します。
 - **準拠** - デバイスがIntune管理センターでIntune管理者が設定したコンプライアンスポリシーを満たしていることを示します。

注:

このルールは、デバイスポスチャ用に構成する他のルールと組み合わせて使用できません。

4. ポリシー構成を完了し、**作成**をクリックします。

CrowdStrike と Device Posture サービスの統合

CrowdStrike Zero Trust Assessment (ZTA) は、各エンドデバイスに対して1から100までのZTAセキュリティスコアを計算することで、セキュリティポスチャ評価を提供します。ZTAスコアが高いほど、エンドデバイスのポスチャが良好であることを意味します。

Citrix Device Posture Service は、エンドデバイスのZTAスコアを使用することで、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として分類できます。この分類は、組織が仮想アプリとデスクトップ、SaaSおよび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 統合を構成する

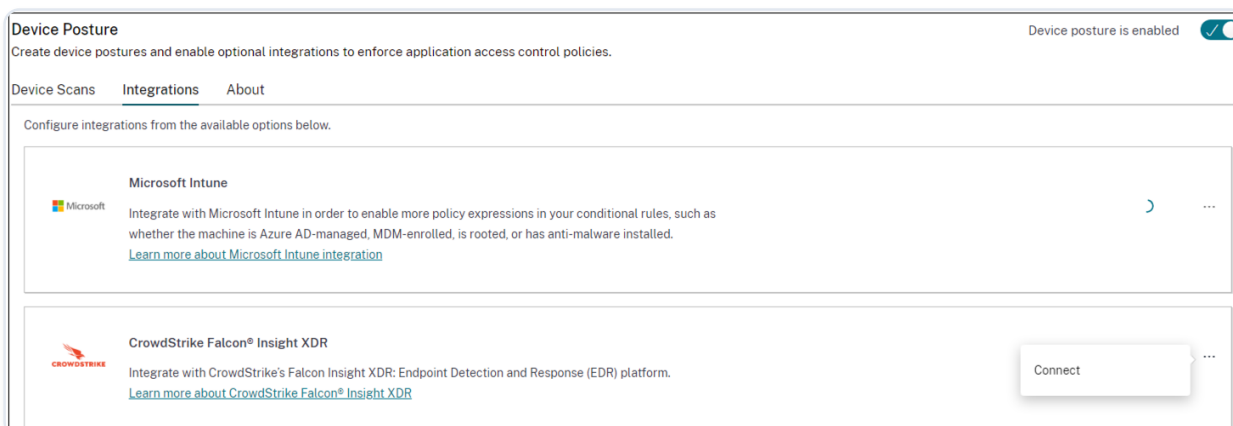
CrowdStrike統合の構成は2段階のプロセスです。

1. Citrix Device PostureサービスとCrowdStrike ZTAサービス間の信頼を確立する(/ja-jp/device-posture/device-posture-third-party-integrations.html#establish-trust-between-citrix-device-posture-service-and-crowdstrike-zta-service)。これは一度限りのアクティビティです。
2. アクセス ポリシーを構成する(/ja-jp/device-posture/device-posture-third-party-integrations.html#configure-device-posture-policies-for-crowdstrike-integration)。アクセス ポリシーは、CrowdStrike ZTAスコアをルールとして使用し、Citrix DaaSおよびCitrix Secure Private Accessリソースへのスマートなアクセスを提供します。

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****を選択します。
2. **タブをクリックし、**をクリックします。
3. ****タブをクリックします。



注：

または、Secure Private AccessサービスGUIの左側のナビゲーションペインで**オプションに移動し、**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、****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、****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（>）から取得できます。
- 信頼を確立するために、**Zero Trust Assessment** および **Host** スコープを読み取り権限で選択していることを確認してください。

ステータスが**未構成**から**構成済み**に変わると、統合は成功と見なされます。

統合が成功しない場合、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。

CrowdStrike統合のデバイスポスチャポリシーを構成する

CrowdStrike ZTAスコアをルールとして使用し、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ためのポリシーを構成するには、以下の手順を実行します。

1. デバイスポスチャポリシーを構成します。詳細については、「[デバイスポスチャポリシーの構成](#)」を参照してください。
2. **ポリシー規則**で、**CrowdStrike**を選択します。
3. **リスクスコア修飾子**について、条件を選択し、リスクスコアを入力します。
4. CrowdStrike Falconセンサーが実行されているかどうかをチェックする修飾子を追加するには、****+****をクリックします。

注：

このルールは、デバイスポスチャ用に構成する他のルールと組み合わせて使用できます。

5. ポリシー構成を完了し、**作成**をクリックします。

サードパーティ統合障害通知

Device Postureサービスは、Microsoft Intune、CrowdStrike、Jamf Proなどのサードパーティソリューションと統合されています。これらのサードパーティクラウドサービスのダウンタイムやエラーは、予期しないデバイスポスチャスキャン結果につながる可能性があります。この機能は、

サードパーティ統合障害が発生した場合に管理者へメール通知を提供します。これらのエラーは、Secure Private AccessおよびDevice Postureサービスのダッシュボードにも表示されます。これにより、お客様は関連するエラー情報を持ってサードパーティサービスサポートに直接連絡でき、Citrixサポートを介さずにダウンタイムを削減できます。

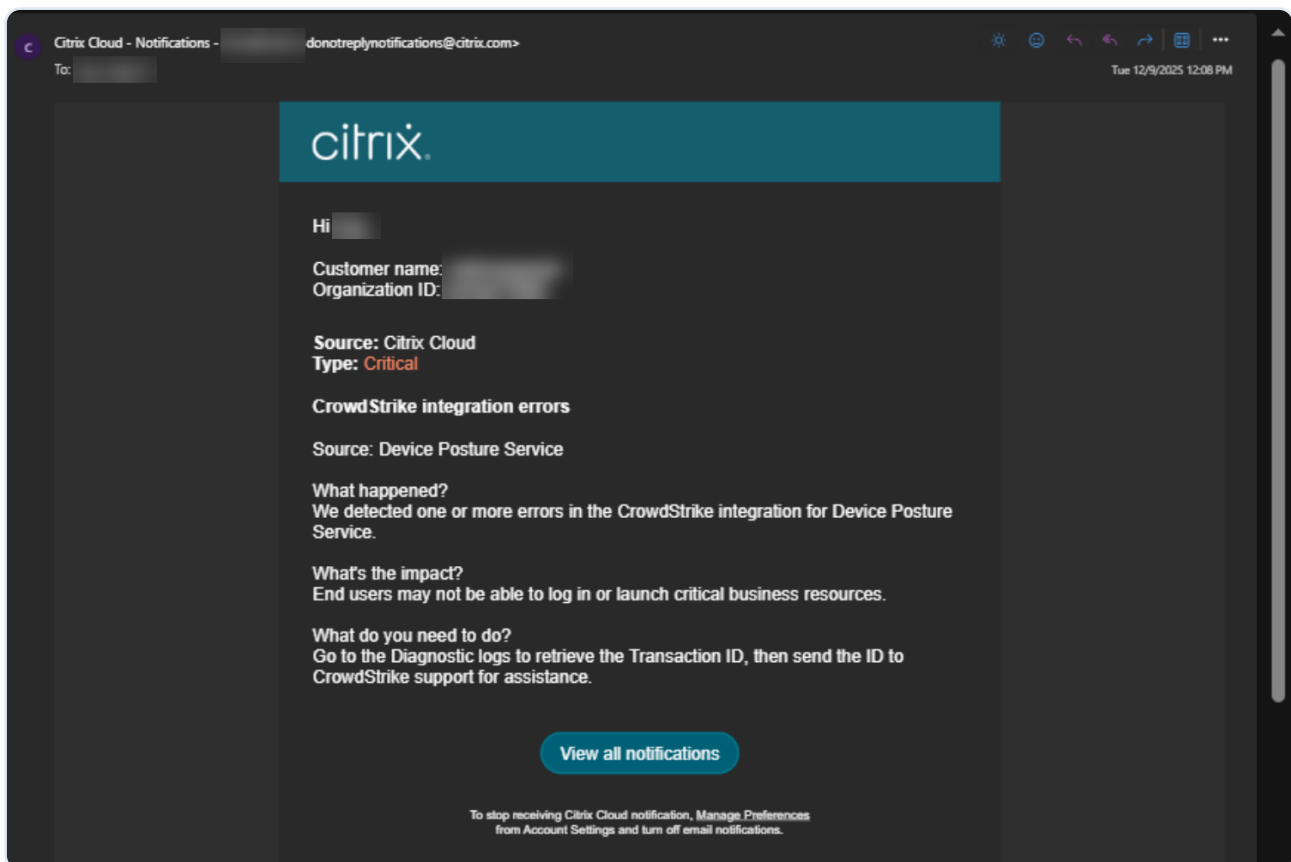
ユースケース

CrowdStrikeスキャンを設定してデバイスを準拠としてマークする顧客を考えてみましょう。そうでない場合、デバイスは非準拠としてマークされます。

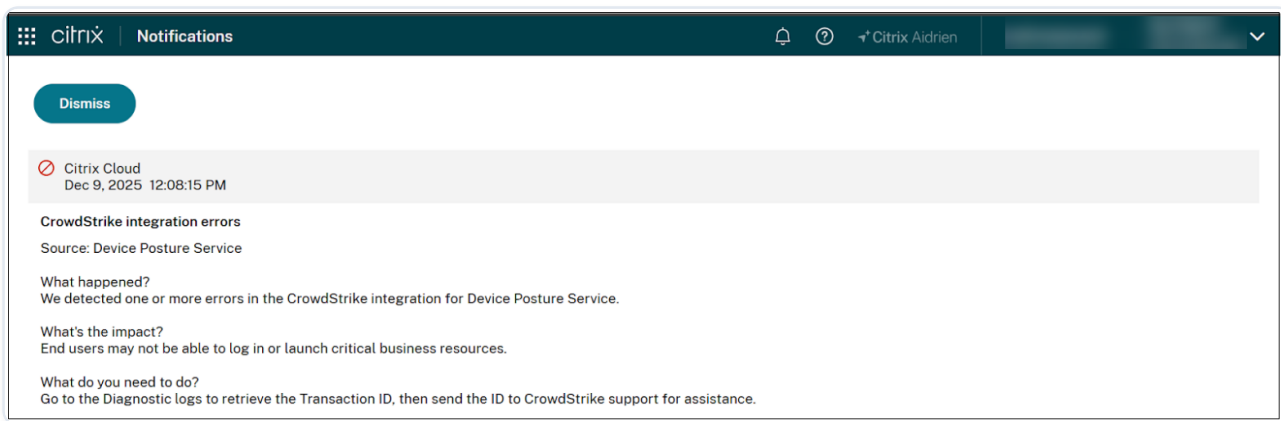
CrowdStrikeの障害が発生した場合、Citrix Device PostureサービスはCrowdStrikeに接続してデバイスのコンプライアンス詳細を取得できません。その結果、エンドユーザーデバイスは自動的に非準拠としてマークされます。

この障害が発生すると、お客様はメール通知を受け取り、Device PostureとSecure Private Accessの両方の診断ダッシュボードで詳細なエラー情報を確認できます。この可視性により、お客様はサードパーティのサポートチームに直接連絡して問題を解決し、ダウンタイムを削減できます。

