



# Windows 向け Citrix Workspace アプリ

## Contents

|  |            |
|--|------------|
| このリリースについて                               | 3          |
| システム要件と互換性                               | 45         |
| インストールとアンインストール                          | 51         |
| 展開                                       | 62         |
| アップデート                                   | 68         |
| はじめに                                     | 76         |
| 構成                                       | 95         |
| 認証                                       | 186        |
| セキュリティで保護された通信                           | 202        |
| <b>Storebrowse</b>                       | <b>213</b> |
| <b>Citrix Workspace アプリ Desktop Lock</b> | <b>221</b> |
| <b>SDK および API</b>                       | <b>226</b> |
| <b>ICA 設定リファレンス</b>                      | <b>228</b> |

## このリリースについて

November 12, 2021

### 2109.1 の新機能

#### Windows 11 のサポート

Windows 向け Citrix Workspace アプリが Windows 11 オペレーティングシステムでサポートされるようになりました。

このリリースで解決された問題の一覧については、「[2109.1 で解決された問題](#)」を参照してください。

### 2109 の新機能

#### アダプティブオーディオ

アダプティブオーディオを使用すれば、VDA でオーディオ品質ポリシーを構成する必要はありません。アダプティブオーディオは環境の設定を最適化し、非推奨のオーディオ圧縮形式を置き換え、優れたユーザーエクスペリエンスを提供します。

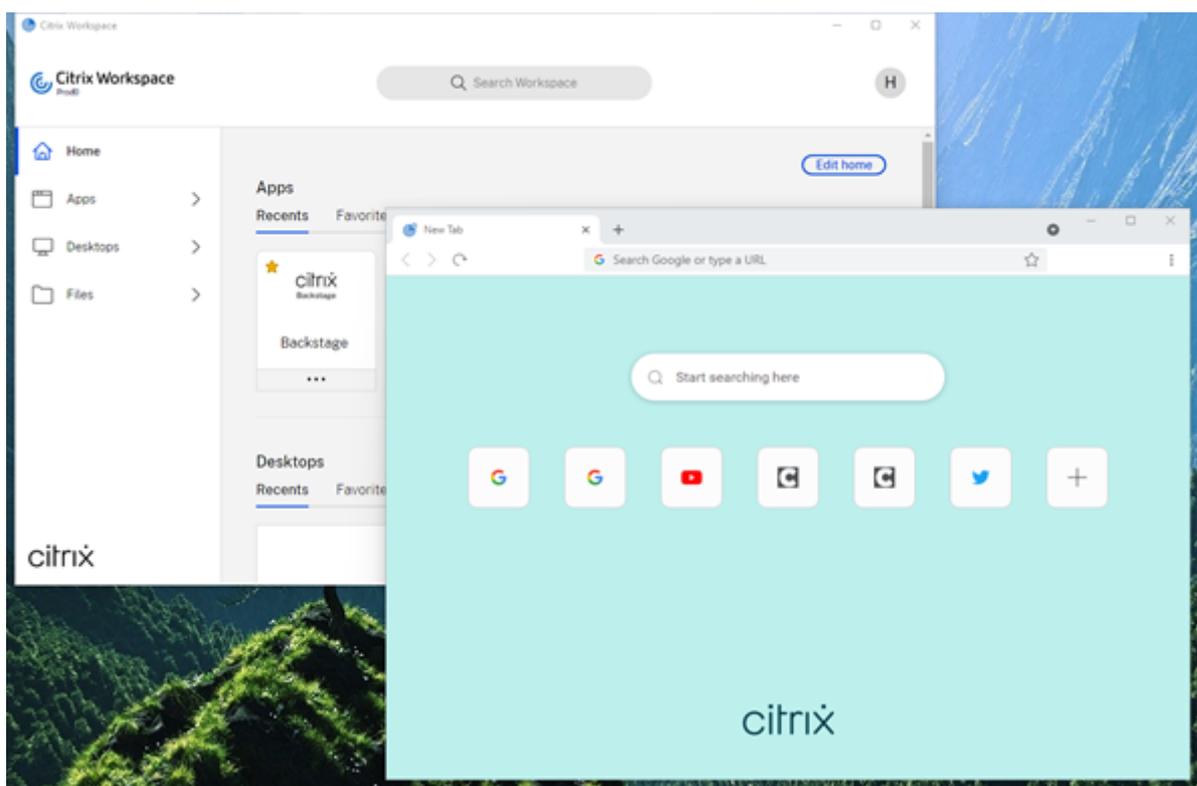
注:

リアルタイムオーディオアプリケーションに UDP でのオーディオ配信が必要な場合、UDP でのオーディオ配信にフォールバックできるようにするには、VDA でアダプティブオーディオを無効にする必要があります。

詳しくは、「[アダプティブオーディオ](#)」を参照してください。

### Citrix Workspace Browser

Citrix Workspace Browser は、クライアントマシンで実行されるネイティブブラウザーです。これにより、ユーザーは Citrix Workspace アプリから安全な方法で、Web および SaaS アプリケーションを開くことができます。



新しいブラウザは、ユーザーエクスペリエンスの向上に引き続き重点を置いており、次の機能を備えた、強化された、よりネイティブブラウザのようなユーザーエクスペリエンスを提供します：

- 内部 Web ページへの VPN レスアクセス
- マイクと Web カメラのサポート
- タブブラウジングエクスペリエンス
- マルチウィンドウビュー
- 編集可能なオムニボックス
- ブックマーク
- 新しいタブページのショートカット
- カスタマイズ可能な設定
- プロキシ認証のサポート
- 分析

管理者は、URL ごとにさまざまな組み合わせで、キーロガー対策、スクリーンキャプチャ対策、ダウンロード、印刷、クリップボード制限、透かし機能などの、Secure Workspace Access (SWA) やアプリ保護ポリシーを有効にできます。

詳しくは、「[概要](#)」を参照してください。

### StoreFront から Workspace への URL の移行

組織がオンプレミスの StoreFront から Workspace に移行すると、エンドユーザーは新しい Workspace URL をエンドポイントの Workspace アプリに手動で追加する必要があります。この機能により、管理者は最小限のユーザー操作でユーザーを StoreFront ストアから Workspace ストアにシームレスに移行できます。

この機能について詳しくは、「[StoreFront から Workspace への URL の移行](#)」を参照してください。

### カスタム Web ストアのサポート

このリリースでは、Windows 向け Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。

この機能を使用するには、管理者はドメインまたはカスタム Web ストアを Global App Configuration Service で許可されている URL の一覧に追加する必要があります。これが完了したら、Citrix Workspace アプリの [アカウントの追加] 画面でカスタム Web ストアの URL を指定できます。カスタム Web ストアはネイティブの Workspace アプリウィンドウで開きます。

カスタム Web ストアの構成について詳しくは、「[カスタム Web ストア](#)」を参照してください。

### Windows Hello ベースの認証および FIDO2 セキュリティキーベースの認証のサポート

このリリースでは、Windows Hello および FIDO2 セキュリティキーを使用して、Citrix Workspace への認証を行うことができます。

詳しくは、「[Citrix Workspace への認証を行う他の方法](#)」を参照してください。

### ID プロバイダーとして Microsoft Azure Active Directory (AAD) を使用し AAD 参加済みのマシンから Citrix Workspace アプリにシングルサインオン (SSO)

このリリースでは、ID プロバイダーとして Microsoft Azure Active Directory (AAD) を使用し AAD 参加済みのマシンから Citrix Workspace アプリにシングルサインオンできます。

詳しくは、「[Citrix Workspace への認証を行う他の方法](#)」を参照してください。

### Azure Active Directory での条件付きアクセスのサポート

このリリースでは、Workspace 管理者は、Citrix Workspace アプリへの認証を行うユーザーに対して Azure Active Directory の条件付きアクセスポリシーを構成および適用できます。

詳しくは、「[Azure AD を使用した条件付きアクセスのサポート](#)」を参照してください。

### サービス継続性のサポート

このリリースでは、Citrix Workspace Web 拡張機能によるサービス継続性がサポートされます。Google Chrome 用の Workspace Web 拡張機能、または Windows 向け Workspace アプリ 2109 を使用する Microsoft Edge を

使用できます。これらの拡張機能は、[Google Chrome ウェブストア](#)および[Microsoft Edge アドオン Web サイト](#)で入手できます。

Workspace アプリは、Web ブラウザー拡張機能用のネイティブメッセージングホストプロトコルを使用して、Citrix Workspace Web 拡張機能と通信します。Workspace アプリと Workspace Web 拡張機能は、Workspace 接続リリースを使用して、停止中に Web ブラウザーユーザーがアプリとデスクトップにアクセスできるようにします。詳しくは、「[サービス継続性](#)」を参照してください。

### Microsoft Teams の機能強化

次の機能は、Microsoft Teams から今後の更新がロールアウトされてからのみ使用できます。

更新が Microsoft によってロールアウトされたら、CTX253754 でドキュメントの更新と発表を確認できます。

- **WebRTC** のサポート: このリリースでは、WebRTC 1.0 がサポートされており、ギャラリービューとともにビデオ会議のエクスペリエンスが向上しています。
- 画面共有の強化: Microsoft Teams の画面共有機能を使用して、個別のアプリケーション、ウィンドウ、または全画面を共有できます。Citrix Virtual Delivery Agent 2109 は、この機能の前提条件です。
- アプリ保護の互換性: アプリ保護が有効になっている場合、HDX 最適化で Microsoft Teams を介してコンテンツを共有できるようになりました。  
この機能を使用すると、仮想デスクトップで実行されているアプリケーションウィンドウを共有できます。Citrix Virtual Delivery Agent 2109 は、この機能の前提条件です。

#### Note:

Full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group.

- ライブキャプション: このリリースでは、Microsoft Teams でライブキャプションが有効になっているときにスピーカーが話す内容のリアルタイムの文字起こしがサポートされています。

### Microsoft Teams 最適化

このリリースでは、VM Hosted App で最適化された Microsoft Teams でのピアツーピアの音声、ビデオ通話、電話会議、および画面共有がサポートされています。

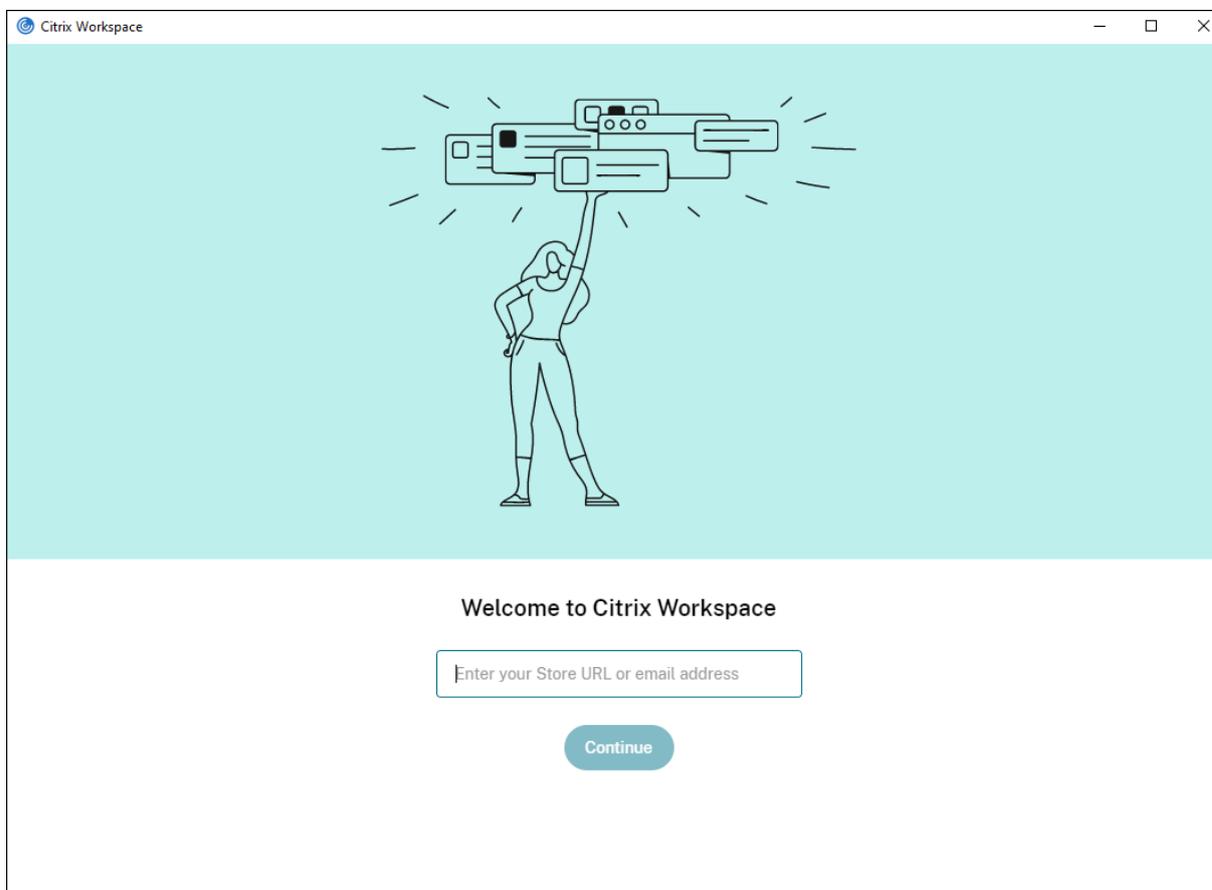
### Bloomberg キーボード 5 のサポート

このリリースには、Bloomberg キーボード 5 のサポートが含まれています。Bloomberg キーボード 5 を使用するには、レジストリエディターを構成する必要があります。キーボードの構成について詳しくは、「[Bloomberg キーボード](#)」の「Bloomberg キーボード 5 の構成」を参照してください。

## 2108 の新機能

### アカウントの追加画面の刷新

このリリースでは、刷新されたアカウントの追加画面が導入されています。



### Citrix Workspace セッションの無操作状態によるタイムアウト

管理者は、無操作状態によるタイムアウト値を構成して、ユーザーが Citrix Workspace アプリセッションから自動的にサインアウトされるまでのアイドル時間を指定できます。指定された時間内にマウス、キーボード、またはタッチによるアクティビティがない場合は、自動的に Workspace からサインアウトされます。無操作状態によるタイムアウトは、すでに実行中の Citrix Virtual Apps and Desktops セッションまたは Citrix StoreFront ストアには影響しません。

詳しくは、「[Workspace セッションの無操作状態によるタイムアウト](#)」を参照してください。

注:

管理者は、Workspace (クラウド) セッションに対してのみ無操作状態によるタイムアウトを構成できます。

### カスタム **Web** ストアのサポート **[Technical Preview]**

このリリースでは、Windows 向け Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。この機能を使用するには、管理者はドメインまたはカスタム Web ストアを Global App Configuration Service で許可されている URL の一覧に追加する必要があります。これが完了したら、Citrix Workspace アプリの [アカウントの追加] 画面でカスタム Web ストアの URL を指定できます。カスタム Web ストアはネイティブの Workspace アプリウィンドウで開きます。

カスタム Web ストアの構成については、「[カスタム Web ストア](#)」を参照してください。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビューのサポートケースは受け付けていませんが、機能向上のための [フィードバック](#) はお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。ベータビルドは実稼働環境に展開しないことをお勧めします。

### StoreFront から **Workspace** への URL の移行 **[Technical Preview]**

組織がオンプレミスの StoreFront から Workspace に移行すると、エンドユーザーは新しい Workspace URL をエンドポイントの Workspace アプリに手動で追加する必要があります。

この機能により、管理者は最小限のユーザー操作でユーザーを StoreFront ストアから Workspace ストアにシームレスに移行できます。

この機能について詳しくは、「[\[StoreFront から Workspace への URL の移行 \[Technical Preview\]\]](#)」 ([/ja-jp/citrix-workspace-app-for-windows/configure.html#storefront-to-workspace-url-migration](#)) を参照してください。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビューのサポートケースは受け付けていませんが、機能向上のための [フィードバック](#) はお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。ベータビルドは実稼働環境に展開しないことをお勧めします。

## 2107 の新機能

### EPA の機能強化

このリリース以降、Citrix Workspace アプリは、ワークスペース展開で EPA プラグインをダウンロードしてインストールできます。インストールが完了すると、Advanced Endpoint Analysis (EPA) がデバイスをスキャンして、Citrix Gateway で設定されているエンドポイントのセキュリティ要件を確認します。スキャンが完了すると、Citrix Workspace アプリのログインウィンドウが表示されます。

注:

この機能は、環境で nFactor 認証を構成した場合にのみ有効になります。

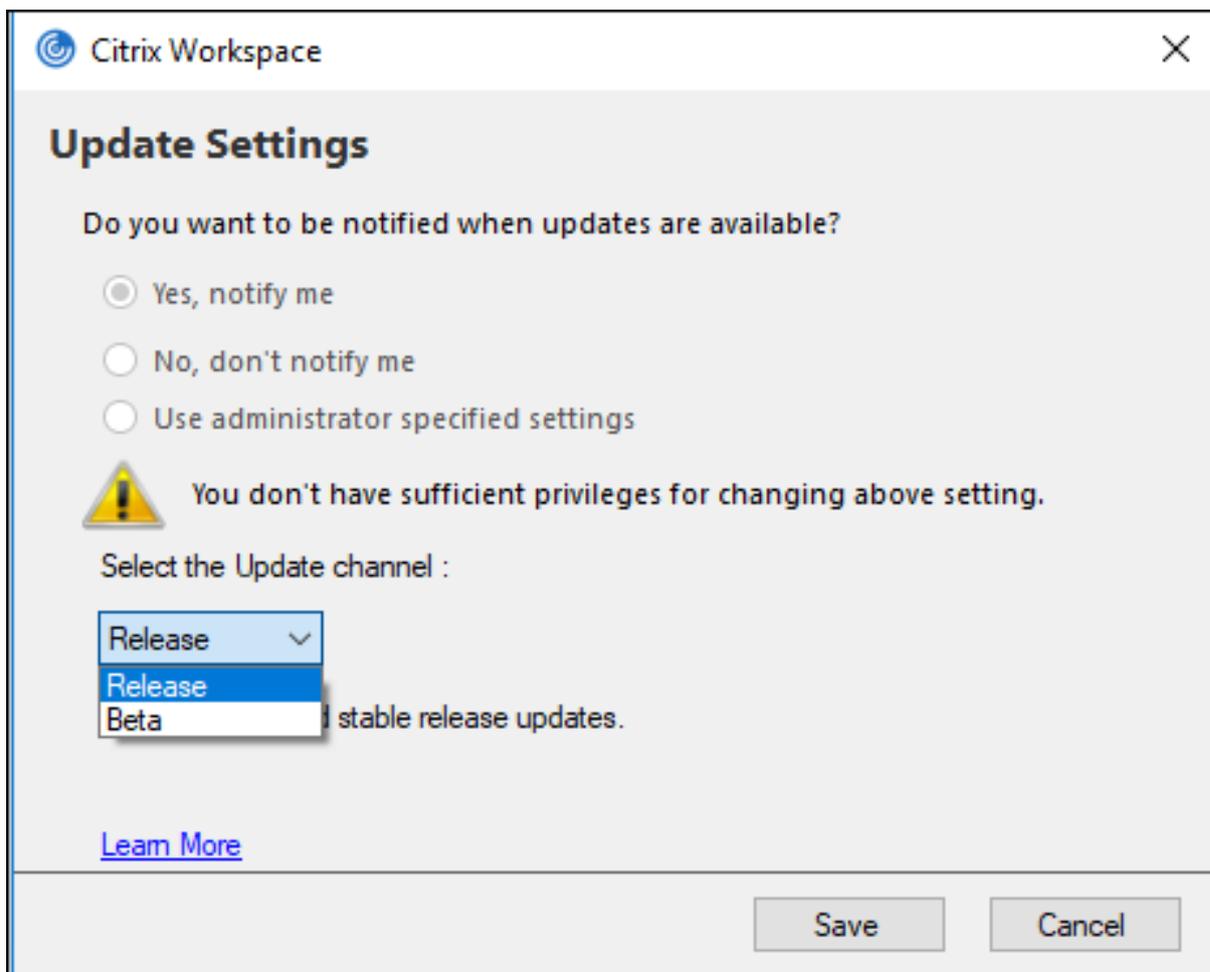
EPA スキャンについて詳しくは、「[Advanced Endpoint Analysis スキャン](#)」を参照してください。

### Citrix Workspace アプリのベータプログラム

このリリース以降、Citrix Workspace アプリの既存のインストールを最新のベータビルドに自動的に更新して、それらをテストすることができます。ベータビルドは、完全にサポートされている安定版リリースアップデートが一般提供される前にリリースされる、早期アクセスバージョンです。Citrix Workspace アプリが自動更新用に構成されている場合は、更新通知を受け取ります。

ベータビルドに更新するには、[設定の更新] ウィンドウのドロップダウンメニューから Beta チャンネルを選択します。

- **Release** - 完全にサポートされている安定版リリースの更新プログラム
- **Beta** - 一般提供前に簡単にテストして問題を報告できる早期アクセスリリース



### 注:

ベータビルドは、お客様が非実稼働環境または制限のある稼働環境で使用し、フィードバックを共有する機会を提供するためのものです。ベータビルドのサポートケースは受け付けていませんが、機能向上のためのフィードバックはお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。ベータビルドは実稼働環境に展開しないことをお勧めします。

自動更新チャンネルをインストールする方法について詳しくは、「[Citrix Workspace アプリのベータプログラムのインストール](#)」を参照してください。

### 次の認証メカニズムのサポート **[Technical Preview]**

このリリース以降、次のメカニズムを使用して Citrix Workspace アプリへの認証を行うことができます:

- Windows Hello
- FIDO2 ベースの認証メカニズム
- ID プロバイダーとして Microsoft Azure Active Directory (AAD) を使用し AAD 参加済みのマシンから Citrix Workspace アプリにシングルサインオン (SSO)

### システム要件

Microsoft Edge WebView2 ランタイムバージョン 92 以降。

### 注:

バージョン 2107 以降、Microsoft Edge WebView2 ランタイムインストーラーは Citrix Workspace アプリのインストーラーとともにパッケージ化されます。Workspace アプリのインストール時、インストーラーが Microsoft Edge WebView2 ランタイムがシステム上に存在するかどうかを確認し、必要に応じてインストールします。

この機能は、Workspace (Cloud) のみでサポートされます。

### 認証メカニズムの有効化

認証メカニズムを有効にするには、管理者は次の手順を実行する必要があります:

1. レジストリエディターを起動します。
2. 次のレジストリパスに移動します:
  - 管理者として:
    - 64 ビットオペレーティングシステムの場合: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
    - 32 ビットオペレーティングシステムの場合: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`

- 管理者以外として:
  - 64 ビットまたは 32 ビットオペレーティングシステムの場合: `\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle`

3. 次の属性でレジストリキーを作成します:

レジストリキー名: EdgeChromiumEnabled

種類: 文字列値

値: True

4. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、フィードバックを共有する機会を提供するためのものです。機能プレビューのサポートケースは受け付けていませんが、機能向上のためのフィードバックはお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。

## Azure AD を使用した条件付きアクセスのサポート [Technical Preview]

このリリースでは、ポリシーが管理者によって構成されている場合、条件付きアクセスを使用して認証できます。

システム要件

Microsoft Edge WebView2 ランタイムバージョン 92 以降。

注:

バージョン 2107 以降、Microsoft Edge WebView2 ランタイムインストーラーは Citrix Workspace アプリのインストーラーとともにパッケージ化されます。Workspace アプリのインストール時、インストーラーが Microsoft Edge WebView2 ランタイムがシステム上に存在するかどうかを確認し、必要に応じてインストールします。

条件付きアクセスを使用した認証の有効化

Azure AD を使用した条件付きアクセスで認証を有効にするには、管理者は次の手順を実行する必要があります:

1. レジストリエディターを起動します。
2. 次のレジストリパスに移動します:
  - 64 ビットオペレーティングシステムの場合: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`

- 32 ビットオペレーティングシステムの場合: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`

3. 次の属性でレジストリキーを作成します:

レジストリキー名: EdgeChromiumEnabled

種類: 文字列値

値: True

4. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

### Workspace アプリ内でのローカルアプリ検出のサポート [Technical Preview]

バージョン 2107 以降、管理者は Citrix Workspace アプリ内にローカルにインストールされたアプリケーションの検出と列挙を構成できます。この機能は、Global App Configuration Service を使用して構成できます。機能の構成については、「[Global App Configuration Service](#)」を参照してください。

この機能は、キオスクモードで実行されているデバイスや、Citrix Workspace 内で仮想化できないアプリケーションに最適です。

注:

Technical Preview は、お客様が非実稼働環境または制限のある稼働環境でテストし、[フィードバック](#)を共有する機会を提供するためのものです。機能プレビューのサポートケースは受け付けていませんが、機能向上のためのフィードバックはお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。

## 2106 の新機能

### Global App Config Service

Citrix Workspace 向けの新しい 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 Workspace アプリの設定を配信できます。

詳しくは、「[Global App Configuration Service](#)」のドキュメントを参照してください。

### Global App Configuration Service による認証トークンの保存を無効にするオプション

Citrix Workspace アプリは、ローカルディスクへの認証トークンの保存を無効にする追加のオプションを提供するようになりました。既存の GPO 構成に加えて、Global App Configuration Service を使用してローカルディスクへの認証トークンの保存を無効にすることもできます。

Global App Configuration Service で、`Store Authentication Tokens`属性を `False` に設定します。

詳しくは、「[Global App Configuration Service](#)」のドキュメントを参照してください。

### サービス継続性

サービス継続性により、接続プロセスに関与するコンポーネントの可用性に依存することがなくなるか、最小限に抑えられます。ユーザーは、クラウドサービスのヘルス状態に関係なく、仮想アプリと仮想デスクトップを起動できます。

詳しくは、Citrix Workspace ドキュメントの「[サービス継続性](#)」セクションを参照してください。

### Microsoft Teams の機能強化

Desktop Viewer が全画面モードの場合、ユーザーは Desktop Viewer がカバーするすべての画面から 1 つを選択して共有できます。ウィンドウモードでは、ユーザーは Desktop Viewer ウィンドウを共有できます。シームレスモードでは、ユーザーはすべての画面から 1 つを選択して共有できます。Desktop Viewer がウィンドウモードを変更（最大化、復元、または最小化）すると、画面共有が停止します。

### Chromium ベースのブラウザでの双方向 URL サポート

コンテンツの双方向リダイレクトを使用すると、サーバーとクライアントのポリシーを使用して、クライアントからサーバーへ、およびサーバーからクライアントへリダイレクトするように URL を構成できます。

サーバーポリシーは Delivery Controller で設定され、クライアントポリシーは、グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して Citrix Workspace アプリで設定されます。

このリリースでは、Google Chrome と Microsoft Edge に URL の双方向リダイレクトのサポートが追加されました。

前提条件:

- Citrix Virtual Apps and Desktops バージョン 2106 以降。
- ブラウザーリダイレクトの拡張バージョン 5.0。

Google Chrome ブラウザーで URL の双方向リダイレクトを登録するには、Citrix Workspace アプリインストールフォルダーから、次のコマンドを実行します:

```
1 %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /  
   verbose
```

Google Chrome ブラウザーで URL の双方向リダイレクトの登録を解除するには、Citrix Workspace アプリインストールフォルダーから、次のコマンドを実行します:

```
1 %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /  
   verbose
```

Citrix Workspace アプリでの URL リダイレクトの構成については、「[コンテンツの双方向リダイレクト](#)」を参照してください。

Web ブラウザーコンテンツのリダイレクトについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Web ブラウザーコンテンツのリダイレクト](#)」を参照してください。

### ICA ファイルのセキュリティの向上 - Technical Preview

以前のリリースでは、Citrix Virtual Apps and Desktops セッションを起動すると、ICA ファイルがローカルディスクにダウンロードされます。

このリリースでは、Citrix Virtual Apps and Desktops セッションの起動時に Citrix Workspace アプリが ICA ファイルを処理する場合のセキュリティが強化されています。

Citrix Workspace アプリでは、ICA ファイルをローカルディスクではなくシステムメモリに保存できるようになりました。この機能は、ローカルに保存されたときに ICA ファイルを悪用する可能性のある攻撃やマルウェアを排除することを目的としています。この機能は、Web 向け Workspace で起動される Citrix Virtual Apps and Desktops セッションにも適用できます。

詳しくは、「[ICA ファイルのセキュリティの向上- Technical Preview](#)」セクションを参照してください。

この機能に関するフィードバックを提供するには、[Podio のフォーム](#)を使用します。

### 2105 の新機能

#### 301 リダイレクトを使用したカスタマイズした URL のサポート

Citrix Workspace アプリでは、HTTP 301 リダイレクトを使用して StoreFront または Citrix Gateway から Citrix Workspace にリダイレクトする URL を追加できるようになりました。

StoreFront から Citrix Workspace に移行する場合は、HTTP 301 リダイレクトを使用して StoreFront URL を Citrix Workspace URL にリダイレクトできます。その結果、古い StoreFront URL を追加すると、Citrix Workspace に自動的にリダイレクトされます。

リダイレクトの例:

StoreFront URL の `https://< Citrix Storefront url>/Citrix/Roaming/Accounts` は、Citrix Workspace URL の `https://<Citrix Workspace url>/Citrix/Roaming/Accounts` にリダイレクトできます。

### Microsoft Teams の機能強化

- メディアトラフィックの優先ネットワークインターフェイスを構成できるようになりました。

`\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` に移動し、`NetworkPreference (REG_DWORD)` という名前でキーを作成します。

必要に応じて、次のいずれかの値を選択します:

- 1: イーサネット

- 2: Wi-Fi
- 3: 携帯ネットワーク
- 5: ループバック
- 6: 任意

デフォルトかつ値が設定されていない場合、WebRTC メディアエンジンは利用可能な最適なルートを選択します。

- オーディオデバイスモジュール 2 (ADM2) を無効にして、従来のオーディオデバイスモジュール (ADM) をクラウドチャンネルマイクに使用できるようになりました。これは、通話中のマイクに関連する問題の解決に役立ちます。

ADM2 を無効にするには、`\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`に移動して`DisableADM2`という名前 (REG\_DWORD) でキーを作成し値を1に設定します。

### 2103.1 の新機能

#### キーボードレイアウト構成の機能拡張

キーボードレイアウト構成に、同期させないオプションが含まれるようになりました。このオプションは、グループポリシーオブジェクト (GPO) ポリシーと GUI 構成の両方で使用できます。

同期させないオプションを選択すると、サーバーのキーボードレイアウトがセッションで使用され、クライアントのキーボードレイアウトはサーバーのキーボードレイアウトに同期されません。

詳しくは、「[キーボードレイアウトと言語バー](#)」を参照してください。

#### 認証トークンの保存を無効にするオプション

認証トークンは暗号化されローカルディスクに保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。

Citrix Workspace アプリは、ローカルディスクへの認証トークンの保存を無効にするオプションを導入します。セキュリティを強化するために、認証トークンストレージを構成するためのグループポリシーオブジェクト (GPO) ポリシーが提供されるようになりました。

注:

この構成は、クラウド展開でのみ適用されます。

詳しくは、「[認証トークン](#)」を参照してください。

### Microsoft Teams の機能強化

- VP9 ビデオコーデックがデフォルトで無効になりました。

- エコーキャンセル、自動利得制御、ノイズ抑制構成の機能強化: Microsoft Teams がこれらのオプションを構成する場合、Citrix リダイレクトの Microsoft Teams は構成された値を優先します。それ以外の場合、これらのオプションはデフォルトで **True** に設定されています。
- **DirectWShow**は現在デフォルトのレンダラーです。

デフォルトのレンダラーを変更するには、次の手順を実行します:

- レジストリエディターを起動します。
- 次のキーの場所に移動します:`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`。
- 次の値を更新します: `"UseDirectShowRendererAsPrimary"=dword:00000000`

その他の設定可能な値:

- \* 0: メディアファンデーション
  - \* 1: DirectShow (デフォルト)
- Citrix Workspace アプリを再起動します。

### 2102 の新機能

#### プロキシ認証のサポート

以前は、プロキシ認証用に構成されたクライアントマシンでプロキシの資格情報が Windows Credential Manager に保存されていない場合、Citrix Workspace アプリに対して認証できませんでした。

このバージョン以降、プロキシ認証用に構成されたクライアントマシンでプロキシの資格情報が Windows **Credential Manager** に保存されていない場合は、認証プロンプトが表示され、プロキシの資格情報の入力を求められます。その後、Citrix Workspace アプリがプロキシサーバーの資格情報を Windows Credential Manager に保存します。これにより、Citrix Workspace アプリにアクセスする前に Windows Credential Manager に資格情報を手動で保存する必要がなくなり、シームレスにログインできます。

#### Microsoft Teams の機能強化

- ビデオレンダリングの強化。
- パフォーマンスと信頼性の向上。

### 2012.1 の新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

### 2012 の新機能

#### イタリア語のサポート

Windows 向け Citrix Workspace アプリがイタリア語で利用できるようになりました。

#### ログ収集

ログ収集では、Citrix Workspace アプリのログを収集するプロセスが簡素化されました。ログは、Citrix でのトラブルシューティングに役立ち、問題が複雑な場合はサポートを容易にします。

GUI を使用してログを収集できるようになりました。

詳しくは、「[ログ収集](#)」を参照してください。

#### Citrix Workspace でのドメインパススルー認証のサポート

このリリースでは、既存の StoreFront のサポートに加えて、Citrix Workspace でドメインパススルー認証がサポートされるようになりました。

#### Citrix Workspace のサイレント認証

Citrix Workspace アプリでは、グループポリシーオブジェクト (GPO) ポリシーが導入され、Citrix Workspace のサイレント認証が有効になります。このポリシーにより、Citrix Workspace アプリがシステムの起動時に Citrix Workspace に自動的にログインできるようになります。このポリシーは、ドメインに参加しているデバイスの Citrix Workspace に対してドメインパススルー (シングルサインオン) が構成されている場合のみ使用してください。

詳しくは、「[サイレント認証](#)」を参照してください。

#### アプリ保護構成の機能強化

以前は、デフォルトで、Authentication Manager と **Self-service Plug-in** のダイアログが保護されていました。

このリリースでは、グループポリシーオブジェクト (GPO) ポリシーが導入され、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に、キーロガー対策および画面キャプチャ対策機能を構成できるようになりました。

#### 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 Gateway Service を使用して制御されます。

詳しくは、「[アプリ保護構成の機能強化](#)」を参照してください。

### Microsoft Teams の機能強化

- ピアに、画面共有セッションで発表者のマウスポインターが表示されるようになりました。
- [WebRTC Media Engine](#) は、クライアントデバイスで構成されたプロキシサーバーを優先するようになりました。

### 2010 の新機能

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

### 2009.6 の新機能

#### FIDO2 認証のサポート

FIDO2 認証により、ユーザーはローカルエンドポイントの FIDO2 コンポーネントを利用できるようになります。ユーザーは、FIDO2 セキュリティキーまたは統合された生体認証を使用して認証できるようになりました。デバイスには、トラステッドプラットフォームモジュール (TPM) 2.0 と Windows Hello が必要です。詳しくは、[FIDO2: WebAuthn & CTAP](#)を参照してください。

### Microsoft Teams の機能強化

- Microsoft Teams は、以前使用した周辺機器を優先デバイスの一覧に表示するようになりました。
- [WebRTC](#)メディアエンジンは、エンドポイントでエンコード可能な最大解像度を正確に判断します。[WebRTC](#)メディアエンジンは、初回の起動時だけでなく、1日に複数回、推定処理を行います。
- Citrix Workspace アプリのインストーラーは、Microsoft Teams の着信音をパッケージ化しています。
- エコーキャンセル機能の向上 - ピアにエコーが発生するスピーカーまたはマイクがある場合のエコーレベルが低下しました。
- 画面共有機能の向上 - 画面共有を行うと、**Desktop Viewer** 画面のみがネイティブビットマップ形式でキャプチャされるようになりました。以前は、**Desktop Viewer** ウィンドウ上に重ねて表示されるクライアントのローカルウィンドウが黒く表示されていました。

### 2009 の新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

### 2008 の新機能

キーボードレイアウトと言語バーのグループポリシーオブジェクト (**GPO**) 管理用テンプレートの構成

既存の GUI による方法に加えて、グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して、キーボードレイアウトと言語バーを構成できるようになりました。

詳しくは、「[キーボードレイアウトと言語バー](#)」を参照してください。

## CryptoKit の更新

Citrix Workspace アプリで、CryptoKit のバージョン 14.2.1 がサポートされるようになりました。

## 言語サポート

Windows 向け Citrix Workspace アプリがポルトガル語（ブラジル）で利用できるようになりました。

## 認証の強化

シームレスなエクスペリエンスを提供するために、Citrix Workspace アプリ内に認証ダイアログが表示されるようになりました。ストアの詳細がログオン画面に表示されます。認証トークンは暗号化され保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。

### 注:

この認証機能強化は、クラウド展開でのみ適用されます。

## アプリ保護の機能強化

以前は、保護されたウィンドウのスクリーンショットを撮影しようとする、バックグラウンドの保護されていないアプリを含む画面全体が黒く表示されていました。

Snipping Tool を使ってスクリーンショットを撮ると、保護されたウィンドウだけが黒く表示されるようになりました。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。

またこのリリースでは、アプリ保護機能を向上させるために問題に対応しています。

## ブラウザコンテンツリダイレクトの機能拡張

- cookie はセッション間で永続的になりました。Web ブラウザーを終了して再起動しても、資格情報の再入力を求められません。
- Web ブラウザーはローカルシステム言語を優先するようになりました。

## 2006.1 の新機能

### Microsoft Teams 画面共有の機能強化

このリリースでは、Microsoft Teams を使用して共有されるコンテンツは、**Desktop Viewer** ウィンドウのコンテンツに限定されます。**Desktop Viewer** ウィンドウ外の領域は切り取られ、Desktop Viewer と重なっているクライアントのローカルアプリが黒く表示されます。

詳しくは、「[画面共有](#)」を参照してください。

## Citrix Analytics Service の更新

Citrix Workspace アプリには、ブラウザーから起動した ICA セッションから Citrix Analytics Service にデータをセキュアに転送するための機能があります。

Citrix Analytics がこの情報を使用する方法については、「[パフォーマンスでのセルフサービス](#)」および「[Virtual Apps and Desktops でのセルフサービス検索](#)」を参照してください。

## 2002 の新機能

### アプリ保護

#### 免責事項

アプリ保護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、このアプリ保護ポリシーは、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きます。引き続きこうした方法に対応していきませんが、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。

アプリ保護は、Citrix Virtual Apps and Desktops の使用時にセキュリティを強化する機能です。この機能により、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性が制限されます。アプリ保護では、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。

#### 注:

保護されたセッションの起動には、ネイティブの Citrix Workspace アプリのみを使用することをお勧めします。

アプリ保護は、StoreFront と Controller の間で構成されます。Controller でのアプリ保護の構成については、Citrix Virtual Apps and Desktops のドキュメントの「[アプリ保護](#)」を参照してください。この構成は、次のいずれかの方法でアプリ保護コンポーネントを含めることで、Citrix Workspace アプリに適用されます:

- GUI
- コマンドラインインターフェイス

Citrix Workspace アプリのインストール時またはオンデマンドインストール時に、アプリ保護コンポーネントを含めることができます。

#### 注:

- この機能は、Windows 10、Windows 8.1、および Windows 7 などの Microsoft Windows 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。
- 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。

Citrix Workspace アプリでのアプリ保護の構成について詳しくは、「[アプリ保護](#)」を参照してください。

### インストーラーの強化

以前のリリースでは、ユーザーがインストールしたアプリのインスタンスを含むシステムに管理者が Citrix Workspace アプリをインストールしようとする、インストールがブロックされていました。

このリリースでは、Citrix Workspace アプリのユーザーがインストールしたインスタンスを管理者が上書きし、インストールを正常に続行できるようになりました。

### Citrix Workspace 更新プログラムの強化

以前のリリースでは、管理者が Citrix Workspace アプリをインストールした場合、管理者以外のユーザーはそのアプリを更新できませんでした。

このリリースでは、管理者以外のユーザーが、管理者がインストールしたインスタンスの Citrix Workspace アプリを更新できます。この処理を行うには、システムトレイ内の Citrix Workspace アプリアイコンを右クリックし、[更新の確認] を選択します。

注:

Citrix Workspace アプリのユーザーがインストールしたインスタンスと管理者がインストールしたインスタンスの両方で、[更新の確認] オプションが使用できるようになりました。

### 送信プロキシのサポート

SmartControl を使用すると、管理者は詳細なポリシーを定義して、Citrix Gateway を使用して Citrix Virtual Apps and Desktops のユーザー環境属性を構成および適用できます。たとえば、ユーザーがドライブをリモートデスクトップにマップできないようにしたい場合があります。Citrix Gateway の SmartControl 機能を使用してこれを実現できます。

ただし、Citrix Workspace アプリと Citrix Gateway が別々のエンタープライズアカウントに属している場合には、シナリオは変わります。このようなシナリオでは、クライアントドメインに Gateway が存在しないため、クライアントドメインは SmartControl 機能を適用できません。代わりに、送信 ICA プロキシを利用できます。送信 ICA プロキシを使用すると、Citrix Workspace アプリと Citrix Gateway が異なる組織に展開されている場合でも、スマートコントロール機能を使用できます。

Citrix Workspace アプリは、Citrix ADC LAN プロキシを使用したセッションの起動をサポートします。単一の静的プロキシを設定することも、送信プロキシプラグインを使用して実行時にプロキシサーバーを選択することもできます。

送信プロキシは、次の方法を使用して構成できます:

- 静的プロキシ: プロキシのホスト名とポート番号を指定してプロキシサーバーを構成します。
- 動的プロキシ: プロキシプラグイン DLL を使用して、1 つ以上のプロキシサーバーから 1 つのプロキシサーバーを選択できます。

グループポリシーオブジェクト管理用テンプレートとレジストリエディターを使用して、送信プロキシを構成できます。

送信プロキシについて詳しくは、Citrix Gateway のドキュメントの「[送信 ICA プロキシのサポート](#)」を参照してください。

送信プロキシの構成について詳しくは、「[送信プロキシのサポート](#)」を参照してください。

### Citrix 組み込みブラウザバイナリ

機能を使用しないように、Citrix 組み込みブラウザバイナリを除外することができるようになりました。

このリリースでは、Citrix 組み込みブラウザバイナリを除外するためのコマンドラインスイッチが導入されました。組み込みブラウザ機能を停止するには、Citrix Workspace アプリのインストール場所から/`InstallEmbeddedBrowser=N`スイッチを実行します。

Citrix 組み込みブラウザバイナリを除外できるのは、次の場合のみです：

- 新規インストール
- Citrix 組み込みブラウザバイナリが含まれていないバージョンからのアップグレード

Citrix Workspace アプリのバージョンに Citrix 組み込みブラウザバイナリが含まれていて、バージョン 2002 にアップグレードする場合には、組み込みブラウザバイナリはアップグレード中に自動的に更新されます。

### Microsoft Teams とのデスクトップ共有の強化

Microsoft Teams を使用してワークスペースを共有する場合、Citrix Workspace アプリは、現在共有されているモニターの領域を囲む赤い枠線を表示します。**Desktop Viewer** ウィンドウのみを共有することも、その上に重ねられたローカルウィンドウを共有することもできます。**Desktop Viewer** ウィンドウを最小化すると、画面共有が一時停止します。

### Microsoft Teams でのエンドポイントエンコーダーのパフォーマンス見積もりツール

`HdxTeams.exe` プロセス（Microsoft Teams のリダイレクトを処理する Citrix Workspace アプリに組み込まれた WebRTC メディアエンジン）を開始すると、エンドポイントの CPU が過負荷状態になることなく維持できる最適なエンコーディングの解像度を見積もります。使用できる値は、240p、360p、720p、1080p です。

`HdxTeams.exe` が初期化されると、パフォーマンスの見積りプロセス（`webrtcapi.EndpointPerformance`とも呼ばれます）が実行されます。マクロブロックコードは、特定のエンドポイントで達成できる最適な解像度を決定します。ピア間、またはピアと会議サーバー間のコーデックネゴシエーション中に、可能な限り高い解像度が使用されます。

エンドポイントエンコーダーの構成について詳しくは、「[エンコーダーのパフォーマンス見積もりツール](#)」を参照してください。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Microsoft Teams の最適化](#)」を参照してください。

## Citrix Analytics Service の機能強化

このリリースの Citrix Workspace アプリには、最新のネットワークホップのパブリック IP アドレスを Citrix Analytics Service にセキュアに送信するための機能があります。このデータは、セッションの起動ごとに収集されます。Citrix Analytics Service は、パフォーマンスの低下に関する問題が特定の地域に関連しているかどうかを分析するのに役立ちます。

デフォルトでは、IP アドレスログは Citrix Analytics Service に送信されます。ただし、レジストリエディターを使用して Citrix Workspace アプリでこのオプションを無効にすることができます。

IP アドレスログの送信を無効にするには、次のレジストリパスに移動し、`SendPublicIPAddress` キーを **Off** に設定します。

- 64 ビット Windows マシンの場合、次のパスです: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`。
- 32 ビット Windows マシンの場合、次のパスです: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`。

### 注:

- IP アドレスの送信はベストエフォートで行われます。Citrix Workspace アプリは起動に使用されるすべての IP アドレスを送信しますが、一部のアドレスは正確でない可能性があります。
- エンドポイントがイントラネット内で動作している閉じられた顧客環境では、URL `https://locus.analytics.cloud.com/api/locateip` がエンドポイントのホワイトリストに登録されていることを確認してください。

パフォーマンス分析がこの情報を使用する方法については、「[パフォーマンスでのセルフサービス](#)」を参照してください。

## 1911 の新機能

### Workspace のインテリジェント機能

このバージョンの Windows 向け Citrix Workspace アプリは、Workspace のインテリジェント機能を使用するように最適化されています。詳しくは、「[Workspace のインテリジェント機能 - マイクロアプリ](#)」を参照してください。

### Citrix Endpoint Management への Windows 10 デバイスの自動登録のサポート

#### 注:

自動登録機能は Technical Preview 段階です。Technical Preview 機能は、Citrix ではテスト環境でのみ使用することをお勧めします。

Citrix Workspace アプリでは、Windows 10 デバイスが Endpoint Management に自動的に登録されるようになりました。

注:

- この機能は、Windows 10 デバイスでのみサポートされています。
- この機能は、クラウド展開でのみ適用できます。

### 1909 の新機能

#### 新しいインストーラスイッチ

このリリースでは、`/forceinstall`と呼ばれる新しいインストーラスイッチが導入されました。

このスイッチは、以下のシナリオで Citrix Workspace アプリの既存の構成およびレジストリエントリをシステム上でクリーンアップするときに使用します。

- Citrix Workspace アプリのサポートされていないバージョンからアップグレードする。
- インストールまたはアップグレードに失敗した。

注:

`/forceinstall`スイッチは、`/rcu`スイッチに置き換わります。

詳しくは、「[一般的なパラメーター](#)」の「インストール」セクションを参照してください。

### 解決された問題

#### 2109.1 で解決された問題

管理者が Google Chrome に外部拡張機能をインストールしている場合、Citrix Workspace Browser を開くとクラッシュします。[CTXBR-2135]

#### 2109 で解決された問題

##### シームレスウィンドウ

一部のサードパーティアプリケーションは前面に残り、起動された他のアプリケーションがバックグラウンドに保持される場合があります。[CVADHELP-16897]

##### ユーザーインターフェイス

Windows 向け Citrix Workspace アプリを使用している場合、[スタート] メニューのショートカットが自動的に更新されないことがあります。この問題は、新しいアプリケーションが追加されたとき、またはバックエンドで変更が加えられたときに発生します。[CVADHELP-17122]

### クライアントデバイスの問題

Citrix Workspace アプリを使用している場合、COM ポートに接続されているデバイスが 9 台を超える場合、セッション内でのマッピングに失敗する可能性があります。[CVADHELP-17734]

### セッション/接続

- Windows 向け Citrix Workspace アプリのバージョン 2106 へのアップグレード後、プロキシサーバーを使用してアプリケーションまたはデスクトップを起動すると、次のエラーメッセージが表示されて失敗する場合があります：

サーバーに接続できません。次のエラーについて、システム管理者に連絡してください：指定されたアドレスで **Citrix XenApp** サーバーが構成されていません（ソケットエラー **10060**） [CVADHELP-18137]

