Citrix Workspace アプリ

Contents

Citrix Workspace アプリ

April 25, 2024

Citrix Workspace アプリについて

Citrix Workspace アプリは、エンドユーザーが生産性を維持するために必要なすべてのリソースへのすばやく、安全で、シームレスなアクセスを提供します。Citrix Workspace アプリには、仮想デスクトップ、仮想アプリ、Web および SaaS アプリへのアクセス、および組み込みブラウザーやシングルサインオン（どこからでも、どのデバイスからでも）などの機能へのアクセスが含まれます。

Citrix Workspace アプリは、クラウド環境とオンプレミス環境の両方のデバイスに展開できるクライアントアプリケーションです。以前は Citrix Receiver と呼ばれていた機能に基づいて構築されており、HDX、Citrix Gateway プラグイン、Secure Private Access などの Citrix のクライアントテクノロジが含まれています。

クライアントアプリは、Windows、macOS、Linux、iOS、Android などのすべてのクライアント OS で実行できるように最適化されています。ブラウザーからもアクセスできます。サポートされているブラウザーについて詳しくは、「Workspace Browser Compatibility」を参照してください。

Citrix Workspace アプリは、Citrix プロトコルと HDX（高品位のエクスペリエンス）を活用し、仮想アプリとデスクトップセッションに最適なパフォーマンスを提供します。機能の向上によって、安全なログインおよびインターネット閲覧エクスペリエンス、アプリとデスクトップの簡単な管理、高度な検索機能などを提供します。

> 注:
>
> アプリの UI は、リソースの展開環境、つまりクラウド（ワークスペースプラットフォームを利用）かまたはオンプレミス（StoreFront プラットフォームを利用）かによって異なる場合があります。

Citrix Workspace アプリで使用できる機能について詳しくは、Citrix Workspace アプリの機能マトリックスを参照してください。

LTSR と最新リリース（CR）の違いについて詳しくは、Citrix Workspace アプリのライフサイクルマイルストーンを参照してください。

Citrix Workspace アプリは、以下のオペレーティングシステム向けに提供されています:

- Android 向け Citrix Workspace アプリ
- ChromeOS 向け Citrix Workspace アプリ
- HTML5 向け Citrix Workspace アプリ
- iOS 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ

- Windows 向け Citrix Workspace アプリ
- Windows（ストア）向け Citrix Workspace アプリ

> 重要
>
> **Citrix Workspace** アプリの更新のために収集される重要なデータ:
>
> インターネットに接続されているデバイスの場合、Citrix Workspace アプリは追加の通知なしにデバイスにダウンロードしてインストールできる更新を確認し、利用可能であることをユーザーに通知する場合があります。このとき、一部の法域で IP アドレスが個人を特定できるとみなされる場合を除き、個人を特定できない情報のみが送信されます。

Global App Configuration Service を使用した **Citrix Workspace** アプリの構成

Global App Configuration Service は、Citrix Workspace アプリ設定を構成するための一元的なインターフェイスをエンドユーザーに提供します。単一のインターフェイスからクラウドストアとオンプレミスストアの両方の設定を構成できます。これらの設定は、管理対象デバイスと非管理デバイス（BYOD）の両方に適用されます。詳しくは、「Global App Configuration Service」を参照してください。

言語サポート

Citrix Workspace アプリは、英語以外の言語での使用に適応しています。このセクションでは、Citrix Workspace アプリの最新リリースでサポートされている言語について説明します。

次の表に、さまざまなオペレーティングシステムまたはプラットフォーム上で、Citrix Workspace アプリでサポートされている言語を示します。☑ は、その言語でアプリを使用できることを示しています。

言語	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows ストア
英語	☑	☑	☑	☑	☑	☑	☑	☑
デンマーク語	☑			☑				
オランダ語	☑	☑	☑	☑	☑	☑	☑	☑
フランス語	☑	☑	☑	☑	☑	☑	☑	☑
ドイツ語	☑	☑	☑	☑	☑	☑	☑	☑
イタリア語	☑	☑	☑	☑	☑	☑	☑	☑
日本語	☑	☑	☑	☑	☑	☑	☑	☑

言語	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows ストア
韓国語	☑	☑	☑	☑	☑		☑	☑
ポルトガル語（ブラジル）	☑	☑	☑	☑	☑	☑	☑	☑
ロシア語		☑	☑		☑		☑	☑
簡体字中国語	☑	☑	☑	☑	☑	☑	☑	☑
スペイン語	☑	☑	☑	☑	☑	☑	☑	☑
スウェーデン語	☑			☑				
繁体字中国語		☑	☑				☑	☑

フィーチャーフラグ

この記事では、フィーチャーフラグの管理と、フィーチャーフラグをサポートするさまざまな Citrix Workspace アプリについて説明します。

フィーチャーフラグ管理

実稼働環境の Citrix Workspace アプリで問題が発生した場合、機能が出荷された後でも、影響を受ける機能を Citrix Workspace アプリで動的に無効にすることができます。無効化するには、フィーチャーフラグと、LaunchDarkly と呼ばれるサードパーティ製サービスを使用します。ファイアウォールまたはプロキシが送信トラフィックをブロックしている場合を除いて、LaunchDarkly へのトラフィックを有効にするために構成する必要はありません。送信トラフィックがブロックされている場合、ポリシー要件に応じて、特定の URL または IP アドレス経由の LaunchDarkly へのトラフィックを有効にします。

次の表で、フィーチャーフラグをサポートするさまざまなアプリと、これらのアプリでフィーチャーフラグが導入されたリリースバージョンを一覧表示します。

アプリ	フィーチャーフラグのサポート	バージョン	ドキュメント
Android 向け Citrix Workspace アプリ	はい	10.7.5	Android 向け Citrix Workspace アプリのフィーチャーフラグ管理

アプリ	フィーチャーフラグのサポート	バージョン	ドキュメント
ChromeOS 向け Citrix Workspace アプリ	はい	1908	ChromeOS 向け Citrix Workspace アプリのフィーチャーフラグ管理
HTML5 向け Citrix Workspace アプリ	はい	1908	HTML5 向け Citrix Workspace アプリのフィーチャーフラグ管理
iOS 向け Citrix Workspace アプリ	はい	10.4.10	iOS 向け Citrix Workspace アプリのフィーチャーフラグ管理
Linux 向け Citrix Workspace アプリ	はい	2109	Linux 向け Citrix Workspace アプリのフィーチャーフラグ管理
Mac 向け Citrix Workspace アプリ	はい	2010	Mac 向け Citrix Workspace アプリのフィーチャーフラグ管理
Windows 向け Citrix Workspace アプリ	はい	2012	Windows 向け Citrix Workspace アプリのフィーチャーフラグ管理

Citrix Receiver に関する重要なお知らせ

2018 年 8 月、Citrix Receiver は Citrix Workspace アプリに置き換えられました。以前のバージョンの Citrix Receiver は引き続きダウンロードいただくことができますが、Citrix Workspace アプリの新機能と拡張機能がリリースされることになります。

Citrix Workspace アプリは新しい Citrix クライアントで、Citrix Receiver と同様の機能を持ち、お客様の組織の Citrix インフラストラクチャと完全に後方互換性があります。Citrix Workspace アプリでは、Citrix Receiver のすべての機能と、組織の Citrix 環境に応じた新しい機能を提供します。

Citrix Workspace アプリは Citrix Receiver テクノロジをベースに構築されており、すべての Citrix ソリューションと完全に後方互換性があります。

詳しくは、Workspace アプリに関する FAQ ページを参照してください。

Citrix Workspace Web 拡張機能

April 25, 2024

Citrix Workspace Web 拡張機能を使用すると、`.ica`ファイルなしで Workspace アプリをどこからでも起動できるため、エクスペリエンスがより安全で信頼性の高いものになります。ブラウザー拡張機能を使用してアプリを開くと、すべてのアプリとデスクトップが 1 つの場所に保持されるため、作業を簡単に追跡できる整然としたデスクトップが実現します。Citrix Workspace Web 拡張機能は、画面キャプチャ対策のアプリ保護とシームレスなサービス継続性というメリットも提供します。

Citrix Workspace Web 拡張機能をインストールする

Citrix Workspace Web 拡張機能をインストールするには、次の手順に従います:

1. ブラウザーの Web ストアに移動します。
    - Chrome ウェブストア
    - Microsoft Edge アドオン
    - Mac App Store
2. 使用するブラウザーのアプリストアを介して Citrix Workspace Web 拡張機能のインストールを追加し、確認します。
3. 必要に応じて、Web 拡張機能を追加するポップアップメッセージを確認します。
4. （オプション）ブラウザーの右上にあるパズルピースアイコンを選択して、簡単にアクセスできるようにブラウザーを固定します。
5. ［拡張機能を追加］を選択します。
6. ピンアイコンを選択して、拡張機能を固定します。

これで、Citrix Workspace Web 拡張機能がインストールされました。

Citrix Workspace Web 拡張機能について詳しくは、Citrix Workspace Web 拡張機能に関するブログを参照してください。

Citrix Workspace インスタンス内で SaaS アプリを開く

使用中の Workspace インスタンスで Citrix Workspace Web 拡張機能がまだ有効になっていない場合は、次の手順に従います:

1. Workspace ウィンドウでアカウントプロファイルを選択します。
2. プロファイルメニューから ［詳細］を選択します。

3. ［アプリおよびデスクトップの起動設定］ウィンドウで ［**Web** ブラウザーを使用］を選択します。
4. ポップアップウィンドウで ［**Open Citrix Workspace Launcher**］を確認します。

これで、SaaS アプリが Citrix Workspace アプリウィンドウ内で開くようになりました。

Citrix Workspace アプリの機能マトリックス

Citrix Workspace アプリは、さまざまなプラットフォームまたはオペレーティングシステムに分散されたさまざまな機能を提供します。この機能マトリックスを見れば、さまざまなプラットフォームでの機能の可用性を明確に理解できます。

Citrix Workspace Web 拡張機能は、サポートされている Web ブラウザーとインターネット接続があれば、どのコンピューターからでもアクセスできます。Citrix Workspace Web 拡張機能のすべての機能を使用する場合、次の種類のブラウザーがサポートされています:

ブラウザー名	バージョン
Google Chrome	最新バージョン
Microsoft Edge	最新バージョン
Apple Safari	最新バージョン

App Protection

March 10, 2024

App Protection は、Citrix Workspace アプリの機能で、Citrix Virtual Apps and Desktops 公開リソースの使用時にセキュリティを強化する機能です。App Protection は、オンプレミスの Citrix Virtual Apps and Desktops 展開と、StoreFront および Workspace を使用した Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）でサポートされています。これは、App Protection がすべてのクラウド環境、オンプレミス環境、およびハイブリッド環境でサポートされていることを意味します。App Protection は、ADC ゲートウェイ経由で StoreFront または Workspace に接続している場合にもサポートされます。

2 つのポリシーは Citrix HDX セッションでキーロガー対策および画面キャプチャ対策機能を提供します。Windows 向け Citrix Workspace アプリ 2203.1 LTSR 以降、Mac 向け Citrix Workspace アプリ 2001 以降、または Linux 向け Citrix Workspace アプリ 2108 のこれらのポリシーは、キーロガーやスクリーンスクレーパーからデータを保護するのに役立ちます。

キーロガー対策を有効にした場合:

- キーロガーには暗号化されたキーストロークが表示されます。

- この機能は、保護ウィンドウにフォーカスがある場合にのみアクティブになります。

画面キャプチャ対策が有効な場合:

- Windows OS および macOS では、画面をキャプチャするときに、保護されたウィンドウのコンテンツのみが空白になります。保護されたウィンドウが最小化されていない場合に、この機能がアクティブになります。Linux OS では、キャプチャ全体が空白になります。この機能は、保護されたウィンドウが最小化されているかどうかに関係なくアクティブです。
- Windows OS の **Print Screen** ボタンを使用してスクリーンショットを撮る場合、データはクリップボードにコピーされません。**Print Screen** ボタンを使用してスクリーンショットを撮るには、保護されているアプリを最小化します。

ポリシーは PowerShell および Web Studio で構成できます。詳しくは、「Virtual Apps and Desktops での App Protection の構成」を参照してください。

この機能の購入後、App Protection ライセンスを有効にしてください。

> 免責事項:
>
> App Protection ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングすることで有効になります（画面のキャプチャまたはキーボードの操作が必要な特定の API 呼び出し）。つまり、この App Protection ポリシーは、カスタムの目的別に構築されたハッカーツールに対しても保護を提供できます。ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てくる場合があります。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。
>
> Citrix App Protection ポリシーは、ICA ファイルなど、基盤となるオペレーティングシステムのコンポーネントと効果的に連携します。ポリシーの整合性を保つため、基盤となるコンポーネントの意図的な改ざんまたは変更が検出された場合、Citrix はサポートを提供できないことがあります。

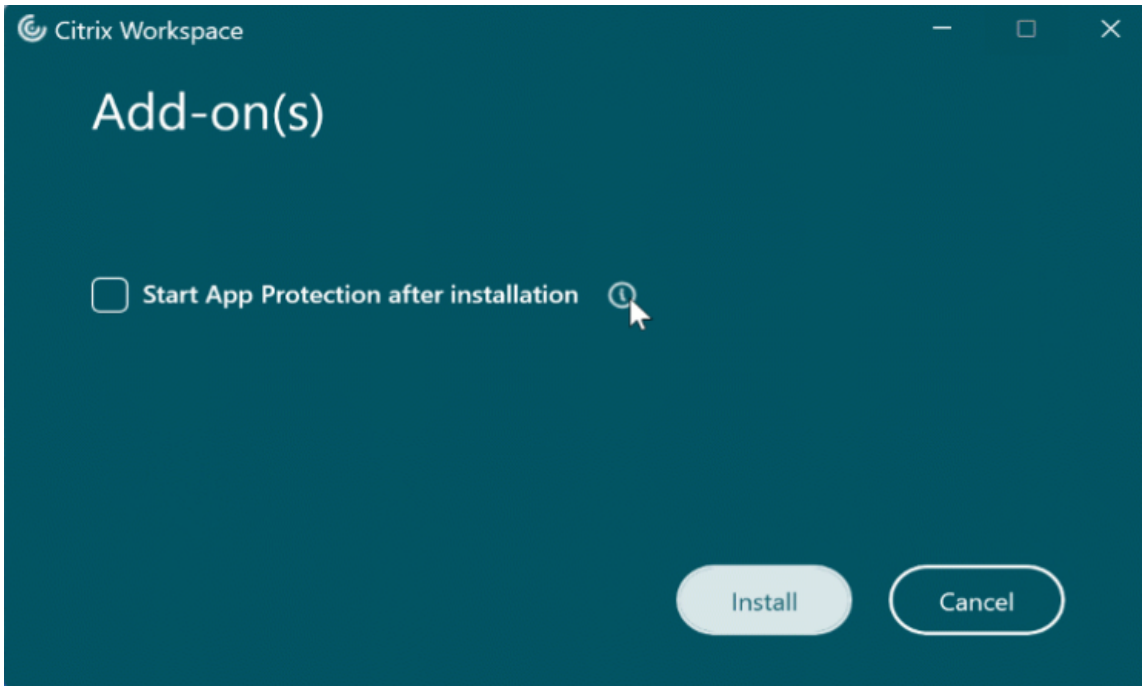
App Protection がインストールされているかの確認

Windows 向け **Citrix Workspace** アプリ

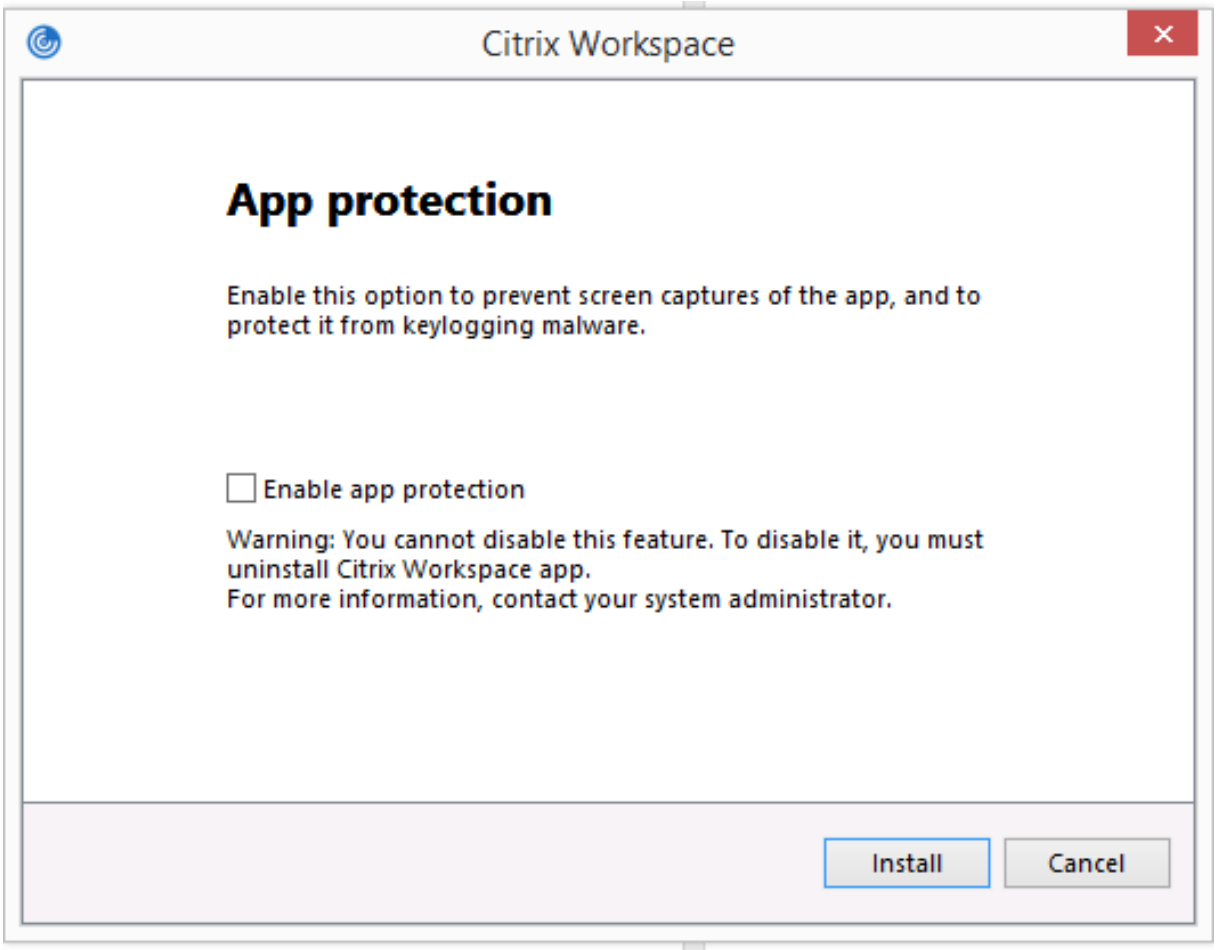
Citrix Workspace アプリバージョン 2212 以降では、App Protection がデフォルトでインストールされます。ただし、ユーザーが［インストール後に **App Protection** を開始する］チェックボックスをオンにしたかどうかによって、コンポーネントがアクティブまたは休止状態になる場合があります。

- 2311 より前のバージョンの Citrix Workspace アプリの場合:

- Citrix Workspace アプリのバージョン 2311 以降:



2212 より前の Citrix Workspace アプリのバージョンでは、Citrix Workspace アプリのインストール時に ［**App Protection** を有効にする］チェックボックスをオンした場合にのみ、App Protection がインストールされ、アクティブな状態になります。



App Protection は、**STOPPED** 状態または **RUNNING** 状態のいずれかになります。

サービスの状態を確認するには、次のいずれかの手順を実行します:

- Citrix Workspace アプリのバージョン 2206 以降の場合は、次のコマンドを実行します。

```
sc query appprotectionsvc
<!--NeedCopy-->
```



```
Command Prompt
Microsoft Windows [Version 10.0.19044.2604]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>sc query appprotectionsvc

SERVICE_NAME: appprotectionsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\WINDOWS\system32>
```