次の図は、メール通知の例を示しています。



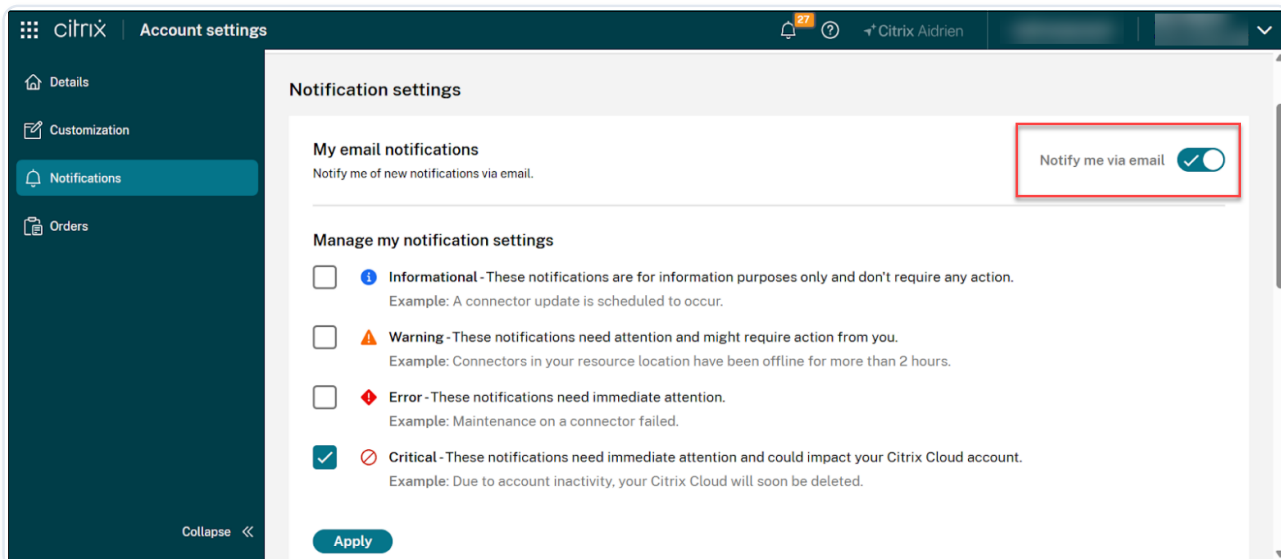
次の図は、ダッシュボード上の通知を示しています。



前提条件

Citrix管理者は、Citrixのアカウント設定 > 通知ページで以下を有効にし、適用をクリックする必要があります。

- メールで通知するトグルスイッチをオンにします。
- 重大通知設定を選択します。



デバイスポスチャサービス管理コンソールで通知を設定する

1. グローバル設定に移動します。
2. デバイスポスチャ統合通知ボックスで、トグルスイッチをオンに切り替えます。

通知設定(/en-us/device-posture/media/dps-integration-failure-notification-setting.png)

デフォルトでは、統合がダウンした場合、15分後に通知が送信されます。要件に基づいて通知頻度をカスタマイズできます。

頻度を変更するには、編集をクリックし、必要な頻度を選択した後、保存をクリックします。

エンドユーザーフロー

デバイスポスチャポリシーが設定され、デバイスポスチャが有効になると、エンドユーザーがCitrix Workspaceにログインする方法に基づいて、以下のエンドユーザーフローが適用されます。

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ブラウザは、説明のために例として使用されています。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経由でCitrix Workspace URL `https://<your-workspace-url>` にログインすると、Citrix EndPointAnalysisアプリケーションを実行するよう求められます。

アプリケーションをインストールする (/en-us/device-posture/media/device-posture-end-user-flow-results1.png)

- エンドユーザーが**Citrix End Point Analysisを開く**をクリックすると、デバイスポスチャクライアントが実行され、デバイスポスチャポリシーの要件に基づいてエンドポイントパラメータをスキャンします。
- デバイスポスチャクライアントがデバイスにインストールされていない場合、ユーザーは**プラグインのダウンロード**オプションが表示されるページにリダイレクトされます。最新のデバイスポスチャクライアントがすでにエンドポイントにインストールされている場合、ユーザーは**デバイスの確認**をクリックしてそれを確認する必要があります。同様に、デバイスにインストールされているEPAが最新バージョンでない場合、ユーザーは**プラグインの更新**オプションが表示されるページにリダイレクトされます。EPAクライアントがすでに更新されている場合、ユーザーは**デバイスの確認**をクリックしてそれを確認する必要があります。

クライアントバージョンを確認する (/en-us/device-posture/media/device-posture-end-user-flow3.png)

どちらのシナリオでも、スキップチェック機能が有効になっている場合、**プラグインのダウンロード**または**プラグインの更新**ページに「または、**制限付きアクセス**でCitrix Workspaceを続行できません。」というメッセージが表示されます。

スキップチェックメッセージ (/en-us/device-posture/media/device-posture-end-user-flow4.png)

Citrix Workspaceアプリケーションによるエンドユーザーフロー

- エンドユーザーがCitrix Workspaceアプリケーション経由で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ているデバイスポスチャクライアントが実行され、デバイスポスチャポリシーの要件に基づいてエンドポイントパラメータをスキャンします。
- 最新のデバイスポスチャ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**と**クライアントのダウンロード**のオプションが表示されるページにリダイレクトされます。ユーザーは**クライアントのダウンロード**をクリックする必要があります。
- エンドポイントに最新のデバイスポスチャクライアントがすでにインストールされている場合、ユーザーは「**再確認**」をクリックする必要があります。

エンドユーザーフロー - デバイスポスチャの結果

デバイスポスチャポリシーの条件に基づいて、3つの可能性があります。

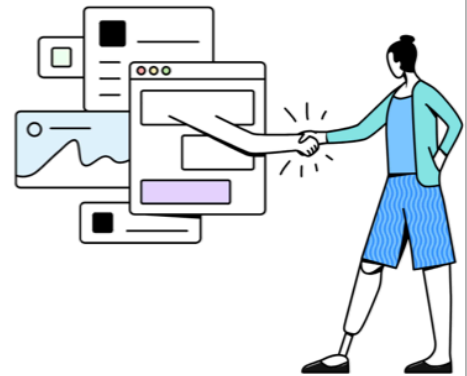
エンドポイントがポリシー条件を満たし、デバイスが次のように分類される場合;

- **準拠** - エンドユーザーは、Secure Private AccessまたはCitrix DaaSリソースへの無制限のアクセスでログインできます。
- **非準拠** - エンドユーザーは、Secure Private AccessまたはCitrix DaaSリソースへの制限付きアクセスでログインできます。

citrix

Checking if your device meets certain policy requirements.

 Searching for EPA plug-in...



 [English](#) [Privacy Policy](#)

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」と分類される場合、「アクセス拒否」メッセージが表示されます。

citrix



Access denied

Device does not meet certain requirements.

[Check device again](#)

If this persists **contact your administrator** and provide this ID:





 [English](#) [Privacy Policy](#)

テストモードでのデバイスポスチャサービス

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ます。これにより、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行動計画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、この分類はエンドユーザーデバイスにいかなるアクションも強制しません。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します。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表示できます。必要に応じて、管理者はテストモードを無効にすることもできます。

注:

EPAクライアントはデバイスにインストールされている必要があります。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. **デバイスポスチャは無効です**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。

 **Enabling device posture will impact the subscriber experience**

Device posture scans all user devices before allowing users to log in. Users who have already logged in must have to relogin to enable device posture service to scan the subscriber devices.

If users have not installed the device posture app, they are prompted to download and install it.

Device posture will be enabled to subscribers in a few minutes (sometimes up to an hour) after it is enabled on the Device Posture page.

☒ Enable device posture in test mode (optional) 

☒ I understand the impact on subscriber experience.

Confirm and enable

Cancel

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、デバイスポスチャのホームページに、その旨を確認するメモが表示されます。

Home > Identity and Access Management > Device Posture

Device Posture

Device posture is enabled (Test mode) 

Create device posture policies to enforce application access based on the end user's device

 Device Posture is enabled in test mode. Go to the Dashboard to view activity

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構成」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。管理者はこのデータをダッシュボードで表示できます。

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」グラフには、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、「**詳細を見る**」リンクをクリックします。

テストモード診断(/en-us/device-posture/media/dp-test-mode-dashboard.png)

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、テストモードを有効にするために次の手順を実行します。

1. ホームページで、「**デバイスポスチャが有効です**」トグルスイッチをオフにします。
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、「**デバイスポスチャが無効です**」トグルスイッチをオンにして、デバイスポスチャを有効にします。
5. 確認ウィンドウで、次の2つ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。

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へ移行するには、まずテストモードでDevice Postureを無効にし、その後、テストモードでデバイスポスチャを有効にするオプションを選択せずに再度Device Postureを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へ移行する前に、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、本番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**アクセス拒否**のユーザーアクセスに影響を与える可能性があります。テストモードでは、**アクセス拒否**は実質的に**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へのアクセスを継続できます。しかし、本番環境では、この結果は直接アクセスをブロックし、ユーザーエクスペリエンスと運用に影響を与える可能性があります。
- また、テストモードから本番環境へ移行する際には、潜在的なダウンタイムが発生する可能性があります。中断を最小限に抑えるために、移行計画を慎重に立てることをお勧めします。

Citrix Secure Access Endpoint Analysis (EPA) クライアントバージョンを、サポートされる最小バージョンを設定して管理する

注:

このトピックでは、EPA は Citrix Secure Access Endpoint Analysis クライアントを指します。これら2つの用語は同じ意味で使用されます。

管理者は、サポートされる最小 EPA バージョンを維持することで、Device Posture サービスを通じて Citrix Secure Access Endpoint Analysis (EPA) クライアントバージョンを管理できます。

以前は、Device Posture サービスはすべてのエンドポイントで単一の固定 EPA クライアントバージョンを必要としていました。

利点:

Device Posture サービスソリューションによる EPA クライアントバージョン管理には、次の利点があります。

- 合理化されたバージョン管理
- サポートのオーバーヘッドの削減
- Device Posture サービスの要件へのエンドポイントの準拠を保証

仕組み

Device Posture サービスは、Device Posture 管理コンソールのプラットフォーム固有の設定に基づいて、クライアントバージョンのインストールまたはアップグレードをユーザーに促します。

- **サポートされる最小バージョン:** 管理者がサポートされる最小バージョンを設定すると、Device Posture サービスは次のように動作します。

クライアントデバイス	DEVICE POSTURE サービスの動作
クライアントがインストールされていないデバイス	ユーザーには最新のEPAクライアントをインストールするよう求められます。
クライアントバージョンが最小バージョンより低いデバイス	ポータルにダウンロードオプションが表示されます。エンドユーザーはクライアントを手動でインストールまたはアップグレードします。管理者権限でインストールしてください。そうしないと、インストールはユーザーモードで実行され、一部の機能が利用できない場合があります。
バージョンが最小バージョン以上であるデバイス	変更なし。

- **常に最新バージョンを使用:** 管理者が常に最新バージョンを使用オプションを設定すると、すべてのエンドポイントで利用可能な最新のEPAクライアントバージョンが実行されます。