- VDA にインストールされている Windows 向け Citrix Workspace アプリを使用して Web カメラをリダイレクトしようとする、Web カメラが機能しなくなる場合があります。[HDX-28691]
- 仮想デスクトップで Desktop Viewer のツールバーが使用されていない、または Desktop Lock が使用されているときに、マルチモニター設定の Windows 向け Workspace アプリ 2106 以降において、HDX 最適化で Microsoft Teams で画面を共有している場合、画面共有ピッカーが個別モニターのキャプチャに失敗します。代わりに、すべてのモニターが 1 つの合成画像にまとめられます。  
このリリースでは、StoreFront または ICA ファイルで Desktop Viewer が無効になっている場合、または Desktop Lock が使用されている場合、マルチモニターの画面共有機能が無効になります。共有できるのはプライマリモニターのみです。[HDX-34200]

### 2108 で解決された問題

#### ログオン/認証

Citrix Gateway セッションがタイムアウトになった場合、アプリケーションの起動時に Citrix Workspace が認証を要求しないことがあります。[RFWIN-23829]

### 2107 で解決された問題

#### キーボード

アプリ保護がインストールされていると、一部の HP G5 シリーズのノートブックではキーボード入力が機能しない場合があります。[RFWIN-24103]

### セッション/接続

- ドラッグアンドドロップ機能を有効にすると、公開アプリケーションのサイズを変更しようとして失敗する場合があります。[CVADHELP-17089]

- ネットワークプロキシ設定を使用してクライアントと VDA を構成すると、Chrome ブラウザーでブラウザーコンテンツリダイレクトが失敗する場合があります。[CVADHELP-17430]
- シングルサインオンでは、UPN 資格情報を使用してサインインし、エンドポイントでパスワードを変更すると、セッションを開始しようとした後に次のエラーメッセージが表示される場合があります：  
ユーザー名またはパスワードが間違っています。再試行してください。[CVADHELP-17620]
- Microsoft Teams の会議中にビデオ通話を開始すると、Desktop Viewer が応答しなくなる場合があります。[HDX-32435]

### 2106 で解決された問題

#### セッション/接続:

- デフォルトの PDF ビューアとして Google Chrome、Mozilla Firefox、または Microsoft Internet Explorer を使用している場合、Citrix PDF プリンターを使用してファイルを印刷しようとすると失敗することがあります。[CVADHELP-16662]
- Windows 向け Citrix Workspace アプリをバージョン 1912 LTSR CU1 または CU2 にアップグレードした後、セッション画面の保持に失敗する可能性があります。この問題は、Enlightened Data Transport (EDT) プロトコルが有効になっていて、接続が Citrix Gateway を経由している場合に発生します。[CVADHELP-16694]
- VPN を接続または切断すると、Windows 向け Citrix Workspace アプリを使用してアプリケーションを起動できないことがあります。[CVADHELP-16714]
- ダブルホップシナリオでは、エンドポイントクライアント名が Delivery Controller または Director に渡されないことがあります。この問題は、VDA バージョン 2003 以降で発生します。[CVADHELP-16783]
- レジストリ `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` で `CurrentAccount` 値を `AllAccount` に設定すると、機能しない場合があります。この問題は、1 つまたは複数のストアアカウントが存在する場合に発生します。[CVADHELP-17229]
- ユーザー名にウムラウト記号が含まれている場合、Windows 向け Citrix Workspace アプリにログオンしようとするとうまく失敗することがあります。[CVADHELP-17267]
- オンプレミスネットワークでホストされているファイルをダウンロードしようとするとうまく失敗する可能性があります。[CVADHELP-17337]
- 電話会議中に、HDX 最適化モードで Microsoft Teams を使用すると、着信のビデオ部分がちらつく場合があります。[CVADHELP-17398]
- マイクロアプリを使用してファイルをダウンロードしようとするとうまく失敗する可能性があります。[CVADHELP-17438]

#### ユーザーインターフェイス:

- 中国語または日本語の入力システム (IME) を使用してテキストボックスにテキストを入力すると、画面の左上隅にあるテキストボックスの外側にテキストが表示されることがあります。[CVADHELP-15614]
- Citrix Receiver for Windows 4.9.6 を Citrix Workspace アプリにアップグレードした後、アプリケーション

オンをショートカットで起動しようとする、一部のデスクトップでショートカットアイコンが点滅することがあります。[CVADHELP-16967]

- [ping.citrix.com](https://ping.citrix.com)でビーコンチェッカーテストを実行しようとする、失敗する可能性があります。[RFFWIN-22672]
- Windows デバイスで Unicode のユーザー名を使っていて Citrix Workspace アカウントで ASCII のユーザー名を使っているユーザーは、サービス継続性がサポートされない可能性があります。Unicode ユーザー名にキリル文字または東アジア文字が含まれている場合、これらのユーザーの Workspace 接続リソースが起動に失敗します。[RFFWIN-23040、RFFWIN-23046]

### 2105 で解決された問題

#### セッション/接続:

- Windows 向け Citrix Workspace アプリを使用している場合、アプリで保護されたリソースの起動に失敗し、接続画面で停止したままになることがあります。この問題は、Windows Server 2019 などのサーバーオペレーティングシステムにインストールされている Citrix Workspace アプリで発生します。[RFFWIN-22120]
- Git Bash でコマンドを実行しようとする、失敗する可能性があります。この問題は、アプリ保護機能が有効になっている Citrix Workspace アプリで発生します。[RFFWIN-22187]
- 最新バージョンの Citrix Workspace アプリをインストールした後、StoreFront にログオンしたときにアップグレードを求めるプロンプトが表示されることがあります。[RFFWIN-22419]
- Citrix Workspace アプリを終了しようとする、失敗する場合があります。この問題は、ユーザーの資格情報を求めるメッセージが繰り返し表示される場合に発生します。[RFFWIN-22491]
- アプリのデスクトップショートカットを作成してクライアントデバイスを再起動した後、ショートカットからアプリを起動する最初の試みが失敗する場合があります。この問題は、コマンドラインインターフェイスを使用して Citrix Workspace アプリをインストールするときに `storedescription` を指定しない場合に発生します。[RFFWIN-22510]
- Citrix Files からファイルをダウンロードすると、英語以外のファイル名が文字化けして表示されることがあります。[RFFWIN-22516]
- ハードウェアによるスタック保護が有効になっていて、HSP または CET 機能がサポートされている場合、アプリケーションは 11 Generation Intel Core プロセッサおよび AMD Ryzen 5000 シリーズプロセッサで予期せず終了する可能性があります。[RFFWIN-22592]
- HDX アダプティブトランスポートポリシーが優先に設定され、EDT MTU 検出が有効になっている場合、アプリケーションまたはデスクトップを起動しようとしたときに、灰色または黒色の警告メッセージ画面が表示されることがあります。[RFFWIN-22697]
- Windows 向け Citrix Workspace アプリは、アプリケーションの列挙に失敗して、灰色の画面のままになることがあります。これは Intel Iris Xe グラフィックスカードに固有の問題です。[RFFWIN-22952]
- Microsoft Teams のピアツーピアビデオ通話中に、HdxRtcEngine.exe プロセスが応答しなくなる場合があります。この問題は、画面解像度が異なるマルチモニター環境で発生します。[HDX-28616]
- Outlook から Microsoft Teams の会議に参加すると、受信ビデオが機能しない場合があります。この問題は、Microsoft Teams を起動せずに会議に参加すると発生します。[HDX-29558]

- Microsoft Teams の会議中に、ビデオの上にマウスポインターを置くと、ビデオ画面がちらつくことがあります。[HDX-29668]

システムの例外:

- gfxrender.dll モジュールに障害がある場合、Wfica32.exe プロセスが予期せずに終了する場合があります。[RFIN-22446]

セキュリティの問題:

- 管理者がインストールした Citrix Workspace アプリのインスタンスでは、管理者以外の権限を持つユーザーが権限レベルを昇格できる場合があります。詳しくは、Citrix Knowledge Center の [CTX307794](#) を参照してください。

### 2103.1 で解決された問題

ログオン/認証:

- [サインインしたままにする] および [今後 60 日間はこのメッセージを表示しない] ポリシーを有効にした場合でも、Microsoft Azure 多要素認証が認証を要求することがあります。

注:

ユーザーは、ストアからログオフするのではなく、ストアを終了することをお勧めします。ユーザーが Web ビュー認証を使用してストアからログオフすると、Internet Explorer の Cookie がクリアされるため、再度認証を求められる場合があります。デフォルトでは、修正が有効になっています (Cookie が保存されます)。GPO オプションを使用して、修正を無効にすることができます。修正を無効にすると、Cookie は保存されずログオフ中にクリアされます。

[CVADHELP-14814]

- Azure Active Directory (AD) に参加しているデバイスで、Citrix Workspace アプリがストアにアクセスしようとしてエンドポイントのログオン資格情報を渡すと、ユーザーにログオンが許可されない場合があります。また、別のユーザーアカウントでログオンするオプションはありません。[CVADHELP-14844]

セキュリティの問題:

- この修正により、基本コンポーネント内のセキュリティが向上します。[RFIN-20912]

セッション/接続:

- ネイティブの Windows 向け Citrix Workspace アプリ経由で公開デスクトップを起動すると、ネイティブの Citrix Workspace アプリがデスクトップのフォアグラウンドで自動的に実行されます。この問題は、ローカルアプリアクセス機能が有効になっている場合に発生します。[CVADHELP-15654]
- プロキシサーバーがポート 8080 を使用しないシナリオでは、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。この問題は、Windows 向け Citrix Workspace アプリがプロキシポートの使用に失敗し、代わりにデフォルトポートの 8080 を使用する可能性があるために発生します。[CVADHELP-15977]

- Windows 向け Citrix Workspace アプリは、プロキシの種類の設定を無視することがあります。この問題は、英語版以外の Microsoft Windows オペレーティングシステムで発生します。[CVADHELP-16017]
- ユーザーセッションで **ALT+Tab** キーを押すと、Windows 向け Citrix Workspace アプリの新しい空白のウィンドウが開く場合があります。[CVADHELP-16379]
- 保護されたウィンドウが最小化されていると、**Print Screen** キーでスクリーンショットがキャプチャされない場合があります。[RFIN-16777]
- Microsoft Teams の通話で Web カメラまたはビデオを使用している場合、**HDXrtengine.exe**が応答しなくなることがあります。この問題を回避するには、Knowledge Center の記事[CTX296639](#)を参照してください。[HDX-29122]
- IME を使用して DBCS テキストを作成しようとする、下線が欠落する可能性があります。この問題は、Windows 10 2004 オペレーティングシステムで発生します。[RFIN-20006]
- **C:\ProgramData\Citrix**フォルダーに権限を誤って設定すると、Citrix Workspace アプリが予期せず終了する可能性があります。[RFIN-22753]
- Microsoft Teams の通話で、音声途切れる可能性があります。この問題は、UDP トラフィックポートが無効になっている場合に発生します。[HDX-27914]
- Microsoft Teams のビデオ通話中に、カメラの LED が点滅し、プレビュービデオが停止する場合があります。[CVADHELP-16383]

### ユーザーインターフェイス:

- [終了] オプションを 1 回クリックしても、Windows 向け Citrix Workspace アプリが閉じない場合があります。この問題を回避するには、[終了] オプションを 2 回選択して Workspace アプリを閉じます。[RFIN-21518]

## 2102 で解決された問題

### セッション/接続:

- vPrefer オプションを有効化した Citrix Workspace アプリを使用して、公開デスクトップの「お気に入り」からアプリケーションを開こうとすると、アプリケーションが回転する円とともに開くことがあります。回転する円が残る場合は、アプリケーションを再度開くことができません。[CVADHELP-13237]
- vPrefer オプションを有効にすると、App-V アプリケーションがローカルサーバーではなくリモートサーバーで起動することがあります。[CVADHELP-15356]
- アプリケーション名が繁体字中国語または日本語で指定されている場合、**StoreBrowse.exe**コマンドで公開アプリケーションの完全な一覧が表示されないことがあります。[CVADHELP-15952]
- **EnableFactoryReset**レジストリ設定が**False**に設定されている場合、Citrix Workspace アプリをアンインストールしようとする、次のエラーメッセージが表示されて失敗することがあります:  
  
この機能は無効になりました。  
  
[CVADHELP-16114]
- ログ収集機能により、CDF トレースが収集できないことがあります。[CVADHELP-16587]

システムの例外:

- `Receiver.exe` プロセスが、予期せずに終了する場合があります。 [CVADHELP-15669]

ユーザーインターフェイス:

- 中国語または日本語の入力システム (IME) を使用してテキストボックスにテキストを入力すると、画面の左上隅にあるテキストボックスの外側にテキストが表示されることがあります。 [CVADHELP-15614]

### 2012.1 で解決された問題

- バージョン 2012 からそれ以降のバージョンへの Citrix Workspace アプリの自動更新は失敗し、次のエラーメッセージが表示されます:

“Could not load file or assemble Newtonsoft.Json” (ファイルを読み込めなかったか、Newtonsoft.Json をアセンブリできませんでした)

この問題は、管理者がインストールした Citrix Workspace アプリのインスタンスで自動更新が有効になっている場合にのみ発生します。

この問題を回避するには、Citrix [ダウンロード](#) ページから Citrix Workspace アプリバージョン 2012.1 以降をダウンロードし、手動でインストールします。

[RFIN-21715]

### 2012 で解決された問題

インストール、アンインストール、アップグレード:

- 手動で作成したショートカットを使用して Citrix Workspace アプリを更新しようとする、ショートカットが削除されてから再作成される場合があります。 [CVADHELP-15397]

セッション/接続:

- マルチモニター環境では、ユーザーセッションを最大化しようとする、失敗する場合があります。この問題は、ノートブックを再接続すると発生します。 [CVADHELP-13614]
- 次のいずれかを実行すると、[セキュリティ警告] ダイアログが表示される場合があります:
  - Storebrowse コマンドを使用して、StoreFront から ICA ファイルを取得する。
  - ブラウザーからではなく、ICA ファイルを使用してアプリケーションを起動する。

[CVADHELP-15221]

- ダブルホップシナリオでは、[スタート] メニューのショートカットを使用してアプリケーションを起動しようとする、失敗することがあります。この問題は、1 ユーザーにつき 1 つのインスタンスのアプリケーション制限を有効にした場合に発生します。 [CVADHELP-15576]

- セッションの確立時にすべてのストアアカウントに接続するように Windows 向け Citrix Workspace アプリを構成します。Citrix Workspace アプリからログオフして再度ログオンすると、ストアアカウント設定が、デフォルトですべてのアカウントに設定されず、1 つのストアアカウントに変更されます。[CVADHELP-15728]
- Microsoft Teams の通話で画面を共有しようとする、黒い画面が表示される場合があります。[HDX-27041]

### ユーザーエクスペリエンス:

- Windows 向け Citrix Workspace アプリを新規インストールした後、または既存のインストールを最新のものにアップグレードした後、セッションを起動しようとする、失敗する場合があります。セッションの起動が「デスクトップを準備しています」画面で停止します。この問題は、Citrix Gateway URL を使用して Desktop Lock を構成するときに発生します。

#### 注:

Citrix Gateway URL と Desktop Lock を使用して Windows 向け Citrix Workspace アプリを初めて構成するときに、Desktop Lock が表示されるまでしばらくの間黒い画面が表示されます。黒い画面が長時間続く場合、物理マシンの場合は Ctrl+Alt+Delete を使用して、仮想マシンの場合は Ctrl+Alt+End を使用してサインアウトします。

[CVADHELP-15334]

- 高 DPI が [はい] または [いいえ] に設定されている場合、デスクトップセッションを起動すると、**CD Viewer** ツールバーの一部の要素が、デバイスの現在の DPI 設定に合わせてスケールアップしないことがあります。この問題は、ユーザーデバイスの DPI 設定が 100% より大きい場合に発生します。[CVADHELP-15418]
- Citrix Workspace アプリをバージョン 1912 からバージョン 1912 CU1 にアップグレードした後、アプリケーションの列挙が遅くなり、完了までに約 10 分かかる場合があります。[CVADHELP-15766]

## 2010 で解決された問題

### キーボード

- 日本語キーボードを使用している場合、ローカルデバイスで起動した Microsoft Excel で全角入力モードが機能しないことがあります。この問題は、アプリ保護機能が有効になっている場合に発生します。[CVADHELP-15410]

### セッション/接続

- Windows 向け Citrix Workspace アプリをバージョン 2006 からバージョン 2008 以降にアップグレードしようとする、失敗することがあります。この問題は、英語以外（スウェーデン語など）の数値形式を実行しているマシンで発生します。[CVADHELP-15988]
- アプリ保護機能を有効にすると、**Pause/Break** および **NumLock** キーが正しくマップされない可能性があります。[RFWIN-20083]

- Windows 向け Citrix Workspace アプリで、ストア URL を使用してクラウドアカウントを追加すると、次のエラーメッセージが表示されることがあります：

「サーバーに接続できません」

この問題は、URL に大文字が含まれている場合に発生します。

[RFIN-20907]

- Microsoft Teams の最適化：マルチモニター環境または単一の高 DPI モニターでは、発信画面共有が正しく機能しないことがあります。他方のピアには、代わりに黒い画面が表示されます。[RFIN-20854]
- Windows 向け Citrix Workspace アプリの通知領域で [ヘルプ] をクリックすると、ヘルプのページが英語ではなく繁体字中国語で表示されます。[RFIN-21069]

### 2009.6 で解決された問題

- VPN を使用して Citrix Workspace アプリに接続し、[アプリ一覧の更新] オプションを選択すると、更新操作が失敗する場合があります。[CVADHELP-14418]
- セルフサービスモードを構成せずに Citrix Workspace アプリをインストールしようとする、例外が発生する場合があります。この問題は、[高度な設定] シートから [ショートカットと再接続] メニューを開いたときに発生します。この問題は、Citrix Workspace アプリのバージョン 1907~2002 で発生します。[CVADHELP-14940]
- レジストリ編集ツールを無効にすると、アップグレードを実行した後、以前インストールされたレジストリキーが保持されない場合があります。その結果、デスクトップを起動しようとする失敗します。[CVADHELP-15104]
- Microsoft Teams の公開インスタンスが実行されているセッションで画面を最大化しようとする、失敗する場合があります。[RFIN-20051]
- デスクトップセッションが断続的に応答しなくなったり、切断されたりする場合があります。この問題は、[音質] オプションを [中] に設定し、Delivery Controller でエコーキャンセル機能を有効にすると発生します。[RFIN-20557]
- Citrix Workspace アプリをアップグレードした後、複数の Workspace アプリのアイコンが通知領域に表示される場合があります。[RFIN-20589]
- ネットワーク上の共有フォルダーにアクセスしようとする、**Windows** セキュリティの認証プロンプトが表示されない場合があります。[RFIN-20599]
- クラウド環境では、プロキシ認証を使用してストアに接続しようとしても機能しない場合があります。[RFIN-20673]
- クラウド展開で既存のストアに接続しようとする失敗し、次のエラーメッセージが表示されることがあります。  
「サーバーに接続できません。」

この問題は、Citrix Workspace アプリをアップグレードした後に発生します。この問題を回避するには、Citrix Workspace アプリをリセットするか、ストアアカウントを削除して再度追加します。[RFIN-20834]

### 2009 で解決された問題

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

### 2008 で解決された問題

インストール、アンインストール、アップグレード

- 自動更新機能を使用して、HDX RealTime Media Engine (RTME) と Citrix Workspace アプリを自動的に更新しようとする場合、失敗する場合があります。RTME を最新バージョンにアップグレードできません。[CVADHELP-15047]

ログオン/認証

- Citrix Workspace アプリを介してシングルサインオン (SSO) をサポートするように Citrix Gateway を構成すると、SSO が失敗する場合があります。この問題は、ユーザー名またはパスワードに %、=、& などの特殊文字が含まれている場合に発生します。[CVADHELP-14564]

セッション/接続

- Citrix Workspace アプリにログオンせずに [スタート] メニューから公開アプリケーションを起動すると、2つのウィンドウが表示され、Citrix Workspace アプリにログオンするように求められます。この問題は、CitrixReceiver.exe コマンドを使用して PNA アドレスを STORE0 として構成した場合に発生します。[CVADHELP-13916]
- Citrix Workspace アプリで vPrefer オプションを有効にすると、App-V アプリケーションの起動に失敗して、次のエラーメッセージが表示されることがあります：  
起動できません  
[CVADHELP-14039]
- Citrix Workspace アプリのアップグレード後、廃止される機能である HDX MediaStream for Flash に関連したレジストリ値 (Flash および Flash2 など) が、レジストリ設定 (HKEY\_LOCAL\_MACHINE \SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0\VirtualDriver) から削除されない場合があります。この問題は、接続エラーを引き起こす可能性があります。[CVADHELP-14850]
- Citrix Workspace アプリを使用すると、Self-service ウィンドウに断続的に空白の画面が表示されることがあります。[RFIN-17563]

### ユーザーエクスペリエンス

- Windows 向け Citrix Workspace アプリでストア URL を使用してアカウントを追加すると、完了までに時間がかかる場合があります。この問題は、URL にポート番号が含まれている場合に発生します。[CVADHELP-14051]

### 2006.1 で解決された問題

#### コンテンツリダイレクト

- ブラウザーコンテンツリダイレクト (BCR) を有効にすると、ページの更新後、入力フィールドにテキストを入力できなくなることがあります。この問題は、シームレスセッションで発生します。[CVADHELP-12922]
- 長い URL をリダイレクトしようとする、URL が VDA にリダイレクトされず、Redirector.exe プロセスが次の例外で予期せず終了することがあります。

INVALID\_CRUNTIME\_PARAMETER

[CVADHELP-13197]

#### セッション/接続

- ストリーミングメディアを起動して終了すると、セッションでオーディオが使用できなくなります。[CVADHELP-13297]
- 2 つの異なるアカウントを使用して Windows 向け Citrix Workspace アプリに 2 つのストアを追加すると、プライマリストアを削除した後、セカンダリストアでサインインボタンが機能しないことがあります。[CVADHELP-13805]
- ダブルホップシナリオでは、セッションを起動しようとする、Citrix HDX Engine が予期せず終了することがあります。[CVADHELP-13915]
- 多要素認証が有効で、Windows セキュリティダイアログボックスを使用してログインする場合、ストアへの認証時に Active Directory フェデレーションサービス (ADFS) ダイアログボックスは表示されません。[CVADHELP-14316]
- アプリの保護が有効になっている場合でも、セッションのスクリーンショット撮影に成功することがあります。[RFWIN-17455]

#### システムの例外

- セッションへ接続しようとする、wfica32.exe プロセスが予期せず終了する場合があります。この問題は、Windows 向け Citrix Workspace アプリのバージョン 1904.1 で発生します。[CVADHELP-12807]

#### ユーザーインターフェイス

- アプリケーションが、現在のアプリケーションに代わって前面に移動しようと断続的に試みることがあります。タスクバーのアイコンが点滅し、アプリケーションが前面への移動を試みていることをユーザーに通知する場合があります。[CVADHELP-13071]
- ローカルアプリアクセスで起動されたアプリケーションを最小化すると、アプリケーションのアイコンがタスクバーに表示されないことがあります。[CVADHELP-13293]
- Windows 向け Workspace アプリの余分なアイコンが、システムトレイに表示されることがあります。[RFIN-17499]

### 2002 で解決された問題

#### Windows 向け Citrix Workspace アプリ 1911との比較

#### HDX MediaStream Windows Media リダイレクト

- マルチモニター環境では、ユーザーセッションで Windows Media Player を使用して MP4 ビデオを再生すると、ビデオがプライマリモニターで正しく再生されます。ただし、プレーヤーを別の画面に移動すると、ドッキングステーションを使用して DisplayLink 経由で接続されたセカンダリモニターまたは拡張モニターに黒い画面が表示される場合があります。[CVADHELP-11848]

#### セッション/接続

- 高速スマートカードを使用して HDX RealTime Media Engine からセッションに再接続しようとする、HDX RealTime Media Engine が予期せず終了する場合があります。[CVADHELP-12605]
- 公開アプリケーションが短期間に短い音を再生するための要求を多数受信すると、wfica32.exe プロセスが予期せず終了する場合があります。[CVADHELP-12855]
- セッションがタイムアウトになると、自動的にログオフする場合があります。セッションを再度起動しようすると、セッションの起動に通常より時間がかかります。この問題は、ネットワークが中断したときに発生します。[CVADHELP-13017]
- ローカルアプリアクセスと Desktop Lock を有効にした場合、Ctrl+Alt+Del キーを押した後にユーザーの切り替え機能を実行すると、ローカルユーザーセッションが再接続されることがあります。ただし、サーバーセッションが再接続しようとする、VDA が白い画面で表示され、デスクトップに接続されたことを示すメッセージが表示されます。デスクトップは表示されません。[CVADHELP-13046]
- シームレスアプリケーションウィンドウは、部分的に欠けた状態になり、手動でウィンドウのサイズを変更するまで欠けたままになることがあります。[CVADHELP-13108]
- Workspace アプリが、更新または起動するたびに、ショートカットアイコンの有無をチェックするようになりました。アイコンがない場合、Workspace アプリは再びアイコンを取得します。これにより、ショートカットが適切に表示されます。[RFIN-15501]
- 双方向コンテンツのリダイレクトポリシー ([コンピューターの構成] > [管理用テンプレート] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザーエクスペリエン

ス]) を有効にしようとする、URL 固有のアプリケーションまたはデスクトップの上書きを有効にしていなくても、URL 固有のエントリの入力を求められます。[RFWIN-15867]

#### システムの例外

- CDF トレースのキャプチャ中に、Receiver.exe プロセスが予期せず終了することがあります。[CVADHELP-13077]

#### 1911 で解決された問題

##### コンテンツリダイレクト

- コンテンツの双方向リダイレクトポリシーを有効にすると、ユーザーデバイスで実行されている Internet Explorer がユーザーのタスクバーに表示されることがあります。また、Internet Explorer ブラウザーのウィンドウは前面に表示されません。[LD1924]

##### インストール、アンインストール、アップグレード

- Citrix HDX RealTime Media Engine プラグインがインストールされている場合、Citrix Receiver for Windows をバージョン 4.9 LTSR 累積更新プログラムにアップグレードすると、セッションを開始することができません。[LD1814]

##### シームレスウィンドウ

- 公開アプリケーション内で新しいウィンドウを開くと、公開アプリケーションのアイコンがタスクバーから消える場合があります。[LD1868]

##### セッション/接続

- ローカルアプリアクセスまたは Desktop Lock を有効にすると、セッションの起動に失敗することがあります。Citrix ログオン画面に、[ログオフ] ボタンと [切断] ボタンとともに「お待ちください」メッセージが表示されます。また、画面が数秒間ちらつき、ちらつきが収まっても「お待ちください」メッセージは残ります。[LD1124]
- ネットワークの停止後にクライアントの自動再接続機能 (ACR) がセッションの再接続を完了すると、元のクライアントマシンの解像度が予期せずユーザーセッションに適用される場合があります。この問題は、ユーザーデバイスで DPI が 100% に設定されておらず、**[Windows 向け Workspace アプリ] > [高度な設定] > [高 DPI]** ページで [はい] を選択した場合に発生します [LD1423]
- Citrix Workspace アプリで Vprefer オプションを有効にすると、公開アプリケーションがローカルで起動することがあり、次の 2 つの問題が発生する可能性があります:

- システム環境は拡張されません。たとえば、コマンドラインパラメーター%computername% は、ローカルクライアントで PC12345 に展開されません。システム環境変数は展開されません。たとえば、コマンドラインパラメーター%computername% は、ローカルクライアントマシンで PC12345 に展開されません。
- コマンドラインパラメーターはクライアントに戻されません。たとえば、selfservice.exe -qlaunch IE11 <http://www.citrix.com>を使用すると、コマンドラインパラメーターは「Iexplore.exe %\*」として渡され、クライアントに戻されません。

[LD1450]

- 高速スマートカードを使用して HDX RealTime Media Engine からセッションに再接続しようとする、HDX RealTime Media Engine が予期せず終了する場合があります。[LD1655]
- Windows 向け Citrix Workspace アプリを使用してデスクトップを最小化、最大化、またはサイズ変更すると、灰色の画面がデスクトップに重なって表示されることがあります。[LD1656]
- Plantronics Blackwire 320 USB ヘッドセットは、USB 2.0 ポートに接続すると、Citrix Workspace の基本設定のデバイス一覧に表示されなくなることがあります。この問題は、最適化モードと一般モードの切り替えを繰り返すと発生します。[LD1864]
- ダブルホップシナリオの第 1 ホップで VDA for Desktop OS が実行され、第 2 ホップで公開アプリケーションが実行されている場合、このエラーメッセージが表示されることがあります：

**Citrix HDX Engine has stopped working.**

**Exception caused the program to stop working correctly. Please close the program.**

この問題は、サードパーティ製アプリケーションをカスタム仮想チャネルで使用し、別のクライアントデバイスから第 1 ホップデスクトップを再接続または取得するときに発生します。

[LD1898]

- 特定のサードパーティアプリケーションがシームレスアプリケーションとして正常に機能しない場合があります。この問題は、ウィンドウスタイル（たとえば、WS\_DISABLED）が正しく適用されていない場合に発生します。[LD1912]
- ローカルアプリアクセスを有効にした場合、ローカルにインストールされたサードパーティアプリケーションを起動すると、次の問題が発生することがあります：
  - Desktop Lock を有効にした場合、アプリケーションが最大化または画面の右上隅に最小化することがあります。タスクバーのアプリケーションアイコンをクリックすると、アプリケーションを復元できます。
  - Desktop Lock を無効にした場合、小さな認証ダイアログウィンドウなどのセカンダリウィンドウにフォーカスを合わせる必要があります。ただし、メインウィンドウは常に一番上にあり、セカンダリウィンドウはメインウィンドウの後ろに隠れています。デスクトップをウィンドウモードに設定するまで、セカンダリウィンドウはフォーカスされません。

[LD1979]

- シームレスアプリケーションウィンドウは、部分的に欠けた状態になり、手動でウィンドウのサイズを変更するまで欠けたままになることがあります。[LD2124]
- SelfServiceMode フラグを false に設定した場合、Citrix Studio でアプリケーションを無効にしても、ショートカットが [スタート] メニューに表示され続けることがあります。[LD2126]

### システムの例外

- CtxUsbm.sys で Driver Verifier を有効にすると、CtxUsbm.sys のメモリリークによりブルースクリーンが発生することがあります。開発ツールである Driver Verifier は、実稼働環境で使用しないでください。[LD1973]

## 1909 で解決された問題

### セッション/接続

- ダブルホップシナリオの第 1 ホップで VDA for Desktop OS が実行され、第 2 ホップで公開アプリケーションが実行されている場合、このエラーメッセージが表示されることがあります:

「Citrix HDX Engine has stopped working.

Exception caused the program to stop working correctly. Please close the program.」

この問題は、サードパーティ製アプリケーションをカスタム仮想チャネルで使用し、別のクライアントデバイスから第 1 ホップデスクトップを再接続または取得するときに発生します。[LD0479]

- 1 台のモニターを閉じて、モニター数を 3 から 2 に減らしてからアプリケーションを最小化して最大化します。白い画面が 2 つ表示されることがあります。この問題は、ノートブックの解像度が他のモニターの解像度と異なる場合に発生します。また、ノートブックをドッキングまたはドッキング解除すると問題が発生します。[LD1558]
- Windows 向け Citrix Workspace アプリ 1902 以降を使用する場合、公開アプリケーションからエンドポイントにテキストをコピーしようとするとうまく失敗することがあります。[LD1972]
- HDX Optimization for Microsoft Teams を使用している場合、User1 が User2 とビデオ通話を開始し、User2 とデスクトップを共有すると、User2 に共有デスクトップではなくビデオアーティファクトが表示されることがあります。[RFWIN-11863]
- HDX Optimization for Microsoft Teams を使用している場合、User1 が User2 とのビデオ通話を開始すると、両方のユーザーが互いの音声と映像を受信できます。ただし、User1 が User2 とデスクトップの共有を開始すると、User2 には共有デスクトップではなく灰色の画面が表示されることがあります。この問題は、AMD クライアントで通話が確立されたときに発生します。[RFWIN-11866]
- HDX Optimization for Microsoft Teams を使用している場合、User1 が User2 とビデオ通話を開始し、User3 をビデオ通話に追加すると、User1 のビデオ画面が黒くなるがあります。その結果、すべてのユーザーに黒いビデオ画面が表示されます。[RFWIN-11875]

- HDX Optimization for Microsoft Teams を使用している場合、User1 がアプリケーションの公開インスタンスから User2 とのビデオ通話を開始し、User2 とデスクトップを共有すると、User2 には User1 の画面ではなく黒い画面のみが表示されることがあります。[RFWIN-11952]
- レジストリパス `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\HotKeys` で、`EnableCtrlAltEnd` 属性の `DWORD` 値が 1 に設定されている場合、公開デスクトップを起動できません。[RFWIN-12091]
- HDX Optimization for Microsoft Teams を使用している場合、HDXTeams.exe プロセスを終了するまで、会議や通話中に Desktop Viewer の表示ウィンドウが応答しなくなることがあります。[RFWIN-15231]

### ユーザーエクスペリエンス

- 複数のアプリケーションの実行中にアプリケーションアイコンの上にマウスポインターを合わせると、タスクバーのプレビューにアクティブなウィンドウのコンテンツだけが表示されることがあります。  
注: クライアントが Flash または Windows Media リダイレクトをレンダリングしている場合、タスクバーのプレビューが正しく機能しないことがあります。[LD1030]
- クライアント名に基づいたアプリケーションの列挙とフィルタリングは、統合エクスペリエンスを有効にしたネイティブの Citrix Receiver では機能しない場合があります。[LD1427]
- Internet Explorer から VDI デスクトップを起動し、マウスポインターを VDI デスクトップウィンドウに移動すると、VDI デスクトップフレームからフォーカスが失われ、マウスポインターがフレームの後ろに隠れることがあります。[LD1486]

### 既知の問題

#### 2109.1 の既知の問題

このリリースで確認されている新しい問題はありません。

#### 2109 の既知の問題

ユーザーとして 2109 より前のバージョンの Workspace アプリをインストールしていて、管理者がバージョン 21.0.9 をインストールした場合、ユーザーとしてデバイスに再度ログインすると、[エントリポイントが見つかりません] というエラーメッセージが表示されます。[OK] をクリックすると、メッセージが消え、Workspace アプリがバージョン 21.0.9 に更新されます。[RFWIN-25008]

管理者が Google Chrome に外部拡張機能をインストールしている場合、Citrix Workspace Browser を開くとクラッシュします。[CTXBR-2135]

### 2108 の既知の問題

ユーザー名にキリル文字または東アジア言語の文字が含まれている場合、クライアントマシンでセッションをオフラインモード（サービス継続性）で起動できません。[RFFWIN-23906]

### 2107 の既知の問題

このリリースで確認されている新しい問題はありません。

### 2106 の既知の問題

- サービス継続性機能が有効になっているストアでは、リソースを起動できない場合があります。この問題は、Unicode ユーザーで発生します。[RFFWIN-23439]
- VDA にインストールされている Windows 向け Citrix Workspace アプリを使用して Web カメラをリダイレクトしようとする、Web カメラが機能しなくなる場合があります。[HDX-28691]

### 2105 の既知の問題

- セッション中に [更新をチェック] をクリックすると、更新が正常にダウンロードされ、現在のセッションが [ダウンロードが完了しました] ダイアログボックスの一覧に表示されません。[RFFWIN-23152]

### 2103.1 での既知の問題

- Self-service Plug-in ウィンドウが空白で、セッションの起動時にアプリが表示されません。この問題は、Intel Xe グラフィックカードを使用している場合に発生します。これはサードパーティの制限事項によるものです。[CVADHELP-17005]
- 日本語、中国語、または韓国語の IME で文字を作成しようとする、正しく機能しない場合があります。テキスト作成ウィンドウが適切に配置されず、シームレスではありません。この問題は、CVAD セッションと SaaS アプリを使用している場合は発生しません。[RFFWIN-21158]
- Citrix Workspace アプリを終了しようとする、失敗する場合があります。この問題は、ユーザーの資格情報を求めるメッセージが繰り返し表示される場合に発生します。[RFFWIN-22491]
- アプリのデスクトップショートカットを作成してクライアントデバイスを再起動した後、ショートカットからアプリを起動する最初の試みが失敗する場合があります。この問題は、コマンドラインインターフェイスを使用して Citrix Workspace アプリをインストールするときに `storedescription` を指定しない場合に発生します。[RFFWIN-22510]
- Citrix Files から .txt ファイルをダウンロードすると、日本語のファイル名が文字化けして表示される場合があります。[RFFWIN-22516]
- Microsoft Teams HDX 最適化を使用してピアツーピア通話を試行する場合、VDA のバージョンが 2103 以下で、Windows 向け Workspace アプリが 2103 以降の場合、通話が失敗することがあります。この問題は、Virtual Delivery Agent (VDA) 2106 で解決されています。

## 2102 の既知の問題

- ICA セッションを起動できないことがあります。この問題は、プロキシサーバーがカスタムポートではなくポート 8080 を使用している場合に発生します。[CVADHELP-15977]
- アプリケーションセッション内で、Microsoft Paint でスキャンする画像を開くと、Microsoft Paint アプリケーションとスキャンプロセスの両方が応答しなくなることがあります。この問題は、ウィンドウモードでセッションを起動したときに発生します。[RFFWIN-21413]
- Azure Active Directory 多要素認証 (MFA) を使用するように構成されたマシンで、[サインインしたままにする] および [今後 60 日間はこのメッセージを表示しない] ポリシーを両方とも選択した場合でもログインを求めるメッセージが表示されます。[RFFWIN-21623]
- Azure Active Directory に参加しているマシンで Citrix Workspace アプリにログインしようとするとき失敗することがあります。この問題は、認証プロンプトが表示されない場合に発生します。[RFFWIN-21624]
- 公開デスクトップセッションを起動すると、Self-service Plug-in ダイアログが前面に表示されます。この問題は、Delivery Controller で [ローカルアプリアクセス] ポリシーが有効になっている場合に発生します。[RFFWIN-21629]
- **ALT+Tab** キーを使ってウィンドウを切り替えようとするとき、Citrix Workspace アプリの画面が空白になることがあります。この問題は、ウィンドウモードでセッションを起動したときに発生します。[RFFWIN-21828]
- Microsoft Teams の通話で Web カメラまたはビデオを使用している場合、**HDXrtengine.exe** が応答しなくなることがあります。この問題を回避するには、Knowledge Center の記事 [CTX296639](#) を参照してください。[HDX-29122]

## 2012.1 の既知の問題

このリリースで確認されている新しい問題はありません。

## 2012 の既知の問題

- 保護されたアプリを「お気に入り」に追加しようとするとき、「現在アプリケーションを使用できません...」というメッセージが表示される場合があります。[OK] をクリックすると、「アプリケーションを追加できません。」というメッセージが表示されます。[お気に入り] 画面に切り替えた後、保護されたアプリはここに一覧表示されますが、[お気に入り] から削除することはできません。[WSP-5497]
- Chrome Web ブラウザーで Web ブラウザーのコンテンツのリダイレクトが有効になっている場合、新しいタブを開くリンクをクリックしてもタブが開かないことがあります。この問題を回避するには、**Pop-ups blocked** メッセージで **Always allow pop-ups and redirects** を選択します。[HDX-23950]
- バージョン 2012 からそれ以降のバージョンへの Citrix Workspace アプリの自動更新は失敗し、次のエラーメッセージが表示されます：  
“Could not load file or assemble Newtonsoft.Json” (ファイルを読み込めなかったか、Newtonsoft.Json をアセンブリできませんでした)

この問題は、管理者がインストールした Citrix Workspace アプリのインスタンスで自動更新が有効になっている場合にのみ発生します。

この問題を回避するには、Citrix [ダウンロード](#) ページから Citrix Workspace アプリバージョン 2012.1 以降をダウンロードし、手動でインストールします。

[RFWIN-21715]

- アプリバーを起動してから、Windows 向け Citrix Workspace アプリでコネクションセンターメニューを開くと、アプリバーがホストサーバーの下に表示されません。[HDX-27504]
- Windows 向け Citrix Workspace アプリを使用していて、アプリバーを縦向きで起動すると、バーが [スタート] メニューまたはシステムクロックトレイに重なって表示されます。[HDX-27505]

### 2010 の既知の問題

このリリースで確認されている新しい問題はありません。

### 2009.6 の既知の問題

- Citrix Workspace アプリの画面を最小化または最大化しようとする、画面が一瞬歪む場合があります。[RFWIN-20692]

### 2009 の既知の問題

このリリースで確認されている新しい問題はありません。

### 2008 の既知の問題

- 保護されたウィンドウが最小化されていると、**Print Screen** キーでスクリーンショットがキャプチャされない場合があります。この問題が発生したら、Citrix Workspace アプリを終了して再起動します。[RFWIN-16777]
- 管理者以外のユーザーが FastConnect API を使用してログインすると、空白の Self-service ウィンドウが表示されます。この問題が発生した場合は、クライアントデバイスを再起動してください。[RFWIN-19804]
- 保護された VDA セッションを起動し、保護されていない VDA でスクリーンショットをキャプチャしようするとブロックされます。[RFWIN-19823]

### 2006.1 の既知の問題

- Windows 2012 R2 マシンで Media Foundation 機能をアンインストールすると、そのサーバーにインストールされている Citrix Workspace アプリのインスタンスが応答しなくなります。[RFWIN-17628]

## 2002 の既知の問題

- 保護された Citrix Workspace アプリセッションが最小化されている場合、PrtScn キーを使用して画面をキャプチャしようとするとう失敗することがあります。[RFWIN-15155]
- 公開セッションとローカルデバイスの両方で Microsoft Word を起動し、アカウントからストアを削除すると、ローカルデバイスでアプリを起動したときに次のエラーメッセージが表示されます：  
このファイルを開くためのアプリケーションを **Citrix Workspace** で選択しますか？  
[RFWIN-15884]
- SSL が有効な VDA でセッションを起動しようとするとう失敗することがあります。[RFWIN-16129]
- 保護されたデスクトップセッションで、保護されていないセッションのスクリーンショットを撮ろうとすると失敗することがあります。[RFWIN-16704]
- グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して追加されたストアの詳細を、GUI を使用して削除できない場合があります。[RFWIN-16754]
- 保護されたセッションで表示を変更しようとするとうセッションが終了します。[RFWIN-16784]

## 1911 の既知の問題

- DUO 認証を使用して StoreFront に接続できません。[LD1497]
- セッションウィンドウが前面に表示されません。[LD2089]
- セッションが、ダブルホップシナリオで応答しなくなることがあります。[LD2185]
- クラウド展開で汎用 USB リダイレクト経由で Web カメラを使用すると、ブルースクリーンでセッションが応答しなくなります。[LD2432]
- セッションの起動中、進行状況バーには選択したアプリ名ではなく接続中.. というメッセージが表示されます。  
[LD2450]
- Dell Wyse RAM で構成されたシステムでは、Citrix Workspace アプリのインストールが次のエラーで失敗します：  
「システムは指定されたデバイスまたはファイルを開けません」。  
[LD2480]
- マルチディスプレイのセットアップでは、テキストが明瞭に表示されないことがあります。[LD2484]
- セッションでノートブックをドッキング解除すると、しばらくの間応答しなくなり、次のエラーが表示されま  
す：  
「接続が中断されました」。  
[LD2496]

- グループポリシーオブジェクト管理ポリシーを使用してコンテンツの双方向リダイレクト機能を構成した場合、**[URL 固有の公開アプリケーションまたはデスクトップの上書きを有効にする]** オプションをオフにすると、構成が失敗し次のエラーが表示されます：

「No entries were added to the list. Make sure you added one entry in the list.」

[LD2510]

- Microsoft Teams ミーティングで、ビデオを **On** に設定するとセルフビデオプレビューが頻繁にちらつくことがあります。[RFFWIN-11993]
- Windows 10 RS 6 システムでは、UDT を **Off** に設定し、ファイアウォールコマンドを使用してネットワークを無効にすると、Common Gateway Protocol が機能しないことがあります。これはサードパーティの制限事項によるものです。この問題を回避するには、DDC で **HDX** アダプティブトランスポートポリシーを有効にします。[RFFWIN-15116]
- 同じリソースが一方のサイトで有効になり、もう一方のサイトで無効になると、リソース名に「1」が追加されます。[ RFFWIN-15395]
- Microsoft Teams では、ビデオプレビューの起動中に切断して再接続した後、ビデオが回復しません。[RFFWIN-15539]

#### 1909 の既知の問題

- コンテンツの双方向リダイレクトを有効にすると、Internet Explorer ウィンドウがフォアグラウンドに表示されません。[LD1924]
- CTRL+ALT+DEL を使用してユーザーを切り替えてセッションに再接続しようとする、セッションが再接続に失敗し、応答なくなり、次のメッセージが表示されます：

「Connected to Desktop」 (デスクトップに接続されました)

[LD2063]

- レジストリエディターで **SelfServiceMode** の値を **False** に設定し、[更新] をクリックすると、アプリのショートカットは [スタート] メニューから削除されません。[LD2126]
- URL のリダイレクトは、2048 文字を超える URL で失敗します。[LD2210]

#### サードパーティ製品についての通知

Windows 向け Citrix Workspace アプリには、次のドキュメントで定義された条件の下でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります：

[Windows 向け Citrix Workspace アプリのサードパーティ製品についての通知](#) (PDF のダウンロード)

## システム要件と互換性

November 12, 2021

### 要件

- 1GB 以上の RAM。
- Microsoft Edge WebView2 ランタイムバージョン 92 以降。

注:

バージョン 2107 以降、Microsoft Edge WebView2 ランタイムインストーラーは Citrix Workspace アプリのインストーラーとともにパッケージ化されます。Workspace アプリのインストール時、インストーラーが Microsoft Edge WebView2 ランタイムがシステム上に存在するかどうかを確認し、必要に応じてインストールします。

管理者以外の権限で Citrix Workspace アプリをインストールまたはアップグレードしようとする、インストールは失敗します。

- Self-Service plug-in には、NET 4.6.2 が必要です。これにより、Citrix Workspace アプリのユーザーインターフェイスまたはコマンドラインからアプリとデスクトップにサブスクライブして起動することができます。詳しくは、「[コマンドラインパラメーターの使用](#)」を参照してください。

Citrix Workspace アプリ 1904 以降にアップグレードまたはダウンロードする場合、必要なバージョンの .NET Framework が Windows システム上にインストールされていないと、Citrix Workspace アプリのインストーラーによって必要なバージョンの .NET Framework がダウンロードおよびインストールされます。

注:

非管理者権限で Citrix Workspace アプリをインストールまたはアップグレードする場合、.NET Framework 4.6.2 以降がシステム上にインストールされていないと、インストールは失敗します。

- Microsoft Visual C++ 再頒布可能パッケージの最新バージョン。

注:

Citrix では Microsoft Visual C++ 再頒布可能パッケージの最新バージョンを使用することをお勧めします。そうしないと、アップグレード中に再起動のプロンプトが表示されることがあります。

バージョン 1904 以降、Microsoft Visual C++ 再頒布可能インストーラーは Citrix Workspace アプリのインストーラーとともにパッケージ化されます。Citrix Workspace アプリのインストール時、インストーラーが Microsoft Visual C++ 再頒布可能パッケージがシステム上に存在するかどうかを確認し、必要に応じてインストールします。

注:

Microsoft Visual C++ 再頒布可能パッケージがインストールされていないシステムに管理者以外の権限で Citrix Workspace アプリをインストールしようとすると、失敗することがあります。

Microsoft Visual C++ 再頒布可能パッケージをインストールできるのは、管理者のみです。

.NET Framework または Microsoft Visual C++ 再頒布可能パッケージのインストールに関する問題のトラブルシューティングについては、Citrix Knowledge Center の記事 [CTX250044](#) を参照してください。

### 互換性マトリックス

Citrix Workspace アプリは、現在サポートされているすべてのバージョンの Citrix Virtual Apps and Desktops および [シトリックス製品マトリックス](#) の一覧にある Citrix Gateway のバージョンと互換性があります。

Windows 向け Citrix Workspace アプリは、以下の Windows オペレーティングシステムと互換性があります。

注:

- Citrix Workspace アプリ 2009.5 以降では、サポートされていないオペレーティングシステムへのインストールができませんになっています。
- Windows 7 のサポートは、バージョン 2006 以降から停止されました。
- Citrix Gateway End-Point Analysis Plugin (EPA) は Citrix Workspace でサポートされています。ネイティブの Citrix Workspace アプリでは、nFactor 認証を使用する場合にのみサポートされます。詳しくは、Citrix ADC ドキュメントの「[nFactor 認証の要素として認証前および認証後の EPA スキャンを構成](#)」を参照してください。

---

### オペレーティングシステム

#### Windows 11

Windows 10 Enterprise (32 ビット版および 64 ビット版)。互換性のある Windows 10 のバージョンについて詳しくは、「[Windows 10 と Windows 向け Citrix Workspace アプリとの互換性](#)」を参照してください。

#### Windows 10 Enterprise (2016 LTSB 1607、LTSC 2019)

Windows 10 (IoT Enterprise\*、Home エディション\*\*、Pro)

#### Windows 8.1 (32 ビット版、64 ビット版、および Embedded エディション)

#### Windows Server 2022

#### Windows Server 2019

#### Windows Server 2016

#### Windows Server 2012 R2 (Standard および Datacenter エディション)

---

\*Windows 10 IoT Enterprise 2015 LTSB、Windows 10 IoT Enterprise 2016 LTSB、Anniversary Update、Creators Update、Falls Creators Update をサポート。

\*\* ドメインパススルー認証、Desktop Lock、FastConnect API、およびドメイン参加済み Windows マシンを必要とする構成はサポートされていません。

## Windows 10 と Windows 向け Citrix Workspace アプリとの互換性

Windows 10 オペレーティングシステムのリリースとともに、Windows を構築、展開、サービス展開するための新しい方法が導入されました：[サービスとしての Windows](#)。新機能は、機能更新プログラム（1703、1709、1803 などのメジャーバージョン）パッケージに含まれます。バグ修正とセキュリティ修正は、品質更新プログラムパッケージに含まれます。これらの更新プログラムは SCCM などの既存の管理ツールを使用して展開できます。

注：

- 半期チャネルバージョンより前にリリースされた Citrix ソフトウェアバージョンのインストールはお勧めしません。
- Windows 10 バージョンがサービス終了になると、Microsoft からバージョンのサービスやサポートが提供されなくなります。シトリックスでは、製造元がサポートするオペレーティングシステムで実行する場合のみ Citrix ソフトウェアをサポートします。Windows 10 のサービス終了について詳しくは、[Microsoft の Windows ライフサイクルファクトシート](#)を参照してください。

次の表は、Windows 10 のバージョン番号と対応する互換性のある Windows 向け Citrix Workspace アプリのリリースを示します。

| Windows 10 のバージョン番号 | ビルド番号     | Citrix Workspace アプリのバージョン |
|---------------------|-----------|----------------------------|
| 21H1                | 19043.928 | 2106 以降                    |
| 20H2                | 19042.508 | 2012 以降                    |
| 2004                | 19041.113 | 2006.1 以降                  |
| 1909                | 18363.418 | 1911 以降                    |
| 1903                | 18362.116 | 1909 以降                    |
| 1809                | 17763.107 | 1812 以降                    |
| 1803                | 17134.376 | 1808 以降                    |

注：

Windows 10 バージョンは、前述の Citrix Workspace アプリリリースとのみ互換性があります。たとえば、Windows 10 バージョン 21H1 は、2106 より前のリリースと互換性がありません。

空きディスクスペースの検証

次の表に、Citrix Workspace アプリをインストールする場合の必要ディスクスペースの詳細を示します：

| インストールの種類 | 必須ディスクスペース |
|-----------|------------|
| 新規インストール  | 572MB      |
| アップグレード   | 350MB      |

Citrix Workspace アプリは、インストールを完了するために必要なディスクスペースがあるかどうかのチェックを実行します。この検証は、新規インストールとアップグレードのどちらの場合にも実行されます。

注：

- インストーラーがディスクスペースのチェックを実行するのは、インストールパッケージの抽出後のみです。
- サイレントインストール時にシステムのディスクスペースが少ない場合、ダイアログは表示されませんが、エラーメッセージが `CTXInstall\*_TrolleyExpress-*.log` に記録されます。

### 接続、証明書、認証

#### 接続

- HTTP ストア
- HTTPS ストア
- Citrix Gateway 10.5 以降

#### 証明書

注：

Windows 向け Citrix Workspace アプリはデジタル署名されています。デジタル署名にはタイムスタンプが付けられています。したがって、証明書は有効期限が切れても有効です。

- プライベート（自己署名）証明書
- ルート証明書
- ワイルドカード証明書
- 中間証明書

#### プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合、Citrix リソースにアクセスするユーザーデバイスに組織の証明機関のルート証明書がインストールされている必要があります。

## 注:

接続時にリモートゲートウェイの証明書を検証できない場合（ローカルのキーストアにルート証明書が含まれていないため）、信頼されていない証明書の警告が表示されます。ユーザーが警告に対してそのまま続行することを選択した場合、アプリの一覧が表示されますが、アプリの起動に失敗することがあります。

## ルート証明書

ドメイン参加コンピューターでは、グループポリシーオブジェクト管理用テンプレートを使用して CA 証明書を配布および信頼できます。

ドメイン非参加コンピューターでは、カスタムインストールパッケージを作成して、CA 証明書を配布およびインストールできます。詳しくは、システム管理者に問い合わせてください。

## ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内のサーバーで使用されます。

Citrix Workspace アプリでは、ワイルドカード証明書がサポートされています。ワイルドカード証明書は、組織のセキュリティポリシーに従って使用する必要があります。実際には、サブジェクトの別名（SAN）拡張領域内のサーバー名一覧に含まれている証明書など、ワイルドカード証明書に代わるものです。このような証明書は、私的証明機関および公的証明機関が発行します。

## 中間証明書

証明書チェーンに中間証明書が含まれる場合は、中間証明書を Citrix Gateway のサーバー証明書に追加する必要があります。詳しくは、「[中間証明書の構成](#)」を参照してください。

## 認証

## StoreFront での認証

|               | <b>Web 向け<br/>Workspace</b> | <b>StoreFront サ<br/>ービスサイト<br/>(ネイティブ)</b> | <b>StoreFront、<br/>Citrix Virtual<br/>Apps and<br/>Desktops (ネ<br/>イティブ)</b> | <b>Citrix<br/>Gateway から<br/>Web 向け<br/>Workspace</b> | <b>Citrix<br/>Gateway から<br/>StoreFront サ<br/>ービスサイト<br/>(ネイティブ)</b> |
|---------------|-----------------------------|--|--|---|--|
| 匿名            | はい                          | はい   |  |   |  |
| ドメイン          | はい                          | はい   | はい   | はい *  | はい *   |
| ドメインパスス<br>ルー | はい                          | はい   | はい   |   |  |

|                                  | <b>Web 向け<br/>Workspace</b> | <b>StoreFront サ<br/>ービスサイト<br/>(ネイティブ)</b> | <b>StoreFront、<br/>Citrix Virtual<br/>Apps and<br/>Desktops (ネ<br/>イティブ)</b> | <b>Citrix<br/>Gateway から<br/>Web 向け<br/>Workspace</b> | <b>Citrix<br/>Gateway から<br/>StoreFront サ<br/>ービスサイト<br/>(ネイティブ)</b> |
|----------------------------------|-----------------------------|--|--|---|--|
| セキュリティ<br>トークン                   |                             |  |  | はい *  | はい *   |
| 2 要素認証 (ド<br>メイン+セキュ<br>リティトークン) |                             |  |  | はい *  | はい *   |
| SMS                              |                             |  |  | はい *  | はい *   |
| スマートカード                          | はい                          | はい   |  | はい  | はい   |
| ユーザー証明書                          |                             |  |  | はい (Citrix<br>Gateway<br>Plug-in)                     | はい (Citrix<br>Gateway<br>Plug-in)                                    |

\* デバイスに Citrix Gateway Plug-in をインストールしている場合としない場合。

注:

Citrix Workspace アプリは、Citrix Gateway から StoreFront ネイティブサービスを通じて 2 要素認証 (ドメイン+セキュリティトークン) をサポートします。

#### 証明書失効リスト

証明書失効一覧 (CRL) によって、Citrix Workspace アプリはサーバー証明書が失効していないかチェックできます。証明書のチェックを行うことにより、TLS サーバーの暗号化認証機能が強化され、ユーザーデバイスとサーバー間の TLS 接続のセキュリティが向上します。

証明書失効一覧のチェック機能はさまざまな設定レベルで有効にできます。たとえば、ローカルの証明書失効一覧だけがチェックされるように Citrix Workspace アプリを構成したり、ローカルおよびネットワーク上の証明書失効一覧がチェックされるように構成したりできます。さらに、すべての証明書失効一覧で証明書の有効性が検証されたときのみログオンするように構成できます。

ローカルコンピューターで証明書チェックを構成する場合は、Citrix Workspace アプリを終了します。コネクショセンターを含むすべての Citrix Workspace コンポーネントが停止していることを確認します。

詳しくは、「[TLS](#)」セクションを参照してください。

## インストールとアンインストール

November 12, 2021

Citrix Workspace アプリは、次のいずれかの方法でインストールできます：

- [CitrixWorkspaceApp.exe](#) インストールパッケージを [ダウンロードページ](#) からダウンロードする。または
- 会社のダウンロードページ（利用可能な場合）からダウンロードする。

このパッケージは次の方法でインストールできます：

- Windows ベースのインタラクティブなインストールウィザードを実行する。または
- コマンドラインインターフェイスを使用して、インストーラーのファイル名、インストールコマンド、インストールプロパティを入力する。コマンドラインインターフェイスを使用した Citrix Workspace アプリのインストールについて詳しくは、「[コマンドラインパラメーターの使用](#)」を参照してください。

管理者権限と非管理者権限によるインストール：

Citrix Workspace アプリは、ユーザーおよび管理者の両方がインストールできます。Windows 向け Citrix Workspace アプリで [パススルー認証](#) および [Citrix Ready ワークスペースハブ](#) を使用する場合にのみ、管理者権限が必要です。

次の表では、Citrix Workspace アプリを管理者またはユーザーとしてインストールした場合の違いについて説明します：

|      | インストールフォルダー                                   | インストールの種類     |
|------|---|---------------|
| 管理者  | C:\Program Files (x86)\Citrix\ICA Client      | システムごとのインストール |
| ユーザー | %USERPROFILE%\AppData\Local\Citrix\ICA Client | ユーザーごとのインストール |

注：

ユーザーがインストールした Citrix Workspace アプリがシステム上に存在する場合、管理者はインストールできません。管理者としてインストールする前に、ユーザーがインストールしたすべての Citrix Workspace アプリをアンインストールすることをお勧めします。

### Windows 向けインストーラーの使用

以下の方法で [CitrixWorkspaceApp.exe](#) インストーラーパッケージを手動で実行することで、Windows 向け Citrix Workspace アプリをインストールできます：

- インストールメディア

- ネットワーク共有
- Windows エクスプローラー
- コマンドラインインターフェイス

デフォルトでは、インストーラーのログは%temp%\CTXReceiverInstallLogs\*.logsにあります。

1. CitrixWorkspaceApp.exeファイルを起動して [開始] をクリックします。
2. EULA を読んで同意してから、インストールを続行します。
3. 管理者権限でドメイン参加のマシンにインストールしようとする時、シングルサインオンのダイアログボックスが開きます。詳しくは、「[ドメインパススルー認証]」(/ja-jp/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication) を参照してください。
4. Windows 向けインストーラーの手順に従ってインストールを完了します。

### コマンドラインパラメーターの使用

さまざまなコマンドラインオプションを指定して、Citrix Workspace アプリのインストーラーをカスタマイズできます。インストーラーパッケージは自己展開型であり、セットアッププログラムが起動する前にシステムの一時フォルダーに展開されます。領域要件には、プログラムファイル、ユーザーデータ、およびいくつかのアプリケーションを起動した後の一時ディレクトリが含まれます。

Windows のコマンドラインを使用して Citrix Workspace アプリをインストールするには、コマンドプロンプトを起動します。インストーラーのファイル名、インストールコマンド、インストールプロパティを入力します。以下は、使用可能なインストールコマンドとプロパティです：

CitrixWorkspaceApp.exe [commands] [properties]

### コマンドラインパラメーター一覧

パラメーターは大まかに次のように分類されます：

- [一般的なパラメーター](#)
- [インストールパラメーター](#)
- [HDX 機能のパラメーター](#)
- [基本設定とユーザーインターフェイスのパラメーター](#)
- [認証パラメーター](#)

#### 一般的なパラメーター

- `/?`または`/help` - すべてのインストールコマンドとプロパティを一覧表示します。
- `/silent` - インストール中のインストールダイアログとプロンプトを無効にします。
- `/noreboot` - インストール中に再起動のプロンプトを表示しません。再起動プロンプトを表示しない場合、一時停止状態だった USB デバイスは認識されません。USB デバイスは、デバイスの再起動後のみアクティブ化されます。

- `/includeSSON` - 管理者としてインストールする必要があります。Citrix Workspace アプリはシングルサインオンコンポーネントとともにインストールされます。詳しくは、「[ドメインパススルー認証]」([/ja-jp/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication](#)) を参照してください。
- `/rcu` - このスイッチは、サポートされていないバージョンのソフトウェアからアップグレードする場合のみ有効です。既存のバージョンをアンインストールして、Citrix Workspace アプリをインストールまたはアップグレードします。`/rcu`スイッチにより、既存の設定や古い設定も消去されます。

注:

`/rcu`スイッチは、バージョン 1909 以降廃止されます。詳しくは、「[廃止](#)」を参照してください。

- `/forceinstall` - このスイッチは、システム上の Citrix Workspace アプリの既存の構成またはエントリをクリーンアップするときに役立ちます。このスイッチは、次のシナリオで使用します:
  - Citrix Workspace アプリのサポートされていないバージョンからアップグレードする。
  - インストールまたはアップグレードに失敗した。

インストールパラメーター

### **`/AutoUpdateCheck`**

Citrix Workspace アプリが、利用可能な更新を検出したことを示します。

注:

これは、`/AutoUpdateStream`、`/DeferUpdateCount`、`/AURolloutPriority`などの他のパラメーターを構成するために設定する必要がある必須パラメーターです。

- `Auto` (デフォルト) - 更新が利用可能になると通知します。例: `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto`。
- `Manual` - 更新が利用可能になっても通知されません。手動で更新をチェックします。例: `CitrixWorkspaceApp.exe /AutoUpdateCheck=manual`。
- `Disabled` - 自動更新を無効にします。例: `CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled`。

### **`/AutoUpdateStream`**

自動更新を有効にすると、更新するリリーストラックを選択できます。詳しくは、「[ライフサイクルマイルストーン](#)」を参照してください。

- `LTSR` - 長期サービスリリース (LTSR) 累積更新プログラム (CU) にのみ自動更新します。例: `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`。
- `Current` - Citrix Workspace アプリの最新バージョンにのみ自動更新します。例: `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`。

## **/DeferUpdateCount**

更新が利用可能な場合に通知を延期できる回数を示します。詳しくは、「[Citrix Workspace 更新プログラム](#)」を参照してください。

- -1 (デフォルト) - 通知を何度でも延期できます。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`。
- 0 - 利用可能な更新ごとに 1 回 (のみ) 通知を受信します。更新について再度通知されることはありません。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`。
- 任意の数の「n」 - 通知を「n」回延期できます。[後で通知する] オプションは、「n」回表示されます。例: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`。

## **/AURolloutPriority**

新しいバージョンのアプリがリリースされると、特定の配信期間に更新プログラムが Citrix からロールアウトされます。このパラメーターを使用すると、配信期間中に更新を受信するタイミングを制御できます。

- Auto (デフォルト) — 配信期間中に Citrix での構成に従って更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`。
- Fast — 配信期間の開始時に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`。
- Medium — 配信期間の中頃に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`。
- Slow - 配信期間の最後に更新を受信します。例: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`。

## **/includeappprotection**

セキュリティを強化し、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性を抑制します。

- `CitrixWorkspaceApp.exe /includeappprotection`

詳しくは、「[アプリ保護](#)」を参照してください。

## **/InstallEmbeddedBrowser**

Citrix 組み込みブラウザバイナリを除外します。組み込みブラウザ機能を停止するには、`/InstallEmbeddedBrowser=N`スイッチを実行します。

## **INSTALLDIR**

Citrix Workspace アプリをインストールするためのカスタムインストールディレクトリを指定します。デフォルトのパスは `C:\Program Files\Citrix` です。例: `CitrixWorkspaceApp.exe INSTALLDIR=C:\`

Program Files\Citrix。

## ADDLOCAL

1 つまたは複数の指定したコンポーネントをインストールします。例: `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,WebHelper,BrowserEngine, WorkspaceHub, USB`。

注:

デフォルトでは、Citrix Workspace アプリのインストール時に `ReceiverInside`、`ICA_Client`、および `AM` がインストールされます。

## HDX 機能のパラメーター

### ALLOW\_BIDIRCONTENTREDIRECTION

クライアントとホスト間でコンテンツの双方向リダイレクトを有効化します。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「[双方向のコンテンツリダイレクトのポリシー設定](#)」を参照してください。

- 0 (デフォルト) - 双方向のコンテンツリダイレクトを無効化します。例: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`。
- 1 - 双方向のコンテンツリダイレクトを有効化します。例: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`。

### FORCE\_LAA

Citrix Workspace アプリはクライアント側ローカルアプリアクセスのコンポーネントとともにインストールされます。このコンポーネントを動作させるには、管理者権限で Workspace アプリをインストールする必要があります。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「[\[ローカルアプリアクセス\]](#)」([/ja-jp/citrix-virtual-apps-desktops/general-content-redirect/laa-url-redirect.html](#)) を参照してください。

- 0 (デフォルト) - ローカルアプリアクセスのコンポーネントがインストールされていないことを示します。例: `CitrixWorkspaceApp.exe FORCE_LAA =0`。
- 1 - クライアント側ローカルアプリアクセスのコンポーネントがインストールされます。例: `CitrixWorkspaceApp.exe FORCE_LAA =1`。

### LEGACYFTAICONS

サブスクリブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアイコンを表示するかどうかを指定します。

- False (デフォルト) - サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアイコンが表示されることを示します。False に設定すると、特定のアイコンが割り当てられていないドキュメントのアイコンがオペレーションシステムで生成されます。生成されたアイコンでは、標準的なアイコン上にアプリケーションの小さいアイコンが重なって表示されます。例: `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`。
- True - サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントまたはファイルに、そのアイコンが表示されないことを示します。例: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`。

## ALLOW\_CLIENTHOSTEDAPPSURL

ユーザーデバイスの URL リダイレクト機能を有効にします。詳しくは、Citrix Virtual Apps and Desktops のドキュメントで「[ローカルアプリアクセス]」([/ja-jp/citrix-virtual-apps-desktops/general-content-redirect/laa-url-redirect.html](https://docs.citrix.com/ja-jp/citrix-virtual-apps-desktops/general-content-redirect/laa-url-redirect.html)) を参照してください。

- 0 (デフォルト) - ユーザーデバイスの URL リダイレクト機能を無効にします。例: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`。
- 1 - ユーザーデバイスの URL リダイレクト機能を有効にします。例: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`。

基本設定とユーザーインターフェイスのパラメーター

## ALLOWADDSTORE

指定されたパラメーターを基にしてストア (HTTP または https) の構成を許可します。

- S (デフォルト) - ストアの追加や削除を許可します (HTTPS で構成されたセキュアなストアのみ)。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`。
- A - ストアの追加や削除を許可します (HTTPS または HTTP で構成されたストア)。Citrix Workspace アプリがユーザー単位でインストールされている場合は使用できません。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`。
- N - ユーザーによるストアの追加や削除を許可しません。例: `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`。

## ALLOWSAVEPWD

ストア認証情報をローカルに保存できます。このパラメーターは、Citrix Workspace アプリプロトコルを使用するストアにのみ適用されます。

- S (デフォルト) - (HTTPS が構成された) セキュアなストアにのみパスワードの保存を許可します。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`。
- N - パスワードの保存を許可しません。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`。

- A - セキュアなストア (HTTPS) およびセキュアではないストア (HTTP) の両方にパスワードの保存を許可します。例: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`。

## STARTMENUDIR

[スタート] メニューのショートカットのディレクトリを指定します。

- <Directory Name> - デフォルトでは、[スタート] > [すべてのプログラム] の下にアプリケーションのショートカットが追加されます。ショートカットを配置するフォルダーを `\Programs` からの相対パスで指定します。たとえば、[スタート] > [すべてのプログラム] > [Workspace] にショートカットを配置するには、`STARTMENUDIR=\Workspace` と指定します。

## DESKTOPDIR

デスクトップのショートカット用ディレクトリを指定します。

注:

DESKTOPDIR オプションを使用するときは、`PutShortcutsOnDesktop` キーを `True` に設定します。

- <Directory Name> - ショートカットは相対パスで指定できます。たとえば、[スタート] > [すべてのプログラム] > [Workspace] にショートカットを配置するには、`DESKTOPDIR=\Workspace` と指定します。

## SELFSERVICEMODE

セルフサービスの Workspace アプリのユーザーインターフェイスに対するアクセスを制御します。

- True - ユーザーはセルフサービスのユーザーインターフェイスにアクセスできます。例: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`。
- False - ユーザーはセルフサービスのユーザーインターフェイスにアクセスできません。例: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`。

## ENABLEPRELAUNCH

セッションの事前起動を制御します。詳しくは、「[アプリケーションの起動時間]」(</ja-jp/citrix-workspace-app-for-windows/configure.html#application-launch-time>) を参照してください。

- True - セッションの事前起動が有効です。例: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`。
- False - セッションの事前起動が無効です。例: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`。

## DisableSetting

[高度な設定] シートで [ショートカット] と [再接続] オプションが表示されないようにします。詳しくは、「[\[高度な設定\] シートから特定の設定を非表示にする](#)」を参照してください。

- 0 (デフォルト) - [高度な設定] シートで [ショートカット] と [再接続] の両方のオプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=0`。
- 1 - [高度な設定] シートで [再接続] オプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=1`。
- 2 - [高度な設定] シートで [ショートカット] オプションを表示します。例: `CitrixWorkspaceApp.exe DisableSetting=2`。
- 3 - [高度な設定] シートで [ショートカット] と [再接続] の両方のオプションを非表示にします。例: `CitrixWorkspaceApp.exe DisableSetting=3`。

## EnableCEIP

カスタマーエクスペリエンス向上プログラムに参加することを示します。詳しくは、「[CEIP](#)」を参照してください。

- True (デフォルト) - カスタマーエクスペリエンス向上プログラム (CEIP) にオプトインします。例: `CitrixWorkspaceApp.exe EnableCEIP=True`。
- False - カスタマーエクスペリエンス向上プログラム (CEIP) をオプトアウトします。例: `CitrixWorkspaceApp.exe EnableCEIP=False`。

## EnableTracing

常時トレース機能を制御します。

- True (デフォルト) - 常時トレース機能を有効にします。例: `CitrixWorkspaceApp.exe EnableTracing=true`。
- False - 常時トレース機能を無効にします。例: `CitrixWorkspaceApp.exe EnableTracing=false`。

## CLIENT\_NAME

サーバーでユーザーデバイスを識別するために使用される名前です。

- `<ClientName>` - サーバーでユーザーデバイスを識別するために使用される名前です。デフォルト名は `%COMPUTERNAME%` です。例: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`。

## ENABLE\_DYNAMIC\_CLIENT\_NAME

クライアント名をコンピューター名と同じ名前にできます。この場合、ユーザーがコンピューター名を変更すると、クライアント名もそれに応じて変更されます。

- Yes (デフォルト) - クライアント名をコンピューター名と同じ名前にできます。例: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`。
- No - クライアント名をコンピューター名と同じ名前にできません。CLIENT\_NAME プロパティの値を指定する必要があります。例: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`。

認証パラメーター

### ENABLE\_SSON

Workspace アプリが `/includeSSON` コマンドでインストールされた場合、シングルサインオンを有効にします。詳しくは、「[\[ドメインパススルー認証\]](#)」([/ja-jp/citrix-workspace-app-for-windows/authentication.html#domain-pass-through-authentication](#)) を参照してください。

- Yes (デフォルト) - シングルサインオンが有効になっています。例: `CitrixWorkspaceApp.exe ENABLE_SSON=Yes`。
- No - シングルサインオンが無効になっています。例: `CitrixWorkspaceApp.exe ENABLE_SSON=No`。

### ENABLE\_KERBEROS

HDX エンジンが Kerberos 認証を使用する必要があるかどうかを指定します。これは、シングルサインオン認証が有効な場合にのみ適用されます。詳しくは、「[Kerberos を使用したドメインパススルー認証](#)」を参照してください。

- Yes - HDX エンジンが Kerberos 認証を使用します。例: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`。
- No - HDX エンジンが Kerberos 認証を使用しません。例: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`。

上記のプロパティに加えて、Workspace アプリで使用するストア URL も指定できます。10 ストアまで追加できます。このためには、以下のプロパティを使用します:

```
STOREx=" storename;http[s]://servername.domain/IISLocation/discovery;[On,Off]; [storedescription]"
```

値のデータ:

- x - ストアを識別するために使用される整数 0~9。
- storename - ストアの名前。これは、StoreFront サーバーで構成される名前と同じである必要があります。
- servername.domain - ストアをホストするサーバーの完全修飾ドメイン名。
- IISLocation - IIS 内のストアへのパス。このストア URL は、StoreFront プロビジョニングファイルに記述されている URL と同じである必要があります。ストア URL は「`/Citrix/store/discovery`」の形式です。URL を取得するには、StoreFront からプロビジョニングファイルをエクスポートしてそれをメモ帳などのテキストエディターで開き、**Address** エレメントから URL をコピーします。
- [On, Off] - **Off** オプションを指定すると、無効なストアを配信できるようになります。これにより、そのストアにアクセスするかをユーザーが選択できるようになります。このオプションを指定しない場合、デフォルトの設定は **On** になります。

- storedescription - ストアの説明 (「HR App Store」など)。

コマンドラインを使用したインストールの例

**Citrix Gateway** のストア URL を指定するには:

```
CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com##Storename;  
On;Store
```

ここで *Storename* は、構成する必要があるストアの名前です。

注:

- Citrix Gateway のストア URL を上記の方法で構成した場合、Citrix Gateway を使用している PNA サービスサイトはサポートされません。
- 複数ストア環境では、Citrix Gateway ストアの URL が一覧の先頭に表示される必要があります。Citrix Gateway ストアの URL は、1 つまでのみ構成できます。

以下のコマンドでは、すべてのコンポーネントをサイレントインストールして **2** つのアプリケーションストアを指定します。

```
CitrixWorkspaceApp.exe /silent  
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App  
Store"  
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery  
;on;Backup HR App Store"
```

注:

- パススルー認証を成功させるには、ストア URL に */discovery* を含める必要があります。
- Citrix Gateway のストア URL は、構成済みのストア URL 一覧で最初のエントリにする必要があります。

## Citrix Workspace アプリのリセット

Citrix Workspace アプリをリセットすると、デフォルト設定が復元されます。

Citrix Workspace アプリのリセットにより、次のアイテムがリセットされます。

- 構成されたすべてのアカウントとストア。
- Self-service Plug-in によって配信されたアプリ、それらのアイコンとレジストリキー。
- Self-service Plug-in によって作成されたファイルタイプの関連付け。
- キャッシュされたファイルと保存されたパスワード。
- ユーザーごとのレジストリ設定。
- マシンごとのインストール、およびそれらのレジストリ設定。
- Citrix Workspace アプリの Citrix Gateway レジストリ設定。

コマンドラインインターフェイスから次のコマンドを実行して、Citrix Workspace アプリをリセットします：

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"-cleanUser
```

サイレントリセットを実行するには、次のコマンドを使用します：

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"/silent -cleanUser
```

注：

パラメーターに大文字の U を使用します。

Citrix Workspace アプリをリセットしても、以下には影響しません：

- Citrix Workspace アプリまたはプラグインのインストール。
- マシンごとの ICA のロックダウン設定。
- Citrix Workspace アプリのグループポリシーオブジェクト (GPO) 管理用テンプレートの構成。

### アンインストール

**Windows** 向けインストーラーの使用：

コントロールパネルの [プログラムと機能] (または [プログラムの追加と削除]) を使って Citrix Workspace アプリをアンインストールできます。

注：

Citrix Workspace アプリのインストール中、Citrix HDX RTME パッケージのアンインストールを求めるメッセージが表示されます。[OK] をクリックしてアンインストールを続行します。

コマンドラインインターフェイスの使用：

ユーザーは、コマンドラインから以下のコマンドを実行して Citrix Workspace アプリをアンインストールすることもできます：

```
CitrixWorkspaceApp.exe /uninstall
```

Citrix Workspace アプリをサイレントアンインストールするには、次のスイッチを実行します：

```
CitrixWorkspaceApp.exe /silent /uninstall
```

注：

GPO 関連のレジストリキーは Citrix Workspace アプリインストーラーによって制御されていないため、アンインストール後も残ります。エントリが見つかった場合は、`gpedit` を使用して更新するか、手動で削除してください。

## 展開

October 5, 2021

次のいずれかの方法で Citrix Workspace アプリを展開できます：

- Active Directory およびサンプルスタートアップスクリプトを使用して Windows 向け Citrix Workspace アプリを展開します。Active Directory については詳しくは、「[Active Directory とサンプルスクリプトの使用](#)」を参照してください。
- Web 向け Workspace 起動する前に、Windows 向け Workspace アプリをインストールします。詳しくは、「[Web 向け Workspace の使用](#)」を参照してください。
- Microsoft System Center Configuration Manager 2012 R2 などの電子ソフトウェア配信 (ESD) ツールを使用します。詳しくは、「[System Center 2012 R2 Configuration Manager の使用](#)」を参照してください。

### Active Directory とサンプルスクリプトの使用

Active Directory のグループポリシースクリプトを使用し、所属する組織の構造に基づいて Citrix Workspace アプリを展開することができます。Citrix では、.msi ファイルの展開ではなくスクリプトの使用をお勧めします。スタートアップスクリプトの概要については、[Microsoft 社のドキュメント](#)を参照してください。

**Active Directory** でスクリプトを使用するには：

1. 各スクリプトの組織単位を作成します。
2. 新しく作成した組織単位のグループポリシーオブジェクトを作成します。

### スクリプトの編集

各ファイルのヘッダーセクションにあるスクリプトの次のパラメーターを編集します：

- **CURRENT VERSION OF PACKAGE** (パッケージの現在のバージョン) - ここに指定するバージョン番号が検証され、そのバージョンが存在しない場合は展開 (インストール) が開始されます。たとえば、`DesiredVersion= 3.3.0.XXXX`に、展開するバージョンの番号を指定します。バージョンの一部 (たとえば 3.3.0) を指定すると、その接頭辞を持つすべてのバージョン (3.3.0.1111、3.3.0.7777 など) に一致します。
- **PACKAGE LOCATION/DEPLOYMENT DIRECTORY** (パッケージの場所/展開ディレクトリ) - パッケージを格納するネットワーク共有です。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーで読み取りアクセス許可を EVERYONE に設定する必要があります。
- **SCRIPT LOGGING DIRECTORY** (スクリプトのログディレクトリ) - インストールログをコピーするネットワーク共有です。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーに Everyone の読み取り/書き込みアクセス許可を設定する必要があります。

- **PACKAGE INSTALLER COMMAND LINE OPTIONS** (パッケージインストーラーのコマンドラインオプション) - インストーラーに渡すコマンドラインオプションです。コマンドライン構文については、「[コマンドラインパラメーターの使用](#)」を参照してください。

## スクリプト

Citrix Workspace アプリインストーラーには、Citrix Workspace アプリのインストールおよびアンインストール用のコンピューター単位およびユーザー単位でのサンプルスクリプトの両方が含まれています。スクリプトは、Windows 向け Citrix Workspace アプリのページから[ダウンロード](#)できます。

| 展開の種類     | 展開する                                      | 削除する                                       |
|-----------|---|--|
| コンピューター単位 | CheckAndDeployWorkspaceF<br>.bat          | CheckAndRemoveWorkspacePerMachineS<br>.bat |
| ユーザー単位    | CheckAndDeployWorkspacePerUserLog<br>.bat | CheckAndRemoveWorkspacePerUserLog<br>.bat  |

スタートアップスクリプトを追加するには:

1. グループポリシー管理コンソールを開きます。
2. [コンピューターの構成] または [ユーザーの構成] > [ポリシー] > **[Windows の設定]** > [スクリプト] の順に選択します。
3. グループポリシー管理コンソールの右ペインで [ログオン] を選択します。
4. [ファイルの表示] を選択して適切なスクリプトを表示されたフォルダーにコピーします。
5. ダイアログを閉じます。
6. [スタートアップのプロパティ] ダイアログボックスで [追加] をクリックし、[参照] をクリックして新しく作成したスクリプトを検索し追加します。

**Windows** 向け **Citrix Workspace** アプリを展開するには:

1. 作成した組織単位に展開対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動してログオンします。
3. 新しくインストールしたパッケージが [プログラムと機能] に表示されることを確認します。

**Windows** 向け **Citrix Workspace** アプリを削除するには:

1. 作成した組織単位に削除対象のユーザーデバイスを移動します。
2. ユーザーデバイスを再起動してログオンします。
3. 新しくインストールしたパッケージが [プログラムと機能] に表示されないことを確認します。

## Web 向け Workspace の使用

Web 向け Workspace を使用すると、ユーザーはブラウザの Web ページを経由して StoreFront ストアにアクセスできます。

ブラウザからアプリに接続する前に、次の操作を実行します：

1. Windows 向け Citrix Workspace アプリをインストールします。
2. Web 向け Workspace を使用した Citrix Workspace アプリの展開

Web 向け Workspace で適切なバージョンの Citrix Workspace アプリがインストールされていないことが検出されると、Windows 向け Citrix Workspace アプリをダウンロードしてインストールするためのページが表示されます。

注：

Web 向け Workspace は、メールアドレスによるアカウント検出をサポートしていません。

ユーザーの混乱を避けるため、サーバーアドレスの入力のみが求められるようにします。

1. `CitrixWorkspaceApp.exe` をローカルコンピューターにダウンロードします。
2. `CitrixWorkspaceApp.exe` を `CitrixWorkspaceAppWeb.exe` という名前に変更します。
3. 名前を変更した実行可能ファイルを通常の方法で展開します。StoreFront を使用している場合は、StoreFront のドキュメントの「[構成ファイルを使った StoreFront の構成](#)」を参照してください。

## Microsoft System Center 2012 R2 Configuration Manager の使用

Microsoft System Center Configuration Manager (SCCM) を使用して、Citrix Workspace アプリを展開できます。

次の 4 段階で SCCM を使用して Citrix Workspace アプリを展開できます：

1. Citrix Workspace アプリを SCCM 展開環境に追加する
2. 配布ポイントを追加する
3. Citrix Workspace アプリをソフトウェアセンターに展開する
4. デバイスコレクションを作成する

### Citrix Workspace アプリを SCCM 展開環境に追加する

1. ダウンロードした Citrix Workspace アプリのインストールフォルダーを Configuration Manager サーバー上のフォルダーにコピーして、Configuration Manager コンソールを起動します。
2. [ソフトウェアライブラリ]、[アプリケーション管理] の順に選択します。[アプリケーション] を右クリックして、[アプリケーションの作成] を選択します。  
アプリケーションの作成ウィザードが開きます。
3. [全般] ページで [アプリケーションの情報を手動で指定する] をクリックし、[次へ] をクリックします。

4. [一般情報] ペインで、アプリケーションの情報（名前、製造元、ソフトウェアバージョンなど）を指定します。
5. アプリケーションカタログウィザードで、追加の情報（言語、アプリケーション名、ユーザーカテゴリなど）を指定して、[次へ] をクリックします。

注:

ユーザーはここで指定した情報を表示できます。

6. [展開の種類] ペインで、[追加] を選択して Windows 向け Citrix Workspace アプリのセットアップで展開の種類を構成します。

展開の種類の作成ウィザードが開きます。

7. [全般] ペイン: 展開の種類を Windows インストーラー (\*.msi ファイル) に設定し、[展開の種類の情報を手動で指定する] を選択して、[次へ] をクリックします。
8. [一般情報] ペイン: 展開の種類の詳細（例: Workspace の展開）を指定して、[次へ] をクリックします。
9. [コンテンツ] ペイン:

- a) Citrix Workspace アプリセットアップファイルのある場所へのパスを指定します。例: SCCM サーバー上のツール。

- b) [インストールプログラム] に次のいずれかを指定します:

- `CitrixWorkspaceApp.exe /silent`を指定して、サイレントインストールする。
- `CitrixWorkspaceApp.exe /silent /includeSSON`を指定して、ドメインパススルーを有効にする。
- `CitrixWorkspaceApp.exe /silent SELFSEVICEMODE=false`を指定して、セルフサービスモード以外で Citrix Workspace アプリをインストールします。

- c) [アンインストールプログラム] に `CitrixWorkspaceApp.exe /silent /uninstall` を指定します (SCCM でのアンインストールを有効にする)。

10. [検出方法] ペイン: [この展開の種類のプレゼンスを検出する規則を構成する] を選択して [句の追加] をクリックします。

[検出方法] ダイアログボックスが開きます。

- [設定の種類] をファイルシステムに設定します。
- [このアプリケーションを検出するためのファイルまたはフォルダーを指定してください] で、次のように設定します:
  - 種類 - ドロップダウンリストから、[ファイル] を選択します。
  - パス - `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`
  - ファイルまたはフォルダー名 - `receiver.exe`
  - プロパティ - ドロップダウンリストから [バージョン] を選択します
  - 演算子 - ドロップダウンリストから [次のもの以上] を選択します
  - 値 - **4.3.0.65534** を入力します

注:

この規則の組み合わせは、Windows 向け Citrix Workspace アプリのアップグレードにも適用されま  
す。

11. [ユーザー側の表示と操作] ペインで、次の値を設定します:

- [インストールの動作] - [システム用にインストールする]
  - [必要なログオン状態] - [ユーザーのログオン状態に関係なし]
  - [インストールプログラムの表示] - [通常]
- [次へ] をクリックします。

注:

この展開の種類には、要件や依存関係を指定しないでください。

12. [概要] ペインで、この展開の種類の設定を確認します。[次へ] をクリックします。

成功メッセージが表示されます。

13. [完了] ペインの [展開の種類] 一覧に新しい展開の種類 (Workspace の展開) が表示されます。

14. [次へ] をクリックして、[閉じる] をクリックします。

配布ポイントを追加する

1. **Configuration Manager** コンソールで Citrix Workspace アプリを右クリックして、[コンテンツの配布]  
を選択します。

コンテンツの配布ウィザードが開きます。

2. [コンテンツの配布] ペインで、[追加] > [配布ポイント] を選択します。

[配布ポイントの追加] ダイアログボックスが開きます。

3. コンテンツが利用可能な SCCM サーバーに移動して、[OK] をクリックします。

[完了] ペインで、成功メッセージが表示されます。

4. [閉じる] をクリックします。

**Citrix Workspace** アプリをソフトウェアセンターに展開する

1. Configuration Manager コンソールで Citrix Workspace アプリを右クリックして、[展開] を選択します。

ソフトウェアの展開ウィザードが開きます。

2. アプリケーションを展開するコレクション (デバイスコレクションまたはユーザーコレクション) を検索し  
て、[次へ] をクリックします。

3. [展開設定] ペインで [アクション] を [インストール] に [目的] を [必須] に設定します (無人インストー  
ルを有効にする)。[次へ] をクリックします。

4. [スケジュール] ペインで、対象のデバイスでソフトウェアを展開するスケジュールを指定します。
5. [ユーザー側の表示と操作] ペインで、[ユーザーへの通知] 動作を設定します。[メンテナンスの期限または期間中の変更を確定する (再起動が必要)] を選択し、[次へ] をクリックしてソフトウェアの展開ウィザードを終了します。

[完了] ペインで、成功メッセージが表示されます。

対象のエンドポイントデバイスを再起動します (すぐにインストールを開始する場合のみ必要)。

エンドポイントデバイスの Citrix Workspace アプリは、利用可能なソフトウェアのソフトウェアセンターに表示されます。構成されたスケジュールに基づいて、自動的にインストールが開始します。また、オンデマンドでスケジュール設定したり、インストールしたりできます。インストールの状態は、インストールの開始後、ソフトウェアセンターに表示されます。

デバイスコレクションを作成する

1. **Configuration Manager** コンソールを起動して、[資産とコンプライアンス]、[概要]、[デバイス] の順に選択します。
2. [デバイスコレクション] を右クリックして、[デバイスコレクションの作成] を選択します。  
デバイスコレクションの作成ウィザードが開きます。
3. [全般] ペインでデバイスの [名前] を入力して、[参照] をクリックして [限定コレクション] を検索します。  
これによって、デバイスの対象が決定されます。SCCM で作成されるデフォルトのデバイスコレクションの場合もあります。  
[次へ] をクリックします。
4. [メンバーシップの規則] ペインで、[規則の追加] を選択してデバイスを絞り込みます。  
ダイレクトメンバーシップの規則の作成ウィザードが開きます。
  - [リソースの検索] ペインで、絞り込みたいデバイスに基づいて [属性名] を選択し、属性名を入力して、デバイスを選択します。
5. [次へ] をクリックします。[リソースの選択] ペインで、デバイスコレクションの一部にする必要があるデバイスを選択します。  
[完了] ペインで、成功メッセージが表示されます。
6. [閉じる] をクリックします。
7. [メンバーシップの規則] ペインで、新しい規則の一覧が [次へ] をクリックの下に表示されます。
8. [完了] ペインで、成功メッセージが表示されます。[閉じる] をクリックして、デバイスコレクションの作成ウィザードを完了します。  
[デバイスコレクション] の一覧に新しいデバイスコレクションが表示されます。新しいデバイスコレクションは、ソフトウェアの展開ウィザードの参照中のデバイスコレクションの一部です。

注:

**MSIRESTARTMANAGERCONTROL** 属性を **False** に設定した場合、SCCM を使用して Citrix Workspace アプリを構成しようとすると失敗することがあります。

分析によると、Windows 向け Citrix Workspace アプリはこのエラーの原因ではありません。再試行で展開が成功することがあります。

## アップデート

August 17, 2021

### 手動更新

既に Windows 向け Citrix Workspace アプリをインストールしている場合は、[シトリックスのダウンロードページ](#)から最新バージョンのアプリをダウンロードしてインストールします。

### 自動更新

新しいバージョンの Citrix Workspace アプリがリリースされると、Citrix Workspace アプリがインストールされたシステムで更新がプッシュされます。

注:

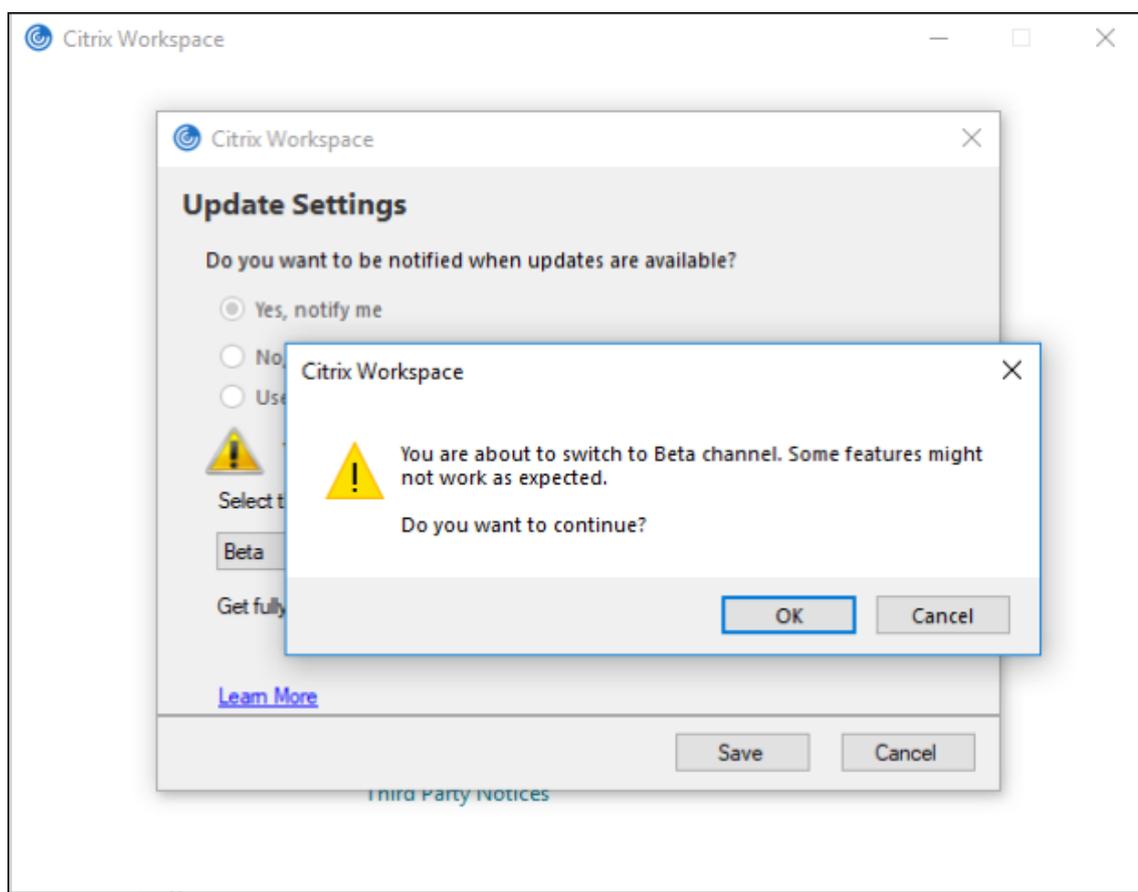
- 送信プロキシをインターセプトするよう SSL を構成している場合、Workspace の自動更新署名サービス (<https://citrixupdates.cloud.com/>) およびダウンロード場所 (<https://downloadplugins.citrix.com/>) に例外を追加してシトリックスからの更新を受信します。
- 更新を受信するには、システムがインターネットに接続している必要があります。
- デフォルトでは、VDA で Citrix Workspace の更新が無効になっています。リモートデスクトップのマルチユーザーサーバーマシン、VDI、リモート PC アクセスマシンでも同様です。
- Citrix Workspace の更新は、Desktop Lock がインストールされたマシンでは無効になっています。
- Web 向け Workspace のユーザーは、StoreFront ポリシーを自動的にダウンロードできません。
- Citrix Workspace の更新は、LTSR 更新のみに限定されます。
- Citrix Workspace の更新に Windows 用の HDX RTME が含まれています。Citrix Workspace アプリの LTSR と最新リリースの両方で使用可能な HDX RTME の更新が通知されます。
- バージョン 2105 から、Citrix Workspace の更新ログのパスが変更されています。Workspace の更新ログは、C:\Program Files (x86)\Citrix\Logs にあります。ログの詳細について詳しくは、「[ログ収集](#)」セクションを参照してください。

### Citrix Workspace アプリのベータプログラムのインストール

Citrix Workspace アプリが自動更新用に構成されている場合は、更新通知を受け取ります。システムにベータビルドをインストールするには、次の手順を実行します：

1. システムトレイから Citrix Workspace アプリを開きます。
2. [高度な設定] > [Citrix Workspace 更新プログラム] に移動します。
3. ベータビルドが利用可能になったら、ドロップダウンリストから [Beta] を選択し、[保存] をクリックします。

通知ウィンドウが開きます。



4. [OK] をクリックして、ベータビルドに更新します。

ベータビルドからリリースビルドに切り替えるには、次の手順を実行します：

1. システムトレイから Citrix Workspace アプリを開きます。
2. [高度な設定] > [Citrix Workspace 更新プログラム] に移動します。
3. [設定の更新] 画面で、更新チャンネルのドロップダウンリストから [Release] を選択し、[保存] をクリックします。

### 注:

ベータビルドは、お客様が非実稼働環境または制限のある稼働環境で使用し、フィードバックを共有する機会を提供するためのものです。ベータビルドのサポートケースは受け付けられませんが、改善に関する[フィードバック](#)をお待ちしております。重要度と重大度により、フィードバックに対応する場合としない場合があります。ベータビルドは実稼働環境に展開しないことをお勧めします。

### 自動更新の詳細設定 (**Citrix Workspace** の更新)

Citrix Workspace の更新は、次の方法で構成できます:

1. グループポリシーオブジェクト (GPO) 管理用テンプレート
2. コマンドラインインターフェイス
3. グラフィカルユーザーインターフェイス
4. StoreFront

グループポリシーオブジェクト管理用テンプレートを使用した **Citrix Workspace** 更新プログラムの構成

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、[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**] > [**Citrix Workspace** の更新] の順に移動します。

1. 更新を有効または無効にする — [有効] または [無効] を選択して、Workspace の更新を有効または無効にします。

注:

[無効] を選択すると、新しい更新が通知されません。これにより、[高度な設定] シートの [Workspace の更新] オプションも非表示になります。

2. 更新通知 — 更新が利用可能になったときに、自動的に通知を受信するか、手動で確認するかを選択できます。Workspace の更新を有効にした後、[**Citrix Workspace** の更新ポリシーを有効にする] ドロップダウンリストの次のオプションから選択します:
  - Auto - 更新が利用可能になると通知します (デフォルト)。
  - Manual - 更新が利用可能になっても通知されません。手動で更新をチェックします。
3. [LTSR のみ] を選択して LTSR の更新のみを取得します。

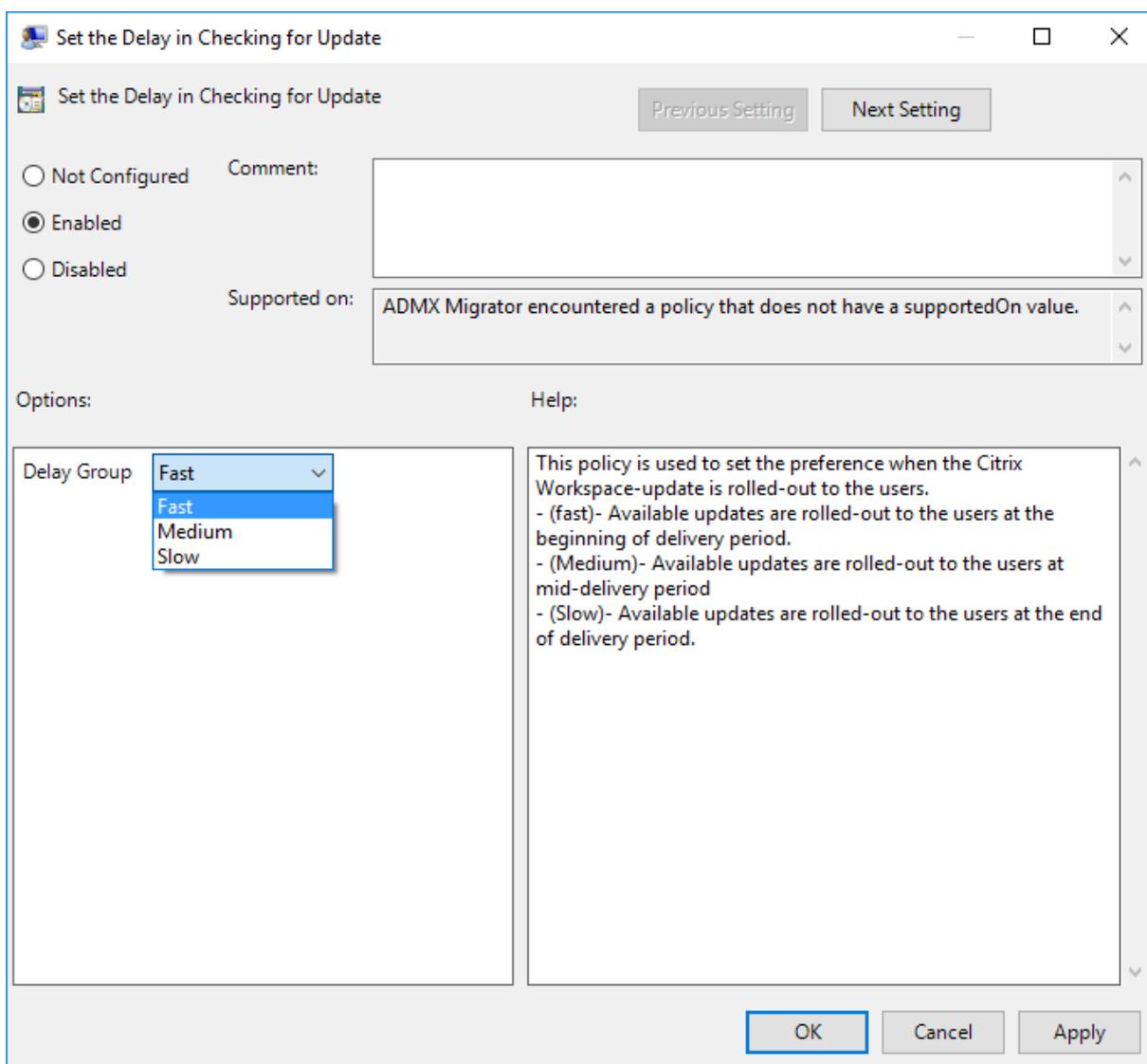
4. **[Citrix-Workspace-Update-DeferUpdate-Count]** ドロップダウンリストから、-1~30 の値を選択します:

- -1 - 何度でも通知を延期できます (デフォルト)。
- 0 - 更新の通知を一度のみ受信します。

更新のチェックで遅延を構成

新しいバージョンの Workspace アプリがリリースされると、特定の配信期間に更新プログラムがロールアウトされます。このプロパティを使用すると、配信期間中に更新を受信するタイミングを制御できます。

配信期間を構成するには、`gpedit.msc`を実行してグループポリシーオブジェクト管理用テンプレートを起動します。[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] > [更新のチェックで遅延を設定] の順に移動します。



[有効] を選択し、[遅延グループ] ドロップダウンリストの次のオプションから選択します:

- **Fast** - 配信期間の最初に更新がロールアウトされます。
- **Medium** - 配信期間の中頃に更新がロールアウトされます。
- **Slow** - 配信期間の最後に更新がロールアウトされます。

注:

[無効] を選択すると、利用可能な更新が通知されません。これにより、[高度な設定] シートの [Workspace の更新] オプションも非表示になります。

コマンドラインインターフェイスを使用した **Citrix Workspace** 更新プログラムの構成

**Workspace** アプリのインストール中にコマンドラインパラメーターを指定する:

Citrix Workspace アプリのインストール中にコマンドラインパラメーターを指定することで、Workspace の更新を構成できます。詳しくは、「[インストールパラメーター](#)」を参照してください。

**Citrix Workspace** アプリのインストール後にコマンドラインパラメーターを使用する:

Citrix Workspace の更新は、Windows 向け Citrix Workspace アプリのインストール後にも構成できます。Windows コマンドラインを使用して、`CitrixReceiverUpdater.exe`の場所に移動します。

通常、`CitrixWorkspaceUpdater.exe` は `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver` にあります。このバイナリは、[インストールパラメーター](#) セクションに記載されているコマンドラインパラメーターとともに実行できます。

例:

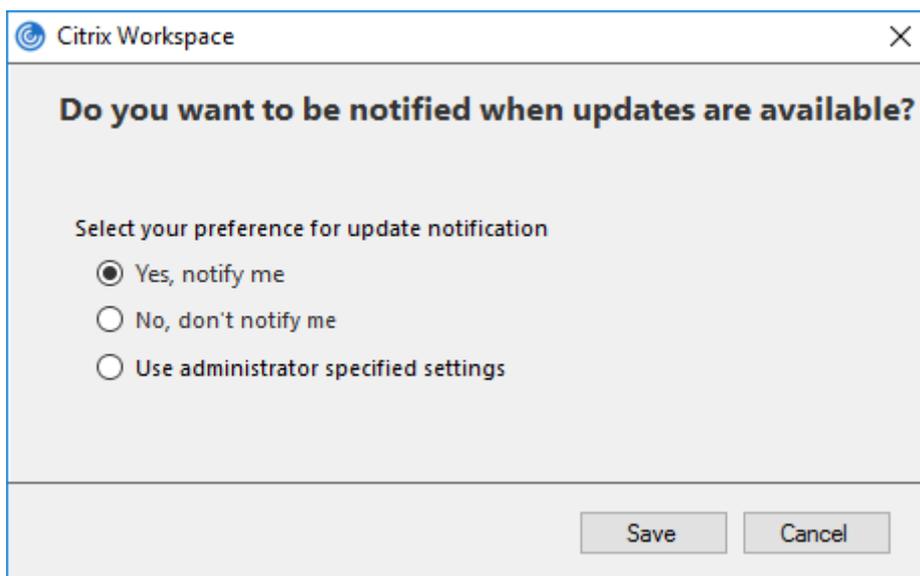
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority= fast
```

注:

`/AutoUpdateCheck` は、`/AutoUpdateStream`、`/DeferUpdateCount`、`/AURolloutPriority` などの他のパラメーターを構成するために設定する必要がある必須パラメーターです。

グラフィカルユーザーインターフェイスを使用した **Citrix Workspace** 更新プログラムの構成

各ユーザーが [高度な設定] ダイアログボックスで [Citrix Workspace の更新] 設定を上書きできます。このような、ユーザーごとの構成および設定は、現在のユーザーにのみ適用されます。システムトレイの Citrix Workspace アプリアイコンを右クリックします。[高度な設定] > [**Workspace** の更新] を選択します。通知設定を選択し、[保存] をクリックします。



注:

システムトレイの [Citrix Workspace アプリ] アイコンで [高度な設定] シートの一部または全部を非表示にすることができます。詳しくは、「[高度な設定シート](#)」セクションを参照してください。

### StoreFront を使用した Citrix Workspace 更新プログラムの構成

1. テキストエディターを使ってストアの `web.config` ファイルを開きます。このファイルは通常、`C:\inetpub\wwwroot\Citrix\Roaming directory` にあります。
2. このファイルで、ユーザーアカウント要素の場所を見つけます（「Store」は使用環境のアカウント名です）。

たとえば、次のようになります: `<account id=... name="Store">`

`</account>` タグの前に、ユーザーアカウントのプロパティに移動します:

```
1 <properties>
2     <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. `<clear/>` タグの後に、自動更新タグを追加します。

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store">
```

```
7      description="" published="true" updaterType="Citrix"
8          remoteAccessType="None">
9      <annotatedServices>
10
11      <clear />
12
13      <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15          <metadata>
16
17              <plugins>
18
19                  <clear />
20
21              </plugins>
22
23              <trustSettings>
24
25                  <clear />
26
27              </trustSettings>
28
29              <properties>
30
31                  <property name="Auto-Update-Check" value="auto" />
32
33                  <property name="Auto-Update-DeferUpdate-Count" value
34                      ="1" />
35
36                      <property name="Auto-Update-LTSR-Only" value
37                          ="FALSE" />
38
39                          <property name="Auto-Update-Rollout-Priority" value=
40                              "fast" />
41
42                      </properties>
43
44                  </metadata>
45
46              </annotatedServiceRecord>
47
48          </annotatedServices>
49
50      </metadata>
```

```
48
49     <plugins>
50
51         <clear />
52
53     </plugins>
54
55     <trustSettings>
56
57         <clear />
58
59     </trustSettings>
60
61     <properties>
62
63         <clear />
64
65     </properties>
66
67 </metadata>
68
69 </account>
70
71 <!--NeedCopy-->
```

以下は、プロパティの意味と使用可能な値の詳細です：

- **Auto-update-Check**: Citrix Workspace アプリが、利用可能な更新を自動的に検出したことを示します。
- **Auto-update-LTSR-Only**: リリースの更新が LTSR のみであることを示します。
- **Auto-update-Rollout-Priority**: 更新を受信できる配信期間を示します。
- **Auto-update-DeferUpdate-Count**: リリースの更新通知を延期できる回数を示します。

はじめに

November 12, 2021

この記事は、Citrix Workspace アプリのインストール後、環境をセットアップする場合に参照できます。

前提条件：

「[システム要件](#)」セクションに記載されたすべての要件を確認してください。

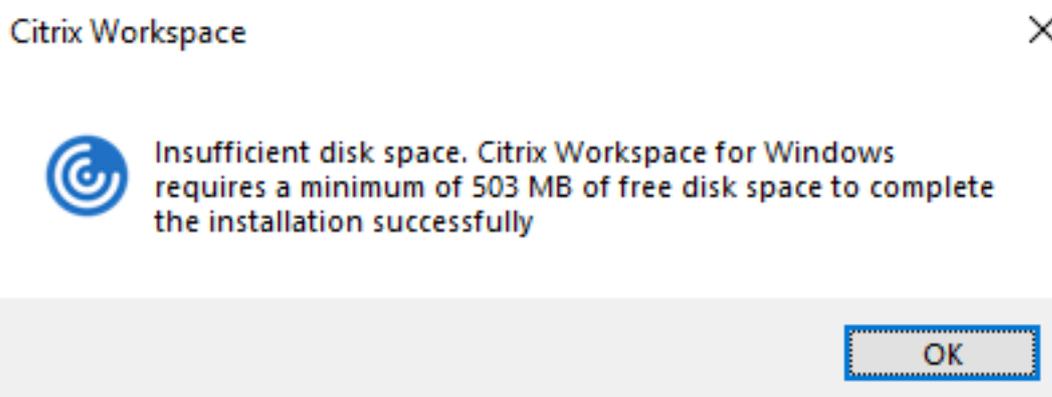
## 空きディスクスペースの検証

インストール前に必要なディスクスペースの詳細については、次の表を参照してください:

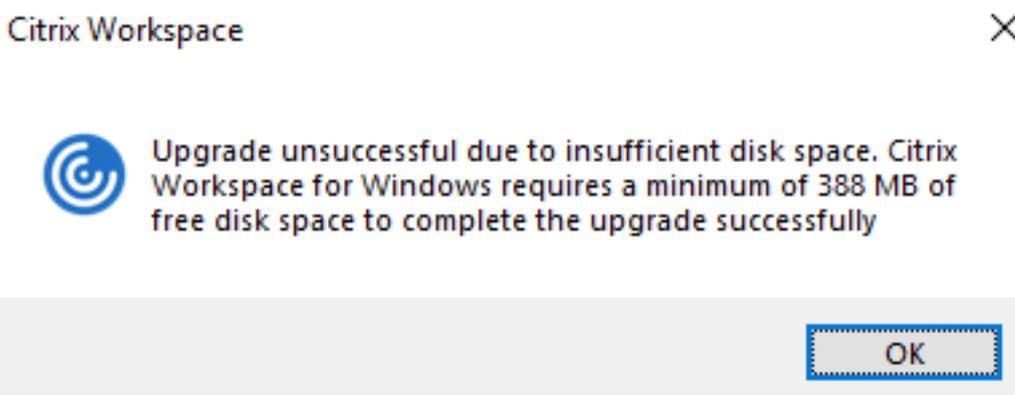
| インストールの種類 | 必要な最小ディスク容量 |
|-----------|-------------|
| 新規インストール  | 572MB       |
| アップグレード   | 350MB       |

Citrix Workspace アプリは、インストールを完了できるだけの十分なディスクスペースがあるかどうかを検証するチェックを実行します。この検証は、新規インストールとアップグレードのどちらの場合にも実行されます。

新規インストール時にディスクスペースが不十分な場合は、インストールが停止し、次のダイアログが表示されます。



Citrix Workspace アプリのアップグレード時にディスクスペースが不十分な場合は、インストールが終了し、次のダイアログが表示されます。



注:

- インストーラーがディスクスペースのチェックを実行するのは、インストールパッケージの抽出後のみです。
- サイレントインストール時にシステムのディスクスペースが少ない場合、ダイアログは表示されません

が、エラーメッセージが `CTXInstall\*_TrolleyExpress-*.log` に記録されます。

Citrix Workspace アプリを使用する前に、次の構成を完了します：

- [グループポリシーオブジェクト管理用テンプレート](#)
- [StoreFront](#)
- [Citrix Gateway ストア](#)
- [ユーザーアカウント](#)
- [クライアント側ドライブのマッピング](#)
- [DNS 名前解決](#)

### グループポリシーオブジェクト管理用テンプレート

次の規則を構成するには、グループポリシーオブジェクト管理用テンプレートを使用することをお勧めします：

- ネットワークルーティング
- プロキシサーバー
- 信頼するサーバーの構成
- ユーザールーティング
- リモートユーザーデバイス
- ユーザーエクスペリエンス

ドメインポリシーおよびローカルコンピューターのポリシーで `receiver.admx/receiver.adml` テンプレートファイルを使用することができます。ドメインポリシーの場合、グループポリシー管理コンソールを使ってテンプレートファイルをインポートします。インポートは、組織全体に存在する多くの異なるユーザーデバイスに Citrix Workspace アプリの設定を適用するのに有用です。単一ユーザーデバイスで変更する場合は、デバイス上のローカルのグループポリシーエディターを使ってテンプレートをインポートします。

Windows グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して Citrix Workspace アプリを構成することをお勧めします。

インストールディレクトリに、`CitrixBase.admx` および `CitrixBase.adml` 管理用テンプレートファイル (`receiver.adml` または `receiver.admx` 'receiver.adml') が含まれています。

注：

.admxml ファイルおよび .adml ファイルは、Windows Vista、Windows Server 2008、および以降の Windows バージョンで使用されます。

例： `<installation directory>\Online Plugin\Configuration`。

Citrix Workspace アプリを VDA なしでインストールする場合、admxml/adml ファイルは通常 `C:\Program Files\Citrix\ICA Client\Configuration` ディレクトリにあります。

Citrix Workspace アプリの各テンプレートファイルとその配置場所については以下の表を参照してください。

## 注:

最新バージョンの Citrix Workspace アプリと共に提供される GPO テンプレートファイルを使用することをお勧めします。

| ファイルタイプ         | ファイルの場所   |
|-----------------|---|
| receiver.adm    | <Installation Directory>\ICA Client\Configuration               |
| receiver.admx   | <Installation Directory>\ICA Client\Configuration               |
| receiver.adml   | <Installation Directory>\ICA Client\Configuration\[MUIculture\] |
| CitrixBase.admx | <Installation Directory>\ICA Client\Configuration               |
| CitrixBase.adml | <Installation Directory>\ICA Client\Configuration\[MUIculture\] |

## 注:

- CitrixBase.admx\adml がローカル GPO に追加されないと、[ICA ファイルの署名を有効にします] ポリシーが失われることがあります。
- Citrix Workspace アプリをアップグレードする場合、最新のテンプレートをローカル GPO に追加します。以前の設定はインポート後も保持されます。詳しくは、次の手順を参照してください:

ローカル **GPO** に **receiver.admx/adml** テンプレートファイルを追加するには:

adm テンプレートファイルを使用して、ローカル GPO とドメインベース GPO の両方を構成できます。ADMX ファイルの管理については、[こちらの Microsoft MSDN の記事](#)を参照してください。

Citrix Workspace アプリをインストールしてから、以下のテンプレートファイルをコピーします:

| ファイルタイプ       | コピー元   | コピー先                               |
|---------------|--|------------------------------------|
| receiver.admx | Installation Directory<br>\ICA Client\<br>Configuration\receiver<br>.adm | %systemroot%\<br>policyDefinitions |

| ファイルタイプ         | コピー元  | コピー先   |
|-----------------|---|--|
| CitrixBase.admx | Installation Directory<br>\ICA Client\<br>Configuration\<br>CitrixBase.admx                 | %systemroot%\<br>policyDefinitions                 |
| receiver.adml   | Installation Directory<br>\ICA Client\<br>Configuration\<br>MUIculture]receiver.<br>adml    | %systemroot%\<br>policyDefinitions\<br>MUIculture] |
| CitrixBase.adml | Installation Directory<br>\ICA Client\<br>Configuration\<br>MUIculture]\CitrixBase<br>.adml | %systemroot%\<br>policyDefinitions\<br>MUIculture] |

注:

CitrixBase.admx/CitrixBase.adml を \PolicyDefinitions フォルダに追加して、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] のテンプレートファイルを表示します。

## StoreFront

さらに、リモートユーザー（インターネットを介して接続するユーザーや遠隔地のユーザーなど）が内部ネットワークにアクセスできるように Citrix Gateway を構成する必要もあります。

注:

[すべてのストアを表示する] オプションを選択すると、古い StoreFront ユーザーインターフェイスが表示されることがあります。

**StoreFront** を構成するには:

[StoreFront](#) のドキュメントを参照して、StoreFront をインストールして構成します。Citrix Workspace アプリを使用するには、HTTPS 接続が必要です。HTTP 構成された StoreFront では、「[コマンドラインパラメーターの使用](#)」の説明に従ってレジストリキーを設定します。

注:

独自の Windows 向け Citrix Workspace アプリダウンロードサイトを作成するためのテンプレートが提供されています。

## Citrix Gateway ストア

グループポリシーオブジェクト管理用テンプレートを使用して **Citrix Gateway** を追加または指定するには:

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] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [StoreFront] の順に移動します。
3. **Citrix Gateway URL/StoreFront** アカウント一覧を選択します。
4. 設定を編集します。
  - [ストア名] - ストアの表示名を指定します。
  - [ストア URL] - ストアの URL を指定します。
  - [#Store name] - Citrix Gateway の背後にあるストアの名前を指定します。
  - ストアの有効状態 - ストアの状態 (オンまたはオフ) を示します。
  - [ストアの説明] - ストアの説明を入力します。
5. Citrix Gateway URL を追加または指定します。URL 名をセミコロンで区切って入力します:

例: CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com##Storename ;On;Store

#Storename は Citrix Gateway の背後にあるストアの名前です。

バージョン 1808 以降、**Citrix Gateway URL/StoreFront** アカウント一覧ポリシーに加えられた変更は、Citrix Workspace アプリを再起動するとセッションに適用されます。リセットは不要です。

注:

Citrix Workspace アプリのバージョン 1808 以降では、新規インストール時のリセットは必要ありません。1808 以降にアップグレードする場合は、変更を有効にするために Citrix Workspace アプリをリセットする必要があります。

制限事項:

- Citrix Gateway URL は先頭に入力し、その後に StoreFront の URL を続ける必要があります。
- 複数の Citrix Gateway URL はサポートされていません。
- Citrix Gateway の URL を上記の方法で構成した場合、Citrix Gateway の後ろにある PNA サービスはサポートされません。

### ワークスペースコントロール再接続の管理

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。Citrix

Workspace アプリの場合、クライアントデバイスのワークスペースコントロールの管理はレジストリを変更して行います。これはまた、グループポリシーを使用するドメイン参加クライアントデバイスに対しても実行できます。

### 注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

**WSCReconnectModeUser** を作成し、既存のレジストリキー **WSCReconnectMode** を Master Desktop Image または Citrix Virtual Apps サーバーで変更します。公開デスクトップでは Citrix Workspace アプリの動作を変更できます。

Citrix Workspace アプリの WSCReconnectMode キー設定は次のとおりです：

- 0 = いずれに既存のセッションにも再接続しない
- 1 = アプリケーションの起動時に再接続する
- 2 = アプリケーションの更新時に再接続する
- 3 = アプリケーションの起動または更新時に再接続する
- 4 = Citrix Workspace インターフェイスを開いたときに再接続する
- 8 = Windows ログオン時に再接続する
- 11 = 3 と 8 の組み合わせ

ワークスペースコントロールを無効にする

ワークスペースコントロールを無効にするには、次のキーを作成します：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 ビット版)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 ビット版)

名前: **WSCReconnectModeUser**

種類: REG\_SZ

値のデータ: 0

次のキーをデフォルト値の3から 0 に変更

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 ビット版)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 ビット版)

名前: **WSCReconnectMode**

種類: REG\_SZ

値のデータ: 0

### 注:

新しいキーを作成しない代わりに、**WSCReconnectAll** を `false` に設定することができます。

### 状態インジケータータイムアウトの変更

ユーザーがセッションを起動しているときに状態インジケータが表示される時間を変更できます。タイムアウト期間を変更するには、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA_CLIENT\Engine\`に `REG_DWORD` 値として `SI_INACTIVE_MS` を作成します。状態インジケータをすぐに非表示したい場合は、`REG_DWORD` 値を4に設定します。

### コマンドラインを使用したアプリケーションショートカットの場所のカスタマイズ

[スタート] メニュー統合およびデスクトップショートカットのみの機能により、公開アプリケーションのショートカットを **Windows** の [スタート] メニューやデスクトップ上に配置できます。ユーザーが Citrix Workspace のユーザーインターフェイスからアプリケーションをサブスクライブする必要はありません。これらの機能により、ユーザーのグループにシームレスなデスクトップエクスペリエンスを提供して、ユーザーは頻繁に使用するアプリケーションに一貫した方法でアクセスできるようになります。

このフラグは **SelfServiceMode** と呼ばれ、デフォルトで `True` に設定されています。管理者が **SelfServiceMode** フラグを `False` に設定すると、セルフサービスのユーザーインターフェイスにアクセスできなくなります。その代わりに、サブスクライブされたアプリには [スタート] メニューから、およびデスクトップショートカットを介してアクセスできます。これは、「ショートカットのみのモード」と呼ばれています。

ユーザーおよび管理者は、複数のレジストリ設定を使用してアプリケーションのショートカットをカスタマイズできます。

### ショートカットの操作

- ユーザーはアプリケーションを削除できません。**SelfServiceMode** フラグを `false` に設定（ショートカットのみのモード）すると、すべてのアプリケーションが必須アプリケーションになります。デスクトップからショートカットアイコンを削除しても、システムトレイの Citrix Workspace アプリアイコンで [更新] を選択すると、アイコンが再表示されます。
- ユーザーはストアを1つだけ構成できます。アカウントおよび基本設定オプションは使用できません。このため、ユーザーが追加のストアを構成できません。管理者はユーザーに特別な権限を付与し、これによりユーザーはグループポリシーオブジェクトテンプレートを使用して、またはクライアントマシンでレジストリキー (`HideEditStoresDialog`) を手動で追加して1つまたは複数のアカウントを追加できます。管理者がユーザーにこの権限を付与すると、ユーザーのシステムトレイの Receiver アイコンに [基本設定] オプションが表示され、アカウントを追加および削除できるようになります。
- ユーザーは **Windows** のコントロールパネルを介してアプリケーションを削除することはできません。

- カスタマイズ可能なレジストリ設定を介してデスクトップショートカットを追加できます。デスクトップショートカットはデフォルトでは追加できません。レジストリ設定を編集後、Citrix Workspace アプリを再起動する必要があります。
- ショートカットは、[スタート] メニューにデフォルトのカテゴリパス UseCategoryAsStartMenuPath で作成されます。

注:

Windows 8、Windows 8.1、Windows 10 では、[スタート] メニュー内には階層分けされたフォルダーを作成できません。アプリケーションは個々に、または Citrix Virtual Apps で定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- インストール時にフラグ [/DESKTOPDIR="Dir\_name"] を指定すると、すべてのショートカットを単一のフォルダー内に配置できます。デスクトップショートカットのため CategoryPath がサポートされません。
- 変更アプリの自動再インストール機能は、レジストリキー `AutoReInstallModifiedApps` を使って有効にできます。`AutoReInstallModifiedApps` が有効な場合、管理者がサーバー上の公開アプリおよび公開デスクトップの属性を変更すると、その変更がすべてクライアントマシンに反映されます。`AutoReInstallModifiedApps` が無効な場合、アプリとデスクトップの属性は更新されず、クライアント上で削除されたショートカットも更新時に復元されません。デフォルトで、`AutoReInstallModifiedApps` は有効になっています。

レジストリエディターを使用したアプリケーションショートカットの場所のカスタマイズ

注:

- デフォルトでは、レジストリキーは文字列形式を使用します。
- ストアを構成する前に、レジストリキーを変更します。レジストリキーをカスタマイズする場合には管理者かユーザーかに関わらず、Citrix Workspace アプリをリセットしてからレジストリキーを構成し、その後でストアを再構成する必要があります。

### 32 ビットマシンのレジストリキー

レジストリキー: **WSCSupported**

値: True

キーのパス:

- ```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID + \Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

レジストリキー: **WSCReconnectAll**

値: True

キーのパス:

```
1 - `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
2 - `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID + \Properties`
3 - `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
4 - `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`
```

レジストリキー: **WSCReconnectMode**

値: 3

キーのパス:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

レジストリキー: **WSCReconnectModeUser**

値: インストール中はレジストリが作成されません。

キーのパス:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
   +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**64** ビットマシンのレジストリキー:

レジストリキー: **WSCSupported**

値: True

キーのパス:

```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
```

- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

レジストリキー: **WSCReconnectAll**

値: True

キーのパス:

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

レジストリキー: **WSCReconnectMode**

値: 3

キーのパス:

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

レジストリキー: **WSCReconnectModeUser**

値: インストール中はレジストリが作成されません。

キーのパス:

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

### ユーザーアカウント

以下を使用して、仮想デスクトップおよびアプリケーションにアクセスするために必要なアカウント情報をユーザーに提供できます：

- メールアドレスによるアカウント検出を構成する
- プロビジョニングファイル
- アカウント情報をユーザーに手入力させる

#### 重要

インストール後に Citrix Workspace アプリを再起動することをお勧めします。これは、ユーザーがアカウントを追加し、Citrix Workspace アプリがインストール時に一時停止状態だった USB デバイスを検出できるようにするためです。

インストールに成功したことを示すダイアログボックスが表示され、[アカウントの追加] ダイアログボックスが開きます。初めて使用するユーザーは、[アカウントの追加] ダイアログボックスにメールまたはサーバーアドレスを入力してアカウントをセットアップする必要があります。

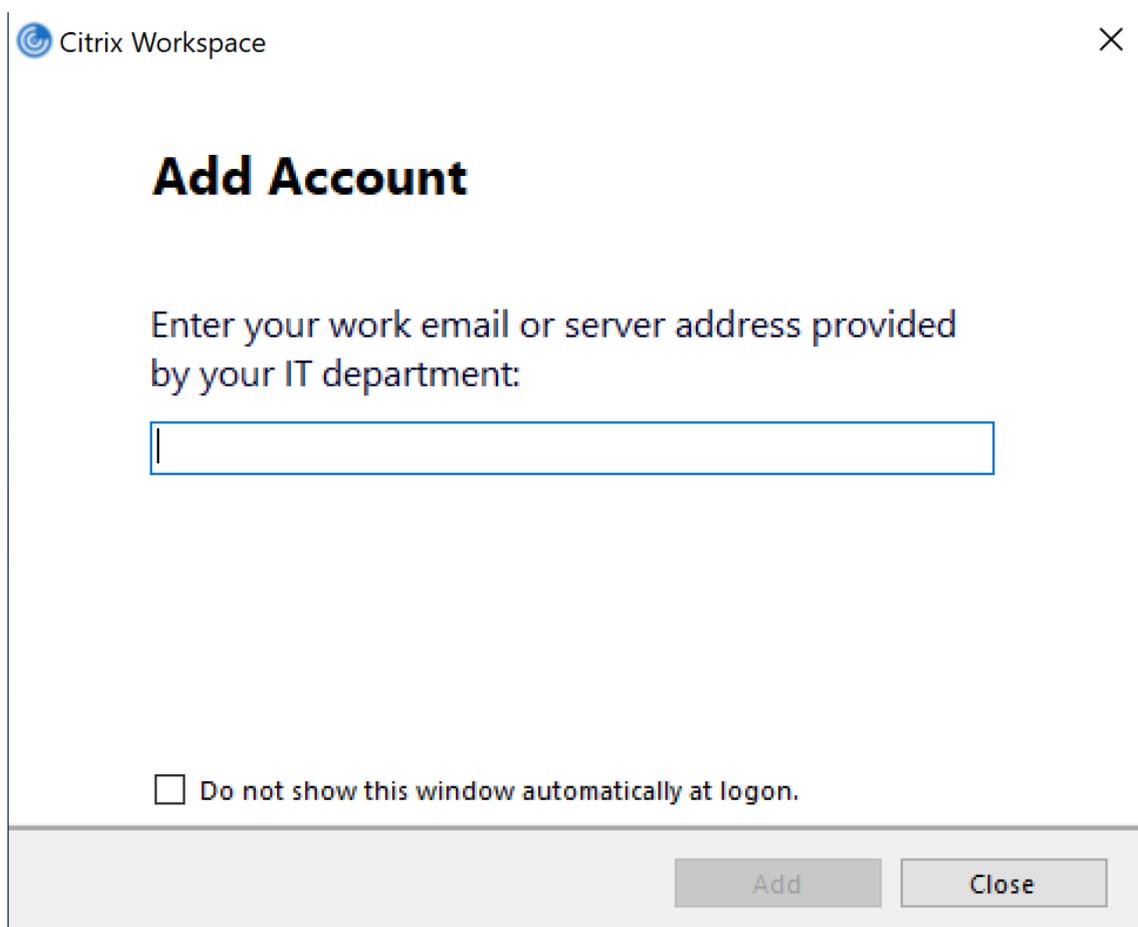
#### [アカウントの追加] ダイアログボックスを非表示にする

ストアが構成されていない場合、[アカウントの追加] ダイアログボックスが表示されます。[アカウントの追加] ダイアログボックスを使って、メールアドレスまたはサーバー URL を入力して Citrix Workspace アプリアカウントをセットアップすることができます。

Citrix Workspace アプリにより、入力したメールアドレスに関連付けられている Citrix Gateway、StoreFront サーバー、または Endpoint Management 仮想アプライアンスが識別され、表示のためにログオンするようメッセージが表示されます。

[アカウントの追加] ダイアログボックスは次の方法で非表示にできます：

1. システムログオン時



次回以降のログオン時に [アカウントの追加] ダイアログボックスがポップアップ表示されないようにするには、[ログオン時に自動的にこのウィンドウを表示しない] チェックボックスをオンにします。これはユーザーごとの設定で、Windows 向け Citrix Workspace アプリのリセット時にリセットされます。

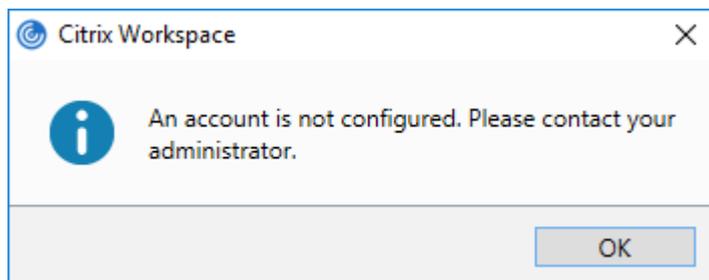
## 2. コマンドラインインストール

管理者として、次のスイッチを指定して Windows 向け Citrix Workspace アプリをインストールします。

```
CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
```

これはマシンごとの設定です。したがって、この動作は、そのマシンのすべてのユーザーに適用されます。

ストアが構成されていない場合は、次のメッセージが表示されます。



[アカウントの追加] ダイアログボックスは次の方法で非表示にできます。

- **Citrix** 実行ファイルの名前を変更する:

ファイルの名前を **CitrixWorkspaceApp.exe** から **CitrixWorkspaceAppWeb.exe** に変えて、[アカウントの追加] ダイアログボックスの動作を変更します。名前を変更することにより、[アカウントの追加] ダイアログボックスが [スタート] メニューに表示されなくなります。

- レジストリエディター:

Citrix Workspace アプリのインストールウィザードで [アカウントの追加] オプションを非表示するには、`HKEY_CURRENT_USER\Software\Citrix\Receiver`パスに移動して `DWORD HideAddAccountOnRestart` キーを値「00000001」に設定します。

### メールアドレスによるアカウント検出を構成する

管理者がメールアドレスによるアカウント検出機能を有効にした場合、ユーザーは Citrix Workspace アプリの初期設定時にサーバーの URL の代わりに自分のメールアドレスを入力できます。Citrix Workspace アプリで、DNS (Domain Name System) サービス (SRV) レコードによりメールアドレスに関連付けられている Citrix Gateway または StoreFront サーバーが検出され、仮想デスクトップやアプリケーションにアクセスするためのログオンを求めるメッセージが表示されます。

詳しくは、「[メールアドレスによるアカウント検出を構成する](#)」を参照してください。

### ユーザーにプロビジョニングファイルを提供する

StoreFront により提供されるプロビジョニングファイルを使用して、ユーザーはストアに接続できます。

管理者は、StoreFront を使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、Citrix Workspace アプリを自動的に構成できるようにします。Citrix Workspace アプリのインストール後、ファイルを開いて Citrix Workspace アプリを構成するだけです。Web 向け Workspace を構成すると、ユーザーはそれらのサイトから Citrix Workspace アプリのプロビジョニングファイルを取得することもできます。

詳しくは、StoreFront のドキュメントの「[ユーザーに配布するストアプロビジョニングファイルをエクスポートするには](#)」を参照してください。

### アカウント情報をユーザーに手入力させる

ユーザーが手動でアカウントをセットアップできるようするには、ユーザーが仮想デスクトップとアプリケーションへ接続するために必要とする情報を提供します。

- StoreFront ストアへの接続の場合は、そのサーバーの URL を提供します。例: `https://servername.company.com`。
- Citrix Gateway を介する接続の場合は、ユーザーがすべての構成済みストアを表示する必要があるのか、または特定の Citrix Gateway に対するリモートアクセスが有効になった単一のストアだけにアクセスする必要があるのかを最初に判断します。

- 構成済みストアをすべて表示させる場合は、ユーザーに Citrix Gateway の完全修飾ドメイン名を提供します。
- 特定のストアへのアクセスに限定する場合は、ユーザーに Citrix Gateway の完全修飾ドメイン名とストア名を次の形式で提供します。

### CitrixGatewayFQDN?MyStoreName:

たとえば、「SalesApps」という名前のストアで server1.com へのリモートアクセスが有効で、「HRApps」という名前のストアで server2.com へのリモートアクセスが有効な場合、ユーザーが SalesApps にアクセスするには <server1.com?SalesApps>、HRApps にアクセスするには <server2.com?HRApps> と入力する必要があります。この機能では、新規ユーザーは URL を入力してアカウントを作成する必要があり、電子メールベースの検出は使用できません。

ユーザーが新しいアカウントの詳細を入力すると、Citrix Workspace アプリにより接続が検証されます。検証に成功すると、そのアカウントにログオンするための画面が開きます。

アカウントを管理するには、Citrix Workspace アプリのホームページを開き、、[アカウント] の順にクリックします。

### 複数のストアアカウントの自動的共有

#### 警告

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

複数のストアアカウントがある場合は、セッションの確立時に Windows 向け Citrix Workspace アプリを構成してすべてのアカウントに自動的に接続できます。Citrix Workspace アプリを開くときにすべてのアカウントを自動的に表示するには、次の操作を実行します：

#### 32 ビットシステム：

キーのパス: `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`

キーの名前: `CurrentAccount`

値: `AllAccount`

種類: `REG_SZ`

#### 64 ビットシステム：

キーのパス: `HKEY_LOCAL_MACHINE\\Software\\Wow6432Node\\Citrix\\Dazzle`

キーの名前: `CurrentAccount`

値: `AllAccount`

種類: `REG_SZ`

### クライアントドライブマッピング

Windows 向け Citrix Workspace アプリではクライアント側デバイスのマッピング（割り当て）機能がサポートされており、ユーザーはセッション内でこれらのデバイスを使用できます。次のことを実行できます：

- ローカルのディスクドライブ、プリンター、および COM ポートにセッションから透過的にアクセスする。
- セッションとローカルの Windows クリップボードの間で、データをコピーして貼り付ける。
- セッション内で、サーバー上のサウンドを再生する。

Citrix Workspace アプリでサーバーにログオンすると、使用できるクライアントドライブ、COM ポート、LPT ポートなどがサーバーに通知されます。デフォルトでは、クライアントドライブがサーバーのドライブ文字にマップされ、クライアントプリンターの印刷キューがサーバー上に作成されます。このため、これらのデバイスがサーバーに直接接続されているかのように見えます。マップされたクライアント側デバイスは、そのセッションを実行中のユーザーだけが使用できます。ユーザーがログオフするとマッピングが削除され、そのユーザーが次にログオンしたときに再び作成されます。

ログオン時に特定のデバイスが自動的にマップされないように設定するには、ポリシーのリダイレクト設定を使用します。詳しくは、Citrix Virtual Apps and Desktops ドキュメントを参照してください。

### デバイスマッピングを無効にする

**Windows** のサーバーマネージャーを使用して、ユーザーデバイスマッピング（ドライブ、プリンター、ポートなどのオプション）を構成できます。指定できるオプションについて詳しくは、リモートデスクトップサービスのドキュメントを参照してください。

### クライアントフォルダーのリダイレクト

クライアントフォルダーのリダイレクトは、クライアント側のファイルがホスト側のセッションのへアクセスする方法を変更します。サーバー上でクライアント側ドライブのマッピングのみを有効にすると、クライアントの側の全ボリュームが UNC (Universal Naming Convention) リンクとしてセッションに自動的にマップされます。管理者がサーバー上でクライアントフォルダーのリダイレクトを有効にして、ユーザーがそれをユーザーデバイス上で構成すると、ユーザーが指定したローカルボリュームの一部がリダイレクトされます。

セッション内では、ユーザーデバイス上のすべてのファイルシステムの代わりにユーザー指定のフォルダーのみが UNC リンクとして表示されます。レジストリで UNC リンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。構成方法など、クライアントフォルダーのリダイレクトについて詳しくは Citrix Virtual Apps and Desktops のドキュメントを参照してください。

### クライアントドライブをホスト側のドライブ文字にマップする

クライアント側ドライブのマッピング機能により、ホスト側のドライブ文字をユーザーデバイス上のドライブとしてリダイレクトできます。たとえば、Citrix ユーザーセッション内で表示される H ドライブにアクセスしたときに、

Windows 向け Citrix Workspace アプリを実行するユーザーデバイスの C ドライブにリダイレクトされるように設定できます。

クライアントドライブマッピングは、Citrix の標準デバイスリダイレクト機能に透過的に組み込まれています。この方法でマップされたドライブ文字は、通常のネットワークドライブのマッピングの場合と同様に、ファイルマネージャー、エクスプローラー、およびアプリケーションで使用することができます。

仮想デスクトップやアプリケーションをホストするサーバーにインストールするときに、クライアントドライブが自動的にマップされるサーバーのドライブ文字のセットを設定できます。デフォルトでは、インストール時に、個々のハードディスクおよび CD ドライブに 1 文字ずつ、V からのアルファベットで未使用のドライブ文字がマップされます（クライアントのフロッピーディスクドライブには、元のドライブ文字がそのままマップされます）。この場合、セッションでのドライブマッピングは、次のようになります：

---

| クライアントドライブ文字 | セッション内でアクセスするときのドライブ文字 |
|--------------|------------------------|
| A            | A                      |
| B            | B                      |
| C            | V                      |
| D            | U                      |

---

サーバーの既存のドライブ文字をアルファベットの後ろの方の文字に変更しておくと、サーバー側のドライブ文字がクライアント側のもとの競合しなくなるため、ユーザーはローカルドライブと同じドライブ文字をセッション内で使用できます。たとえば、サーバーの C ドライブを M に変更し、D を N に変更しておくと、クライアントデバイスの既存の C ドライブや D ドライブにそのままアクセスできます。この場合、セッションでのドライブマッピングは、次のようになります：

---

| クライアントドライブ文字 | セッション内でアクセスするときのドライブ文字 |
|--------------|------------------------|
| A            | A                      |
| B            | B                      |
| C            | C                      |
| D            | D                      |

---

サーバーの C ドライブを置き換えるために使用するドライブ文字は、インストール時に定義できます。そのほかの固定ドライブおよび CD/DVD ドライブのドライブ文字は、連続するドライブ文字に置き換えられます。たとえば、C ドライブは M、D は N、E は O に置き換えられます。これらのドライブ文字が、既存のネットワークドライブのマッピングと競合しないようにしてください。ネットワークドライブにマップされたドライブ文字がサーバーのドライブ文字と競合する場合、ネットワークドライブのマッピングが無効になります。

クライアント側デバイスの自動マッピングを無効にしない限り、ユーザーデバイスでサーバーに再接続すると、マッピングが再確立されます。デフォルトでは、クライアントドライブマッピングが有効になっています。設定を変更するには、リモートデスクトップ（ターミナルサービス）構成ツールを使用します。また、ポリシーを使用して、クライアントデバイスマッピングを詳細に制御できます。ポリシーについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントを参照してください。

### HDX Plug-n-Play USB デバイスリダイレクト

HDX Plug-n-Play の USB デバイスリダイレクトにより、カメラ、スキャナー、メディアプレーヤー、および POS 端末など、ユーザー側のさまざまなデバイスをサーバーに動的にリダイレクトできます。管理者やユーザーは、すべてまたは一部のデバイスのリダイレクトを制限できます。サーバー上でポリシーを編集するかユーザーデバイス上でグループポリシーを適用して、リダイレクト設定を構成します。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[USB とクライアント側ドライブの考慮事項](#)」を参照してください。

#### 重要

サーバーポリシーでこの USB デバイスリダイレクトを禁止すると、ユーザー側でこの機能を有効にすることはできなくなります。

ユーザーは、デバイスのリダイレクトを常に許可または拒否するか、またはデバイスの接続時に毎回確認のメッセージを表示するように設定できます。この設定は、Citrix Workspace アプリで行います。この設定は新しく接続するデバイスにのみ適用され、接続済みのデバイスには適用されません。

クライアントの **COM** ポートをサーバーの **COM** ポートにマップするには：

クライアント側 COM ポートのマッピングを有効にすると、セッション内でローカルマシンの COM ポート上のデバイスにアクセスできるようになります。マップされたクライアントの COM ポートは、ほかのネットワークドライブのマッピングと同様の方法で使用できます。

コマンドプロンプトからクライアント COM ポートをマップできます。また、Windows の管理ツールのリモートデスクトップ（ターミナルサービス）構成ツールまたはポリシーを使用して、クライアント COM ポートのマッピングを制御することもできます。ポリシーについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントを参照してください。

#### 重要

COM ポートマッピングは TAPI 対応ではありません。

1. Citrix Virtual Apps and Desktops の展開では、クライアント COM ポートリダイレクトポリシー設定を有効にします。
2. Citrix Workspace アプリにログオンします。
3. コマンドプロンプトで、次のコマンドを実行します：

```
net use comx: \\client\comz:
```

ここで、<x> にはサーバー上の COM ポート番号（ポート 1~9）を指定し、<z> にはクライアントデバイス上の COM ポート番号を指定します。

#### 4. 操作を確認するには、

```
net use
```

と入力し Enter キーを押します。マップされているドライブ、LPT ポート、およびマップされている COM ポートの一覧が表示されます。

この COM ポートを仮想デスクトップやアプリケーションのセッションで使用するには、割り当てられている COM ポートにデバイスをインストールします。たとえば、クライアントの COM1 をサーバーの COM5 にマップするには、セッション内で、COM5 に COM ポートデバイスをインストールします。この方法でマップした COM ポートは、ユーザーデバイスの COM ポートと同じように使用できます。

### DNS 名前解決

Citrix XML Service を使用してサーバーファームに接続するときに、サーバーの IP アドレスの代わりに DNS (Domain Name System: ドメインネームシステム。host.subdomain.co.jp など) 名を要求するように Windows 向け Citrix Workspace アプリを構成できます。

#### 重要:

この機能を使用するために DNS 環境を設定していない場合は、Citrix ではサーバーで DNS アドレス解決を有効にしないことをお勧めします。

デフォルトで、DNS 名前解決はサーバーで無効、Citrix Workspace アプリで有効になっています。サーバーで DNS 名前解決が無効になっている場合、Citrix Workspace アプリが DNS 名を要求すると IP アドレスが返されません。Citrix Workspace アプリで DNS アドレス解決を無効にする必要はありません。

特定のユーザーデバイスの **DNS** アドレス解決を無効にするには:

DNS によるサーバー名解決が使用される環境で特定のユーザーデバイスでの問題を解決するには、そのデバイスの DNS 名前解決を無効にします。

#### 注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. レジストリキー `HKEY\\_LOCAL\\_MACHINE\\Software\\Wow6432Node\\Citrix\\ICA Client\\Engine\\Lockdown Profiles\\All Regions\\Lockdown\\Application Browsing` に 文字列値 `xmlAddressResolutionType` を追加します。
2. 値を **IPv4-Port** に設定します。
3. ユーザーデバイスの各ユーザーでこれを繰り返します。

### カスタム **Web** ストア

この機能は、Technical Preview 段階です。Windows 向け Citrix Workspace アプリから組織のカスタム Web ストアにアクセスできます。この機能を使用するには、管理者はドメインまたはカスタム Web ストアを Global App Configuration Service で許可されている URL の一覧に追加する必要があります。