- Citrix Workspace アプリのバージョン 2206 より前の場合は、次のコマンドを実行します:

```
sc query entryprotectsvc
<!--NeedCopy-->
```

```
C:\Users\[redacted]>sc query entryprotectsvc

SERVICE_NAME: entryprotectsvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

> 注:
>
> 2212 より前の Citrix Workspace アプリのバージョンでは、Citrix Workspace アプリのインストール時に [**App Protection** を有効にする] チェックボックスをオンにせず、前述のコマンドを実行して状態をチェックしなかった場合、次のエラーメッセージが表示されます:
>
> ```
> C:\Windows\system32>sc query appprotectionsvc
> [SC] EnumQueryServicesStatus:OpenService FAILED 1060:
>
> The specified service does not exist as an installed service.
> ```

さまざまな環境での **App Protection** の動作

App Protection の動作は、App Protection ポリシーで構成されたリソースへのアクセス方法によって異なります。このようなリソースとしては、Virtual Apps and Desktops、内部 Web アプリ、SaaS アプリがあります。リソー

スには、サポートされるネイティブの Citrix Workspace アプリクライアントまたは Web ブラウザーを使用してアクセスできます。App Protection は環境によって異なる方法で動作します:

- サポートされていない **Citrix Receiver** または **Citrix Workspace** アプリ - App Protection ポリシーで構成されたリソースは利用できません。
- サポートされている **Citrix Workspace** アプリのバージョン - App Protection ポリシーで構成されたリソースが利用可能であり、適切に起動します。
- **Workspace** ストア **URL** を使用したハイブリッド起動 - App Protection ポリシーで構成されたリソースは常に利用可能です。Workspace ストア URL を使用して Web ブラウザーでリソースを正常に起動するには、「Workspace のハイブリッド起動の App Protection」を参照してください。
- **StoreFront** ストア **URL** を使用したハイブリッド起動 - StoreFront カスタマイズが展開されていない場合、App Protection ポリシーで構成されたリソースは使用できません。StoreFront ストア URL を使用して Web ブラウザーでリソースを正常に起動するには、「StoreFront のハイブリッド起動による App Protection」を参照してください。

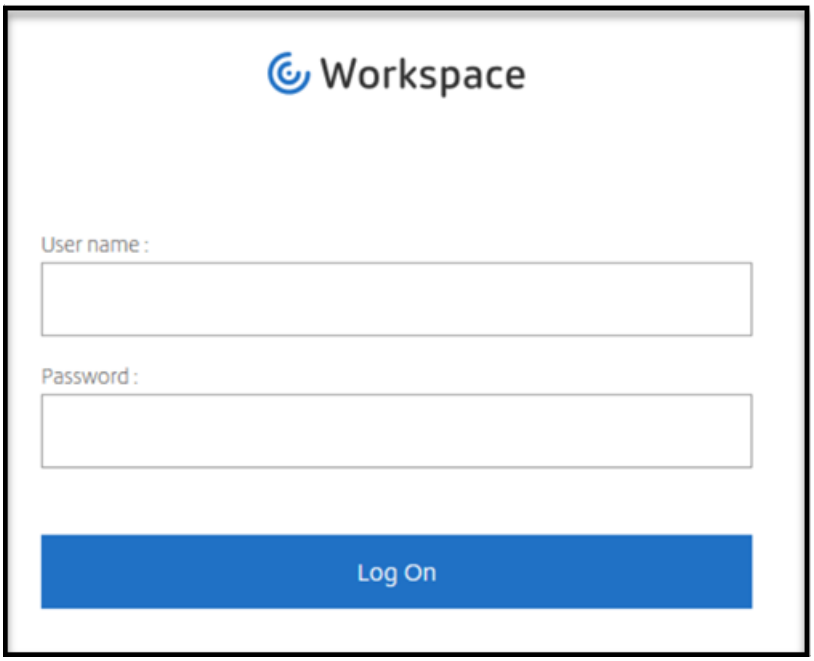
以下の条件下で保護が適用されます:

- 画面キャプチャ対策 - Windows 向け Citrix Workspace アプリおよび Mac 向け Citrix Workspace アプリでは、保護されたウィンドウが画面に表示されている場合に有効になります。保護を無効にする場合は、すべての保護ウィンドウを最小化します。Linux 向け Citrix Workspace アプリでは、保護されたウィンドウがアクティブな場合に有効になります。保護を無効にする場合は、すべての保護ウィンドウを閉じます。
- キーロガー対策 - 保護されたウィンドウにフォーカスがある場合に有効になります。保護を無効にする場合は、フォーカスを別のウィンドウに移動します。

App Protection によって保護される内容

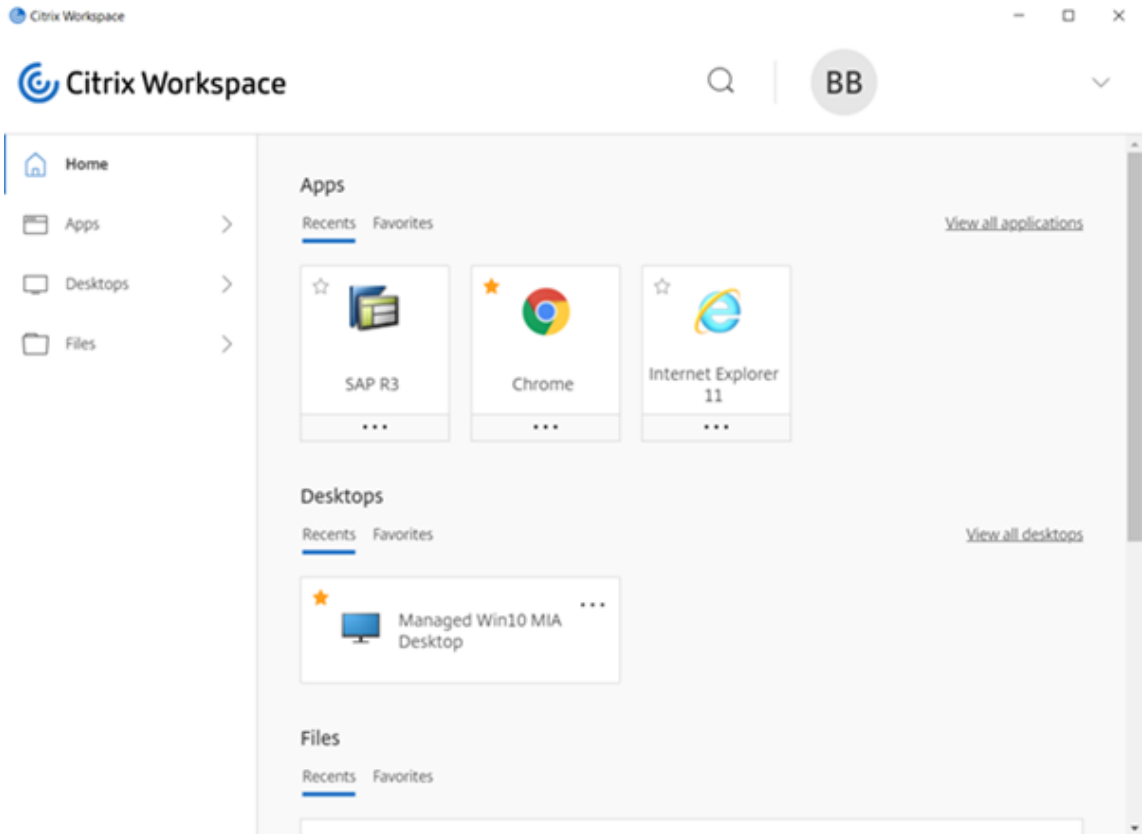
App Protection は次の Citrix のウィンドウを保護します:

- Citrix サインインウィンドウ

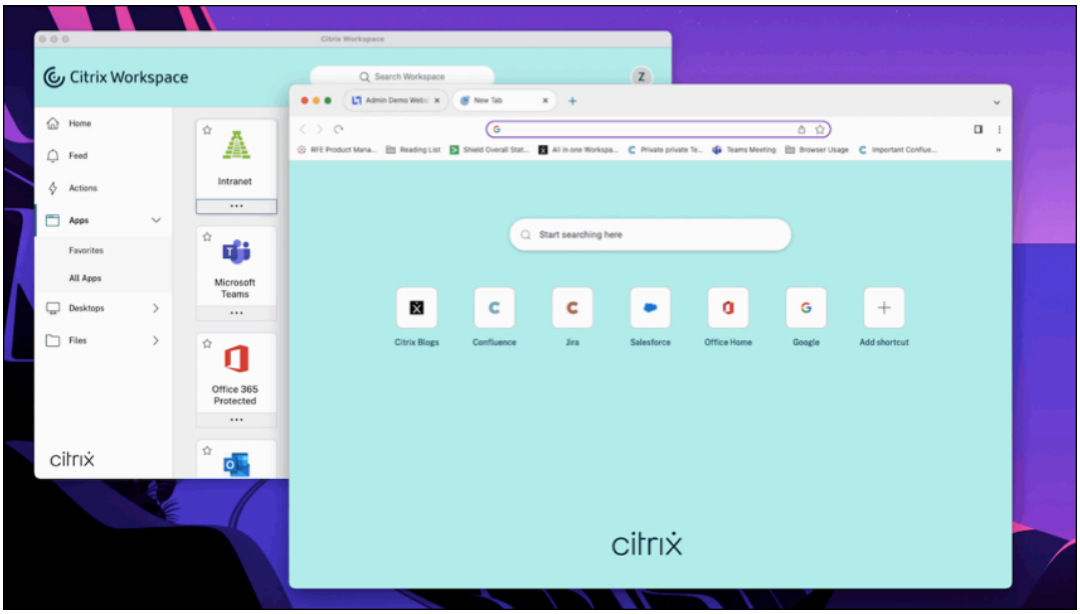


- Citrix Workspace アプリの HDX セッションウィンドウ（管理対象デスクトップなど）

- セルフサービスストアウィンドウ



- Web および SaaS アプリ
  - Windows 向け Citrix Workspace アプリおよび Mac 向け Citrix Workspace アプリ - Citrix Enterprise Browser で、Web アプリと SaaS アプリを開きます。Citrix Secure Private Access によりアプリに App Protection ポリシーが構成されている場合、App Protection はタブごとに適用されます。



  - Linux 向け Citrix Workspace アプリ - Citrix Enterprise Browser はサポートされていません。

App Protection によって保護されない内容

- ナビゲーションバーの Citrix Workspace アプリアイコンの以下の項目:
  - コネクションセンター
  - 高度な設定のすべてのリンク
  - 個人設定
  - 更新プログラムのチェック
  - サインアウト
- 画面キャプチャ対策で仮想デスクトップを保護することを選択した場合でも、ユーザーは仮想デスクトップ内のアプリから画面を共有できます。ただし、仮想デスクトップの外部にあるアプリについては、スクリーンショットを撮ったり、仮想デスクトップを記録したりすることはできません。

制限事項

以下の制限は設計段階で存在します:

- RDP セッション内でアクセスすると、App Protection が有効になっている Virtual Apps and Desktops の起動がブロックされます。
- App Protection は、ダブルホップおよびマルチホップのシナリオではサポートされません。
- Citrix Workspace アプリまたは Citrix Receiver のサポートされていないバージョンを使用する場合、App Protection はサポートされません。この場合、リソースは非表示になります。
- App Protection 機能が Virtual Apps and Desktops に適用されている場合、最適化を使用すると発信画面共有が影響を受ける可能性があります。
- App Protection 機能を備えた Citrix Workspace アプリは、同様の基盤となる技術を使用する他のセキュリティソリューションまたはアプリと互換性がない場合があります。
- Citrix Secure Browser 内からリソースを起動する場合、または Remote Browser Isolation を使用してリソースを起動する場合、App Protection はサポートされません。
- Linux 向け Citrix Workspace アプリでは、App Protection がインストールされている場合、スナップアプリケーションを使用できません。

コンテキストに基づく **App Protection**

コンテキストに基づく App Protection により、ユーザー、ユーザーのデバイス、ネットワークポスチャなど、ユーザーのサブセットを条件にして、App Protection ポリシーを詳細かつ柔軟に適用できます。詳しくは、次の記事を参照してください:

- StoreFront のコンテキストに基づく App Protection

- Workspace のコンテキストに基づく App Protection

ハイブリッド起動の **App Protection**

Citrix Virtual Apps and Desktops のハイブリッド起動は、ブラウザー（Citrix Workspace for Web）から Citrix Workspace アプリにログインし、ネイティブの Citrix Workspace アプリでアプリケーションを使用する場合の起動です。ハイブリッドという用語は、ユーザーが Citrix Workspace for Web アプリとネイティブの Citrix Workspace アプリの組み合わせでリソースに接続して使用することを意味します。App Protection は、Workspace と StoreFront でのハイブリッド起動をサポートしています。詳しくは、次の記事を参照してください：

- Workspace のハイブリッド起動の App Protection
- StoreFront のハイブリッド起動による App Protection

システム要件と互換性

April 10, 2024

システム要件

前提条件として、管理者権限を使用して Citrix Workspace アプリをインストールしてください。

Citrix コンポーネントの最小バージョン

- Linux 向け Citrix Workspace アプリ 2108
- Windows 向け Citrix Workspace アプリ 2203.1 LTSR
- Windows 向け Citrix Workspace アプリ 2002
- Windows（ストア）向け Citrix Workspace アプリ 2305.1
- Mac 向け Citrix Workspace アプリ 2001
- StoreFront 1912 LTSR
- Delivery Controller 1912
- 有効な Citrix ライセンス。詳しくは、Citrix の営業担当者または Citrix パートナーにお問い合わせください。

> 注：
>
> ユーザーが App Protection をサポートしていないデバイスまたは Workspace アプリのバージョンを使用

> している場合、保護されたリソースにアクセスできません。保護されたリソースには、Virtual Apps and Desktops や Web アプリおよび SaaS アプリが含まれます。

ライセンス

次のセクションでは、製品、プラットフォーム、ユースケースに基づいて、App Protection を利用できるさまざまな種類のライセンスについて説明します。

IT 管理の VDI　IT 管理の VDI のすべてのエディションで、App Protection はアドオンとして利用できます。詳しくは、「IT 管理の VDI」を参照してください。

ハイパースケーラー向け **Citrix DaaS**

- Azure
- Google
- AWS

Citrix DaaS　「Feature Matrix for Citrix DaaS」の記事で、「**DaaS cloud Services**」>「**Security and Monitoring**」>「**App Protection**」にアクセスしてください。

Citrix Secure Private Access　App Protection は、Citrix Secure Private Access のスタンドアロンの添付ファイルとして利用できます。詳しくは、「Service descriptions for Citrix Services」の記事の「**Citrix Cloud Services**」>「**Citrix Secure Private Access**」にアクセスしてください。

Citrix Universal サブスクリプション　App Protection は次のサービスに含まれています:

- Citrix Universal Premium
- Citrix Universal Premium Plus

次のエディションのアドオンとして利用できます:

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

詳しくは、こちらの記事を参照してください。

オペレーティングシステムプラットフォーム

App Protection ポリシーランタイムは、接続元のエンドポイントにインストールされ、接続先の VDA にはインストールされません。そのため、重要になるのはエンドポイントのオペレーティングシステムのバージョンだけです。（App Protection は、「Citrix Virtual Apps and Desktops のシステム要件」記載のサポートされるオペレーティングシステム上にホストされている VDA に接続できます。）

App Protection 機能は、次のオペレーティングシステムを実行しているエンドポイントでサポートされています：

- **Windows**：
  - Windows 11（64 ビット版）
  - Windows 10（32 ビット版および 64 ビット版）

    > 注：
    >
    > App Protection は、Windows オペレーティングシステムの Arm64 版を搭載したデバイスではサポートされません。

- **macOS**：
  - High Sierra（10.13）以降
- **Linux**：
  - 64 ビット Ubuntu 22.04
  - 64 ビット RHEL 9
  - ARM64 Raspberry Pi OS（Debian 11（bullseye）ベース）

> 注：
>
> App Protection を使用するには、Linux 向け Citrix Workspace アプリに、サポートされているオペレーティングシステムのほかに Gnome Display Manager が必要です。

互換性マトリックス

Citrix Cloud ベースの製品の互換性マトリックス

Citrix Cloud ベースの製品と互換性のある App Protection 機能は次のとおりです。

機能	Citrix Cloud	Citrix Cloud Japan
仮想アプリとデスクトップのキーロガー対策と画面キャプチャ対策	はい	はい

機能	Citrix Cloud	Citrix Cloud Japan
Web または SaaS アプリのキーロガー対策と画面キャプチャ対策	はい	いいえ
Windows 用の DLL 対策	はい	グループ ポリシー オブジェクト (GPO) を介してはい
DLL 対策の許可リスト	はい	GPO を介してはい
Global Admin Configuration Service（GACS）	はい	いいえ
Linux の認証またはセルフサービスプラグイン画面の保護	はい	AuthManConfig.xml を介してはい
Mac の認証またはセルフサービスプラグイン画面の保護	GACS を介してはい	GACS を介してはい
Windows の認証またはセルフサービスプラグイン画面の保護	はい	GPO を介してはい
CAS App Protection のスクリーンショットイベント	はい	いいえ
コンテキストに基づく App Protection	はい	ユーザーに基づいてはい
ポリシーの改ざんの検出	はい	はい
App Protection のセキュリティ態勢チェック	はい	はい
ローカルアプリの許可リストまたはフィルター - Windows	はい	GPO を介してはい
ローカルの App Protection - Windows	はい	GPO を介してはい

App Protection 機能

April 25, 2024

この記事では、Windows 向け Citrix Workspace アプリ、Linux 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリによってサポートされる App Protection 機能について説明します。

キーロガー対策

暗号化を使用すると、App Protection のキーロガー対策機能により、ユーザーが物理キーボードとスクリーンキーボードの両方で入力しているテキストが暗号化されます。キーロガー対策機能は、キーロガーツールがテキストにアクセスする前に、カーネルまたは OS レベルでテキストを暗号化します。クライアントエンドポイントにインストールされたキーロガーは、OS またはドライバーからデータを読み取り、ユーザーが入力しているキーストロークの代わりにハッシュ化されたテキストをキャプチャします。App Protection ポリシーは、公開アプリケーションとデスクトップだけでなく、Citrix Workspace 認証ダイアログに対しても有効です。Citrix Workspace は、ユーザーが最初の認証ダイアログを開いた瞬間から保護されます。App Protection はキーストロークを暗号化し、解読できないテキストをキーロガーに返します。

管理者は、次の種類のリソースに対してキーロガー対策を有効にすることを選択できます:

- Virtual Apps and Desktops
- 社内 Web アプリと SaaS アプリ
- 認証画面
- Self-Service Plug-in（SSP）画面

画面キャプチャ対策

画面キャプチャ対策は、アプリが仮想アプリまたはデスクトップセッション内で画面のスクリーンショットや録画を試みることを防ぎます。画面キャプチャソフトウェアは、キャプチャ領域内のコンテンツを検出できません。アプリによって選択された領域がグレー表示になります。または、アプリはコピーするはずの画面セクションの代わりに何もキャプチャしません。画面キャプチャ対策機能は、Windows の
切り取り & スケッチ、Snipping Tool、**Shift + Ctrl + Print Screen** キーに適用されます。

画面キャプチャ対策のもう 1 つのユースケースは、GoToMeeting、Microsoft Teams、Zoom などの仮想会議や Web 会議アプリケーションで機密データの共有を防止することです。App Protection は、アプリが保護されている場合に Web 会議で空白の画面を返すことで、意図しない共有を防ぎます。この機能により、機密データが組織から誤って漏えいすることがなくなります。この機能は、データ侵害を開示する場合の意図を問わないため、規制された業界でのコンプライアンスに役立ちます。

管理者は、次の種類のリソースに対して画面キャプチャ対策を有効にすることを選択できます:

- Virtual Apps and Desktops
- 社内 Web アプリと SaaS アプリ
- 認証画面
- Self-Service Plug-in（SSP）画面

> 注:
>
> 2 つの仮想デスクトップを起動し、一方の仮想デスクトップでは画面キャプチャ対策機能が有効になっており、もう一方の仮想デスクトップでは画面キャプチャ対策機能が有効になっていない場合、画面キャプチャ対策機

> 能は両方の仮想デスクトップに適用されます。どちらの仮想デスクトップでもスクリーンショットを撮ることはできません。
>
> 画面キャプチャ対策が有効になっている仮想デスクトップを最小化した場合でも、画面キャプチャ対策機能は画面キャプチャ対策機能のない仮想デスクトップに引き続き適用されます。

画面キャプチャの検出と通知

Windows 向け Citrix Workspace アプリでは、保護されたリソースで画面キャプチャが試行された可能性がある場合に、通知を表示できます。App Protection によって保護されるリソースについては、「[App Protection によって保護される内容]」を参照してください (/en-us/citrix-workspace-app/app-protection.html#what-does-app-protection-protect)

次の場合に通知が表示されます:

- 画面キャプチャツールを使用して、スクリーンショットを撮ったり、ビデオを録画したりしようとした。
- Print Screen キーを使用してスクリーンショットを撮ろうとした。

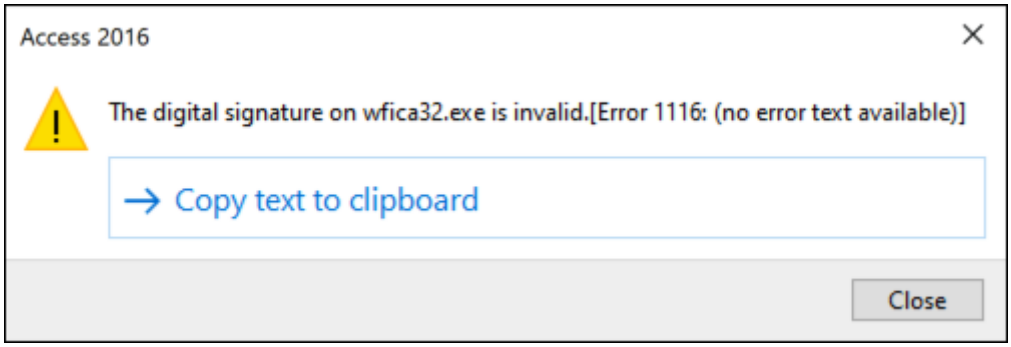
> 注:
>
> - この通知は、スクリーンショットツールの実行中のインスタンスごとに 1 回だけ表示されます。ツールを再起動して画面をキャプチャしようとすると、通知が再度表示されます。
> - Windows 向け Citrix Workspace アプリ 2212 以降では、サインインウィンドウとセルフサービス（ストア）ウィンドウはデフォルトで保護されていません。

DLL インジェクション対策

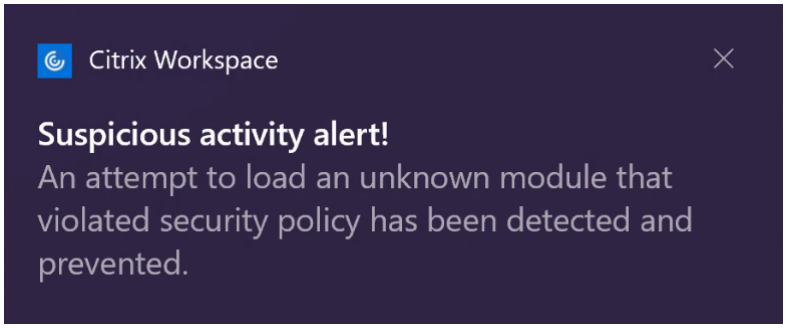
DLL インジェクション対策はセキュリティが強化され、Citrix Workspace アプリを特定の不正なダイナミックリンクライブラリ（DLL）または信頼されていないモジュールから保護します。こうした信頼できないモジュールがインジェクトされた場合、Citrix Workspace アプリはこれらの介入を検出し、そのモジュールの読み込みを停止します。また、セッションの起動前に信頼できないまたは悪意のある DLL が検出された場合、App Protection はセッションの起動をブロックし、エラーメッセージを表示します。エラーメッセージを閉じると、仮想アプリと仮想デスクトップのセッションが終了します。

この機能は、保護されたすべての仮想アプリとデスクトップ、および Citrix Workspace アプリの認証ウィンドウ（オンプレミス展開/StoreFront）に適用できます。

特定の信頼できない、または悪意のある DLL が保護されたコンポーネントに存在する場合、すぐにセッションを終了します。



この機能強化では、信頼されていない、または悪意のある DLL がブロックされたときに通知を表示します。メッセージを閉じると、仮想アプリと仮想デスクトップのセッションが終了します。



免責事項：この機能はオペレーティングシステムの必須機能へのアクセス（DLL の読み 込みが必要な特定の API 呼び出し）をフィルタリングすることで機能します。これにより、この機能は、目的別に構築された特定のカスタムのハッカーツールからも保護できます。ただし、オペレーティングシステムの進化とともに、DLL の読み込みにも新しい方法が出てきます。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。

この機能は、Windows 向け Citrix Workspace アプリバージョン 2206 以降でサポートされています。

> 注：
>
> 以前は、Citrix 認証画面と Citrix Workspace アプリ画面では、スクリーンキャプチャ対策機能とキーロギング防止機能がデフォルトで適用されていました。しかし、2212 以降、これらの機能はデフォルトで無効となり、現在はグループポリシーオブジェクトを使用して構成する必要があります。GPO 構成について詳しくは、「App Protection 構成の機能強化」を参照してください。

Microsoft Teams の HDX 最適化との互換性

最適化された Microsoft Teams は、App Protection が有効になっている Citrix Workspace アプリが Desktop Viewer モードの場合にのみ、画面共有をサポートします。Microsoft Teams で［コンテンツを共有］をクリックすると、画面選択メニューに次のオプションが表示されます：

- 開いているアプリを共有する ［ウィンドウ］オプション - このオプションは、VDA バージョンが 2109 以降の場合にのみ表示されます。

- VDA デスクトップ上のコンテンツを共有する ［デスクトップ］オプション - このオプションは、Citrix Workspace アプリの次のバージョンでのみ表示されます:
  - Linux 向け Citrix Workspace アプリバージョン 2311 以降
  - Mac 向け Citrix Workspace アプリバージョン 2308 以降
  - Windows 向け Citrix Workspace アプリバージョン 2309 以降

> 注:
>
> Linux 向け Citrix Workspace アプリの場合、デスクトップ共有オプションはデフォルトで無効になっています。これを有効にするには、次のように *config.json* ファイルに `UseGbufferScreenSharing`パラメーターを追加します:
>
> ```
> mkdir -p /var/.config/citrix/hdx_rtc_engine
> vim /var/.config/citrix/hdx_rtc_engine/config.json
> {
>
>  "UseGbufferScreenSharing":1
>  }
>
> <!--NeedCopy-->
> ```

App Protection が有効になっている最適化された Microsoft Teams は、仮想モニターを個別に共有できる Citrix 仮想モニターレイアウトもサポートしています。

> 制限事項:
>
> - App Protection が有効になっている最適化された Microsoft Teams は、ローカルアプリアクセス (LAA) が有効になっている公開デスクトップでの画面共有をサポートしていません。
> - BCR を使用したブラウザーコンテンツなど、クライアントがレンダリングしたコンテンツはキャプチャまたは共有できません。画面をキャプチャしようとすると、黒い画面として表示されます。
>
> 注:
>
> Linux 向け Citrix Workspace アプリの場合、この機能は Technical Preview 段階にあります。

ローカルの **App Protection**（プレビュー）

App Protection は、エンドポイントでキーロガー、偶発的および悪意のあるスクリーンキャプチャから顧客を守るために強化されたセキュリティを提供します。現在、App Protection 機能は Workspace リソースに対してのみ提供されています。この機能により、App Protection 機能はエンドポイント上のローカルアプリに拡張されます。Windows 向け Citrix Workspace アプリ 2210 以降、Windows デバイスのローカルアプリに App Protection を適用できます。

Podio フォームを使用して、この機能のプレビューに登録してください。

ポリシーの改ざんの検出

ポリシー改ざん検出機能は、App Protection の画面キャプチャ対策ポリシーとキーロガー対策ポリシーが改ざんされている場合、ユーザーが仮想アプリまたはデスクトップセッションにアクセスできないようにします。ポリシーの改ざんが検出された場合、仮想アプリまたはデスクトップセッションは終了します。

> 注:
>
> ポリシー改ざん検出機能は、将来のバージョンではデフォルトで有効になる予定です。

ポリシー改ざんの検出を構成するには、「ポリシー改ざん検出の構成」を参照してください。

セキュリティ態勢チェック

ポリシー改ざん検出機能をサポートしていないバージョンの Citrix Workspace アプリから App Protection ポリシーで有効になっている仮想アプリおよびデスクトップの起動を検出してブロックするには、App Protection のセキュリティ態勢チェックを有効にします。

> 注:
>
> セキュリティ態勢チェックが有効で、セキュリティ態勢チェックをサポートしていないバージョンの Citrix Workspace アプリを使用している場合、App Protection ポリシーが有効になっているセッションは終了します。

セキュリティ態勢チェックを構成するには、「セキュリティ態勢チェックの構成」を参照してください。

> 制限事項:
>
> Microsoft Azure でホストされている Windows Workstation VDA を使用している場合、セキュリティ態勢チェックが断続的に動作を停止します。

ダブルホップシナリオでの **App Protection**

App Protection 機能は、ダブルホップシナリオではサポートされません。ダブルホップとは、Citrix Virtual Desktops セッション内で実行される Citrix Virtual Apps または Virtual Desktops セッションを意味します。ダブルホップシナリオでは、App Protection ポリシーが有効になっている仮想アプリとデスクトップを起動できましたが、App Protection 機能は適用されませんでした。

Windows 向け Citrix Workspace バージョン 2309 以降では、Windows グループポリシーが導入され、ダブルホップシナリオで App Protection ポリシーが有効になっている仮想アプリおよびデスクトップの起動をブロックできるようになりました。［ダブルホップ起動をブロックする］設定を有効にする方法について詳しくは、「ダブルホップ起動をブロックする設定を有効にする」を参照してください。

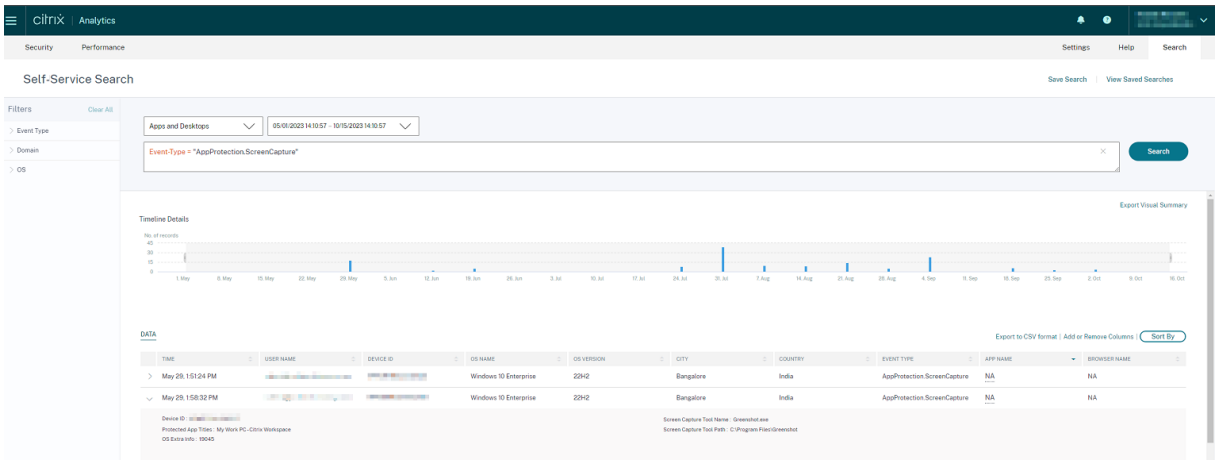
App Protection のための **Citrix Analytics** サービス

Citrix Virtual Apps and Desktops を使用すると、アクティビティやアクションに対応するユーザーイベントが生成されます。Citrix Analytics for Security には、これらのユーザーイベントを記録し、それらに関する詳細情報を提供するセルフサービス検索という機能があります。セルフサービス検索を使用すると、これらのユーザーイベントを検索し、フィルタリングし、調査できるため、どのようなユーザーイベントが実行されたかを理解し、イベントの重大度に応じてアクションを実行できます。セルフサービス検索について詳しくは、「セルフサービス検索」を参照してください。

アプリとデスクトップのセルフサービス検索には、`AppProtection.ScreenCapture`というイベントの種類があり、これを使用して、App Protection ポリシーが有効になっている仮想アプリまたはデスクトップのスクリーンショットを取ろうとしたかどうかを判断できます。ユーザー イベントを検索する方法について詳しくは、「イベントをフィルタリングするための検索クエリを指定する」を参照してください。

このサービスは次の情報を提供します:

- デバイス ID
- 保護されたアプリのタイトル
- OS の追加情報
- 画面キャプチャのツール名
- 画面キャプチャのツールパス



スクリーンショットの許可リスト

Citrix Workspace アプリ、仮想アプリとデスクトップ、または SaaS アプリで、App Protection のスクリーンキャプチャ対策ポリシーが有効になっている場合は、スクリーンショットツールを使用して画面をキャプチャすることはできません。

ただし、Windows 向け Citrix Workspace アプリ 2402 リリース以降では、スクリーンショットの許可リスト機能を使用して、アプリをスクリーンショットの許可リストに追加できるようになりました。この機能を使用すると、許可リストに登録されたアプリを使用して、App Protection のスクリーンキャプチャ対策ポリシーが有効になってい

るリソースの画面をキャプチャできます。アプリをスクリーンショット許可リストに追加するには、「スクリーンショット許可リストの構成」を参照してください。

> 重要:
>
> セキュリティ態勢が低下するため、許可リストに登録されたアプリをデバイス上で長期間実行することはお勧めしません。許可リストに登録されたアプリをトラブルシューティングなどのシナリオで使用して、一時的に画面を共有できます。以下の条件に従うことをお勧めします:
>
> - App Protection の画面キャプチャ対策機能が有効になっているリソースとともに、許可リストに登録されているアプリを短時間実行します。
> - 必要なタスクが完了したら、許可リストに登録されたアプリを直ちに終了します。
> - セキュリティを強化するために、App Protection の画面キャプチャ対策機能が有効になっているリソースを使用して画面を共有するときに、ウォーターマークを追加します。

プロセスの除外リスト

デバイス上でプロセスまたはアプリケーションを起動すると、App Protection が有効になっている場合は、各プロセスに App Protection DLL が挿入されます。場合によっては、DLL との互換性の問題により、プロセスまたはアプリケーションが動作しなくなることがあります。

Windows 向け Citrix Workspace アプリ 2402 リリース以降では、プロセスの除外リストに任意のプロセスを追加して、特定のプロセスへの App Protection DLL の挿入を回避し、App Protection DLL の存在によって発生する互換性の問題から回復することができます。プロセス除外リストを構成するには、「プロセス除外リストの構成」を参照してください。

> 重要:
>
> セキュリティ態勢が低下するため、プロセスを除外することはお勧めしません。これは、アプリケーションの使用を一時的にブロック解除して、詳しく調査をするためにサポートチケットを発行する場合に使用できます。

USB フィルタードライバー除外リスト

場合によっては、Citrix Workspace アプリでゲーミングキーボードなどの特殊な外付けキーボードを使用すると、App Protection USB フィルタードライバーによって互換性の問題が発生し、キーボードの使用がブロックされることがあります。

Windows 向け Citrix Workspace アプリ 2402 リリース以降では、USB フィルタードライバーの除外リスト機能により、デバイスのベンダー ID と製品 ID を使用して、Citrix Workspace アプリとの互換性の問題がある USB デバイスを除外できます。USB フィルタードライバー除外リストにデバイスを追加するには、「USB フィルタードライバー除外リストの構成」を参照してください。

> 注:
>
> デバイスを永続的に除外することはお勧めしません。この機能は、ユーザーによるデバイスの使用を一時的にブロック解除し、サポート チケットを発行して互換性の問題をさらに調査するために使用します。

App Protection の構成

April 10, 2024

App Protection は、Citrix Workspace アプリの使用時のセキュリティを強化します。この機能は、クライアントがキーロガーや画面キャプチャマルウェアによって侵害される可能性を軽減します。App Protection では、画面に表示されるユーザーの資格情報や個人情報などの機密情報の流出を防ぎます。この機能を使うと、ユーザーおよび攻撃者がスクリーンショットを撮る、またはキーロガーを使用することにより機密情報を収集、悪用することを防ぐことができます。

この記事では、さまざまなプラットフォームの Citrix Workspace アプリで App Protection を構成する方法について説明します。

App Protection は、次のプラットフォームの Citrix Workspace アプリで利用できます:

- Windows 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ

> 免責事項
>
> App Protection ポリシーはオペレーティングシステムの必要な機能へのアクセスをフィルタリングします。画面のキャプチャまたはキーボードの操作には、特定の API 呼び出しが必要です。App Protection ポリシーは、カスタムの目的別に構築されたハッカーツールに対しても保護を提供します。ただし、オペレーティングシステムの進化によって、画面のキャプチャやキーのログ記録には新しい方法が出てくる場合があります。引き続きこうした方法に対応していきますが、特定の構成や展開では完全な保護を保証することはできません。

Windows 向け Citrix Workspace アプリ

前提条件

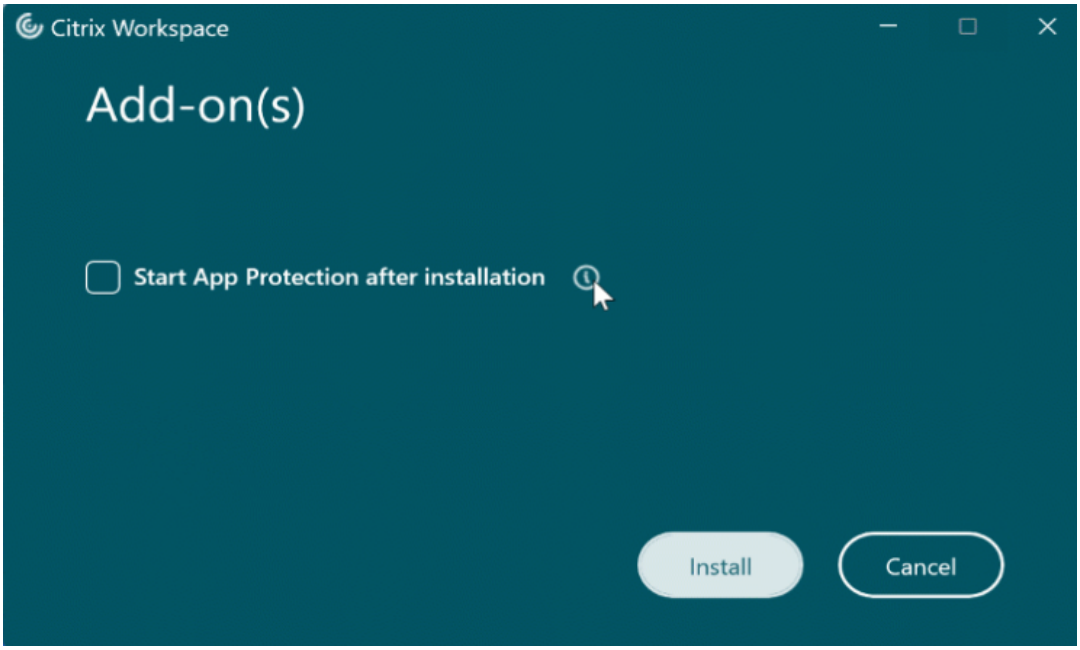
- Citrix Virtual Apps and Desktops バージョン 1912 LTSR 以降。
- StoreFront バージョン 1912 LTSR または Workspace。
- Citrix Workspace アプリバージョン 2203.1 LTSR 以降。
- 有効な App Protection ライセンス

- Citrix Workspace アプリバージョン 2212 以降、Citrix Workspace アプリのインストール中に、App Protection コンポーネントがデフォルトでインストールされます。

  インストール中に表示される ［**App Protection** を有効にする］チェックボックスは、インストール後に、［**App Protection** を開始する］チェックボックスに置き換えられます。

  – 2311 より前のバージョンの Citrix Workspace アプリの場合：

  – Citrix Workspace アプリのバージョン 2311 以降：



このチェックボックスをオンにすると、インストール直後に App Protection が開始されます。

> 注:
>
> このチェックボックスをオンにしない場合、App Protection は、App Protection の権限を持っている顧客の保護されたリソースまたはコンポーネントが最初に起動したときに自動的に開始されます。

構成

Windows 向け Citrix Workspace アプリの次の App Protection 機能を構成します:

- キーロガー対策および画面キャプチャ対策:
  - Virtual Apps and Desktops の場合、「Virtual Apps and Desktops のキーロガー対策および画面キャプチャ対策の構成」を参照してください。
  - Web アプリまたは SaaS アプリの場合、「Web アプリまたは SaaS アプリのキーロガー対策と画面キャプチャ対策の構成」を参照してください。
  - 認証および Self-service Plug-in の場合:
    - Global App Configuration Service の UI を使用する場合は、「Global App Configuration Service の UI を使用した認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策の構成」を参照してください
    - グループポリシーオブジェクトを使用する場合は、「グループポリシーオブジェクトを使用した認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策の構成」を参照してください
    - API を使用する場合は、「GACS API を使用した認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策の構成」を参照してください

- DLL インジェクション対策機能を構成するには、「DLL インジェクション対策機能の構成」を参照してください。
- App Protection のポリシー改ざんの構成を行うには、「App Protection のポリシー改ざんの構成」を参照してください。
- App Protection のセキュリティ態勢チェックを構成するには、「App Protection のセキュリティ態勢チェックの構成」を参照してください。
- ダブルホップ起動をブロックする設定を有効にするには、「ダブルホップ起動のブロック」を参照してください。

制限事項

- この機能は、Windows 11、Windows 10 などのデスクトップオペレーティングシステムでのみサポートされます。
- バージョン 2006.1 以降、Citrix Workspace アプリは Windows 7 ではサポートされていません。そのため、App Protection は Windows 7 では機能しません。詳しくは、「廃止」を参照してください。
- この機能は、リモートデスクトッププロトコル（RDP）ではサポートされません。

コマンドラインインターフェイス

コマンドラインパラメーターの`/startappprotection`を使用して App Protection コンポーネントを開始することができます。ただし、以前の`/includeappprotection`スイッチは廃止されました。

次の表に、展開に応じて保護される画面に関する情報を示します：

App Protection の展開	保護される画面	保護されない画面
Citrix Workspace アプリに含まれる	Self-service Plug-in と Authentication Manager/［ユーザー資格情報］ダイアログボックス	コネクションセンター、デバイス、Citrix Workspace アプリのエラーメッセージ、クライアントの自動再接続、アカウントの追加
Controller で構成	ICA セッション画面（アプリとデスクトップの両方）	コネクションセンター、デバイス、Citrix Workspace アプリのエラーメッセージ、クライアントの自動再接続、アカウントの追加

スクリーンショットを撮っているときは、保護されたウィンドウだけが黒く表示されます。保護されたウィンドウの外側の領域のスクリーンショットは撮ることができます。ただし、**PrtScr** キーを使用して Windows 10 デバイスでスクリーンショットをキャプチャする場合は、保護されたウィンドウを最小化する必要があります。

以前は、Citrix 認証画面と Citrix Workspace アプリ画面では、画面キャプチャ防止機能とキーロギング防止機能がデフォルトで適用されていました。しかし、2212 以降、これらの機能はデフォルトで無効となり、現在はグループポリシーオブジェクトを使用して構成する必要があります。

> 注:
>
> この GPO ポリシーは、ICA および SaaS セッションには適用されません。ICA および SaaS セッションは、引き続き Delivery Controller および Citrix Secure Private Access を使用して制御されます。

App Protection の機能強化:

Windows 向け Citrix Workspace アプリ 2305 以降では、次の基準のいずれかが満たされる場合、認証画面と Self-service Plug-in 画面でキーロガー対策が有効になります:

- 次のいずれかを使用して App Protection を有効にしました:
  - インストール中に ［**App Protection** を開始する］チェックボックスをオンにする。
  - コマンドラインパラメーターの**/startappprotection** を使用して App Protection コンポーネントを開始する。
- インストール中に ［**App Protection** を開始する］チェックボックスをオンにしていない場合、または**/startappprotection** コマンドラインパラメーターを使用していない場合は、最初の保護されたリソースを起動した後にキーロガー対策保護が有効になります。

> 注:
>
> Global App Configuration Service とグループポリシーオブジェクトの設定は、直前の動作を上書きします。たとえば、これらの画面に対して GACS または GPO ポリシーを無効にしている場合、認証画面と SSP 画面ではキーロガー対策が有効になりません。

Linux 向け **Citrix Workspace** アプリ

バージョン 2108 以降、App Protection 機能の全機能が使用可能になりました。この機能は Virtual Apps and Desktops をサポートし、デフォルトで有効になっています。ただし、`AuthManConfig.xml`ファイルで App Protection 機能を構成して、Authentication Manager と Self-service Plug-in インターフェイスで有効にする必要があります。

前提条件

App Protection は、Gnome Display Manager と併せて、次のオペレーティングシステムで最適に機能します:

- 64 ビット Ubuntu 22.04、Ubuntu 20.04、および Ubuntu 18.04
- 64 ビット Debian 10 および Debian 9
- 64 ビット CentOS 7

- 64 ビット RHEL 7
- ARMHF 32 ビット Raspberry Pi OS（Debian 10（buster）ベース）
- ARM64 Raspberry Pi OS（Debian 11（bullseye）ベース）

> 注:
>
> バージョン 2204 より前の Citrix Workspace アプリを使用している場合、App Protection 機能は`glibc` 2.34 以降を使用するオペレーティングシステムをサポートしません。
>
> `glibc` 2.34 以降を使用する OS に App Protection 機能を有効にした Citrix Workspace アプリをインストールした場合、システムの再起動時に OS の起動に失敗することがあります。OS の起動エラーから回復するには、次のいずれかを実行します:
>
> - OS を再インストールします。
> - OS のリカバリモードに移動し、ターミナルを使用して Citrix Workspace アプリをアンインストールします。
> - ライブ OS から起動し、既存の OS から`rm -rf /etc/ld.so.preload`ファイルを削除します。

App Protection コンポーネントのアンインストール

1. tarball パッケージを使用して Citrix Workspace アプリをインストールすると、次のメッセージが表示されます: **App Protection** コンポーネントをインストールしますか**?** 警告: この機能を無効にすることはできません。無効にするには、**Citrix Workspace** アプリをアンインストールする必要があります。詳しくは、システム管理者に問い合わせてください。**[**デフォルトは **$INSTALLER_N]:**
2. **Y** を入力して、App Protection コンポーネントをインストールします。App Protection はデフォルトではインストールされません。
3. 変更を反映するためにマシンを再起動します。App Protection は、マシンを再起動した後にのみ正常に機能します。

RPM パッケージへの **App Protection** コンポーネントのインストール　バージョン 2104 以降、Citrix Workspace アプリの RPM バージョンで App Protection がサポートされています。

App Protection をインストールするには、次の手順を実行します:

1. Citrix Workspace アプリをインストールします。
2. Citrix Workspace アプリインストーラーから App Protection`ctxappprotection<version>.rpm`パッケージをインストールします。
3. 変更を反映するにはシステムを再起動します。

Debian パッケージへの **App Protection** コンポーネントのインストール　バージョン 2101 以降、Citrix Workspace アプリの Debian バージョンで App Protection がサポートされています。

App Protection コンポーネントをインストールするには、Citrix Workspace アプリをインストールする前に、ターミナルから次のコマンドを実行します:

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
    install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

Citrix Workspace アプリではバージョン 2106 以降、Authentication Manager インターフェイスと Self-service Plug-in インターフェイスの両方で、キーロガー対策および画面キャプチャ対策機能を個別に構成できるオプションが導入されます。

構成

Linux 向け Citrix Workspace アプリの次の App Protection 機能を構成します:

- 認証画面のキーロガー対策と画面キャプチャ対策を構成するには、「Authentication Manager での AuthManConfig.xml を使用した構成」を参照してください。
- Self-service Plug-in 画面のキーロガー対策と画面キャプチャ対策を構成するには、「Self-Service Plug-in インターフェイスでの AuthManConfig.xml を使用した構成」を参照してください。
- Virtual Apps and Desktops のキーロガー対策と画面キャプチャ対策を構成するには、「Virtual Apps and Desktops のキーロガー対策および画面キャプチャ対策の構成」を参照してください。
- App Protection のポリシー改ざんの構成を行うには、「App Protection のポリシー改ざんの構成」を参照してください。
- App Protection のセキュリティ態勢チェックを構成するには、「App Protection のセキュリティ態勢チェックの構成」を参照してください。

Mac 向け Citrix Workspace アプリ

Mac 向け Citrix Workspace アプリの次の App Protection 機能を構成します:

- Global App Configuration Service の UI を使用した認証と Self-service Plug-in のキーロガー対策と画面キャプチャ対策の構成については、「Global App Configuration Service の UI を使用した認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策の構成」を参照してください。
- API を使用した認証と Self-service Plug-in のキーロガー対策と画面キャプチャ対策の構成については、「GACS API を使用した認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策の構成」を参照してください。

- Virtual Apps and Desktops のキーロガー対策と画面キャプチャ対策を構成するには、「Virtual Apps and Desktops のキーロガー対策および画面キャプチャ対策の構成」を参照してください。
- Web アプリと SaaS アプリのキーロガー対策と画面キャプチャ対策を構成するには、「Web アプリと SaaS アプリのキーロガー対策および画面キャプチャ対策の構成」を参照してください。
- App Protection のポリシー改ざんの構成を行うには、「App Protection のポリシー改ざんの構成」を参照してください。
- App Protection のセキュリティ態勢チェックを構成するには、「App Protection のセキュリティ態勢チェックの構成」を参照してください。

推奨

App Protection ポリシーは、主にエンドポイントのセキュリティと保護を強化することに重点を置いています。環境に関するその他のセキュリティ推奨事項とポリシーをすべて確認します。セキュリティと制御のポリシーテンプレートは、許容率が低い環境での推奨構成に使用できます。詳しくは、「ポリシーテンプレート」を参照してください。

キーロガー対策および画面キャプチャ対策の構成

April 10, 2024

以下に関して、キーロガー対策および画面キャプチャ対策を構成できます:

- 認証および Self-service Plug-in
- Virtual Apps and Desktops
- Web および SaaS アプリ

認証および **Self-service Plug-in** のキーロガー対策および画面キャプチャ対策の構成

以下の方法で、認証および Self-service Plug-in のキーロガー対策および画面キャプチャ対策を構成できます:

構成方法	Linux 向け Citrix Workspace アプリ	Mac 向け Citrix Workspace アプリ	Windows 向け Citrix Workspace アプリ
グループポリシーオブジェクトの使用	いいえ	いいえ	はい
Global App Configuration Service の使用	いいえ	はい	はい
AuthManConfig.xml の使用	はい	いいえ	いいえ

グループポリシーオブジェクトの使用

1. `gpedit.msc`を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［**Citrix** コンポーネント］> ［**Citrix Workspace**］の順に移動します。
3. App Protection を Authentication Manager 用に構成しているか、Self-service Plug-in 用に構成しているかに応じて、次のいずれかの手順を使用します：
   - **Authentication Manager**
     Authentication Manager のキーロガー対策と画面キャプチャ対策を構成するには、［ユーザー認証］> ［**App Protection** の管理］ポリシーを選択します。
   - **Self-service Plug-in** インターフェイス
     Self-service Plug-in インターフェイスのキーロガー対策および画面キャプチャ対策を構成するには、［**Self Service**］> ［**App Protection** の管理］ポリシーを選択します。
4. 次のオプションのいずれか 1 つまたは両方を選択します：
   - キーロガー対策：キーロガーがキーストロークをキャプチャするのを防ぎます。
   - 画面キャプチャ対策：ユーザーがスクリーンショットを撮ったり、画面を共有したりできないようにします。
5. ［適用］、［**OK**］の順にクリックします。

想定される動作：

想定される動作は、保護されたリソースが含まれる StoreFront ストアにアクセスする方法によって異なります。

Global App Configuration Service の **UI** の使用

Windows 向け Citrix Workspace アプリ 2302 または Windows 向け Citrix Workspace 2301 バージョン以降、Citrix Workspace アプリで、Global App Configuration Service（GACS）を使用して認証画面および Self-service Plug-in の App Protection を構成できます。

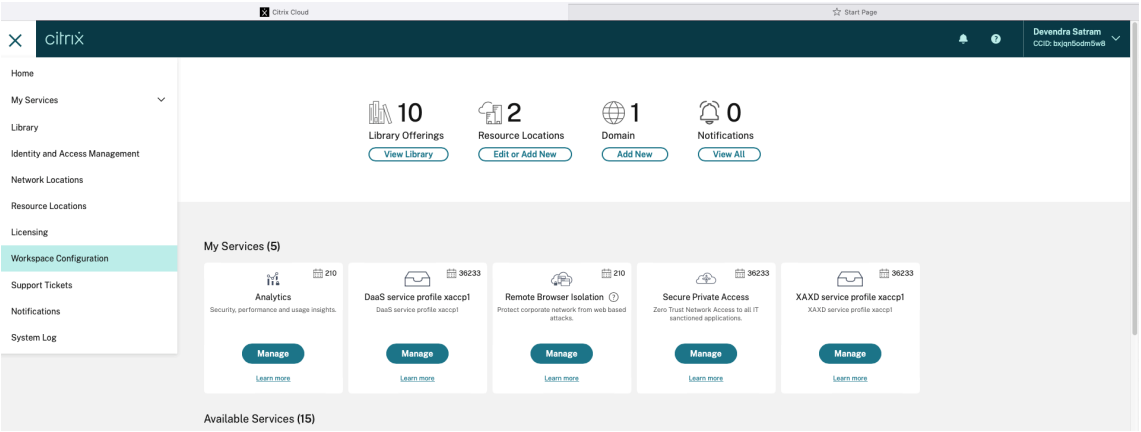
GACS を使用してキーロガー対策および画面キャプチャ対策を有効にすると、それらの機能を認証と Self-service Plug-in の両方に適用できます。

> 注：
>
> - GACS を使用して認証と Self-service Plug-in のキーロガー対策および画面キャプチャ対策を構成すると、Windows 向け Citrix Workspace アプリと Mac 向け Citrix Workspace アプリに適用できます。Linux 向け Citrix Workspace アプリには適用できません。
> - GACS の構成は、仮想アプリおよびデスクトップ、Web アプリ、および SaaS アプリには適用されません。これらのリソースは、引き続き Delivery Controller および Citrix Secure Private Access を使用

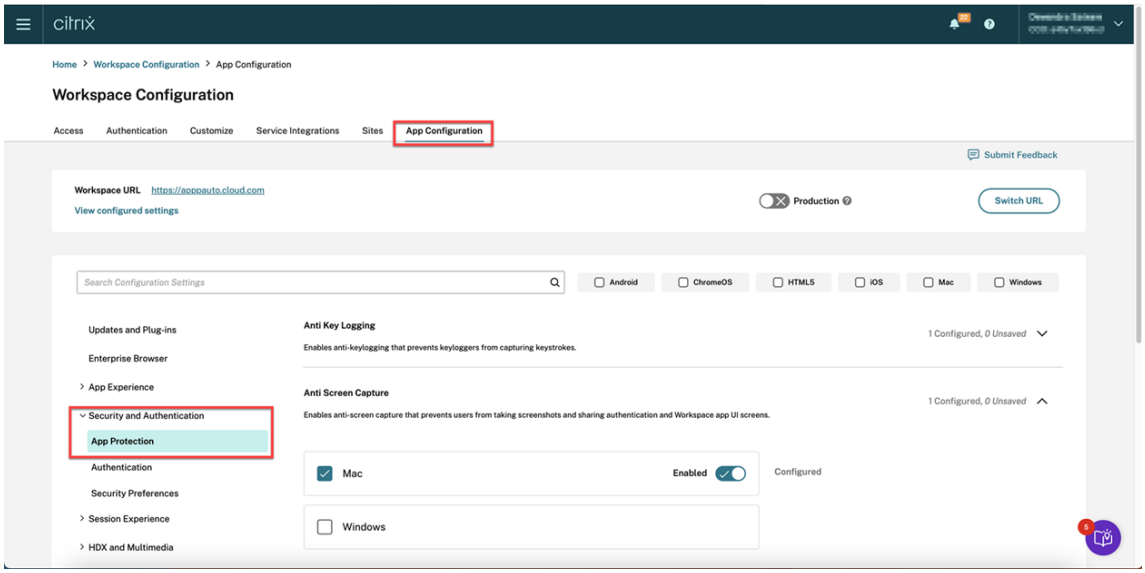
> して制御されます。
>
> - Mac 向け Citrix Workspace アプリ 2311 バージョン以降、クラウドストアとオンプレミスの両方で、Global App Configuration サービス UI を使用して認証および Self-service Plug-in の App Protection を構成できるようになりました。ただし、2311 バージョンより前の Mac 向け Citrix Workspace アプリを使用している場合は、クラウドストアに対してのみ構成できます。

管理者は、ワークスペース構成 UI を使用して App Protection を構成できます:

1. Citrix Cloud アカウントにサインインし、［ワークスペースの構成］を選択します。

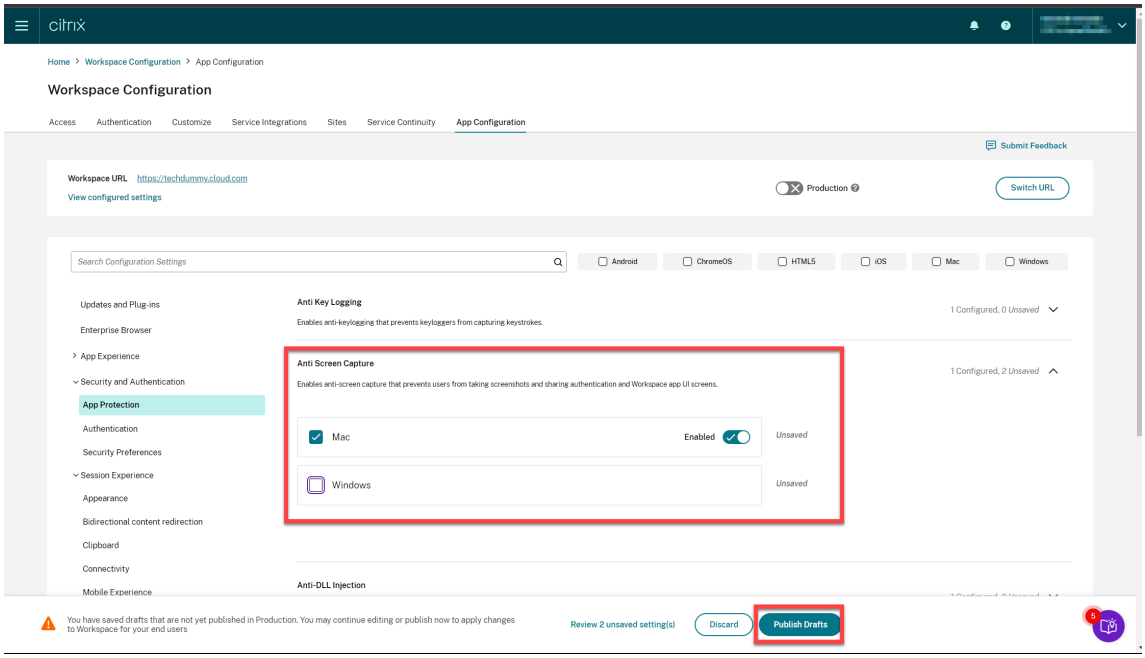


2. ［アプリ構成］ > ［セキュリティと認証］ > ［**App Protection**］を選択します。



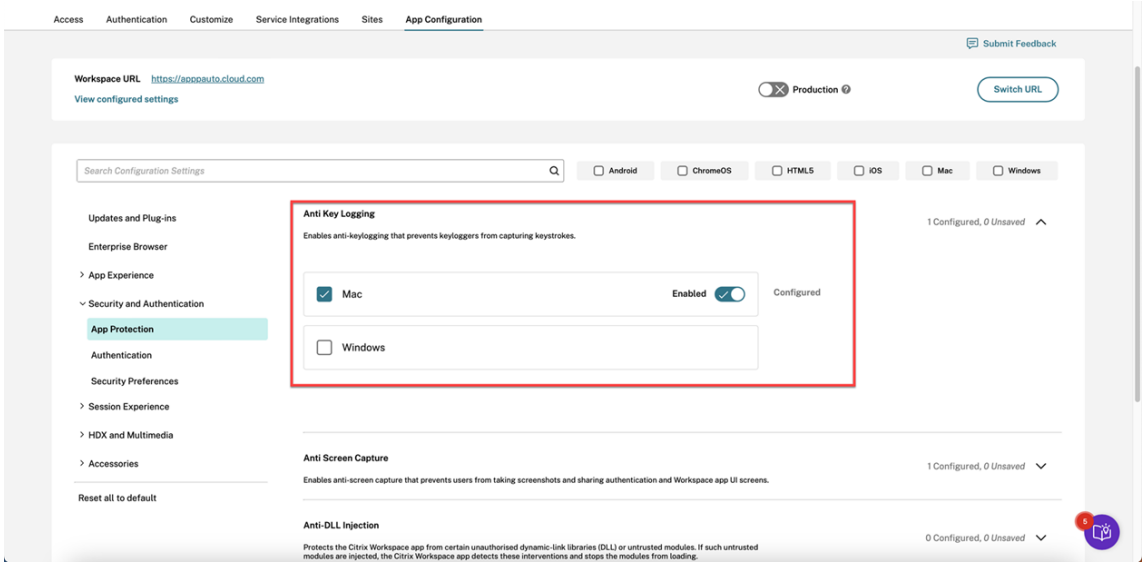
3. ［画面キャプチャ対策］をクリックし、関連するオペレーティングシステム（Windows または Mac）を選択します。

4. ［有効］トグルボタンをクリックし、［下書きの公開］をクリックします。

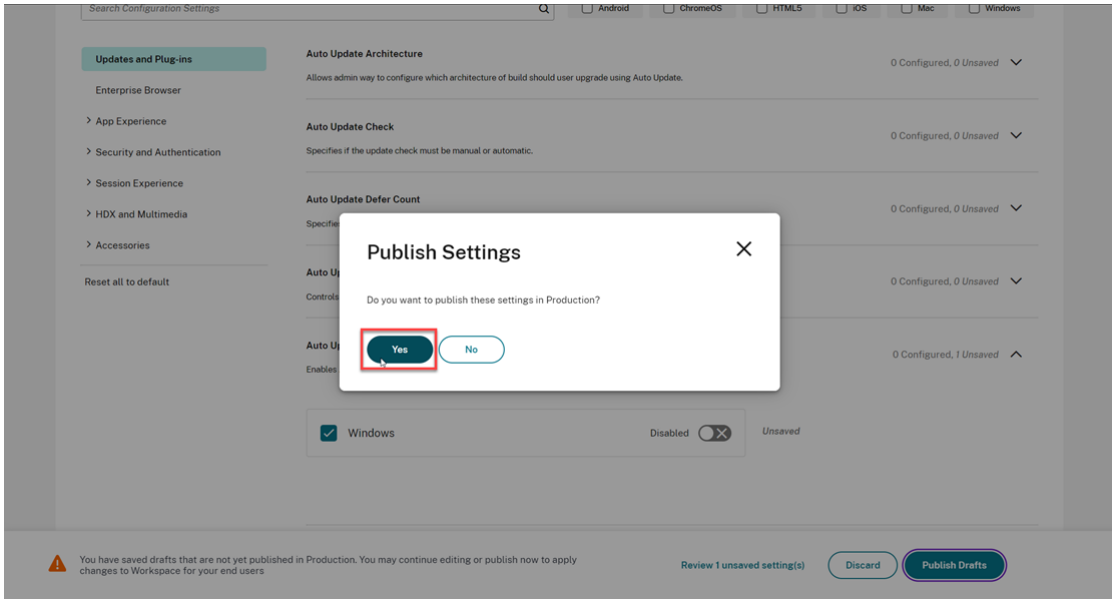


5. ［キーロガー対策］をクリックし、関連するオペレーティングシステム（Windows または Mac）を選択します。

6. ［有効］トグルボタンをクリックし、［下書きの公開］をクリックします。



7. ［設定の公開］ダイアログボックスで、［はい］をクリックします。



Global App Configuration Service API の使用

管理者は、API を使用して、これらの App Protection 機能を構成できます。設定項目は次のとおりです:

- 画面キャプチャ対策機能を有効または無効にする設定:

  “name”:” enable anti screen capture for auth and ssp”
  “value” : “true” または “false”

- キーロガー対策機能を有効または無効にする設定:

  “name”: “enable anti key-logging for auth and ssp”
  “value” : “true” または “false”

例: GACS で Citrix Workspace アプリの画面キャプチャ防止機能とキーロガー対策機能を有効にするための JSON ファイルの例を次に示します:

```
{


        "category": "App Protection",

        "userOverride": true,

        "assignedTo": [

          "AllUsersNoAuthentication"

        ],

        "settings": [
```



```
15
16              {
17
18
19                "name": "enable anti screen capture for auth and ssp",
20
21                "value": true
22
23               }
24  ,
25
26              {
27
28
29                "name": "enable anti key-logging for auth and ssp",
30
31                "value": true
32
33               }
34
35
36            ] }
```

Authentication Manager での **AuthManConfig.xml** の使用

`$ICAROOT/config/AuthManConfig.xml`に移動し、次のようにファイルを編集します:

```
1  /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
      authmananti -A 1
2      <key>AuthManAntiScreenCaptureEnabled</key>
3      <value>true</value>
4      <key>AuthManAntiKeyLoggingEnabled</key>
5      <value>true </value>
6
7  <!--NeedCopy-->
```

Self-service Plug-in インターフェイスでの **AuthManConfig.xml** の使用

`$ICAROOT/config/AuthManConfig.xml`に移動し、次のようにファイルを編集します:

```
1  /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
      protection -A 4
2  <!-- Selfservice App Protection configuration -->
3      <Selfservice>
4        <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5        <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6      </Selfservice>
7
8  <!--NeedCopy-->
```


Virtual Apps and Desktops のキーロガー対策と画面キャプチャ対策の構成

2 つのポリシーがセッションでのキーロガー対策および画面キャプチャ対策機能を提供します。Virtual Apps and Desktops のキーロガー対策と画面キャプチャ対策を、次のように構成できます:

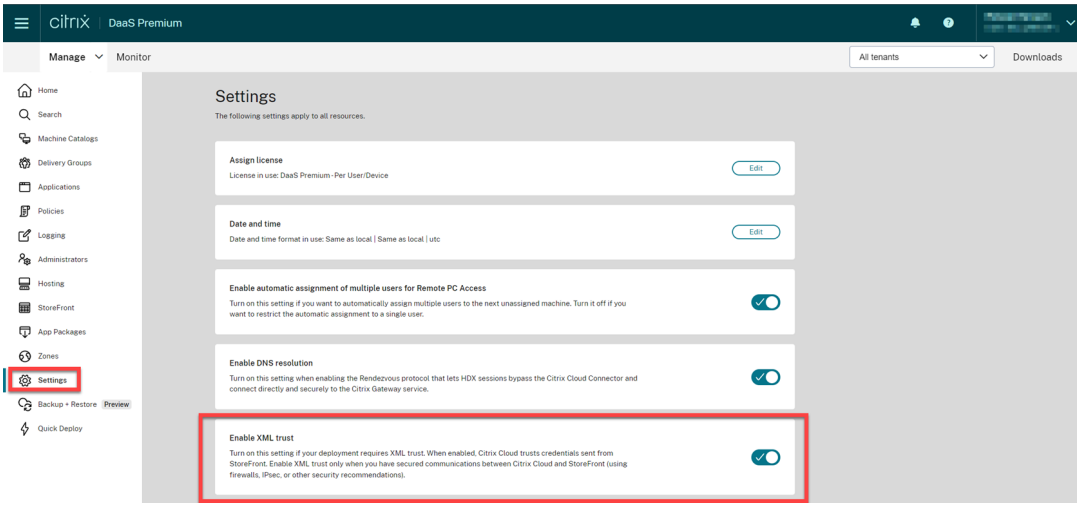
> 注:
>
> バージョン 2103 以降、Citrix DaaS は StoreFront および Workspace で App Protection をサポートします。

Web Studio の使用

Web Studio を使用して Citrix Virtual Apps または Desktops のキーロガー対策と画面キャプチャ対策を構成するには、次の手順を実行します:

1. App Protection には XML 信頼が必要です。XML 信頼を有効にするには、次の手順を実行します:

   a) Citrix DaaS アカウントにサインインし、［管理］ > ［設定］ > ［**XML** 信頼を有効にする］に移動します。

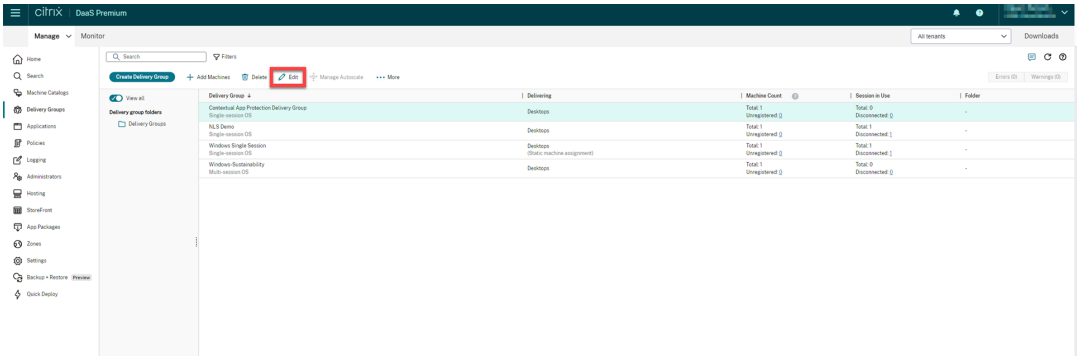


   b) ［**XML** 信頼を有効にする］トグルをオンにします。

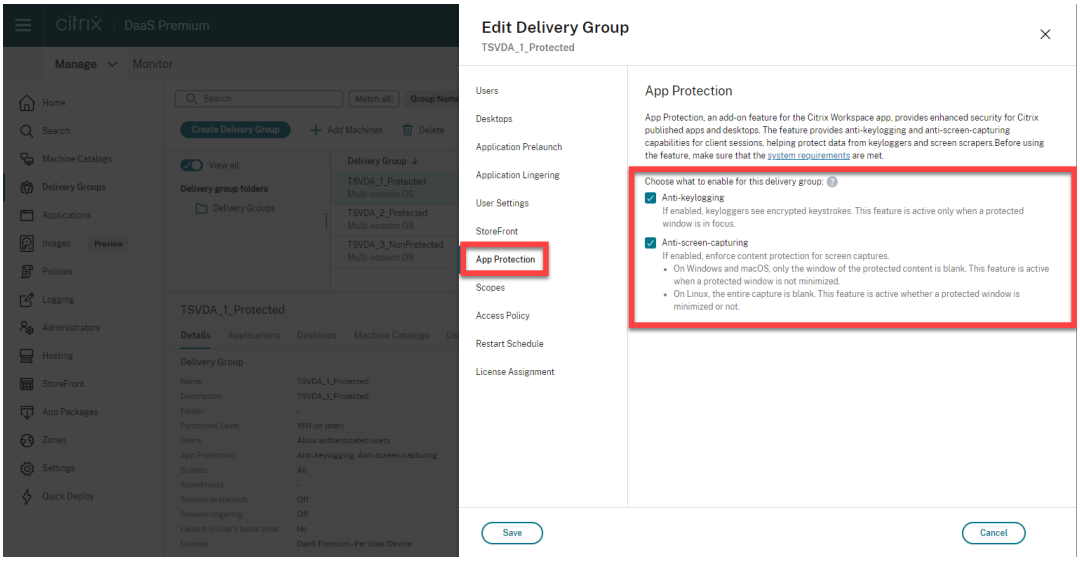
2. デリバリーグループの App Protection 方法を選択するには、次の手順を実行します:

   a) Citrix DaaS で、［管理］ > ［デリバリーグループ］に移動します。

   b) デリバリーグループを選択して、操作バーの ［編集］をクリックします。



c) ［**App Protection**］をクリックしてから、［キーロガー対策］および ［画面キャプチャ対策］チェックボックスを選択します。



d) ［保存］をクリックします。

PowerShell の使用

> 注:
>
> Citrix DaaS 環境では、任意のマシン（Citrix Cloud Connector マシンを除く）のCitrix Virtual Apps and Desktops Remote PowerShell SDKにあるコマンドレットを使用して、このセクションのコマンドを発行します。

インストール済みの任意の Delivery Controller マシンで、または FMA PowerShell スナップインとともにスタンドアロンの Studio がインストールされたマシンで、Citrix Virtual Apps and Desktops SDKを使用して、App Protection デリバリーグループの次のプロパティを有効にします。

- `AppProtectionKeyLoggingRequired`: `True`
- `AppProtectionScreenCaptureRequired`: `True`

いずれかのポリシーを各デリバリーグループで個別に有効にできます。たとえば、DG1 でのみキーロガーからの保護を構成でき、DG2 でのみ画面キャプチャからの保護を構成できます。DG3 で両方のポリシーを有効にできます。

例:

DG3 という名前のデリバリーグループで両方のポリシーを有効にするには、サイトの Delivery Controller で次のコマンドを実行します:

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

この設定を検証するには、次のコマンドレットを実行します:

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

また、XML 信頼を有効にします:

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

StoreFront とブローカーの間のネットワークを確実に保護してください。詳しくは、Knowledge Center のCTX236929および「XenApp および XenDesktop XML Service の保護」を参照してください。

Web アプリまたは **SaaS** アプリのキーロガー対策と画面キャプチャ対策の構成

Windows 向け Citrix Workspace アプリおよび Mac 向け Citrix Workspace アプリの Citrix Enterprise Browser で、Web アプリと SaaS アプリを開きます。Citrix Secure Private Access によりアプリに App Protection ポリシーが構成されている場合、App Protection はタブごとに適用されます。

以下の方法で、Web アプリと SaaS アプリの App Protection を構成します:

- Workspace の Web アプリおよび SaaS アプリの App Protection を構成するには、「Citrix Workspace の Citrix Secure Private Access」を参照してください。
- StoreFront の Web アプリおよび SaaS アプリの App Protection を構成するには、「StoreFront の Citrix Secure Private Access のサポート」を参照してください。

DLL インジェクション対策の構成

March 10, 2024

デフォルトでは、DLL インジェクション対策機能は無効になっています。この機能を有効にするには、以下を使用します:

- グループポリシーオブジェクト（GPO）
- Global Admin Configuration Service（GACS）

グループポリシーオブジェクトを使用した構成

DLL インジェクション対策機能を構成するために、次のポリシーが追加されました:

- DLL インジェクション対策
- DLL インジェクション対策のモジュール許可リスト

DLL インジェクション対策ポリシーの使用

このポリシーを使用して、DLL インジェクション対策機能を有効または無効にします。このポリシーが構成されていない場合、DLL インジェクション対策機能は無効になります。使用できる値は以下のとおりです:

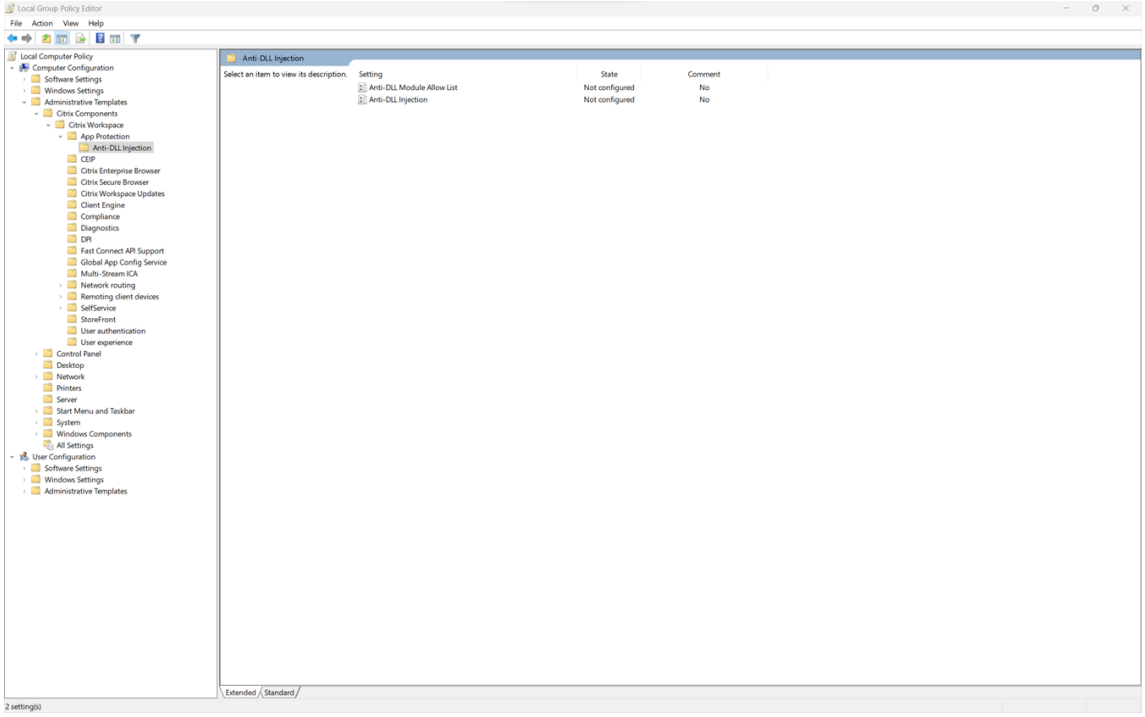
- 有効 - Citrix Authentication Manager、Citrix Workspace アプリの UI、および Citrix Virtual Apps and Desktops で DLL インジェクション対策機能が有効になっています。管理者は、DLL インジェクション対策機能を有効にするために必要なコンポーネントを選択できます。
- 無効 - Citrix Authentication Manager、Citrix Workspace アプリの UI、および Citrix Virtual Apps and Desktops で DLL インジェクション対策機能が無効になっています。

DLL インジェクション対策ポリシーを有効にするには、次の手順を実行します:

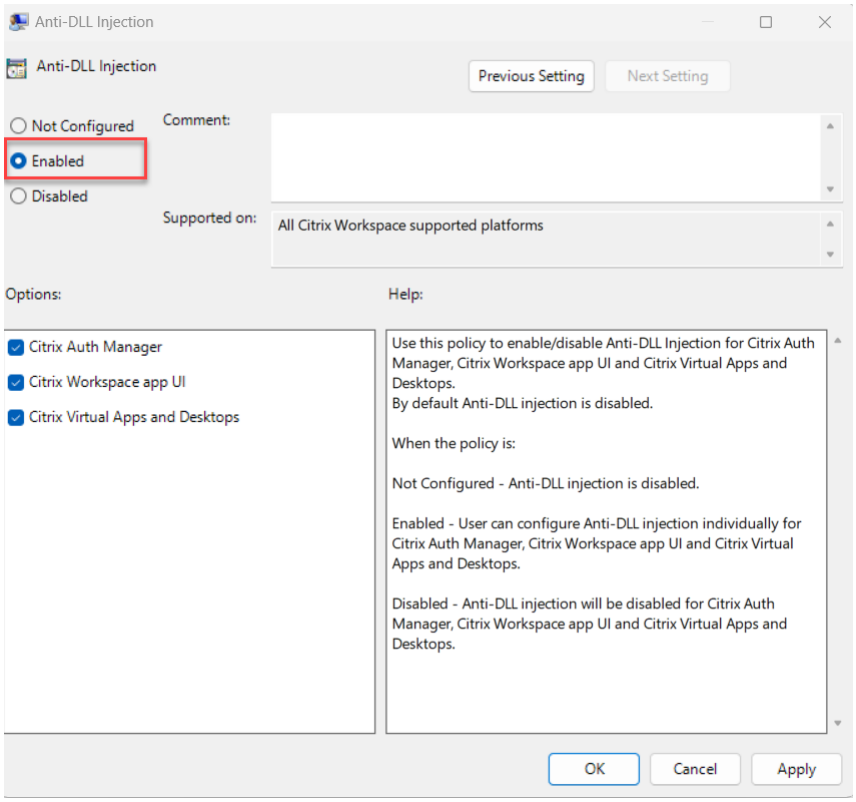
1. 次のコマンドを実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます:

   ```
   gpedit.msc
   ```

2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** のコンポーネント] > [**Citrix Workspace**] > [**App Protection**] > [**DLL** インジェクション対策] に移動します。



3. ［**DLL** インジェクション対策］ポリシーをクリックし、［有効］を選択します。すべてのコンポーネントが選択されます。ただし、［オプション］セクションからコンポーネントの選択を変更できます。



4. ［**OK**］をクリックします。

DLL インジェクション対策のモジュール許可リストポリシーの使用

管理者は、このポリシーを使用して、DLL インジェクション対策機能から DLL を除外できます。このポリシーは、例外的なシナリオを処理する場合にのみ使用することをお勧めします。このポリシーが構成されていない場合、DLL は許可リストに含まれません。すべての DLL は、DLL インジェクション対策に含まれます。使用できる値は以下のとおりです:

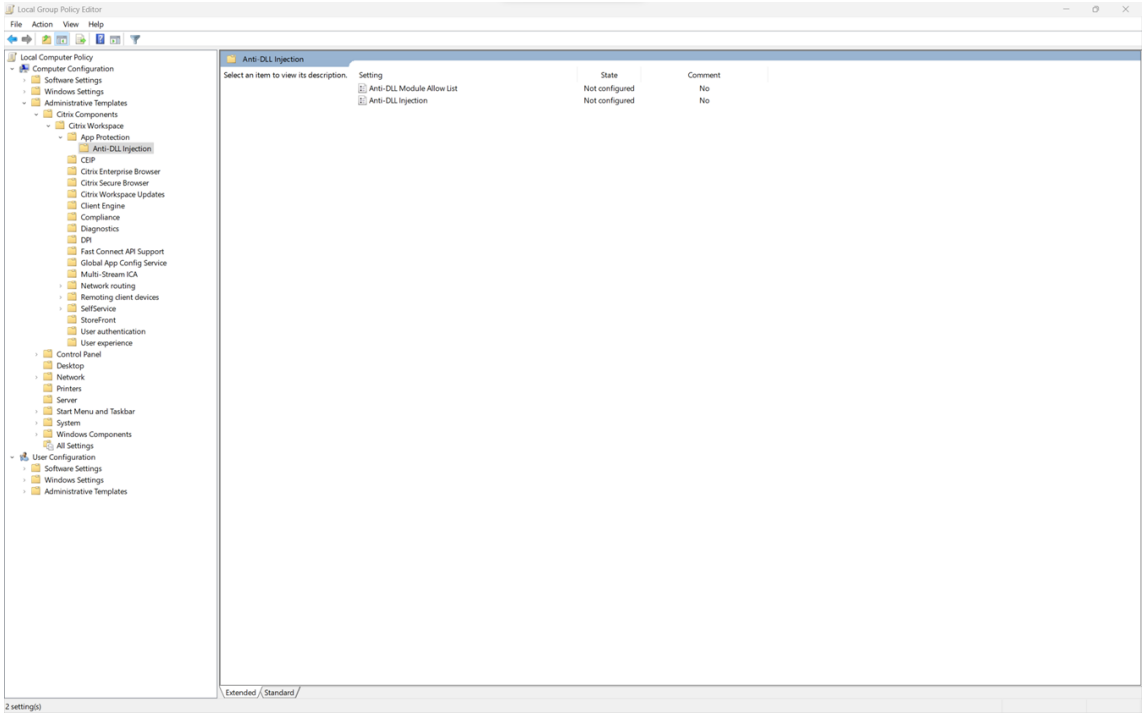
- 有効 - 許可リストに追加された DLL を DLL インジェクション対策から除外します。
- 無効 - 許可リストに追加された DLL の一覧をクリアします。

DLL インジェクション対策のモジュール許可リストポリシーを有効にするには、次の手順を実行します:

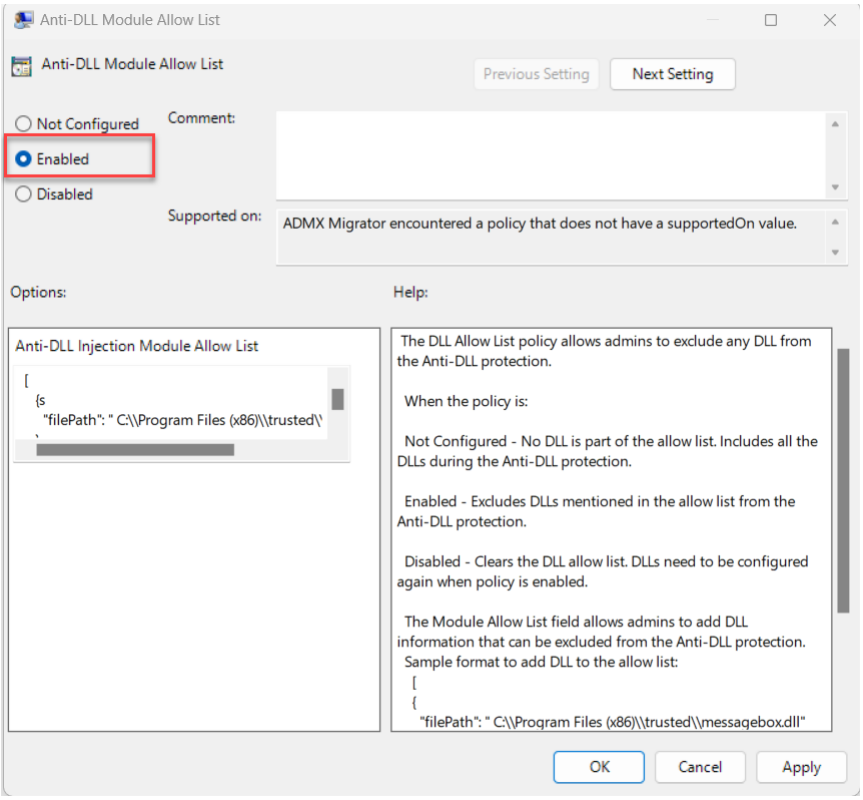
1. 次のコマンドを実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます:

   ```
   gpedit.msc
   ```

2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** のコンポーネント] > [**Citrix Workspace**] > [**App Protection**] > [**DLL** インジェクション対策のモジュール許可リスト] に移動します。



3. [**DLL** インジェクション対策のモジュール許可リスト] ポリシーをクリックし、[有効] を選択します。



4. ［**DLL** インジェクション対策のモジュール許可リスト］フィールドに、DLL インジェクション対策から除外するモジュールの一覧を追加します。
   許可リストに DLL を追加する形式の例:

```
[
    {

        "filePath":"C:\Program Files (x86)\trusted\messagebox.dll"
     }
 ,
    {

        "filePath":"%PROGRAMFILES%\trusted\logging.dll"
     }

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

5. ［**OK**］をクリックします。

Global App Configuration Service を使用した構成

管理者は、GACS を使用して DLL インジェクション対策機能を構成できます。設定項目は次のとおりです:

- anti dll injection –DLL インジェクション対策機能を有効にするために必要なモジュールを追加します

- anti dll module allow list –DLL インジェクション対策から除外する必要な DLL を追加します

詳しくは、「Global App Configuration Service」を参照してください。

GACS で Windows 向け Citrix Workspace アプリの **anti dll injection** と **anti dll module allow list** のモジュール許可リストを有効にするための JSON ファイルの例を次に示します:

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "assignmentPriority": 0,
          "settings": [
            {

              "name": "anti dll injection",
              "value": [
                "Citrix Auth Manager",
                "Citrix Virtual Apps And Desktops",
                "Citrix Workspace app UI"
              ]
             }
 ,
            {

              "name": "anti dll module allow list",
              "value": [
                {

                  "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                     \wfica32.exe"
                 }
 ,
                {

                  "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                     \AuthManager\AuthManSvr.exe"
                 }
```



```

                ]
               }

            ]
           }

        ]
       }
  ,
     "name": "name",
     "description": "desc",
     "useForAppConfig": true
    }

  }

<!--NeedCopy-->
```

ポリシー改ざんの検出の構成

January 10, 2024

前提条件

ポリシー改ざん検出機能を構成するには、次のものがそろっていることを確認してください:

- クラウド展開の場合 - Cloud Desktop Delivery Controller のバージョン 115 以降
- オンプレミス展開の場合 - Citrix Virtual Apps and Desktops のバージョン 2308 以降
- Windows Virtual Delivery Agent インストーラーのバージョン 2308 以降
- Windows の場合 - Windows 向け Citrix Workspace アプリ 2309 以降
- Mac の場合 - Mac 向け Citrix Workspace アプリ 2308 以降
- Linux の場合 - Linux 向け Citrix Workspace アプリ 2308 以降

ポリシー改ざん検出を有効にするには、App Protection で構成された仮想アプリとデスクトップをホストしている TS/WS VDA で管理者が **Citrix AppProtection Service** を開始する必要があります。

ポリシー改ざん検出を有効にするには、次の手順のいずれかを実行します:

- コマンドプロンプトを使用する場合:

  1. タスクバーの左端にある ［検索］アイコンをクリックします。「**cmd**」と入力し、［管理者として実行］をクリックします。コマンドプロンプト画面が表示されます。
  2. 次のコマンドを実行します:


```
sc config ctxappprotectionsvc start=auto
sc start ctxappprotectionsvc

<!--NeedCopy-->
```

- ユーザーインターフェイスを使用する場合:

  1. タスクバーの左端にある ［検索］アイコンをクリックします。「**services.msc**」と入力し、**Enter** キーを押します。［サービス］画面が表示されます。
  2. ［**Citrix AppProtection Service**］を選択し、［開始］をクリックします。
  3. ［**Citrix AppProtection Service**］を右クリックし、［プロパティ］を選択します。
  4. ［一般］ > ［スタートアップの種類］ > ［自動］を選択し、［**OK**］をクリックして、システムの起動時にサービスが自動的に開始されるようにします。

ポリシー改ざん検出機能が正常に有効になりました。

ポリシー改ざん検出をサポートしていない以前のバージョンの Citrix Workspace アプリを検出してブロックするには、App Protection のセキュリティ態勢チェックを構成します。App Protection の状態チェックについて詳しくは、「App Protection のセキュリティ態勢チェック」を参照してください。

App Protection のセキュリティ態勢チェックを構成する

March 10, 2024

App Protection のセキュリティ態勢チェックを有効にするには、この機能に関連する新しい VDA Citrix ポリシーを構成します。

前提条件

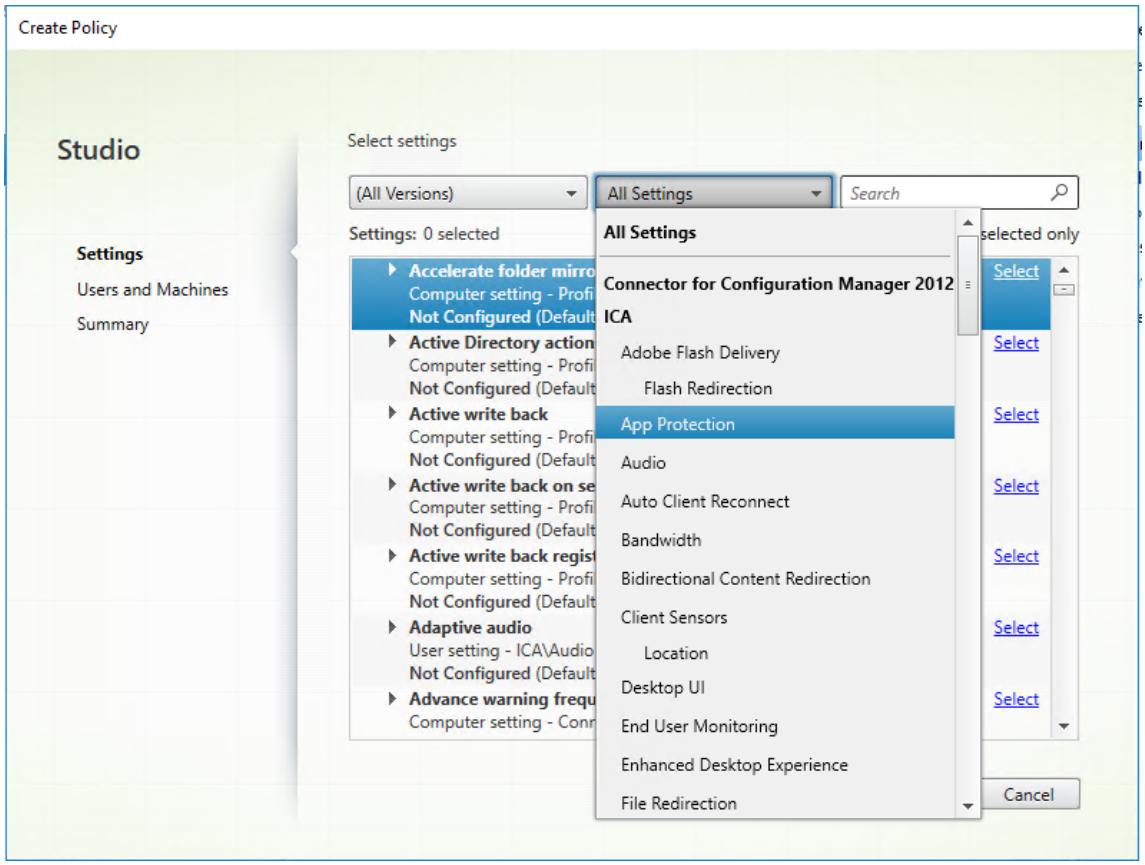
以下が割り当てられていることを確認してください:

- クラウド展開の場合 - Cloud Desktop Delivery Controller のバージョン 115 以降
- オンプレミス展開の場合 - Citrix Virtual Apps and Desktops のバージョン 2308 以降
- Windows Virtual Delivery Agent インストーラーのバージョン 2308 以降
- Windows の場合 - Windows 向け Citrix Workspace アプリ 2309 以降
- Mac の場合 - Mac 向け Citrix Workspace アプリ 2308 以降
- Linux の場合 - Linux 向け Citrix Workspace アプリ 2308 以降

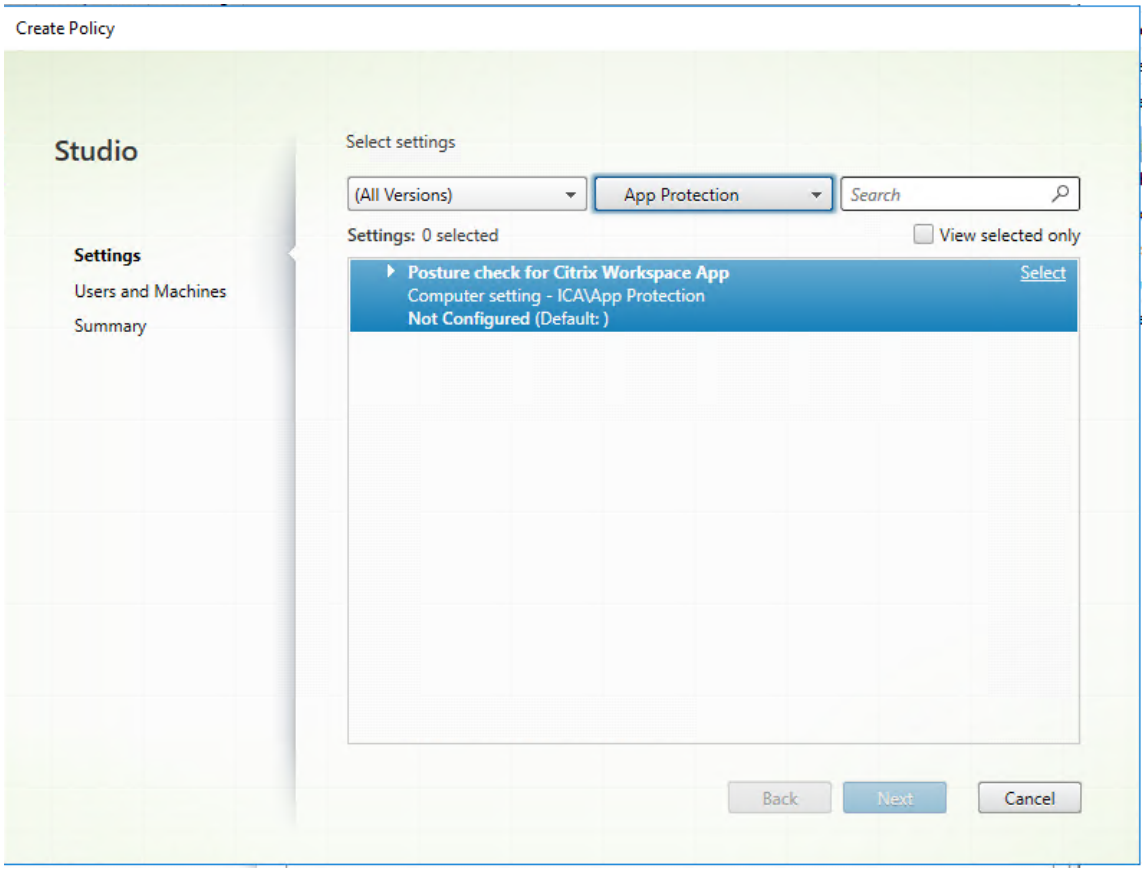
次のように、セキュリティ態勢チェック用の新しい VDA Citrix ポリシーを構成します:

> 注:
>
> この新しい VDA Citrix ポリシーは、Citrix Studio と Web Studio の両方を使用して展開できます。次の手順は Citrix Studio を使用した展開ですが、Web Studio でも同じ手順を使用できます。

1. オンプレミスの場合は Desktop Delivery Controller (DDC)、クラウド展開の場合は Web Studio で Citrix Studio アプリを開き、［ポリシー］を選択します。
2. ［操作］で、［ポリシー］ > ［ポリシーの作成］を選択します。
3. ［すべての設定］ドロップダウンメニューをクリックし、［**ICA**］の下の ［**App Protection**］を選択します。



4. ［**Citrix Workspace** アプリのセキュリティ態勢チェック］を選択し、［選択］をクリックします。

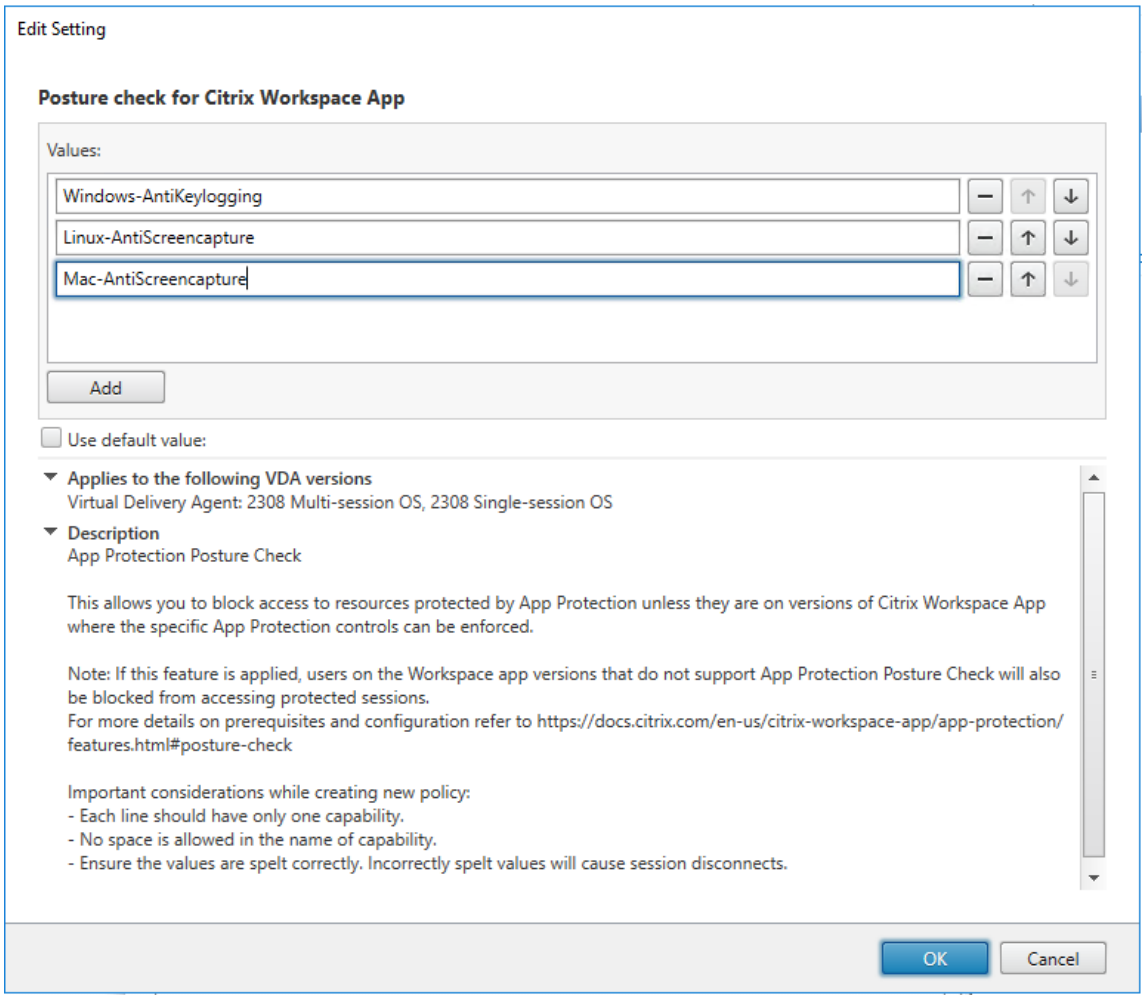


［設定の変更］ウィンドウが開きます。

5. ［デフォルト値を使用］チェックボックスをオフにします。
6. ［追加］をクリックし、次の関連する値を入力します：

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

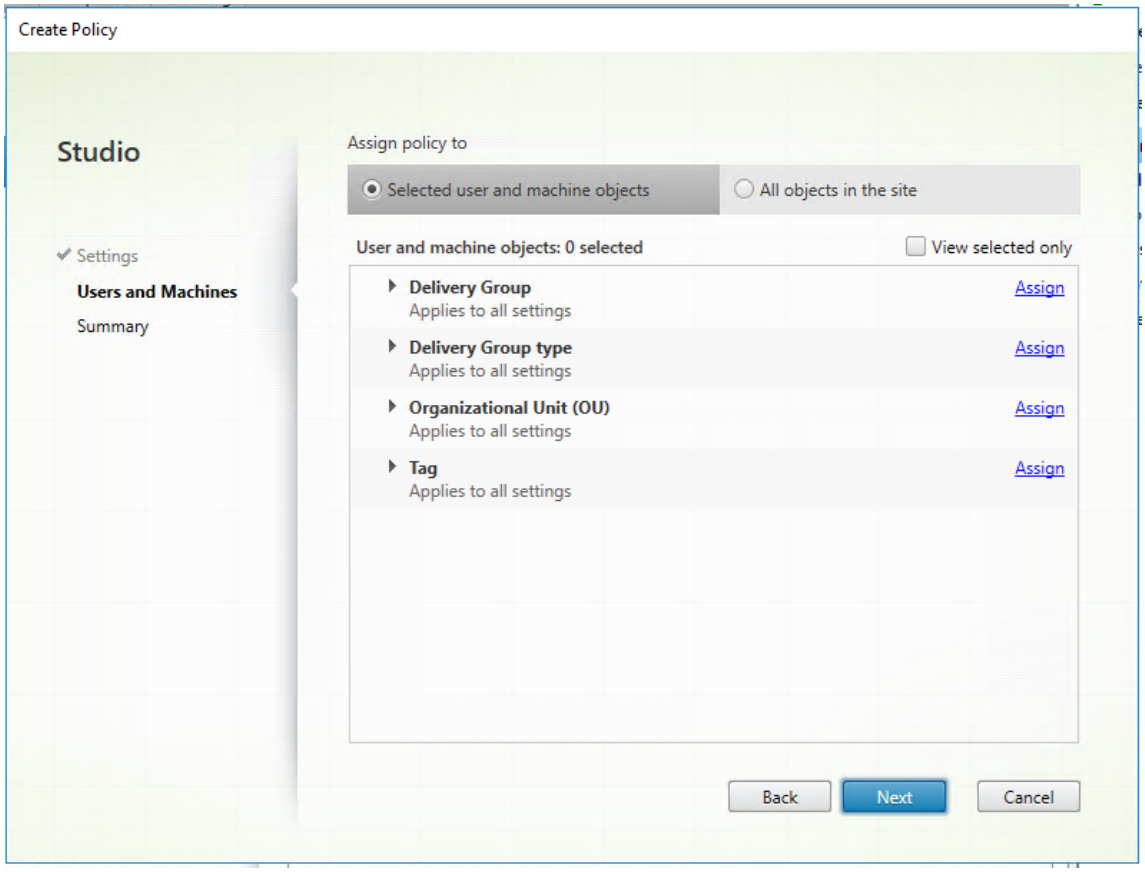
   たとえば、「Windows-AntiScreencapture」と「Windows-AntiKeylogging」を追加した場合、セキュリティ態勢チェックをサポートし、これらの機能を備えた Windows 向け Citrix Workspace アプリは VDA への接続が許可されます。



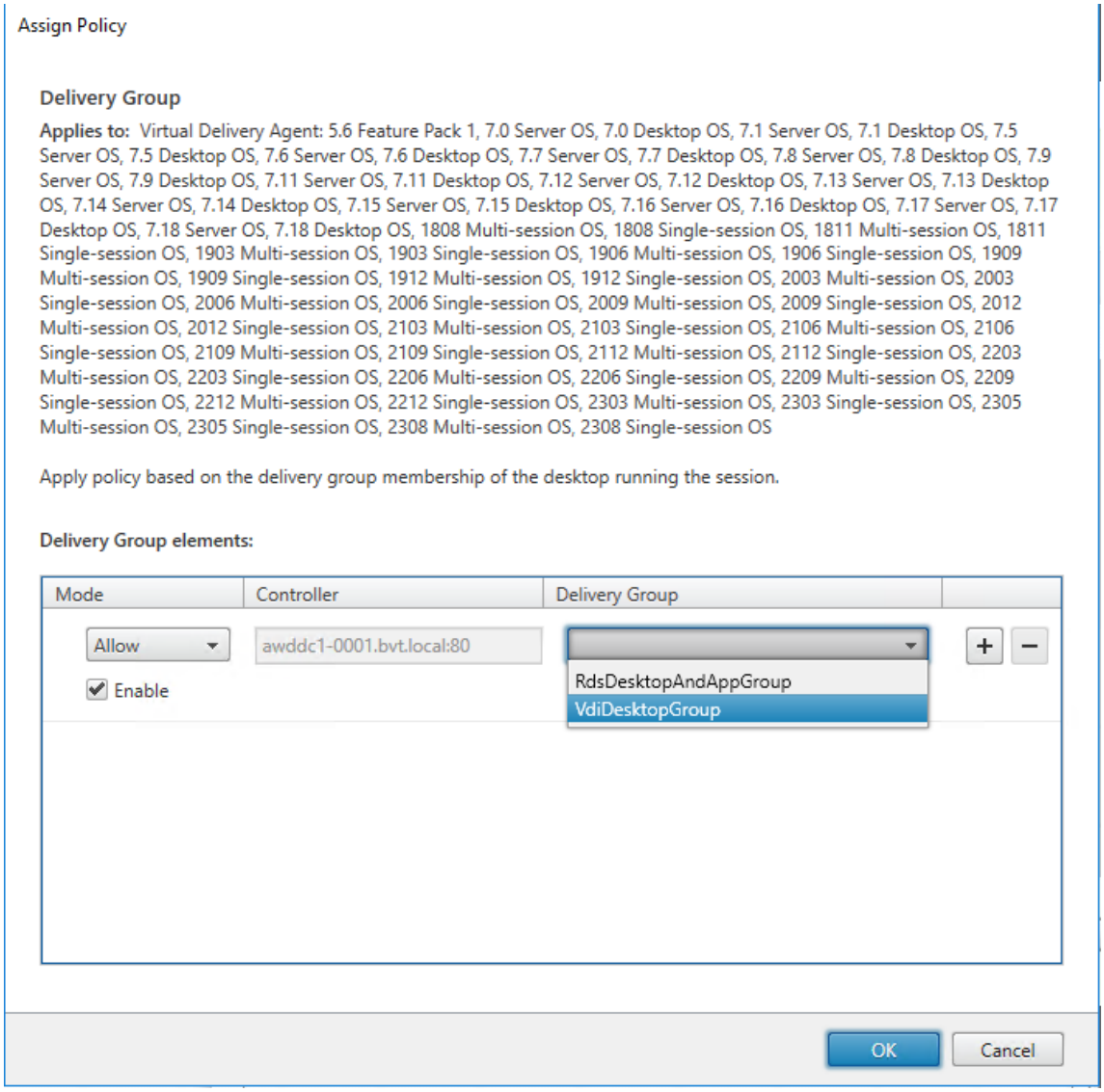
注:

- 各エントリには 1 つの機能のみが含まれている必要があります。
- 機能の名前にスペースを使用することはできません。
- 値のスペルが正しいことを確認してください。値のスペルが間違っていると、セッションが終了します。
- プレフィックスに Windows-、Linux-、または Mac-のない値は無視されます。

7. 必要な値をすべて追加したら、［**OK**］をクリックします。
8. ［次へ］をクリックします。
9. ［ポリシーの割り当て先］ > ［選択したユーザーおよびマシンオブジェクト］を選択します。

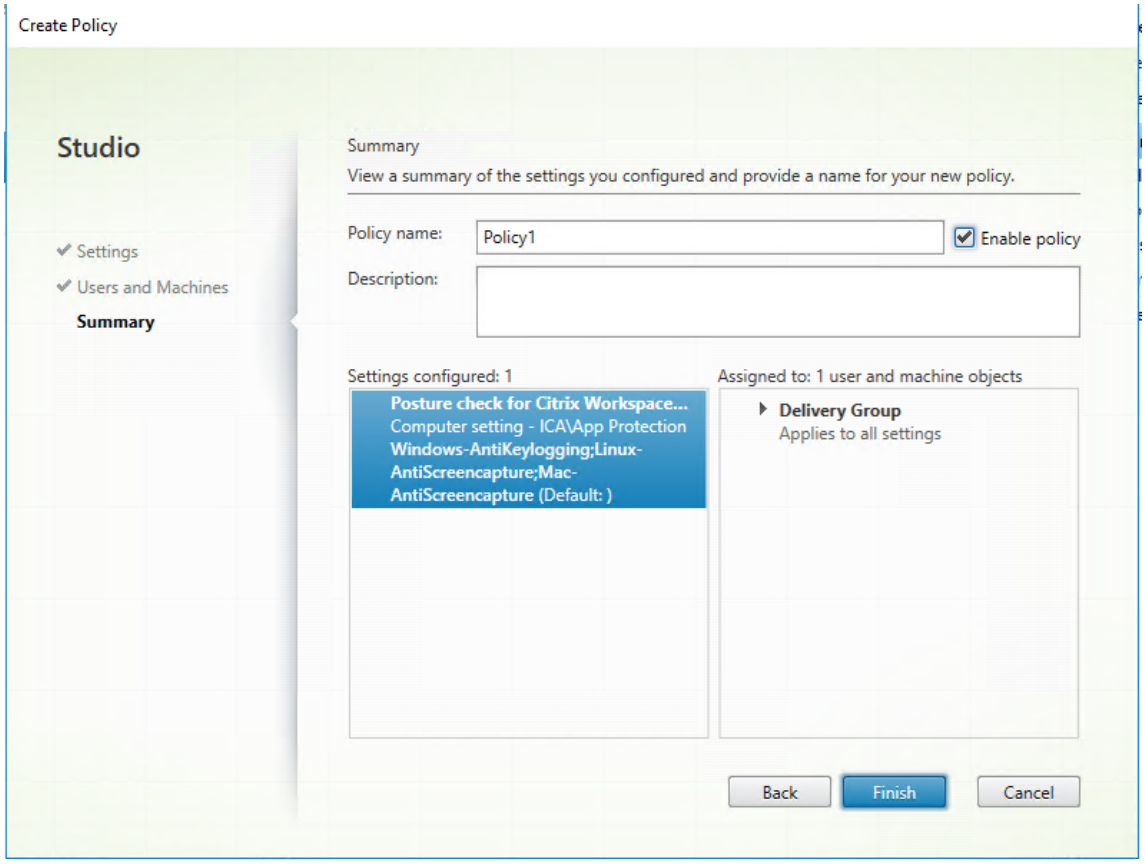


10. このポリシーを展開する必要があるデリバリーグループを選択し、［**OK**］をクリックします。



11. ［次へ］をクリックします。

12. ［ポリシー名］フィールドにポリシー名を入力し、［ポリシーの有効化］チェックボックスをオンにします。

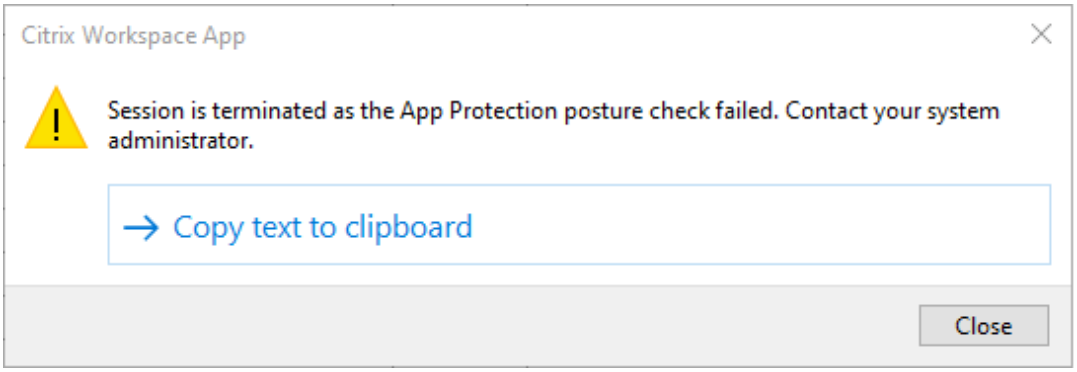


13. ［完了］をクリックします。

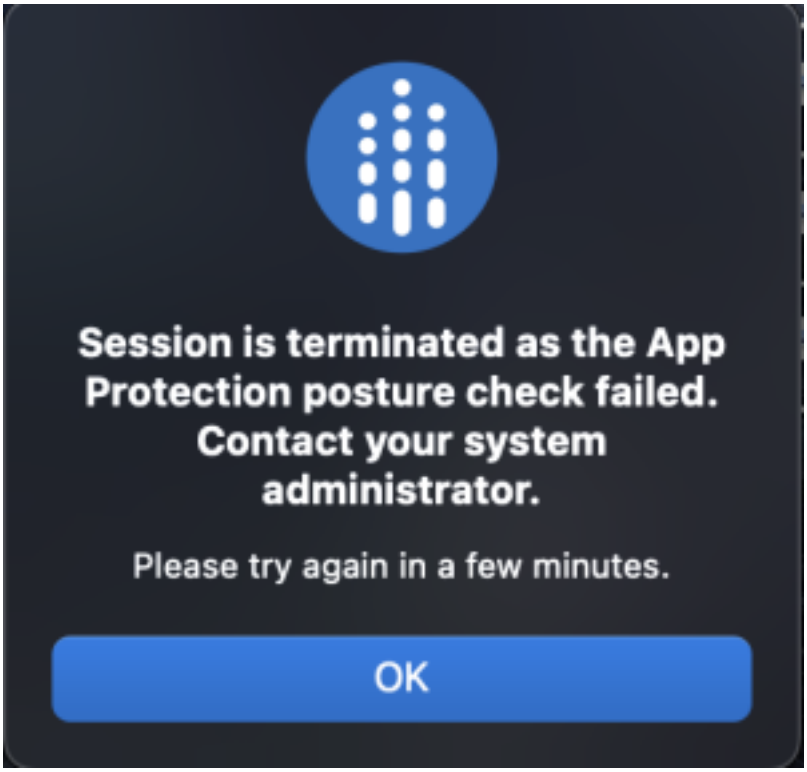
セキュリティ態勢チェック用のポリシーが作成されます。

App Protection のセキュリティ態勢チェックが失敗した場合に想定される動作

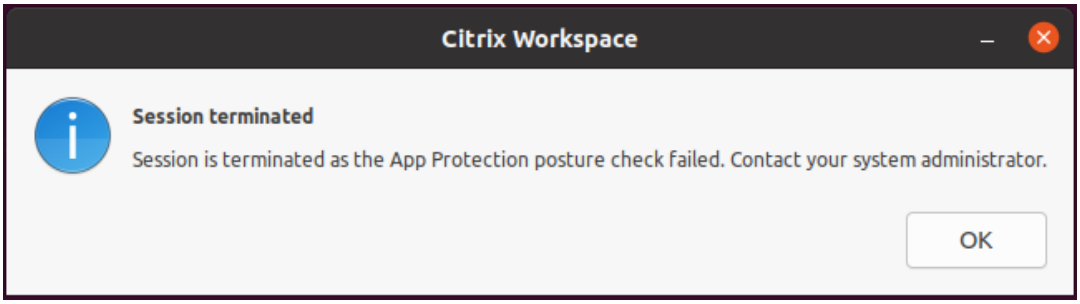
- セキュリティ態勢チェックの VDA Citrix ポリシーが有効で、セキュリティ態勢チェック機能をサポートしていないバージョンの Citrix Workspace アプリを使用している場合、エラーメッセージが表示されずにセッションが終了します。
- セキュリティ態勢チェック機能をサポートしているバージョンの Citrix Workspace アプリを使用している場合、次のエラーメッセージがそれぞれ表示されてセッションが終了します:
  - Windows:



- Mac



- Linux



ダブルホップ起動のブロック

March 10, 2024

ダブルホップ起動をブロックするには、最初のホップで Windows 向け Citrix Workspace アプリ 2309 以降を実行していることを確認します。

最初のホップで、すべての VDA に次の構成を展開します:

1. 最新の GPO ポリシーを更新します。詳しくは、「最新の GPO ポリシーの更新」を参照してください。
2. グループポリシーエディターを起動し、［コンピューターの構成］>［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Workspace**］>［**App Protection**］>［ダブルホップ起動をブロックする］に移動します。
3. ［有効］を選択して ［**OK**］をクリックします。

   ［ダブルホップ起動をブロックする］設定が有効になり、ダブルホップ起動を実行しようとするとブロックされます。

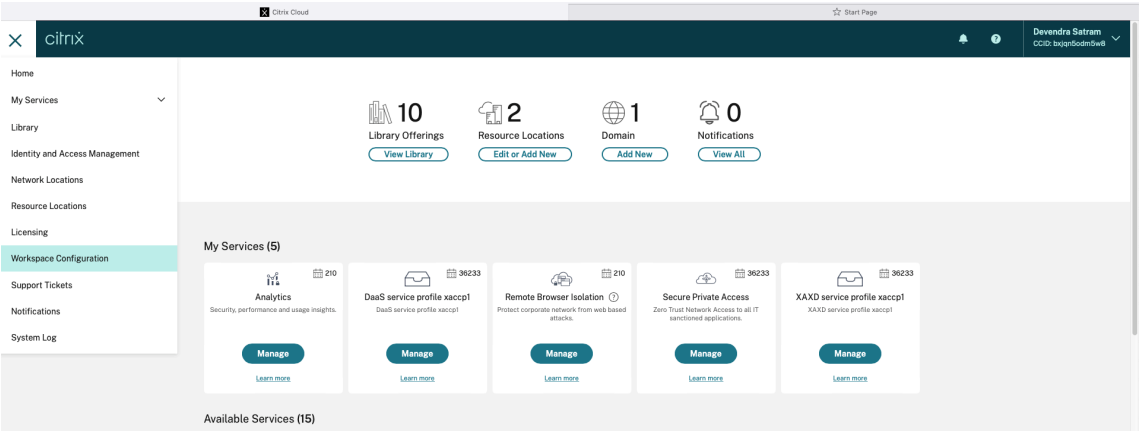
> 注:
>
> Windows Server OS は App Protection をサポートしていません。そのため、最初のホップで Windows Server OS を実行している場合、App Protection が有効になっている Virtual Apps and Desktops は表示されません。

スクリーンショット許可リストの構成

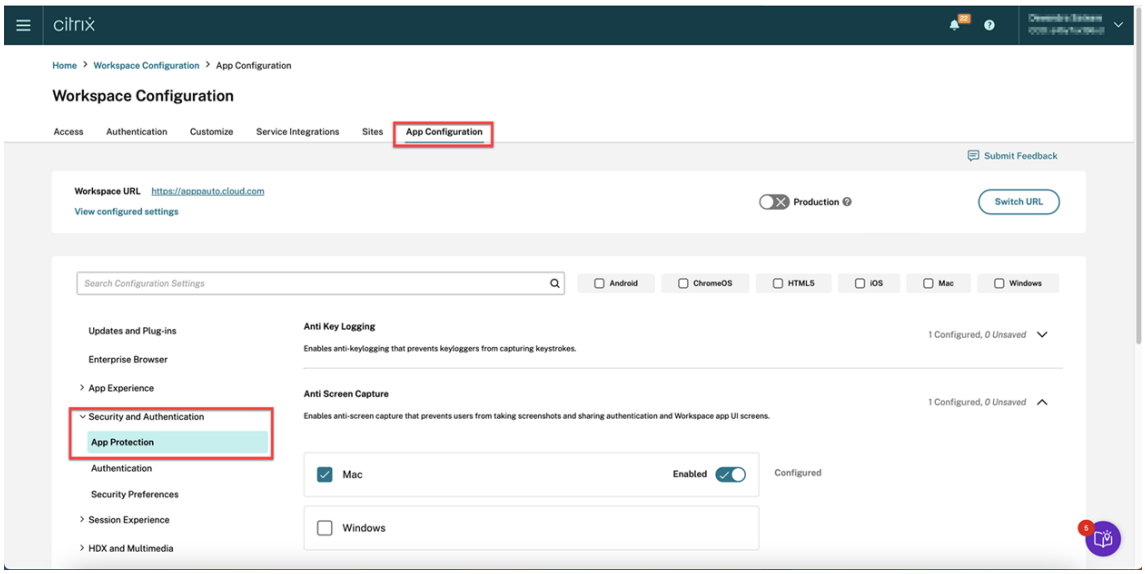
April 25, 2024

アプリをスクリーンショット許可リストに追加するには、次の手順を実行します:

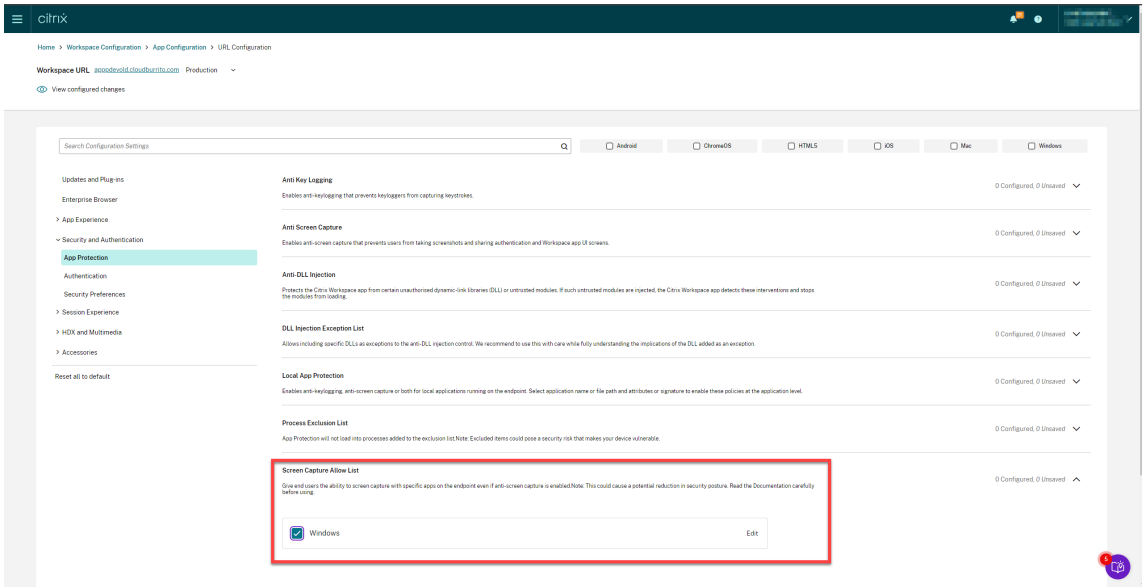
1. Citrix Cloud アカウントにサインインし、［ワークスペースの構成］を選択します。



2. ［アプリ構成］ > ［セキュリティと認証］ > ［構成］ > ［**App Protection**］を選択します。



3. ［スクリーンショット許可リスト］をクリックし、［**Windows**］チェックボックスを選択します。



4. ［編集］オプションをクリックします。

   Manage settings for Windows 画面が表示されます。

5. スクリーンショット許可リストに追加する、アプリに関する情報を追加します。

   例:

```
[
 {

  "name": "ScreenshotTool_1.exe",
  "signature": "ScreenshotTool_1 Signature",
```



```
 "publisher": "ScreenshotTool_1 Publisher"
  }
 ,
 {

  "name": "Screenshottool_2.exe",
  "signature": "",
  "publisher": ""
  }

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

Manage settings for Windows

```
[
  {
    "name": "ScreenshotTool_1.exe",
    "signature": "ScreenshotTool_1_Signature",
    "publisher": "ScreenshotTool_1_Publisher"
  },
  {
    "name": "ScreenshotTool_2.exe",
    "signature": "",
    "publisher": ""
  }
]
```

Save draft　Cancel

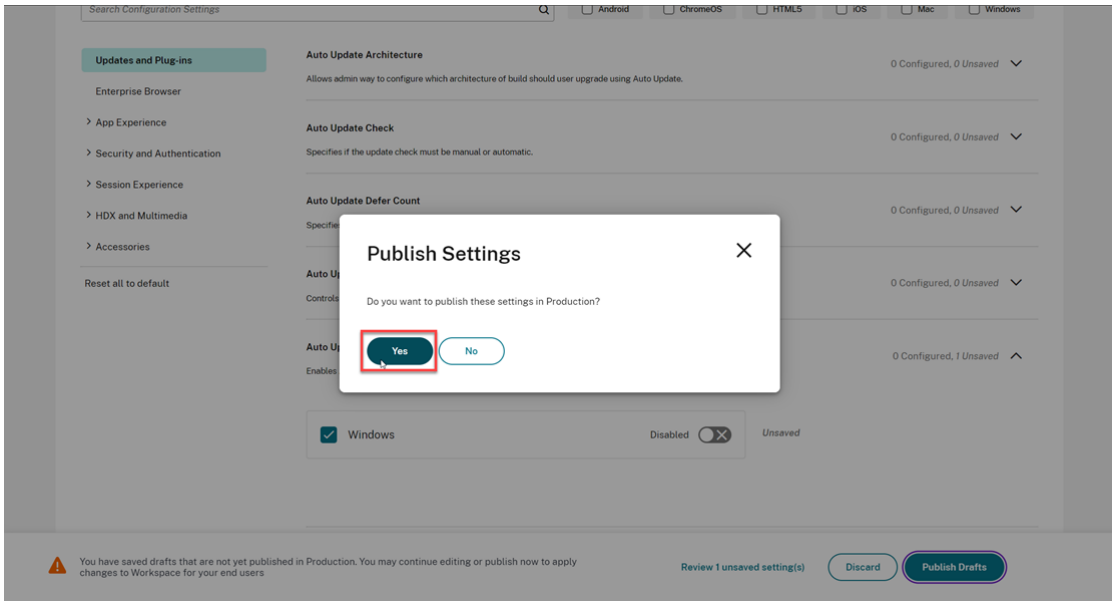
注:

- nameは必須のフィールドです。一方、publisherとsignatureは必須ではありません。ただし、許可リストに登録されたアプリのみがスクリーンショットを撮ることができるように、関連するpublisherとsignatureを追加することをお勧めします。

> - publisherとsignatureの値がない場合は、同じ名前の悪意のあるアプリケーションがスクリーンショットをキャプチャする可能性があります。
> - また、このブロックに複数のエントリを追加することで、スクリーンショット許可リストに複数のアプリを追加することができます。

publisherおよびsignature情報を取得するには、「publisherおよびsignature情報を取得する」を参照してください。

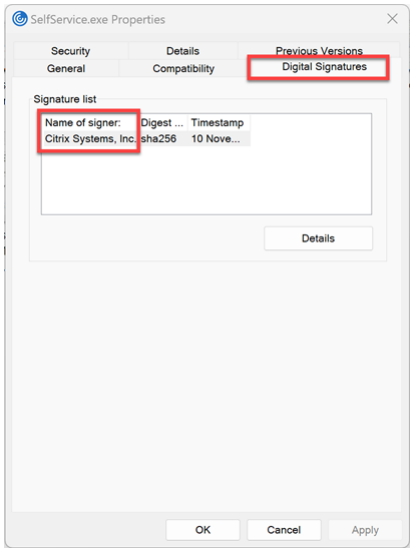
6. ［下書きを保存］をクリックし、［下書きの公開］をクリックします。
7. ［設定の公開］ダイアログボックスで、［はい］をクリックします。



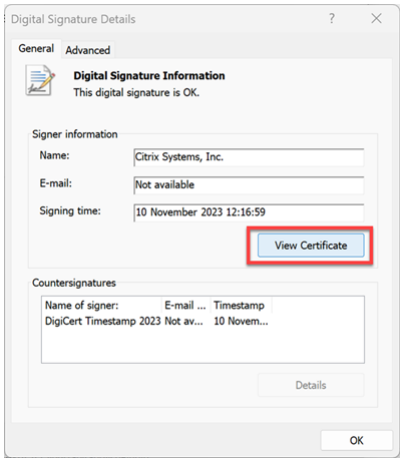
publisher および signature 情報を取得する

publisherおよびsignature情報を取得するには、次の手順を実行します：

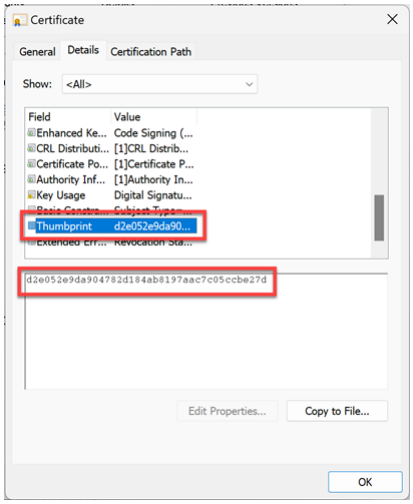
1. アプリの関連する.exeファイルがあるファイルの場所を開きます。
2. .exeファイルを右クリックし、［**Properties**］をクリックします。プロパティのポップアップ画面が表示されます。
3. ［**Digital Signatures**］をクリックします。［**Name of signer**］はpublisherの値です。



4. ［**Name of signer**］の最初のエントリをクリックしてから、［**Details**］> ［**View Certificate**］の順にクリックします。



5. ［**Details**］> ［**Thumbprint**］の順にクリックします。テキストボックスに表示される内容は`signature`です。

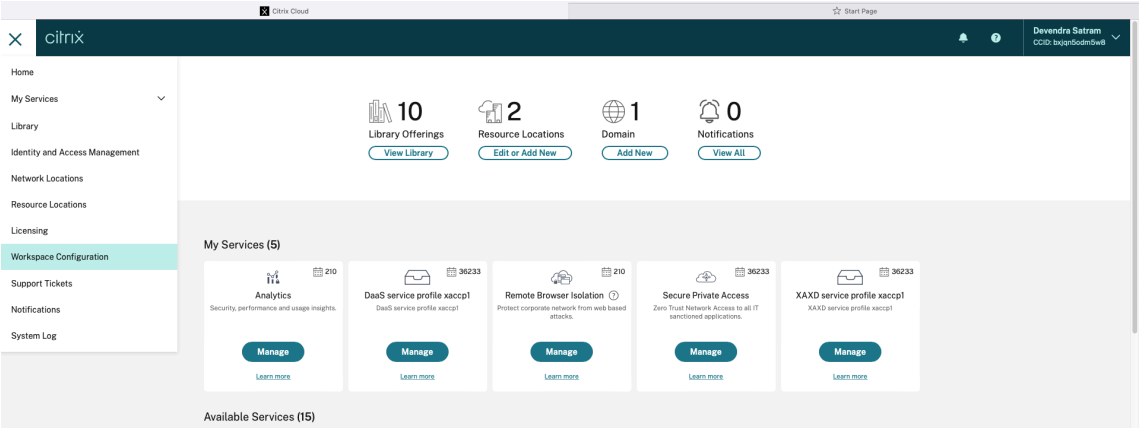


プロセス除外リストの構成

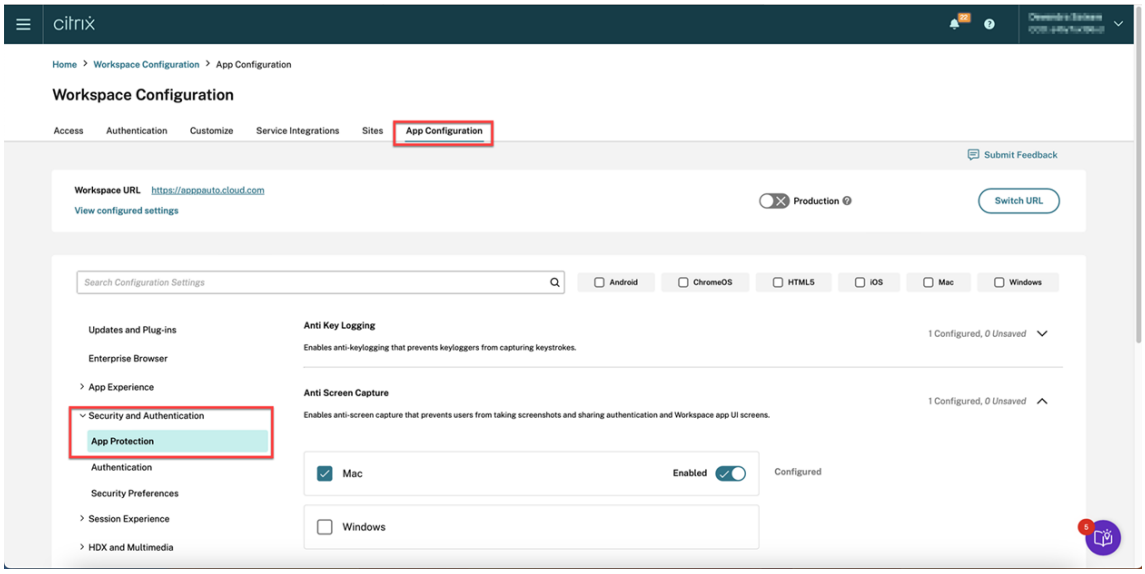
April 25, 2024

プロセスをプロセス除外リストに追加するには、次の手順を実行します：

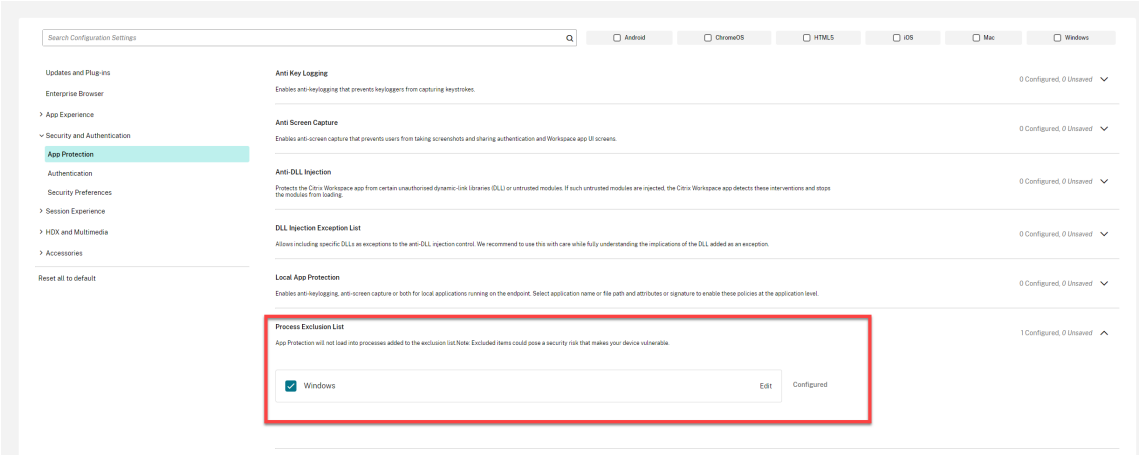
1. Citrix Cloud アカウントにサインインし、［ワークスペースの構成］を選択します。



2. ［アプリ構成］＞［セキュリティと認証］＞［構成］＞［**App Protection**］を選択します。



3. ［プロセス除外リスト］をクリックし、［**Windows**］チェックボックスを選択します。



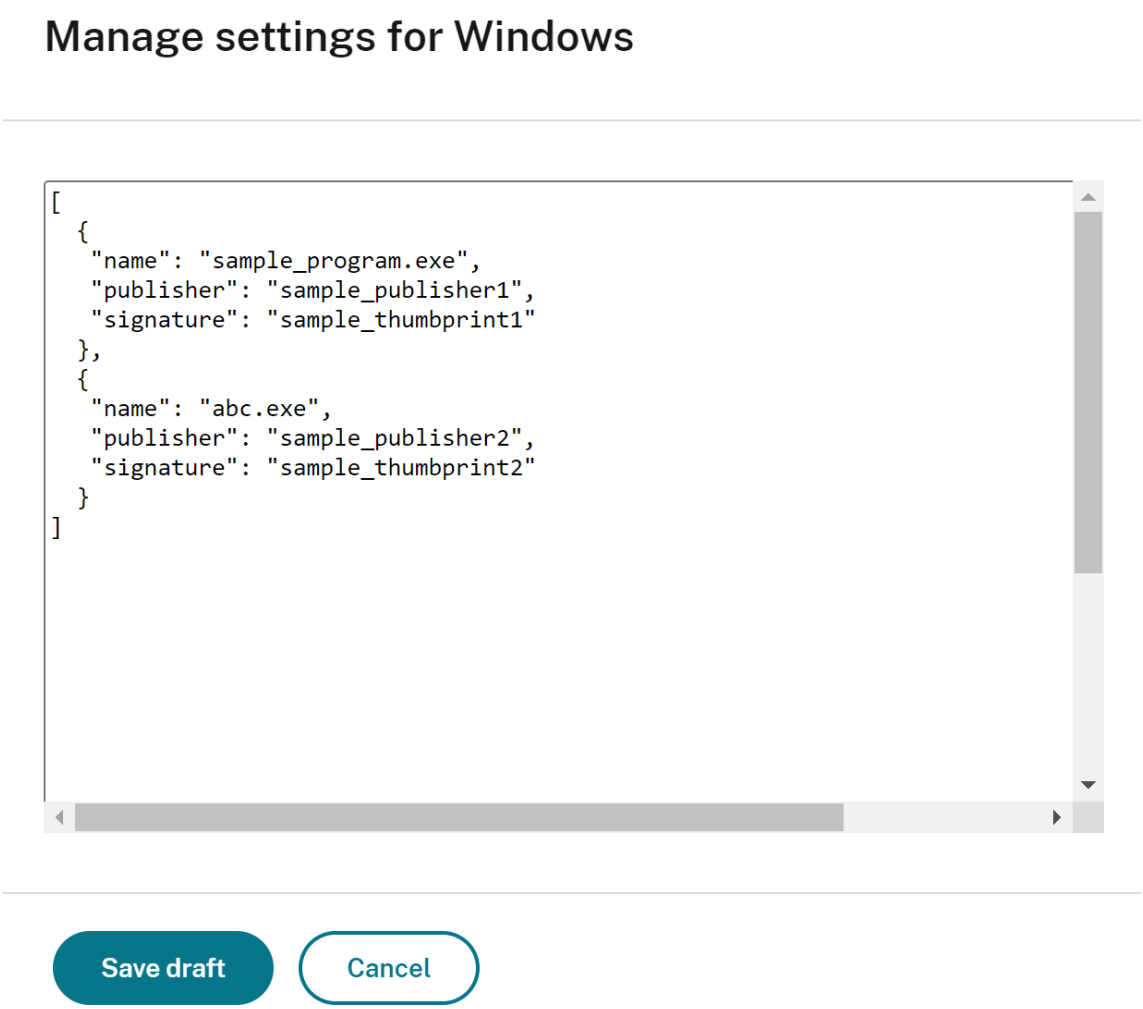
4. ［編集］オプションをクリックします。

   Manage settings for Windows 画面が表示されます。

5. プロセス除外リストに追加するための、プロセスに関する情報を追加します。

   例:

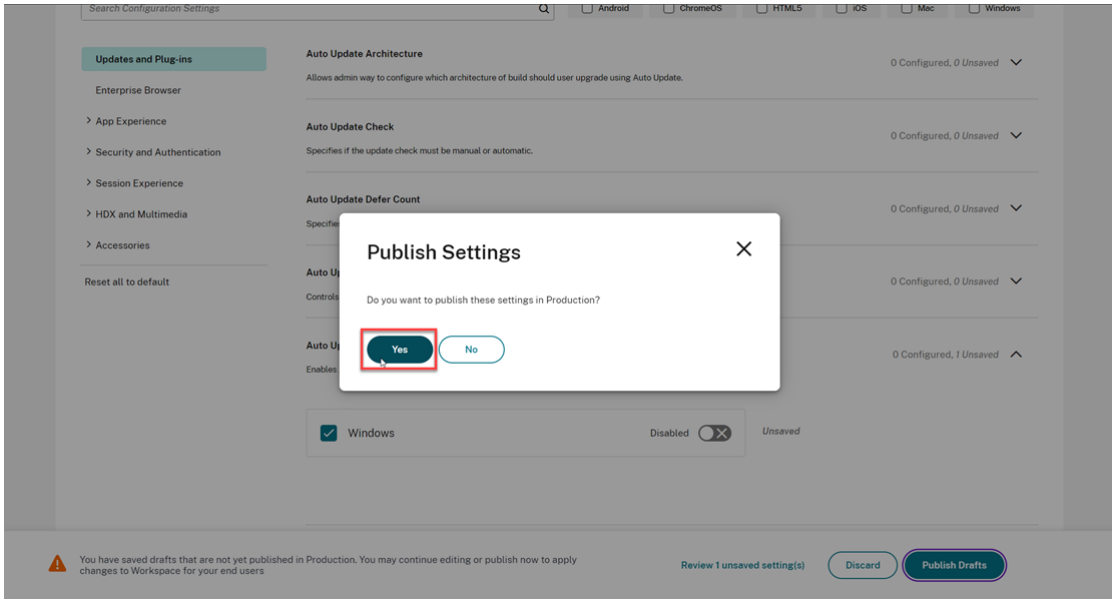
```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

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

> 注:
>
> - nameは必須のフィールドです。一方、publisherとsignatureは必須ではありません。ただし、正しいプロセスがリストに追加されるように、publisherとsignatureを追加することをお勧めします。
> - また、このブロックに複数のエントリを追加することで、プロセス除外リストに複数のプロセスを追加することができます。

publisherおよびsignature情報を取得するには、「publisherおよびsignature情報を取得する」を参照してください。

6. ［下書きを保存］をクリックし、［下書きの公開］をクリックします。
7. ［設定の公開］ダイアログボックスで、［はい］をクリックします。



8. Citrix Workspace アプリを再起動します。

USB フィルタードライバー除外リストの構成

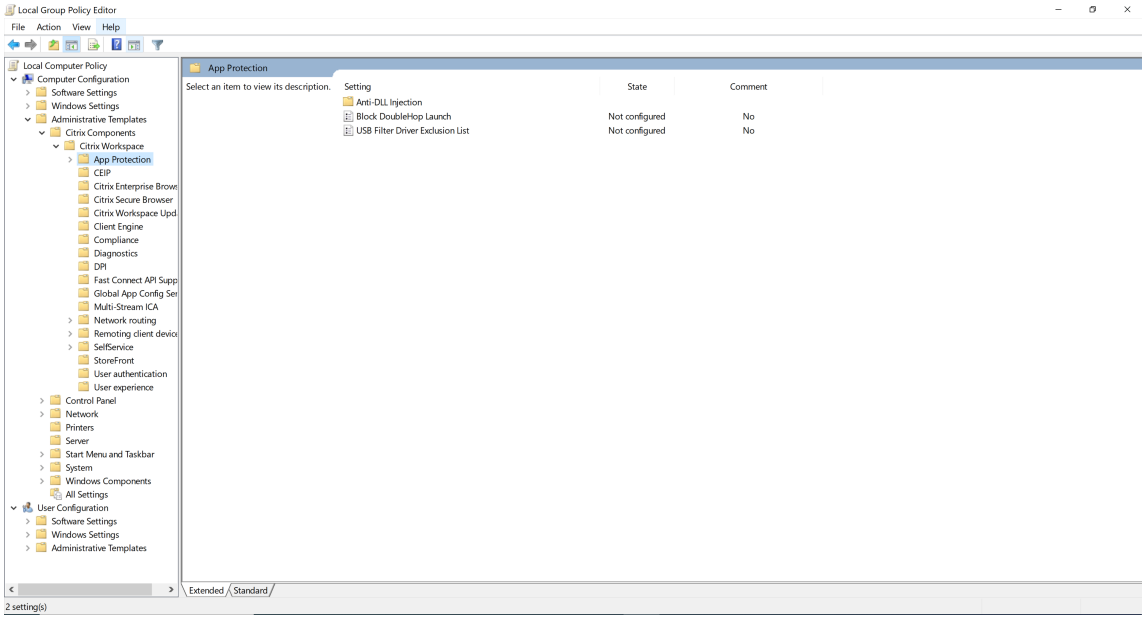
April 25, 2024

次のいずれかの方法を使用して、USB デバイスを USB フィルタードライバー除外リストに追加できます:

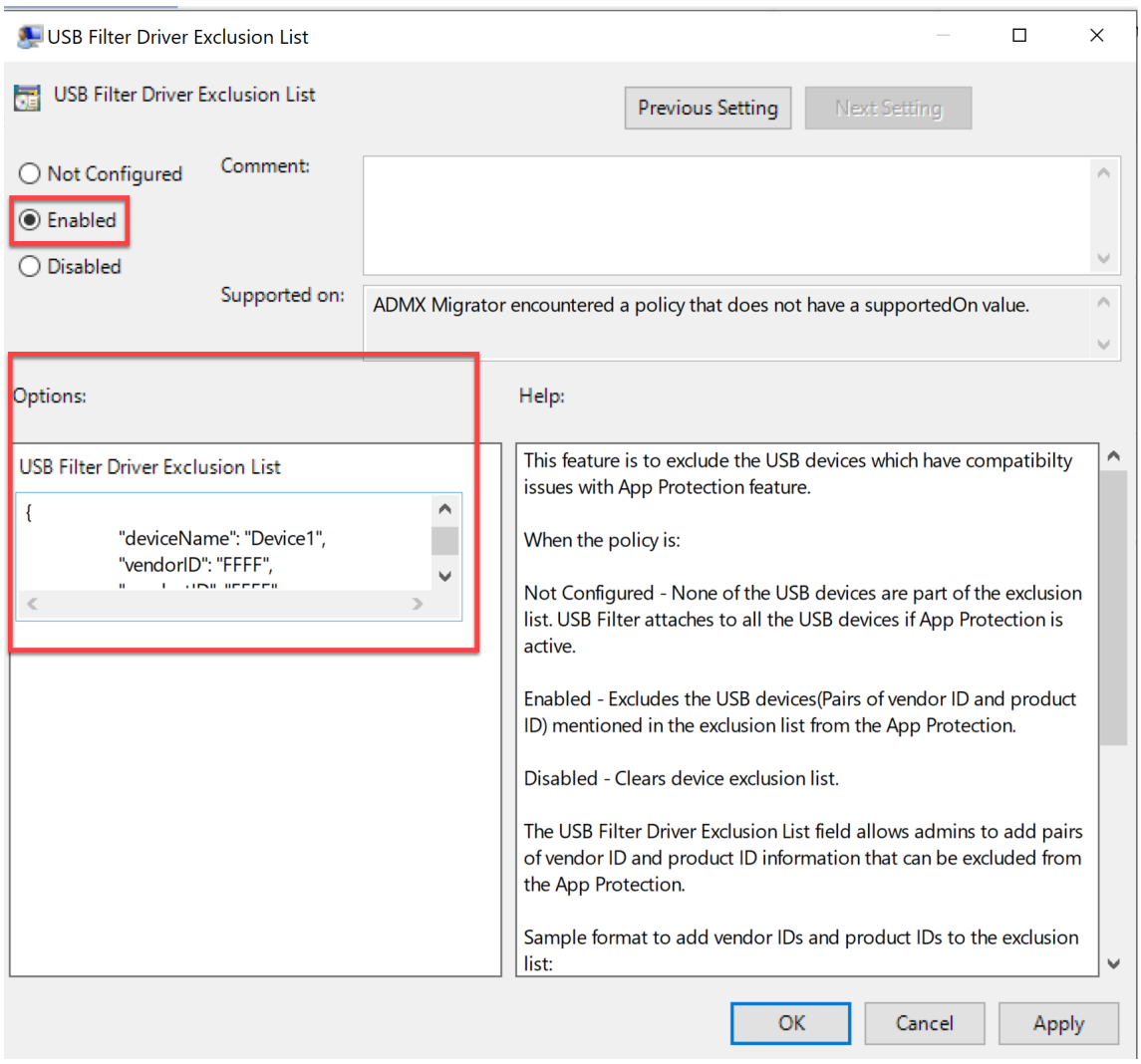
- グループポリシーオブジェクトの使用
- Global App Configuration Service の UI の使用

グループポリシーオブジェクトの使用

1. `gpedit.msc`を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。詳しくは、「グループポリシーオブジェクト」を参照してください。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [**Citrix** のコンポーネント] > [**Citrix Workspace**] > [**App Protection**] > [**USB** フィルタードライバー除外リスト] に移動します。



3. ［有効］を選択し、［オプション］テキストボックスに除外する USB デバイスのベンダー **ID** と製品 **ID** を入力します。



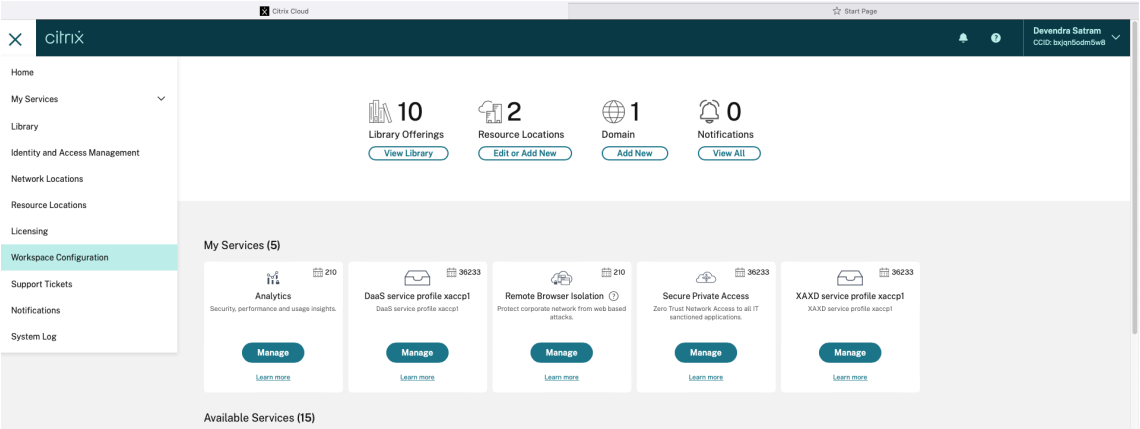
> 注:
>
> - productIDとvendorIDは必須のフィールドです。一方、deviceNameは必須ではありません。
> - また、このブロックに複数のエントリを追加することで、除外リストに複数の USB デバイスを追加することができます。

productIDとvendorIDを取得するには、「productIDを取得するvendorID」を参照してください。

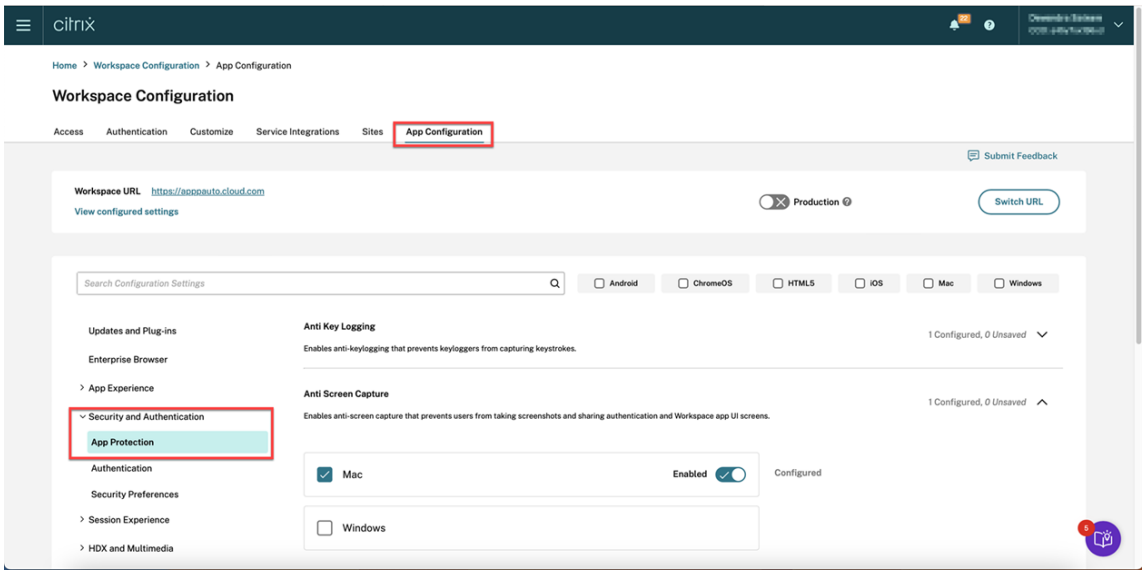
4. [**OK**] をクリックします。

Global App Configuration Service の UI の使用

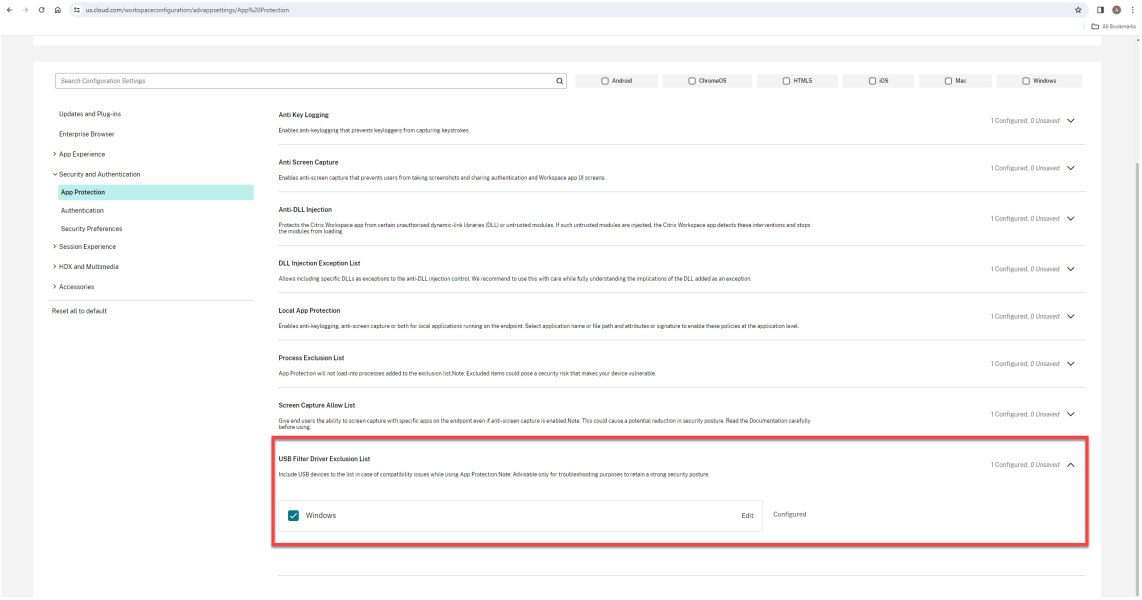
1. Citrix Cloud アカウントにサインインし、[ワークスペースの構成] を選択します。



2. ［アプリ構成］ > ［セキュリティと認証］ > ［構成］ > ［**App Protection**］を選択します。



3. ［**USB** フィルタードライバー除外リスト］をクリックし、［**Windows**］チェックボックスを選択します。



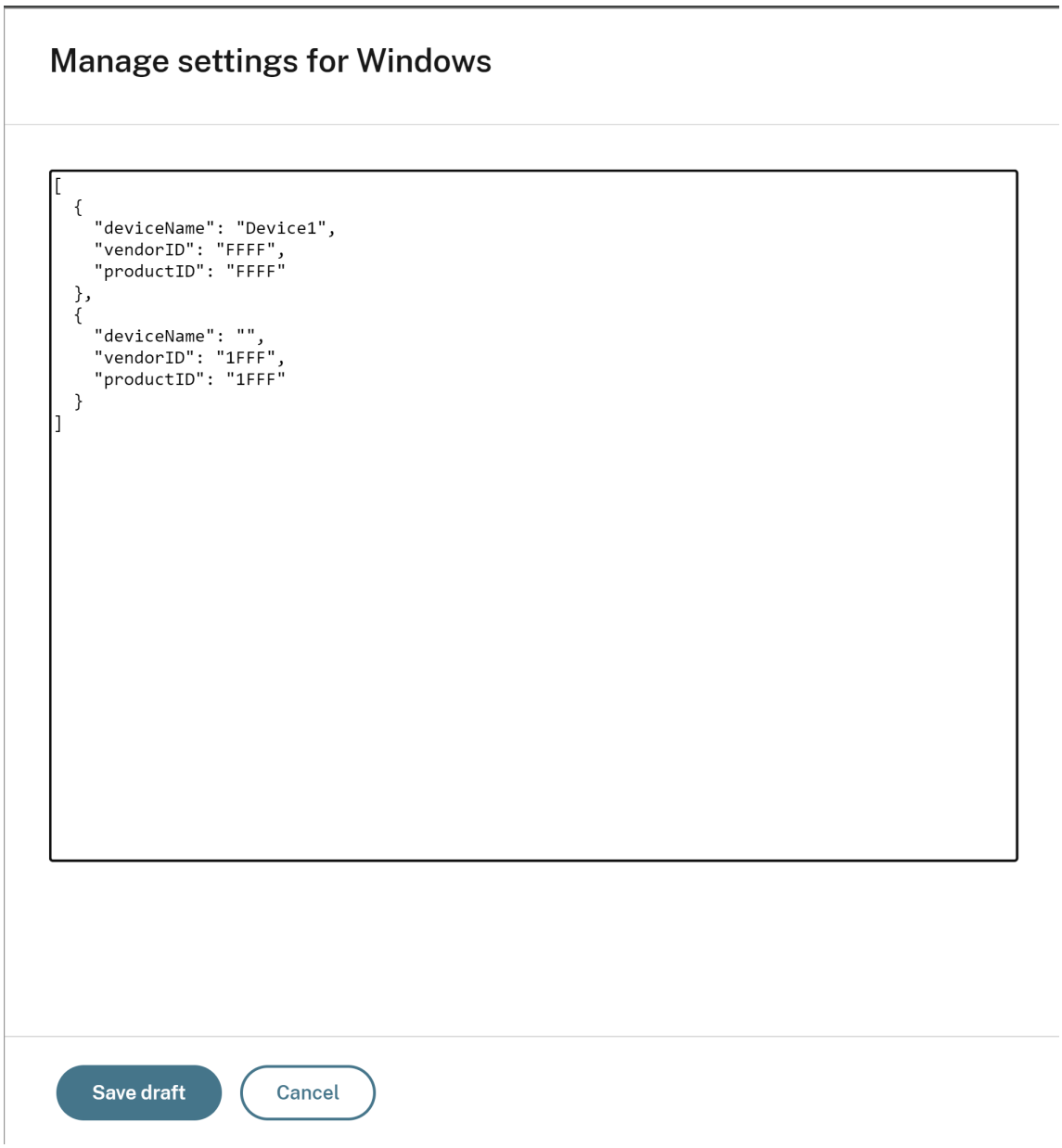
4. ［編集］オプションをクリックします。

   Manage settings for Windows 画面が表示されます。

5. USB フィルタードライバー除外リストに追加するための、プロセスに関する情報を追加します。

   例:

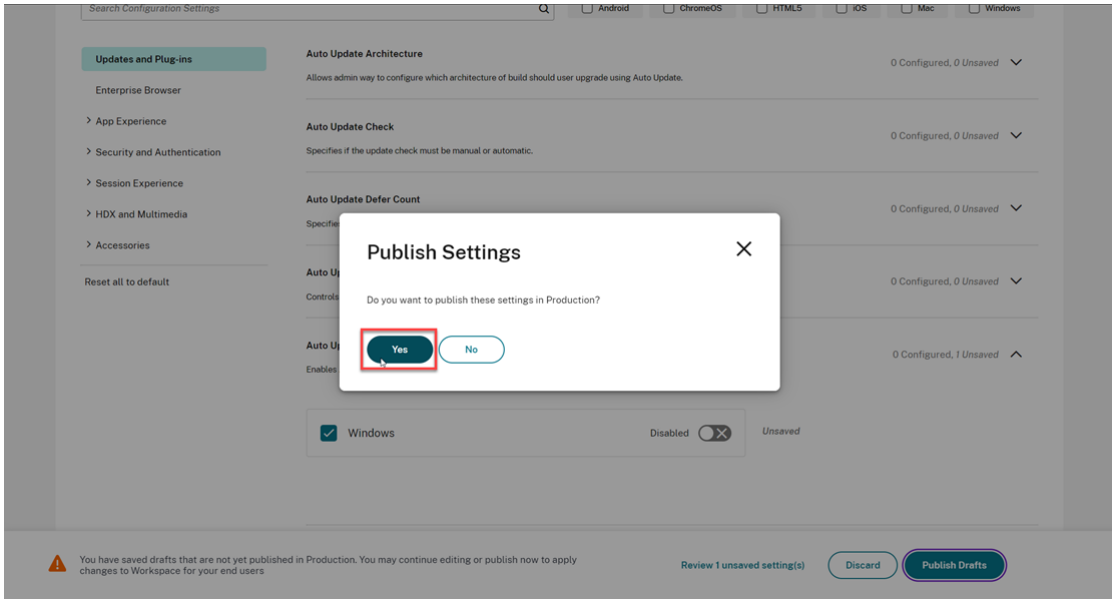
```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