EPAクライアントがインストールされていないか、または古い場合、デバイスポスチャサービスは次のように動作します。

クライアントデバイス	デバイスポスチャサービスの動作
クライアントがインストールされていないデバイス	ユーザーには最新のEPAクライアントをインストールするよう求められます。
古いバージョンのデバイス	ポータルにダウンロードオプションが表示されます。エンドユーザーはクライアントを手動でインストールまたはアップグレードします。管理者権限でインストールしてください。そうしないと、インストールはユーザーモードで実行され、一部の機能が利用できない場合があります。

例:

特定のプラットフォームの例を次に示します。最小サポートバージョンは24.8、最新バージョンは25.8です。

次の表は、管理コンソールで設定された設定に基づく Device Posture サービスの動作をまとめたものです。

クライアントデバイス	最小サポートバージョンとして 24.8が選択されている場合	常に最新バージョンを使用する が選択されている場合
EPAクライアントがインストールされていない	最新のEPAクライアントのインストールを促される。	最新のEPAクライアントのインストールを促される。
EPAバージョン < 24.8	最新バージョンへのアップグレードを促される	最新バージョンへのアップグレードを促される
EPAバージョン ≥ 24.8 (ただし最新ではない)	そのまま	最新バージョンへのアップグレードを促される
EPAバージョン == 最新	そのまま維持されます	そのまま維持されます

注:

Device Postureサービスが更新されたEPAクライアントを必要とする新機能を導入する場合、管理者は互換性と最適な機能を確保するために、サポートされる最小バージョンを改訂する必要があります。

EPAクライアントのバージョン管理オプションを設定する

1. **Device Posture > Device Scans** に移動し、**Settings** をクリックします。
2. EPAクライアントの最小バージョン切り替えを有効にし、**Edit** をクリックします。
3. 各プラットフォームについて、クライアントバージョン管理のために以下のいずれかのオプションを選択します。
 - 常に最新バージョンを使用する
 - 記載されている最小バージョン (例: Windows の場合は 24.8.1.19)
4. **Save** をクリックします。

Endpoint Analysis (EPA) client minimum version

SaveCancel

Select the minimum version of the EPA client that is required to be installed on endpoint devices.

☒ Enable EPA client minimum version check

Platform	Select Minimum Version	
Linux	Always use latest version	View Support Matrix
Mac	25.9.16	View Support Matrix
Windows	25.10.1.10	View Support Matrix

On mobile devices, the EPA client version is inherited from Citrix Workspace app.

重要:

- EPAクライアントのバージョン管理は、ドロップダウンリストに表示されているバージョンをサポートしています。エンドユーザーには、これらのバージョンまたはそれ以降のバージョンを使用することをお勧めします。ドロップダウンメニューに表示されていないバージョンは、本番環境での使用は推奨されません。
- 最新のクライアントバージョンについては、[Citrix Endpoint Analysis](#) を参照してください。

EPAクライアントの配布とバージョン管理に関する考慮事項

EPAクライアントの配布とバージョン管理については、以下の点を考慮してください。

- **配布戦略:** 標準的なエンドポイント管理ツール（例：Windows用SCCM、macOS用Jamf）を使用して、EPAクライアントを展開またはパッチ適用します。
- **標準化されたロールアウト:** 展開スケジュールに合わせて最小サポートバージョンを設定することで、クライアントの更新を段階的にロールアウトします。
- **即時機能ロールアウト:** 「常に最新バージョンを使用」設定が有効になっていることを確認し、リリース時にすべてのユーザーが最新のEPAバージョンを受け取れるようにします。
- **互換性の確保:** 新しいデバイスポスチャサービスに依存する機能がリリースされるたびに、サポートされていないクライアントバージョンを避けるために、最小サポートバージョンを更新します。

複数のクラウドストアのサポート

管理者は、異なるクラウドストアに個別のデバイスポスチャポリシーを適用でき、きめ細かな制御と簡素化されたセキュリティ管理を実現します。

以前は、デバイスポスチャサービスはすべてのクラウドストアでグローバルに有効になっていたため、管理者はURLごとに特定の要件を適用できませんでした。

複数のストアをサポートすることで、次のことができるようになりました。

- 特定のストアに対して個別のデバイスポスチャチェックを適用する。
- ユーザーがアクセスするストアに基づいて、さまざまなレベルのデバイスコンプライアンスを適用する。
- ストアに展開する前に、テストストアでデバイスポスチャチェックを作成およびテストする。

重要な考慮事項

ストアごとに異なるルールを実装する前に、次の点に注意してください。

- マルチワークスペースURLのサポートは、Chrome Extension Premium (CEP) では利用できません。
- マルチワークスペースURLは、NetScaler Gateway URLではサポートされていません。
- マルチワークスペースモードに切り替えると、既存のデバイスポスチャ構成が各ワークスペースURLにクローンされます。
- 既存のお客様は、テストURLを設定し、デバイスポスチャサービスでマルチワークスペースURLサポートを有効にできます。本番URLでデバイスポスチャサービスをアクティブに保ちながら、テストURLで変更を試すことができます。このアプローチにより、より広範なユーザーベースを中断することなく、ポスチャチェックの変更を検証できます。

注:

マルチワークスペース展開におけるデバイスポスチャサービスのサービス継続性は、Delivery Controller™ (DDC) バージョン26.03以降でサポートされています。

前提条件

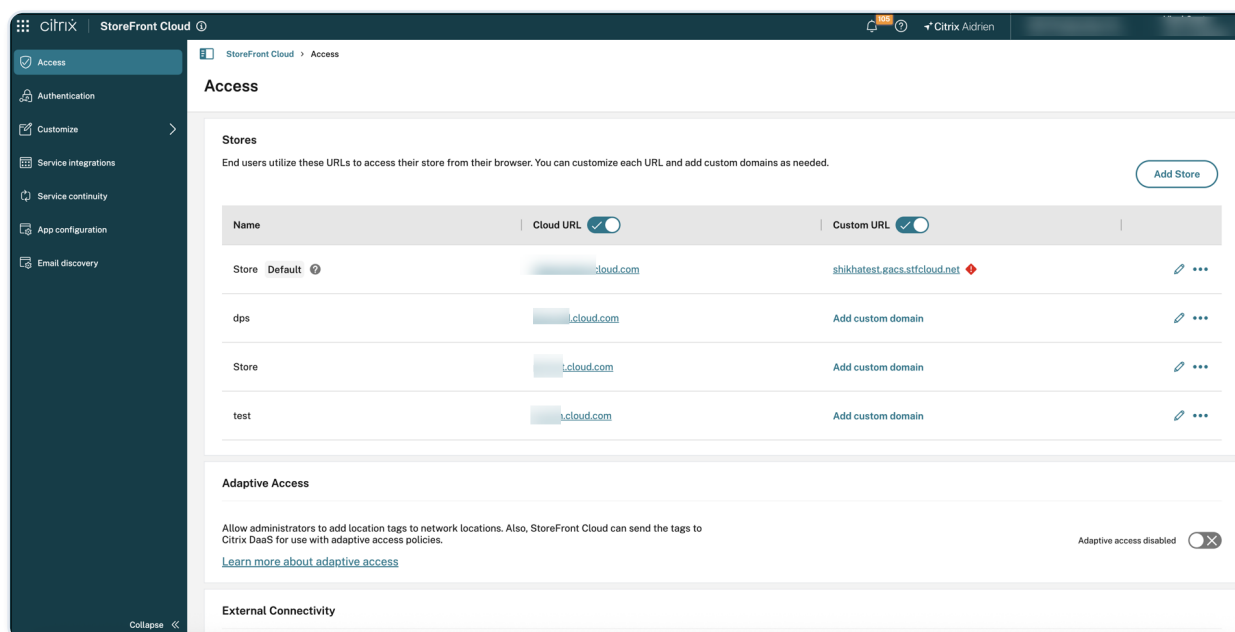
- サポートされているプラットフォーム: Windows、macOS、iOS
- マルチワークスペースURLのサポートは、次のEPAクライアントで利用できます。
 - Windows: バージョン 25.7.1.11 以降。 [ダウンロードリンク](#)。
 - macOS: バージョン 25.11.19 以降。 [ダウンロードリンク](#)。
 - iOS: Citrix Workspace app (CWA) バージョン 25.5.0 以降 (App Storeからインストール)。

注:

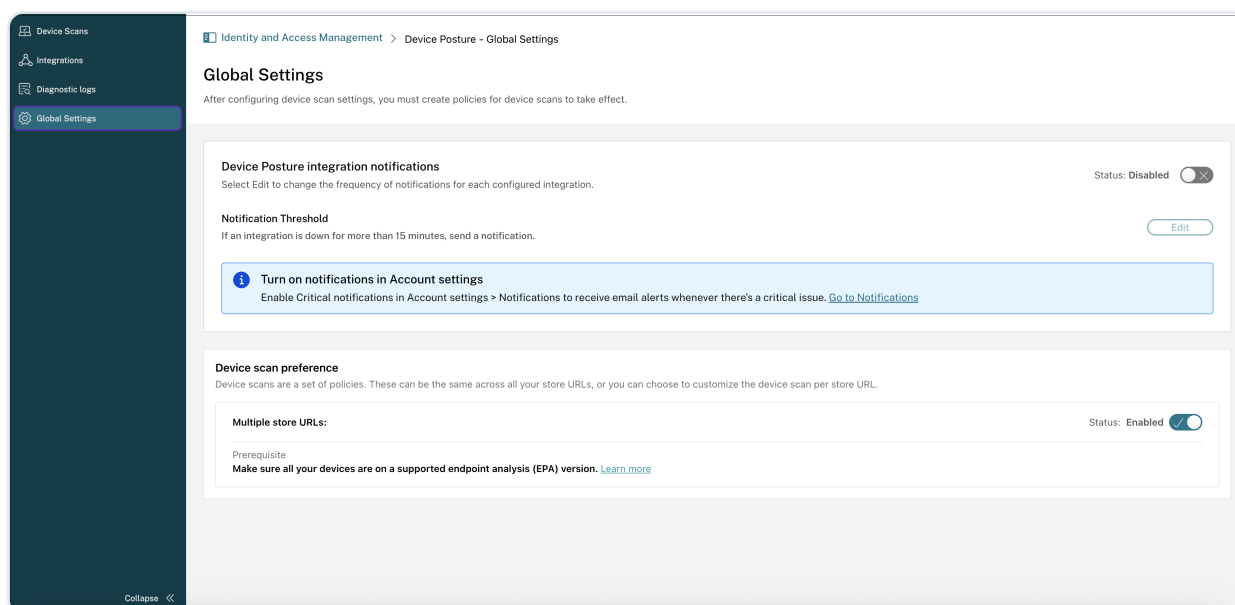
- Windows、macOS、または iOS 以外のプラットフォームを実行しているデバイスからアクセスするユーザーは、サポートされていないデバイスを使用していると見なされ、Device Posture サービスコンソールで管理者が構成したデフォルトの動作に従います。これは、**スキップチェック**が構成されている場合にのみ適用されます。それ以外の場合、ユーザーは最新のクライアントをダウンロードするように求められます。
- サポートされていないプラットフォーム上のデバイスは、デフォルトで**非準拠**とマークされます。
- Device Posture ページの**設定**タブから、分類を**非準拠**から**ログイン拒否**に変更できます。
- 「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。
- エンドポイントの EPA クライアントは、前提条件セクションで指定されたバージョンを使用する必要があります。クライアントが古いバージョンを使用している場合、デバイススキャンは開始に失敗します。Windows 管理者にとっては、EPA クライアントが Citrix Secure Access™ Client for Windows 2505 にバンドルされているため、この要件は簡素化されます。
- サポートされていないデバイスのデバイスポスチャチェックをスキップすることもできます。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。

ストアURLを構成する

1. ワークスペースURLが**StoreFront Cloud > アクセス**を介して構成されていることを確認します。



2. Device Posture にアクセスするには、Citrix Cloud™ にログインし、Device Posture ナビゲーションバーでID およびアクセス管理 > Device Posture > グローバル設定に移動します。



3. Device Posture の構成をクリックし、次に設定をクリックします。
4. 「ワークスペースURLごとに異なるデバイススキャンを使用」を選択します。
5. デバイスポスチャの環境設定を変更するには、「変更」をクリックします。



Change device scan preference?