エンドユーザー向けの Web ストア URL の構成について詳しくは、「[Global App Configuration Service](#)」を参照してください。

Citrix Workspace アプリの [アカウントの追加] 画面でカスタム Web ストアの URL を指定できるようになりました。カスタム Web ストアはネイティブの Workspace アプリウィンドウで開きます。

カスタム Web ストアを削除するには、[アカウント] > [アカウントの追加または削除] に移動して、カスタム Web ストアの URL を選択し、[削除] をクリックします。

### 構成

December 9, 2021

Windows 向け Citrix Workspace アプリを使用する場合、ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、以下の構成を行う必要があります。

### Microsoft Teams

- [エンコーダーのパフォーマンス見積もりツール](#)
- [画面共有](#)

### 画面共有

バージョン 2006.1 以降、HDX 最適化を使用する Microsoft Teams アプリケーションの送信画面共有機能に新しい機能が導入されました。

Microsoft Teams を使用して共有されるコンテンツは、**Desktop Viewer** ウィンドウのコンテンツに限定されます。**Desktop Viewer** ウィンドウ外の領域（クライアントのローカルデスクトップ、アプリ）は黒く表示されます。

Windows 10 オペレーティングシステムでは、**Desktop Viewer** ウィンドウと重なっても、次の項目は黒く表示されません：

- [スタート] メニュー、[検索] メニュー、タスクビュー
- 通知バーとタスクバーの右側に表示される通知。
- 異なる DPI 設定でセットアップされたマルチモニターで、ローカルアプリが 2 つの異なるモニターで重なっていて、その DPI が Desktop Viewer ウィンドウが表示されているメインモニターと一致しない場合。
- タスクバーのアプリのアイコンにマウスカーソルを合わせると、[アプリとプレビュー] が表示されます。

## エンコーダーのパフォーマンス見積もりツール

`HdxTeams.exe`は、Microsoft Teams のリダイレクトを処理する Citrix Workspace アプリに組み込まれた WebRTC メディアエンジンです。`HdxTeams.exe`は、エンドポイントの CPU が過負荷状態になることなく維持できる最適なエンコーディングの解像度を見積もることができます。使用できる値は、240p、360p、720p、1080p です。

`HdxTeams.exe` が初期化されると、パフォーマンスの見積プロセス (`webrtcapi.EndpointPerformance`とも呼ばれます) が実行されます。マクロブロックコードは、特定のエンドポイントで達成できる最適な解像度を決定します。コーデックネゴシエーションには、可能な限り高い解像度が使用されます。コーデックネゴシエーションは、ピア間、またはピアと会議サーバー間で行われることがあります。

エンドポイントには次の 4 つのパフォーマンスカテゴリがあり、それぞれ使用可能な最大解像度が指定されています:

| エンドポイントのパフォーマンス | 最大解像度                                                             | レジストリキー値 |
|-----------------|-------------------------------------------------------------------|----------|
| fast            | 1080p                                                             | 3        |
| medium          | 720p                                                              | 2        |
| slow            | 360p                                                              | 1        |
| very slow       | 240p                                                              | 0        |
| fast            | 1080p (1920x1080 16:9 @ 30fps)                                    | 3        |
| medium          | 720p (1280x720 16:9 @ 30fps)                                      | 2        |
| slow            | 360p (640x360 16:9 @ 30fps<br>または 640x480 4:3 @ 30fps の<br>いずれか)  | 1        |
| very slow       | 240p (320x180 16:9 @ 30 fps<br>または 320x240 4:3 @ 30fps の<br>いずれか) | 0        |

構成フラグを使用して、VP9 または H264 コーデックを無効にできます。

H264 が CPU 上で使用する CPU は比較的少ない量であり、より多くの帯域幅を消費します。一方、VP9 はより少ない帯域幅を使用してより多くの CPU リソースを消費します。

**Citrix Workspace** アプリのレジストリパス:

レジストリパス `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` に移動し、次のキーを作成します: \

| 名前                  | 種類    | 値       | 説明                                                                |
|---------------------|-------|---------|-------------------------------------------------------------------|
| DisableVP9          | DWORD | 1; 0    | 1 - VP9 コーデックを無効にする。0 - 有効にする                                     |
| DisableH264         | DWORD | 1;0     | 1 - H.264 コーデックを無効にする。0 - 有効にする                                   |
| OverridePerformance | DWORD | 0;1;2;3 | 目的のパフォーマンスを適用する。値は 0~3 の範囲にする必要があります。0 は非常に遅く、3 は非常に高速であることを示します。 |

Microsoft Teams の最適化について詳しくは、「[Microsoft Teams の最適化](#)」を参照してください。

#### 管理者のタスクと注意事項

ここでは、Windows 向け Citrix Workspace アプリの管理者に関連するタスクと注意事項について説明します。

#### 機能フラグ管理

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、機能フラグと、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。

LaunchDarkly へのトラフィックと通信は、次の方法で有効化できます：

次の **URL** へのトラフィックを有効にする

- [events.launchdarkly.com](https://events.launchdarkly.com)
- [stream.launchdarkly.com](https://stream.launchdarkly.com)
- [clientstream.launchdarkly.com](https://clientstream.launchdarkly.com)
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- [mobile.launchdarkly.com](https://mobile.launchdarkly.com)

### IP アドレスの許可リストを作成する

IP アドレスの許可リストを作成する必要がある場合、現在のすべての IP アドレス範囲については、「[LaunchDarkly のパブリック IP 一覧](#)」を参照してください。この一覧を使用すると、インフラストラクチャの更新に合わせてファイアウォールの構成が自動的に更新されます。インフラストラクチャの変更の状態について詳しくは、[LaunchDarkly Statuspage](#)のページを参照してください。

### LaunchDarkly のシステム要件

Citrix ADC の分割トンネリングが以下のサービスに対して [オフ] に設定されている場合、アプリがこれらのサービスと通信できることを確認してください：

- LaunchDarkly サービス。
- APNs リスナーサービス

### アプリ保護

#### 免責事項

アプリ保護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、このアプリ保護ポリシーは、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きます。引き続きこうした方法に対応していきませんが、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。

アプリ保護は、Citrix Virtual Apps and Desktops の使用時にセキュリティを強化する機能です。この機能により、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性が制限されます。アプリ保護では、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。

アプリ保護では、ライセンスサーバーにアドオンライセンスをインストールする必要があります。Citrix Virtual Desktops ライセンスも必要です。ライセンスについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[構成](#)」セクションを参照してください。

#### 要件：

- Citrix Virtual Apps and Desktops バージョン 1912 以降。
- StoreFront バージョン 1912。
- Citrix Workspace アプリバージョン 1912 以降。

#### 前提条件：

- Controller でアプリ保護機能を有効にする必要があります。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[アプリ保護](#)」セクションを参照してください。

以下のいずれかの方法で、Citrix Workspace アプリにアプリ保護コンポーネントを追加できます：

- Citrix Workspace アプリのインストール中（コマンドラインインターフェイスまたは GUI を使用）、または
- アプリの起動中（オンデマンドインストール）。

注:

- この機能は、Windows 10、Windows 8.1 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。注：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。したがって、アプリ保護は 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。

オンプレミスの **HDX** セッション保護:

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。これらのポリシーは、PowerShell を使用して構成する必要があります。この目的のために利用可能な GUI はありません。

注:

バージョン 2103 以降、Citrix Cloud Virtual Apps and Desktops サービスは StoreFront でのみアプリ保護をサポートします。

Citrix Virtual Apps and Desktops でのアプリ保護の構成については、「[アプリ保護](#)」を参照してください。

アプリ保護 - **Citrix Workspace** アプリの構成

注:

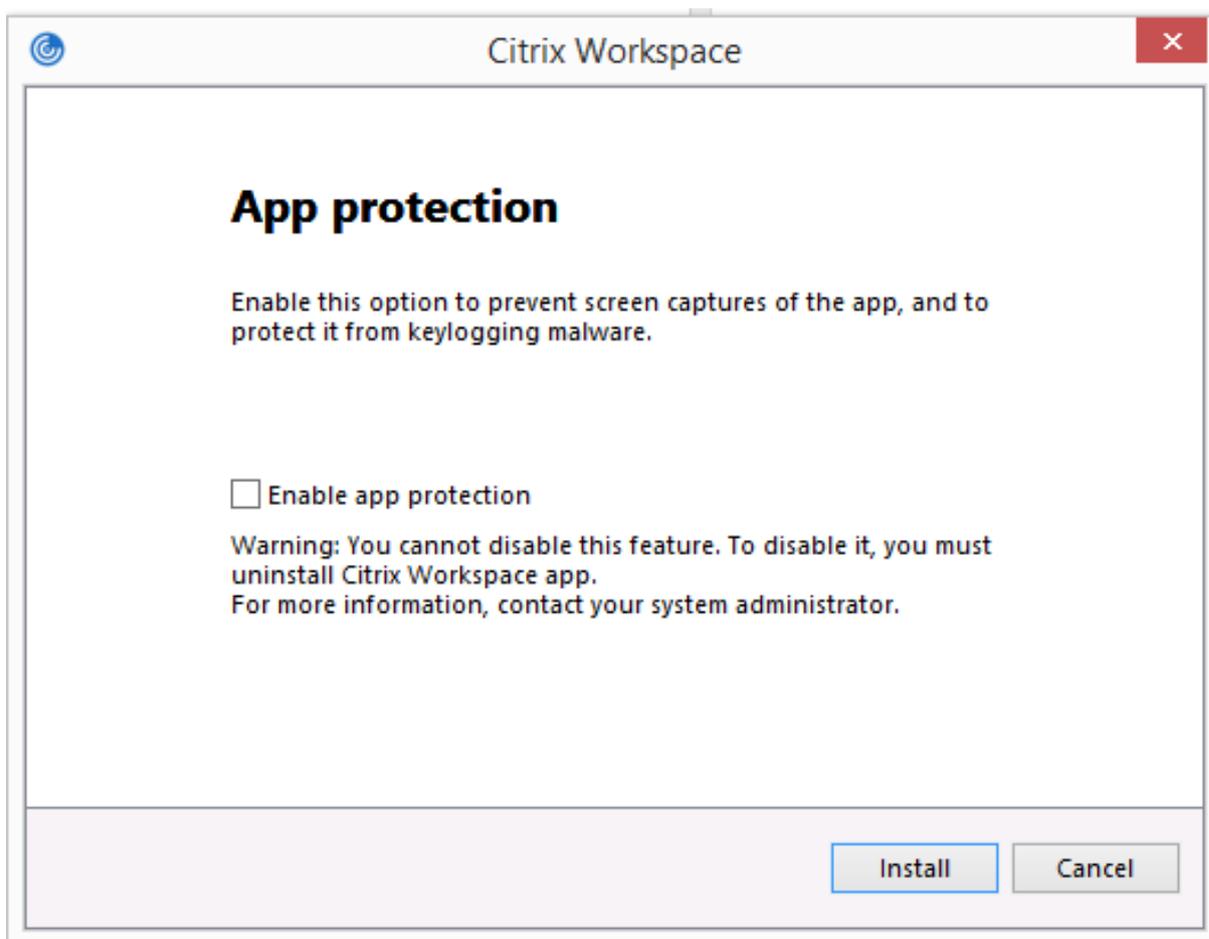
- 管理者から指示があった場合にのみ、Citrix Workspace アプリにアプリ保護コンポーネントを含めません。
- アプリ保護コンポーネントを追加すると、デバイスの画面キャプチャ機能に影響が及ぶ場合があります。

Citrix Workspace アプリのインストール中に、次のいずれかの方法でアプリ保護を追加できます:

- GUI
- コマンドラインインターフェイス

### GUI

Citrix Workspace アプリのインストール中に、次のダイアログボックスを使用してアプリ保護コンポーネントを追加します。[アプリ保護を有効にする] を選択し、[インストール] をクリックしてインストールを続行します。



## 注:

インストール中にアプリの保護を有効にしないと、保護されたアプリを起動するときにプロンプトが表示されます。その場合、プロンプトに従ってアプリ保護コンポーネントをインストールします。

## コマンドラインインターフェイス

Citrix Workspace アプリのインストール中にコマンドラインスイッチ/`includeappprotection`を使用して、アプリ保護コンポーネントを追加します。

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:

| アプリ保護の展開                  | 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 Auth Manager/ [ユーザー認証情報] 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 |

| アプリ保護の展開       | 保護される画面                    | 保護されない画面                                                            |
|----------------|----------------------------|---------------------------------------------------------------------|
| 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 |

以前のリリースでは、保護されたウィンドウのスクリーンショットを撮影しようとする、バックグラウンドの保護されていないアプリを含む画面全体が黒く表示されていました。

バージョン 2008 以降、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。

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。

注:

- 保護されたセッションの起動には、ネイティブの Citrix Workspace アプリのみを使用することをお勧めします。

• **Web 向け Workspace** での動作:

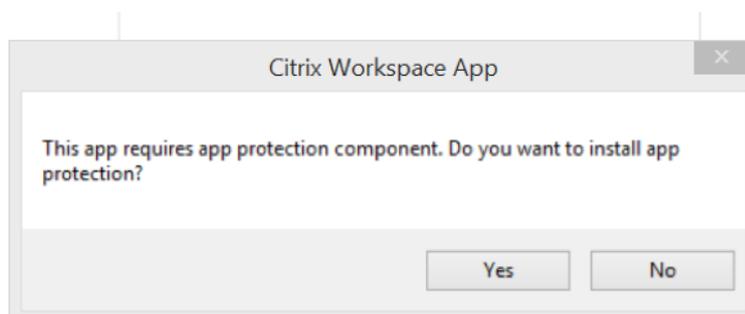
アプリ保護コンポーネントは、Web 向け Workspace の構成ではサポートされません。アプリ保護ポリシーで保護されているアプリケーションは列挙されません。割り当てられるリソースについては、システム管理者にお問い合わせください。

• アプリ保護をサポートしない **Citrix Workspace** アプリバージョンでの動作:

Citrix Workspace アプリのバージョン 1911 以前では、アプリ保護ポリシーで保護されているアプリケーションは StoreFront で列挙されません。

• **Controller** にアプリ保護機能が構成されているアプリの動作:

アプリ保護機能が構成されている Controller で、保護されているアプリケーションを起動しようとする、アプリ保護はオンデマンドでインストールされます。次のダイアログボックスが開きます:



[はい] をクリックして、アプリ保護コンポーネントをインストールします。保護されているアプリを起動できるようになります。

- リモートデスクトッププロトコル (**RDP**) の場合の保護されたセッションの動作
  - リモートデスクトッププロトコル (RDP) セッションを起動すると、アクティブな保護されたセッションが切断されます。
  - リモートデスクトッププロトコル (RDP) セッションでは、保護されたセッションを起動できません。

### アプリ保護構成の機能強化

以前は、デフォルトで、Authentication Manager と Self-service Plug-in のダイアログが保護されていました。

バージョン 2012 以降、Citrix Workspace アプリにはグループポリシーオブジェクト (GPO) ポリシーが導入され、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に、キーロガー対策および画面キャプチャ対策機能を構成できるようになりました。

#### 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 Gateway Service を使用して制御されます。

### Self-service Plug-in インターフェイスのアプリ保護の構成:

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. Self-service Plug-in ダイアログ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] > [アプリ保護の管理] 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。

### Authentication Manager のアプリ保護の構成:

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. 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] > [アプリ保護の管理] 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。

アプリ保護のエラーログ:

バージョン 2103 以降、アプリ保護のログは Citrix Workspace アプリログの一部として収集されます。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。

アプリ保護のログを収集するために、別途サードパーティのアプリをインストールしたり使用したりする必要はありません。ただし、DebugView は引き続きログ収集に使用できます。

アプリ保護のログはデバッグ出力に登録されます。これらのログを収集するには、次の手順を実行します:

1. Microsoft の Web サイトから [DebugView](#) アプリをダウンロードしてインストールします。
2. コマンドプロンプトを起動して、次のコマンドを実行します:

```
Dbgview.exe /t /k /v /l C:\logs.txt
```

上記の例から、`log.txt` ファイル内のログを表示することができます。

このコマンドでは以下が表示されます:

- `/t` — DebugView アプリが、システムトレイで最小化されて開始されます。
- `/k` — カーネルキャプチャを有効にします。
- `/v` — 詳細カーネルキャプチャを有効にします。
- `/l` — 出力を特定のファイルに記録します。

アプリ保護コンポーネントのアンインストール:

アプリ保護コンポーネントをアンインストールするには、システムから Citrix Workspace アプリをアンインストールする必要があります。変更を保存するには、システムを再起動します。

注:

アプリ保護は、バージョン 1912 以降のアップグレードでのみサポートされます。

既知の問題または制限事項:

- この機能は、Windows Server 2012 R2 や Windows Server 2016 などの Microsoft サーバーのオペレーティングシステムではサポートされません。
- この機能は、ダブルホップのシナリオではサポートされません。
- この機能を適切に機能させるには、VDA でクライアントクリップボードリダイレクトポリシーを無効にします。

### ICA ファイルのセキュリティの向上 - Technical Preview

以前のリリースでは、Citrix Virtual Apps and Desktops セッションを起動すると、ICA ファイルがローカルディスクにダウンロードされます。

バージョン 2106 以降では、Citrix Virtual Apps and Desktops セッションの起動時に Citrix Workspace アプリが ICA ファイルを処理する場合のセキュリティが強化されています。

Citrix Workspace アプリでは、ICA ファイルをローカルディスクではなくシステムメモリに保存できるようになりました。この機能は、ローカルに保存されたときに ICA ファイルを悪用する可能性のある攻撃やマルウェアを排除することを目的としています。この機能は、Web 向け Workspace で起動される Citrix Virtual Apps and Desktops セッションにも適用できます。

この機能に関するフィードバックを提供するには、[Podio のフォーム](#)を使用します。

### 構成

注:

この構成手順は、Technical Preview のビルドにのみ適用されます。

**ICA** ファイルのセキュリティを有効にするには:

1. レジストリエディターを起動します。
2. 次のレジストリパスに移動します:
  - 管理者の場合は、`\HKEY_LOCAL_MACHINE\SOFTWARE\[WOW6432Node]\Citrix\Dazzle` に移動します。
  - 管理者以外の場合は、`\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` に移動します。
3. 次の属性でレジストリキーを作成します:  
レジストリキー名: `EnableIcaFileInMemory`  
種類: 文字列値  
値: `True`
4. Windows 向け Citrix Workspace アプリのセッションを再起動して、この変更を有効にします。

ICA ファイルのセキュリティは、Citrix Workspace または StoreFront に Web 経由でアクセスする場合にもサポートされます。Web 経由でアクセスした場合にこの機能が動作するためには、クライアントの検出が前提条件です。上記の構成に加えて、ブラウザーを使用して StoreFront にアクセスしている場合は、StoreFront 展開の `web.config` ファイルで次の属性を有効にします:

| StoreFront のバージョン | 属性                           |
|-------------------|------------------------------|
| 2.x               | <code>pluginassistant</code> |
| 3.x               | <code>protocolHandler</code> |

ブラウザーからストアにログオンするときは、必ず **[Workspace を検出]** をクリックしてください。プロンプトが表示されない場合は、ブラウザーの Cookie をクリアして、再試行してください

Workspace 展開の場合、[アカウント設定] > [詳細] > [アプリおよびデスクトップの起動設定] に移動してクライアント検出設定を見つけることができます。

システムメモリに保存されている ICA ファイルを使用してのみセッションが開始されるように、追加の対策を講じることができます。次のいずれかの方法を使用します：

- クライアント上のグループポリシーオブジェクト (GPO) 管理用テンプレート。
- Global App Config Service。
- Web 向け Workspace。

### **GPO** の使用：

ローカルディスクに保存されている ICA ファイルからのセッションの起動をブロックするには、次の手順を実行します：

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] > [クライアントエンジン] の順に移動します。
3. [ICA ファイルからの直接起動を禁止する] ポリシーを選択し、[有効] に設定します。
4. [適用]、[OK] の順にクリックします。

### **Global App Config Service** の使用：

ローカルディスクに保存されている ICA ファイルからのセッションの起動をブロックするには、次の手順を実行します：

**Block Direct ICA File Launches** 属性を **True** に設定します。

Global App Config Service について詳しくは、[Global App Config Service](#) のドキュメントを参照してください。

### **Web** 向け **Workspace** の使用：

Web 向け Workspace を使用しているときにローカルディスクへの ICA ファイルのダウンロードを禁止するには、次の手順を実行します：

PowerShell モジュールを実行します。「[DisallowICADownload を構成する](#)」を参照してください。

注：

**DisallowICADownload** ポリシーは、StoreFront 展開では使用できません。

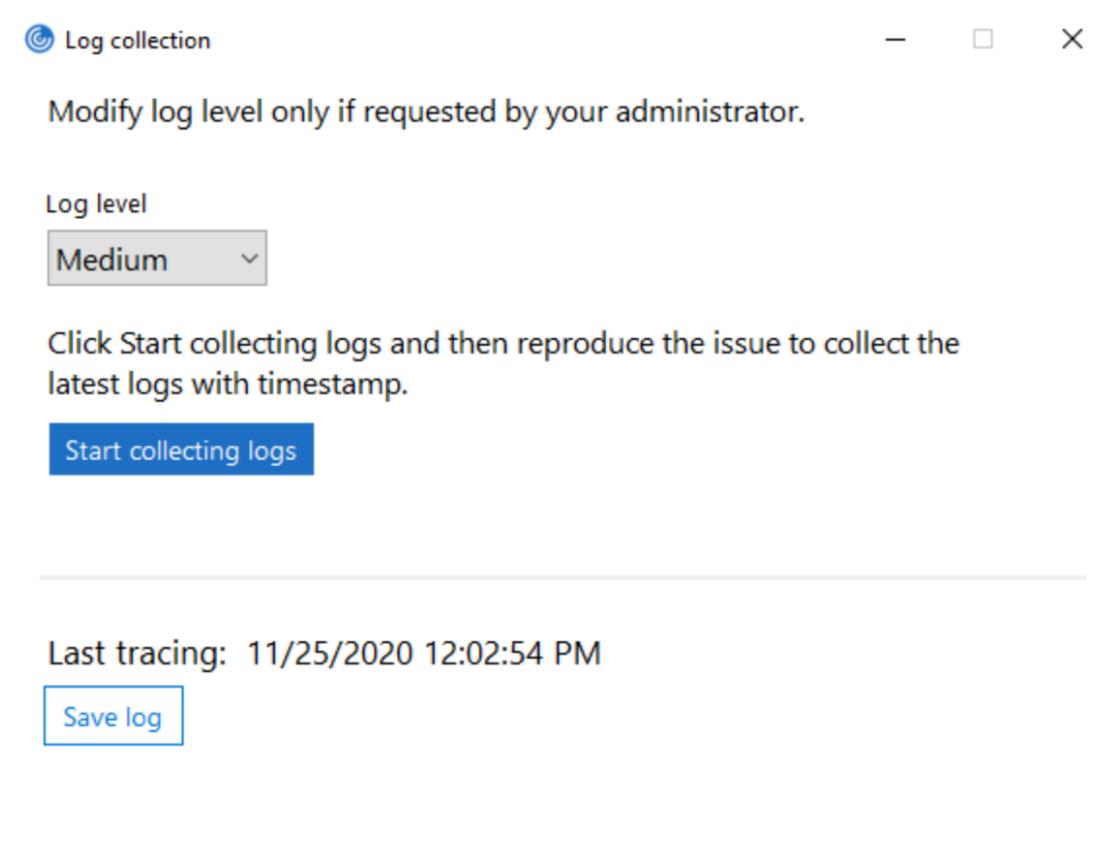
### ログ収集

ログ収集では、Citrix Workspace アプリのログを収集するプロセスが簡素化されました。ログは、Citrix でのトラブルシューティングに役立ち、問題が複雑な場合はサポートを容易にします。

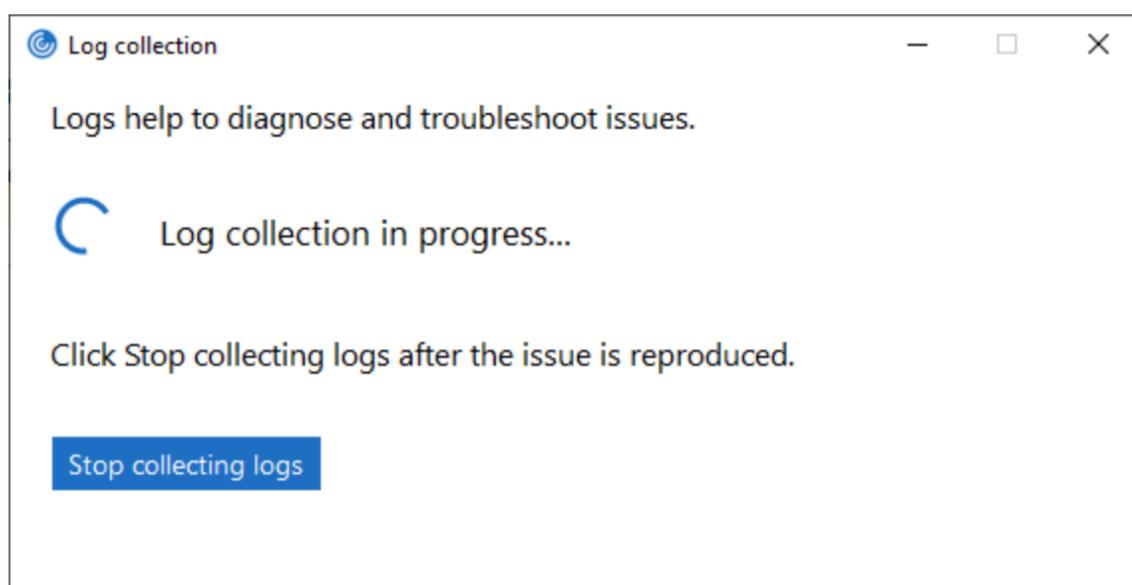
グラフィカルユーザーインターフェイスを使用してログを収集できます。

ログの収集：

1. システムトレイで Citrix Workspace アプリアイコンを右クリックし、[高度な設定] をクリックします。
2. [ログ収集] を選択します。  
[ログ収集] ダイアログが表示されます。



3. 次のログレベルのいずれかを選択します：
  - Low
  - Medium
  - Verbose
4. [ログ収集を開始する] をクリックし、問題を再現して、最新のログを収集します。  
ログ収集プロセスが開始されます。



5. 問題が再現されたら、[ログ収集を停止する] をクリックします。
6. [ログを保存] をクリックして、収集したログを保存します。

## HDX アダプティブスループット

HDX アダプティブスループットは、出力バッファを調整することで、ICA セッションのピークスループットをインテリジェントに微調整します。出力バッファの数は、最初は大きい値に設定されます。値を大きくすることで、特に高遅延のネットワークで、データをより迅速かつ効率的にクライアントに送信できます。

高い双方向性、高速なファイル転送、スムーズなビデオ再生、および高いフレームレートと解像度により、優れたユーザーエクスペリエンスを実現します。

セッションの双方向性を常に測定して、ICA セッション内のデータストリームが双方向性に悪影響を及ぼしているかどうかを判別します。悪影響を及ぼしている場合、スループットを低下させて、大規模データストリームがセッションに与える影響を減らし、双方向性を回復できるようにします。

この機能は、Windows 向け Citrix Workspace アプリ 1811 以降でのみサポートされています。

### 重要:

HDX アダプティブスループットでは、このメカニズムをクライアントから VDA に移行することにより、出力バッファの設定方法を変更しています。そのため、[CTX125027](#)に記載されているとおり、クライアント上の出力バッファ数を調整しても効果はありません。

## アダプティブトランスポート

アダプティブトランスポートはデータ転送メカニズムであり、高速で拡張性が高く、アプリケーションの対話機能を向上させ、要求の厳しい長距離の WAN とインターネット接続でのインタラクティブ性を高めます。アダプティ

ブトランスポートでは、サーバーの高スケーラビリティと帯域幅の使用効率が維持されます。アダプティブトランスポートを使用すると、ICA 仮想チャネルはネットワーク状況の変化に自動的に対応します。Enlightened Data Transport (EDT) と呼ばれる Citrix プロトコルと TCP との間で、基になるプロトコルをインテリジェントに切り替えて、最適なパフォーマンスを実現します。これにより、Thinwire ディスプレイリモート、ファイル転送 (クライアントドライブマッピング)、印刷、マルチメディアリダイレクトなど、すべての ICA 仮想チャネルのデータスループットが向上します。同じ設定を LAN と WAN の両方の条件に適用できます。

以前のリリースでは、**HDXoverUDP** を [優先する] に設定すると、可能な場合、EDT 上のデータ転送が使用され、TCP にフォールバックします。

セッション画面の保持を有効にすると、初期接続、セッション画面の保持による再接続、自動クライアント再接続中に EDT と TCP が同時に試行されます。この機能強化により、EDT が優先される状態で必要なベースの UDP トランスポートが利用できず、TCP を使用する必要がある場合、接続時間が短縮されます。

デフォルトでは、TCP にフォールバックした後、アダプティブトランスポートは 5 分ごとに EDT を検索し続けます。

要件:

- Citrix Virtual Apps and Desktops 7.12 以降。
- StoreFront 3.8。
- IPv4 VDA のみ。IPv6 および IPv6 と IPv4 の混在構成はサポートされません。
- VDA の UDP ポート 1494 および 2598 での受信トラフィックを許可するファイアウォール規則を追加します。

注:

TCP ポート 1494 および 2598 も必須で、VDA をインストールするときに自動的に開かれます。ただし、UDP ポート 1494 および 2598 は自動的に開かれません。これらを有効に設定します。

VDA と Citrix Workspace アプリ間の通信でポリシーを使用する前に、ポリシーを適用して、VDA でアダプティブトランスポートを構成する必要があります。

Citrix Workspace アプリでは、デフォルトでアダプティブトランスポートが許可されます。ただし、同じくデフォルトで、クライアントがアダプティブトランスポートの使用を試みるのは、Citrix Studio ポリシーで VDA が [優先する] に構成され、その VDA に設定が適用されている場合だけです。

**HDX** アダプティブトランスポートポリシー設定を使用してアダプティブトランスポートを有効化できます。可能な場合、アダプティブトランスポートを使用し、TCP にフォールバックするには、新しいポリシーを [優先する] に設定します。

特定のクライアントでアダプティブトランスポートを無効にするには、Windows 向け 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使用して、EDT オプションを適切に設定します。

**Citrix Workspace** アプリグループポリシーオブジェクト (**GPO**) 管理用テンプレートを使用してアダプティブトランスポートを構成するには

以下に、環境をカスタマイズするオプションの構成手順を示します。たとえば、セキュリティ上の理由で特定のクライアントに対して機能を無効にすることを選択する場合があります。

注:

デフォルトでは、アダプティブトランスポートは無効 ([オフ]) になっており、常に TCP が使用されます。

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 Workspace] > [ネットワークルーティング] の順に移動します。
3. [Citrix Workspace のトランスポートプロトコル] ポリシーを [有効] に設定します。
4. 必要な場合は、**Citrix Workspace** の通信プロトコルを選択します。
  - [オフ] - データ転送に TCP を使用することを示します。
  - [優先] - Citrix Workspace アプリが、UDP でサーバーに接続してから、TCP のフォールバックに切り替えることを示します。
  - [オン] - Windows 向け Citrix Workspace アプリが、UDP のみを使用してサーバーに接続することを示します。このオプションでは、TCP にフォールバックしません。
5. [適用]、[OK] の順にクリックします。
6. コマンドラインから `gpupdate /force` コマンドを実行します。

また、アダプティブトランスポート構成を有効にするには、Citrix Workspace アプリテンプレートファイルをポリシー定義フォルダーに追加します。テンプレートファイルをローカル GPO に追加する方法については、「[グループポリシーオブジェクトテンプレート](#)」を参照してください。

ポリシー設定の有効化を確認するには:

HKEY\\_\\_LOCAL\\_\\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDTに移動して **HDXOverUDP** キーがあるかを確認します。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[アダプティブトランスポート](#)」を参照してください。

## 高度な設定シート

バージョン 4.10 以降、システムトレイの Citrix Workspace アプリアイコンの右クリックメニューにある [高度な設定] シートの使用およびシートの内容をカスタマイズできます。これによって、ユーザーはシステムで管理者が指定した設定のみを適用できるようになります。具体的には、次の操作が可能になります。

- [高度な設定] シートをすべて非表示にする
- シートから以下の特定の設定を非表示にする
  - データ収集
  - コネクションセンター
  - 構成チェッカー
  - キーボードと言語バー
  - 高 DPI
  - サポート情報
  - ショートカットと再接続
  - Citrix Files
  - Citrix Casting

右クリックメニューの [高度な設定] オプションを非表示にする

Citrix Workspace アプリグループポリシーオブジェクト (GPO) 管理用テンプレートを使用して、[高度な設定] シートを非表示にすることができます:

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 Workspace] > [Self Service] > [高度な設定] オプションの順に移動します。
3. [高度な設定を無効にする] ポリシーを選択します。
4. システムトレイの Citrix Workspace アプリアイコンを右クリックし [有効] を選択して、[高度な設定] オプションを非表示にします。

注:

デフォルトでは、[未構成] オプションが選択されています。

[高度な設定] シートから特定の設定を非表示にする

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使用して、[高度な設定] シートからユーザーが構成可能な特定の設定を非表示にすることができます。これを行うには、次の操作を行います。

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 Workspace] > [Self Service] > [高度な設定] オプションの順に移動します。
3. 非表示にする設定のポリシーを選択します。

以下の表は、選択できるオプションとそれぞれの効果です。

| オプション    | 操作 (アクション) |
|----------|------------|
| 未構成      | 設定を表示します   |
| Enabled  | 設定を非表示にします |
| Disabled | 設定を表示します   |

[高度な設定] シートでは、以下の設定を非表示にできます。

- 構成チェッカー
- コネクションセンター
- 高 DPI
- データ収集
- 保存したパスワードの削除
- キーボードと言語バー
- ショートカットと再接続
- サポート情報
- Citrix Files
- Citrix Casting

レジストリエディターを使用して [高度な設定] シートから [**Workspace** をリセット] オプションを非表示にする

レジストリエディターを使用して [高度な設定] シートから [**Workspace** をリセット] オプションを非表示にすることができます。

1. レジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` にアクセスします。
3. 文字列値キー **EnableFactoryReset** を作成し、次のいずれかのオプションに設定します。
  - True - [高度な設定] シートで [Workspace をリセット] オプションが表示されます
  - False - [高度な設定] シートで [Workspace をリセット] オプションが非表示になります

[高度な設定] シートから [**Citrix Workspace** 更新プログラム] オプションを非表示にする

注:

[Citrix Workspace 更新プログラム] オプションのポリシーパスは、[高度な設定] シートにある他のオプションのポリシーパスとは異なります。

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**] > [**Citrix Workspace** の更新] の順に移動します。

3. [Citrix Workspace の更新] ポリシーを選択します。
4. [高度な設定] シートで [Workspace の更新] 設定を非表示にするには、[無効] を選択します。

## StoreFront から Workspace への URL の移行

この機能は、Technical Preview 段階です。StoreFront から Workspace への URL 移行により、最小限のユーザー操作でエンドユーザーを Storefront ストアから Workspace ストアにシームレスに移行できます。

すべてのエンドユーザーが Workspace アプリに StoreFront ストア `storefront.com` を追加することを前提とします。管理者は、Global App Configuration Service で StoreFront URL から Workspace URL へのマッピング `{'storefront.com': 'xyz.cloud.com'}` を構成できます。Global App Config Service は、StoreFront URL `storefront.com` が追加された、管理対象デバイスと非管理対象デバイスの両方で、すべての Citrix Workspace アプリインスタンスに設定をプッシュします。

設定が検出されると、Citrix Workspace アプリはマップされた Workspace URL `xyz.cloud.com` を別のストアとして追加します。エンドユーザーが Citrix Workspace アプリを起動すると、Citrix Workspace ストアが開きます。以前に追加された StoreFront ストア `storefront.com` は、Workspace アプリに追加されたままです。ユーザーは、Workspace アプリの [アカウントの切り替え] オプションを使用して、いつでも StoreFront ストア `storefront.com` に戻すことができます。管理者は、Global App Config Service で提供される別の設定を使用して、ユーザーのエンドポイントの Workspace アプリから StoreFront ストア `storefront.com` を削除するタイミングを制御できます。

この機能を有効にするには、次の手順を実行します。

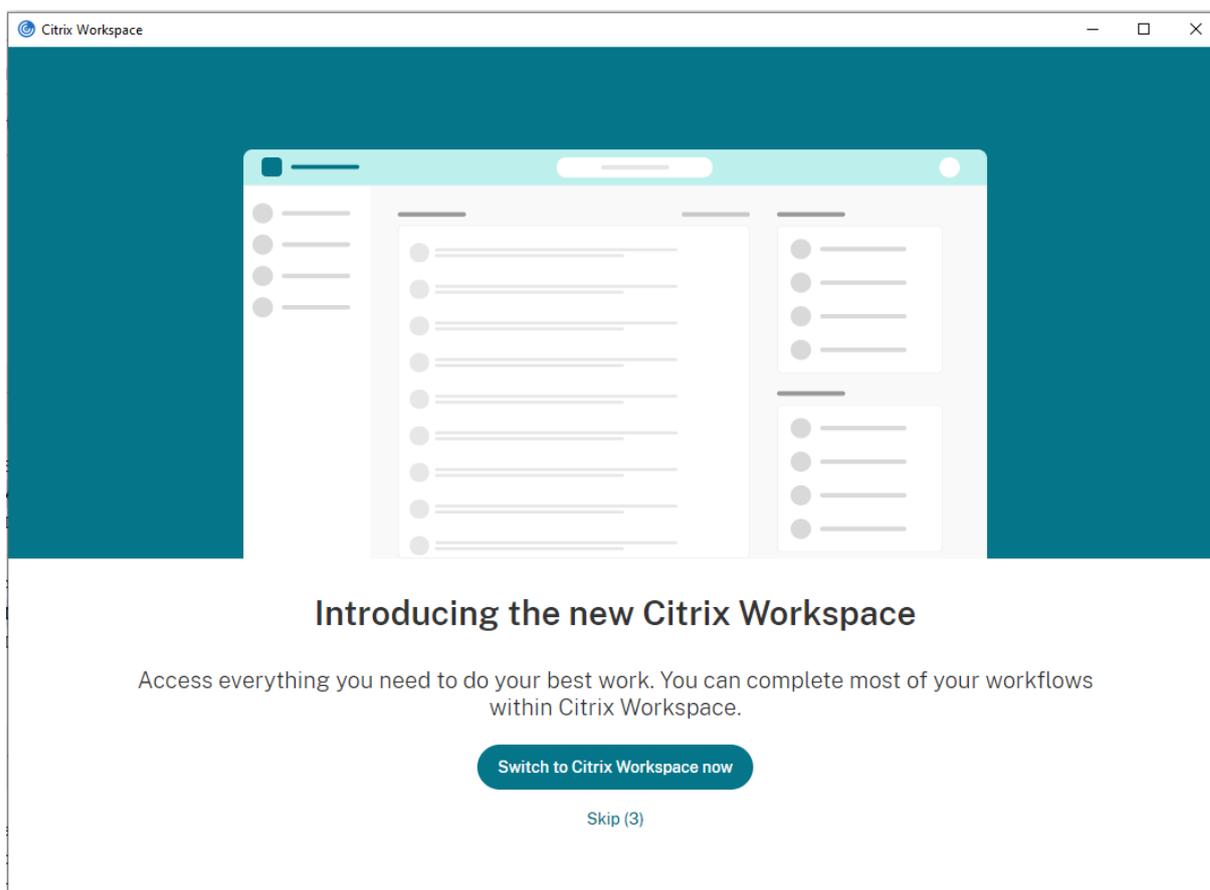
1. App Config Service でペイロードを編集します。

```
“serviceURL”:{
  “url”: “storefront.com”,
  “migrationUrl”: [
    {
      “url”: “xyz.cloud.com”,
      “storeFrontValidUntil”: “2023-05-01”
    }
  ]
}
```
2. Global App Config Service を使用して、StoreFront から Workspace へのマッピングを構成します。Global App Config Service について詳しくは、[Global App Config Service](#) を参照してください。
3. StoreFront URL `storefront.com` を **serviceURL** セクションの **URL** の値として指定します。
4. セクション **migrationUrl** 内で Workspace URL `xyz.cloud.com` を構成します。
5. **storeFrontValidUntil** を使用して、Workspace アプリから StoreFront ストアを削除するためのスケジュールを設定します。このフィールドはオプションです。要件に基づいて、次の値を設定できます。
  - YYYY-MM-DD 形式の有効な日付

注:

指定された日付が過去の場合、StoreFront ストアは URL の移行と同時に削除されます。日付が未来の場合、StoreFront ストアは設定された日付に削除されます。

App Config Service 設定がプッシュされると、次の画面が表示されます:



ユーザーが **[Switch to Citrix Workspace now]** をクリックすると、Workspace URL が Citrix Workspace アプリに追加され、認証プロンプトが表示されます。ユーザーのオプションは制限されており、移行を最大 3 回遅らせることができます。

### アプリケーションの配信

Citrix Virtual Apps and Desktops を使用してアプリケーションを配信する場合は、次のオプションを検討してユーザーエクスペリエンスを強化してください:

- **Web アクセスモード** - いずれの構成も行わない場合、Citrix Workspace アプリではアプリケーションおよびデスクトップへのブラウザーベースのアクセスが提供されます。Web 向け Workspace を Web ブラウザーで開き、使用するアプリケーションを選択して実行できます。このモードでは、ユーザーのデスクトップにショートカットは置かれません。

- セルフサービスモード - StoreFront アカウントを Citrix Workspace アプリに追加するか、StoreFront サイトをポイントするように Citrix Workspace アプリを構成して、セルフサービスモードを構成できます。このモードでは、Citrix Workspace アプリのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

注:

Citrix Workspace アプリのデフォルトでは、[スタート] メニューに表示するアプリケーションを選択できます。

- アプリケーションショートカットのみのモード - Windows 向け Citrix Workspace アプリ管理者として、Citrix Workspace アプリ Enterprise エディションの場合と同様に、Citrix Workspace アプリでアプリケーションやデスクトップのショートカットを [スタート] メニューまたはデスクトップに直接配置するよう構成できます。新しい「ショートカットのみ」のモードにより、アプリケーションの検索で使い慣れた Windows のナビゲーションスキーマ内で公開アプリケーションを見つけることができます。

詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[デリバリーグループの作成](#)」セクションを参照してください。

### セルフサービスモードの構成

StoreFront アカウントを Citrix Workspace アプリに追加するか、StoreFront サイトをポイントするように Citrix Workspace アプリを構成して、「セルフサービスモード」を構成できます。このモードでは、Citrix Workspace アプリのユーザーインターフェイスを介してアプリケーションをサブスクライブできます。この拡張ユーザーエクスペリエンスはモバイルアプリケーションストアのものと同様です。

注:

Citrix Workspace アプリのデフォルトでは、ユーザーは [スタート] メニューに表示するアプリケーションを選択できます。

セルフサービスモードでは、必要に応じて必須設定、自動プロビジョニング設定、お勧めのアプリケーションキーワード設定を構成できます。

デリバリーグループアプリケーションの説明に、適切なキーワードを追加します:

- 個々のアプリケーションを必須にして Citrix Workspace アプリから削除できないようにするには、アプリケーションの説明に「KEYWORDS: Mandatory」という文字列を追加します。ユーザーが必須アプリケーションをサブスクリプション解除するための削除オプションはありません。
- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、説明に「KEYWORDS: Auto」という文字列を追加します。ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- 説明に「KEYWORDS: Featured」という文字列を追加すると、そのアプリケーションが Citrix Workspace の [おすすりめ] 一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

グループポリシーオブジェクトテンプレートを使用したアプリケーションショートカットの場所のカスタマイズ

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] > [Self Service] の順に移動します。
3. [SelfServiceMode を管理します] ポリシーを選択します。
  - a) Self Service ユーザーインターフェイスを表示するには、[有効] を選択します。
  - b) アプリを手動でサブスクライブするには、[無効] を選択します。このオプションは、Self Service ユーザーインターフェイスを非表示にします。
4. [アプリのショートカットを管理します] ポリシーを選択します。
5. 必要に応じてオプションを選択します。
6. [適用]、[OK] の順にクリックします。
7. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

アプリケーションショートカットをカスタマイズするための **StoreFront** アカウント設定の使用

[スタート] メニュー内およびデスクトップ上のショートカットを StoreFront サイトからセットアップできます。C:\inetpub\wwwroot\Citrix\Roamingにある web.config ファイルの **<annotatedServices>** セクションに次の設定を追加できます：

- デスクトップ上にショートカットを置くには、PutShortcutsOnDesktop を使用します。設定："true" または "false" (デフォルトは false)。
- [スタート] メニュー内にショートカットを置くには、PutShortcutsInStartMenu を使用します。設定："true" または "false" (デフォルトは true)。
- [スタート] メニュー内のカテゴリパスを使用するには、UseCategoryAsStartMenuPath を使用します。設定："true" または "false" (デフォルトは true)。

注：

Windows 8、Windows 8.1、Windows 10 では、[スタート] メニュー内には階層分けされたフォルダーを作成できません。アプリケーションは個々に、または Citrix Virtual Apps and Desktops で定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。

- [スタート] メニュー内のすべてのショートカットを単一のフォルダー内に置くには、StartMenuDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- 管理者により変更されたアプリケーションが再インストールされるようにする (変更アプリケーションの自動再インストール機能) には、AutoReinstallModifiedApps を使用します。設定："true" または "false" (デフォルトは true)。
- デスクトップ上のすべてのショートカットを単一のフォルダー内に置くには、DesktopDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- クライアントの 'add/remove programs' でエントリを作成しないようにするには、DontCreateAddRemoveEntry を使用します。設定："true" または "false" (デフォルトは false)。

- 以前はストアから実行できたが今は実行できなくなったアプリケーションのショートカットや Citrix Workspace アイコンを削除するには、`SilentlyUninstallRemovedResources`を使用します。設定: "true" または "false" (デフォルトは false)。

web.config ファイルで、アカウントの **XML** セクションに変更を追加します。次の開始タグを検索し、このセクションに移動します。

```
<account id=... name="Store"
```

このセクションは、`</account>` タグで終わります。

このタグ内にある、次のような最初のプロパティセクションに移動します。

```
<properties> <clear> <properties>
```

このセクションの `<clear />` タグの後ろにプロパティを追加できます。1 行ごとに名前と値を記述します。例:

```
<property name="PutShortcutsOnDesktop" value="True" />
```

注:

`<clear />` タグの前に追加されたプロパティの要素により、それが無効になることがあります。プロパティ名と値の追加が任意の場合は、`<clear />` タグを削除します。

プロパティの追加例:

```
<properties <property name="PutShortcutsOnDesktop" value="True"><property name="DesktopDir" value="Citrix Applications">
```

重要

複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上で Citrix StoreFront 管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。詳しくは、[StoreFront](#)のドキュメントを参照してください。

### Citrix Virtual Apps and Desktops 7.x のアプリごとの設定を使ったショートカットの場所のカスタマイズ

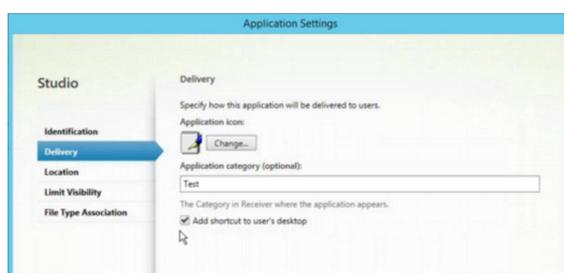
アプリケーションおよびデスクトップショートカットを [スタート] メニュー内に直接またはデスクトップ上に自動的に配置するよう、Citrix Workspace アプリを構成できます。この機能は、以前にリリースされたバージョンの Windows 向け Workspace の機能と似ていますが、バージョン 4.2.100 では Citrix Virtual Apps を使ってアプリケーション設定ごとにアプリケーションショートカットの配置を制御できる機能が導入されています。この機能は、終始一貫した場所に表示する必要がある一部のアプリケーションが存在する環境で有用です。