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

> 注:
>
> - productIDとvendorIDは必須のフィールドです。一方、deviceNameは必須ではありません。
> - また、このブロックに複数のエントリを追加することで、除外リストに複数の USB デバイスを追加することができます。

productIDとvendorIDを取得するには、「productIDを取得するvendorID」を参照してください。

6. ［下書きを保存］をクリックし、［下書きの公開］をクリックします。
7. ［設定の公開］ダイアログボックスで、［はい］をクリックします。

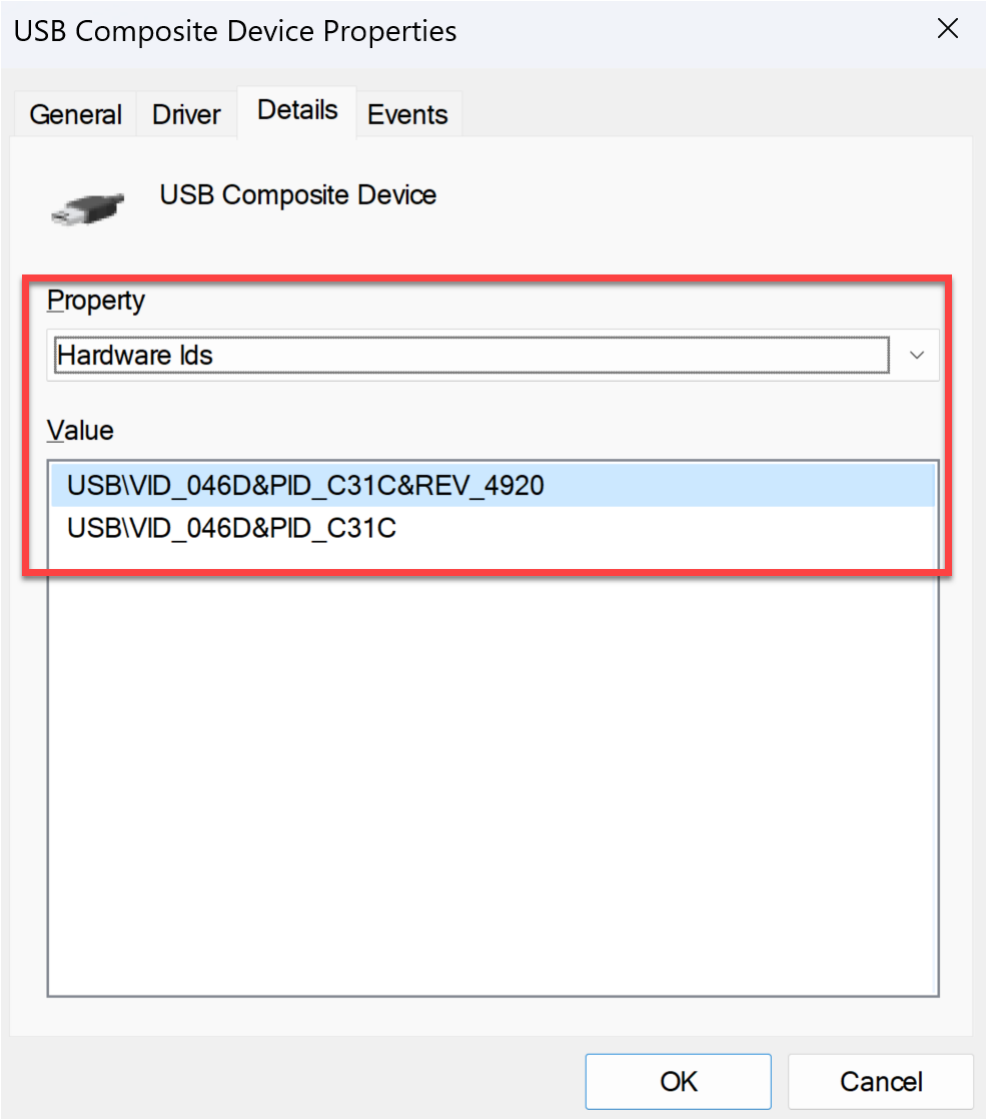


8. Citrix Workspace アプリを再起動します。

productID と vendorID を取得する

productIDとvendorIDを取得するには、次の手順を実行します:

1. デバイスマネージャーを開き、除外リストに追加するデバイスを見つけます。
2. デバイス名を右クリックし、[**Properties**] をクリックします。プロパティのポップアップ画面が表示されます。
3. [**Details**] をクリックし、[**Property**] 一覧から [**Hardware Ids**] オプションを選択します。
4. [値] フィールドでは、プレフィックスVID_が付いた値はvendorIDであり、プレフィックスPID_が付いた値はproductIDです。



トラブルシューティング

March 10, 2024

この記事では、さまざまなプラットフォーム向けの Citrix Workspace アプリで App Protection のトラブルシューティングを行う方法について説明します。

トラブルシューティングのシナリオについては、以下を参照してください:

- 一般的なトラブルシューティングのシナリオ
- ポリシーの改ざんの検出
- App Protection のセキュリティ態勢チェック

Windows 向け Citrix Workspace アプリ

1. 「ログ収集」の手順に従ってログを収集します。
2. **Windows + R** キーを押して［実行］ボックスを開き、「`cmd`」と入力して **Enter** キーを押します。
3. 次のコマンドを実行します：
   - バージョン 2311 より前の Windows 向け Citrix Workspace アプリを使用している場合は、次のコマンドを実行します：
     - `sc query appprotectionsvc`
     - `sc query entryprotectdrv`
     - `sc query epinject6`
     - `sc query epusbfilter`
   - バージョン 2311 以降の Windows 向け Citrix Workspace アプリを使用している場合は、次のコマンドを実行します：
     - `sc query appprotectionsvc`
     - `sc query ctxapdriver`
     - `sc query ctxapinject`
     - `sc query ctxapusbfilter`

ログ収集ツールから収集されたトレース情報とともに結果を提供します。

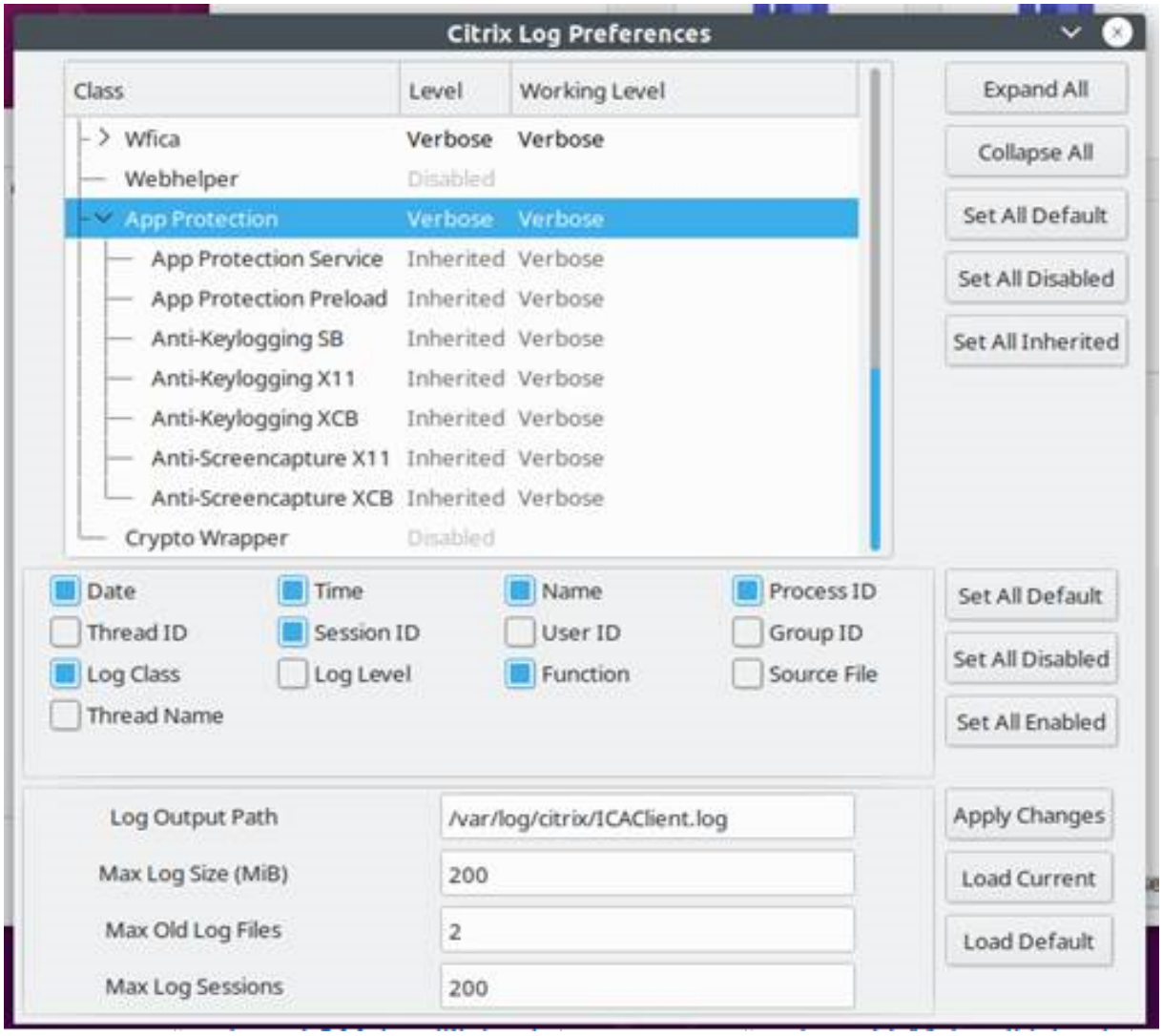
Mac 向け Citrix Workspace アプリ

「ログの収集」で説明された手順に従って収集したログを提供します。

Linux 向け Citrix Workspace アプリ

1. インストールの *util* フォルダーにある setlog 実行可能ファイルを実行します。例：`/opt/Citrix/ICAClient/util/setlog`。
2. ［すべて無効に設定］をクリックします（この手順はオプションであり、必要なログのみが収集されるようにしてください）。
3. App Protection のログ記録に移動します。
4. 右クリックして［詳細］を選択し、App Protection のログレベルを［詳細］に設定します（警告とエラーのみがログに記録されます）。
5. App Protection のクラスを展開し、その子要素を右クリックします。［グループ］**>**［継承］を選択します。

6. **wfica** のログを有効にします。**wfica** を右クリックし、［詳細］を選択します。App Protection がインストールされていないか、**wfica** で検出できない場合は、次のようなログが取得されます。［**NCS**］**< P3563 > citrix-wfica: App Protection is not installed**。
7. セッションを起動すると、setlog のログ出力パスに記載されているファイルにログが記録されます。



一般的なトラブルシューティング

March 10, 2024

App Protection ポリシーが有効になっているリソースがネイティブアプリに表示されない場合

App Protection ポリシーが有効になっているリソースがネイティブアプリに表示されない場合は、以下の手順を実行します:

1. Citrix Workspace アプリが以下より古い場合は、新しいバージョンに更新します:
   - Linux 向け Citrix Workspace アプリ 2108
   - Windows 向け Citrix Workspace アプリ 2203.1 LTSR
   - Windows 向け Citrix Workspace アプリ 2002
   - Windows（ストア）向け Citrix Workspace アプリ 2305.1
   - Mac 向け Citrix Workspace アプリ 2001
2. Windows 2016 や Windows 2022 などの Windows マルチセッションオペレーティングシステムに、Citrix Workspace アプリがインストールされていないことを確認してください。
3. 上記の条件が満たされていてもリソースが表示されない場合は、ログを収集し、Citrix テクニカル サポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

オンプレミスストアの使用中に、**App Protection** ポリシーが有効になっているリソースがブラウザーに表示されない

オンプレミスストアの使用中に、App Protection ポリシーが有効になっているリソースがブラウザーに表示されない場合は、以下の手順を実行します:

1. Delivery Controller のバージョンがバージョン 1912 より前でないことを確認してください。

   > 注:
   >
   > バージョン 1912 より前の Delivery Controller を使用している場合、App Protection はサポートされません。

2. StoreFront バージョン 1912～2203 を使用している場合は、StoreFront のカスタマイズが有効になっているかどうかを確認してください。StoreFront のカスタマイズを有効にする方法について詳しくは、「StoreFront のカスタマイズの有効化」を参照してください。
3. StoreFront バージョン 2308 以降を使用している場合は、StoreFront のカスタマイズを有効にする必要はありません。StoreFront バージョン 2308 以降のハイブリッド起動を使用して、StoreFront でのハイブリッド起動の App Protection が正しく有効になっているかどうかを確認します。
4. デリバリーグループの App Protection 機能が正しく有効になっているかどうかを確認してください。
5. 上記の条件が満たされていてもリソースが表示されない場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログの収集について詳しくは、「Citrix Workspace アプリのログの収集」および「StoreFront のログの収集」を参照してください。

App Protection が有効なリソースを起動するときに安全な環境を確立できない

Windows 向け Citrix Workspace アプリの場合、App Protection サービスが開始され安全な環境が確立されるように、インストール中に ［インストール後に **App Protection** を開始する］チェックボックスを有効にする必要があります。インストール中に ［インストール後に **App Protection** を開始する］チェックボックスを有効にしなかった場合、App Protection ポリシーが有効になっているリソースを起動すると、App Protection サービスが自動的に開始されます。システム負荷に応じて、App Protection の起動に時間がかかる場合があります。起動する場合もあれば、タイムアウトする場合もあります。したがって、インストール中に ［インストール後に **App Protection** を開始する］チェックボックスをオンにすることをお勧めします。通常は、App Protection を有効にしてリソースを再起動し、安全な接続を確立する必要があります。ただし、それでも App Protection が有効になっているリソースを起動できない場合は、次の手順を実行します:

1. 管理者としてコマンドプロンプトを開き、次のコマンドを実行して、App Protection サービスが実行されているかどうかを確認します:

```
sc query AppProtectionSvc
<!--NeedCopy-->
```

2. App Protection サービスが実行されていない場合は、次のコマンドを実行してサービスを開始します:

```
sc start AppProtectionSvc
<!--NeedCopy-->
```

3. 引き続きエラーが発生する場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

App Protection を有効または無効にできない

Web Studio または PowerShell を使用してオンプレミスまたはクラウドのデリバリーグループの App Protection を有効または無効にできない場合は、次の手順を実行します:

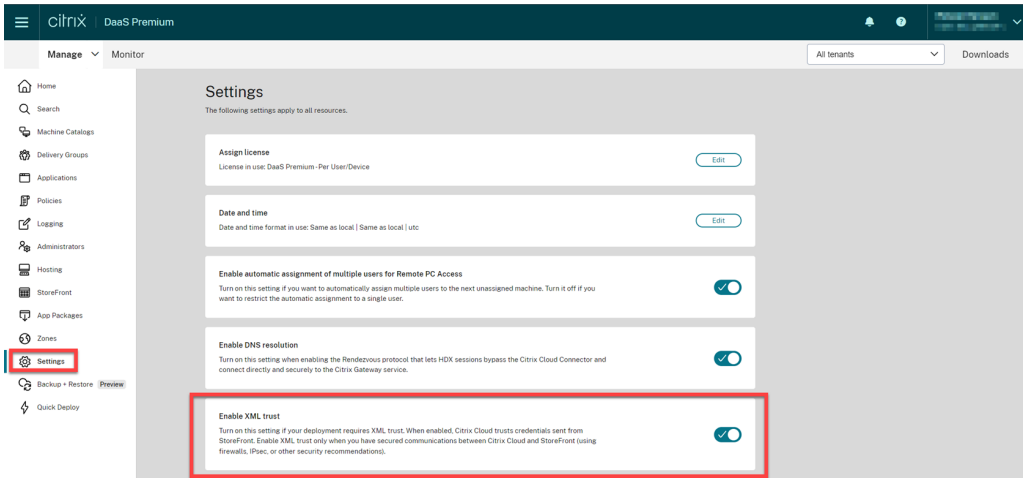
1. 必要なライセンスがあるかどうかを確認してください。必要なライセンスが利用できない場合、App Protection を有効にすることはできません。
2. 必要なライセンスが利用できない場合は、必要なライセンスを取得してライセンスを追加します。
3. ライセンスを追加した後、ライセンスサーバーを再起動し、App Protection を再度有効にしてみてください。
4. 有効なライセンスが利用可能であるにもかかわらず、App Protection を有効または無効にできない場合は、次のコマンドを実行して`TrustRequestsSentToTheXmlServicePort`が有効になっているかどうかを確認します:

```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
<!--NeedCopy-->
```


5. `TrustRequestsSentToTheXmlServicePort`が有効になっていない場合は、次のいずれかの方法を使用して XML 信頼 を有効にします:

   - **Web Studio** の使用:

     a) Citrix DaaS アカウントにサインインし、［管理］ > ［設定］ > ［**XML** 信頼を有効にする］に移動します。

     b) ［**XML** 信頼を有効にする］トグルをオンにします。

   - **PowerShell** の使用: 次のコマンドを実行して XML 信頼を有効にします:

     ```
     Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
     <!--NeedCopy-->
     ```

6. `TrustRequestsSentToTheXmlServicePort`を有効にした後、App Protection を再度有効にします。

7. 上記の条件が満たされているにもかかわらず、App Protection を有効または無効にできない場合は、Citrix テクニカルサポートにお問い合わせください。

App Protection ポリシーが適切に適用されていない

1. 次の条件が満たされていることを確認してください:

   - Citrix Workspace アプリのサポートされているバージョンを使用します。
   - デリバリーグループの適切な機能が有効になっています。
   - この機能がエンドポイントにインストールされています。
   - Citrix Workspace アプリのインストール時に/`includeappprotection`スイッチを有効にします。

2. 上記の条件が満たされていても App Protection ポリシーが適切に適用されない場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログの収集について詳しくは、「Citrix Workspace アプリのログの収集」を参照してください

Citrix ウィンドウ以外でスクリーンショットが機能していません:

- 保護されている Citrix ウィンドウ（Citrix Workspace アプリを含む）を最小化するか閉じます。

ポリシーの改ざんの検出に関するトラブルシューティング

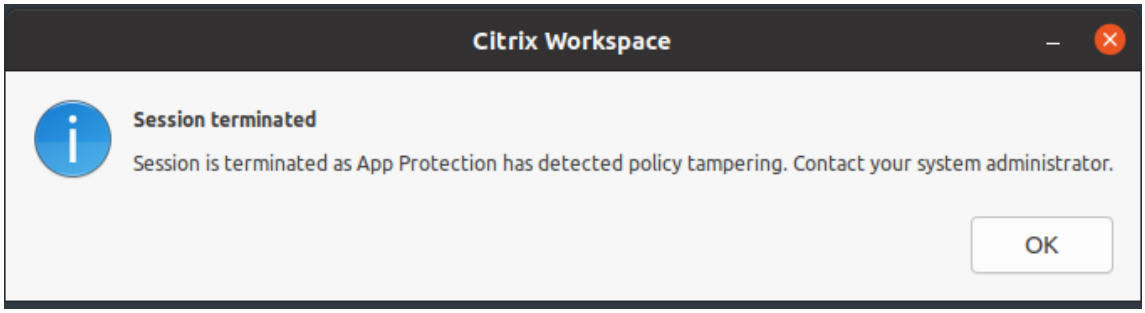
March 10, 2024

次のセクションでは、発生する可能性のあるいくつかの問題とそのトラブルシューティング方法について説明します:

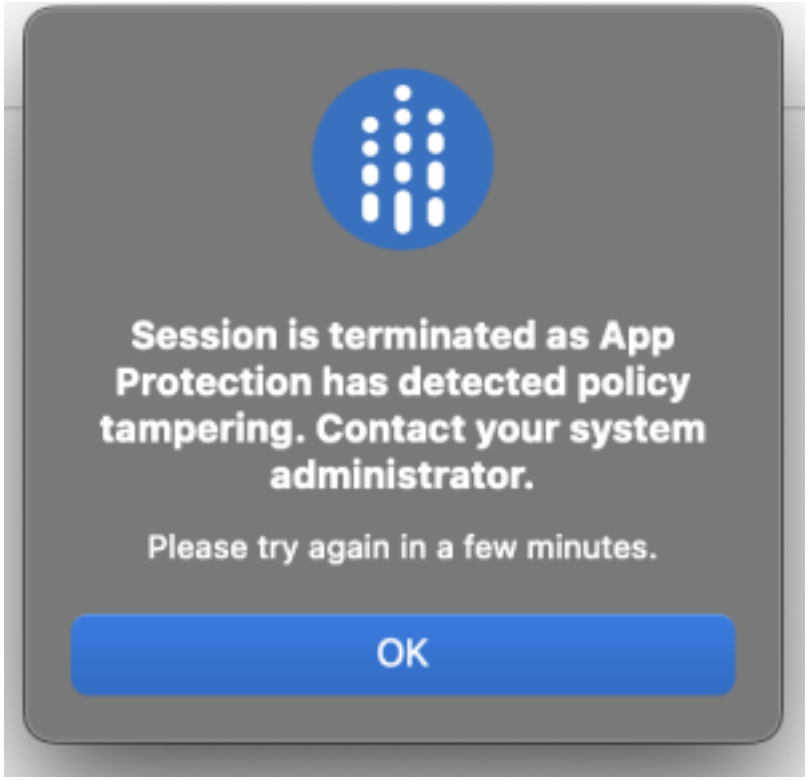
ICA ファイルは改ざんされているがセッションはまだ実行中である

App Protection のポリシーの改ざんの検出機能が有効になっている仮想アプリまたはデスクトップセッションの ICA ファイルが改ざんされた場合、次のいずれかのエラーメッセージを表示してセッションを終了する必要があります:

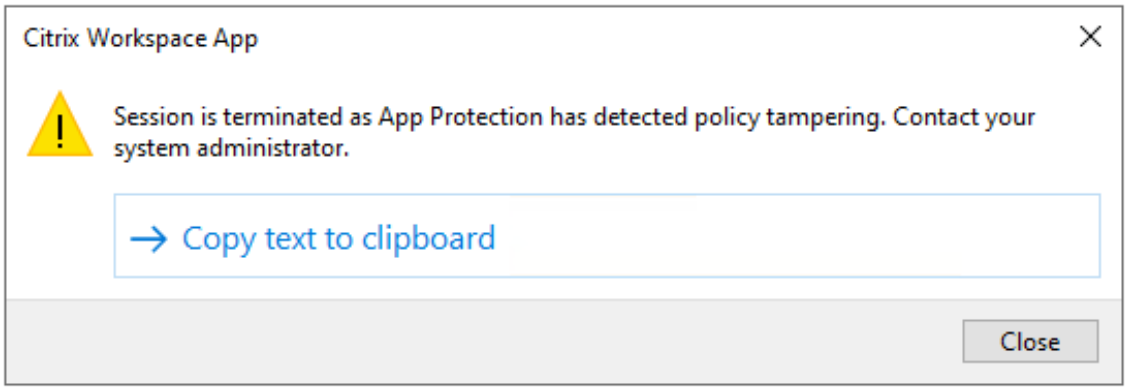
- Linux 向け Citrix Workspace アプリ



- Mac 向け Citrix Workspace アプリ



- Windows 向け Citrix Workspace アプリ



ただし、ICA ファイルが改ざんされていて、ポリシーの改ざんの検出が有効になっている場合でもセッションが実行されている場合は、次の手順を実行します:

1. Virtual Delivery Agent で以下の手順を実行します:

   a) 次のコマンドを実行して、`ctxappprotectionsv`サービスが実行されているかどうかを確認します:

   ```
   sc query ctxappprotectionsvc
   ```

   b) `ctxappprotectionsvc`サービスが実行されていない場合は、以下の手順を実行してサービスを開始します:

i. 以下のコマンドを実行して、`ctxappprotectionsvc`サービスのスタートアップの種類を自動に変更します：

```
sc config ctxappprotectionsvc start=auto
```

ii. 次のコマンドを実行してサービスを起動します：

```
sc start ctxappprotectionsvc
```

2. クライアントで、以下の手順を実行します：

   a) *vdappp.dll* ファイルが Citrix Workspace アプリのインストール場所にあるかどうかを確認します。Citrix Workspace アプリのデフォルトのインストール場所は以下のとおりです：

      - Windows - C:\Program Files (x86)\Citrix\ICA Client
      - Linux - /opt/Citrix/ICAClient
      - Mac - 該当なし

   b) Windows 向け Citrix Workspace アプリの場合は、*procexp.exe* を使用して、*vdappp.dll* ファイルが *wfica32.exe* に読み込まれているかどうかを確認します。

   c) Linux 向け Citrix Workspace アプリの場合は、*vdappp.dll* ファイルが *wfica.exe* に読み込まれているかどうかを確認します。

3. セッションがまだ実行中の場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

Virtual Delivery Agent を再起動すると、ポリシーの改ざんの検出が機能しなくなる

Virtual Delivery Agent を再起動し、ポリシーの改ざんの検出機能が動作しなくなった場合は、再起動後に App Protection サービスが実行されていないことが原因である可能性があります。Virtual Delivery Agent で以下の手順を実行します：

1. 次のコマンドを実行して、`ctxappprotectionsvc`サービスが実行中で、自動に設定されているかどうかを確認します：

```
sc query ctxappprotectionsvc
```

2. `ctxappprotectionsvc`サービスが実行されていない場合は、以下の手順を実行してサービスを開始します：

   a) 以下のコマンドを実行して、`ctxappprotectionsvc`サービスのスタートアップの種類を自動に変更します：

```
sc config ctxappprotectionsvc start=auto
```

   b) 次のコマンドを実行してサービスを起動します：

```
sc start ctxappprotectionsvc
```


3. ポリシーの改ざんの検出セッションがまだ実行中の場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

App Protection のセキュリティ態勢チェックに関するトラブルシューティング

March 10, 2024

次のセクションでは、発生する可能性のあるいくつかの問題とそのトラブルシューティング方法について説明します:

セッションがエラー メッセージなしで終了した

仮想アプリまたはデスクトップのセッションがエラーメッセージを表示せずに突然終了した場合は、以下の手順を実行します:

1. Citrix Workspace アプリのバージョンが次のいずれかのバージョンよりも古いかどうかを確認します:
   - Windows 向け Citrix Workspace アプリ 2309
   - Mac 向け Citrix Workspace アプリ 2308
   - Linux 向け Citrix Workspace アプリ 2308

   > 注:
   >
   > Citrix Workspace アプリのバージョンが手順 1 でリストされたバージョンよりも古く、App Protection のセキュリティ態勢チェック機能が有効になっている場合、仮想アプリまたはデスクトップセッションはエラーメッセージを表示せずに終了します。ただし、Citrix Workspace アプリが手順 1 でリストされたバージョン以降のバージョンで、App Protection のセキュリティ態勢チェック機能が有効になっている場合、仮想アプリまたはデスクトップセッションはエラーメッセージを表示して終了します。

2. App Protection のセキュリティ態勢チェック機能が有効になっているかどうかを確認します。
3. Citrix Workspace アプリが以前のバージョン以降のバージョンで、セキュリティ態勢チェック機能も有効である場合は、ログを収集し、Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

App Protection のセキュリティ態勢チェックが有効になってるが、古いバージョンではセッションが終了していない

通常、App Protection のセキュリティ態勢チェック機能が有効になっており、古いバージョンの Citrix Workspace アプリを介して接続している場合は、セッションを終了する必要があります。

ただし、セッションが終了していない場合は、次の手順を実行します:

1. Virtual Delivery Agent で以下の手順を実行します:

   a) 次のコマンドを実行して、`ctxappprotectionsvc`サービスが実行されているかどうかを確認します:

   ```
   sc query ctxappprotectionsvc
   ```

   b) `ctxappprotectionsvc`サービスが実行されていない場合は、以下の手順を実行してサービスを開始します:

      i. 以下のコマンドを実行して、`ctxappprotectionsvc service`のスタートアップの種類を自動に変更します:

      ```
      sc config ctxappprotectionsvc start=auto
      ```

      ii. 次のコマンドを実行してサービスを起動します:

      ```
      sc start ctxappprotectionsvc
      ```

2. 入力したセキュリティ態勢チェック値に次のいずれかのプレフィックスが付いているかどうかを確認します:

   - Windows 向け Citrix Workspace アプリの場合: `windows-`
   - Linux 向け Citrix Workspace アプリの場合: `linux-`
   - Mac 向け Citrix Workspace アプリの場合: `mac-`

3. セキュリティ態勢チェック値はプラットフォーム固有であるため、対応するプラットフォームに従って正しく追加されているかどうかを確認します。

4. `reg`の場所（`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`）をチェックして、セキュリティ態勢チェックが Virtual Delivery Agent と同期されているかどうかを確認します。

5. 前述の条件がすべて満たされており、古いバージョンの Citrix Workspace アプリでセッションがまだ接続されている場合は、ログを収集して Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

App Protection のセキュリティ態勢チェックが、1 つのプラットフォームで機能しても別のプラットフォームでは機能しない

場合によっては、App Protection のセキュリティ態勢チェック機能が、1 つのプラットフォームでは動作し、別のプラットフォームでは動作しないことがあります。たとえば、App Protection のセキュリティ態勢チェック機能が Windows 向け Citrix Workspace アプリでは動作するものの、Linux 向け Citrix Workspace アプリでは動作しないとします。

このようなシナリオでは、次の手順を実行します:

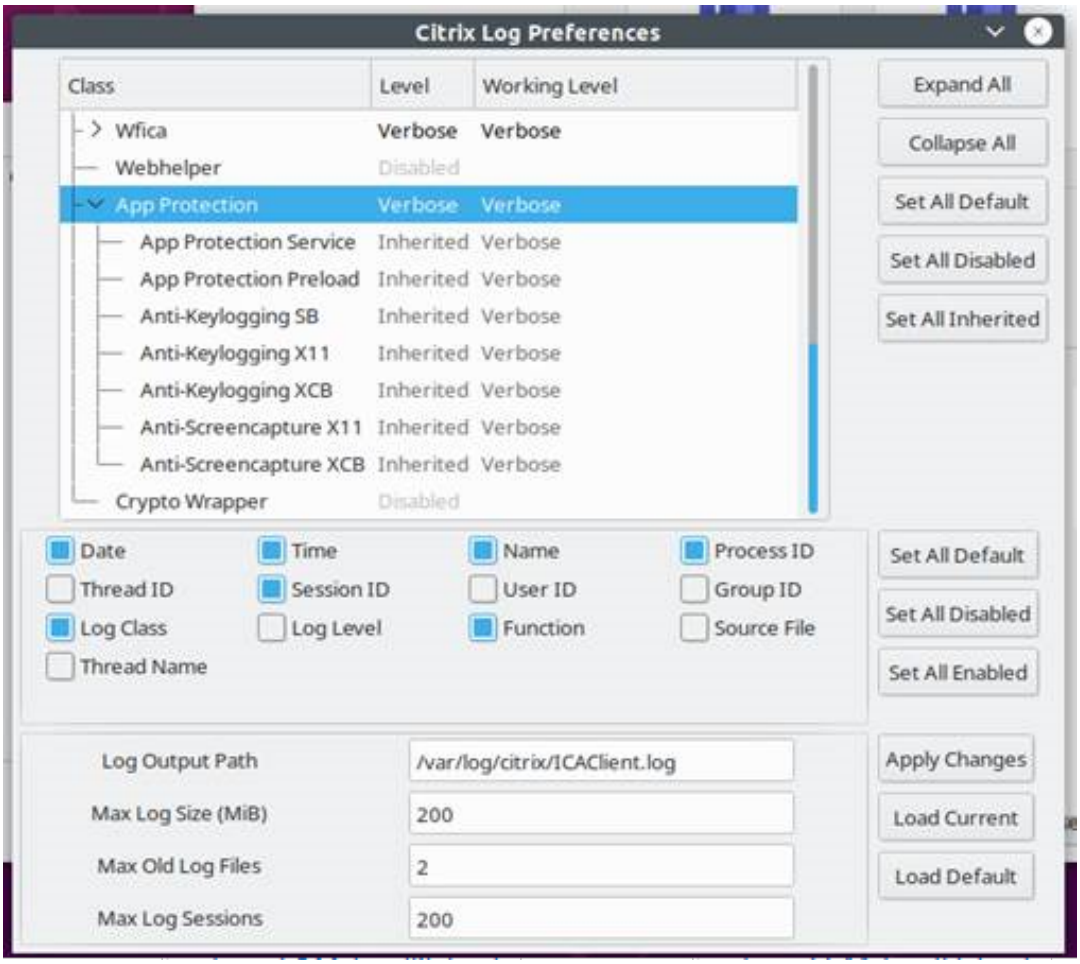
1. 入力したセキュリティ態勢チェック値に次のいずれかのプレフィックスが付いているかどうかを確認します：
   - Windows 向け Citrix Workspace アプリの場合：`windows-`
   - Linux 向け Citrix Workspace アプリの場合：`linux-`
   - Mac 向け Citrix Workspace アプリの場合：`mac-`
2. セキュリティ態勢チェック値はプラットフォーム固有であるため、対応するプラットフォームに従って正しく追加されているかどうかを確認します。
3. `reg`の場所（`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`）をチェックして、セキュリティ態勢チェックが Virtual Delivery Agent と同期されているかどうかを確認します。これらは Studio で設定された内容と一致する必要があります。
4. 前述の条件がすべて満たされており、古いバージョンの Citrix Workspace アプリでセッションがまだ接続されている場合は、ログを収集して Citrix テクニカルサポートにお問い合わせください。ログ収集について詳しくは、「ログ収集」を参照してください。

ログ収集

March 10, 2024

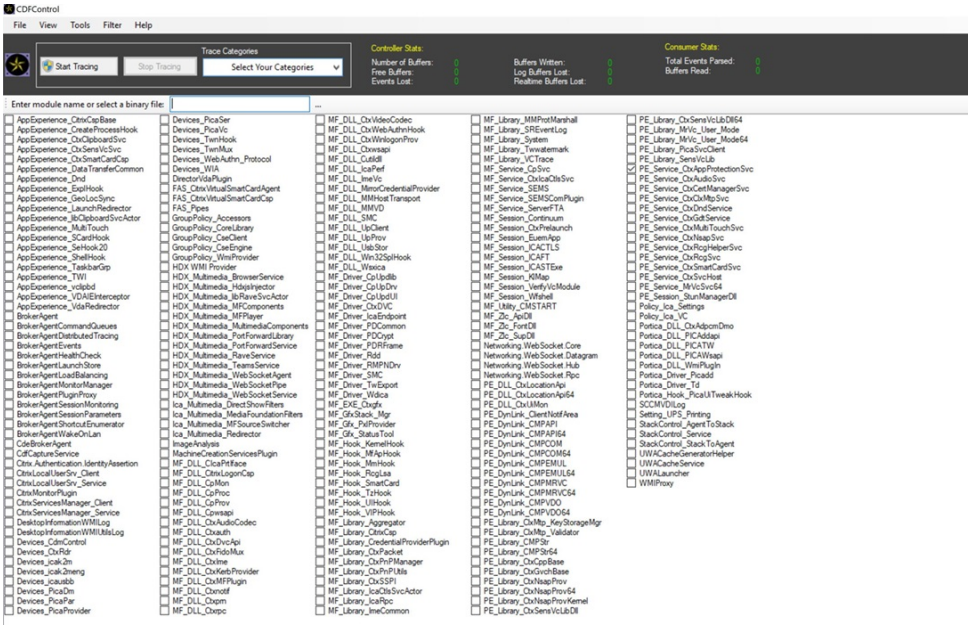
- Windows 向け Citrix Workspace アプリのログを収集するには、「Windows のログ収集」を参照してください。
- Mac 向け Citrix Workspace アプリのログを収集するには、「Mac のログ収集」を参照してください。
- Linux 向け Citrix Workspace アプリのログを収集するには、次の手順を実行します：
  1. インストールの *util* ディレクトリにある setlog 実行可能ファイルを実行します。例：*/opt/Citrix/ICA-Client/util/setlog*。
  2. （オプション）［すべて無効に設定］をクリックして、必要なログのみが収集されるようにします。
  3. App Protection のログ記録に移動します。
  4. 右クリックして ［詳細］を選択し、App Protection のログレベルを［詳細］に設定します（警告とエラーのみがログに記録されます）。
  5. App Protection のクラスを展開し、その子要素を右クリックします。［グループ］>［継承］を選択します。
  6. Linux のログ作成ユーティリティ（*install dir* から *util/setlog* を起動）を使用し、仮想チャネルのログレベルを［詳細］に変更します。
  7. **wfica** のログを有効にします。**wfica** を右クリックし、［詳細］を選択します。App Protection がインストールされていないか、**wfica** で検出できない場合は、次のようなログが取得されます。［**NCS**］**< P3563 > citrix-wfica: App Protection is not installed**。

8. **wfica** をクリックし、**winstation driver** のログレベルを ［詳細］に変更します。
9. セッションを起動すると、setlog のログ出力パスに記載されているファイルにログが記録されます。



- Virtual Delivery Agent でログを収集するには、以下の手順を実行します:

  1. CDF コントロールを通じて App Protection サービスからトレースを取得するには、すべてのモジュールを選択します。



2. 場合によっては、別のマシンからの CDF トレースのキャプチャが必要な場合があります。CDF トレースを収集するには、CTX237216を参照してください。

Workspace のコンテキストに基づく **App Protection**

March 10, 2024

コンテキストに基づく App Protection により、ユーザー、ユーザーのデバイス、ネットワークポスチャなど、ユーザーのサブセットを条件にして、App Protection ポリシーを詳細かつ柔軟に適用できます。

コンテキストに基づく **App Protection** の実装

ブローカーアクセスポリシー規則で定義された接続フィルターを使用して、コンテキストに基づく App Protection を実装できます。ブローカーアクセスポリシーは、デリバリーグループへのユーザーアクセスを制御する規則を定義するものです。ポリシーは一連の規則で構成されます。各規則は 1 つのデリバリーグループに関連付けられ、接続フィルターとアクセス権制御のセットが含まれます。

ユーザーの接続の詳細が、1 つあるいはそれ以上のブローカーアクセスポリシー規則の接続フィルターに一致すると、デリバリーグループにアクセスできるようになります。デフォルトでは、ユーザーはサイト内のどのデリバリーグループにもアクセスできません。要件に応じて、追加のブローカーアクセスポリシーを作成できます。複数の規則を同じデリバリーグループに適用できます。詳細については、「New-BrokerAccessPolicyRule」を参照してください。

ブローカーアクセスポリシー規則の次のパラメーターにより、ユーザーの接続がアクセスポリシー規則で定義された接続フィルターと一致する場合に、コンテキストに基づく柔軟な App Protection が可能になります:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

ブローカーアクセスポリシー規則で参照されているスマートアクセスポリシーを使用して、接続フィルターをさらに調整します。スマートアクセスポリシーを使用してコンテキストに基づく App Protection 設定する方法については、この記事で説明されているシナリオを参照してください。

コンテキストに基づく **App Protection** のシナリオ

以下は、コンテキストに基づく App Protection を有効にする方法に関するシナリオの一部です。

- Access Gateway を経由する外部ユーザーの App Protection を有効にする
- 信頼できないデバイスの App Protection を有効にする
- デバイスのセキュリティ態勢の結果に基づいて App Protection を有効にする
- 特定のユーザーグループに対して App Protection を有効にする

前提条件

March 10, 2024

以下が割り当てられていることを確認してください:

- ネットワークの場所サービス（NLS）（ユーザーのネットワークの場所に基づくシナリオで）
- ライセンスの要件
  - DaaS の App Protection
  - アダプティブ認証の使用権（Smart Access ポリシーを使用するシナリオ）

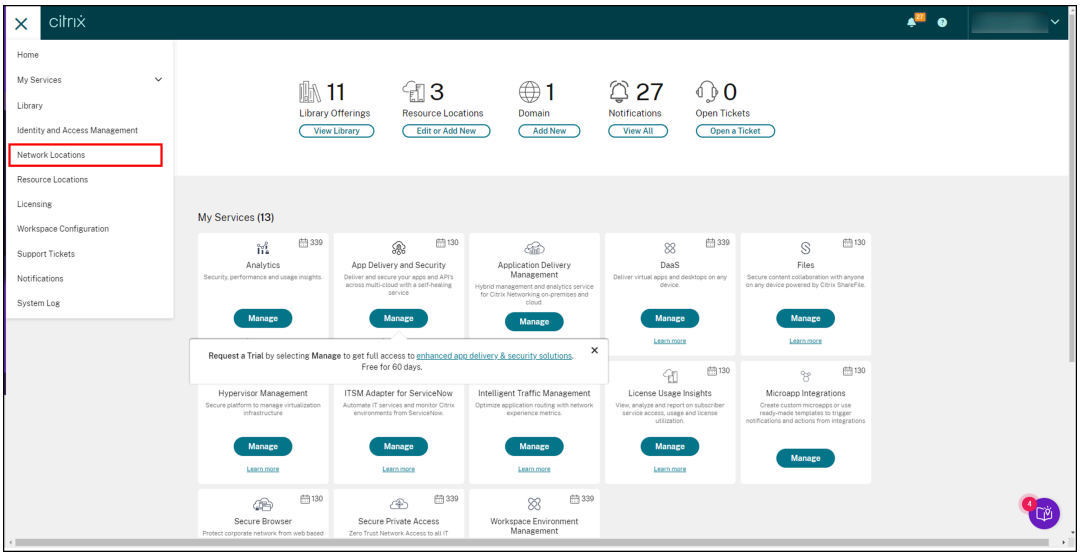
シナリオ **1**

April 10, 2024

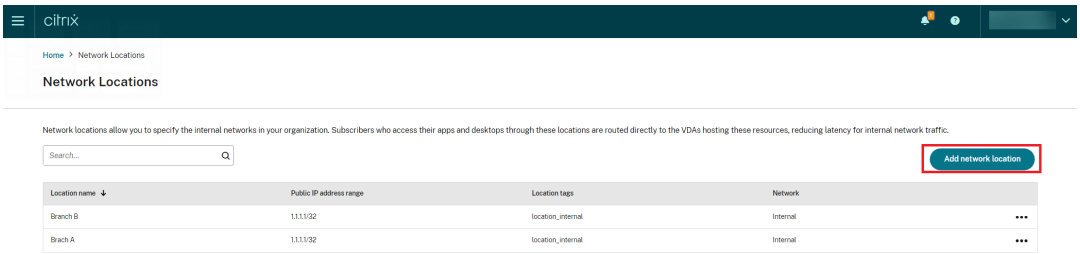
このシナリオでは、**Access Gateway** を経由する外部ユーザーの **App Protection** を有効にする方法について説明します。

1. アダプティブ認証を構成します。
2. ネットワークの場所に基づいてアダプティブアクセスを構成し、

a) Citrix Cloud にサインインして［ネットワークの場所］に移動します。



b) ［ネットワークの場所を追加］をクリックします。



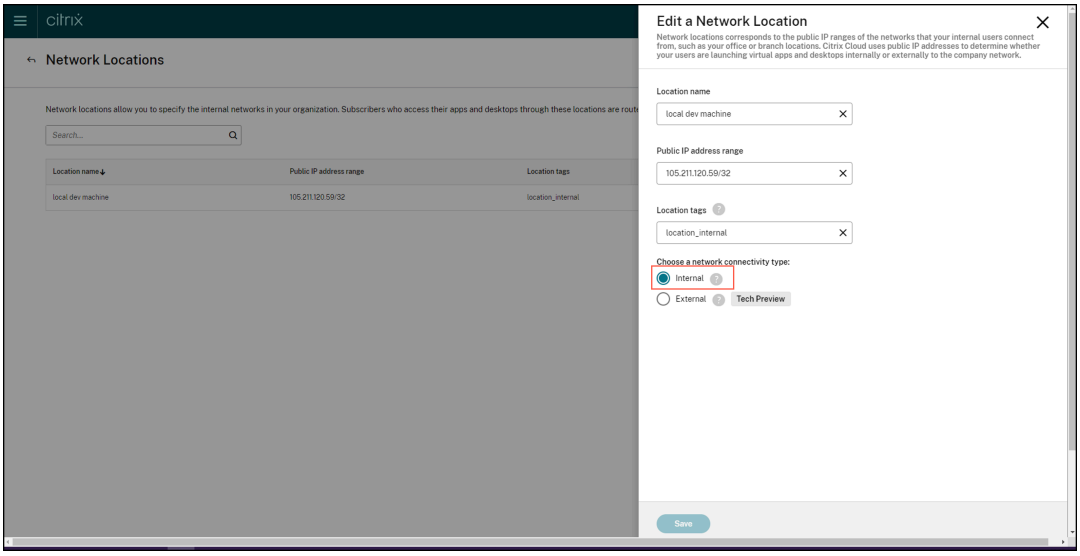
［ネットワークの場所の追加］画面が表示されます。

c) ［場所名］フィールドに、関連する場所の名前を入力します。

d) ［パブリック **IP** アドレス範囲］フィールドに、内部ネットワークとして考慮するネットワーク IP アドレスまたはサブネットを入力します。

e) ［場所のタグ］フィールドに「**location_internal**」と入力します。場所のタグの詳細については、「場所のタグ」を参照してください。

f) ［ネットワーク接続の種類の選択］で、［内部］を選択します。



［ネットワーク接続の種類の選択］設定で IP アドレスが［内部］として構成されているデバイスから Cloud ストアにサインインすると、接続は内部接続と見なされます。