If you change your device scan preference to use a common scan for all Workspace URLs, you will need to create new policies for that device scan.

Your current configuration using a common scan will be saved if you wish to go back to using a common scan in the future.

Change

Cancel

注:

- 「ワークスペースURLごとに異なるデバイススキャンを使用」オプションが有効になっている場合、各ワークスペースURLに対して個別に新しいスキャンを設定する必要があります。
- 新しいスキャンを設定した後、ユーザーは1～2時間以内に再認証を求められ、新しい構成を使用してログインセッションが評価されるようになります。

Device Posture ユーザーイベントの SIEM システムへのエクスポート

Device Posture サービスイベントは、セキュリティ情報およびイベント管理 (SIEM) にエクスポートされます。これにより、SIEM で Device Posture サービスに関連付けられた以下のユーザーイベントを表示できます。

- Device Posture サービスに関連するすべてのイベントタイプ。
- Device Posture 評価イベント。これは、定義されたポリシーに対するデバイスのポスチャの評価に関する情報を提供します。

SIEM システムにイベントをエクスポートする利点は次のとおりです。

- セキュリティ運用チームが、異なるログからのデータを関連付け、分析し、検索できるようにします。
- セキュリティ運用チームがセキュリティリスクを特定し、迅速に修正するのに役立ちます。
- セキュリティアラートを一元的に可視化します。
- リスク指標、ユーザープロファイル、リスクスコアなどの組織のリスク分析機能のために、潜在的なセキュリティ脅威を検出するための一元的なアプローチ。
- ユーザーアカウントの Citrix Analytics リスクインテリジェンス情報を、SIEM 内に接続された外部データソースと組み合わせて関連付ける機能。

詳細については、以下のトピックを参照してください。

- [Device Posture サービスイベント](#)
- [Device Posture サービスイベントの障害を診断する](#)
- [セキュリティ情報およびイベント管理 \(SIEM\) の統合](#)

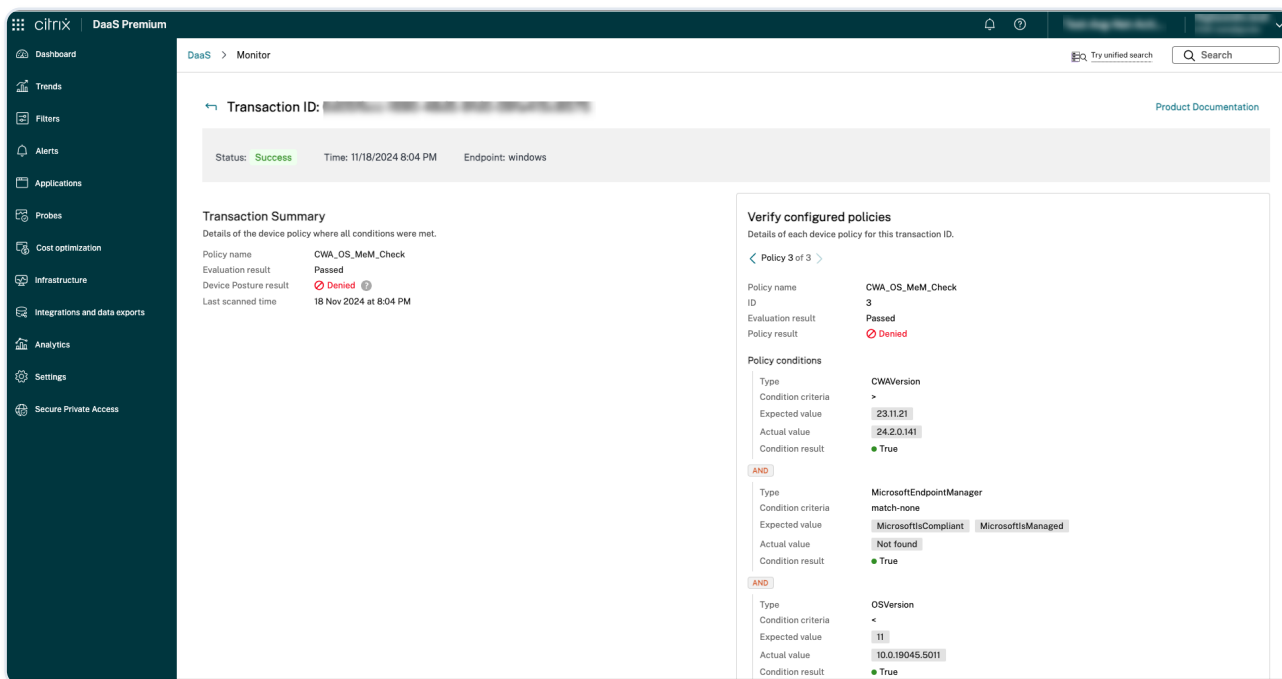
DaaS Monitor を使用したデバイスポスチャの問題のトラブルシューティング

ユーザーがSecure Private AccessまたはDaaSを介して接続する際に各セッションで生成されるトランザクションIDを使用して、DaaS Monitorでデバイスポスチャの問題/エラーをトラブルシューティングできます。トランザクションIDを見つけると、DaaS Monitorはセッションと適用された関連するデバイスポスチャポリシーに関する情報を表示します。Monitorは、デバイスがポスチャチェックに合格したか失敗したかを含むポリシー結果も表示します。

Citrix DaaS™ Monitorで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. エンドユーザーデバイスから、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をコピーします。
2. Citrix Cloudにサインインします。
3. DaaSタイルで、**Manage**をクリックし、次に**Monitor**タブをクリックします。Monitor UIで、32桁のトランザクションIDを検索し、**Details**をクリックします。



詳細については、次のトピックを参照してください。

- Monitorを使用したデバイスポスチャサービスのポリシーとトランザクションのトラブルシューティング
- デバイスポスチャイベントのSIEMデータエクスポート形式の確認

デバイスポスチャのログとイベント

管理者は、デバイスポスチャダッシュボードを通じてデバイスのコンプライアンスを監視できます。組織のリソースにアクセスするエンドポイントのコンプライアンス要件を定義する、構成済みのすべてのデバイスポスチャポリシーを表示できます。また、すべてのデバイスのリアルタイムのコンプライアンスステータスも表示でき、これには以下のように分類された詳細な評価結果が含まれます。

- **準拠:** 指定されたすべてのセキュリティ要件とポリシー基準を満たすデバイス。
- **非準拠:** 1つ以上のセキュリティ要件を満たさないが、限定的なアクセスが許可される可能性があるデバイス。
- **アクセス拒否:** 重大なセキュリティリスクをもたらし、リソースへのアクセスがブロックされているデバイス。

デバイスポスチャのログとイベントは、[Secure Private Accessダッシュボード](#) および [Identity and Access Managementコンソールのデバイスポスチャダッシュボード](#) で表示できます。

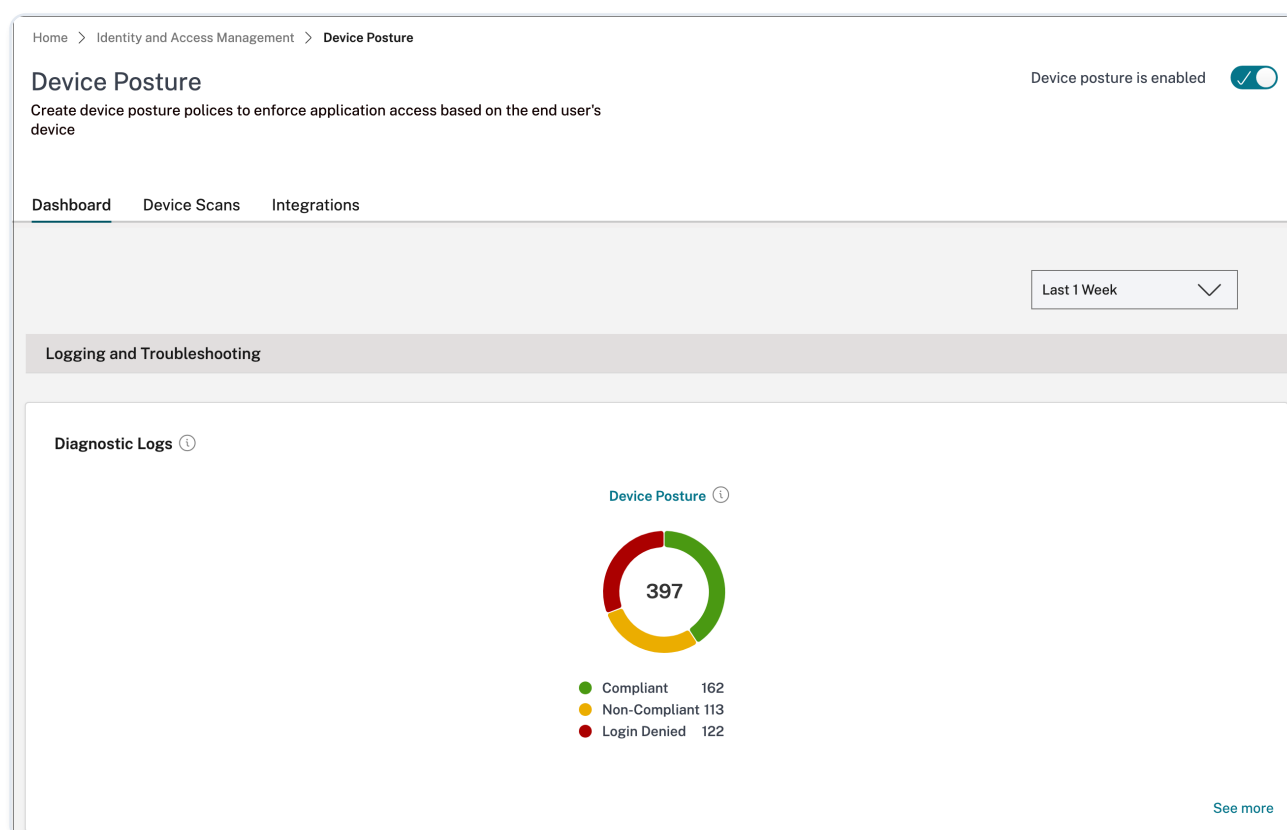
Identity and Access Managementコンソールのデバイスポスチャダッシュボード