### XenApp 7.6 のアプリケーションごとの設定を使った、アプリケーションショートカットの場所のカスタマイズ

XenApp 7.6 でアプリケーションごとの公開ショートカットを構成するには

1. Citrix Studio で、[アプリケーション設定] 画面を開きます。

2. [アプリケーション設定] 画面で [配信] を選択します。この画面を使って、アプリケーションがユーザーにどのように配信されるかを指定できます。
3. アプリケーションの適切なアイコンを選択します。[変更] をクリックして、必要なアイコンの場所を参照します。
4. [アプリケーションカテゴリ] に、アプリケーションが表示される Citrix Workspace アプリのカテゴリを指定します。たとえば、ショートカットを Microsoft Office アプリケーションに追加している場合は、「Microsoft Office」と入力します。
5. [ユーザーのデスクトップにショートカットを追加する] チェックボックスをオンにします。
6. [OK] をクリックします。



#### 列挙遅延またはアプリケーションスタブデジタル署名の削減

ユーザーのログオン時にアプリケーションの列挙に遅延が生じる場合、またはアプリケーションスタブにデジタル署名が必要な場合、ネットワーク共有から.EXE スタブをコピーする機能が Citrix Workspace アプリにより提供されます。

この機能を実行するには、次の複数の手順を実行します：

1. クライアントマシンにアプリケーションスタブを作成します。
2. アプリケーションスタブをネットワーク共有からアクセスできる場所にコピーします。
3. 必要な場合は、許可リストを作成します（または、エンタープライズ証明書でスタブに署名します）。
4. レジストリキーを追加し、ネットワーク共有からスタブをコピーして Windows 向け Workspace がスタブを作成できるようにします。

**RemoveappsOnLogoff** および **RemoveAppsonExit** が有効で、ユーザーのログオン時にアプリケーション列挙に遅延が生じる場合、次の解決策により遅延を削減させます。

1. Regedit を使って、`HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"` を追加します。
2. Regedit を使って、`HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"` を追加します。HKEY\_CURRENT\_USER は、HKEY\_LOCAL\_MACHINE よりも優先されます。

### 注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

ネットワーク共有に格納されている事前作成のスタブ実行可能ファイルをマシンが使用できるようにします。

1. クライアントマシン上で、すべてのアプリケーションに対するスタブ実行可能ファイルを作成します。これを実行するには、Citrix Workspace アプリを使ってすべてのアプリケーションをマシンに追加します。Citrix Workspace アプリは実行可能ファイルを生成します。
2. %APPDATA%\Citrix\SelfServiceからスタブ実行可能ファイルを取得します。必要なのは.exe ファイルだけです。
3. 実行可能ファイルをネットワーク共有にコピーします。
4. ロックダウンされる各クライアントマシンに対して次のレジストリキーを設定します。
  - a) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"`
  - b) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v`
  - c) `CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"`。また、必要な場合は HKEY\_CURRENT\_USER でこれらの設定を構成することもできます。HKEY\_CURRENT\_USER は、HKEY\_LOCAL\_MACHINE よりも優先されます。
  - d) Citrix Workspace アプリのセッションを終了後再起動して、この変更を適用します。

ユースケースの例:

このトピックでは、アプリケーションショートカットのユースケースについて紹介します。

[スタート] メニューに何を置くか、ユーザーが選べるようにする (**Self-servic**)

数十（または数百の）アプリがある場合は、ユーザーがお気に入りのアプリケーションを選択して、[スタート] メニューに追加できるようにするのが最も便利です:

---

[スタート] メニューに置くアプリケーションをユーザーが選べるようにするには、

Citrix Workspace アプリをセルフサービスモードに構成します。このモードでは、「自動プロビジョニング」設定および「必須」アプリケーションキーワード設定も構成できます。

ユーザーが [スタート] メニューに置くアプリケーションを選べるようにして、また特定のアプリケーションショートカットをデスクトップに置くには、

Citrix Workspace アプリをオプション設定なしで構成して、デスクトップに置くアプリケーションについてアプリケーションごとの設定を使用します。必要に応じて、「自動プロビジョニング」および「必須」アプリケーションを使用します。

[スタート] メニュー内にアプリケーションショートカットなし

コンピューターを家族で共有して使用していて、アプリケーションショートカットを一切置きたくないとします。このような場合、最も簡単なのはブラウザーアクセスです。いずれの構成も行わずに Citrix Workspace アプリをインストールし、Web 向け Workspace にアクセスします。また、ショートカットをどこにも配置しないでセルフサービスアクセス用に Citrix Workspace アプリを構成することもできます。

Citrix Workspace アプリが [スタート] メニューに自動的にアプリケーションショートカットを配置しないようにするには

Citrix Workspace アプリで `PutShortcutsInStartMenu=False` と構成します。アプリケーションごとの設定を使ってショートカットを置かない限り、セルフサービスモードであっても Citrix Workspace アプリにより [スタート] メニュー内にアプリケーションは配置されません。

[スタート] メニュー内、またはデスクトップ上にすべてにアプリケーションショートカットを置く

ユーザーが所有するアプリケーションが少ない場合は、そのすべてを [スタート] メニュー内やデスクトップ上にあるいはデスクトップ上のフォルダー内に置くことができます。

Citrix Workspace アプリによって [スタート] メニューにすべてのアプリケーションショートカットを自動的に配置するには

Citrix Workspace アプリで `SelfServiceMode=False` と構成します。使用可能なすべてのアプリケーションが [スタート] メニュー内に表示されます。

すべてのアプリケーションショートカットをデスクトップ上に置く場合は、

Citrix Workspace アプリで `PutShortcutsOnDesktop=true` と構成します。使用可能なすべてのアプリケーションがデスクトップに表示されます。

すべてのショートカットをデスクトップ上のフォルダー内に置く場合は、

Citrix Workspace アプリで DesktopDir=Name アプリケーションショートカットを置くデスクトップフォルダーの名前と構成します。

### XenApp 6.5 または 7.x でのアプリケーションごとの設定

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenApp のアプリケーションごとの設定を使用します。

セルフサービスモードか、または [スタート] メニューモードかには関係なく、アプリケーションごとの設定によりアプリケーションを配置する場所を決定する場合は、

Citrix Workspace アプリで PutShortcutsInStartMenu=false と構成して、アプリケーションごとの設定を有効にします。

### カテゴリフォルダーまたは特定のフォルダーのアプリケーション

特定のフォルダー内にアプリケーションを表示する場合は、次のオプションを使用します。

Citrix Workspace アプリにより [スタート] メニューに置かれたアプリケーションショートカットを関連カテゴリ (フォルダー) 内に表示するには

Citrix Workspace アプリで UseCategoryAsStartMenuPath=True と構成します。

Citrix Workspace アプリにより [スタート] メニューに置かれたアプリケーションを特定のフォルダー内に配置するには

Citrix Workspace アプリで StartMenuDir= [スタート] メニューフォルダーの名前と構成します。

### ログオフまたは終了時にアプリケーションを削除

エンドポイントをほかのユーザーと共有していて、自分のアプリケーションがそのユーザーには表示されないようにしたい場合は、ログオフまたは終了時にアプリケーションが削除されるようにすることができます。

|                                                         |                                                                    |
|---------------------------------------------------------|--------------------------------------------------------------------|
| ログオフ時に Citrix Workspace アプリによりすべてのアプリケーションが削除されるようにするには | Citrix Workspace アプリで <code>RemoveAppsOnLogoff=True</code> と構成します。 |
| 終了時に Citrix Workspace アプリによりアプリが削除されるようにするには            | Citrix Workspace アプリで <code>RemoveAppsOnExit=True</code> と構成します。   |

### ローカルアプリアクセスのアプリケーションの構成

ローカルアプリアクセスのアプリケーションを構成する場合は次のようにします。

- 説明に「KEYWORDS:prefer="<pattern>」という文字列を追加すると、Citrix Workspace アプリでアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

Citrix Workspace アプリは、ユーザーのコンピューターにアプリケーションをインストールする前に `pattern` で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Workspace アプリはそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix Workspace アプリからそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

ユーザーが Citrix Workspace アプリを使用せずに優先アプリケーションをアンインストールすると、Citrix Workspace アプリの次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Workspace アプリを使用して優先アプリケーションをアンインストールすると、Citrix Workspace アプリはそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

#### 注:

Citrix Workspace アプリでアプリケーションをサブスクライブすると、キーワード `prefer` が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。

同じアプリケーションに対して複数回 `prefer` キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせで指定できます。

- 説明に「KEYWORDS:prefer="<pattern>」という文字列を追加すると、Citrix Workspace アプリでアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

Citrix Workspace アプリは、ユーザーのコンピューターにアプリケーションをインストールする前に `pattern` で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Workspace アプリはそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix

Workspace アプリからそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

ユーザーが Citrix Workspace アプリを使用せずに優先アプリケーションをアンインストールすると、Citrix Workspace アプリの次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Workspace アプリを使用して優先アプリケーションをアンインストールすると、Citrix Workspace アプリはそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

注:

Citrix Workspace アプリでアプリケーションをサブスクライブすると、キーワード prefer が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。

同じアプリケーションに対して複数回 prefer キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせて指定できます。

- prefer="<ApplicationName>"

ショートカットファイルに指定されているアプリケーション名にマッチします。単語または語句を指定できますが、語句の場合は引用句を使用する必要があります。単語やファイルパスの一部がマッチしても無視され、大文字/小文字も区別されません。アプリケーション名によるマッチは、管理者が手作業で設定する場合に便利です。

| KEYWORDS:prefer= | Programs 配下のショートカット                   | マッチする? |
|------------------|---------------------------------------|--------|
| Word             | \Microsoft Office\Microsoft Word 2010 | はい     |
| Microsoft Word   | \Microsoft Office\Microsoft Word 2010 | はい     |
| Console          | McAfee\VirusScan Console              | はい     |
| Virus            | McAfee\VirusScan Console              | いいえ    |
| Console          | McAfee\VirusScan Console              | はい     |

- prefer="\\Folder1\Folder2\...\ApplicationName"

[スタート] メニューのショートカットファイルの絶対パスおよびアプリケーション名にマッチします。Programs フォルダーは、[スタート] メニューディレクトリのサブフォルダーであるため、フォルダーのアプリケーションを対象にするには絶対パスに Programs フォルダーを含む必要があります。パスにスペースが含まれている場合は、引用句を使用する必要があります。また、大文字と小文字は区別されます。絶対パスによるマッチは、Citrix Virtual Apps and Desktops でプログラマ的に優先アプリケーションを設定する場合に便利です。

| KEYWORDS:prefer=                               | Programs 配下のショートカット                            | マッチする? |
|------------------------------------------------|------------------------------------------------|--------|
| \Programs\Microsoft Office\Microsoft Word 2010 | \Programs\Microsoft Office\Microsoft Word 2010 | はい     |
| \Microsoft Office                              | \Programs\Microsoft Office\Microsoft Word 2010 | いいえ    |
| \Microsoft Word 2010                           | \Programs\Microsoft Office\Microsoft Word 2010 | いいえ    |
| \Programs\Microsoft Word 2010                  | \Programs\Microsoft Word 2010                  | はい     |

- prefer="Folder1\Folder2\...\ApplicationName"

[スタート] メニューのショートカットファイルの相対パスにマッチします。相対パスにはアプリケーション名を含める必要があり、そのショートカットの親フォルダー名を含めることもできます。ショートカットのファイルパスの末尾が、指定したパターンに一致すると、そのアプリケーションに設定が適用されます。パスにスペースが含まれている場合は、引用符を使用する必要があります。また、大文字と小文字は区別されます。相対パスによるマッチは、プログラマ的に優先アプリケーションを設定する場合に便利です。

| KEYWORDS:prefer=                      | Programs 配下のショートカット                   | マッチする? |
|---------------------------------------|---------------------------------------|--------|
| \Microsoft Office\Microsoft Word 2010 | \Microsoft Office\Microsoft Word 2010 | はい     |
| \Microsoft Office                     | \Microsoft Office\Microsoft Word 2010 | いいえ    |
| \Microsoft Word 2010                  | \Microsoft Office\Microsoft Word 2010 | はい     |
| \Microsoft Word                       | \Microsoft Word 2010                  | いいえ    |

ほかのキーワードについては、StoreFront のドキュメントの「[ユーザーエクスペリエンスの最適化](#)」セクションを参照してください。

### 仮想ディスプレイレイアウト

この機能では、リモートデスクトップに適用する仮想モニターレイアウトを定義し、1つのクライアントモニターをリモートデスクトップ上の最大8つのモニターに仮想分割できます。仮想モニターは、Desktop Viewer の [モニターレイアウト] タブで設定できます。ここでは、垂直または水平の線で画面を仮想モニターに分けることができます。画面は、クライアントのモニター解像度で指定されたパーセンテージに従って分割されます。

DPI スケーリングまたは DPI マッチングに使用される仮想モニター用 DPI を設定できます。仮想モニターレイアウトを適用した後、セッションのサイズを変更するか、再接続します。

この構成は、全画面、単一モニターのデスクトップセッションにのみ適用され、公開アプリケーションには影響しません。この構成は、以降のこのクライアントからのすべての接続に適用されます。

Windows 向け Citrix Workspace アプリ 2106 以降、仮想ディスプレイレイアウトは、全画面のマルチモニターデスクトップセッションでもサポートされており、デフォルトで有効になっています。マルチモニターシナリオでは、仮想ディスプレイの総数がサポートされているディスプレイ数の最大 8 を超えない場合、同じ構成済みの仮想ディスプレイレイアウトがすべてのセッションモニターに適用されます。この制限を超えた場合、仮想ディスプレイレイアウトは無視され、どのセッションモニターにも適用されません。

次のレジストリキーを設定すると、マルチモニターの機能強化を無効にできます：

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

名前: **SplitAllMonitors**

種類: DWORD

値のデータ:

1 - 有効

0 - 無効

### アプリケーションの起動時間

セッションの事前起動機能を使用すると、通常時および高トラフィック負荷時のアプリケーションの起動時間が短縮され、ユーザーエクスペリエンスが向上します。事前起動機能により、ユーザーが Citrix Workspace アプリにログオンするとき、またはログオン済みの場合は予定された時間に事前起動セッションを作成できます。

この事前起動セッションにより、最初のアプリケーションの起動時間が短縮されます。ユーザーが Windows 向け Citrix Workspace アプリで新しいアカウント接続を追加した後、次のセッションまで事前起動セッションは適用されません。このセッションでは、デフォルトのアプリケーション `ctxprelaunch.exe` が実行されます。ただし、このアプリケーションはユーザーには表示されません。

詳しくは、Citrix Virtual Apps and Desktops の記事「[デリバリーグループの管理](#)」のセッションの事前起動とセッションの残留に関するガイダンスを参照してください。

セッションの事前起動機能はデフォルトでは無効になっています。この機能を有効にするには、Workspace のコマンドラインで `ENABLEPRELAUNCH=true` パラメーターを指定するか、レジストリキー `EnablePreLaunch` に `true` を設定します。デフォルト値 (null) は、事前起動が無効であることを示します。

注:

ドメインパススルー (SSON) 認証をサポートするようにクライアントマシンが構成されている場合、事前起動機能が自動的に有効になります。事前起動なしでドメインパススルー (SSON) を使用する場合は、**EnablePreLaunch** レジストリキーの値を

false に設定します。

レジストリの場所は以下のとおりです。

- `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle`
- `HKEY_CURRENT_USER\Software\Citrix\Dazzle`

事前起動には 2 つの種類があります：

- 即時事前起動 - トラフィック量にかかわらず、ユーザーの資格情報が認証されると直ちに事前起動が開始されます。この設定は、通常のトラフィック負荷時に使用します。ユーザーは、Citrix Workspace アプリを再起動することで事前起動セッションを起動できます。
- 予定事前起動 - 予定した時間に事前起動が開始されます。予定事前起動は、ユーザーデバイスが実行中で認証済みの場合のみ開始されます。これら 2 つの条件が満たされない場合は、予定された事前起動時間になってもセッションが起動しません。ネットワークとサーバーの負荷を分散するため、セッションは予定された時刻を含む一定期間内に起動します。たとえば、事前起動を午後 1 時 45 分に設定すると、午後 1 時 15 分から午後 1 時 45 分の間にセッションが起動されます。この設定は、高トラフィック負荷時に使用します。

Citrix Virtual Apps サーバーでの事前起動の構成には、事前起動アプリケーションの作成、変更、または削除と、事前起動アプリケーションを制御するユーザーポリシー設定の更新が含まれます。

`receiver.admx` ファイルで事前起動機能をカスタマイズすることはできません。ただし、Windows 向け Citrix Workspace アプリのインストール時またはインストール後にレジストリ値を変更することで、事前起動構成を変更することができます。

- `HKEY_LOCAL_MACHINE` 値は、Workspace のインストール時に追加されます。
- `HKEY_CURRENT_USER` 値では、同一マシン上の特定ユーザーに `HKEY_LOCAL_MACHINE` とは異なる値を設定できます。ユーザーは、管理者権限がなくても `HKEY_CURRENT_USER` 値を変更できます。管理者は、この機能を設定するためのスクリプトをユーザーに提供できます。

**HKEY\_LOCAL\_MACHINE** レジストリ値：

64 ビット Windows オペレーティングシステムの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch`

32 ビット Windows オペレーティングシステムの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch`

値の名前：**UserOverride**

種類：REG\_DWORD

値のデータ：

0 - `HKEY_CURRENT_USER` の値が存在しても、`HKEY_LOCAL_MACHINE` の値を使用します。

1 - 存在する場合は `HKEY_CURRENT_USER` の値を使用します。そうでない場合は、`HKEY_LOCAL_MACHINE` の値を使用します。

値の名前：**State**

種類：REG\_DWORD

値のデータ:

0 - 事前起動を無効にします。

1 - 即時事前起動を有効にします (ユーザーの資格情報が認証されたら事前起動が開始されます)。

2 - 予定事前起動を有効にします (Schedule 値に指定した時刻に事前起動が開始されます)。

値の名前: **Schedule**

種類: REG\_DWORD

値:

予定事前起動を開始する、24 時間形式の時刻と曜日です。入力形式は次のとおりです:

|       |                                                                                                                                        |                                                            |
|-------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| HH:MM | M:T:W:TH:F:S:SU - ここで、HH は時、MM は分です。<br>M:T:W:TH:F:S:SU は曜日です。<br>月曜日、水曜日、および金曜日の午後 1 時 45 分に予定事前起動を有効にするには、<br>Schedule=13:45 と設定します。 | 1:0:1:0:1:0:0。セッションが実際に起動するのは午後 1 時 15 分から午後 1 時 45 分の間です。 |
|-------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|

**HKEY\_CURRENT\_USER** レジストリ値:

`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\PreLaunch`

値については、HKEY\_LOCAL\_MACHINE と同じ State および Schedule 値を使用します。

コンテンツの双方向リダイレクト

双方向のコンテンツリダイレクトポリシーによって、クライアントからホスト (およびホストからクライアント) への URL リダイレクトを有効にするか無効にできます。サーバーポリシーは Citrix Studio で設定し、クライアントポリシーは、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で設定します。

URL リダイレクトに関しては、Citrix ではホストからクライアントへのリダイレクトおよびクライアント用のローカルアプリケーションアクセスが利用可能ですが、ドメインに参加している Windows クライアントに関しては、双方向のコンテンツリダイレクトを使用することをお勧めします。

次のいずれかの方法を使用して、コンテンツの双方向リダイレクトを有効にできます:

1. グループポリシーオブジェクト (GPO) 管理用テンプレート
2. レジストリエディター

注:

- ローカルアプリアクセスが有効であるセッション上では、コンテンツの双方向リダイレクトは機能しません

ん。

- コンテンツの双方向リダイレクトは、サーバーとクライアントの両方で有効である必要があります。サーバーとクライアントのいずれかで無効になると、機能が無効になります。
- URL が複数ある場合、URL を 1 つずつ指定することもできますが、セミコロンで区切った URL の一覧で指定しても構いません。ワイルドカード文字としてアスタリスク (\*) を使用できます。

**GPO** 管理用テンプレートを使用してコンテンツの双方向リダイレクトを有効化するには:

Windows 向け Citrix Workspace アプリを初めてインストールした場合のみ、グループポリシーオブジェクト管理用テンプレート構成を使用します。

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. [ユーザー構成] ノードで、[管理用テンプレート] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザーエクスペリエンス] の順に移動します。
3. [コンテンツの双方向リダイレクト] ポリシーを選択します。

Bidirectional Content Redirection

Previous Setting Next Setting

Not Configured  Enabled  Disabled

Comment:

Supported on: All Citrix Workspace supported platforms

Options:

Published Application/Desktop Name:

Above Name is for Published Type: Application

Allowed URLs to be redirected to VDA:

Enable URL-specific published application or desktop overrides?

URL-specific published application or desktop overrides:

Show...

Allowed URLs to be redirected to Client:

Help:

Bidirectional Content Redirection is the feature that allows URLs to be redirected from client to server and vice versa based on configuration.

- Published Application/Desktop Name : Indicates the name of the published application / desktop used to launch the redirected URL. This is not used when Bidirectional Content Redirection is enabled on any of the active ICA sessions. Whether its Desktop or Application is decided based on the Type specified below.
- Above Name is for Published Type : This indicates the above Name is whether Application or Desktop.
- Allowed URLs to be redirected to VDA : This indicates the list of URLs that will be opened on VDA. Semi Colon ";" acts as a delimiter. "\*" can be used as wild card. For example \*.xyz.com.
- Enable URL-specific published application or desktop overrides : This indicates whether the URL-specific overrides, specified below, are active.
- URL-specific published application or desktop overrides : This indicates the URL-specific overrides for Published Application/Desktop Name. The "Value name" should exactly match an entry in the "Allowed URLs to be redirected to VDA"

OK Cancel Apply

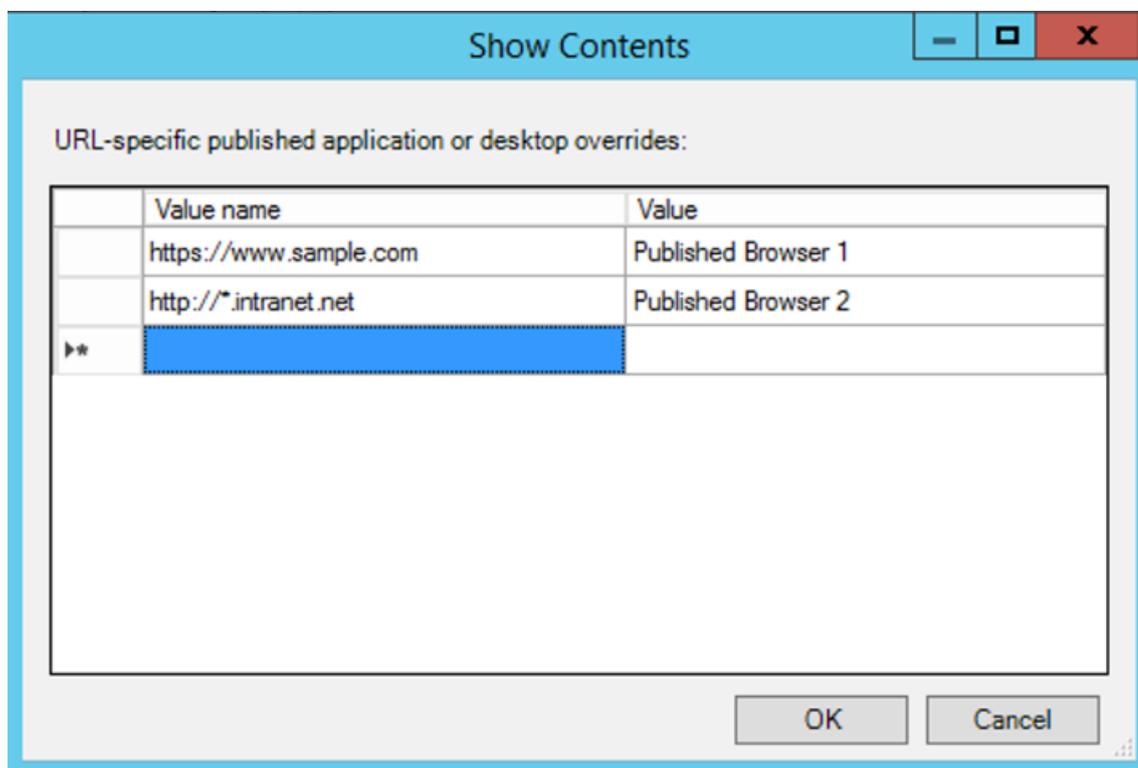
1. [公開アプリケーション名またはデスクトップ名] フィールドに、リダイレクトされた URL の起動に使用するリソースの名前を入力します。

注:

URL が複数ある場合、URL を 1 つずつ指定するか、セミコロンで区切った URL の一覧で指定します。ワイルドカード文字としてアスタリスク (\*) を使用できます。

2. [上記の名前の種類] で、必要に応じてリソースの [アプリケーション] または [デスクトップ] を選択します。
3. [VDA へのリダイレクトを許可する URL] フィールドに、リダイレクトする必要がある URL を入力します。一覧はセミコロンで区切ります。

4. **[URL 固有の公開アプリケーションまたはデスクトップの上書きを有効にしますか?]** オプションを選択して URL を上書きします。
5. **[表示]** をクリックして、**[VDA へのリダイレクトを許可する URL]** フィールドのいずれかと一致する必要がある値の名前の一覧を表示します。値は公開アプリケーション名と一致する必要があります。



6. **[クライアントへのリダイレクトを許可する URL:]** フィールドに、サーバーからクライアントにリダイレクトする必要がある URL を入力します。一覧はセミコロンで区切ります。

注:

URL が複数ある場合、URL を 1 つずつ指定するか、セミコロンで区切った URL の一覧で指定します。ワイルドカード文字としてアスタリスク (\*) を使用できます。

7. **[適用]**、**[OK]** の順にクリックします。
8. コマンドラインから `gpupdate /force` コマンドを実行します。

レジストリを使用してコンテンツの双方向リダイレクトを有効化するには:

コンテンツの双方向リダイレクトを有効化するには、Citrix Workspace アプリインストールフォルダー (C:\Program Files (x86)\Citrix\ICA Client) から、`redirector.exe /RegIE` コマンドを実行します。

重要:

- リダイレクト規則がループした構成になっていないことを確認してください。VDA 規則が、たとえば 1

- つの URL、[https://www.my\\\_\\\_company.com](https://www.my\_\_company.com)がクライアントにリダイレクトされるように構成され、同じ URL が VDA にリダイレクトされるように構成されている場合、ループ構成になります。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
  - 同じ表示名を持つ 2 つのアプリケーションが複数の StoreFront アカウントを使用するように構成されている場合、プライマリ StoreFront アカウントの表示名を使用して、アプリケーションまたはデスクトップのセッションが起動されます。
  - 新しいブラウザーウィンドウが開くのは、URL がクライアントにリダイレクトされた場合だけです。URL が VDA にリダイレクトされたときにブラウザーが既に開いていた場合、リダイレクトされた URL は新しいタブで開かれます。
  - ドキュメント、メール、PDF などの、ファイルに埋め込まれたリンクがサポートされます。
  - 同じマシンで、サーバーファイルタイプの関連付けとホストコンテンツのリダイレクトポリシーのいずれか 1 つだけが [有効] に設定されていることを確認します。URL リダイレクトが正しく機能するように、Citrix ではサーバーファイルタイプの関連付け機能またはホストコンテンツ (URL) リダイレクト機能を無効にすることをお勧めします。

### 制限事項:

セッションの起動に関する問題のため、リダイレクトが失敗してもフォールバックメカニズムは存在しません。

## Chromium ベースのブラウザーでの双方向 URL サポート

コンテンツの双方向リダイレクトを使用すると、サーバーとクライアントのポリシーを使用して、クライアントからサーバーへ、およびサーバーからクライアントへリダイレクトするように URL を構成できます。

サーバーポリシーは Delivery Controller で設定され、クライアントポリシーは、グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して Citrix Workspace アプリで設定されます。

バージョン 2106 以降、Google Chrome と Microsoft Edge に URL の双方向リダイレクトのサポートが追加されています。

### 前提条件:

- Citrix Virtual Apps and Desktops バージョン 2106 以降。
- ブラウザーリダイレクトの拡張バージョン 5.0。

Google Chrome ブラウザーで URL の双方向リダイレクトを登録するには、Citrix Workspace アプリインストーラフォルダーから、次のコマンドを実行します:

```
1 `"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
   verbose`
```

### 注:

Chrome ブラウザーでこれらのコマンドを使用すると、[コンテンツの双方向リダイレクト拡張機能](#)が Chrome

ウェブストアから自動的にインストールされます。

Google Chrome ブラウザーで URL の双方向リダイレクトの登録を解除するには、Citrix Workspace アプリインストールフォルダーから、次のコマンドを実行します：

```
1 `"%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /
   verbose`
```

注：

ブラウザー拡張機能ページにアクセスしたときに次のエラーが発生した場合は、エラーメッセージを無視してください：

```
WebSocket connection to wss://... failed.
```

Citrix Workspace アプリでの URL リダイレクトの構成については、「[コンテンツの双方向リダイレクト](#)」を参照してください。

Web ブラウザーコンテンツのリダイレクトについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Web ブラウザーコンテンツのリダイレクト](#)」を参照してください。

非アクティブな **Desktop Viewer** ウィンドウの減光を無効にするには：

Desktop Viewer の複数のウィンドウを使用する場合、デフォルトではアクティブでないウィンドウが減光されます。この機能により、複数のデスクトップを同時に表示する必要がある場合は、非アクティブなデスクトップ上の情報が読みづらくなる可能性があります。レジストリエディターを編集してデフォルトの設定を無効にし、**Desktop Viewer** ウィンドウの減光を防ぐことができます。

注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

- ユーザーデバイスで、デバイスの現在のユーザーまたはデバイス自体で減光を防止するかどうかによって、**DisableDimming** という REG\_DWORD エントリを次のいずれかのキーで作成します。デバイスで Desktop Viewer を使用したことがある場合は、エントリが既に存在します：
  - HKEY\_CURRENT\_USER\Software\Citrix\XenDesktop\DesktopViewer
  - HKEY\_LOCAL\_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

または、減光を制御する代わりに、同じ REG\_WORD エントリを次のキーのどちらかに作成することによって、ローカルポリシーを定義できます。

- HKEY\_CURRENT\_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

これらのキーを使用する前に、Citrix Virtual Apps and Desktops 管理者がこの機能のポリシーを設定しているかどうか確認してください。

エントリーを 1 または true のような 0 以外の値に設定します。

エントリーが未指定、または 0 に設定されている場合は、**Desktop Viewer** ウィンドウが減光します。複数のエントリーが指定されている場合、次の方法が使用されます。次の一覧の上位のエントリーの値によって、ウィンドウを減光するかどうかが決まります。

1. HKEY\_CURRENT\_USER\Software\Policies\Citrix\...
2. HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\...
3. HKEY\_CURRENT\_USER\Software\Citrix\...
4. HKEY\_LOCAL\_MACHINE\Software\Citrix\...

## Citrix Casting

Citrix Ready ワークスペースハブは、デジタル環境と物理環境を組み合わせ、セキュアなスマートスペース内にアプリやデータを配信します。このシステム全体が、モバイルアプリやセンサーなどのデバイス（「モノ」）を接続して、インテリジェントで応答性の高い環境を作ります。

Citrix Ready ワークスペースハブは Raspberry Pi 3 プラットフォーム上に構築されます。Citrix Workspace アプリを実行しているデバイスは Citrix Ready ワークスペースハブに接続し、デスクトップまたはアプリをより大きなディスプレイにキャストします。Citrix Casting は、Microsoft Windows 10 バージョン 1607 以降、または Windows Server 2016 でのみサポートされます。

Citrix Casting は、モバイルデバイスから簡単かつセキュアに任意のアプリにアクセスして、大きな画面に表示できるようにする機能です。

### 注:

- Citrix Casting for Windows は、Citrix Ready ワークスペースハブバージョン 2.40.3839 以降をサポートしています。以前のバージョンのワークスペースハブが検出されないか、キャストエラーが発生することがあります。
- Citrix Casting 機能は、Windows（ストア）向け Citrix Workspace アプリではサポートされていません。

### 前提条件:

- ハブ検出のためにデバイス上で Bluetooth が有効になっている。
- Citrix Ready ワークスペースハブと Citrix Workspace アプリが、同じネットワーク上に存在する。
- Citrix Workspace アプリが実行されているデバイスと Citrix Ready ワークスペースハブとの間でポート 55555 をブロックしないでください。
- Citrix Casting の場合、ポート 1494 をブロックしないでください。
- ポート 55556 は、モバイルデバイスと Citrix Ready ワークスペースハブの間の SSL 接続のデフォルトポートです。Raspberry Pi の設定ページで別の SSL ポートを構成できます。SSL ポートがブロックされている場合、ユーザーはワークスペースハブへの SSL 接続を確立できません。
- Citrix Casting は、Microsoft Windows 10 バージョン 1607 以降、または Windows Server 2016 でのみサポートされます。

### Citrix Casting の起動の構成

注:

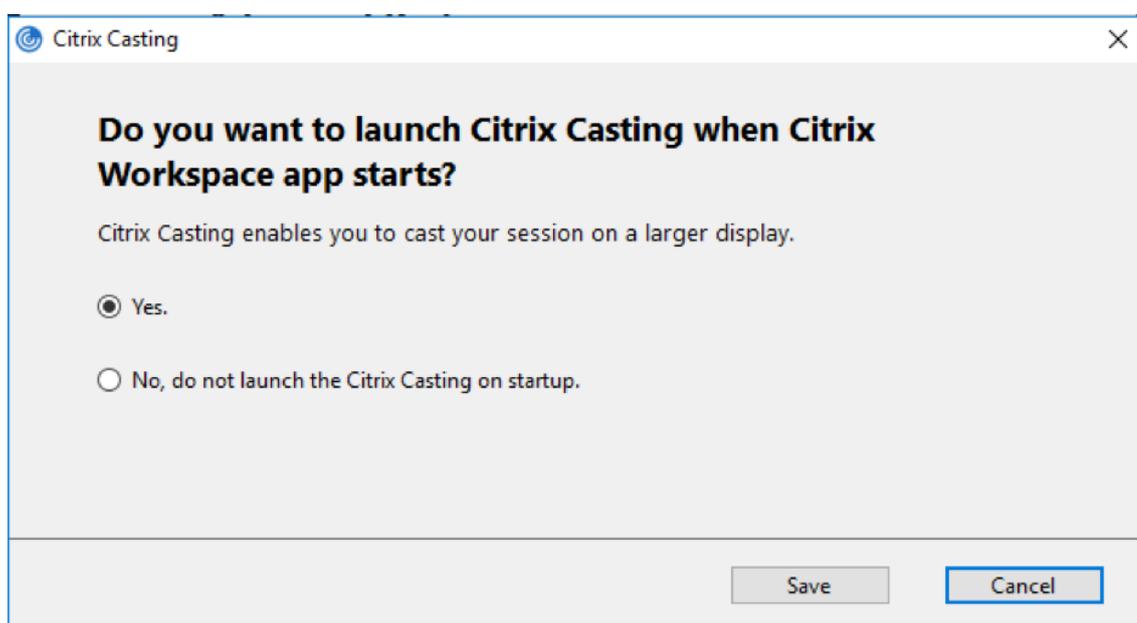
システムトレイの [Citrix Workspace アプリ] アイコンで [高度な設定] シートの一部または全部を非表示にすることができます。詳しくは、「[高度な設定シート](#)」を参照してください。

1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、[高度な設定] をクリックします。

[高度な設定] ダイアログボックスが表示されます。

2. [Citrix Casting] を選択します。

[Citrix Casting] ダイアログボックスが表示されます。



3. 次のいずれかのオプションを選択します:

- はい – Citrix Workspace アプリの起動時に Citrix Casting が起動されます。
- いいえ。スタートアップ時に Citrix Casting を起動しません – Citrix Workspace アプリの起動時に Citrix Casting は起動されません。

注:

いいえを選択しても、現在の画面キャストのセッションは終了しません。この設定は、次回の Citrix Workspace アプリの起動時にのみ適用されます。

4. [保存] をクリックして変更を適用します。

### Citrix Workspace アプリで Citrix Casting を使用方法

1. Citrix Workspace アプリにログオンし、デバイス上で Bluetooth を有効にします。

使用可能なハブの一覧が表示されます。一覧は、Citrix Ready ワークスペースハブビューコンパッケージの RSSI 値を基準として並べ替えられます。

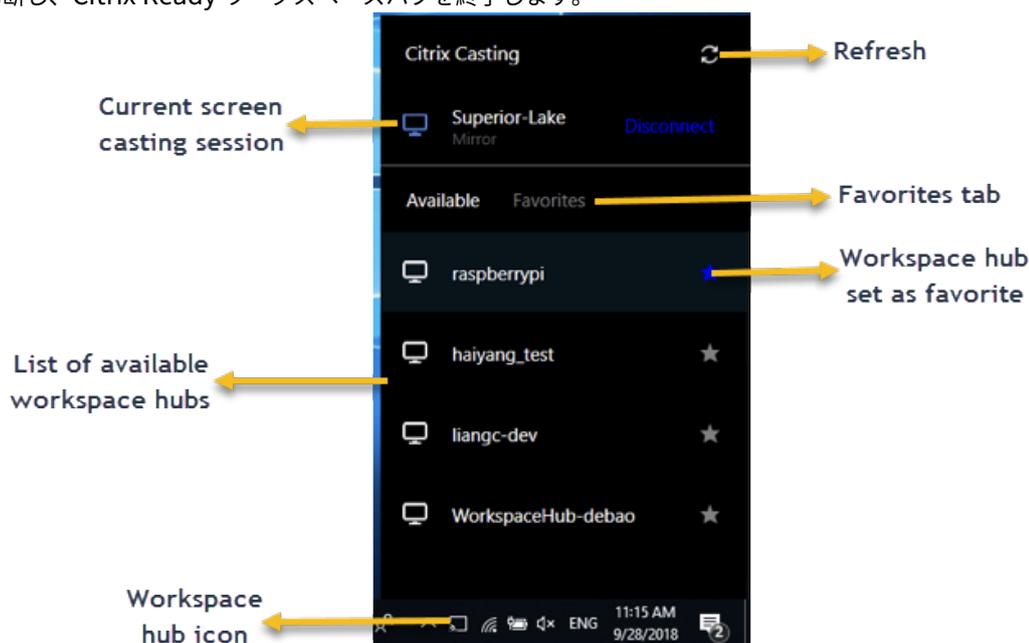
2. 画面をキャストするワークスペースハブを選択し、次のいずれかを選択します。
  - ミラーリング: プライマリ画面を複製し、接続されたワークスペースハブデバイスに表示をキャストします。
  - 拡張: ワークスペースハブデバイス画面をセカンダリ画面として使用します。

注:

Citrix Workspace アプリを終了しても、Citrix Casting は終了しません。

[Citrix Casting の通知] ダイアログボックスには、次のオプションがあります:

1. 現在の画面キャストのセッションが上部に表示されます。
2. アイコンを [更新] します。
3. [切断] を選択して、現在の画面キャストのセッションを停止します。
4. 星アイコンをクリックして、ワークスペースハブを [お気に入り] に追加します。
5. システムトレイのワークスペースハブアイコンを右クリックし、終了を選択して画面キャストのセッションを切断し、Citrix Ready ワークスペースハブを終了します。



#### セルフチェッカー一覧

Citrix Workspace アプリが範囲内の使用可能なワークスペースハブを検出して通信することができない場合は、セルフチェッカーの一環として以下を確認してください:

1. Citrix Workspace アプリと Citrix Ready ワークスペースハブが同じネットワークに接続している。

2. Citrix Workspace アプリが起動されたデバイスで Bluetooth が有効になり、正常に動作している。
3. Citrix Workspace アプリが起動されたデバイスが、Citrix Ready ワークスペースハブの範囲内（10 メートル未満。壁などの障害物がない）にある。
4. Citrix Workspace アプリでブラウザを起動して、[http://<hub\\_ip>:55555/device-details.xml](http://<hub_ip>:55555/device-details.xml) を入力し、ワークスペースハブデバイスの詳細が表示されるかを確認します。
5. Citrix Ready ワークスペースハブで 更新 をクリックして、ワークスペースハブへの再接続を試みる。

### 既知の問題と制限事項

1. デバイスが Citrix Ready ワークスペースハブと同じネットワークに接続されていないと、Citrix Casting は機能しません。
2. ネットワークに問題がある場合、ワークスペースハブデバイスに表示に時間差が発生する可能性があります。
3. [拡張] を選択すると、Citrix Ready Workspace アプリが起動されるプライマリ画面が数回点滅します。
4. [拡張] モードでは、セカンダリディスプレイをプライマリディスプレイとして設定することはできません。
5. デバイスのディスプレイ設定が変更された場合、画面キャストのセッションは自動的に切断されます。たとえば、画面の解像度を変更されたり、画面の方向が変更されたりした場合などです。
6. 画面キャストのセッション中に、Citrix Workspace アプリを実行しているデバイスがロック、スリープまたは休止状態になると、ログイン時にエラーが表示されます。
7. 複数の画面キャストのセッションはサポートされていません。
8. Citrix Casting でサポートされている画面の最大解像度は 1920 x 1440 です。
9. Citrix Casting は、Citrix Ready ワークスペースハブバージョン 2.40.3839 以降をサポートしています。以前のバージョンのワークスペースハブが検出されないか、キャストエラーが発生することがあります。
10. この機能は、Windows (ストア) 向け Citrix Workspace アプリではサポートされていません。
11. Windows 10 ビルド 1607 では、[拡張] モードの Citrix Casting が正しく配置されないことがあります。

Citrix Ready ワークスペースハブについて詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[Citrix Ready ワークスペースハブ](#)」のセクションを参照してください。

### 複合 **USB** デバイスリダイレクト

USB 2.1 以降は、複数の子デバイスが同じ USB バスで単一の接続を共有する USB 複合デバイスの概念をサポートしています。このようなデバイスは、単一の構成スペースと共有バス接続を採用しており、一意のインターフェイス番号 00-ff を使用して各子デバイスを識別します。これは、USB ハブとは異なります。USB ハブは、他の個別にアドレス指定された USB デバイスが接続する USB バスの新しい起点を提供します。

クライアントエンドポイントで検出された複合デバイスは、次のいずれかとして仮想ホストに転送できます：

- 単一の複合 USB デバイス、または
- 独立した子デバイスのセット（分割デバイス）

複合 USB デバイスが転送されると、デバイス全体がエンドポイントで使用できなくなります。これにより、最適化された HDX リモートエクスペリエンスに必要な Citrix Workspace クライアントを含む、エンドポイント上のすべて

のアプリケーションでのデバイスのローカル使用がブロックされます。

オーディオデバイスとミュートとボリュームコントロール用の HID ボタンの両方を備えた USB ヘッドセットデバイスを検討してください。デバイス全体が汎用 USB チャンネルを使用して転送される場合、デバイスは最適化された HDX オーディオチャンネルを介したりダイレクトで使用できなくなります。ただし、汎用 USB リモート処理経由でホスト側のオーディオドライバーを使用して送信されるオーディオとは異なり、最適化された HDX オーディオチャンネル経由で送信されるオーディオでは、最高のエクスペリエンスを実現できます。これは、USB オーディオプロトコルの性質がノイズが多いためです。

また、システムキーボードまたはポインティングデバイスが、リモートセッションのサポートに必要な他の統合機能を備えた複合デバイスの一部である場合にも問題が発生します。完全な複合デバイスが転送されると、システムのキーボードまたはマウスは、リモートデスクトップセッションまたはアプリケーション内を除いて、エンドポイントで操作できなくなります。

これらの問題を解決するために、複合デバイスを分割し、汎用 USB チャンネルを使用する子インターフェイスのみを転送することを Citrix ではお勧めします。これにより、最適化された HDX エクスペリエンスを提供する Citrix Workspace アプリなど、クライアントエンドポイント上のアプリケーションで他の子デバイスを使用できるようになり、必要なデバイスのみを転送してリモートセッションで使用できるようになります。

デバイス規則:

通常の USB デバイスと同様に、エンドポイントのポリシーまたはクライアント Citrix Workspace アプリ構成で設定されたデバイス規則は、転送する複合デバイスを選択します。Citrix Workspace アプリは、これらの規則を使用して、リモートセッションへの転送を許可または禁止する USB デバイスを決定します。

各規則は、アクションキーワード (Allow、Connect、または Deny)、コロン (:)、エンドポイント USB サブシステムの実際のデバイスに一致する 0 個以上のフィルターパラメーターから構成されています。これらのフィルターパラメーターは、すべての USB デバイスが自身を識別するために使用する USB デバイスの記述子メタデータに対応します。

デバイス規則はクリアテキストであり、各規則は 1 行に表示され、オプションのコメントは # 文字の後に記載されています。規則はトップダウンで照合されます (優先度の降順)。デバイスまたは子インターフェイスに一致する最初の規則が適用されます。同じデバイスまたはインターフェイスを選択する後続の規則は無視されます。

サンプルデバイス規則:

```
1 `ALLOW: vid=046D pid=0102 # Allow a specific device by vid/pid`
2 `ALLOW: vid=0505 class=03 subclass=01 # Allow any pid for vendor 0505 w
  /subclass=01`
3 `DENY: vid=0850 pid=040C # deny a specific device (incl all child
  devices)`
4 `DENY: class=03 subclass=01 prot=01 # deny any device that matches all
  filters`
5 `CONNECT: vid=0911 pid=0C1C # Allow and auto-connect a specific device`
6 `ALLOW: vid=0286 pid=0101 split=01 # Split this device and allow all
  interfaces`
```

```

7 `ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Split and allow only 2
  interfaces`
8 `CONNECT: vid=1050 pid=0407 split=01 intf=02 # Split and auto-connect
  interface 2`
9 `DENY: vid=1050 pid=0407 split=1 intf=03 # Prevent interface 03 from
  being remotd`

```

次のフィルターパラメーターのいずれかを使用して、検出されたデバイスに規則を適用できます：

| フィルターパラメーター           | 説明                                                       |
|-----------------------|----------------------------------------------------------|
| vid=xxxx              | USB デバイスのベンダー ID (4 桁の 16 進コード)                          |
| pid=xxxx              | USB デバイスの製品 ID (4 桁の 16 進コード)                            |
| rel=xxxx              | USB デバイスのリリース ID (4 桁の 16 進コード)                          |
| class=xx              | USB デバイスのクラスコード (2 桁の 16 進コード)                           |
| subclass=xx           | USB デバイスのサブクラスコード (2 桁の 16 進コード)                         |
| prot=xx               | USB デバイスのプロトコルコード (2 桁の 16 進コード)                         |
| split=1 (または split=0) | 分割する (または分割しない) 複合デバイスを選択します                             |
| intf=xx[,xx,xx,...]   | 複合デバイスの子インターフェイスの特定のセットを選択します (2 桁の 16 進コードのコンマで区切られた一覧) |

最初の 6 つのパラメーターは、規則を適用する必要がある USB デバイスを選択します。パラメーターが指定されていない場合、規則はそのパラメーターが ANY の値を持つデバイスと一致します。

USB インプリメンターズフォーラム (USB-IF) は、[Defined Class Code](#) のクラス、サブクラス、およびプロトコル値の定義済み一覧を維持しています。USB-IF は、登録されたベンダー ID の一覧も所有しています。特定のデバイスのベンダー、製品、リリース、およびインターフェイス ID は、Windows デバイスマネージャーで直接確認するか、UsbTreeView などの無料ツールを使用して確認できます。

最後の 2 つのパラメーター (存在する場合) は USB 複合デバイスにのみ適用されます。split パラメーターは、複合デバイスを分割デバイスとして転送するか、単一の複合デバイスとして転送する必要があるかを決定します。

- `_Split=1_` は、複合デバイスの選択された子インターフェイスを分割デバイスとして転送する必要があることを示します。
- `_Split=0_` は、複合デバイスを分割するべきではないことを示します。

注:

split パラメーターを省略した場合、\_Split=0\_ と見なされます。

\_intf\_ パラメーターは、アクションを適用する必要がある複合デバイスの特定の子インターフェイスを選択します。省略した場合、アクションは複合デバイスのすべてのインターフェイスに適用されます。

3 つのインターフェイスを備えた複合 USB ヘッドセットデバイスについて考えてみましょう

- インターフェイス 0 - オーディオクラスのデバイスエンドポイント
- インターフェイス 3 - HID クラスのデバイスエンドポイント (音量ボタンとミュートボタン)
- インターフェイス 5 - 管理/更新インターフェイス