3. ブローカーアクセスポリシー規則の構成

すべてのデリバリーグループに対して、デフォルトで 2 つのブローカーアクセスポリシーが作成されます。1 つのポリシーは Access Gateway 経由の接続用で、もう 1 つのポリシーは直接接続用です。App Protection は、外部接続である Access Gateway 経由の接続に対してのみ有効にできます。次の手順を使用してブローカーアクセスポリシー規則を構成します：

a) Citrix ブログ「Getting started with PowerShell automation for Citrix Cloud」（Citrix Cloud の PowerShell 自動化を開始する）の説明に従って、Citrix PowerShell SDK をインストールし、クラウド API に接続します。

b) コマンド`Get-BrokerAccessPolicyRule`を実行します。

存在するすべてのデリバリーグループのすべてのブローカーアクセスポリシーの一覧が表示されます。

c) 変更するデリバリーグループの「**DesktopGroupUid**」を見つけます。


```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) **DesktopGroupUid** を使用して次のコマンドを実行し、デリバリーグループに適用できるポリシーを取得します。2 つ以上のポリシーがあり、1 つは *ViaAG* の *AllowedConnections*、もう 1 つは *NotViaAG* の AllowedConnections があります。

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```



```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule -DesktopGroupUid 15


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

スクリーンショットで、次の 2 つのポリシーを確認できます:

- App Protection_AG - *ViaAG* の *AllowedConnections*（Access Gateway 経由の接続のポリシー）
- App Protection_Direct - *NotViaAG* の *AllowedConnections*（Access Gateway 経由ではない接続のポリシー）

4. 次のコマンドを使用して、外部接続に対してのみ App Protection ポリシーを有効にし、内部接続を無効にします:

   - `Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ $false`
   - `New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols HDX, RDP`
   - `Remove-BrokerAccessPolicyRule "App Protection_Direct”`

5. 確認:

   Citrix Workspace アプリからサインアウトし、再度サインインします。保護されたリソースを外部接続から起動します。App Protection ポリシーが適用されていることがわかります。最初の手順で構成した IP アドレス範囲内のデバイスである内部接続から同じリソースを起動します。App Protection ポリシーが無効になっていることがわかります。

シナリオ 2

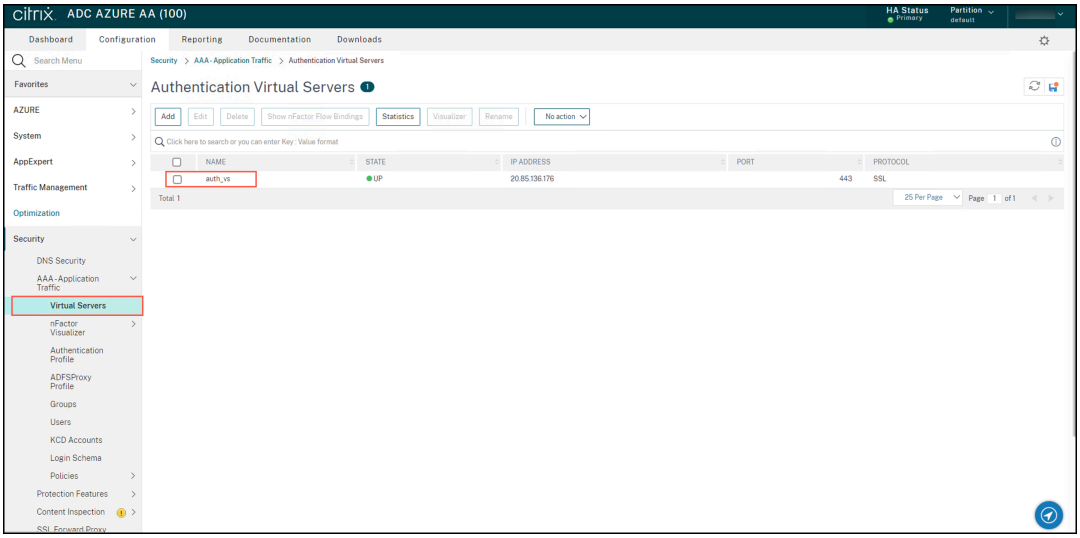
April 10, 2024

このシナリオでは、信頼できないデバイスに対して **App Protection** を有効にする方法について説明します。

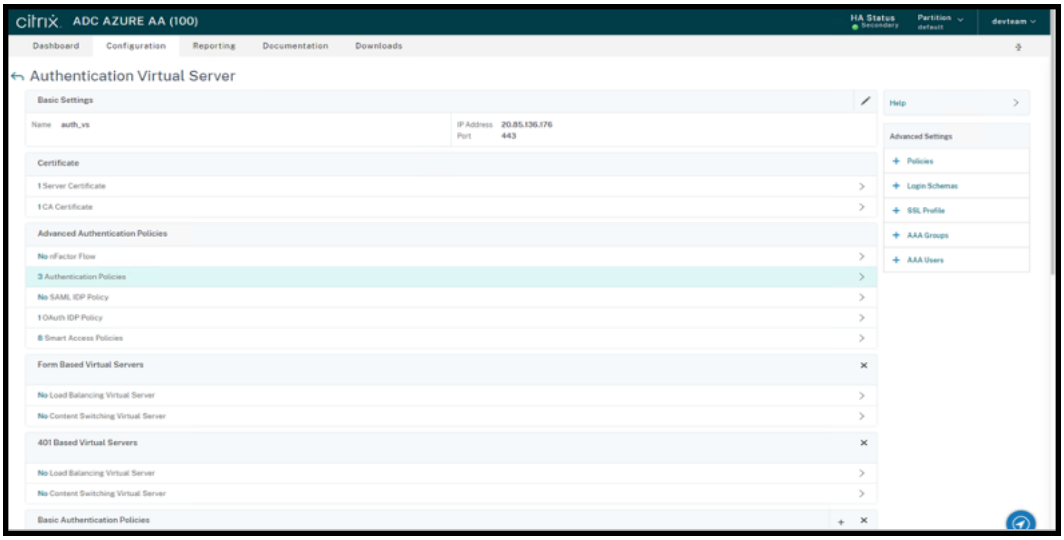
信頼できるデバイスと信頼できないデバイスに対する多くの定義があります。このシナリオでは、エンドポイント分析（EPA）のスキャンが成功した場合の、信頼されているデバイスについて考えてみましょう。他のすべてのデバイスは信頼できないデバイスと見なされます。

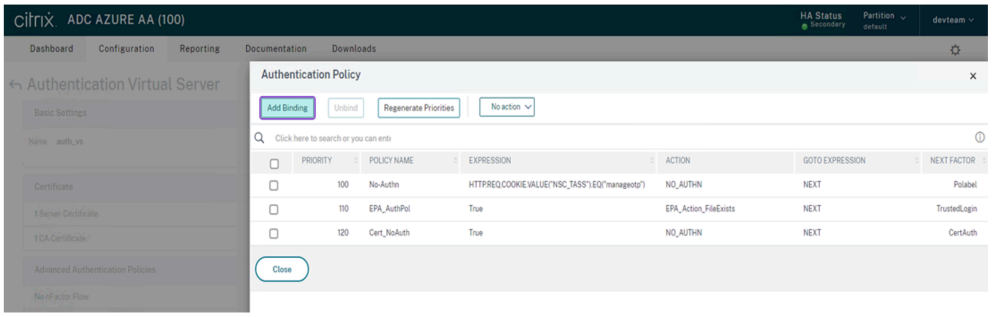
1. アダプティブ認証を構成します。
2. 以下の手順で、EPA スキャンを使用して認証ポリシーを作成します:

   a) Citrix ADC 管理 UI にサインインします。[**Configuration**] タブで、[**Security**] > [**AAA-Application Traffic**] > [**Virtual Servers**] に移動します。使用する仮想サーバー（今回は *auth_vs*）をクリックします。

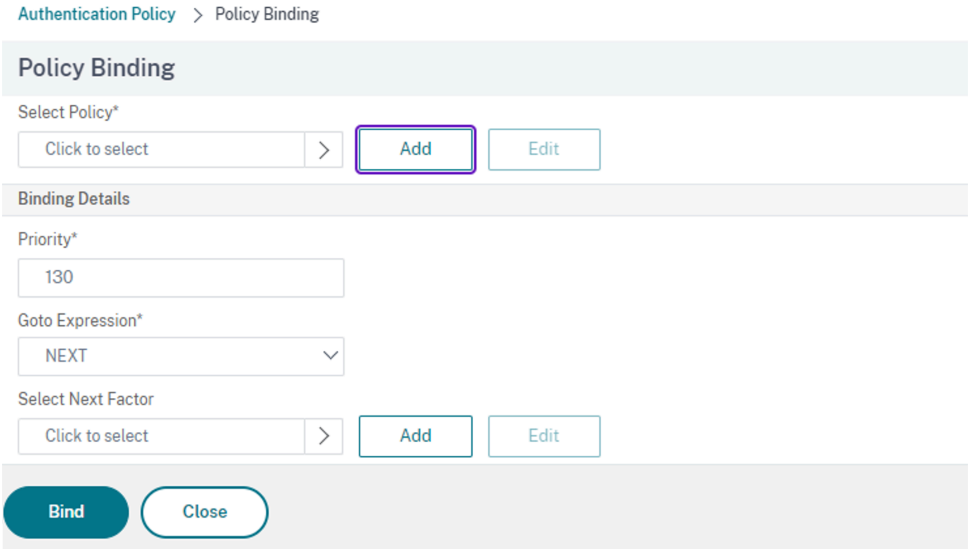


   b) [**Authentication Policies**] > [**Add Binding**] に移動します。

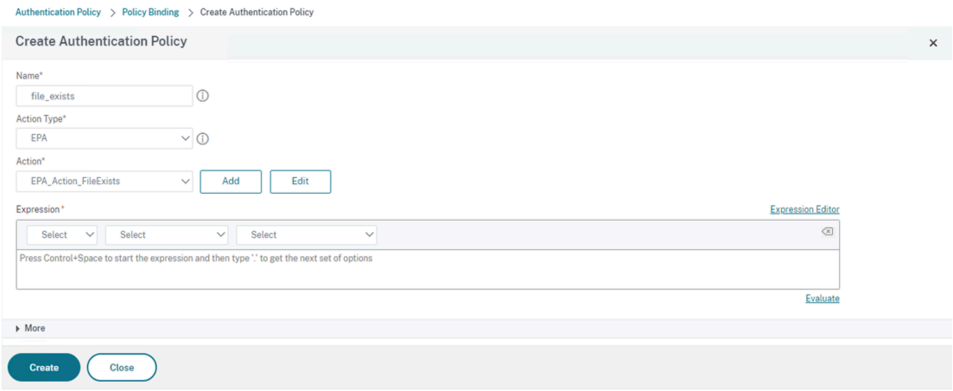




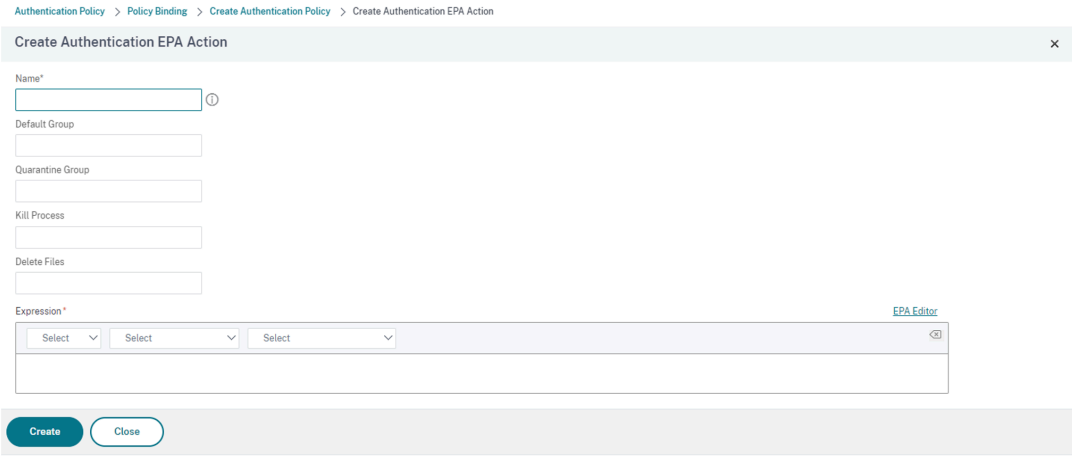
c) ［**Add**］をクリックしてポリシーを作成します。



d) EPA スキャンに基づいて認証ポリシーを作成します。ポリシーの名前を入力します。［**Action Type**］で ［*EPA*］を選択します。［**Add**］をクリックして操作を作成します。



［**Create Authentication EPA Action**］画面が開きます。

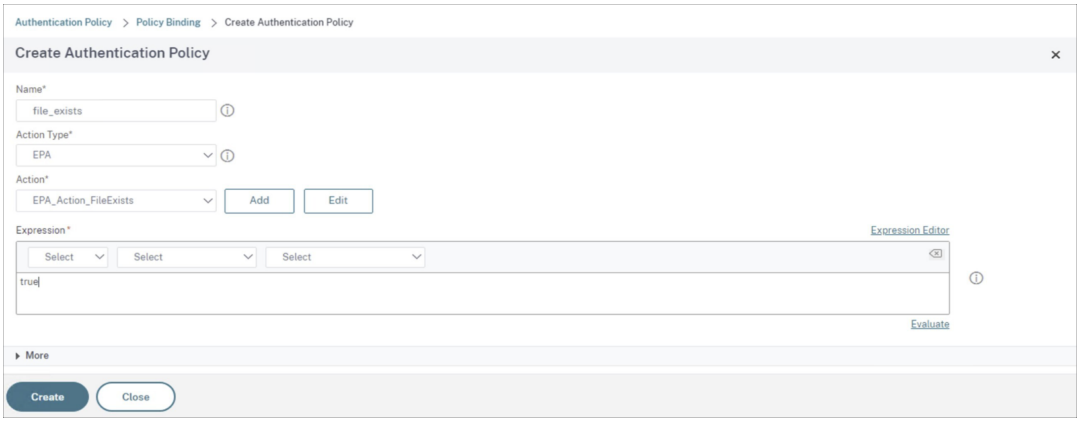


e) ［**Create Authentication EPA Action**］画面で、次の詳細を入力し、［**Create**］をクリックしてアクションを作成します：

- **Name**：EPA アクションの名前。今回は「*EPA_Action_FileExists*」。
- デフォルトグループ：デフォルトのグループ名を入力します。EPA 式が *True* の場合、ユーザーはデフォルトのグループに追加されます。今回の **Default Group** は「*FileExists*」です。
- 検疫グループ：検疫グループ名を入力します。EPA 式が *False* の場合、ユーザーは検疫グループに追加されます。
- 式：スキャンする EPA 式を追加します。次の例は、特定のファイルが存在して EPA スキャンが成功する場合です：`sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")`

［**Create Authentication Policy**］画面に戻ります。

f) ［Expression］エディターに「**true**」を入力し、［**Create**］をクリックします。



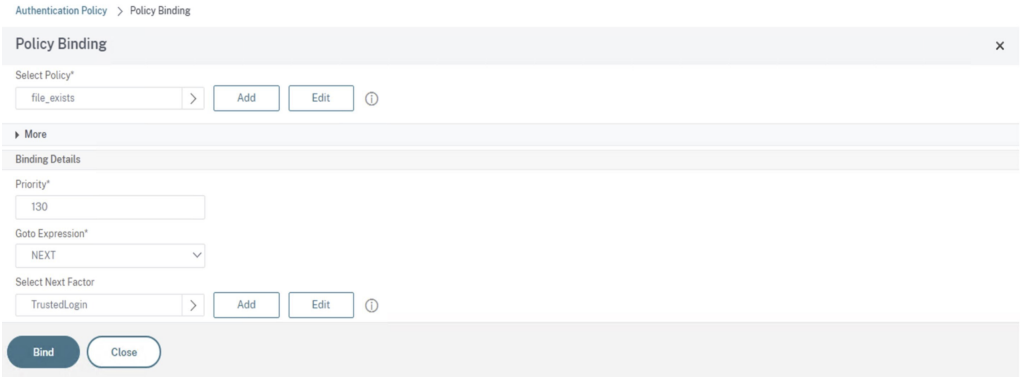
［**Policy Binding**］画面に戻ります。

g) ［**Policy Binding**］画面で、次の操作を実行します。

i. ［**Goto Expression**］で ［**NEXT**］を選択します。

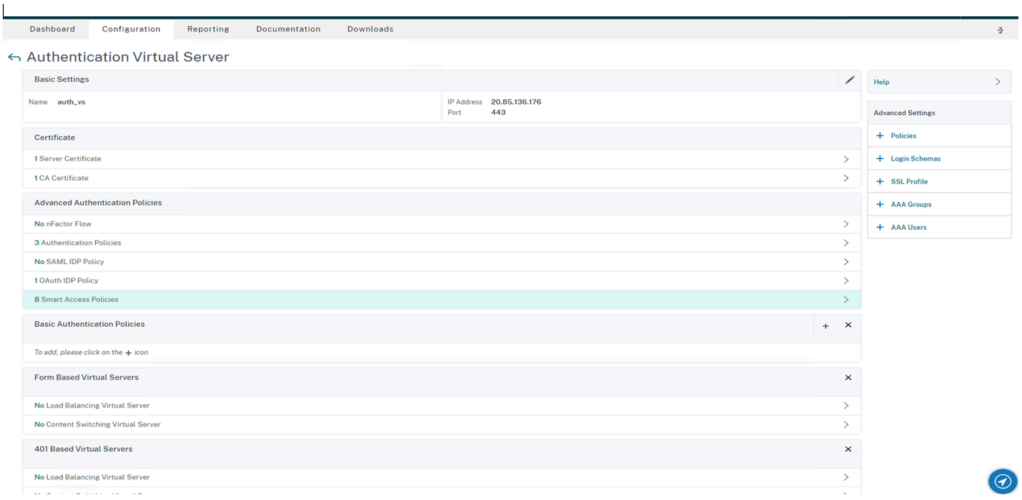
ii. ［**Select Next Factor**］セクションで、アプリケーションデリバリーコントローラー（ADC）の認証用に構成した LDAP ポリシーを選択します。

iii. ［**Bind**］をクリックします。

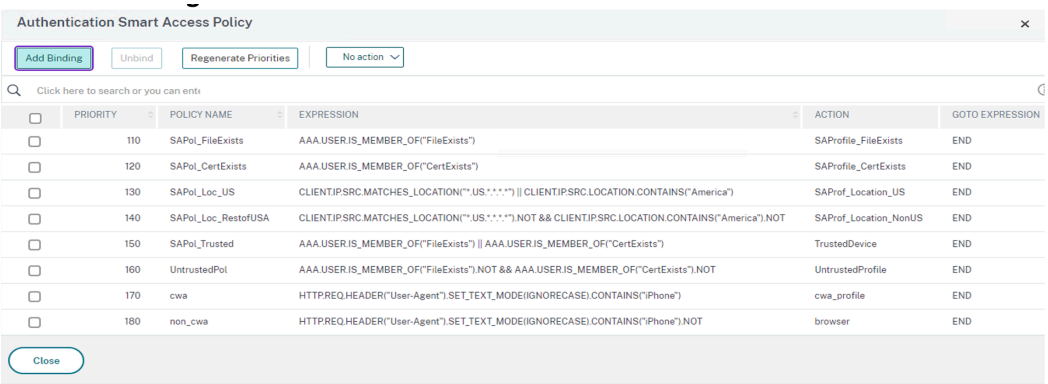


3. 信頼できるデバイスのスマートアクセスポリシーを作成します。

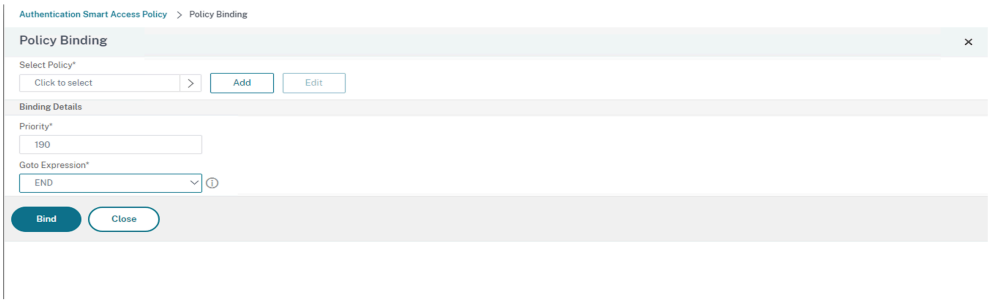
a) *auth_vs* サーバーの ［**Authentication Virtual Server**］ページで ［**Smart Access Policies**］を選択します。



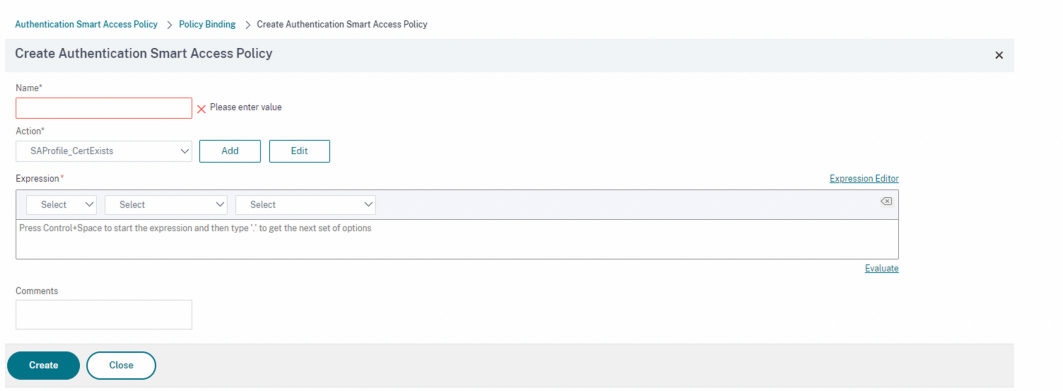
b) ［**Add Binding**］をクリックします。



c) ［**Policy Binding**］画面で、［**Select Policy**］セクションの ［**Add**］をクリックします。



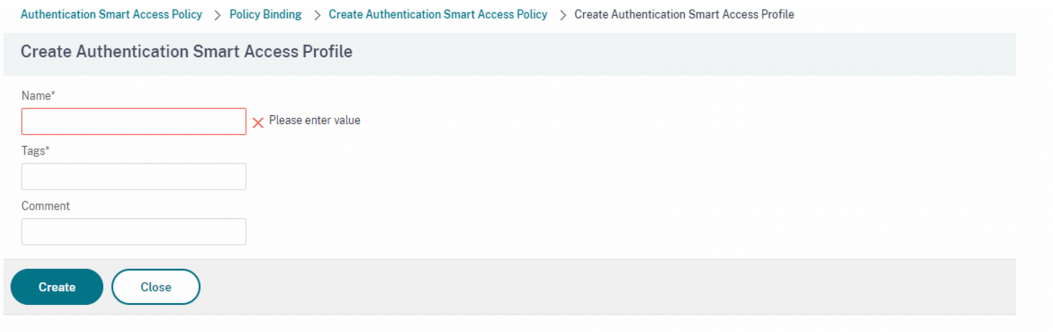
［**Create Authentication Smart Access Policy**］画面が表示されます。



d) ［**Create Authentication Smart Access Policy**］画面で、スマートアクセスポリシーの ［**Name**］を入力し、［**Add**］をクリックしてスマートアクセスプロファイルを作成します。

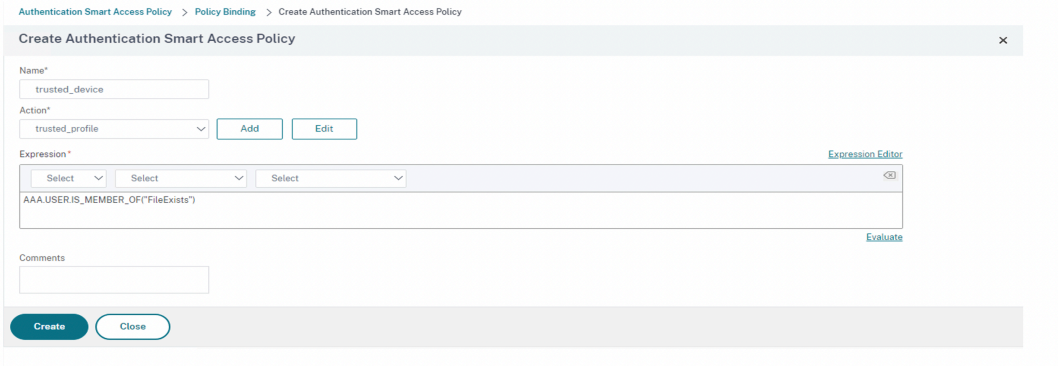
［**Create Authentication Smart Access Profile**］画面が開きます。

e) アクションの ［**Name**］を追加します。［**Tags**］に「*trusted*」と入力します。タグは、後で構成の際に、ブローカーアクセスポリシー規則で参照されます。［**Create**］をクリックします。



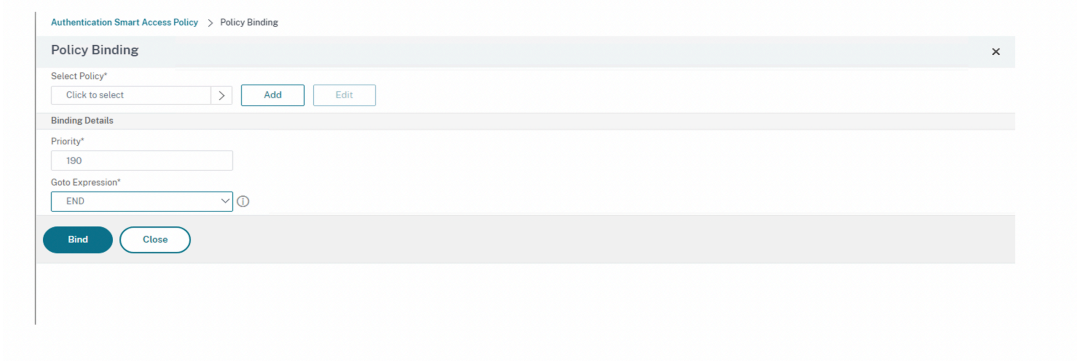
［**Create Authentication Smart Access Policy**］画面に戻ります。

f) ［**Expression**］セクションで、タグをプッシュする式を入力します。今回、タグは信頼できるデバイス用にプッシュするため、「`AAA.USER.IS_MEMBER_OF("FileExists")`」と入力します。［**Create**］をクリックします。



［**Policy Binding**］画面に戻ります。

g) ［*End*］で［**Goto Expression**］を選択し、［**Bind**］をクリックします。



4. 信頼できないデバイスのスマートアクセスポリシーを作成します：

   a) 前の手順で示した指示に従います（サブ手順の **v** と **vi** を除く）。

   b) サブ手順の **v** では、［**Create Authentication Smart Access Profile**］画面で、アクションの［**Name**］を追加します。［**Tags**］に「*untrusted*」と入力します。タグは、後で構成の際に、ブローカーアクセスポリシー規則で参照されます。［**Create**］をクリックします。

   c) サブ手順 **vi** では、［**Create Authentication Smart Access Policy**］画面の［**Expression**］セクションに、タグをプッシュする式を入力します。今回、タグは信頼できないデバイス用にプッシュするため、「`AAA.USER.IS_MEMBER_OF("FileExists").NOT`」と入力します。

5. ブローカーアクセスポリシー規則の構成：

   a) Citrix ブログ「Getting started with PowerShell automation for Citrix Cloud」（Citrix Cloud の PowerShell 自動化を開始する）の説明に従って、Citrix PowerShell SDK をインストールし、クラウド API に接続します。

   b) コマンド`Get-BrokerAccessPolicyRule`を実行します。

      存在するすべてのデリバリーグループのすべてのブローカーアクセスポリシーの一覧が表示されます。

   c) 変更するデリバリーグループの「**DesktopGroupUid**」を見つけます。


```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) 次のコマンドを使用して、特定のデリバリーグループにのみ適用されるポリシーを取得します：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) 信頼できるデバイスを使用してユーザーをフィルタリングするには、コマンドを使用して別のブローカーアクセスポリシーを作成します：

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) 信頼できるデバイスの App Protection を無効にし、信頼されていないデバイスの App Protection を有効にするには、次のコマンドを使用します：

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false
```

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

6. 確認：

Citrix Workspace アプリからサインアウトし、再度サインインします。信頼できるデバイス（EPA スキャン条件を満たすデバイス）から、保護されたリソースを起動します。App Protection ポリシーが適用されていないことがわかります。信頼できないデバイスから、同じリソースを起動します。App Protection ポリシーが適用されていることがわかります。

シナリオ 3

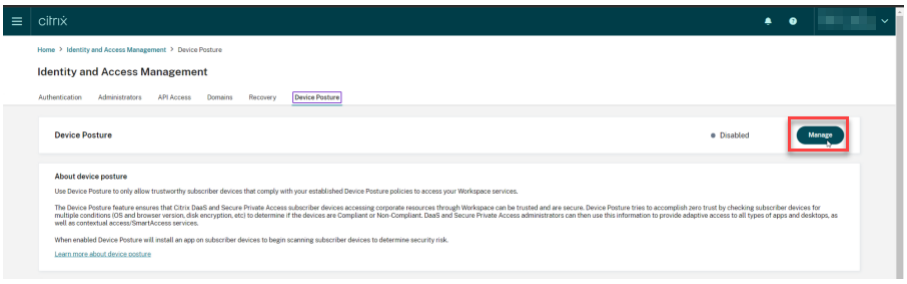
March 10, 2024

このシナリオでは、デバイスのセキュリティ態勢の結果に基づいて **App Protection** を有効にする方法について説明します。

1. デバイスのセキュリティ態勢サービスを構成する：

   a) Citrix Cloud にサインインします。

   b) ［**Identity and Access Management**］>［デバイスのセキュリティ態勢］に移動し、［管理］をクリックします。

   c) ［**Create device policy**］をクリックします。

   ［**Create device policy**］ページが表示されます。

   d) ［**Policy rules**］で、［**Select Rule**］ドロップダウンメニューをクリックし、［*Citrix Workspace app Version*］を選択します。

   e) ［**Select Rule**］ドロップダウンメニューをクリックし、［*Greater or equal to* >=］を選択します。

   f) 条件として設定する Citrix Workspace アプリのバージョンを入力します。この例では、「*23.7.0.19*」です。

   g) ［**Policy result,**］で ［**Compliant**］を選択します。

   h) ［**Name**］フィールドに、ポリシーの名前を入力します。

   i) ［**Priority**］フィールドに、ポリシーの優先度を入力します。

   j) ポリシーを作成したときに有効にするには、［**Enable when created**］チェックボックスを選択します。

k) ［**Create**］をクリックします。

2. ブローカーアクセスポリシー規則の構成：

a) Citrix ブログ「Getting started with PowerShell automation for Citrix Cloud」（Citrix Cloud の PowerShell 自動化を開始する）の説明に従って、Citrix PowerShell SDK をインストールし、クラウド API に接続します。

b) コマンド`Get-BrokerAccessPolicyRule`を実行します。

存在するすべてのデリバリーグループのすべてのブローカーアクセスポリシーの一覧が表示されます。

c) 変更するデリバリーグループの「**DesktopGroupUid**」を見つけます。

```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                       : True
AllowedConnections                 : ViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_AG
Uid                                : 37

AllowRestart                       : True
AllowedConnections                 : NotViaAG
AllowedProtocols                   : {HDX, RDP}
AllowedUsers                       : AnyAuthenticated
AppProtectionKeyLoggingRequired    : False
AppProtectionScreenCaptureRequired : False
Description                        :
DesktopGroupName                   : App Protection
DesktopGroupUid                    : 15
Enabled                            : True
ExcludedClientIPFilterEnabled      : False
ExcludedClientIPs                  : {}
ExcludedClientNameFilterEnabled    : False
ExcludedClientNames                : {}
ExcludedSmartAccessFilterEnabled   : False
ExcludedSmartAccessTags            : {}
ExcludedUserFilterEnabled          : False
ExcludedUsers                      : {}
HdxSslEnabled                      : False
IncludedClientIPFilterEnabled      : False
IncludedClientIPs                  : {}
IncludedClientNameFilterEnabled    : False
IncludedClientNames                : {}
IncludedSmartAccessFilterEnabled   : True
IncludedSmartAccessTags            : {}
IncludedUserFilterEnabled          : True
IncludedUsers                      : {}
MetadataMap                        : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                               : App Protection_Direct
Uid                                : 36
```

d) 次のコマンドを使用して、特定のデリバリーグループにのみ適用されるポリシーを取得します：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) 準拠デバイスに App Protection を適用するには、次のコマンドを実行します。

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) 非準拠デバイスに App Protection を適用するには、次のコマンドを実行します。


```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
 $true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
 Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. 確認:

   Citrix Workspace アプリからサインアウトします。デバイスポリシーに準拠する Citrix Workspace アプリのバージョンからサインインします。App Protection ポリシーが適用されていないことがわかります。再度、Citrox Workspace アプリからサインアウトし、デバイスポリシーに準拠していないバージョンの Citrix Workspace アプリからサインインします。App Protection ポリシーが適用されていることがわかります。

シナリオ **4**

March 10, 2024

このシナリオでは、特定のユーザーグループに対して **App Protection** を有効にする方法について説明します。

次の手順により、特定のグループのユーザーに対して App Protection を有効にすることができます:

1. ユーザーに対して App Protection ポリシーを有効にする Active Directory ユーザーグループを選択します。この例では、Active Directory ユーザーグループは「**ProductManagers**」です。
2. ブローカーアクセスポリシー規則の構成:

   a) Citrix ブログ「Getting started with PowerShell automation for Citrix Cloud」(Citrix Cloud の PowerShell 自動化を開始する) の説明に従って、Citrix PowerShell SDK をインストールし、クラウド API に接続します。

   b) コマンド`Get-BrokerAccessPolicyRule`を実行します。

      存在するすべてのデリバリーグループのすべてのブローカーアクセスポリシーの一覧が表示されます。

   c) 変更するデリバリーグループの「**DesktopGroupUid**」を見つけます。


```
PS C:\Windows\System32> Get-BrokerAccessPolicyRule


AllowRestart                      : True
AllowedConnections                : ViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_AG
Uid                               : 37

AllowRestart                      : True
AllowedConnections                : NotViaAG
AllowedProtocols                  : {HDX, RDP}
AllowedUsers                      : AnyAuthenticated
AppProtectionKeyLoggingRequired   : False
AppProtectionScreenCaptureRequired : False
Description                       :
DesktopGroupName                  : App Protection
DesktopGroupUid                   : 15
Enabled                           : True
ExcludedClientIPFilterEnabled     : False
ExcludedClientIPs                 : {}
ExcludedClientNameFilterEnabled   : False
ExcludedClientNames               : {}
ExcludedSmartAccessFilterEnabled  : False
ExcludedSmartAccessTags           : {}
ExcludedUserFilterEnabled         : False
ExcludedUsers                     : {}
HdxSslEnabled                     : False
IncludedClientIPFilterEnabled     : False
IncludedClientIPs                 : {}
IncludedClientNameFilterEnabled   : False
IncludedClientNames               : {}
IncludedSmartAccessFilterEnabled  : True
IncludedSmartAccessTags           : {}
IncludedUserFilterEnabled         : True
IncludedUsers                     : {}
MetadataMap                       : {[IfBuiltInAccessPolicyRuleOfDeliveryGroup, True], [IfCreatedByOrchAccessPolicyRuleOfDeliveryGroup, True]}
Name                              : App Protection_Direct
Uid                               : 36
```

d) 次のコマンドを使用して、特定のデリバリーグループにのみ適用されるポリシーを取得します：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) **ProductManagers** ユーザーグループ内のユーザーに対して App Protection ポリシーを有効にするには、次のコマンドを実行します：

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) **ProductManagers** ユーザーグループに属していないユーザーの App Protection ポリシーを無効にするには、次のコマンドを実行します：

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. 確認：

Citrix Workspace アプリが開いている場合は、サインアウトします。**ProductManagers** の Active Directory ユーザーグループのユーザーとして Citrix Workspace アプリにサインインします。保護されたリ

ソースを起動すると、App Protection が無効になっていることがわかります。Citrix Workspace アプリからサインアウトし、**ProductManagers** の Active Directory ユーザーグループに属していないユーザーとして再度サインインします。保護されたリソースを起動すると、App Protection が有効になっていることがわかります。

StoreFront のコンテキストに基づく **App Protection**

March 10, 2024

コンテキストに基づく App Protection により、ユーザー、ユーザーのデバイス、ネットワークポスチャなど、ユーザーのサブセットを条件にして、App Protection ポリシーを詳細かつ柔軟に適用できます。

コンテキストに基づく **App Protection** の実装

ブローカーアクセスポリシー規則で定義された接続フィルターを使用して、コンテキストに基づく App Protection を実装できます。ブローカーアクセスポリシーは、デリバリーグループへのユーザーアクセスを制御する規則を定義するものです。ポリシーは一連の規則で構成されます。各規則は 1 つのデリバリーグループに関連付けられ、接続フィルターとアクセス権制御のセットが含まれます。

ユーザーの接続の詳細が、1 つあるいはそれ以上のブローカーアクセスポリシー規則の接続フィルターに一致すると、デリバリーグループにアクセスできるようになります。デフォルトでは、ユーザーはサイト内のどのデスクトップグループにもアクセスできません。要件に応じて、追加のブローカーアクセスポリシーを作成できます。複数の規則を同じデリバリーグループに適用できます。詳細については、「New-BrokerAccessPolicyRule」を参照してください。

ブローカーアクセスポリシー規則の次のパラメーターにより、ユーザーの接続がアクセスポリシー規則で定義された接続フィルターと一致する場合に、コンテキストに基づく柔軟な App Protection が可能になります:

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

ブローカーアクセスポリシーで参照されているスマートアクセスフィルターを使用して、接続フィルターを調整します。スマートアクセスフィルターの構成については、こちらのCTX227055を参照してください。スマートアクセスポリシーを使用してコンテキストに基づく App Protection を設定する方法は、以下のシナリオを参照してください。

> 注:
>
> デリバリーグループで App Protection が有効になっている場合、デフォルトではコンテキストに基づく App Protection を適用できません。次のコマンドを使用して、デリバリーグループの App Protection を無効にします。


```
Set-BrokerDesktopGroup -Name "Admin Desktop" -
    AppProtectionKeyLoggingRequired $false -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

前提条件

StoreFront のコンテキストに基づく App Protection を有効にするには、「前提条件」セクションに記載されている要件を満たしていることを確認してください。

コンテキストに基づく **App Protection** を有効にする

1. Citrix ダウンロードページから、お使いの Citrix Virtual Apps and Desktops バージョンの「コンテキストに基づく App Protection ポリシー」（機能テーブル）をダウンロードします。
2. Delivery Controller で、次の PowerShell コマンドを実行します：

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. 次のコマンドを実行して、Delivery Controller でコンテキストに基づく App Protection を有効にします：

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   例：

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
       AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```

コンテキストに基づく **App Protection** のシナリオ

以下は、コンテキストに基づく App Protection を有効または無効にする方法に関するシナリオの一部です。

- 特定のデバイスタイプの App Protection を無効にする
- Web ブラウザーからのアクセスで開始した接続の App Protection を無効にし、Citrix Workspace アプリからの接続の App Protection を有効にする
- 特定の Active Directory グループ内のユーザーに対して App Protection を無効にする
- EPA スキャン結果に基づいてデバイスの App Protection を有効にする
- 特定のユーザーグループに対して App Protection を有効にする

前提条件

March 10, 2024

以下が割り当てられていることを確認してください:

- Citrix Virtual Apps and Desktops バージョン 2109 以降
- Delivery Controller バージョン 2109 以降
- StoreFront バージョン 1912 LTSR 以降
- VPN 仮想サーバーまたはゲートウェイと認証仮想サーバーの構成
- NetScaler と StoreFront 間の正常な接続。詳しくは、「NetScaler Gateway と StoreFront の統合」を参照してください
- Citrix Virtual Apps and Desktops バージョン 2006 までは XML テーブルのインポートが必要です
- Citrix Virtual Apps and Desktops バージョン 2209 まではコンテキストに基づく App Protection 機能テーブルのインポートが必要です
- スマートアクセスタグが必要なシナリオでは、NetScaler Gateway でスマートアクセスを有効にします。詳しくは、こちらのサポート記事を参照してください。
- ライセンスの要件
  - App Protection オンプレミスライセンス
  - スマートアクセスタグを使用するシナリオ向けの Citrix Gateway ユニバーサルライセンス

シナリオ 1

March 10, 2024

このシナリオでは、特定のデバイスの種類に対して **App Protection** を無効にする方法について説明します。

以下は、「`Win10Desktop`」というデリバリーグループで iPhone ユーザーの App Protection を無効にする手順です:

1. Smart Access ポリシーを作成します:

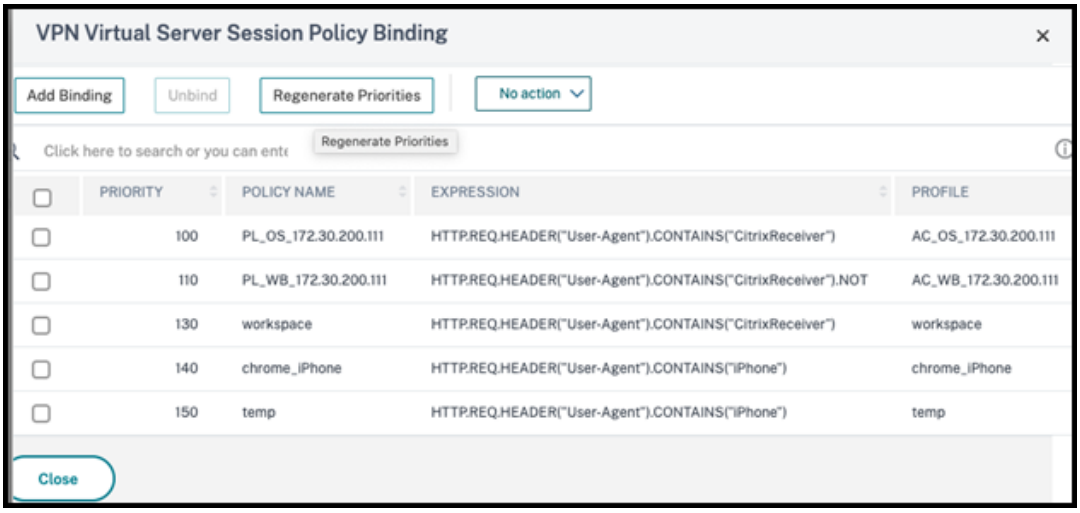
   a) Citrix ADC 管理 UI にサインインします。

   b) 左側のナビゲーションメニューで、[**Citrix Gateway**] > [**Virtual Servers**] に移動します。

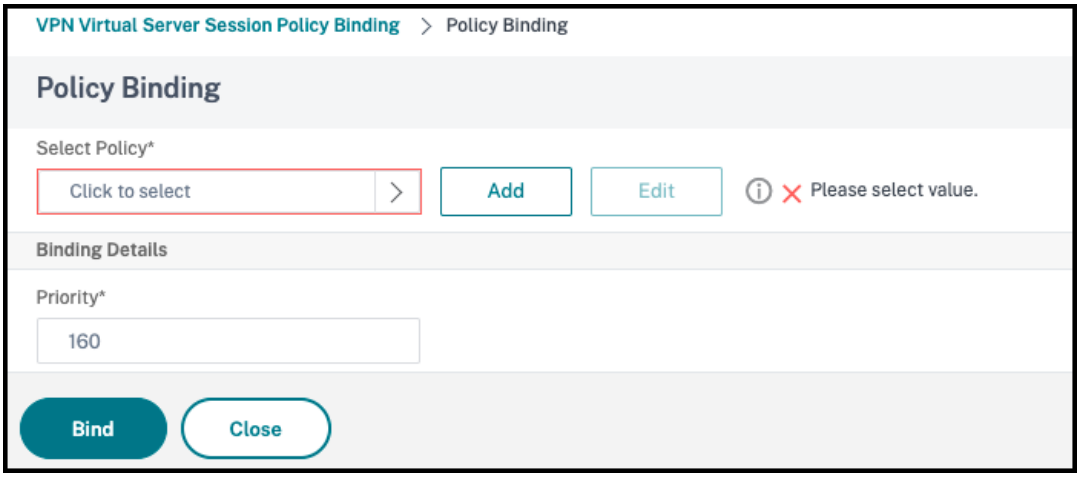
   後でブローカーアクセスポリシーを構成するために必要になるため、VPN 仮想サーバー名を書き留めておきます。

   c) [**VPN Virtual Server**] をクリックします。ページの一番下までスクロールし、[**Session policies**] をクリックします。セッションポリシーの一覧が表示されます。