Identity and Access Managementコンソールのデバイスポスチャダッシュボードのログとイベントを表示するには、次の手順を実行します。

1. Citrix Cloudにサインインします。
2. Citrix Cloudメニューから、**Identity and Access Management**を選択します。
3. **Device Posture > Manage**をクリックし、次に**Dashboard**をクリックします。

Logging and Troubleshooting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。

4. ログの詳細を表示するには、**See more**リンクをクリックします。ポリシー結果（**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。



Add filter オプションを使用して、ポリシー情報、ポリシー結果、オペレーティングシステム、トランザクションID、情報コード、デバイスIDなどのさまざまな基準に基づいて検索を絞り込むことができます。たとえば、検索フィールドで**Device-ID**をクリックし、**~ (contains some value)**を選択して「6273」と入力します。6273を含むデバイスIDに関連するすべてのログが表示されます。

各ログエントリの横にある展開アイコンをクリックすると、スキャンタイプ、クライアントアプリバージョン、クライアントライブラリバージョン、エンドポイント情報などの詳細が表示されます。

デバイスポスチャダッシュボード2(/en-us/device-posture/media/device-posture-dashboard2.png)

注:

- **ClientAppVersion**フィールドと**ClientLibraryVersion**フィールドには、それぞれEPAクライアントバージョンとライブラリバージョンが表示されます。
- アクセスが拒否された場合、トランザクションIDもエンドユーザーに表示されます。
- エラーまたはスキャン失敗が発生した場合、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サービスダッシュボードで確認できます。ログで問題が解決しない場合、エンドユーザーはCitrixサポートにトランザクションIDを共有して問題を解決できます。

ログの場所

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。

- ~/Library/Application Support/Citrix/EPAPLugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPLugin/epaplugin.log

Secure Private Accessダッシュボード

Device Postureサービスのログとイベントを表示するには、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、**Manage**をクリックし、次に**Dashboard**をクリックします。

Logging and Troubleshootingセクションには、Device Postureサービスに関連する診断ログが表示されます。

3. ログの詳細を表示するには、**See more**リンクをクリックします。ポリシー結果（**Compliant**、**Non-Compliant**、**Login Denied**）に基づいて検索を絞り込むことができます。

ダッシュボード(/en-us/device-posture/media/device-posture-end-user-flow-results33.png)

デバイスポスチャのエラーログ

Device Postureサービスに関連する以下のログは、Citrix MonitorおよびSecure Private Accessダッシュボードで表示できます。これらのログについてはすべて、解決のためにCitrixサポートに連絡することをお勧めします。

- 構成された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/式の処理に失敗しました
- エンドポイントの詳細の保存に失敗しました
- エンドポイントからのスキャン結果の処理に失敗しました

デバイスポスチャデータの書き出し

Device Postureサービスイベント（デバイスポスチャの結果やイベントタイプなど）は、Security Information and Event Management (SIEM) サービスにエクスポートできます。これらのイベントは、Citrix Endpoint Analysis (EPA) クライアントが、Citrix Virtual Apps and Desktops™ または Citrix Secure Private Accessリソースへのアクセスを試みるデバイスに対してポスチャチェックを実行したときに生成されます。

- Device PostureサービスログをSIEMにセットアップ、構成、エクスポートする方法については、「[Security Information and Event Management \(SIEM\) integration](#)」を参照してください。
- Device Postureサービスからエクスポートできるイベントとログの詳細については、「Device Postureサービスイベント」([/ja-jp/security-analytics/siem-integration/siem-messages-schema#device-posture-service-events](#))を参照してください。
- Device Postureサービスのトランザクションを診断およびトラブルシューティングする方法については、「Device Postureサービストランザクションの診断」([/ja-jp/citrix-daas/monitor/troubleshoot-deployments/user-issues/diagnose-device-posture-service-transactions](#))を参照してください。

デバイスポスチャサービス トランザクションの診断

管理者は、デバイスポスチャサービス トランザクションを効果的に診断し、トラブルシューティングできるようになりました。このアップデートにより、Citrix Monitor のトラブルシューティング機能が強化され、デバイスポスチャポリシーの評価、コンプライアンスチェック、エラー診断に関する詳細なインサイトが提供されます。

デバイスポスチャサービス評価フローの理解

一般的なSecure Private AccessまたはVDIアプリのアクセス起動には、次の3つの段階があります。

1. **事前認証:** デバイスポスチャサービスを使用して、基本的なエンドポイント衛生チェックが実行されます。デバイスがコンプライアンスポリシーを満たさない場合、認証前にアクセスがブロックされます。
2. **認証:** この段階でユーザーを認証します。資格情報の不一致またはIDプロバイダーのエラーがある場合、認証は失敗します。
3. **アプリケーションアクセス:** この段階には、次の2つのサブステージが含まれます。
 - **ポリシー仲介および列挙ステージ:** ユーザーのデバイスコンテキストがポリシー設定に違反している場合、アプリケーションへのアクセスは制限されます。
 - **アプリケーション起動ステージ:** Citrix Enterprise Browser™、Secure Private Accessクライアント、またはネイティブエンドポイントクライアントを使用してアプリケーションのトランザクションが完了する最終段階です。

Citrix Monitorにおけるトラブルシューティングの強化

このアップデートにより、Citrix Monitorは検索ベースのデバイスポスチャサービストラブルシューティングを提供し、ITチームは次のことを行えます。

- ユーザーIDまたはトランザクションIDでトランザクションをフィルタリングし、ターゲットを絞ったデバッグを行う。
- デバイスが準拠しているか、準拠していないか、またはポリシー違反によりブロックされているかなど、ポリシー評価の結果を分析する。
- 詳細なコンプライアンスチェック、期待値、およびリアルタイムのコンテキスト値を調べることで、ポリシーの失敗を特定する。
- より詳細な診断のために、デバイスのメタデータ、ポリシー構成、およびログを確認する。
- システムエラーによる失敗したトランザクションを特定し、エラーメッセージをナレッジベースの記事にリンクして迅速な解決を図ります。

ITチームがトラブルシューティングの強化をどのように活用できるか

以下のセクションでは、問題のトラブルシューティングに関する詳細情報を提供します。

デバイスポスチャの問題のトリアージ

ユーザーから報告されたトランザクションIDを検索して、関連するデバイスポスチャサービスログをすばやく見つけます。コンプライアンスチェックが合格したか失敗したかを確認し、根本原因を特定します。

たとえば、トランザクションIDを検索すると、デバイスポスチャチェックポリシーの結果（成功（準拠または非準拠）したか、エラーにより失敗したか）を確認できます。システムは、クライアントメタデータ、ポリシーの詳細、その他のトランザクションの詳細を含む、デバイスポスチャサービス評価の完全なコンテキストを提供します。

Transaction ID: d61b8781-2666-4339-8a4d-69869b427805

Status: **Success** Time: 11/13/2024 2:10 PM User name: dps0929@citrix.com Endpoint: windows

Transaction Summary
Details of the device policy where all conditions were met.

Policy name	CWACheckWithMonitorEvent
Evaluation result	Passed
Device Posture result	Compliant
Last scanned time	13 Nov 2024 at 2:10 PM

Verify configured policies
Details of each device policy for this transaction ID.

< Policy 3 of 4 >

Policy name	CWACheckWithMonitorEvent
ID	3
Evaluation result	Passed
Policy result	Compliant

Policy conditions

Type	CWAVersion
Condition criteria	>=
Expected value	10.0.0.0
Actual value	24.5.10.29
Condition result	True

ポリシーベースのアクセスブロックの調査

デバイスが非準拠の場合、IT部門は失敗した正確なポリシーパラメータを検査できます。システムは、設定された期待値とデバイスのリアルタイムデータを並べて比較して表示します。

DaaS > Monitor

Try unified search

Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427783

Product Documentation

Status: **Success** Time: 11/13/2024 1:26 PM User name: dps0924@citrix.com Endpoint: windows

Transaction Summary

Details of the device policy where all conditions were met.

Policy name	CWAVersion_Mem_Check
Evaluation result	Passed
Device Posture result	Non Compliant
Last scanned time	13 Nov 2024 at 1:26 PM

Verify configured policies

Details of each device policy for this transaction ID.

< Policy 2 of 3 >

Policy name	CWAVersion_Mem_Check
ID	3
Evaluation result	Passed
Policy result	Non Compliant
Policy conditions	
Type	CWAVersion
Condition criteria	>
Expected value	22.11.0.67
Actual value	23.55.66.77
Condition result	True
AND	
Type	MicrosoftEndpointManager
Condition criteria	Is
Expected value	[MicrosoftIsManaged MicrosoftIsCompliant]
Actual value	MicrosoftIsManaged
Condition result	True

精密検索による大規模なポリシーセットのデバッグ

管理者は、複数のポリシーを持つ複雑な環境で特定のパラメータを検索し、期待されるユーザーコンテキストが存在するかどうかを確認できます。パラメータ値の不一致が発生した場合、システムは失敗条件を視覚的に強調表示し、根本原因の特定を加速します。また、管理者はポリシーをナビゲートして、どのポリシーが評価され、どのポリシーが現在のトランザクション結果を生成したかを確認できます。

DaaS > Monitor

Try unified search

Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427791

Product Documentation

Status: **Success** Time: 11/13/2024 1:26 PM User name: dps0924@citrix.com Endpoint: windows

Transaction Summary

Details of the device policy where all conditions were met.

Policy name	CWAVersion_Mem_Check
Evaluation result	Passed
Device Posture result	Denied
Last scanned time	13 Nov 2024 at 1:26 PM

Verify configured policies

Details of each device policy for this transaction ID.

Policy 1 of 3

Policy name	CWAVersion_CW_Check
ID	1
Evaluation result	Failed
Policy conditions	
Type	CWAVersion
Condition criteria	>
Expected value	21.09.1.32
Actual value	20.55.66.77
Condition result	False
AND	
Type	CrowdStrikeRiskScore
Condition criteria	>
Expected value	50
Actual value	20
Condition result	False

大規模なポリシーパラメータの作業セットをトラブルシューティングするには、パラメータを検索して、目的のユーザーコンテキストがリアルタイムで存在するかどうかを確認できます。

Verify configured policies

Details of each device policy for this transaction ID.

< Policy 1 of 4 >

Actual value	10.0.22621.4169
Condition result	● True

AND

Type	MACAddress
Condition criteria	in
Expected value	00-B0-D0-63-C2-26 12:34:56:78:9A:BC 12:34:56:78:9A:BC DE:AD:BE:EF:00:11 01:23:45:67:89:AB FE:DC:BA:98:76:54 12:34:56:78:9A:BC 12:34:56:78:9A:BC +2 more
Actual value	00005e0053af
Condition result	● False

例えば、前のスクリーンショットでは、強調表示されたフィールドを検索しても結果が得られませんでした（次の画像に記載）。これは、パラメータ値が一致しなかったことを示唆しています。この不一致により、条件の結果がfalseとなり、その結果、全体的なポリシーの結果が拒否されました。

OSDomainCheck

Policy condition: MACAddress in

Expected value (10)

トランザクションの失敗とエラーの処理

システムエラーによりポリシー評価が失敗した場合、Citrix Monitorに以下の詳細が表示されます。

- コンテキストの詳細を含むエラーの説明。
- トラブルシューティングドキュメントへのリンクにより、迅速な解決が可能になります。

DaaS > Monitor
Try unified search
Search

Transaction ID: d61b8781-2666-4339-8a4d-69869b427855
Product Documentation

Status: **Failed**
Time: 09/26/2024 3:50 PM

Transaction Summary

 An internal error occurred during the device posture scan. Please use the provided error code to troubleshoot further.