この種類のデバイスに推奨される規則は次のとおりです:

```
1 `CONNECT: vid=047F pid=C039 split=1 intf=03 # Allow and auto-connect
   HID device`
2 `DENY:    vid=047F pid=C039 split=1 intf=00 # Deny audio end points`
3 `ALLOW:  vid=047F pid=C039 split=1 intf=05 # Allow mgmt intf but don't
   auto-connect`
```

デバイス規則ポリシーを有効にする:

Windows 向け Citrix Workspace アプリには、特定の望ましくないクラスのデバイスをフィルタリングし、顧客が頻繁に遭遇するデバイスのクラスを許可するデフォルトのデバイス規則セットが含まれています。

これらのデフォルトのデバイス規則は、次のいずれかのシステムレジストリで確認できます:

- HKEY\_LOCAL\_MACHINE\Software\Citrix\ICA Client\GenericUSB (32 ビット Windows) または
- HKEY\_LOCAL\_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB (64 ビット Windows)、**DeviceRules** という名前のマルチストリング値。

ただし、Windows 向け Citrix Workspace アプリでは、**USB** デバイス規則ポリシーを適用して、これらのデフォルトの規則を上書きできます。

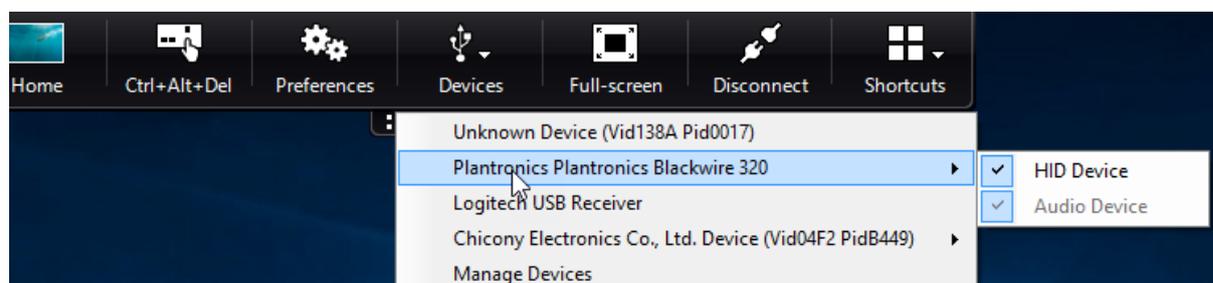
Windows 向け Citrix Workspace アプリのデバイス規則ポリシーを有効にするには:

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. [ユーザー構成] ノード配下で、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に移動します。
3. **USB** デバイス規則ポリシーを選択します。
4. [有効] をクリックします。
5. [**USB** デバイス規則] テキストボックスに、展開する USB デバイス規則を貼り付けます (または直接編集します)。
6. [適用]、[OK] の順にクリックします。

このポリシーを作成するときは、クライアントに付属しているデフォルトの規則を保存してから元の規則をコピーし、新しい規則を挿入して必要に応じて動作を変更することを Citrix ではお勧めします。

### USB デバイスの接続:

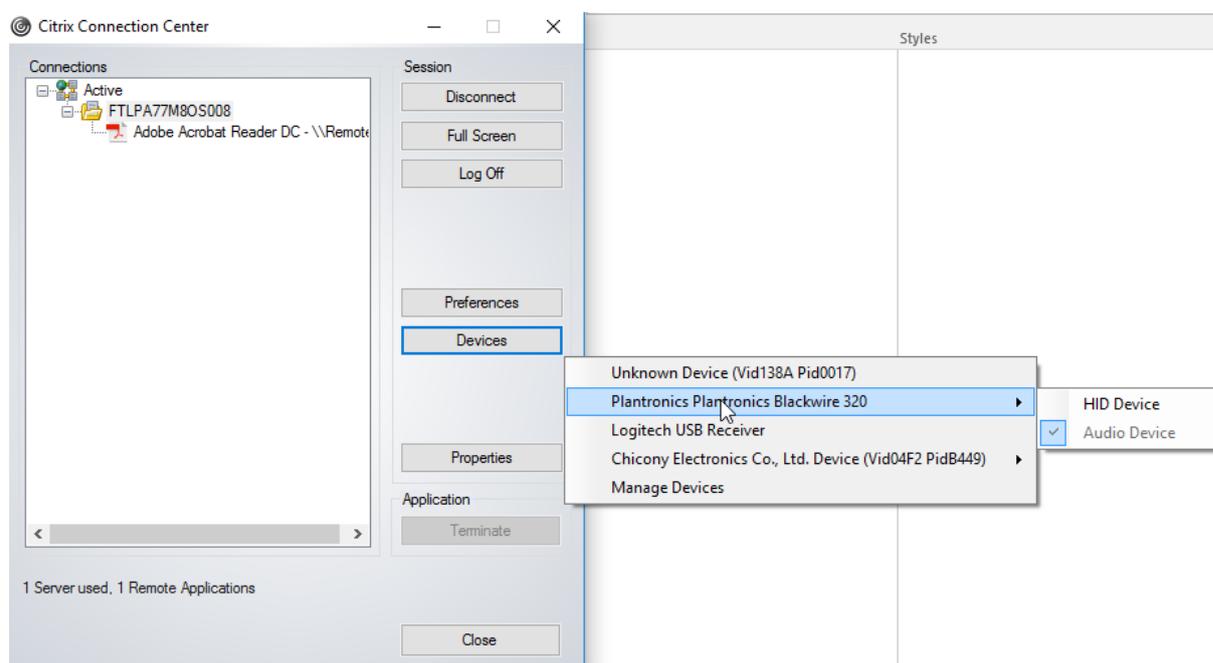
デスクトップセッションでは、分割された USB デバイスは [デバイス] の Desktop Viewer で表示されます。また、[基本設定] > [デバイス] から分割された USB デバイスを表示できます。



注:

CONNECT キーワードは、USB デバイスの自動接続を有効にします。ただし、汎用 USB リダイレクト用に複数 USB デバイスを分割するときに CONNECT キーワードが使用されない場合、Desktop Viewer またはコネクションセンターからデバイスを手動で選択する必要があります。

アプリケーションセッションでは、分割デバイスはコネクションセンターで表示されます。



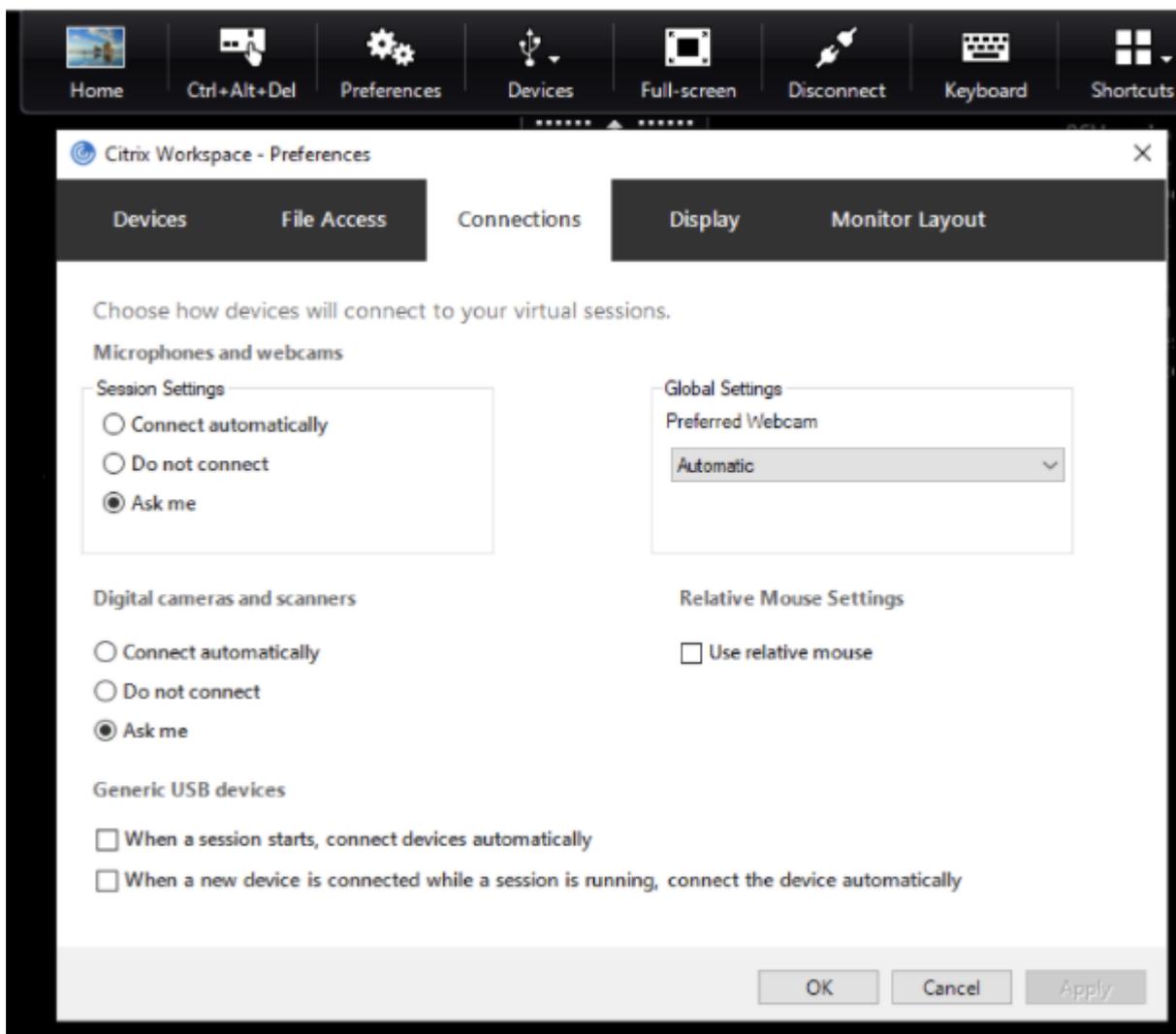
インターフェイスを自動的に接続するには:

Windows 向け Citrix Workspace アプリ 2109 で導入された CONNECT キーワードにより、USB デバイスの自動リダイレクトが可能になります。セッションで自動的に接続することを管理者がデバイスまたは選択したインターフェイスに許可している場合、CONNECT 規則は ALLOW 規則に置き換えることができます。

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. [ユーザー構成] ノード配下で、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に移動します。
3. **USB** デバイス規則ポリシーを選択します。
4. [有効] をクリックします。
5. [**USB** デバイス規則] テキストボックスで、自動接続する USB デバイスを追加します。  
たとえば、CONNECT: vid=047F pid=C039 split=01 intf=00,03 は複合デバイスの分割と、インターフェイス 00 および 03 インターフェイスの自動接続を可能にし、そのデバイスの他のインターフェイスを制限します。
6. [適用] および [**OK**] をクリックしてポリシーを保存します。

### **USB** デバイスの自動接続設定の変更:

Citrix Workspace アプリは、現在のデスクトップリソースの設定に基づいて、CONNECT アクションでタグ付けされた USB デバイスを自動的に接続します。次の図に示すように、**Desktop Viewer** のツールバーで設定を変更できます。



ペインの下部にある2つのチェックボックスは、デバイスが自動的に接続する必要があるか、セッションで手動接続を待つ必要があるかを制御します。これらの設定はデフォルトでは有効になっていません。汎用 USB デバイスを自動的に接続する必要がある場合は、設定を変更できます。

または、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、ユーザー設定を上書きできます。マシンポリシーとユーザーポリシーは両方とも、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順でアクセスできます。対応するポリシーには、それぞれ [既存の USB デバイス] と [新しい USB デバイス] のラベルが付いています。

分割デバイスのデフォルト設定の変更:

デフォルトでは、Windows 向け Citrix Workspace アプリは、デバイス規則で `_Split=1_` として明示的にタグ付けされた複合デバイスのみを分割します。ただし、デフォルトの配置を変更して、一致するデバイス規則で `_Split=0_` としてタグ付けされていないすべての複合デバイスを分割することは可能です。

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. [ユーザー構成] ノード配下で、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [クライアントデバイスをリモート処理します] > [一般的な **USB** のリモート処理] の順に移動します。
3. **SplitDevices** ポリシーを選択します。
4. [有効] をクリックします。
5. [適用] および [OK] をクリックしてポリシーを保存します。

注:

Citrix ではデフォルトを変更するのではなく、明示的なデバイス規則を使用して、分割する必要がある特定のデバイスまたはインターフェイスを識別することをお勧めします。この設定は、将来のリリースで廃止されます。

制限事項:

Citrix では Web カメラのインターフェイスは分割しないことをお勧めします。代わりに、汎用 USB リダイレクトを使用してデバイスを単一のデバイスにリダイレクトします。パフォーマンスを向上させるには、最適化された仮想チャネルを使用してください。

## Bloomberg キーボード

Citrix Workspace アプリは、Citrix Virtual Apps and Desktops セッションで Bloomberg キーボードの使用をサポートします。必要なコンポーネントはプラグインとともにインストールされます。Bloomberg キーボード機能は、Windows 向け Citrix Workspace アプリのインストール時またはレジストリエディターで有効にできます。

Bloomberg キーボードは、標準のキーボードと比較すると、ユーザーが金融市場データにアクセスして取引を実行できるという別の機能を提供します。

Bloomberg キーボードは、1 つの物理シェルに組み込まれた複数の USB デバイスで構成されています:

- キーボード
- 指紋リーダー
- オーディオデバイス
- これらのすべてのデバイスをシステムに接続するための USB ハブ
- オーディオデバイスの HID ボタン (ミュート、音量大、音量小など)

これらのデバイスの通常の機能に加えて、オーディオデバイスには、一部のキー、キーボードの制御、およびキーボード LED のサポートが含まれています。

セッション内で特殊な機能を使用するには、オーディオデバイスを USB デバイスとしてリダイレクトする必要があります。このリダイレクトは、オーディオデバイスをセッションで使用できるようにして、ローカルでは使用されないようにします。さらに、特殊な機能は 1 つのセッションでのみ使用でき、複数のセッション間で共有することはできません。

複数のセッションで Bloomberg キーボードを使用しないでください。このキーボードはシングルセッション環境でのみ動作します。

**Bloomberg** キーボード 5 の構成:

Bloomberg キーボードのさまざまなインターフェイスを構成する必要があります。Windows 向け Citrix Workspace アプリ 2109 から、新しい CONNECT キーワードが導入され、セッションの起動時とデバイスの挿入時に USB デバイスを自動的に接続できるようになりました。ユーザーが USB デバイスまたはインターフェイスを自動的に接続する場合は、CONNECT キーワードを使用して ALLOW キーワードを置き換えることができます。次の例では、CONNECT キーワードを使用しています。

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. [ユーザー構成] ノード配下で、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [クライアントデバイスをリモート処理します] > [一般的な USB のリモート処理] の順に移動します。
3. **SplitDevices** ポリシーを選択します。
4. [有効] をクリックします。
5. [USB デバイス規則] テキストボックスに、次の規則を追加します（存在しない場合）。

```
CONNECT: vid=1188 pid=A101 ## Bloomberg 5 Biometric module
```

```
DENY: vid=1188 pid=A001 split=01 intf=00 ## Bloomberg 5 Primary keyboard
```

```
CONNECT: vid=1188 pid=A001 split=01 intf=01 ## Bloomberg 5 Keyboard HID
```

```
DENY: vid=1188 pid=A301 split=01 intf=02 ## Bloomberg 5 Keyboard Audio Channel
```

```
CONNECT: vid=1188 pid=A301 split=01 intf=00,01 ## Bloomberg 5 Keyboard Audio HID
```

6. [適用] および [OK] をクリックしてポリシーを保存します。
7. [設定] ウィンドウで、[接続] タブを選択し、1 つまたは両方のチェックボックスを選択してデバイスを自動的に接続します。[設定] ウィンドウには、デスクトップツールバーまたは接続マネージャーからアクセスできます。

この手順により、Bloomberg キーボード 5 を使用できるようになります。手順で説明されている DENY 規則は、プライマリキーボードとオーディオチャンネルが汎用 USB 経路でリダイレクトされるのではなく、最適化されたチャンネル経路でリダイレクトされることを強制します。CONNECT 規則は、指紋モジュール、キーボードの特殊キー、およびオーディオ制御に関連するキーの自動リダイレクトを有効にします。

### **Bloomberg** キーボード **4** または **3** の構成:

#### 注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックス

では一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

1. レジストリで次のキーを検索します:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

2. 次のいずれかを行います:

- この機能を有効にするには、種類が **DWORD** で名前が **EnableBloombergHID** の値のデータを 1 に設定します。
- この機能を無効にするには、値のデータを 0 に設定します。

Bloomberg キーボード 3 のサポートは、Online Plug-in 11.2 for Windows 以降のバージョンで利用できます。

Bloomberg キーボード 4 のサポートは、Windows Receiver 4.8 以降のバージョンで利用できます。

**Bloomberg** キーボードのサポートが有効になっているかどうかの確認:

- Bloomberg キーボードのサポートが Online Plug-in で有効になっているかどうかを確認するには、Desktop Viewer で Bloomberg キーボードのデバイスがどのように報告されているかを確認します。Desktop Viewer を使用しない場合は、Online Plug-in が実行されているマシンのレジストリを確認できます。
- Bloomberg キーボードのサポートが有効になっていない場合は、Desktop Viewer に次が表示されています:
  - **Bloomberg Fingerprint Scanner** および **Bloomberg Keyboard Audio** として表示される Bloomberg キーボード 3 用の 2 つのデバイス。
  - Bloomberg キーボード 4 用の 1 つのポリシーリダイレクトデバイス。このデバイスは、**Bloomberg LP Keyboard 2013** として表示されます。
- Bloomberg キーボードのサポートが有効になっている場合は、Desktop Viewer に 2 つのデバイスが表示されます: 1 つは以前と同じように **Bloomberg Fingerprint Scanner** として表示され、もう 1 つは **Bloomberg Keyboard Features** として表示されます。
- Bloomberg Fingerprint Scanner デバイスのドライバーがインストールされていない場合、Bloomberg Fingerprint Scanner エントリが Desktop Viewer に表示されない場合があります。エントリが見つからない場合、Bloomberg Fingerprint Scanner はリダイレクトに使用できない可能性があります。Bloomberg キーボードのサポートが有効になっている他の Bloomberg デバイスの名前は引き続き確認できます。
- レジストリの値をチェックして、サポートが有効になっているかどうかを確認することもできます:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

値が存在しないか、0 (ゼロ) の場合、Bloomberg キーボードのサポートは有効になっていません。値が 1 の場合、サポートが有効になっています。

**Bloomberg** キーボードのサポートの有効化:

注:

Citrix Receiver for Windows 4.8 では、**SplitDevices** ポリシーを通じて複合デバイスのサポートが導入されました。ただし、Bloomberg キーボード 4 の場合、このポリシーの代わりに Bloomberg キーボード機能を使用する必要があります。

Bloomberg キーボードのサポートにより、特定の USB デバイスがセッションにリダイレクトされる方法が変わります。このサポートはデフォルトでは有効になっていません。

- インストール時にサポートを有効にするには、インストールコマンドラインで **ENABLE\_HID\_REDIRECTION** プロパティの値を TRUE に指定します。例:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net" ENABLE_HID_REDIRECTION="TRUE"
```

- Online Plug-in のインストール後にサポートを有効にするには、Online Plug-in が実行されているシステムで Windows レジストリを編集します。
  1. レジストリエディターを開きます。
  2. 次のキーに移動します:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB。`
  3. 値 **EnableBloombergHID** が存在する場合は、値データが 1 になるように変更します。
  4. 値 **EnableBloombergHID** が存在しない場合は、EnableBloombergHID という名前で DWORD 値を作成し、値データを 1 として指定します。

**Bloomberg** キーボードのサポートの無効化:

次のように、Online Plug-in で Bloomberg キーボードのサポートを無効にできます:

1. Online Plug-in ソフトウェアを実行しているシステムでレジストリエディターを開きます。
2. 次のキーに移動します:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB。`
3. 値 **EnableBloombergHID** が存在する場合は、値データが 0 (ゼロ) になるように変更します。

値 **EnableBloombergHID** が存在しない場合は、Bloomberg キーボードのサポートが有効になっていないことを示しています。このような場合、レジストリ値を変更する必要はありません。

サポートを有効にせずに **Bloomberg** キーボードを使用:

- Online Plug-in で Bloomberg キーボードのサポートを有効にしなくても、キーボードを使用できます。ただし、複数のセッション間で特殊な機能を共有するメリットは使用できず、オーディオによってネットワーク帯域幅が増加する可能性があります。

- Bloomberg キーボードの通常のキーは、他のキーボードと同じように使用できます。特別なアクションは必要ありません。
- 専用の Bloomberg キーボードを使用するには、Bloomberg キーボードオーディオデバイスをセッションにリダイレクトする必要があります。Desktop Viewer を使用している場合は、USB デバイスの製造元名とデバイス名が表示され、Bloomberg キーボードオーディオデバイスが **Bloomberg Keyboard Audio** として表示されます。
- 指紋リーダーを使用するには、デバイスを Bloomberg Fingerprint Scanner にリダイレクトする必要があります。指紋リーダーのドライバーがローカルにインストールされていない場合、デバイスには次の情報のみが表示されます：
  - Online Plug-in がデバイスを自動的に接続するように設定されているか、または
  - ユーザーがデバイスの接続を選択できるようにするかが設定されているか。

また、セッションを確立する前に Bloomberg キーボードが接続されていて、指紋リーダードライバーがローカルにインストールされていない場合、指紋リーダーは表示されず、セッション内で使用できません。

注:

Bloomberg 3 の場合、指紋リーダーは単一のセッションまたはローカルシステムで使用でき、共有することはできません。Bloomberg 4 ではリダイレクトが禁止されています。

サポートを有効にした後 **Bloomberg** キーボードを使用:

- Online Plug-in で Bloomberg キーボードのサポートを有効にすると、特殊なキーボード機能を複数のセッションで共有できるというメリットがあります。また、オーディオからのネットワーク帯域幅も抑えられます。
- Bloomberg キーボードのサポートを有効にすると、Bloomberg キーボードオーディオデバイスのリダイレクトが妨げられます。代わりに、新しいデバイスが利用可能になります。Desktop Viewer を使用している場合、このデバイスは Bloomberg キーボード機能と呼ばれます。このデバイスをリダイレクトすると、セッションで特殊な Bloomberg キーを使用できます。

Bloomberg キーボードのサポートを有効にすると、専用の Bloomberg キーとオーディオデバイスにのみ影響します。通常のキーと指紋リーダーは、サポートが有効になっていない場合と同じように使用されます。

## DPI スケール

Windows 向け Citrix Workspace アプリでは、オペレーティングシステムがセッションの解像度を制御できます。

セッションに高 DPI を適用できますが、この機能はデフォルトでは無効になっています。つまり、セッションの表示サイズはオペレーティングシステムの解像度に従います。

次のオプションを使用して、DPI スケールを構成できます。

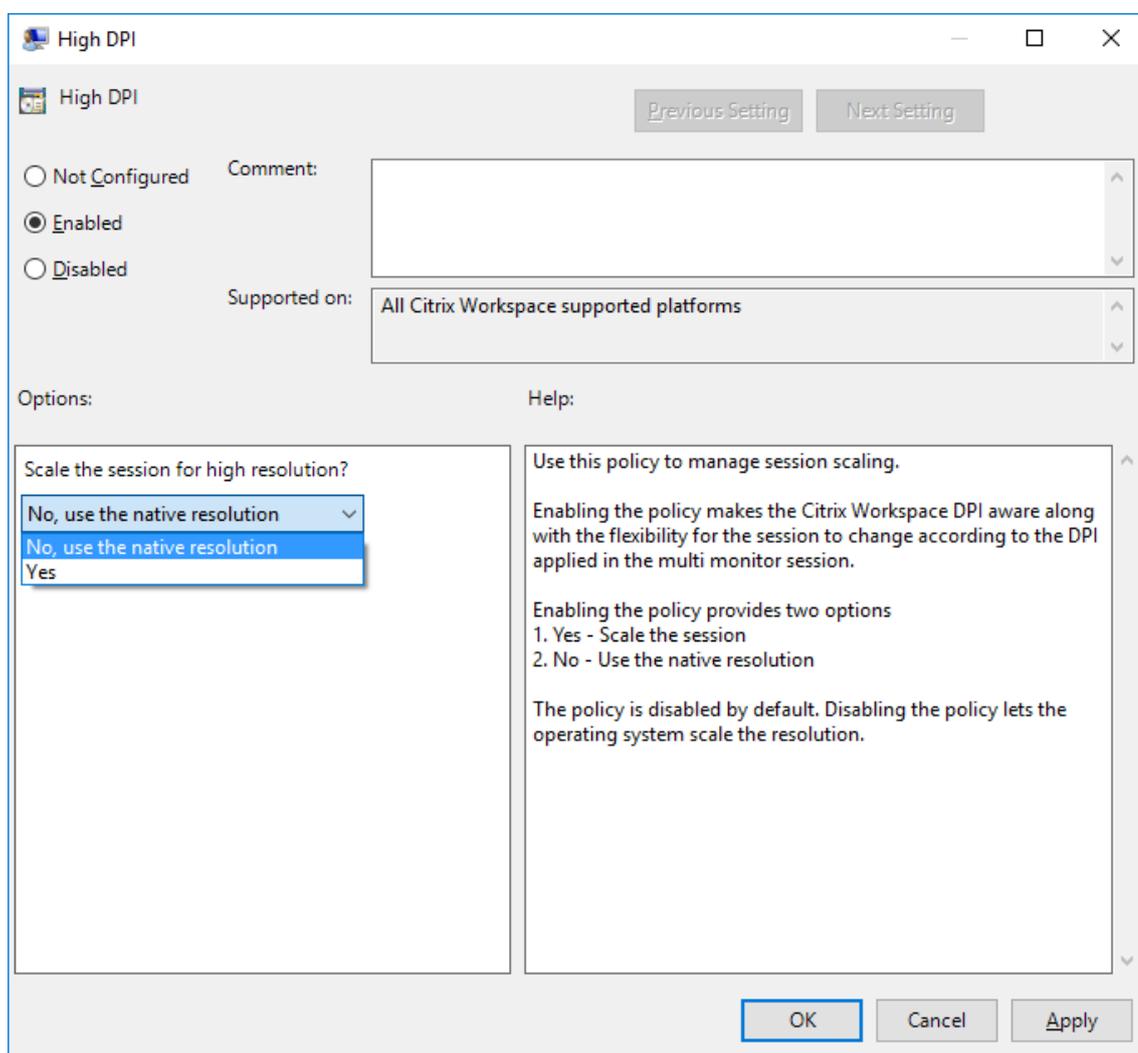
1. グループポリシーオブジェクト (GPO) 管理用テンプレート (マシンごと)
2. 高度な設定 (ユーザーごと)

制限事項:

- この機能を有効にしても、Desktop Viewer の表示がわずかにぼやけます。
- セッションで、DPI 設定を変更して再起動すると、適切なセッションウィンドウのサイズにならないことがあります。この問題を解決するには、セッションウィンドウのサイズを変更します。

**GPO** 管理用テンプレートを使用して **DPI** スケールを構成するには：

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] > [DPI] の順に移動します。
3. 高 **DPI** ポリシーを選択します。



4. 次のいずれかのオプションを選択します：

- a) はい - セッションに高 DPI が適用されます。
- b) いいえ、ネイティブ解像度を使用します - オペレーティングシステムによって設定されている解像度を使用します。

5. [適用]、[OK] の順にクリックします。
6. コマンドラインから `gpupdate /force` コマンドを実行して変更を適用します。

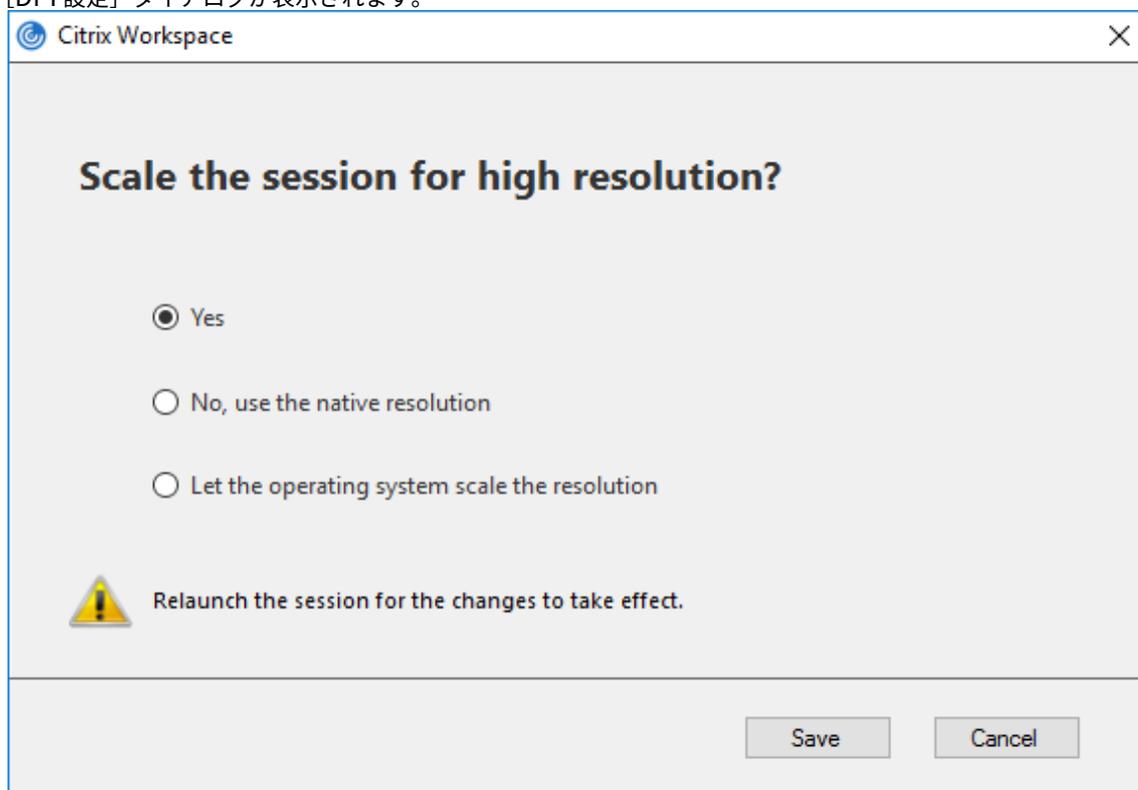
グラフィカルユーザーインターフェイスを使用した **DPI** スケールの構成:

注:

システムトレイの Windows 向け Citrix Workspace アプリアイコンで [高度な設定] シートの一部または全部を非表示にすることができます。詳しくは、「[高度な設定シート](#)」を参照してください。

1. システムトレイの Citrix Workspace アプリアイコンを右クリックします。
2. [高度な設定] を選択して [DPI 設定] をクリックします。

[DPI 設定] ダイアログが表示されます。



3. 次のいずれかのオプションを選択します:
  - a) はい - セッションに高 DPI が適用されます。
  - b) いいえ、ネイティブ解像度を使用します - Workspace アプリは、VDA の DPI を検出して適用します。
  - c) オペレーティングシステムの解像度スケールを適用します - デフォルトではこのオプションが選択されています。これにより、Windows は DPI スケールを処理できます。また、高 DPI ポリシーは無効に設定されます。
4. [保存] をクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

## DPI スケールオプション

Citrix Workspace アプリの DPI スケールでは 3 種類の設定が可能です: Scaled、Unscaled、Operating system scaling。以下は、それぞれの使用例です。

### Scaled:

Scaled 設定は、Operating system scaling と同様に VDA で解像度を変更しますが、異なる DPI が混在するシナリオもサポートします。これは、UI 設定の [はい]、または GPO ポリシーで高 DPI ポリシーを [有効] に設定した場合に相当します。この設定は、最新の VDA に接続するときの異なる DPI が混在するシナリオに適しています。シームレスセッションをスケール設定する唯一の方法です。スケールによって、特にテキスト画面の場合、画像がぼやける可能性があります。古い VDA (6.5、または従来のグラフィック用に構成) に接続すると、パフォーマンスが低下する可能性があります。ローカルアプリアクセス、RTOP、画面の位置 API を使用するその他のプラグインはスケールで機能しません。設計上、シームレスアプリはこのモードでモニター間を移動して、正しいスケール設定を維持します。この設定は、最新の VDA に接続している Windows 10 のユーザーにお勧めします。サーバーのリソースに影響を与えずに、異なる DPI の混在をサポートします。

### Unscaled:

Unscaled 設定は、セッション内のすべてのモニターの高解像度を送信します。これらの解像度はスケールが解除されているため、アプリとデスクトップで小さなテキストやアイコンが表示されることがあります。これは、UI 設定の [いいえ]、または、GPO ポリシーで高 DPI ポリシーを [有効] に設定した場合に相当します。この設定ではスケールによって画面がぼやけることはありませんが、テキストやアイコンは小さくなる可能性があります。デスクトップセッションに接続するときは、DPI を VDA 内で設定して、目的のスケール設定を行うことができます。これは、RDS デスクトップやシームレスアプリケーションでは機能しません。この設定を有効にすると、セッションの解像度が高くなり、サーバーのパフォーマンスとスケーラビリティに影響を与えることがあります。この設定は、追加のサーバーリソースが使用できる場合の、最高画質を必要とするデスクトップセッションにお勧めします。小さなテキストやアイコンがユーザーにとって問題にならない場合にも使用できます。

### Operating system scaling:

Operating system scaling はデフォルトの設定であり、UI 設定の [オペレーティングシステムの解像度スケールを適用します] に相当します。このシナリオでは、高 DPI ポリシーが [無効] に設定されています。これにより、Windows オペレーティングシステムはセッションの DPI スケールを処理します。VDA の解像度は、DPI を基にしてスケール設定され、クライアントデバイスより小さな解像度になります。これは、単一のモニターセッションで適切に動作し、6.5 VDA または従来のグラフィック用に構成された VDA に接続するときに最適です。この方法では、異なる DPI の混在はサポートされません。すべてのモニターが同じ DPI ではない場合、セッションが機能しません。スケールによって、特にテキスト画面の場合、画像がぼやける可能性があります。Windows 10 オペレーティングシステムでカーソルサイズに問題が発生することもあります。

この設定は、最新の VDA に接続している Windows 7 エンドポイントのユーザー、または従来の VDA への接続時にお勧めします。異なる DPI が混在していない場合、Windows 10 でも使用できます。

### 仮想ディスプレイレイアウト

この機能では、リモートデスクトップに適用する仮想モニターレイアウトを定義し、1つのクライアントモニターをリモートデスクトップ上の最大8つのモニターに仮想分割できます。仮想モニターは、Desktop Viewerの[モニターレイアウト]タブで設定できます。ここでは、垂直または水平の線で画面を仮想モニターに分けることができます。画面は、クライアントのモニター解像度で指定されたパーセンテージに従って分割されます。

DPI スケーリングまたは DPI マッチングに使用される仮想モニター用 DPI を設定できます。仮想モニターレイアウトを適用した後、セッションのサイズを変更するか、再接続します。

この構成は、全画面、単一モニターのデスクトップセッションにのみ適用され、公開アプリケーションには影響しません。この構成は、以降のこのクライアントからのすべての接続に適用されます。

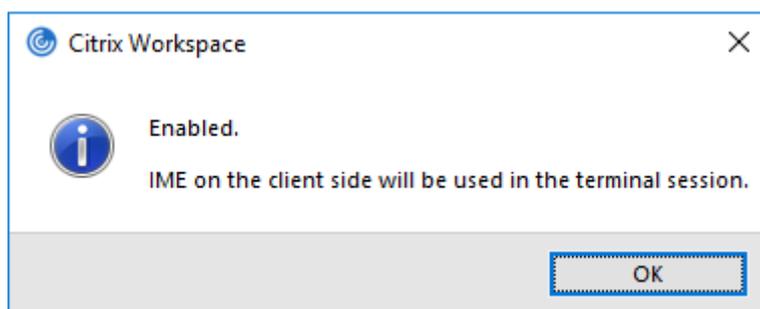
### 汎用クライアント入力システム (IME)

注:

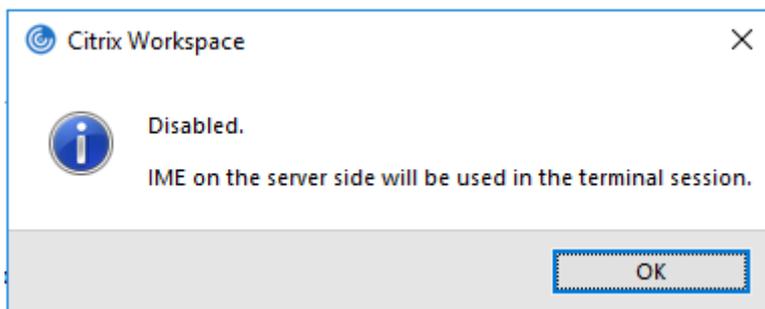
Windows 10 バージョン 2004 オペレーティングシステムを使用している場合、セッションで IME 機能を使用すると、特定の技術的な問題が発生する可能性があります。これらの問題は、サードパーティの制限事項によるものです。詳しくは、[Microsoft 社のサポート記事](#)を参照してください。

コマンドラインインターフェイスを使用した汎用クライアント **IME** の構成:

- 汎用クライアント IME を有効にするには、Citrix Workspace アプリインストールフォルダー (C:\Program Files (x86)\Citrix\ICA Client) から `wfica32.exe /localime:on` コマンドを実行します。



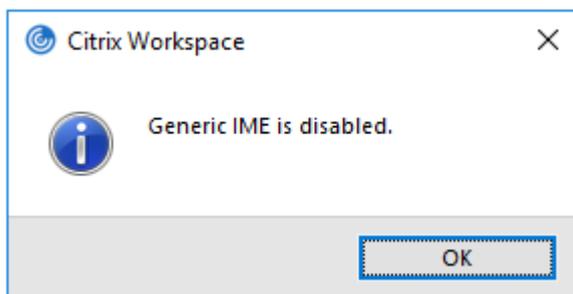
- 汎用クライアント IME を無効にするには、Citrix Workspace アプリインストールフォルダー (C:\Program Files (x86)\Citrix\ICA Client) から `wfica32.exe /localime:off` コマンドを実行します。



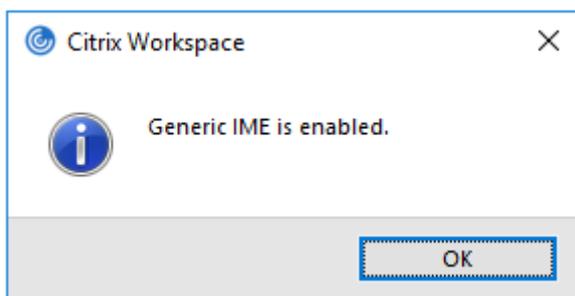
注:

コマンドラインスイッチ `wfica32.exe /localime:on` を使用して、汎用クライアント IME とキーボードレイアウトの同期の両方を有効にすることができます。

- 汎用クライアント IME を無効にするには、Citrix Workspace アプリインストールフォルダー (C:\Program Files (x86)\Citrix\ICA Client) から `wfica32.exe /localgenericime:off` コマンドを実行します。このコマンドは、キーボードレイアウトの同期設定に影響を及ぼしません。



コマンドラインインターフェイスを使用して汎用クライアント IME を無効にした場合、`wfica32.exe /localgenericime:on` コマンドを実行することによって、再び機能を有効化できます。



トグル:

Citrix Workspace アプリは、この機能に対するトグルスイッチ機能をサポートしています。`wfica32.exe /localgenericime:on` コマンドを実行して、機能を有効/無効にできます。ただし、キーボードレイアウトの同期設定は、トグルスイッチより優先されます。キーボードレイアウトの同期がオフに設定されている場合、トグルしても汎用クライアント IME は有効になりません。

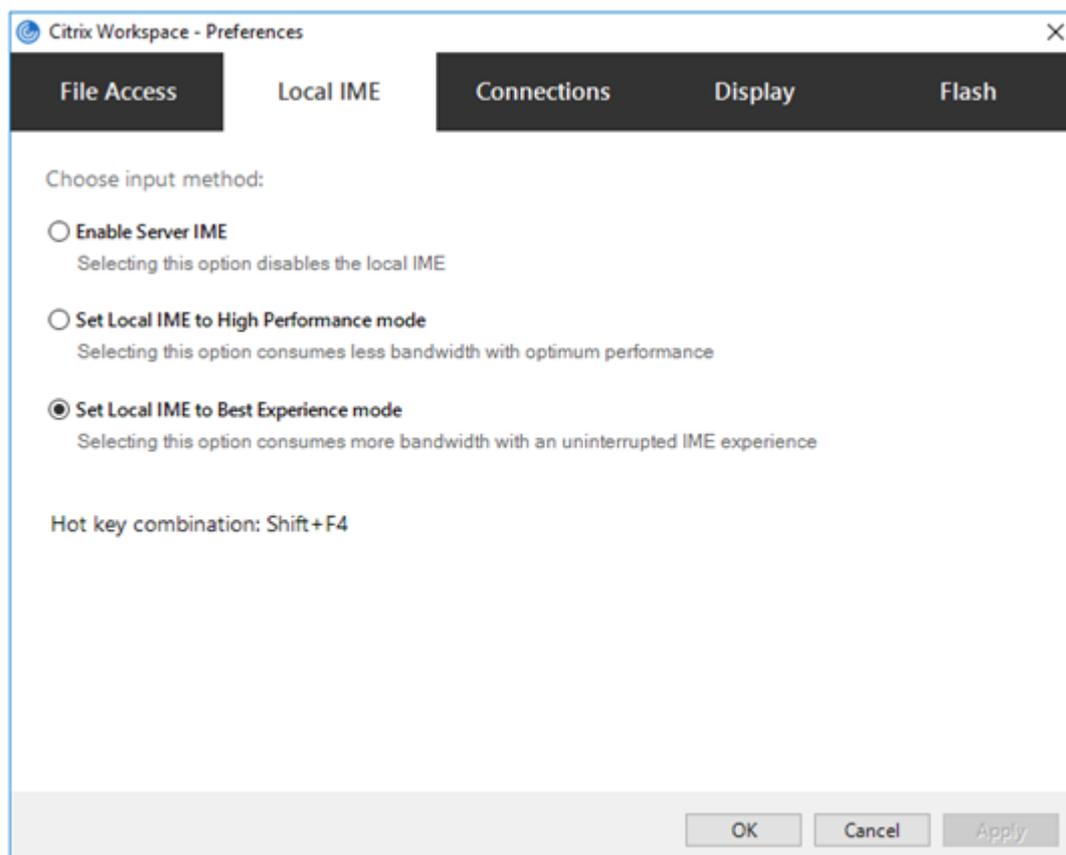
グラフィカルユーザーインターフェイスを使用した汎用クライアント **IME** の構成:

汎用クライアント IME には VDA Version 7.13 以降が必要です。

キーボードレイアウトの同期を有効化することにより、汎用クライアント IME 機能を有効化できます。詳しくは、「[キーボードレイアウトの同期](#)」を参照してください。

Citrix Workspace アプリを使用すると、汎用クライアント IME を使用するためのさまざまなオプションを構成できます。要件および使用状況に基づいて、これらのオプションのいずれかから選択できます。

1. システムトレイの Citrix Workspace アプリアイコンを右クリックして、[コネクションセンター] を選択します。
2. [基本設定]、[ローカル IME] を選択します。



さまざまな IME モードをサポートするために以下のオプションを利用できます。

1. サーバー IME を有効にする - ローカル IME を無効にするため、サーバーの言語セットのみが利用できます。
2. ローカル IME を高パフォーマンスモードに設定する - ローカル IME を限られた帯域幅で使用できます。このオプションは、候補ウィンドウの機能を制限します。
3. ローカル IME を最適なエクスペリエンスモードに設定する - ローカル IME を最適なユーザーエクスペリエンスで使用できます。このオプションは、高帯域を消費します。デフォルトで、汎用クライアント IME が有効の場合、このオプションが選択されます。

変更は、現在のセッションにのみ適用されます。

レジストリエディターを使用したホットキー構成の有効化:

汎用クライアント IME が有効の場合、異なる IME モードを選択するには、**Shift+F4** ホットキーを使用できます。IME モードのさまざまなオプションがセッションの右上隅に表示されます。

デフォルトで、汎用クライアント IME のホットキーは無効です。

レジストリエディターで、`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`に移動します。

**AllowHotKey** を選択して、デフォルト値を 1 に変更します。

**Shift+F4** のホットキーを使用して、セッションで異なる IME モードを選択できます。

これらのホットキーの組み合わせを使用して切り替える場合、IME モードのさまざまなオプションがセッションの右上隅に表示されます。



制限事項:

- 汎用クライアント IME は、Search UI などの UWP (ユニバーサル Windows プラットフォーム) アプリケーションや、Windows 10 オペレーティングシステムの Edge ブラウザーをサポートしません。回避策として、代わりにサーバー IME を使用します。
- 汎用クライアント IME は、保護モードの Internet Explorer バージョン 11 ではサポートされません。回避策として、インターネットオプションを使用して保護モードを無効にできます。そうする場合は、[セキュリティ] をクリックして、[保護モードを有効にする] をオフにします。

## H.265 ビデオエンコーディング

Citrix Workspace アプリは、リモートグラフィックやビデオのハードウェアアクセラレーションで H.265 ビデオコーデックの使用をサポートしています。この機能を活用するには、VDA および Citrix Workspace アプリの両方でサポートされ、有効にする必要があります。エンドポイントの GPU が DXVA インターフェイスを使用する H.265 デコードをサポートしていない場合、グラフィックポリシー設定の H.265 デコードは無視され、セッションは H.264 ビデオコーデックの使用に戻ります。

前提条件:

1. VDA 7.16 以降。
2. VDA で [3D 画像ワークロードの最適化] ポリシーが有効になっている。

3. VDA で [ビデオコーデックにハードウェアエンコーディングを使用します] ポリシーが有効になっている。

注:

H.265 エンコーディングは、NVIDIA 社の GPU でのみサポートされます。

Windows 向け Citrix Workspace アプリでは、この機能がデフォルトで無効になっています。

グループポリシーオブジェクト (GPO) の管理用テンプレートを使用して **Citrix Workspace** アプリで **H.265** ビデオエンコーディングを構成する:

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 Workspace**]、[ユーザーエクスペリエンス] の順に移動します。
3. [グラフィックの **H.265** デコード] ポリシーを選択します。
4. [有効] をクリックします。
5. [適用]、[**OK**] の順にクリックします。

レジストリエディターを使用して **H.265** ビデオエンコーディングを構成する:

**32** ビットオペレーティングシステムのドメイン不参加のネットワークで **H.265** ビデオエンコーディングを有効にする:

1. [ファイル名を指定して実行] コマンドで regedit を使用してレジストリエディターを起動します。
2. HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine にアクセスします。
3. **EnableH265** という名前で DWORD キーを作成し、キーの値を 1 に設定します。

**64** ビットオペレーティングシステムのドメイン不参加のネットワークで **H.265** ビデオエンコーディングを有効にする:

1. [ファイル名を指定して実行] コマンドで regedit を使用してレジストリエディターを起動します。
2. HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine にアクセスします。
3. EnableH265 という名前で DWORD キーを作成し、キーの値を 1 に設定します。

変更を保存するには、セッションを再起動します。

注:

- Windows 向け 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で [グラフィックのハードウェアアクセラレーション] ポリシーが無効になっている場合、[グラフィックの **H.265** デコード] ポリシー設定は無視され、この機能は動作しません。
- HDX Monitor 3.x ツールを実行して、セッション内で H.265 ビデオエンコーダーが有効になっているかを確認します。HDX Monitor 3.x ツールについて詳しくは、Knowledge Center の [CTX135817](#) を参照してください。

### キーボードレイアウトと言語バー

#### キーボードレイアウト

注:

システムトレイの [Citrix Workspace アプリ] アイコンで [高度な設定] シートの一部または全部を非表示にすることができます。詳しくは、「[高度な設定シート](#)」を参照してください。

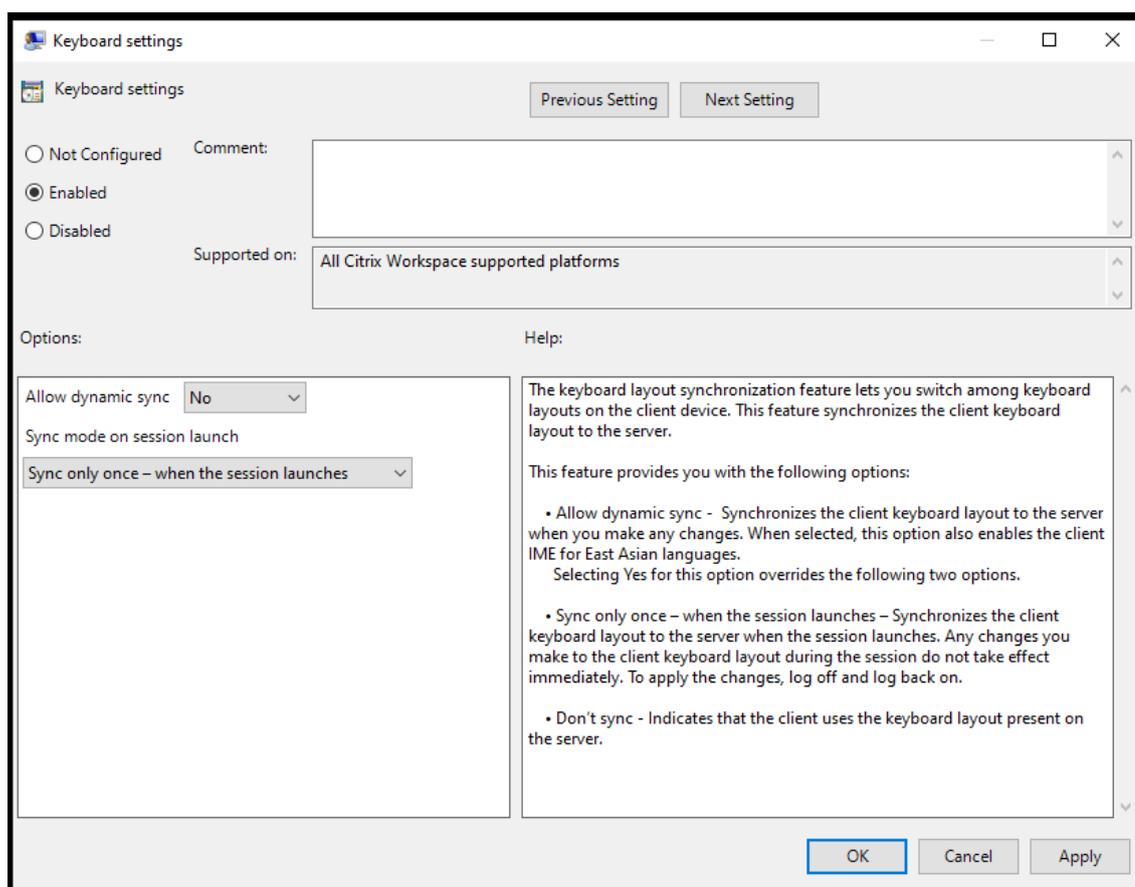
キーボードレイアウトの同期によって、クライアントデバイスの優先キーボードレイアウトを切り替えることができます。この機能はデフォルトでは無効になっています。キーボードレイアウトの同期により、クライアントのキーボードレイアウトが Virtual Apps and Desktops セッションに自動的に同期されます。

**GPO** 管理用テンプレートを使用してキーボードレイアウトの同期を構成:

注:

GPO 構成は、StoreFront および GUI の構成よりも優先されます。

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] または [ユーザー構成] ノードで、[管理用テンプレート] > [管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザーエクスペリエンス] の順に移動します。
3. キーボード設定ポリシーを選択します。



4. [有効] を選択し、次のいずれかのオプションを選択します：

- 動的な同期を許可する - ドロップダウンメニューから [はい] か [いいえ] を選択します。このオプションは、クライアントのキーボードレイアウトを変更したときに、クライアントのキーボードレイアウトをサーバーに同期します。このオプションを選択すると、日本語、中国語、韓国語のクライアント IME も有効になります。

このオプションで [はい] を選択すると、次の 2 つのオプションが上書きされます。

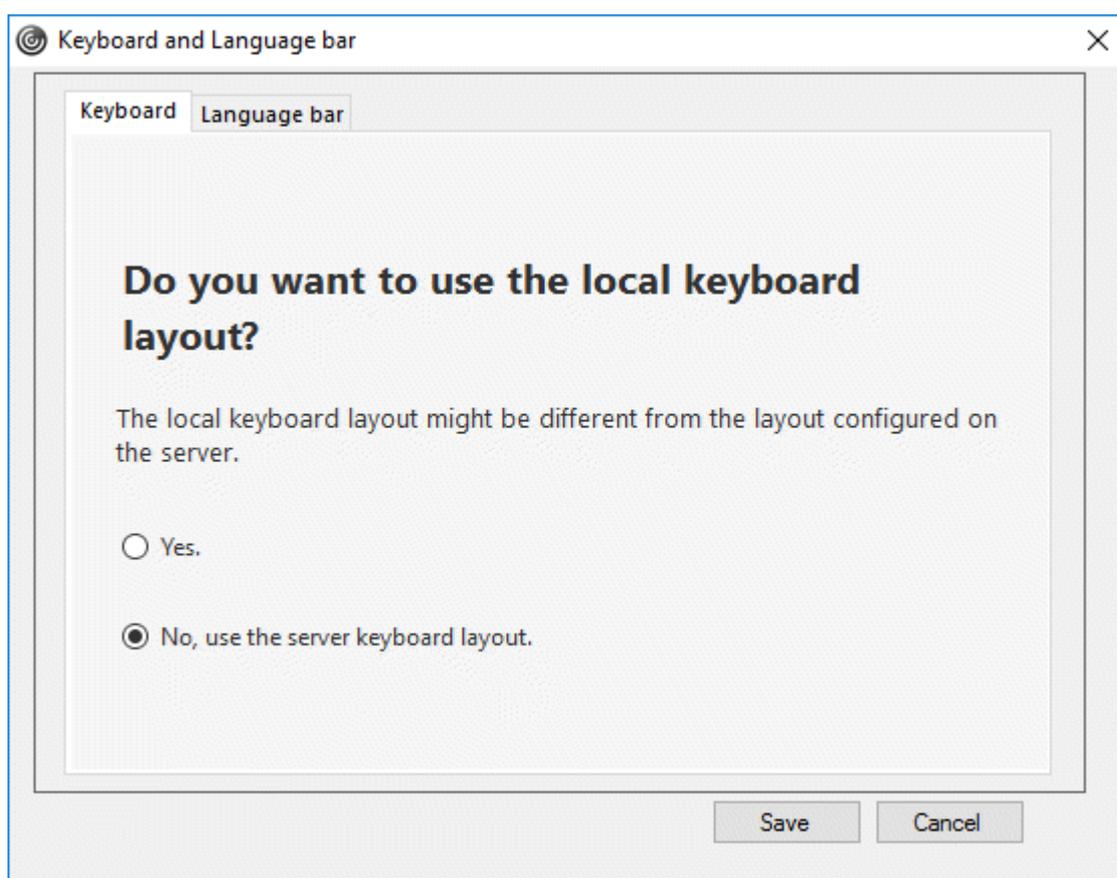
- セッション起動時の同期モード - ドロップダウンメニューから、次のいずれかのオプションを選択します：
  - セッション起動時に **1** 回だけ同期する - セッション起動時にクライアントのキーボードレイアウトをサーバーに同期します。セッション中にクライアントのキーボードレイアウトに加えた変更は、すぐに有効になりません。変更を適用するには、ログオフしてから再度ログオンします。
  - 同期させない - クライアントがサーバーのキーボードレイアウトを使用することを示します。

5. [適用] と [OK] を選択します

グラフィカルユーザーインターフェイスを使用してキーボードレイアウトの同期を構成するには：

- システムトレイの Citrix Workspace アプリアイコンで [高度な設定] > [キーボードと言語バー] の順に選択します。

キーボードと言語バーのダイアログが開きます。



2. 次のいずれかのオプションを選択します：

- [セッション起動時に **1** 回だけ同期させます] - セッション起動時に 1 度のみキーボードレイアウトを VDA から同期させます。
- 動的な同期を許可する - セッション内でクライアントキーボードが変更されると、キーボードレイアウトは VDA に動的に同期されます。
- 同期させない - クライアントがサーバーのキーボードレイアウトを使用することを示します。

3. [保存] をクリックします。

**CLI** を使用してキーボードレイアウトの同期を構成するには：

Windows 向け Citrix Workspace アプリのインストールフォルダーから次のコマンドを実行します。

通常、Citrix Workspace アプリのインストールフォルダーは `C:\Program files (x86)\Citrix\ICA Client` にあります。

- 有効にするには： `wfica32:exe /localime:on`
- 無効にするには： `wfica32:exe /localime:off`

クライアントのキーボードレイアウトオプションで、クライアント IME (Input Method Editor) をアクティブにします。日本語、中国語、または韓国語を使用しているユーザーがサーバー IME を使用する場合、[いいえ] を選択するか、`wfica32:exe /localime:off` を実行してローカルキーボードレイアウトオプションを無効にする必要が

あります。次のセッションに接続すると、セッションは、リモートサーバーで指定されたキーボードレイアウトに戻します。

クライアントのキーボードレイアウトの切り替えがアクティブなセッションで有効にならないことがあります。この問題を解決するには、いったん Citrix Workspace アプリからログオフしてから、再度ログインしてください。

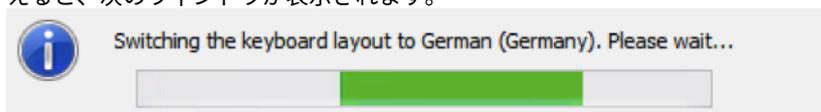
### Windows VDA でのキーボード同期の構成

注:

次の手順は、Windows Server 2016 以降にのみ適用されます。Windows Server 2012 R2 以前では、キーボード同期機能はデフォルトで有効になっています。

1. レジストリエディターを起動して、`HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`に移動します。
2. DWORD エントリ `DisableKeyboardSync` を作成し、その値を 0 に設定します。  
1 はキーボードレイアウトの同期機能を無効にします。
3. 変更を保存するには、セッションを再起動します。

VDA と Citrix Workspace アプリの両方でキーボードレイアウトを有効にした後、キーボードレイアウトを切り替えると、次のウィンドウが表示されます。



このウィンドウは、セッションのキーボードレイアウトがクライアントのキーボードレイアウトに切り替えられていることを示しています。

### Linux VDA でのキーボード同期の構成

コマンドプロンプトを起動して、次のコマンドを実行します:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

変更を保存するには、VDA を再起動します。

Linux VDA でのキーボードレイアウトの同期について詳しくは、「[動的なキーボードレイアウトの同期](#)」を参照してください

キーボードレイアウトの切り替え通知ダイアログを非表示にする:

キーボードレイアウトの変更通知ダイアログでは、VDA セッションがキーボードレイアウトを切り替えるときに通知します。キーボードレイアウトの切り替えには、約 2 秒かかります。通知ダイアログを非表示にする場合、間違った文字入力を避けるために、しばらく待ってから入力を開始してください。

### 警告

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

レジストリエディターを使用してキーボードレイアウトの切り替え通知ダイアログを非表示にする：

1. レジストリエディターを起動して、`HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`に移動します。
2. **HideNotificationWindow** という名前で文字列値キーを作成します。
3. DWORD 値を **1** に設定します。
4. **[OK]** をクリックします。
5. 変更を保存するには、セッションを再起動します。

### 制限事項：

- 管理者権限で実行しているリモートアプリケーション（例：アプリケーションアイコンを右クリックして、[管理者として実行]）は、クライアントのキーボードレイアウトと同期することはできません。この問題を解決するには、サーバー側（VDA）で手動でキーボードレイアウトを変更するか、UAC を無効にします。
- ユーザーがクライアントのキーボードレイアウトをサーバーでサポートされていないレイアウトに変更すると、キーボードレイアウトの同期機能は、セキュリティ上の理由で無効になります。認識されないキーボードレイアウトは、潜在的なセキュリティ上の脅威として扱われるためです。キーボードレイアウト同期機能を復元するには、ログオフしてセッションに再ログインします。
- RDP セッションでは、Alt+Shift のショートカットキーでキーボードレイアウトを変更することはできません。この問題を回避するには、RDP セッションの言語バーを使用してキーボードレイアウトを切り替えます。

### 言語バー

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。言語バーは、デフォルトでセッションに表示されます。

#### 注：

この機能は、VDA 7.17 以降で動作するセッションで使用できます。

### GPO 管理用テンプレートを使用した言語バーの構成：

言語バーには、アプリケーションセッションでの優先される入力言語が表示されます。

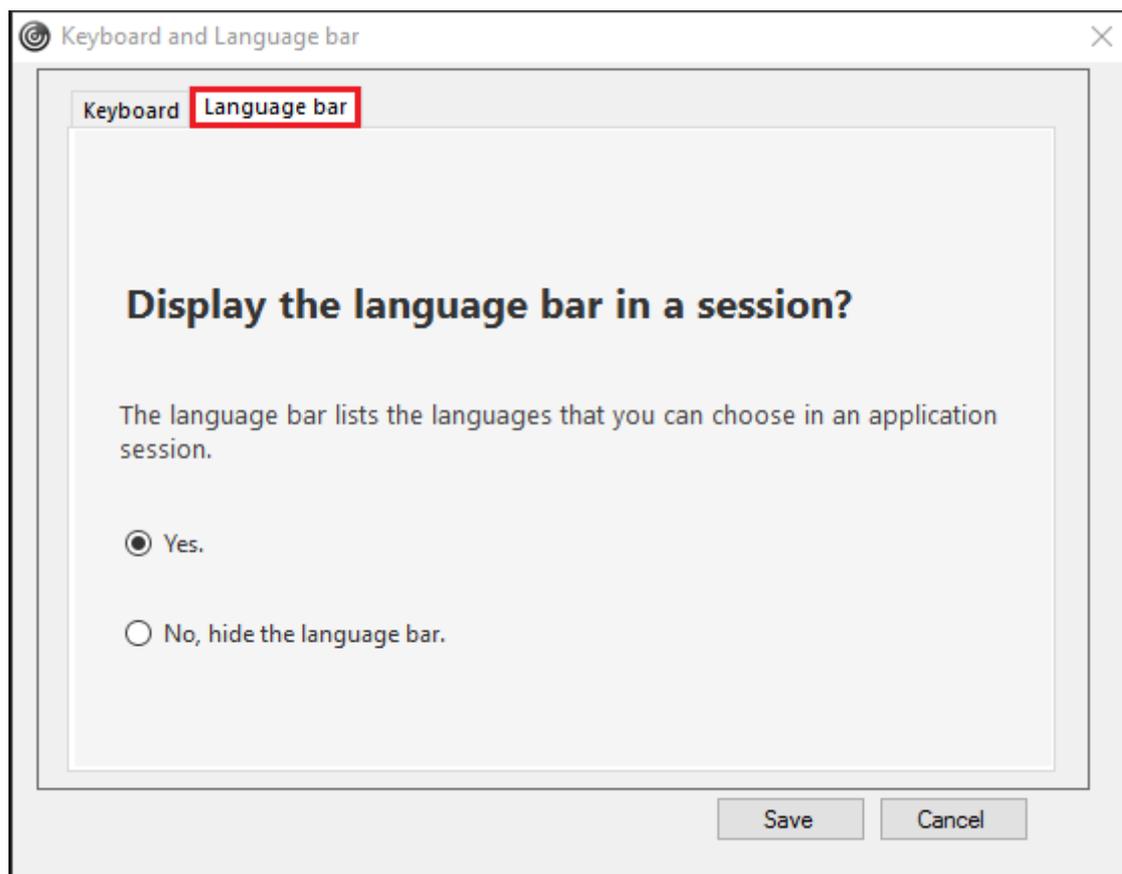
1. `gpedit.msc` を実行して、Citrix Workspace アプリグループポリシーオブジェクト管理用テンプレートを開きます。
2. [コンピューターの構成] または [ユーザー構成] ノードで、[管理用テンプレート] > [管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザーエクスペリエンス] の順に移動します。

3. 言語バーポリシーを選択します。
4. [有効] を選択し、次のいずれかのオプションを選択します：
  - はい - アプリケーションセッションで言語バーが表示されます。
  - いいえ。言語バーを非表示にします - アプリケーションセッションで言語バーが非表示になります。
5. [適用]、[OK] の順にクリックします。

グラフィカルユーザーインターフェイスを使用した言語バーの構成：

1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、[高度な設定] をクリックします。
2. [キーボードと言語バー] を選択します。
3. [言語バー] タブを選択します。
4. 次のいずれかのオプションを選択します：
  - a) はい - セッションで言語バーが表示されます。
  - b) いいえ。言語バーを非表示にします - セッションで言語バーが非表示になります。
5. [保存] をクリックします。

設定の変更は直ちに有効になります。



注:

- アクティブなセッションの設定を変更できます。
- 入力言語が 1 つだけの場合、リモート言語バーはセッションに表示されません。

高度な設定シートで言語バータブを非表示にする:

レジストリを使用して、[高度な設定] シートから言語バータブを非表示にすることができます。

1. レジストリエディターを起動します。
2. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME` にアクセスします。
3. DWORD 値キー **ToggleOffLanguageBarFeature** を作成し、**1** に設定すると、[高度な設定] シートで言語バーオプションが非表示になります。

## USB サポート

USB サポート機能により、Citrix Virtual Apps and Desktops 上で作業しているときにさまざまな種類の USB デバイスを使用できるようになります。コンピューターに USB デバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。この機能では、フラッシュドライブ、スマートフォン、PDA、プリンター、スキャナー、MP3 プレーヤー、セキュリティデバイス、およびタブレットなどの USB デバイスがサポートされます。Desktop Viewer のユーザーは、ツールバーの基本設定を使用して、Citrix Virtual Apps and Desktops で USB デバイスを使用できるようにするかどうかを制御できます。

Web カメラ、マイク、スピーカー、ヘッドセットなどの USB デバイスのアイソクロナス機能は、一般的な低遅延/高速 LAN 環境でサポートされます。これにより、Microsoft Office Communicator や Skype などのパッケージでこれらのデバイスを使用できるようになります。

以下の種類のデバイスは直接サポートされるため、Citrix Virtual Apps and Desktops セッションで USB サポート機能は使用されません。

- キーボード
- マウス
- スマートカード

特殊用途の USB デバイス (Bloomberg キーボードや 3D マウスなど) では、USB サポート機能が使用されるように構成できます。Bloomberg キーボードの構成について詳しくは、「[Bloomberg キーボードの構成](#)」を参照してください。

そのほかの特殊用途の USB デバイスのポリシー規則の構成について詳しくは、Knowledge Center の [CTX122615](#) を参照してください。

デフォルトでは、特定の種類の USB デバイスが Citrix Virtual Apps and Desktops セッションで動作しないように設定されています。たとえば、内部 USB でシステムボードに装着されたネットワークインターフェイスカードの場合、このデバイスのリモート操作は適しません。次の種類の USB デバイスは、Citrix Virtual Apps and Desktops セッションでの使用をデフォルトでサポートしていません。

- Bluetooth ドングル
- 統合ネットワークインターフェイスカード
- USB ハブ
- USB グラフィックアダプター

USB ハブに接続されたデバイスは仮想デスクトップで使用できますが、USB ハブ自体はリモート処理できません。

次の種類の USB デバイスは、Citrix Virtual Apps セッションでの使用をデフォルトでサポートしていません。

- Bluetooth ドングル
- 統合ネットワークインターフェイスカード
- USB ハブ
- USB グラフィックアダプター
- オーディオデバイス
- 大容量記憶装置デバイス

#### USB サポートのしくみ:

ユーザーがエンドポイントに USB デバイスを接続すると、USB ポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。USB ポリシーで拒否されるデバイスは、ローカルのデスクトップ上でのみ使用可能になります。

USB デバイスを接続すると、新しいデバイスについて知らせる通知が表示されます。ユーザーは、USB デバイスを接続するたびに、そのデバイスを仮想デスクトップで使用するかどうかを選択できます。ユーザーは、仮想デスクトップセッションの開始前、またはセッション実行中に接続した USB デバイスが、フォーカスのある仮想デスクトップで自動的に使用可能になるように設定することもできます。

#### 大容量記憶装置デバイス

マストレージデバイス（大容量記憶装置）の場合は、USB サポートに加え、クライアント側ドライブのマッピング機能によるリモートアクセスも可能で、これは Windows 向け Citrix Workspace アプリポリシーの [クライアントデバイスをリモート処理します] > [クライアントドライブマッピング] で設定します。このポリシーを適用すると、ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップ上のドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。

クライアント側リムーバブルドライブマッピングと USB サポートの 2 つの設定の主な違いは以下のとおりです。

| 機能               | クライアント側ドライブのマッピング | USB サポート |
|------------------|-------------------|----------|
| デフォルトで有効         | はい                | いいえ      |
| 読み取り専用アクセスの構成が可能 | はい                | いいえ      |

| 機能                   | クライアント側ドライブのマッピング | USB サポート                                     |
|----------------------|-------------------|----------------------------------------------|
| セッション中にデバイスを安全に取り外せる | いいえ               | はい（ユーザーがシステムトレイの [ハードウェアの安全な取り外し] をクリックする場合） |

汎用 USB とクライアントドライブマッピングの両方のポリシーが有効で、マストレージデバイスがセッションの開始前に装着された場合は、USB サポート機能によるリダイレクトの前にクライアントドライブマッピングによるリダイレクトが実行されます。マストレージデバイスがセッションの開始後に装着された場合は、クライアントドライブマッピングの前に USB サポートによるリダイレクトが実行されます。

デフォルトで許可される **USB** デバイスのクラス:

以下のクラスの USB デバイスは、デフォルトの USB ポリシー規則により仮想デスクトップでの使用が許可されます。

この一覧に記載されていても、一部のクラスは構成を追加しなければ Citrix Virtual Apps and Desktops セッションでリモート処理ができません。それらのクラスについては以下に記述します。

- オーディオ (クラス **01**) - このクラスのデバイスとして、オーディオ入力デバイス (マイク)、オーディオ出力デバイス、および MIDI コントローラーがあります。最近のオーディオデバイスでは一般的にアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。USB サポートを使用する Citrix Virtual Apps でオーディオデバイスをリモート操作できないため、オーディオ (クラス 01) は Citrix Virtual Apps に適用できません。

注:

VoIP 電話などの一部の特殊デバイスには追加の構成が必要です。詳しくは、Knowledge Center の [CTX123015](#) を参照してください。

- 物理インターフェイスデバイス (クラス **05**) - このデバイスはヒューマンインターフェイスデバイス (HID) と似ていますが、一般的に「リアルタイム」の入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。
- 静止画 (クラス **06**) - このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。ほとんどのデジタルカメラは、画像転送プロトコル (PTP) またはメディア転送プロトコル (MTP) を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。また、デジタルカメラはマストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

注:

カメラがマストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USB サ

ポートは必要ありません。

- プリンター (クラス **07**) - 一部のプリンターではベンダー固有のプロトコル (クラス ff) が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USB ハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーや FAX 機能では静止画などの別のクラスが使用されます。

プリンターは通常、USB サポートなしで適切に動作します。

### 注

このクラスのデバイス (特にスキャナー機能を持つプリンター) には追加の構成が必要です。構成手順については、Knowledge Center の[CTX123015](#)を参照してください。

- マスストレージデバイス (クラス **08**) - 最も一般的なマスストレージデバイス (大容量記憶装置) として、USB フラッシュドライブがあります。そのほかには、USB 接続のハードドライブ、CD/DVD ドライブ、および SD/MMC カードリーダーがあります。また、内部ストレージを持つさまざまなデバイスがあり、これらもこのクラスのインターフェイスを提供します。たとえば、メディアプレーヤー、デジタルカメラ、携帯電話などがあります。USB サポートを使用する Citrix Virtual Apps でマスストレージデバイスをリモート操作できないため、マスストレージ (クラス 08) は Citrix Virtual Apps に適用できません。既知のサブクラスには次のものが含まれます:

- 01 制限付きフラッシュデバイス
- 02 一般的な CD/DVD デバイス (ATAPI/MMC-2)
- 03 一般的なテープデバイス (QIC-157)
- 04 一般的なフロッピーディスクドライブ (UFI)
- 05 一般的なフロッピーディスクドライブ (SFF-8070i)
- 06 ほとんどの大容量記憶装置デバイスはこの SCSI のバリエーションを使用します

マスストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USB サポートは必要ありません。

- コンテンツセキュリティ (クラス **0d**) - 通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。
- ビデオ (クラス **0e**) - このクラスのデバイスとして、ビデオ、Web カメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。

### 重要

ほとんどのビデオストリーミングデバイスではアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。動作検知機能付きの Web カメラなど、一部のビデオデバイスには追加の構成が必要です。構成手順については、Knowledge Center の[CTX123015](#)を参照してください。

- パーソナルヘルスケア (クラス **0f**) - このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。

- アプリケーションおよびベンダー固有（クラス **fe** および **ff**） - 多くのデバイスがベンダー独自のプロトコルまたは USB コンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有（クラス **ff**）として分類されます。

### デフォルトで拒否される **USB** デバイスのクラス

次の USB デバイスの異なるクラスは、デフォルトの USB ポリシー規則により拒否されます。

- 通信および CDC コントロール（クラス 02 および 0a）。仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトの USB ポリシーではこれらのデバイスのリモートでの実行は許可されていません。

- ヒューマンインターフェイスデバイス（クラス 03）。さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス（HID）として、キーボード、マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、およびコントロール機能などがあります。

サブクラス 01 は「起動インターフェイス」クラスとして知られ、キーボードおよびマウスで使用されます。

デフォルトの USB ポリシーは USB キーボード（クラス 03、サブクラス 01、プロトコル 1）または USB マウス（クラス 03、サブクラス 01、プロトコル 2）を許可しません。これは、ほとんどのキーボードおよびマウスは USB サポートなしでも適切に処理され、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。

- USB ハブ（クラス 09）。USB ハブを使用すると、より多くのデバイスをローカルのコンピューターに接続できます。これらのデバイスにリモートでアクセスする必要はありません。
- スマートカード（クラス 0b）。スマートカードリーダーには、非接触型および接触型のスマートカードリーダーと、スマートカードと同等のチップを埋め込んだ USB トークンがあります。

スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USB サポートは必要ありません。

- ワイヤレスコントローラー（クラス e0）。これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetooth キーボードやマウスなどの基幹周辺装置を接続していたりするものがあります。

デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。

- その他のネットワークデバイス（クラス **ef**、サブクラス **04**） - これらのデバイスの一部は、重要なネットワークアクセスを提供している可能性があります。デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。

仮想デスクトップで使用できる **USB** デバイスの一覧の変更

Windows 向け Citrix Workspace のテンプレートファイルを編集して、仮想デスクトップセッション内で使用できる USB デバイスの範囲を更新できます。これにより、グループポリシーを使用して Windows 向け Citrix Workspace に変更を加えることができます。このファイルは、次のインストールフォルダーにあります：

`\C:\Program Files\Citrix\ICA Client\Configuration\en`

または、各ユーザーデバイスのレジストリに次のレジストリキーを追加できます：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB 種類 = 文字列名前 = "DeviceRules" 値 =

### 重要

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

製品のデフォルトの規則は、次の場所に保存されています：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB 種類 = MultiSz 名前 = "DeviceRules" 値 =

これらのデフォルトの規則は変更しないでください。

USB デバイスのポリシー設定について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[USB デバイスのポリシー設定](#)」を参照してください。

## USB オーディオの構成

注：

- Windows 向け Citrix Workspace アプリを初めてアップグレードまたはインストールする場合、最新のテンプレートファイルをローカル GPO に追加します。テンプレートファイルをローカル GPO に追加する方法については、「[グループポリシーオブジェクト管理用テンプレート](#)」を参照してください。アップグレードの場合、最新のファイルをインポートする時に既存の設定が保持されます。
- この機能は、Citrix Virtual Apps サーバーでのみ使用できます。

**USB** オーディオデバイスを構成するには：

- 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。
- [コンピューターの構成] ノードで、[管理用テンプレート] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザーエクスペリエンス] の順に移動し、[一般的な USB リダイレクトによるオーディオ] をクリックします。
- 設定を編集します。

4. [適用]、[OK] の順にクリックします。
5. コマンドプロンプトを管理者モードで開きます。
6. 次のコマンドを実行します。