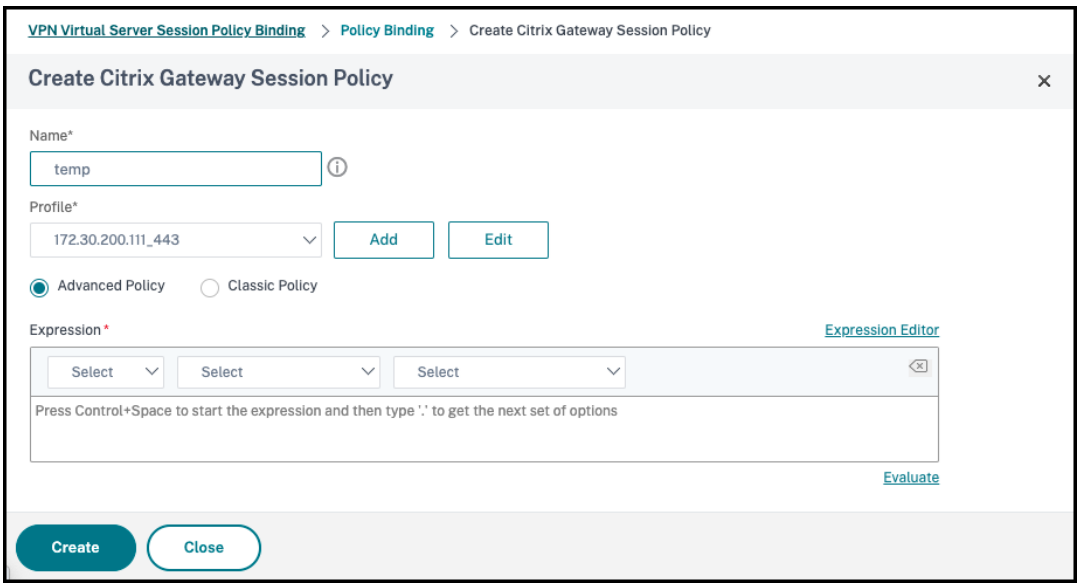
d) ［**Add Binding**］をクリックします。



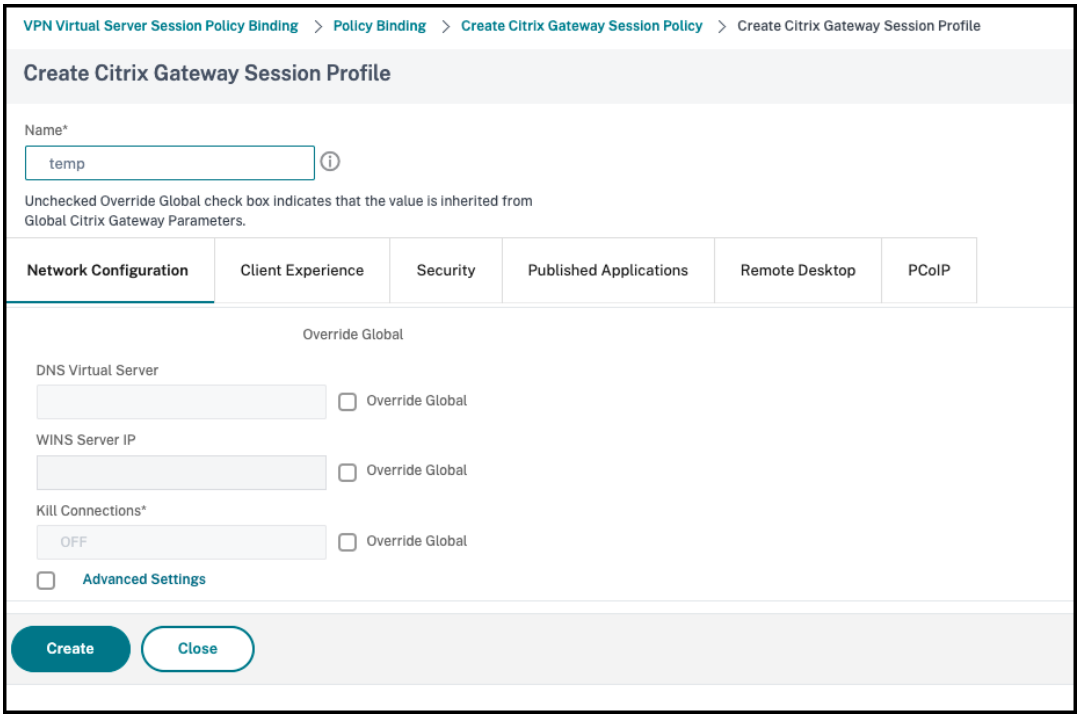
e) ［**Add to create a session policy**］をクリックします。



f) セッションポリシーの名前を入力します。このシナリオでは *temp* です。



g) ［Profile］の横にある ［**Add**］をクリックして、プロファイル名を指定します。［**Create**］をクリックします。



h) ［Session policy］ウィンドウから ［**Expression Editor**］をクリックします。

i) ユーザーエージェント文字列で「*iPhone*」を確認するには、次の式を作成します：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
<!--NeedCopy-->
```


j) [**Bind**] をクリックして、セッションポリシーを作成します。

2. ブローカーアクセスポリシー規則を作成する:

   Access Gateway 経由で`Win10Desktop`にアクセスする iPhone ユーザーにポリシーを適用するには、次の手順を実行します:

   a) Delivery Controller (DDC) で、以下のコマンドを実行します:

```
Get-BrokerAccessPolicyRule
<!--NeedCopy-->
```

   これには、DDC で定義されているすべてのブローカーアクセスポリシーがリストされています。このシナリオでは、「`Win10Desktop`」というデリバリーグループのブローカーアクセスポリシーは、「`Win10Desktop_AG`」と「`Win10Desktop_Direct`」です。次の手順のために、デリバリーグループのデスクトップグループ UID を書き留めておきます。

   b) `Win10Desktop`用のブローカーアクセスポリシー規則を作成し、コマンドを使用して Access Gateway を経由してくる iPhone ユーザーをフィルター処理します:

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -
    AppProtectionKeyLoggingRequired $false -
    AppProtectionScreenCaptureRequired $false -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

   Uid_of_desktopGroup は、手順 1 で GetBrokerAccessPolicy 規則を実行して取得したデリバリーグループの DesktopGroupUID です。

   c) Access Gateway を経由してくる iPhone ユーザーの`Win10Desktop`の App Protection を無効にするには、手順 1 で作成したスマートアクセスタグ「*temp*」を参照します。次のコマンドを使用してスマートアクセスポリシーを作成します:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
    IncludedSmartAccessTags Primary_HDX_Proxy:temp -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
```



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

Primary_HDX_Proxy は、先ほどの「手順 1、スマートアクセスポリシーを作成する」で出てきた VPN 仮想サーバー名です。

d) 残りの`Win10desktop`ユーザーに対して App Protection ポリシーを有効にするには、次のコマンドを使用します:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

3. 確認

iPhone の場合: Citrix Workspace アプリが iPhone ですでに開いている場合はサインアウトします。Access Gateway 経由で外部から Citrix Workspace アプリにサインインします。StoreFront に必要なリソースが表示され、App Protection が無効になっているはずです。

iPhone 以外のデバイスの場合: Citrix Workspace アプリがデバイスですでに開いている場合はサインアウトします。Access Gateway 経由で外部から Citrix Workspace アプリにサインインします。StoreFront に必要なリソースが表示され、App Protection が無効になっているはずです。

シナリオ 2

March 10, 2024

このシナリオは、ブラウザーベースのアクセスで開始した接続の **App Protection** を無効にし、**Citrix Workspace** アプリで開始した接続の **App Protection** を有効にする方法について説明します。

次の手順では、「`Win10Desktop`」というデリバリーグループで、Web ブラウザーからアクセスして接続が開始されたときに App Protection を無効にし、Citrix Workspace アプリからの接続に対して App Protection を有効にします:

1. スマートアクセスポリシーを作成する:

a) 前述のシナリオ「特定のデバイスタイプの **App Protection** を無効にする」で定義されているように、Citrix Workspace アプリから開始された接続をフィルター処理するスマートアクセスポリシーを作成します。ユーザーエージェント文字列で「**CitrixReceiver**」を確認するには、次の式を作成します:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
<!--NeedCopy-->
```

このシナリオでは、スマートアクセスポリシーは「`cwa`」です。

b) 別のスマートアクセスポリシーを作成して、Citrix Workspace アプリから開始されていない接続をフィルター処理します。`HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`。ここでは、このスマートアクセスポリシーは「*browser*」です。

2. ブローカーアクセスポリシー規則を作成する:

a) `GetBrokerAccessPolicyRule`を実行して、`Win10Desktop`の 2 つのブローカーアクセスポリシーを表示します。デリバリーグループ「`Win10Desktop`」の場合、ブローカーアクセスポリシーは、「`Win10Desktop_AG`」と「`Win10Desktop_Direct`」です。`Win10Desktop`のデスクトップグループ UID を書き留めておいてください。

b) `Win10Desktop`向けのブローカーアクセスポリシーを作成し、次のコマンドを使用して Citrix Workspace アプリから開始された接続をフィルタリングします:

```
1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
     DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
     ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
     AnyAuthenticated -AllowRestart $true -Enabled $true -
     IncludedSmartAccessFilterEnabled $true
2 <!--NeedCopy-->
```

Uid_of_desktopGroup は、手順 1 で GetBrokerAccessPolicy 規則を実行して取得したデリバリーグループの DesktopGroupUID です。

c) 次のコマンドを使用して、スマートアクセスタグ「`cwa`」を参照して CWA を経由してくる接続に対してのみ App Protection ポリシーを有効にします:

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
     IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
     AppProtectionScreenCaptureRequired $true -
     AppProtectionKeyLoggingRequired $true
2 <!--NeedCopy-->
```


Primary_HDX_Proxy は、先ほどの「手順 1、スマートアクセスポリシーを作成する」で書き留めておいた VPN 仮想サーバー名です。

d) 次のコマンドを使用して、Web ブラウザーを経由してくる残りの接続に対して App Protection ポリシーを無効にします:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    IncludedSmartAccessTags Primary_HDX_Proxy:browser -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

3. 確認

Citrix Workspace アプリが開いている場合は、サインアウトします。Citrix Workspace アプリに再度サインインし、Access Gateway 経由の外部接続から必要なリソースを起動します。リソースに対して App Protection ポリシーが有効になっていることがわかります。Web ブラウザーから同じリソースを外部接続で起動すると、App Protection ポリシーが無効になっていることがわかります。

シナリオ 3

March 10, 2024

このシナリオでは、特定の **Active Directory** グループ内のユーザーに対して **App Protection** を無効にする方法について説明します。

次の手順では、Active Directory グループ **xd.local\sales** の一部である`Win10Desktop`ユーザーの App Protection を無効にします:

1. `Get-BrokerAccessPolicyRule`を実行して、`Win10Desktop`の 2 つのブローカーアクセスポリシーを表示します。デリバリーグループ「`Win10Desktop`」の場合、ブローカーアクセスポリシーは、「`Win10Desktop_AG`」と「`Win10Desktop_Direct`」です。`Win10Desktop`のデスクトップグループ UID を書き留めておいてください。

2. `Win10Desktop`のブローカーアクセスポリシー規則を作成して、「`xd.local\sales`」という Active Directory グループに属するユーザーからの接続をフィルター処理します。

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
     -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
    AllowRestart $true -Enabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup は、手順 1 で GetBrokerAccessPolicy 規則を実行して取得したデリバリーグループの DesktopGroupUID です。

3. 次のコマンドを使用して、「**xd.local\sales**」という AD グループに属する Windows 10 デスクトップユーザーに対する App Protection ポリシーを無効にします:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
    AllowedUsers Filtered -IncludedUsers xd.local\sales -
    IncludedUserFilterEnabled $true -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

4. 次のコマンドを使用して、「**xd.local\sale**」のユーザーを除く残りのゲートウェイ接続に対して App Protection ポリシーを有効にします:

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

5. 確認

   Citrix Workspace アプリがすでに開いている場合は、サインアウトします。「**xd.local\sales**」という Active Directory グループのユーザーとして Citrix Workspace アプリにサインインします。保護されたリソースを起動すると、App Protection が無効になっていることがわかります。

   Citrix Workspace アプリからサインアウトし、「**xd.local\sales**」に属さないユーザーとして再度サインインします。保護されたリソースを起動すると、App Protection が有効になっていることがわかります。

シナリオ 4

March 10, 2024

このシナリオでは、**EPA** スキャン結果に基づいてデバイスの **App Protection** を有効にする方法について説明します。

次の手順では、EPA スキャンにパスしたデバイスに対して App Protection を有効にします。

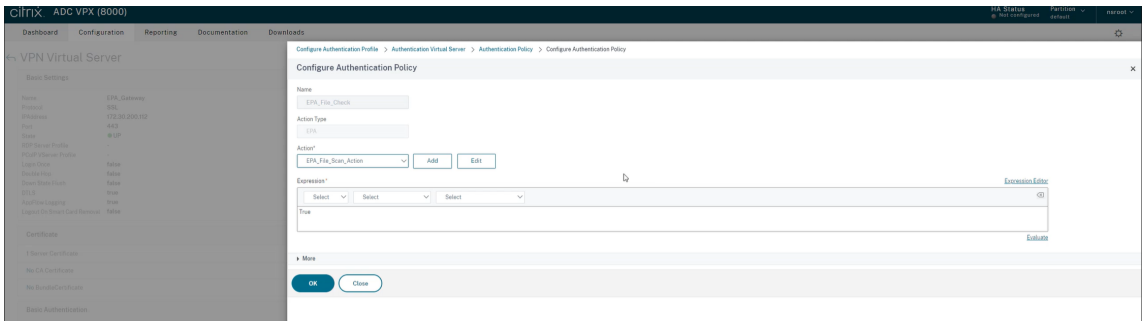
前提条件:

以下が割り当てられていることを確認してください:

- 認証、承認、および監査ユーザーグループ (デフォルトおよび検疫されたユーザーグループの場合) および関連ポリシー
- LDAP サーバー構成と関連ポリシー

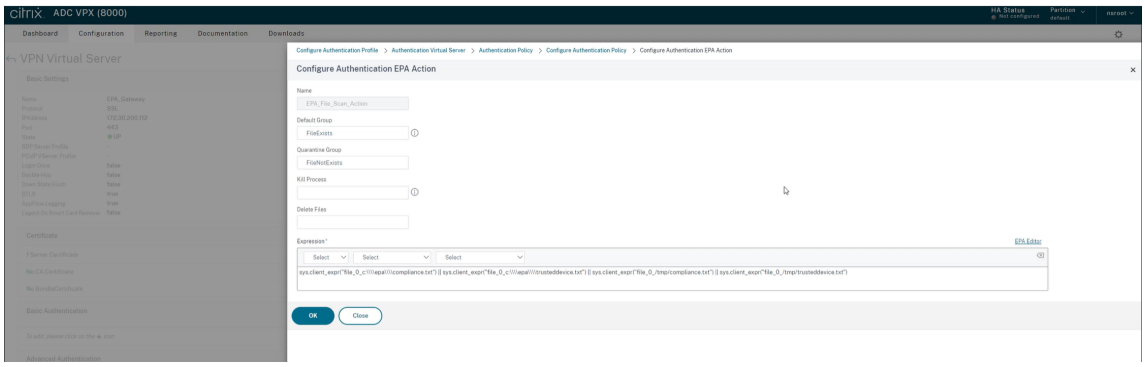
1. Citrix ADC にサインインし、［構成］>［**Citrix Gateway**］>［仮想サーバー］に移動します。

2. 関連する仮想サーバーを選択し、「編集」をクリックします。
3. 既存の認証プロファイルを編集します。
4. 関連する仮想サーバーを選択し、「編集」をクリックします。
5. ［認証ポリシー］ > ［バインドの追加］に移動します。
6. **[**ポリシーの選択**]** で **[**追加**]** をクリックします。
7. ［名前］フィールドに認証ポリシーの名前を入力します。
8. ［アクションタイプ］ドロップダウンリストで、［**EPA**］を選択します。
9. ［式］フィールドに「True」と入力します。



10. ［アクション］で［追加］をクリックします。
11. ［名前］フィールドに、EPA アクションの名前を入力します。
12. デフォルトのグループと検疫グループの名前を入力します。このシナリオでは、デフォルトのグループの名前は「**FileExists**」、検疫グループの名前は「**FileNotExists**」です。
13. 「式」フィールドに次の値を入力します。

```
sys.client_expr("file_0_c:\\epa\\compliance.txt") || sys.
    client_expr("file_0_c:\\epa\\trusteddevice.txt") || sys.
    client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("
    file_0_/tmp/trusteddevice.txt")
<!--NeedCopy-->
```



14. 「作成」をクリックし、「バインド」をクリックします。

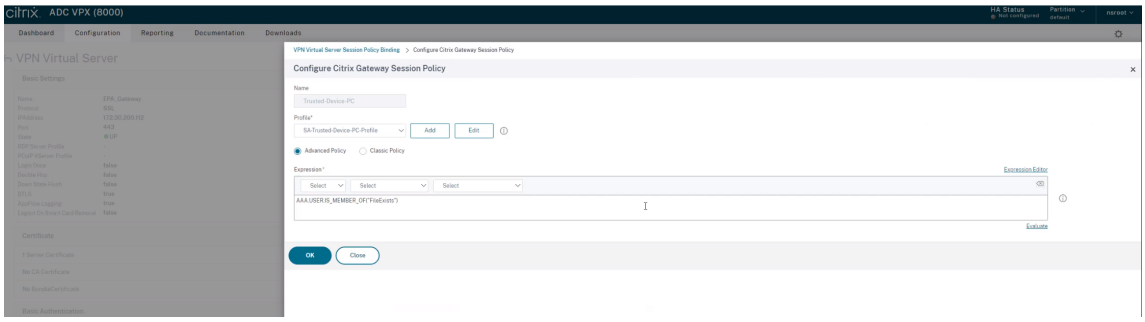
15. ［セッションポリシー］ > ［バインドの追加］に移動します。

16. **[ポリシーの選択]** で **[追加]** をクリックします。

17. ［名前］フィールドにセッションポリシーの名前を入力します。

18. 「式」フィールドに次の値を入力します。

```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```



19. 「作成」をクリックし、「バインド」をクリックします。

20. タスクバーの左端にある ［検索］アイコンをクリックします。

21. 「**Powershell**」と入力し、**Windows Powershell** を開きます。

22. 次のコマンドを使用して、**Smart Access tag**” **EPA_GW:Trusted-Device-PC**” を参照して EPA スキャンにパスしたデバイスの App Protection ポリシーを無効にします。

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

ここで、*EPA_GW* は VPN 仮想サーバー名です。

23. 次のコマンドを使用して、**Smart Access tag**” **EPA_GW:Trusted-Device-PC**” を参照して EPA スキャンにパスしたデバイスの App Protection ポリシーを無効にします:

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
    $true -ExcludedSmartAccessFilterEnabled $true -
    ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    IncludedSmartAccessFilterEnabled $true -
    AppProtectionScreenCaptureRequired $true
<!--NeedCopy-->
```

24. 確認

Citrix Workspace アプリがすでに開いている場合は、サインアウトします。信頼できるデバイスから Citrix

Workspace アプリにサインインします。保護されたリソースを起動すると、App Protection が無効になっていることがわかります。

Citrix Workspace アプリからサインアウトし、信頼できないデバイスから再度サインインします。保護されたリソースを起動すると、App Protection が有効になっていることがわかります。

シナリオ **5**

November 22, 2023

このシナリオでは、特定のユーザーグループに対して **App Protection** を有効にする方法について説明します。

特定のグループのユーザーに対して App Protection を有効にするには、「特定のユーザーグループに対して App Protection を有効にする」を参照してください。

Workspace を介したハイブリッド起動に対する **App Protection** のサポート

March 10, 2024

Citrix Virtual Apps and Desktops のハイブリッド起動は、ネイティブブラウザーでストア URL を入力し、ネイティブの Citrix Workspace アプリとその HDX エンジンで仮想アプリおよび仮想デスクトップを起動して、Citrix Workspace for Web にサインインする場合の起動です。ハイブリッドという用語は、Citrix Workspace for Web アプリとネイティブの Citrix Workspace アプリの組み合わせでリソースに接続して使用することを意味します。

> 注:
>
> エンドポイントにネイティブの Citrix Workspace アプリコンポーネントがインストールされていない場合、それは Citrix Workspace ストアと HDX エンジンの両方がブラウザー内に存在するゼロインストール構成です。このシナリオは HTML5 向け Citrix Workspace アプリと呼ばれ、Citrix Workspace または Citrix StoreFront のいずれかでホストされます。このドキュメントでは、このシナリオには対応していません。

前提条件

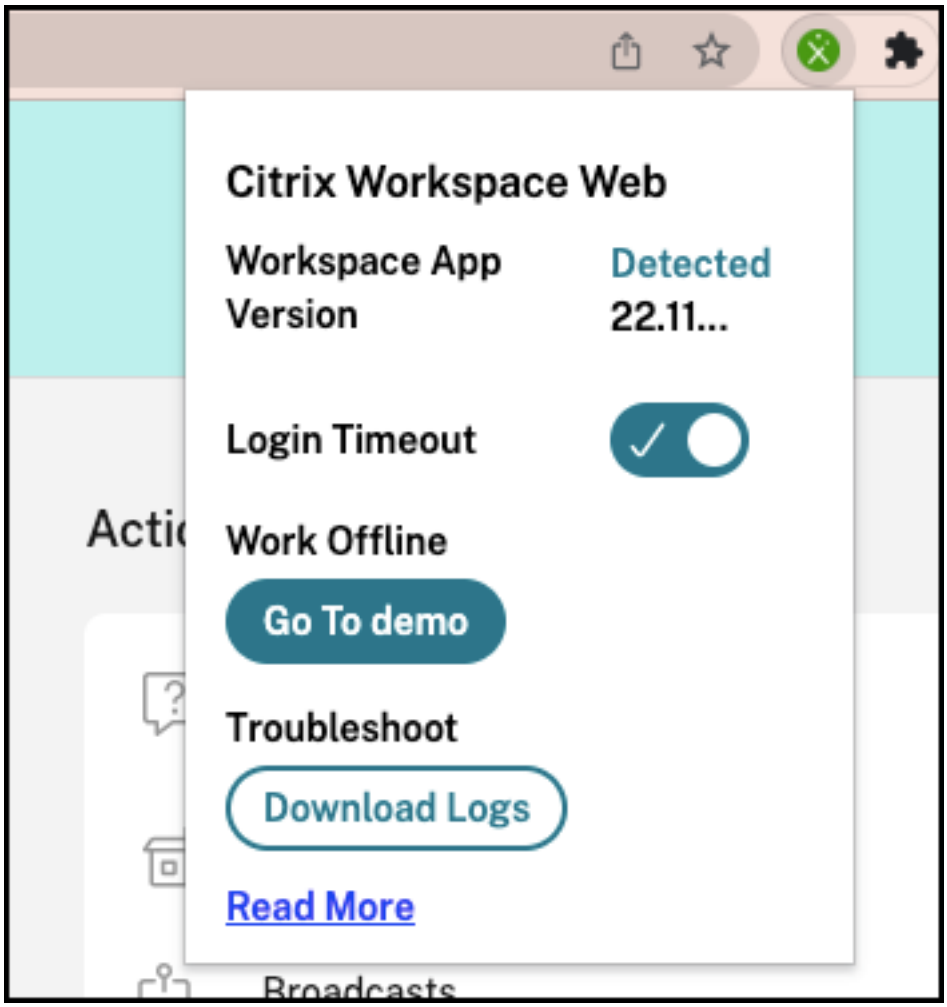
- Citrix Workspace Web 拡張機能をサポートするブラウザーを使用していることを確認します。
- Workspace URL の DNS サフィックスが cloud.com であることを確認します。現在、カスタムドメインはサポートされていません。
- 次のうちいずれかの Citrix Workspace アプリのバージョンを使用していることを確認してください:
  - Windows 向け Citrix Workspace アプリ 2106 以降
  - macOS 向け Citrix Workspace アプリ 2106 以降

ハイブリッド起動の **App Protection** の有効化

1. ストアを追加する前に、使用しているブラウザー用の Citrix Workspace Web 拡張機能をインストールします。使用しているブラウザーに基づいて、次のいずれかのリンクをクリックします:

   - Chrome
   - Edge Chromium

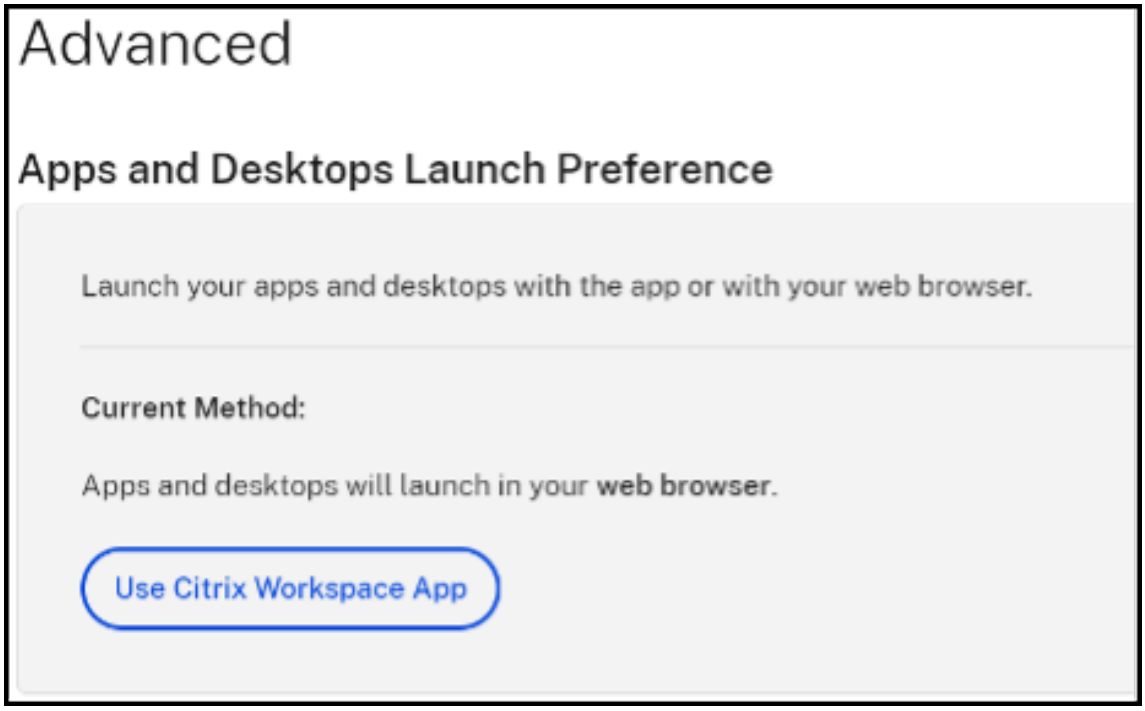
   拡張機能をインストールすると、Web ブラウザーの拡張機能セクションに表示されます。



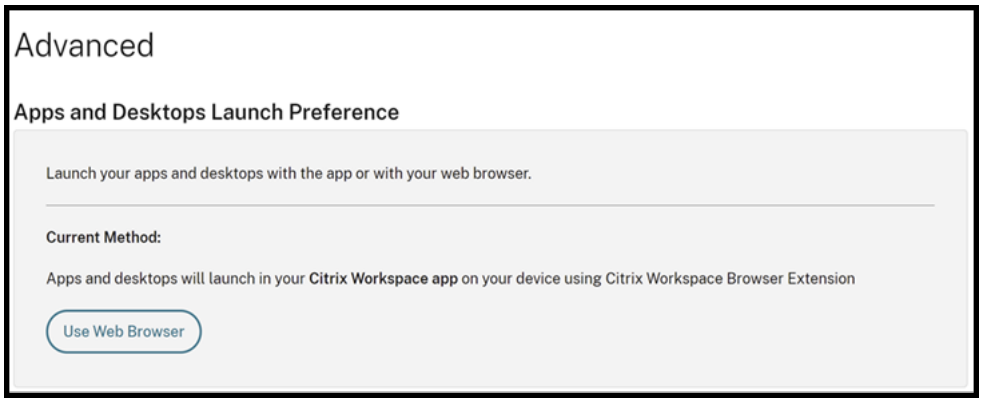
2. ネイティブブラウザーからストアにサインインします。

3. ［プロファイル］ > ［アカウント設定］ > ［詳細設定］に移動します。

   ［アプリおよびデスクトップの起動設定］セクションでは、Web ブラウザーでアプリとデスクトップの現在の起動方法を確認できます。［**Citrix Workspace** アプリの使用］をクリックします。



Citrix Workspace アプリを使用してリソースを起動している場合は、次のオプションが表示されます。このような場合、変更は必要ありません。

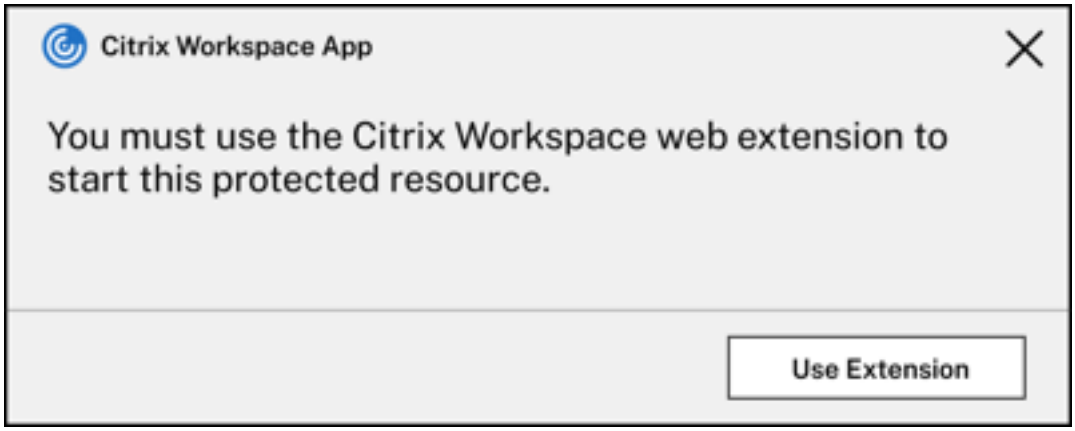


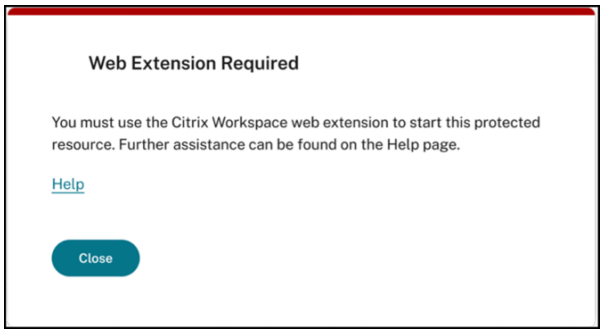
4. 保護された仮想アプリまたは仮想デスクトップを起動できるようになりました。

一般的な障害のシナリオ

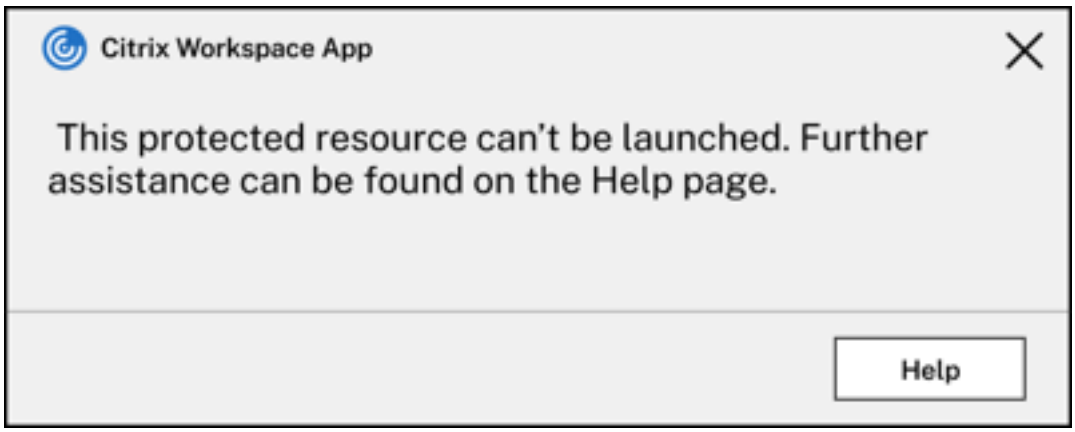
起動が失敗するシナリオとその修正方法をいくつか示します。

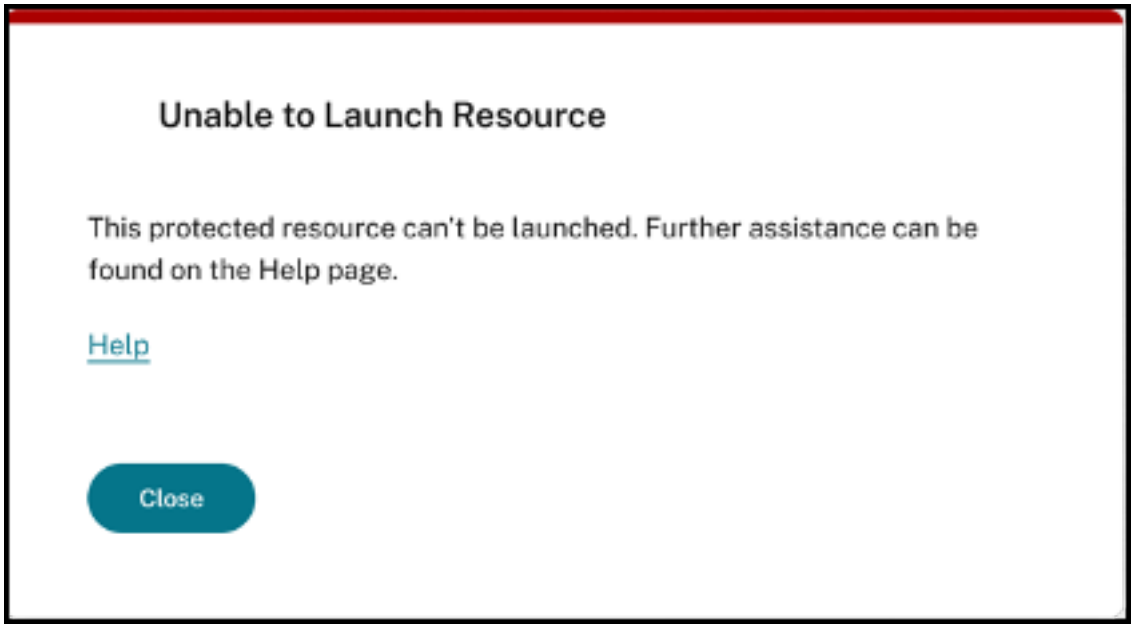
- 保護されたアプリケーションを起動する前に、Citrix Workspace Web 拡張機能を無効にするかアンインストールすると、次のいずれかのエラーが発生します。この問題を避けるには、Citrix Workspace for Web にログインする前に拡張機能をインストールします。





- 起動設定が ［**Web** ブラウザー］に設定されている場合、次のいずれかのエラーが発生します。起動設定を［**Citrix Workspace** アプリの使用］に変更して、このエラーを解決します。詳しくは、こちらのサポート記事を参照してください。





StoreFront を介したハイブリッド起動による App Protection のサポート

March 10, 2024

Citrix Virtual Apps and Desktops のハイブリッド起動では、（ネイティブブラウザーでストア URL を入力して）StoreFront for Web にサインインし、ネイティブの Citrix Workspace アプリとその HDX エンジンで仮想アプリおよび仮想デスクトップを起動します。ハイブリッドという用語は、StoreFront for Web とネイティブの Citrix Workspace アプリの組み合わせでリソースに接続して使用することを意味します。

> 注:
>
> エンドポイントにネイティブの Citrix Workspace アプリコンポーネントがインストールされていない場合、それは Citrix Workspace ストアと HDX エンジンの両方がブラウザー内に存在するゼロインストール構成です。このシナリオは HTML5 向け Citrix Workspace アプリと呼ばれ、Citrix Workspace または Citrix StoreFront のいずれかでホストされます。このドキュメントでは、このシナリオには対応していません。

StoreFront を介したハイブリッド起動による App Protection のサポートは、App Protection が有効なリソースを表示してブラウザーから起動する機能を提供します。

> 注:
>
> ［簡易バージョンを使用］（HTML5 クライアントを使用）または ［インストール済み］オプションを選択すると、Citrix Workspace アプリがブラウザーで正常に検出されないため、App Protection が有効なセッションがブロックされます。

StoreFront 2308 以降を使用している場合、StoreFront が適切に構成されており、ネイティブ Citrix Workspace アプリがブラウザーによって正常に検出されていれば、Web ブラウザーを使用して App Protection ポリシーが有効になっているアプリおよびデスクトップにアクセスできます。StoreFront 1912～2203 のバージョンを使用している場合は、「展開方法」セクションの説明に従ってカスタマイズを適用する必要があります。

> 制限事項:
>
> StoreFront は、Web サイトに初めてサインインするときに Citrix Workspace アプリのバージョンを決定します。その後で別のバージョンの Citrix Workspace アプリをインストールすると、StoreFront はその変更を認識しません。そのため、App Protection ポリシーが有効になっている仮想アプリやデスクトップの起動が誤って許可または禁止される可能性があります。App Protection のセキュリティ態勢チェックを構成して、App Protection をサポートしていない以前のバージョンの Citrix Workspace アプリからの仮想アプリやデスクトップの起動をブロックすることをお勧めします。状態チェックについて詳しくは、「App Protection のセキュリティ態勢チェック」を参照してください。

StoreFront バージョン **2308** 以降によるハイブリッド起動

StoreFront バージョン 2308 以降は、App Protection ポリシーが有効になっている仮想アプリとデスクトップのハイブリッド起動を自動的にサポートします。StoreFront 2308 以降でハイブリッド起動用の App Protection を有効にする方法の詳細については、「StoreFront 経由のハイブリッド起動用の App Protection」を参照してください。

1912 から **2203** までの **StoreFront** バージョンを介したハイブリッド起動

StoreFront バージョン 1912～2203 では、次のようなカスタマイズを使用して、App Protection ポリシーが有効になっている仮想アプリとデスクトップのハイブリッド起動の有効化をサポートします:

StoreFront 2308 以降にアップグレードする場合は、このカスタマイズを削除することをお勧めします。

前提条件

App Protection に必要な Citrix コンポーネントのバージョンについて詳しくは、「システム要件」を参照してください。

展開方法

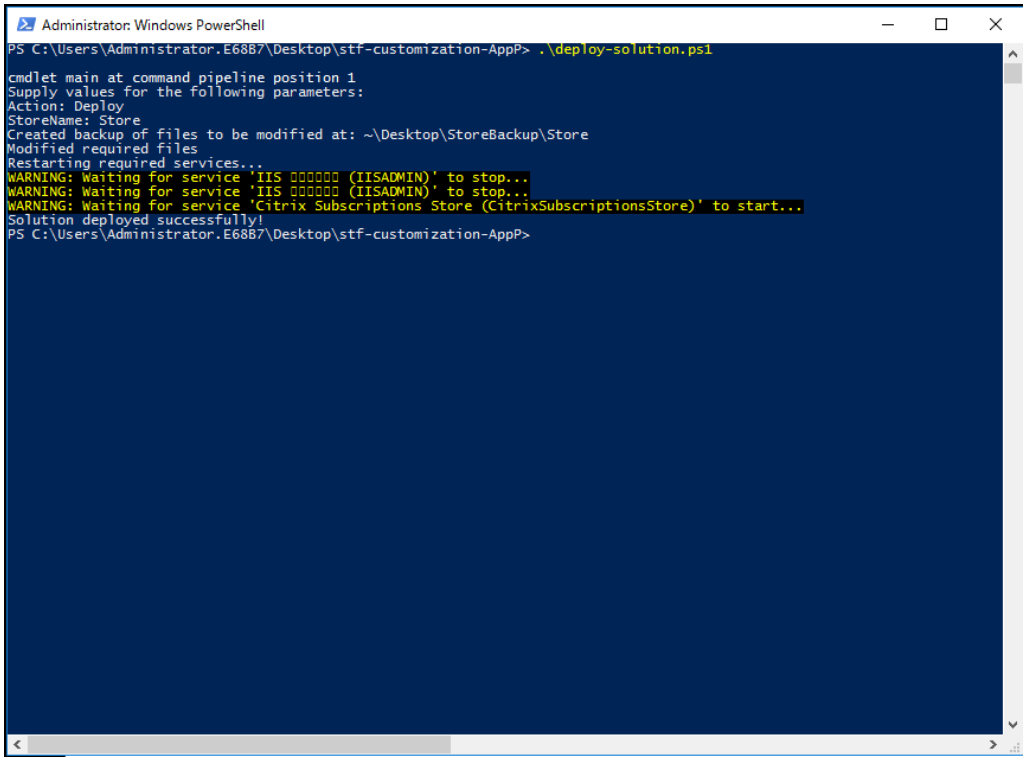
1. *stf-customization-AppP.zip* という名前の Zip ファイルをダウンロードします。これには、StoreFront サーバーマシンに展開する必要があるすべてのファイルが含まれています。Citrix のダウンロードページからファイルをダウンロードします。ファイルには次のものが含まれます:
    - ストアの bin フォルダーにコピーする必要がある DLL

- ソリューションが機能するために必要な JavaScript ファイルおよびその他のファイル
- StoreFront 管理者がソリューションの展開に使用する、*deploy-solution.ps1* PowerShell スクリプト

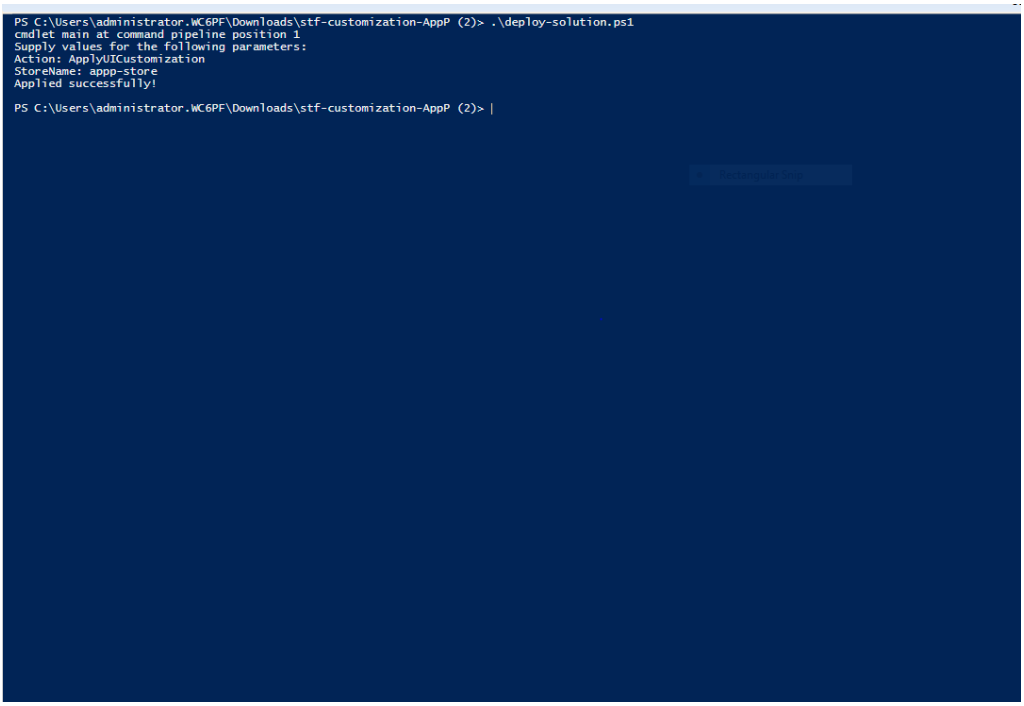
2. *stf-customization-AppP.zip* ファイルを解凍し、ファイルが抽出された新しい管理者 PowerShell を開きます。`deploy-solution.ps1`コマンドを実行します。このコマンドは、次の引数を指定します。

   - `-Action`: スクリプトが実行するアクション。許可される値は次のとおりです:

     - `Deploy`アクションは、ソリューションをシームレスに展開します。このソリューションが変更するファイルのバックアップを作成し、ソリューションファイルをコピーして、サービスを再起動します。次のスクリーンショットは、StoreFront サーバーにソリューションを展開するコマンドです:



     - `ApplyUICustomization`アクションはストア UI にカスタマイズを適用するため、［インストール済み］オプションと ［簡易バージョンを使用］オプションは表示されません。このアクションにより、ブラウザーでネイティブの Citrix Workspace アプリが強制的に検出され、ブロックまたはサポートされていないシナリオを確実に回避できます。



  - `RemoveUICustomization`アクションは`ApplyUICustomization`のアクションを元に戻し、［インストール済み］オプションと ［簡易バージョンを使用］オプションが再び表示されます。

- `-StoreName`: アクションを実行する必要があるストアの名前。このパラメーターは必須であり、`Deploy`アクションとともに渡す必要があります。
- `-BackupDir`: 必要なディレクトリにバックアップを作成するために`Deploy`アクションで渡すことができるパラメーター。渡されない場合、バックアップはデスクトップに作成されます。このパラメーターはオプションのパラメーターです。