Error Code [0x0050001](#)

Verify configured policies

Details of each device policy for this transaction ID.



Evaluation policies haven't been assessed yet because the device didn't meet the posture check requirements.

Device Postureサービス取引を診断する手順

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。



Access denied

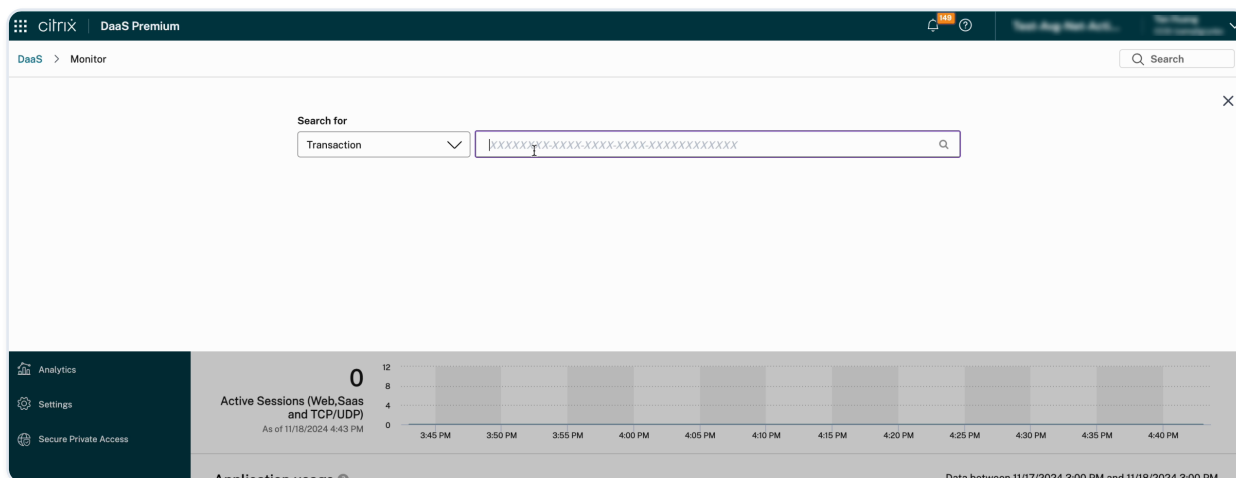
Device does not meet certain requirements

[Check device again](#)

If this persists **contact your administrator** and provide this ID:

0d05fbcc-1690-48d5-9fd0-09fa415c8575


2. Citrix Cloudにサインインします。
3. DaaSタイルで、**Manage**をクリックし、次に**Monitor**タブをクリックします。
4. **Search**フィールドにトランザクションIDを入力し、**Details**をクリックします。



設定されたDevice Postureポリシーのトランザクション概要と検証の詳細を表示できます。ポリシー評価の異なる値は、準拠、非準拠、拒否です。

トランザクションの概要

「トランザクションの概要」ページには、デバイスポスチャポリシーの結果が表示されます。準拠、非準拠、および拒否された結果の場合、概要には以下が含まれます。

- 「プラットフォーム」：クライアントデバイスのOS。
- 「ポリシー名」：デバイスポスチャポリシーの名前。
- 「評価結果」：デバイスポスチャポリシーが合格したか不合格だったかを示します。
- 「デバイスポスチャの結果」：デバイスポスチャの結果が準拠、非準拠、または拒否のいずれであるかを示します。
- 「最終スキャン時刻」：デバイスが最後にスキャンされた時刻。

設定済みポリシーの検証

「設定済みポリシーの検証」セクションでは、ポリシー評価の包括的な詳細を以下のように提供します。

- 失敗の理由。
- 失敗した特定のルール。
- 収集された証拠。

この情報により、管理者はポリシーの詳細に基づいてトラブルシューティングを行い、適切な措置を講じることができます。

デバイスポスチャポリシーの評価プロセス

1. 「ポリシーの失敗とルールの特定」:

- どのルールが失敗したか、そしてなぜ失敗したかを特定します。
- 失敗に関連する証拠を収集します。

2. 結果の決定:

- ポリシー評価に応じて、結果は準拠、非準拠、または拒否のいずれかになります。
- 一致するポリシーがない場合、結果は「一致するポリシーなし」となります。

3. ポリシー詳細の表示:

- 管理者は、特定のトランザクションIDの各デバイスポリシーの詳細を表示できます。
- 戻る矢印と進む矢印を使用して、異なるポリシー間を移動します。

準拠、非準拠、および拒否の結果の場合、デバイスポスチャポリシー評価には、「設定済みポリシーの確認」セクションに次の情報が含まれます。

- **ポリシー名:** デバイスポリシーの名前。
- **ID:** ポリシーが評価される順序。
- **評価結果:** デバイスポスチャポリシーが合格したか失敗したかを示します。
- **ポリシー結果:** デバイスポスチャの結果が準拠、非準拠、または拒否のいずれであるかを示します。
- **ポリシー条件:**
 - **タイプ:** デバイススキャンタイプ。
 - **条件基準:** ポリシールールを評価する条件。
 - **期待値:** ポリシー条件の構成済み値。
 - **実際値:** エンドポイントから収集された証拠。
 - **条件結果:** 条件が合格したか失敗したかを示します。

エラーコード

問題が発生し、Device Posture がポリシーの評価に失敗した場合、エラーコードが表示されます。

失敗した場合は、エラーコードをコピーして Citrix サポートに連絡してください。

ポリシーの詳細とエラーコードにより、ユーザーの問題のトリアージとトラブルシューティングが簡素化されます。

次の表に、エラーコード、エラーメッセージ、およびエラーの解決策を示します。

#	エラーメッセージ	エラーコード	アクション
1	構成されたポリシーの読み取りに失敗しました。	0x00500001	Citrixサポートにお問い合わせください
2	エンドポイントスキャンを評価できませんでした。	0x00500002	Citrixサポートにお問い合わせください
3	ポリシーまたは式を処理できませんでした。	0x00500003	Citrixサポートにお問い合わせください
4	エンドポイントの詳細を保存できませんでした。	0x00500004	Citrixサポートにお問い合わせください
5	エンドポイントからのスキャン結果の処理に失敗しました。	0x00500005	Citrixサポートにお問い合わせください
6	デバイスポスチャモード構成の読み取りに失敗しました。	0x00500006	Citrixサポートにお問い合わせください

Citrix Secure Access Endpoint Analysis (EPA) クライアントの配布とアップグレード

このトピックでは、Citrix Secure Access Endpoint Analysis クライアントを配布およびアップグレードするためのサポートされている方法について説明します。ここで説明する情報は、管理対象および非管理対象の Windows デバイス、ならびにクラウド (Device Posture サービス) およびオンプレミス (NetScaler® Gateway) の両方の展開に適用されます。

注:

このトピックでは、EPA は Citrix Secure Access Endpoint Analysis (EPA) クライアントを指します。この2つの用語は同じ意味で使用されます。

Citrix Secure Access Endpoint Analysis (EPA) クライアントの配布およびアップグレード方法

方法	展開	管理対象	非管理対象	トリガー	構成方法
Citrix Workspace™ アプリリリースにバンドル	クラウドおよびオンプレミス	はい	はい	自動 (Citrix Workspace アプリの更新時)	Citrix Workspace アプリのインストーラーには Citrix Secure Access Endpoint Analysis クライアントが含まれており、Citrix Workspace アプリと

方法	展開	管理対象	非管理対象	トリガー	構成方法
					もにデフォルトでインストールまたはアップグレードされます。
					「 Citrix Workspace アプリのダウンロード 」を参照してください。
					詳細な構成手順については、 「 Citrix Workspace アプリリリースにバンドル 」を参照してください。
Citrix Workspace アプリの自動更新 (クライアントアプリ管理)	クラウドおよびオンプレミス	はい	はい	自動 (Citrix Workspace アプリアップデートサービス)	クライアントを自動アップグレードするには、クライアントアプリ管理 (GACS) コンソールで Citrix Endpoint Analysis プラグイン を有効にします。

方法	展開	管理対象	非管理対象	トリガー	構成方法
					GACSの セットアップの詳細については、 「 Cloud: Configure GACS (Cloud) 」を参照してください。
					オンプレミス: GACSの構成 (StoreFront) 。
					詳細な構成手順については、 「 Citrix Workspace app auto-update (Client App Management) 」を参照してください。
SCCM、Intune、Jamf、またはその他のエンドポイント管理ツールを使用してインストーラー	クラウドおよびオンプレミス	はい	該当なし	手動または管理者管理	管理者は Citrix Downloads からインストーラーをダウンロードします。

方法	展開	管理対象	非管理対象	トリガー	構成方法
をプッシュする					<p>詳細な構成手順については、 「Push the installer using SCCM, Intune, Jamf, or another endpoint management tool」を参照してください。</p>
Device Postureサービスクンソールで最小EPAクライアントバージョンを設定する	クラウドのみ	はい	はい	プロンプトのみ (強制ではない)	<p>より低いバージョンを実行しているクライアントには、ポータルにダウンロードオプションが表示されません。これはサイレントアップグレードや強制アップグレードではありません。エンドユーザーはクライアントを手動でインストールまたはアップグレードしま</p>

方法	展開	管理対象	非管理対象	トリガー	構成方法
					<p>す。管理者権限でインストールしてください。そうしないと、インストールはユーザーモードで実行され、一部の機能が利用できない場合があります。</p> <p>詳細な構成手順については、デバイスポスチャサービスコンソールで最小EPAクライアントバージョンを設定するを参照してください。</p>
プラグインをNetScaler Gateway ポータルにアップロードする	オンプレミス	はい	はい	プロンプトのみ（強制ではない）	ポータルにダウンロードオプションが表示されます。エンドユーザーはクライアントを手動でインストールまたはアップグレードし

方法	展開	管理対象	非管理対象	トリガー	構成方法
					<p>ます。管理者権限でインストールしてください。そうしないと、インストールはユーザーモードで実行され、一部の機能が利用できない場合があります。</p> <p>詳細な構成手順については、プラグインをNetScaler Gatewayポータルにアップロードするを参照してください。</p>

詳細な構成手順

以下のセクションでは、詳細な構成手順を説明します。

Citrix Workspaceアプリリリースにバンドルされています

Citrix Secure Access Endpoint Analysisクライアントは、Citrix Workspaceアプリにバンドルされています。したがって、Citrix Workspaceアプリをインストールまたはアップグレードすると、EPAクライアントも自動的にインストールまたはアップグレードされます。

1. Citrix Workspaceアプリのリリースノートで、Citrix Workspaceアプリの提供状況を追跡します。

2. 通常のチャネル（Citrix Workspaceアプリの自動更新、手動ダウンロード、またはモバイルデバイス管理（MDM）ツール）を通じてCitrix Workspaceアプリを配布します。

インストール中に、バンドルされているCitrix Secure Access Endpoint Analysisクライアントがインストールまたはアップグレードされます。個別の操作は不要です。

適用範囲: クラウドおよびオンプレミス。エンドユーザーがCitrix Workspaceアプリを自分でインストールまたは更新する、管理対象および非管理対象デバイス。

Citrix Workspaceアプリの自動更新（クライアントアプリ管理）

Citrix Workspaceアプリの自動更新サービスは、クライアントアプリ管理で**Citrix Endpoint Analysis plug-in**が有効になっている場合、Citrix Secure Access Endpoint Analysisクライアントをアップグレードします。クライアントアプリ管理コントロールは**Citrix Endpoint Analysis plug-in**という名前で、アップグレードされるクライアントはWindowsコントロールパネルに**Citrix Secure Access Endpoint Analysis**として表示されます。

1. クライアントアプリ管理コンソールを開きます。クラウドの場合は、[グローバルアプリ構成サービスを構成する（クラウド）](#)を参照してください。オンプレミスの場合は、[グローバルアプリ構成サービスを構成する（StoreFront）](#)を参照してください。
2. 自動更新のために**Citrix Endpoint Analysis plug-in**を有効にします。
3. 構成されたバージョンが、必要なCitrix Secure Access Endpoint Analysisのバージョンをターゲットとしていることを確認します。

Citrix Workspaceアプリの自動更新サービスは、Citrix Workspaceアプリのアップデーターサービスを通じて、対象となるエンドポイント上のEPAクライアントを自動的にアップグレードします。

構成されたバージョンはポータルダウンロードオプションに表示され、エンドユーザーは自分でクライアントをダウンロードしてインストールまたはアップグレードします。

適用範囲: クラウドおよびオンプレミス。管理対象デバイスおよび非管理対象デバイス。

SCCM、Intune、Jamf、またはその他のエンドポイント管理ツールを使用してインストーラーをプッシュする

管理対象エンドポイントの場合、管理者はSCCM、Intune、Jamf、またはその他のエンドポイント管理ツールを使用して、Citrix Secure Access Endpoint Analysisインストーラーを配布できます。

1. [Citrix Downloads](#)からCitrix Secure Access Endpoint Analysisインストーラーをダウンロードします。
2. エンドポイント管理プラットフォームでインストーラーをパッケージ化します。
3. 標準のソフトウェア配布プロセスを使用して、必要な管理対象Windowsデバイスにパッケージを展開します。
4. Windowsコントロールパネルまたは管理インベントリからインストールされたバージョンを検証します。

適用範囲: クラウドおよびオンプレミス。管理対象デバイスのみ。

デバイスポスチャサービスコンソールで最小EPAクライアントバージョンを設定する

Device Postureサービスコンソールで、EPAクライアントの最小バージョンを設定できます。それより低いバージョンを実行しているクライアントには、ポータルにダウンロードオプションが表示され、エンドユーザーはクライアントをインストールまたはアップグレードできます。

1. Device Postureサービスコンソールで、Endpoint Analysis (EPA) クライアントの最小バージョンをターゲットバージョン (例: 26.5.1.7) に設定します。詳細については、「[Device Posture サービスによるEPAクライアントのバージョン管理](#)」を参照してください。

次のポスチャ評価時に、それより低いバージョンを実行しているクライアントには、ポータルにダウンロードオプションが表示されます。

2. エンドユーザーはクライアントをダウンロードしてインストールまたはアップグレードします。

注:

管理者権限でインストールしてください。そうしないと、インストールはユーザーモードで実行され、一部の機能が利用できない場合があります。

注:

この方法では、エンドユーザーにクライアントの更新を促します。サイレントアップグレードや自動アップグレードは強制されません。

適用範囲: クラウドのみ。エンドユーザーが通常管理者である、管理対象デバイスおよび管理対象外デバイス。

プラグインをNetScaler Gatewayポータルにアップロードする

Citrix Secure Access Endpoint Analysis プラグインをNetScaler Gatewayポータルにアップロードできます。ログオン時に、ゲートウェイはユーザーにクライアントのダウンロードまたはアップグレードを促します。

設定手順については、「[ユーザーがNetScaler Gatewayプラグインに接続する方法](#)」を参照してください。

注:

この方法は検出とプロンプトのみを行います。エンドユーザーは操作を拒否でき、サイレントセルフインストールは強制されません。

管理者権限でインストールしてください。そうしないと、クライアントはユーザーモードでインストールされ、一部の機能が利用できない場合があります。

適用範囲: オンプレミス。管理対象デバイスおよび管理対象外デバイスで、同じ検出とプロンプトの動作。

EPAクライアントをNetScalerおよびDevice Postureサービス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、エンドデバイスが最新のEPAクライアントバージョンを実行しているのに対し、NetScalerが異なるバージョンのEPAクライアントを使用しているシナリオが発生する可能性があります。この不一致により、NetScalerがエンドユーザーに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促すことがあります。この競合を避けるために、以下の構成変更をお勧めします。