> 注:
>
> *StoreCustomization_Input.dll* または *StoreCustomization_Launch.dll* に既存のカスタマイズがある場合、このソリューションを展開するとそれらが上書きされます。

App Protection が有効なアプリとデスクトップは、カスタマイズを展開した後にのみ表示されます。展開しない場合、アプリとデスクトップは表示されません。

StoreFront のカスタマイズを元に戻す方法

以前の StoreFront のカスタマイズを元に戻すには、次の手順を実行します:

1. *\Desktop\StoreBackup<store name>* ディレクトリに移動して、次のファイルを対応するディレクトリにコピーします:

- *StoreCustomization_Input.dll* および *StoreCustomization_Launch.dll* ファイルを *IISINETPub\Citrix<store name>\bin* ディレクトリにコピー
- *web.config* ファイルを *IISINETPub\Citrix\StoreWeb* ディレクトリにコピー
- **.js* および *style.css* ファイルを *IISINETPub\Citrix\StoreWeb\Custom* ディレクトリにコピー

> 注:
>
> 上記ファイル以外のカスタマイズファイルが存在する場合、「\Desktop\StoreBackup<store name>」ディレクトリに移動し、必要に応じてそれらのファイルとディレクトリを関連するディレクトリにコピーします。

2. PowerShell を開きます。
3. 次のコマンドを実行して、**IISADMIN** サービスと **CitrixSubscriptionsStore** サービスを停止します:

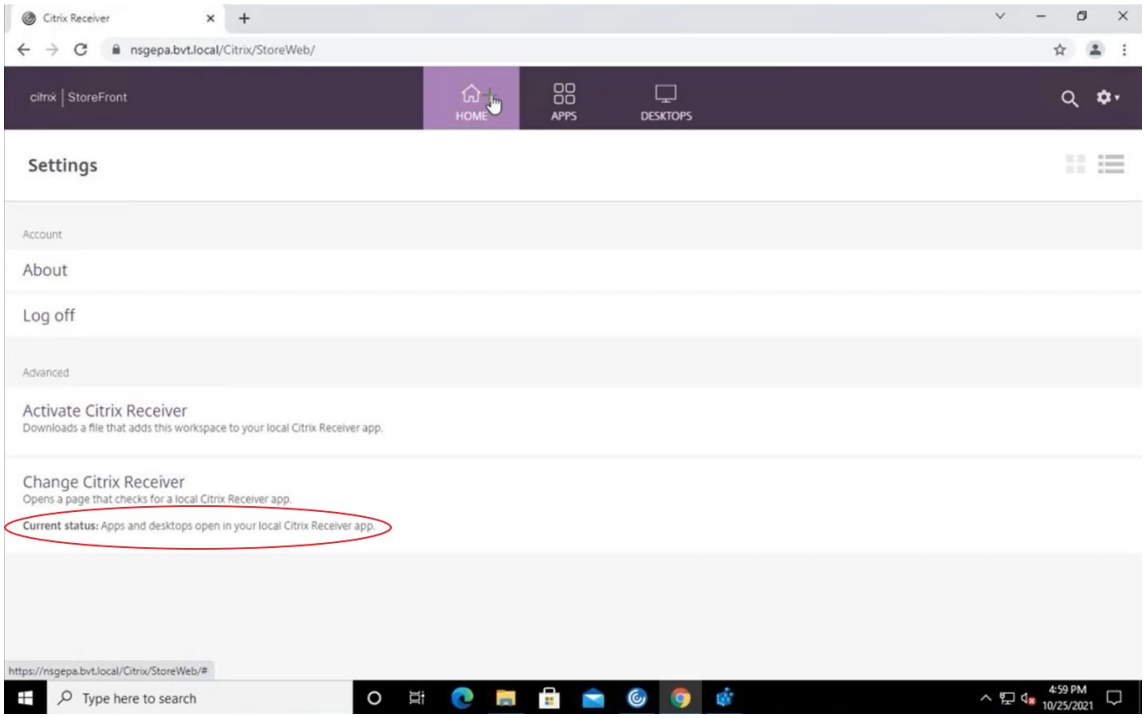
```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
<!--NeedCopy-->
```

4. 次のコマンドを実行して、**IISADMIN** サービスと **CitrixSubscriptionsStore** サービスを再度開始します:

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
<!--NeedCopy-->
```

保護されたリソースのハイブリッド起動に関するエンドユーザーエクスペリエンス

1. 管理者が StoreFront サーバーにソリューションを展開後、クライアント側でストアにサインインし、Web ブラウザーで URL を使用して StoreFront にアクセスします。
2. Citrix Workspace アプリがブラウザーで正常に検出されたかどうかを確認するには、［アカウント設定］で［現在のステータス］を確認します。



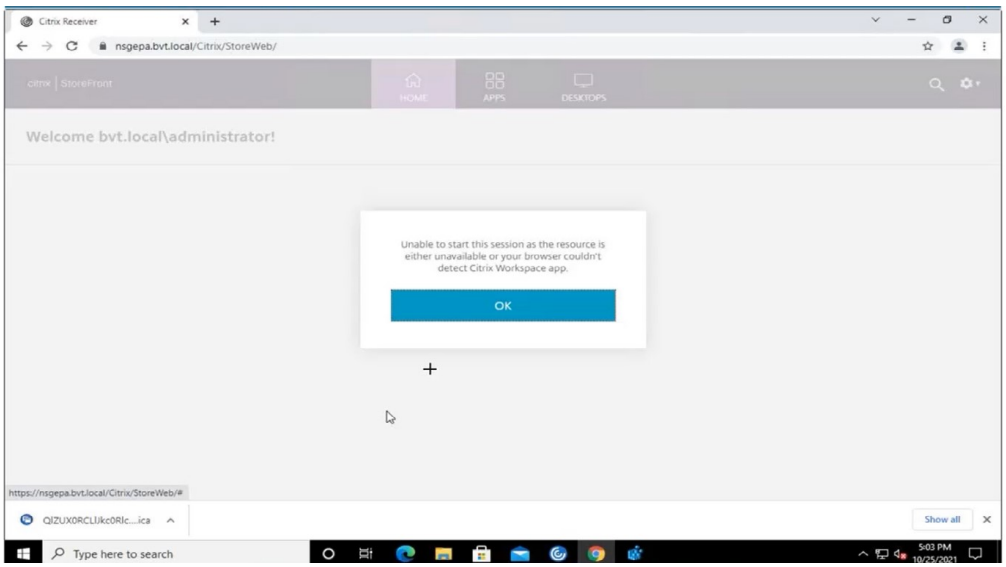
Citrix Workspace アプリが検出されると、App Protection が有効になっているすべての仮想アプリとデスクトップを表示して起動できます。

StoreFront でトレースを有効にする

StoreFront でトレースを有効にするには、StoreFront のドキュメントを参照してください。このトレースを使用して、構成された NetScaler Gateway セッションポリシーラベルがストアに適切に渡されているかどうかを確認できます。

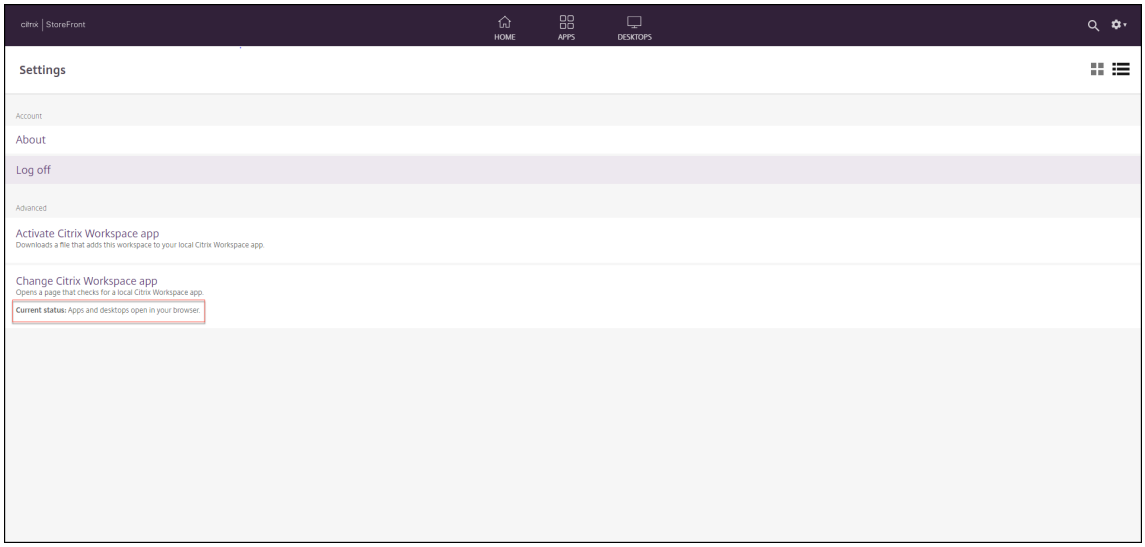
トラブルシューティング

App Protection が有効なセッションを起動すると、次のエラーが発生することがあります:

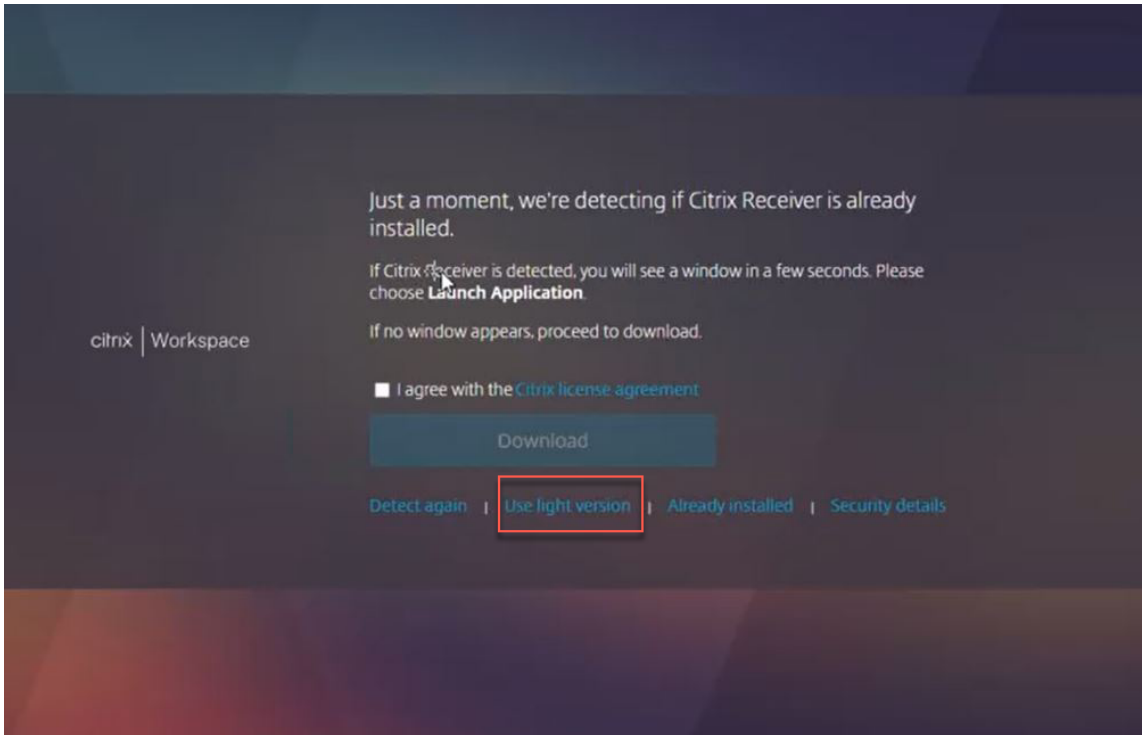


このエラーの考えられる原因は次のとおりです:

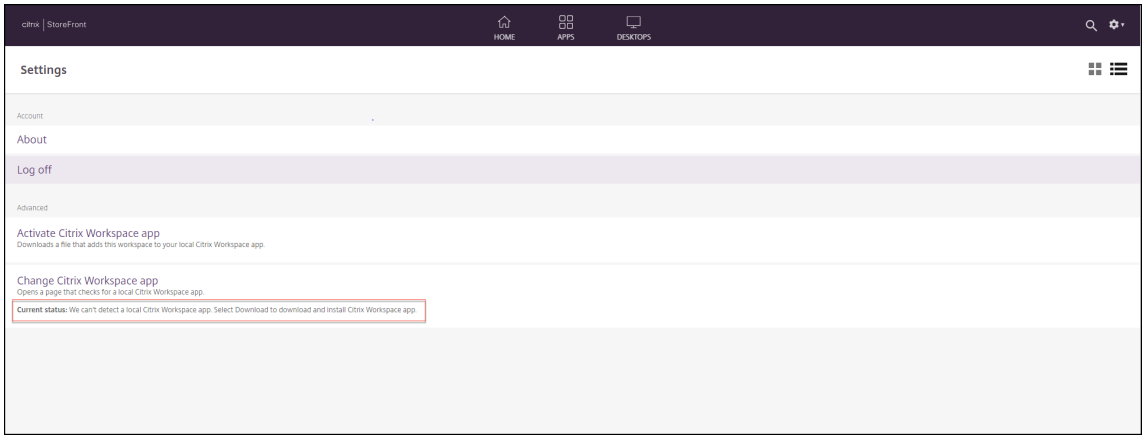
- アプリとデスクトップが、ブラウザーで開くように構成されています。



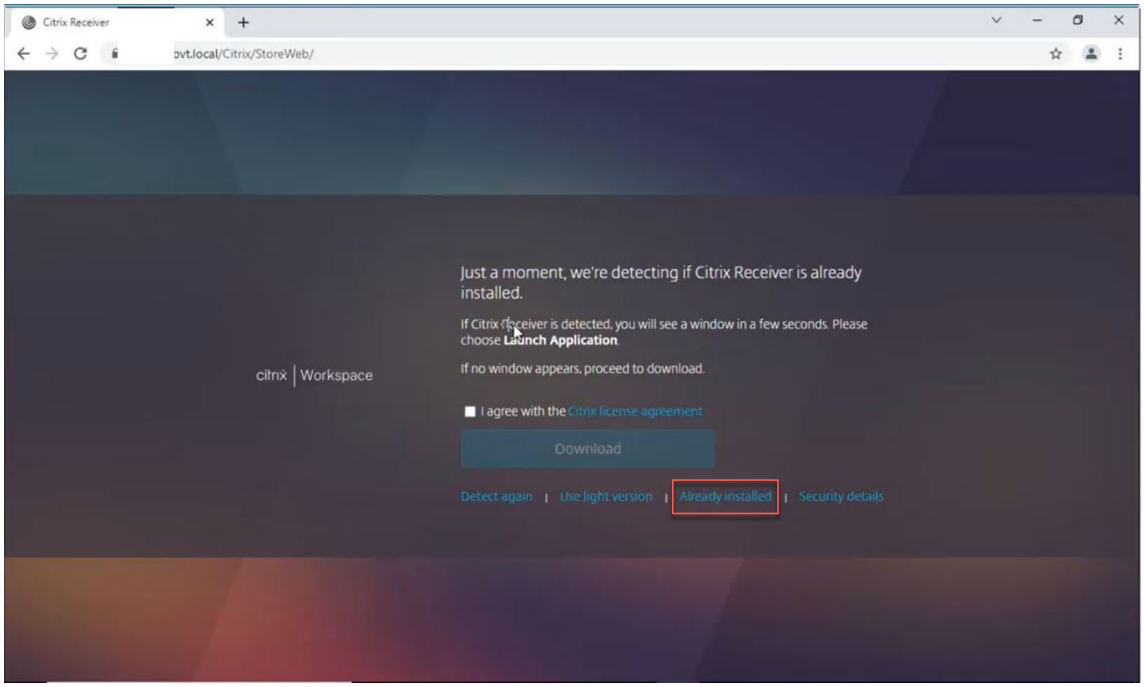
次の画面に示すように、Citrix Workspace アプリの検出中に ［簡易バージョンを使用］をクリックすると、このシナリオに直面します。



- ブラウザーが Citrix Workspace アプリを検出しません。



次の画面に示すように、Citrix Workspace アプリの検出中に ［インストール済み］をクリックすると、このシナリオに直面します。



ソリューション: 上記のシナリオに対応し、App Protection が有効なセッションを起動するには、[アカウント設定] で [**Citrix Workspace** アプリを変更] をクリックし、Citrix Workspace アプリが検出されるまで待ちます。

最適化

App Protection が有効なセッションを開始するには、Citrix Workspace アプリの検出が必須です。保護されたセッションのハイブリッド起動中の障害を回避するために、StoreFront 管理者は`deploy-solution.ps1`コマンドの`ApplyUICustomization`アクションを使用して、[簡易バージョンを使用] オプションと [インストール済み] オプションを非表示にすることができます。

Citrix Workspace アプリのリリーススケジュール

April 25, 2024

このリリーススケジュールは、Citrix Workspace アプリのリリース間隔およびリリース日程の目標を示したものです。リリース日は変更される可能性がありますが、お客様が今後の計画を検討するために、または、Citrix Workspace アプリ展開環境の管理にあたって参考にしていただければ幸いです。

Citrix Workspace アプリのダウンロードページから新しいリリースをダウンロードできます。Android 向け Citrix Workspace アプリ、iOS 向け Citrix Workspace アプリ、Windows（ストア）向け Citrix Workspace アプリは、それぞれのアプリストアからもダウンロードできます。Mac 向けまたは Windows 向け Citrix Workspace アプリで Citrix Workspace 更新プログラムを有効にしていると、更新のダウンロードおよびインストールに関して同意を

求める通知が送信されます。RSS フィードを購読すると、新しいリリースが利用可能になったときにアラートを受信できます。

Citrix Workspace アプリごとに利用可能な機能については、Citrix Workspace アプリの機能マトリックスを参照してください。

ライフサイクル情報については、「Citrix Workspace アプリのライフサイクルマイルストーン」を参照してください。

リリース間隔（目標）

次の Citrix Workspace アプリプラットフォームは、四半期ごとにリリースされます：

- Linux
- Mac
- Windows

次の Citrix Workspace アプリプラットフォームは、6 週間ごとにリリースされます：

- ChromeOS
- HTML5

次の Citrix Workspace アプリプラットフォームは、月 1 回リリースされます：

- Android
- iOS

> 注：
>
> Windows 向け Citrix Workspace アプリ、Mac 向け Citrix Workspace アプリ、Android 向け Citrix Workspace アプリ、および iOS 向け Citrix Workspace アプリは、今後、四半期ごとにメジャーリリースとマイナーリリースが行われる予定です。マイナーリリースは「.10」で示され、これらのリリースには品質とパフォーマンスの向上に関するマイナーな機能強化が含まれます。「.10」のマイナーリリースには、主な機能は含まれない予定です。

デスクトップアプリのリリース日程（目標）

Citrix Workspace アプリ	2024 年 2 月	2024 年 3 月	2024 年 4 月	2024 年 5 月	2024 年 6 月	2024 年 7 月	2024 年 8 月	2024 年 9 月	2024 年 10 月	2024 年 11 月	2024 年 12 月
Windows		-	☑	☑	☒	-	☑	☒	-	☑	-

Citrix Workspace アプリ	2024 年 2 月	2024 年 3 月	2024 年 4 月	2024 年 5 月	2024 年 6 月	2024 年 7 月	2024 年 8 月	2024 年 9 月	2024 年 10 月	2024 年 11 月	2024 年 12 月
Windows LTSR	☒	-	☑	-	☒	-	-	☒	-	-	☒
Mac	-	-	☑	☑	☒	-	☑	☒	-	☑	-
ChromeOS と HTML5	☑	-	☑	☑	☑	-	☑	☑	☑	-	☑
Linux	-	☑	-	☑	-	-	☑	-	-	☑	-

注：☑ 記号はメジャーリリースを表し、☒ 記号はマイナーリリースを表します。☒ 記号は累積更新プログラム (CU) を示します。

モバイルアプリとタブレットアプリのリリース日程（目標）

Android 向け Citrix Workspace アプリと iOS 向け Citrix Workspace アプリは、月 1 回リリースされます。

Citrix Workspace アプリ	2024 年 3 月	2024 年 4 月	2024 年 5 月	2024 年 6 月	2024 年 7 月	2024 年 8 月	2024 年 9 月	2024 年 10 月	2024 年 11 月	2024 年 12 月
Android と iOS 注：☑ 記号はメジャーリリースを表し、☒ 記号はマイナーリリースを表します。マイナーリリースは、特定の要件や改善点に合わせて調整されたオプションのリリースです。	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒

免責事項：

製品の開発、リリース、タイミングに関して記載された内容はシトリックスの独自の裁量に委ねられており、予告または協議なく変更される場合があります。提供されたデータは、情報提供のみを目的としたものであり、資料、コード、または機能を提供することを約束するものではなく、その法的義務もありません。したがって、購入の意思決定の際に依拠したり、契約に組み込むものではありません。

Citrix Workspace アプリの機能マトリックス

April 25, 2024

Citrix Workspace アプリは、さまざまなプラットフォームまたはオペレーティングシステムに分散されたさまざまな機能を提供します。この機能マトリックスを見れば、さまざまなプラットフォームでの機能の可用性を明確に理解できます。各セクションには、機能マトリックスとともに、すべての機能を簡潔に説明した機能定義表があります。

Citrix Workspace

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Citrix Virtual Apps	はい	はい	はい	はい	はい	はい	はい	はい
Citrix Virtual Desktops	はい	はい	はい	はい	はい	はい	はい	はい
Citrix Secure Private Access	はい	はい	いいえ	はい	はい	はい	いいえ	いいえ
Citrix Enterprise Browser (旧称 Citrix Workspace Browser)	はい	いいえ	はい	はい	いいえ	いいえ	いいえ	いいえ

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
SSO を使用する Web アプリまたは SaaS アプリ	はい	はい	はい	はい	はい	はい	はい	はい
Citrix モバイルアプリ	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ
アプリの個人設定サービス	はい	いいえ	いいえ	はい	はい	はい	いいえ	いいえ

機能	定義
Citrix Virtual Apps	Citrix DaaS または Citrix Virtual Apps and Desktops の資格情報で Citrix Virtual Apps にアクセスします。
Citrix Virtual Desktops	Citrix DaaS または Citrix Virtual Apps and Desktops の資格情報で Citrix Virtual Desktops にアクセスします。
Citrix Secure Private Access	Citrix Secure Private Access を使用すると、IT 管理者は承認された SaaS アプリへのアクセスを管理できます。シンプルなシングルサインオン環境では、管理者は、特定の Web サイトや Web サイトカテゴリへのアクセスをフィルター処理することで、マルウェアやデータ漏えいから組織のネットワークやエンドユーザーデバイスを保護できます。
Citrix Enterprise Browser	SaaS アプリおよび Web アプリに安全にアクセスするための Citrix Workspace アプリに付属している Web ブラウザー。

機能	定義
SSO を使用する Web アプリまたは SaaS アプリ	SSO が可能な Secure Workspace Access で構成した SaaS アプリまたは Web アプリへのアクセス。
Citrix モバイルアプリ	Citrix Endpoint Management（旧称 XenMobile）によって集約された Citrix モバイルアプリへのアクセス。
Citrix モバイルアプリのアップグレード	Citrix Endpoint Management（旧称 XenMobile）によって集約された Citrix モバイルアプリへのアクセス。
アプリの個人設定サービス	個人設定可能な企業エクスペリエンスを提供できます。アプリのワークフロー全体で、Citrix Workspace アプリのカスタムアプリ名とブランド提携アイコンを使用できます。

ワークスペース管理

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
DNS を使用したメールベースによるアカウント検出の自動構成	はい	はい	いいえ	はい	はい	はい	いいえ	いいえ
一元管理設定	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
Global App Config Service (Workspace)	はい	はい	いいえ	はい	はい	はい	はい	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Global App Config Service (StoreFront)	はい	はい	いいえ	はい	はい	はい	はい	はい
App Store の更新	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ
Citrix 自動更新	はい	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ
クライアントアプリ管理	はい	いいえ	いいえ	いいえ	該当なし	該当なし	該当なし	該当なし

機能	定義
DNS を使用したメールベースによるアカウント検出の自動構成	自動検出設定で Citrix Workspace アプリを構成できるようにします。
一元管理設定	一元化されたサービス（Google Chrome 管理や GPO など）からのアプリ設定。
Global App Config Service（Workspace）	Citrix Workspace 向けの Citrix Global App Configuration Service を使用すると、Citrix 管理者は一元管理されたサービスによって Workspace サービスの URL と Citrix Workspace アプリの設定を配信できます。
Global App Config Service（StoreFront）	Citrix StoreFront 向けの Citrix Global App Configuration Service を使用すると、Citrix 管理者は一元管理されたサービスによって Citrix Workspace アプリの設定を配信できます。
App Store の更新	ベンダーアプリケーションストアからの更新

機能	定義
Citrix 自動更新	Citrix 自動アップグレード機能を介した Windows および Mac 用の更新
クライアントアプリ管理	Citrix Workspace アプリが、Secure Access Agent や EPA（End Point Analysis：エンドポイント解析）プラグインなどのエージェントをインストールおよび管理するためにエンドポイントで必要とされる単一のクライアントアプリとして機能できるようにします。この機能により、管理者は必要なエージェントを 1 つの管理コンソールから簡単に展開および管理できます。

ユーザーインターフェイス

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Desktop Viewer/ツールバー	はい	はい	はい	はい	はい	はい	はい	はい
マルチタスク	はい	はい	はい	はい	はい	はい	はい	はい
Follow Me セッション（ワークスペースコントロール）	はい	はい	はい	はい	はい	はい	はい	はい

機能	定義
Desktop Viewer/ツールバー	ツールバーでの Ctrl+Alt+Del 送信など、セッション機能のセッション制御を有効にします。
マルチタスク	複数のアプリとデスクトップを同時に使用できるようにします。
Follow Me セッション（ワークスペースコントロール）	ユーザーがデバイス間を移動して、すべてのセッションに自動的に接続できるようにします。

HDX ホストコア

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
アダプティブトランスポート	はい	はい	はい	はい	はい	はい	いいえ	いいえ
HDX アダプティブスループット	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
SDWAN のサポート	はい	はい	はい	はい	いいえ	いいえ	はい	はい
セッション画面の保持	はい	はい	はい	はい	はい	はい	はい	はい
自動クライアント再接続	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
セッション共有	はい	はい	はい	はい	はい	はい	はい	はい

マルチポート ICA	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

機能	定義
アダプティブトランスポート	HDX の EDT トランスポートを有効にして、ネットワークの状態に関係なくスループットを向上させます。
SDWAN のサポート	QoS（サービス品質）、TCP、圧縮、および重複排除のため、SDWAN アクセラレーションを有効にします。
セッション画面の保持	セッションの保持は、ICA セッションをアクティブのまま保持し、ネットワークの接続が切断されても、セッションの画面を表示したままにできます。
自動クライアント再接続	接続が中断されると、プロンプトを表示してセッションに再接続します。
セッション共有	公開アプリケーションが、同じサーバーで既に実行されている場合に、他の公開アプリケーションと同じ接続で実行できるようにします。
マルチポート ICA	QoS（サービス品質）を向上させるために、HDX トラフィック用の複数の TCP ポートをサポートすることを許可します。

HDX IO / デバイス / 印刷

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
ローカル印刷	はい	はい	はい	はい	はい	いいえ	はい	はい
汎用 USB リダイレクト	はい	はい	はい	はい	はい	はい	はい	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
クライアントドライブマッピング / ファイル転送	はい	はい	はい	はい	はい	はい	はい	はい
TWAIN 2.0	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

機能	定義
ローカル印刷	ユーザーが共有プリンターまたはローカルプリンターでドキュメントを印刷できるようにします。
汎用 USB リダイレクト	セッション内で USB デバイスを使用できるようにします。たとえば、キーボード、マウス、外部 Web カメラなどです。
クライアントドライブマッピング / ファイル転送	データストレージ用に組み込まれた、または接続されたクライアントドライブを使用できるようにします。
TWAIN	デジタルカメラやスキャナーなどのクライアント TWAIN デバイスのマッピングを許可します。

HDX 統合

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
ローカルアプリアクセス	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
マルチタッチ	はい	はい	いいえ	いいえ	はい	はい	はい	はい
モビリティパック	はい	はい	いいえ	いいえ	はい	はい	はい	はい
HDX Insight	はい	はい	はい	はい	いいえ	いいえ	はい	はい
NSAP VC を使用した HDX Insight	はい	はい	はい	はい	はい（*3*）	はい（*3*）	いいえ	いいえ
EUEM エクスペリエンスマトリックス	はい	はい	はい	はい	いいえ	はい	はい	はい
コンテンツの双方向リダイレクト	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
URL のリダイレクト	はい	はい	はい	はい	はい	はい	はい	はい
ブラウザーコンテンツリダイレクト	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Citrix Workspace アプリでファイルを開く	はい	はい	はい	いいえ	はい	はい	いいえ	はい
位置情報ベースのサービス（API を介して利用できる位置情報）	はい	はい	いいえ	いいえ	はい	はい	いいえ	いいえ

機能	定義
ローカルアプリアクセス	セッション内のクライアントデバイス上のローカルアプリケーションへのアクセス。
マルチタッチ	Windows または Linux デスクトップおよびアプリの 10 本指マルチタッチコントロールを有効にします。
モビリティパック	ネイティブデバイスエクスペリエンス機能（自動ポップアップキーボードやローカルデバイスの UI コントロールなど）とタブレット向けに最適化されたデスクトップを有効にします。
HDX insight	ICA ネットワークパフォーマンスメトリックを使用して、セッションの開始時間または終了時間を可視化します。
NSAP VC を使用した HDX Insight	NetScaler App Experience または NSAP Virtual チャネルを使用して、セッションの開始時間または終了時間を可視化し、HDX の洞察を取得します。
EUEM エクスペリエンスマトリックス	Citrix 管理者は、Citrix Virtual Desktops（旧称 XenDesktop 7 Director）を介してログオン期間のメトリックを表示できます。

機能	定義
コンテンツの双方向リダイレクト	「クライアントからホスト」と「ホストからクライアント」の URL リダイレクトを有効にします。
URL のリダイレクト	クライアント上でローカルにアプリケーションを実行できるようにします。
ブラウザーコンテンツリダイレクト	Web ページ全体（Web ブラウザーのビューポート）をエンドポイントにリダイレクトしてローカルレンダリングできるようにし、サーバーの負荷を軽減します。
Citrix Workspace アプリでファイルを開く	ホストされるアプリケーション（クライアントからサーバーへのコンテンツリダイレクト）を使用して、Citrix Workspace アプリでローカルファイルを開けるようにします。
位置情報ベースのサービス（API を介して利用できる位置情報）	Citrix Virtual Desktops（旧称 XenDesktop）によって配信されるアプリケーションが位置情報を使用できるようにします。

HDX マルチメディア

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
オーディオ再生	はい	はい	はい	はい	はい	はい	はい	はい
双方向オーディオ (VoIP)	はい	はい	はい	はい	はい	はい	はい	はい
Web カメラリダイレクト	はい	はい	はい	はい	はい	はい	はい	はい
ビデオ再生	はい	はい	はい	はい	はい	はい	はい	はい
Microsoft Teams の最適化	はい	はい	はい（x64 のみ）	はい	いいえ	いいえ	はい	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Skype for Business Optimization Pack	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
Cisco Jabber 統合コミュニケーションの最適化	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
Windows マルチメディアリダイレクト	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ
UDP オーディオ	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ

機能	定義
オーディオ再生	サーバーでレンダリングされるオーディオ再生を有効にします。
双方向オーディオ（VoIP）	ホストされるソフトフォンまたは音声チャットコラボレーションアプリケーションを使用できるようにします。
Web カメラリダイレクト	ローカル Web カメラを使用したビデオチャットコラボレーションアプリケーションを使用できるようにします。
ビデオ再生	録画したビデオの表示を有効にします。

機能	定義
Microsoft Teams の最適化	Microsoft Teams のメディア処理を Citrix サーバーからユーザーデバイスにオフロードします。
Skype for Business の最適化	Skype for Business メディア処理を Citrix サーバーからユーザーデバイスにオフロードします。Android 向け Citrix Workspace アプリの場合、Chrome デバイスでのみサポートされます。
Cisco Jabber 統合コミュニケーションの最適化	Jabber のメディア処理を Citrix サーバーからユーザーデバイスにオフロードします。
Windows マルチメディアリダイレクト	Windows マルチメディアでのユーザーデバイスのレンダリングを有効にし、サーバーをオフロードします。
UDP オーディオ	UDP でのオーディオ入力および出力のサポート。

セキュリティ

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
TLS 1.2	はい	はい	はい	はい	はい	はい	はい	はい
TLS 1.0/1.1	はい	はい	はい	はい	はい	はい	はい	はい
DTLS 1.0	はい	はい	はい	はい	はい	はい	いいえ	いいえ
DTLS 1.2	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
SHA2 証明書	はい	はい	はい	はい	はい	はい	はい	はい
スマートアクセス	はい	はい	はい	はい	はい	はい	はい	はい
Citrix Gateway を介したリモートアクセス	はい *(1)*	はい	はい	はい	はい	はい	はい	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Web アクセス用ワークスペース	はい	はい	はい	はい	ICA ファイル経由	はい	はい	はい
IPV6	はい	はい	はい	はい	はい	はい	はい	はい
App Protection	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ

機能	定義
TLS 1.2	SSL の後継、強力な通信チャネルセキュリティ。
TLS 1.0/1.1	SSL の後継、強力な通信チャネルセキュリティ。
DTLS 1.0	DTLS は、SSL プロトコルから派生したものです。同じセキュリティサービス（整合性、認証、および機密性）を提供しますが、UDP プロトコルの下にあります。
DTLS 1.2	DTLS は、SSL プロトコルから派生したものです。同じセキュリティサービス（整合性、認証、および機密性）を提供しますが、UDP プロトコルの下にあります。
SHA2 証明書	SHA2 証明書を使用する機能。
スマートアクセス	Gateway のポリシーとフィルターを使用して、利用可能なアプリへのアクセスを制御します。
Gateway を介したリモートアクセス	VPN クライアントがない環境でも、エンタープライズアプリ、仮想デスクトップ、およびデータへの安全なアクセスをユーザーに提供します。
Web アクセス用ワークスペース	Web ブラウザーを使用した、ホストされるアプリケーションまたは仮想デスクトップへのアクセス。
IPV6	IPV6 ネットワークで使用できるようにします。

HDX グラフィック

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
H.264 拡張 SuperCodec	はい	はい	はい	はい	はい	はい	はい	はい
クライアント側ハードウェアアクセラレーション	はい	はい	はい	はい	いいえ	はい	いいえ	いいえ
3DPro グラフィック	はい	はい	はい	はい	はい	はい	はい	はい
外部モニターのサポート	はい	はい	はい	はい	はい	はい	はい	はい
デスクトップコンポジションリダイレクト	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
True マルチモニター	はい	はい	はい	はい	いいえ	いいえ	はい	はい

機能	定義
H.264 拡張 SuperCodec	XenApp/Desktop 7.X H264 拡張 Supercodec を使用して、アプリケーションの最適化された配信を有効にします。

機能	定義
クライアント側ハードウェアアクセラレーション	グラフィック、Web カメラなどの HDX 機能のハードウェアアクセラレーションを有効にします。ハードウェア機能の使用は、Citrix Workspace アプリによって異なります。
3DPro グラフィック	データセンターでホストされる 3D プロフェッショナルグラフィックスアプリケーションを使用できるようにします。
外部モニターのサポート	外部モニターを使用できるようにします。
デスクトップコンポジションリダイレクト	リモートでクライアントのレンダリングを実行するグラフィックコマンドを有効にし、サーバーのスケーラビリティを確保します。Receiver for Mac 12.9 バージョンでは廃止されています。
True マルチモニター	XenApp または XenDesktop が、クライアントでサポートされているのと同じ数のモニターを作成します。

認証

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
フェデレーション認証 (SAML/Azure AD)	はい	はい	はい	はい	はい	はい	はい	はい
ADC フル VPN	はい	はい	はい	はい	いいえ	いいえ	いいえ	いいえ
RSA ソフトトークン	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
チャレンジレスポンス SMS (Radius)	はい	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ
Gateway を介したユーザー証明書認証（ネイティブ Workspace アプリ経由）	いいえ	いいえ	いいえ	いいえ	はい	はい	はい	はい
Gateway を介したユーザー証明書認証（Web ブラウザー経由）	はい（*4*）	はい（*4*）	いいえ	はい	いいえ	いいえ	はい	はい
スマートカード (CAC、PIV など)	はい	はい	はい	はい	はい	はい	いいえ	はい
近接型/非接触型カード	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
資格情報の挿入（Fast Connect、Storebrowse など）	はい	はい	はい	いいえ	いいえ	いいえ	いいえ	はい
パススルー認証	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
資格情報の保存 * オンプレミスおよび StoreFront のみ	はい	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ
ADC nFactor 認証	はい	はい	はい	はい	はい	はい	はい	はい
ADC ネイティブ OTP	はい	はい	はい	はい	はい	はい	はい	はい
生体認証（Touch ID、Face ID）	いいえ	いいえ	いいえ	いいえ	はい	いいえ	いいえ	いいえ

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
Citrix モバイルアプリへのシングルサインオン	いいえ	いいえ	いいえ	いいえ	はい	はい	いいえ	いいえ
匿名ストアアクセス	はい	はい	はい	はい	はい	はい	はい	はい

機能	定義
フェデレーション認証（SAML/Azure AD）	Azure AD または SAML のいずれかにより、Microsoft ADFS サーバー（または他の SAML 対応 IdP）に委任するユーザー認証用 FAS サーバーを有効にします。
ADC（NetScaler）フル VPN	Gateway 用のフル VPN トンネルを構築します。
RSA ソフトトークン	RSA ソフトトークン使用時の簡略化された認証を有効にします。
チャレンジレスポンス SMS（Radius）	SMS パスコードの使用など、チャレンジレスポンス認証を使用できるようにします。
Gateway を介したユーザー証明書認証（Web ブラウザー経由のみ）	Windows の Web ブラウザーベース認証用である Gateway の認証の 1 つとして、ユーザー証明書を使用できるようにします。
スマートカード（CAC、PIV など）	認証および署名用に、標準の PC/SC 互換の暗号化スマートカードを使用できるようにします。
近接型/非接触型カード	近接型または非接触型スマートカードで認証することにより、ユーザーが Citrix アプリまたはデスクトップを使用できるようにします。

機能	定義
資格情報の挿入（Fast Connect、Storebrowse など）	近接型または非接触型スマートカードで認証することにより、ユーザーが Citrix アプリまたはデスクトップを使用できるようにします。Storebrowse は、Windows 向け Citrix Workspace アプリで使用できるコマンドラインユーティリティツールです。Storebrowse ユーティリティをスクリプト化することにより、Storebrowse を使用して Citrix Workspace アプリをカスタマイズできます。
パススルー認証	ユーザーの資格情報を Web Interface サイトに渡してから、Citrix Virtual Apps and Desktops サーバーに渡します。このプロセスにより、ユーザーは Citrix アプリの起動プロセス中の任意の時点で、明示的に認証できなくなります。
資格情報の保存 * オンプレミスおよび StoreFront のみ	オンプレミスおよび Citrix StoreFront を使用するのみで資格情報を保存できるようにします。
Gateway ネイティブ OTP	Gateway は、NetScaler アプライアンスの構成全体を保持することにより、サードパーティのサーバーを使用せずにワンタイムパスワード（OTP）をサポートします。
NetScaler nFactor 認証	nFactor 認証は、ユーザープロファイルに基づいた動的認証フローを可能にします。これらのフローは、ユーザーが直感的に理解できるように単純なフローである場合があります。必要な NetScaler の最小バージョンは 12.1.49.x です。
生体認証（Touch ID、Face ID）	Touch ID や Face ID などの生体認証を可能にします。
Citrix モバイルアプリへのシングルサインオン	Citrix モバイルアプリへのシングルサインオンを有効にします。
匿名ストアアクセス	認証が不要なユーザー（匿名ユーザー）のアクセスのサポート

入力エクスペリエンス

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
キーボードレイアウトの同期 - クライアントから VDA (Windows VDA)	はい	はい	はい	はい	はい	はい	いいえ	いいえ
キーボードレイアウトの同期 - クライアントから VDA (Linux VDA)	はい	はい	はい	はい	はい	はい	いいえ	いいえ
キーボードレイアウトの同期 - VDA からクライアント (Windows VDA)	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
キーボードレイアウトの同期 - VDA からクライアント (Linux VDA)	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
Unicode キーボードレイアウトマッピング	いいえ	いいえ	はい	はい	はい	はい	はい	はい
キーボード入力モード - Unicode	いいえ	いいえ	はい	はい	はい	はい	はい	はい
キーボード入力モード - スキャンコード	はい	はい	はい	はい	いいえ	いいえ	はい	はい
サーバー IME	はい	はい	はい	はい	はい	はい	はい	はい
CJK IME 用の汎用クライアント IME (CTXIME)	はい	はい	いいえ	はい	はい	はい	はい	はい

機能	Windows 2311.1 および Windows ストア 2309.1	Windows 2402 LTSR	Linux 2402	Mac 2402	iOS 24.3.5	Android 24.3.5	HTML5 2404	ChromeOS 2402.1
コマンドラインインターフェイス	はい	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
キーボード同期設定の UI と構成	はい	はい	はい	はい	はい	はい	いいえ	いいえ
入力モード設定の UI と構成	いいえ	いいえ	はい	はい	はい	いいえ	いいえ	いいえ
言語バー設定の UI と構成	はい	はい	いいえ	はい	いいえ	いいえ	いいえ	いいえ

機能	定義
キーボードレイアウトの同期 - クライアントから VDA (Windows VDA)	アクティブなキーボードレイアウトを同期する、または、クライアントデバイスの優先キーボードレイアウトを切り替えることができるようにします。クライアントデバイスのキーボードレイアウトは、Windows VDA で自動的に設定されます。
キーボードレイアウトの同期 - クライアントから VDA (Linux VDA)	アクティブなキーボードレイアウトを同期する、または、クライアントデバイスの優先キーボードレイアウトを切り替えることができるようにします。クライアントデバイスのキーボードレイアウトは、Linux VDA で自動的に設定されます。
キーボードレイアウトの同期 - VDA からクライアント (Windows VDA)	アクティブなキーボードレイアウトを同期する、または、Windows VDA の優先キーボードレイアウトを切り替えることができるようにします。Windows VDA のキーボードレイアウトは、クライアントデバイスで自動的に設定されます。

機能	定義
キーボードレイアウトの同期 - VDA からクライアント（Linux VDA）	アクティブなキーボードレイアウトを同期する、または、Linux VDA の優先キーボードレイアウトを切り替えることができるようにします。Linux VDA のキーボードレイアウトは、クライアントデバイスで自動的に設定されます。
Unicode キーボードレイアウトマッピング	Windows 向け以外の Citrix Workspace アプリで、Windows VDA の Unicode キーボードレイアウトマッピングをサポートします。
キーボード入力モード - Unicode	Unicode 入力モードでは、クライアント側のキーボードから VDA にキーを送信し、VDA は同じ文字を生成します。クライアント側のキーボードレイアウトを適用します。
キーボード入力モード - スキャンコード	スキャンコード入力モードでは、クライアント側のキーボードから VDA にキー位置を送信し、VDA が対応する文字を生成します。サーバー側のキーボードレイアウトを適用します。
サーバー IME	サービス（または VDA）側入力システム（IME）のユーザビリティとエクスペリエンスを提供します。
CJK IME 用の汎用クライアント IME（CTXIME）	クライアント IME のユーザビリティが強化され、東アジア言語（中国語、日本語、韓国語）でのシームレスなエクスペリエンスが向上します。
コマンドラインインターフェイス	ユーザーは、コマンドラインインターフェイスを使用してクライアント IME を有効または無効にできます。
キーボード同期設定の UI と構成	ユーザーは、GUI を使用してさまざまなキーボードレイアウト同期オプションを選択できます。
入力モード設定の UI と構成	ユーザーは、GUI を使用してさまざまなキーボード入力モードオプションを選択できます。
言語バー設定の UI と構成	ユーザーは、GUI を使用して、VDA アプリセッションでリモート言語バーの表示/非表示を選択できます。言語バーには、セッションで優先される入力言語が表示されます。
キーボードレイアウトの同期の GPO 管理用テンプレート	管理者は、Citrix Workspace アプリのグループポリシーオブジェクト管理用テンプレートから対応するポリシーを展開することにより、キーボードレイアウトの同期構成を上書きできます。

テーブルインジケーター

インジケーター	説明
1	StoreFront のみ
2	HDX 3D Pro は、Citrix Workspace アプリ向けに JPEG に戻ります。H.264 深圧縮の 1.5Mbps と比較して、3Mbps が推奨されます。
3	NSAP VC の場合、iOS/Android 向けの Workspace アプリはサポートしますが、ADC/ADM のサポートはまだ保留中です。
4	Gateway を介したユーザー証明書認証（Web ブラウザー経由のみ）の認証方法は、Citrix Workspace アプリクライアントの検出をサポートしていません。ICA ファイルがダウンロードされている場合にのみ、Citrix Workspace アプリを使用して仮想アプリまたはデスクトップを開くことができます。

> 注:
>
> Citrix 製品の機能の開発、リリース、タイミングについては Citrix の独自の裁量に委ねられています。ここで提供された情報は、情報提供のみを目的としたものであり、資料、コード、または機能を提供することを約束するものではなく、その法的義務もありません。したがって、購入の意思決定の際に依拠したり、契約に組み込むものではありません。Citrix 製品の機能の開発、リリース、タイミングについては Ctirxi の独自の裁量に委ねられており、予告または協議なく変更される場合があります。