- 適応型認証、オンプレミス認証、またはゲートウェイ仮想サーバーでEPAを設定している場合は、NetScalerで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。これにより、クライアントアプリ管理 (GACS) またはDevice Posture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します。
- CLIまたはGUIを使用して、EPAバージョン管理を**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: 適応型認証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を制御する](#)」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:Alw  
ays;vpn_linux:Always;\""
```

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

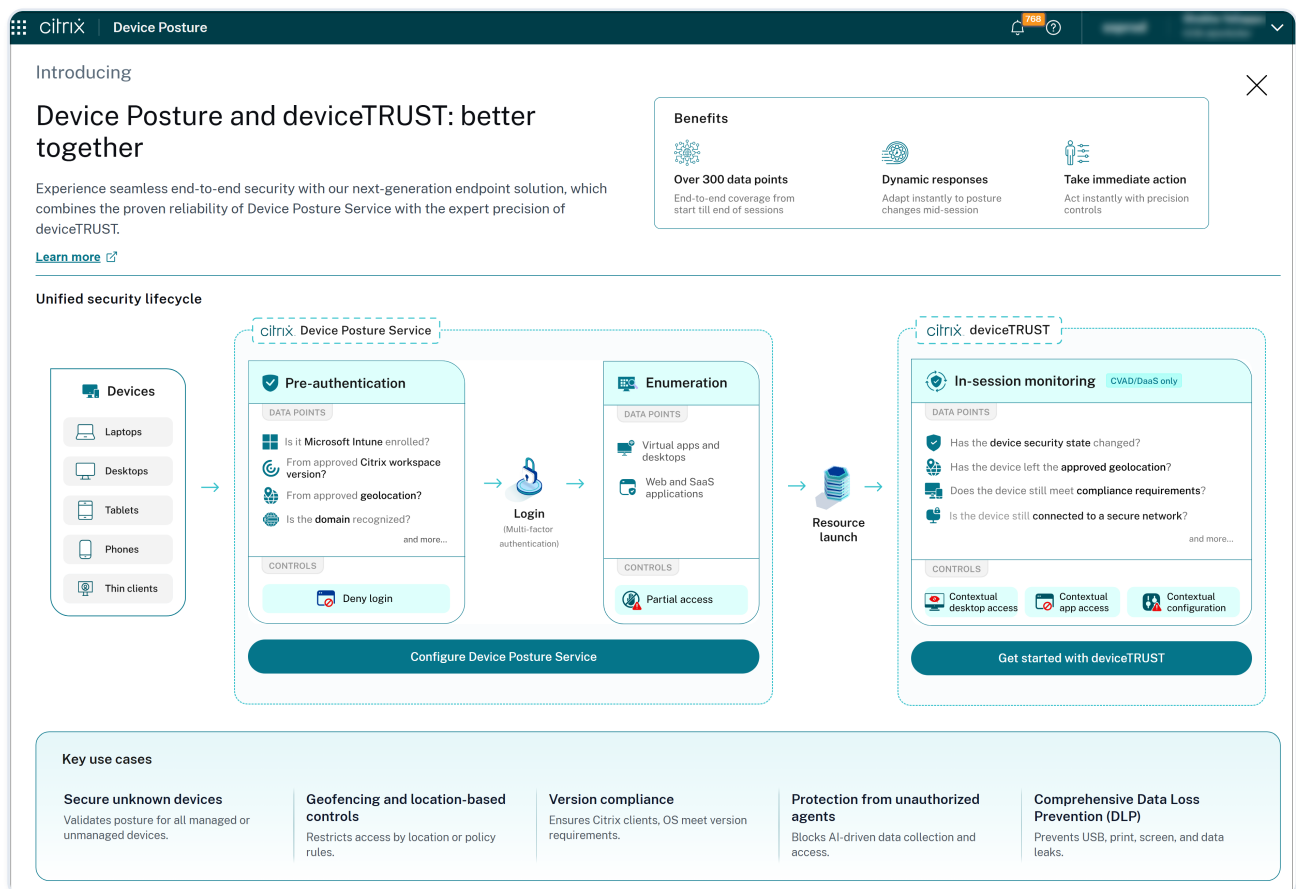
```
bind authentication vserver <Authentication_Vserver_Name> -policy  
<rewrite_action_policy> -priority 10 -type RESPONSE
```

Device PostureサービスとdeviceTRUST - より良い連携

企業アプリケーションとデータへのアクセスを保護するには、静的なポリシーだけでは不十分です。ユーザーのジャーニー全体で継続的に適応する、リアルタイムでコンテキストを認識した制御が必要です。Citrix Device PostureサービスとdeviceTRUSTの統合は、認証前、列挙、セッション中のあらゆるフェーズで、包括的なコンテキストアクセス範囲を提供します。

特定の環境向けにDevice PostureサービスとdeviceTRUSTを構成するには、次のトピックを参照してください。

- デバイスポスチャを使用したコンテキストアクセス（スマートアクセス）の構成
- deviceTRUST クイックセットアップ



Device PostureサービスとdeviceTRUSTの連携方法

以下のセクションでは、Device PostureサービスとdeviceTRUSTがどのように連携するかについて説明します。

認証前: ログイン前の信頼確立

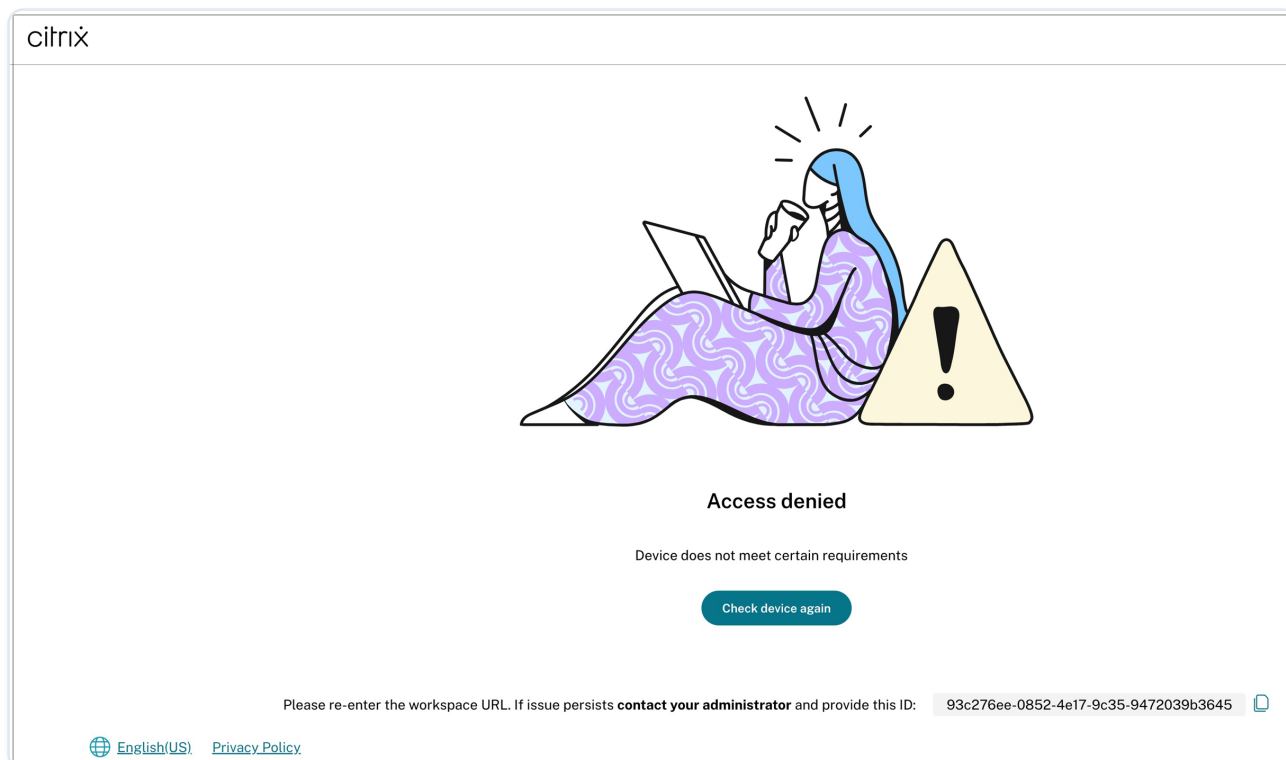
Device Postureサービスは、第一線の防御として機能し、ユーザーが認証を許可される前にエンドポイントの衛生状態チェックを実行します。管理者は、次のようなデバイスプロパティを検査するポリシーを定義できます。

- Citrix Workspaceアプリのバージョン
- OSバージョン
- セキュリティソフトウェアのステータス（ウイルス対策）
- MDMソリューションによる企業登録
- デバイス証明書
- 企業標準への準拠

デバイスがこれらの要件を満たさない場合、認証が開始される前にアクセスがブロックされます。

例:

ユーザーが個人デバイスからログインしようとする、Device Postureサービスはアンチウイルスソフトウェアがインストールされ、実行されていることを確認します。デバイスが管理者によって作成されたポリシー要件を満たさない場合、ログインは拒否され、信頼されたデバイスのみが機密リソースにアクセスできるようになります。

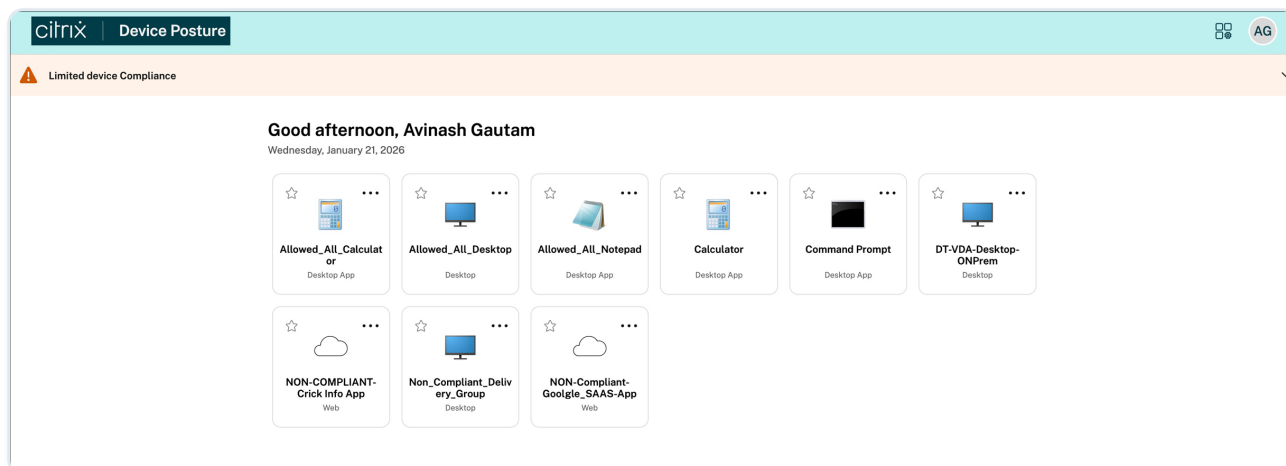


列挙: アプリケーションへのコンテキストに応じたアクセス

列挙フェーズ中、Device Postureサービスは、ユーザーがストアでアプリケーションを閲覧または列挙する際にデバイスのポスチャを評価することで、ポリシーの適用を継続します。管理者は、コンテキストに基づいて、どのアプリケーションまたはデスクトップが表示またはアクセス可能であることを制限できます。

例:

デバイスが準拠している場合、ユーザーはすべての権限のあるアプリケーションを表示できます。準拠していない場合、特定のアプリが非表示になったり、クリップボードやファイル転送機能の無効化など、アクセスが制限されたりする可能性があります。



セッション中: 継続的なコンテキストに応じたアクセス評価

セッションが確立されると、deviceTRUSTが引き継ぎ、継続的なセッション内コンテキストアクセス制御を提供します。ログイン時にのみデバイスのポスチャをチェックする従来のソリューションとは異なり、deviceTRUSTはセッション全体でデバイスのコンテキストを監視し、エンドポイントの条件が変化するにつれてポリシーの動的な適用を可能にします。

詳細な制御: 管理者は、デバイスのコンテキストが変更された場合（たとえば、不正なUSBスティックの接続、ファイアウォールの無効化、暗号化されていないWi-Fiへの接続、ネットワークロケーションの変更など）に、セッションの切断、ポップアップ通知、監査などのアクションを設定できます。

例:

ユーザーが準拠デバイスからセッションを開始します。セッション中に、deviceTRUSTは変更を検出します。たとえば、デバイスが保護されていないネットワークに接続されたり、禁止されている周辺機器が接続されたりした場合です。システムは自動的にアクセスを制限したり、セッションを切断したり、必要なアクションをユーザーに通知したりして、継続的なコンプライアンスを維持できます。

アクセス拒否メッセージ(/en-us/device-posture/media/device-posture-device-trust-access-denied-message.png)

Device PostureサービスとdeviceTRUST連携のユースケース

Device PostureサービスとdeviceTRUST連携は、次のようなさまざまな重要なユースケースをサポートします。

- バージョンコンプライアンス (承認されたオペレーティングシステムおよびアプリケーションバージョンへのアクセスを制限する)
- ジオフェンシング (デバイスの位置情報に基づいてアクセスを制御する)
- 次のようなセキュリティ状態の継続的な監視。
 - アンチウイルスステータス
 - 不正なソフトウェアエージェントからの保護 - クリップボード、ファイル転送、印刷の動的な制限による包括的なデータ損失防止 (DLP)
 - BYODシナリオにおける、不明または管理されていないデバイスの保護。

これらの機能により、管理者は動的なハイブリッド環境で継続的なコンプライアンスを維持し、リスクを軽減し、エンタープライズデータを保護できます。

バージョンコンプライアンス

承認されたバージョンのオペレーティングシステムとCitrix Workspaceアプリ (CWA) を実行しているデバイスのみがリソースにアクセスできるようにします。これにより、古くなったエンドポイントや脆弱なエンドポイントの接続を防ぎ、パッチが適用されていないシステムからのリスクを軽減します。

詳細なポリシー構成手順については、この[チュートリアル](#)を参照してください。

ジオフェンシング

デバイスの物理的な位置に基づいて、アプリケーションとデスクトップへのアクセスを制限します。たとえば、承認された国や企業オフィスからのみアクセスを許可し、デバイスが国境を越えた場合はアクセスを取り消します。

詳細なポリシー設定手順については、この[チュートリアル](#)を参照してください。

デバイスのセキュリティ状態の監視

アンチウイルスチェック: アンチウイルスチェックは、ログイン時およびユーザーセッション全体を通じて、信頼され保護されたデバイスのみがエンタープライズリソースにアクセスできるようにするための基本的なセキュリティ対策です。これは、デバイスのコンプライアンスが前提とされない動的、ハイブリッド、またはBYOD環境において特に重要です。

詳細なポリシー設定手順については、この[チュートリアル](#)を参照してください。

データガバナンス

このトピックでは、Device Postureサービスによるログの収集、保存、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。

データレジデンシー

Citrix Device Postureの顧客コンテンツデータは、AWSおよびAzureクラウドサービスに存在します。これらは、可用性と冗長性のために以下のリージョンにレプリケートされます。

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

以下は、サービス構成、ランタイムログ、およびイベントの異なる保存先です。

- システム監視およびデバッグログ用のSplunkサービスは、米国ロケーションのみです。
- 診断およびユーザーアクセスログ用のCitrix Analytics Serviceについては、詳細情報として[Citrix Analytics Service Data Governance](#)を参照してください。
- 管理者監査ログ用のCitrix Cloud System Logsサービス。詳細については、[Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations](#)を参照してください。

データ収集

Citrix Device Postureサービスにより、お客様管理者はDevice Posture UIを通じてサービスを構成できます。デバイスポスチャポリシーの構成とプラットフォームに基づいて、以下の顧客コンテンツが収集されます。

- 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インストールの更新の詳細
- 最終Windows更新の詳細
- ファイルシステム – ファイル名、ファイルハッシュ、変更時刻
- ドメイン名

サービスコンポーネントによって収集されるランタイムログについては、主要な情報は以下のとおりです。

- 顧客/テナントID
- デバイスID (Citrixが生成した一意の識別子)
- デバイスポスチャスキャン出力
- 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によって保護された宛先にログを送信します。

データ制御

Citrix Device Postureサービスは現在、顧客がログの送信をオフにしたり、顧客コンテンツがグローバルに複製されるのを防ぐためのオプションを提供していません。

データ保持

Citrix Cloud™のデータ保持ポリシーに基づき、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。

- 詳細については、Analyticsログの保持ポリシーに関する[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、90日後に最終的に削除されます。

データエクスポート

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。

- 管理者監査ログは、Citrix Cloud System Logコンソールからアクセスできます。
- デバイスポスチャサービスの診断ログは、Citrix Analytics Service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、ストレージのために顧客アカウントにアップロードされたデータ、またはCitrixがサービスを実行するためにアクセスを許可された顧客環境内のデータを意味します。
- 「ログ」とは、パフォーマンス、安定性、使用状況、セキュリティ、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の目的のために前述したCitrix Cloudサービスを意味します。