```
gpupdate /force
```

## vPrefer 起動

以前のリリースでは、**Citrix Studio** の KEYWORDS:prefer="application" 属性を設定することで、VDA にインストールされたアプリケーションのインスタンス（このドキュメントではローカルインスタンスと呼びます）を公開アプリケーションよりも優先して起動するよう指定できました。

バージョン 4.11 から、ダブルホップシナリオ（セッションをホストしている VDA で Citrix Workspace アプリが実行されている）では、VDA にインストールされたアプリケーションのローカルインスタンス（ローカルアプリとして使用できる場合）を、Citrix Workspace アプリがアプリケーションのホストされたインスタンスよりも優先して起動するかを制御できるようになりました。

vPrefer は、StoreFront バージョン 3.14 および Citrix Virtual Desktops 7.17 以降で使用できます。

アプリケーションを起動すると、Citrix Workspace アプリは StoreFront サーバー上のリソースデータを読み取り、列挙時に **vprefer** フラグに基づいてこの設定を適用します。Citrix Workspace アプリは、VDA の Windows レジストリでアプリケーションのインストールパスを検索し、存在する場合はアプリケーションのローカルインスタンスを起動します。それ以外の場合は、アプリケーションのホストされたインスタンスを起動します。

VDA にインストールされていないアプリケーションを起動すると、ホストされているアプリケーションが起動します。StoreFront でローカル起動を処理する方法について詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[公開デスクトップ上のアプリケーションのローカル起動を制御する](#)」を参照してください。

アプリケーションのローカルインスタンスを VDA で起動しない場合は、Delivery Controller で PowerShell を使用して **LocalLaunchDisabled** を **True** に設定します。詳しくは、[Citrix Virtual Apps and Desktops](#) ドキュメントを参照してください。

この機能によって、アプリケーションをよりすばやく起動できるため、より良いユーザーエクスペリエンスを実現できます。この機能は、グループポリシーオブジェクト（GPO）管理用テンプレートで構成できます。デフォルトでは、vPrefer はダブルホップシナリオでのみ有効です。

### 注:

Citrix Workspace アプリを初めてアップグレードまたはインストールする場合、最新のテンプレートファイルをローカル GPO に追加します。テンプレートファイルをローカル GPO に追加する方法については、「[グループポリシーオブジェクト管理用テンプレート](#)」を参照してください。アップグレードの場合、最新のファイルをインポートする時に既存の設定が保持されます。

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 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] > [SelfService] の順に移動します。
3. **vPrefer** ポリシーを選択します。

4. [有効] を選択し、[アプリを許可] ドロップダウンメニューの次のオプションから選択します。
  - [すべてのアプリを許可]: このオプションは、VDA 上のすべてのアプリケーションのローカルインスタンスを起動します。Citrix Workspace アプリは、インストールされているアプリケーション（メモ帳、電卓、ワードパッド、コマンドプロンプトなどのネイティブ Windows アプリを含む）を検索し、ホストされているアプリの代わりに VDA で起動します。
  - インストール済みアプリを許可: このオプションは、VDA 上のすべてのアプリケーションのローカルインスタンスを起動します。アプリが VDA にインストールされていない場合は、ホストされているアプリを起動します。**vPrefer** ポリシーが [有効] に設定されている場合、デフォルトで [インストール済みアプリを許可] が選択されます。このオプションは、メモ帳、電卓などのネイティブ Windows オペレーティングシステムアプリケーションを除外します。
  - ネットワークアプリを許可: このオプションは、共有ネットワークに公開されているアプリのインスタンスを起動します。
5. [適用]、[OK] の順にクリックします。
6. 変更を保存するには、セッションを再起動します。

### 制限事項:

- Web 向け Workspace はこの機能をサポートしていません。

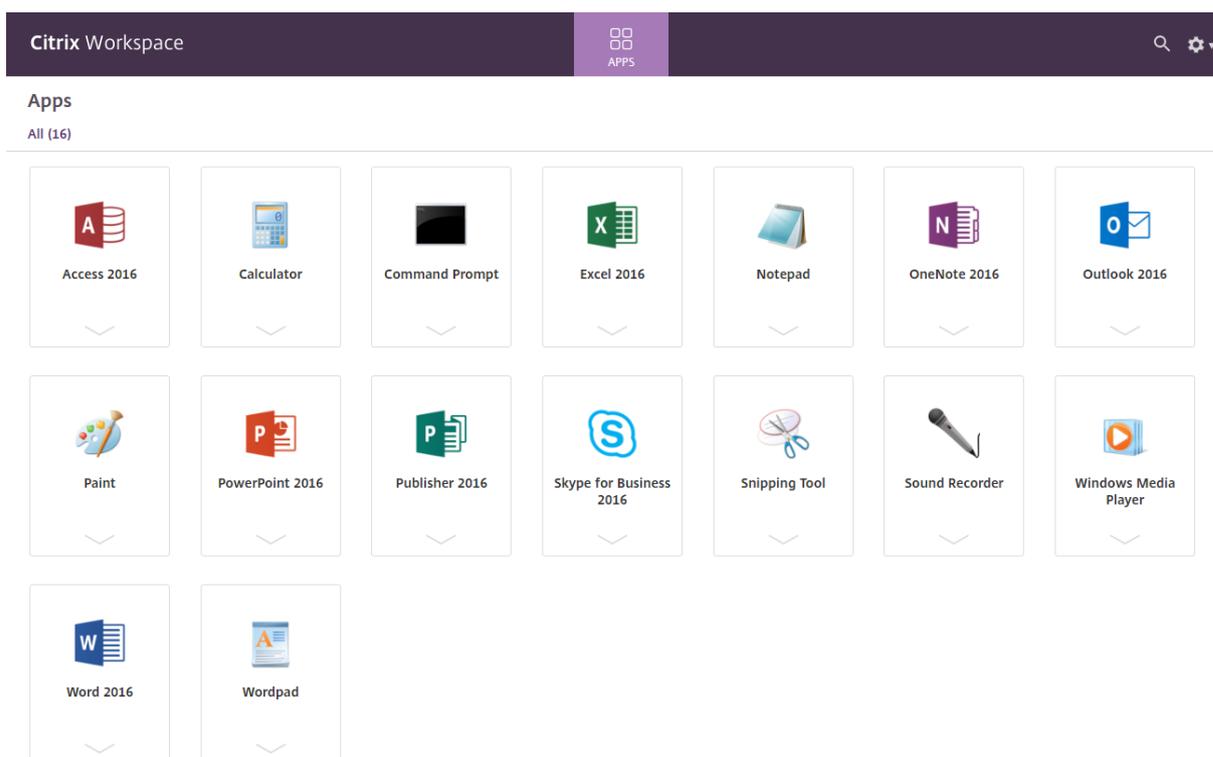
## Workspace の構成

Windows 向け Citrix Workspace アプリでは、Citrix Cloud から提供されている 1 つまたは複数のサービスを使用している利用者が使用できる Workspace を構成できるようになりました。

Citrix Workspace アプリには、ユーザーが権限を持つ特定のワークスペースリソースのみがインテリジェントに表示されます。Citrix Workspace アプリで使用可能なデジタルワークスペースリソースの提供はすべて、Citrix Cloud のワークスペース環境サービスが行います。

ワークスペースはデジタルワークスペースソリューションの一部で、これによって IT 部門は、任意のデバイスからアプリケーションへの安全なアクセスを提供できます。

このスクリーンショットは、利用者に表示されるワークスペースの例です。インターフェイスは進化しているため、現在利用者に表示される内容とは異なる場合があります。例えば、ページ上部に「Workspace」ではなく、「StoreFront」と表示されるようになっています。



### Content Collaboration サービスの統合

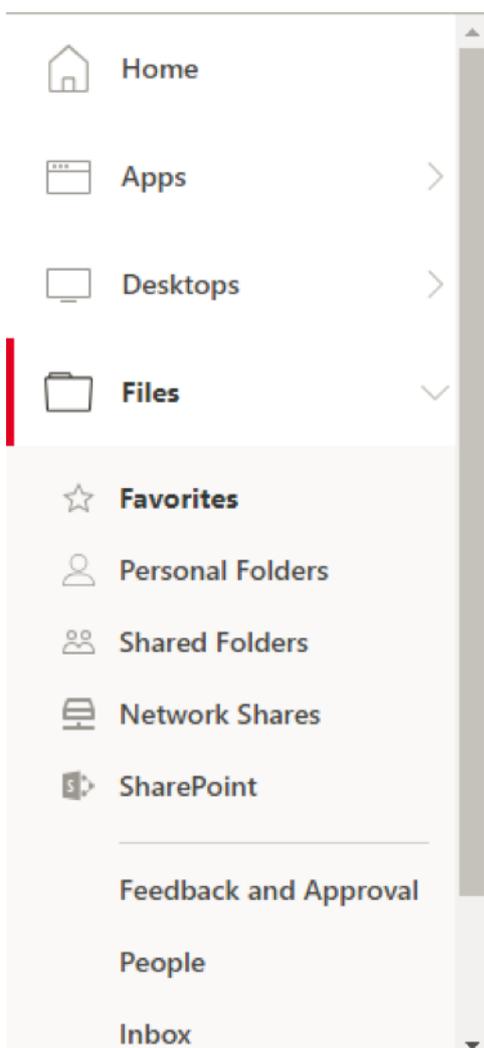
このリリースでは、Citrix Content Collaboration サービスが Citrix Workspace アプリに統合されました。Citrix Content Collaboration を使用すると、ドキュメントを簡単かつセキュアに交換したり、メールで大容量のドキュメントを送信したり、サードパーティへのドキュメント転送をセキュアに処理したり、コラボレーションスペースにアクセスすることができます。また、Web ベースのインターフェイス、モバイルクライアント、デスクトップアプリ、Microsoft Outlook や Gmail との統合など、Citrix Content Collaboration により、さまざまな方法で作業できます。

Citrix Content Collaboration 機能には、Citrix Workspace アプリの [ファイル] タブからアクセスできます。[ファイル] タブは、Citrix Cloud コンソールのワークスペース構成で Content Collaboration サービスが有効になっている場合にのみ表示されます。

注:

オペレーティングシステムでセキュリティオプションが設定されているため、Citrix Workspace アプリでの Citrix Content Collaboration の統合は、Windows Server 2012 および Windows Server 2016 ではサポートされていません。

次の図は、新しい Citrix Workspace アプリの [ファイル] タブの例です:



制限事項:

- Citrix Workspace アプリをリセットしても、Citrix Content Collaboration はログオフされません。
- Citrix Workspace アプリでストアを切り替えても、Citrix Content Collaboration はログオフされません。

レジストリエディターを使用した **Citrix Files** のダウンロード場所の構成:

1. レジストリエディターを起動して、`HKEY_CURRENT_USER\Software\Citrix\Dazzle\` に移動します。
2. **DownloadPreference** という名前で文字列値キーを作成します。
3. Citrix Files の優先ダウンロードパスをコピーして [値] 列に貼り付けます。
4. ダウンロードごとにプロンプトが表示されるようにするには、[値] 列を \* に設定します。

[高度な設定] UI を使用して Citrix Files のダウンロード場所を構成する方法については、Windows 向け Citrix Workspace アプリのヘルプドキュメントで [Configuring download location using Advanced Preferences](#) を参照してください。

### SaaS アプリ

SaaS アプリへのセキュリティ保護されたアクセス機能によって、統合されたユーザーエクスペリエンスで公開 SaaS アプリをユーザーに提供できます。SaaS アプリはシングルサインオンで利用できます。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るようになりました。

Windows 向け Citrix Workspace アプリは、Citrix Secure Workspace Access を使用した SaaS アプリの使用をサポートします。このサービスにより、管理者は一貫したエクスペリエンスを提供し、シングルサインオンを統合し、コンテンツ検査を利用することができます。

SaaS アプリをクラウドで提供する利点は次のとおりです：

- シンプルな構成 - 操作、更新、使用が簡単です。
- シングルサインオン - シングルサインオンで簡単にログオンできます。
- さまざまなアプリの標準テンプレート - 一般的なアプリをテンプレートを使用して構成できます。

前提条件：

- シングルサインオン機能を適用するには、SaaS アプリケーションが SAML 2.0 認証をサポートしている必要があります。
- 組み込みブラウザが SaaS アプリケーションのレンダリングで使用されるように、Citrix Secure Workspace Access で [セキュリティ強化を有効にする] オプションを有効にする必要があります。このオプションが有効になっていない場合、SaaS アプリはクライアントに設定されたデフォルトのブラウザを使用して起動されます。

注：

Citrix Workspace アプリは、オンプレミス環境とクラウド環境の両方から公開されたアプリ、デスクトップ、ファイルを集約して、ユーザーエクスペリエンスを統合します。

Citrix Workspace アプリには、SaaS アプリを起動するためのブラウザが組み込まれています。これによって、セキュアな SaaS アプリにアクセスするときに、より快適なユーザーエクスペリエンスを実現できます。

注：

- Web 向け Workspace の場合、SaaS アプリは、組み込みブラウザではなく、クライアントで設定されたデフォルトのブラウザでのみ起動されます。
- ICA セッションアプリとセキュリティ保護された SaaS アプリのユーザーエクスペリエンスが異なる場合があります。

組み込みブラウザではツールバー、クリップボード、印刷、ダウンロード、透かしなどの操作を使用できます。これらの操作は、Citrix Secure Workspace Access のポリシー構成で定義されている Citrix Workspace アプリに適用されます。

組み込みブラウザを使用して実行できる操作：

ツールバー - アプリでツールバーオプションを有効にすると、起動したアプリで「戻る」、「進む」、「更新」オプションを表示できます。ツールバーには、クリップボード操作を含む省略記号も表示されます。

クリップボード - アプリでクリップボードアクセスを有効にすると、起動したアプリのツールバーに表示される切り取り、コピー、貼り付けのオプションを使用できます。このオプションを無効にすると、カット、コピー、貼り付けのオプションが灰色表示になります。

印刷 - 起動したアプリで印刷オプションを有効にすると、印刷コマンドを実行できます。無効にすると、起動したアプリに印刷オプションは表示されません。

ナビゲーション - ナビゲーションオプションを有効にすると、起動されたアプリのツールバーに「次へ」および「戻る」アイコンが表示されます。

ダウンロード - ダウンロードオプションを有効にすると、起動したアプリからファイルをダウンロードできます。起動したアプリを右クリックし、[名前を付けて保存] を選択します。保存先を選択して、[ダウンロード] をクリックします。

**注:**

ファイルをダウンロードすると、ダウンロード状況を示す進行状況バーは表示されませんが、ダウンロードは正常に完了します。

透かし - 透かしオプションを有効にすると、起動したアプリに、クライアントマシンのユーザー名と IP アドレスを含む透かしが表示されます。透かしは半透明で、他の情報を表示するために編集することはできません。

### **GPO** を使用したキャッシュの構成:

複数のユーザーが同じデバイスを使用してセキュアな SaaS アプリにログインすると、1 ユーザーのキャッシュが次のユーザーに適用され、ユーザー間で閲覧情報を共有することになります。

この問題を回避するため、Citrix Workspace アプリに新しいグループポリシーオブジェクト (GPO) 管理ポリシーが導入されました。このポリシーを使用すると、ローカルデバイスにブラウザのキャッシュを保存することはできません。

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 Workspace**] > [**Citrix Secure Browser**] の順に移動します。
3. [キャッシュ] ポリシーを選択します。  
注: デフォルトでは、このポリシーは [有効] に設定されています。
4. 無効にするには、[無効] を選択して [適用]、[OK] をクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

### 制限事項:

1. 印刷オプションを有効にしてダウンロードを無効にした公開アプリを起動し、起動したアプリで印刷コマンドを発行すると、ダウンロード機能が制限されている場合でも PDF を保存できることがあります。ダウンロード機能を厳密に無効にするには、印刷オプションを無効にします。
2. アプリに埋め込まれた動画が機能しないことがあります。

ワークスペース構成について詳しくは、Citrix Cloud の「[ワークスペース構成](#)」を参照してください。

Citrix Secure Workspace Access を使用して SaaS アプリを構成する方法については、「[Citrix Secure Workspace Access](#)」に関するドキュメントを参照してください。

### PDF 印刷

Windows 向け Citrix Workspace アプリは、セッションでの PDF 印刷をサポートしています。Citrix PDF ユニバーサルプリンタードライバを使用すると、Citrix Virtual Apps and Desktops で実行されているホストアプリケーションやデスクトップを使用して起動したドキュメントを印刷できます。

[印刷] ダイアログボックスで [**Citrix PDF** プリンター] オプションを選択すると、ドライバがファイルを PDF に変換して、これをローカルデバイスに転送します。その後、デフォルトの PDF ビューアで PDF を表示したり、ローカルに接続されたプリンターで印刷したりできます。

Citrix では PDF の表示には、Google Chrome ブラウザーまたは Adobe Acrobat Reader をお勧めします。

Delivery Controller で Citrix Studio を使用して、Citrix PDF 印刷を有効にできます。

前提条件:

- Citrix Workspace アプリバージョン 1808 以降。
- Citrix Virtual Apps and Desktops バージョン 7 1808 以降。
- 少なくとも 1 つの PDF ビューアがコンピューターにインストールされている。

PDF 印刷を有効にするには:

1. Delivery Controller で Citrix Studio を使用して、左ペインの [ポリシー] ノードを選択します。ポリシーを作成するか、既存のポリシーを編集することができます。
2. ポリシーの [**PDF** ユニバーサルプリンターの自動作成] ポリシーを [有効] にします。

Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

制限事項:

- PDF の表示と印刷は、Microsoft Edge ブラウザーではサポートされていません。

### Windows Continuum を使用して Windows 10 のタブレットモードを拡張

Windows Continuum は、クライアントデバイスの使用方法に対応する Windows 10 の機能です。Windows 向け Citrix Workspace アプリバージョン 4.10 以降では、モードの動的変更を含む Windows Continuum がサポートされています。

タッチ操作可能なデバイスの場合、キーボードまたはマウスが接続されていないと、Windows 10 VDA はタブレットモードで起動します。キーボード、マウス、またはその両方が接続されている場合は、デスクトップモードで起動します。Surface Pro のような 2 in 1 デバイスの画面やクライアントデバイスでキーボードを接続したり、接続解除したりすると、タブレットモードとデスクトップモードが切り替わります。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[タッチスクリーンデバイス用タブレットモード](#)」を参照してください。

Windows 10 VDA は、セッションに接続または再接続されると、タッチ操作可能なクライアントデバイス上でキーボードまたはマウスを検出します。また、セッション中にキーボードやマウスの接続や接続解除も検出します。この機能は VDA でデフォルトで有効になっています。この機能を無効にするには、Citrix Studio を使用して [タブレットモードの切り替え] ポリシーを変更します。

タブレットモードでは、タッチスクリーンにより適した以下のユーザーインターフェイスが提供されます。

- やや大きめのボタン
- スタート画面や開始したすべてのアプリケーションを全画面で開く
- タスクバーに [戻る] ボタンを表示
- タスクバーからアイコンを削除

デスクトップモードでは、PC でキーボードとマウスを使用するのと同じように操作できる従来のユーザーインターフェイスが提供されます。

注:

Web 向け Workspace は Windows Continuum の機能をサポートしていません。

### Web ブラウザーコンテンツのリダイレクト

Web ブラウザーのコンテンツリダイレクトのために、VDA 側の許可リストに登録された Web ページのレンダリングができません。この機能は、Citrix Workspace アプリを使用してクライアント側の対応するレンダリングエンジンをインスタンス化し、URL から HTTP および HTTPS コンテンツを取得します。

注:

禁止リストを使用することで、Web ページを VDA 側にリダイレクトする（クライアント側ではリダイレクトされない）ように指定できます。

ブラウザーコンテンツリダイレクトは、Internet Explorer ブラウザーだけでなく、Google Chrome ブラウザーでも使用できます。Web ブラウザーのコンテンツをクライアントデバイスにリダイレクトし、Citrix Workspace アプリに埋め込まれた対応する Web ブラウザーを作成します。この機能は、ネットワーク使用量、ページ処理、およびグラフィックレンダリングをエンドポイントにオフロードします。そうすることで、要求の多い Web ページ、特に HTML5 または WebRTC ビデオを組み込んだ Web ページを閲覧する際のユーザーエクスペリエンスが向上します。

詳しくは、「[Web ブラウザーコンテンツのリダイレクト](#)」を参照してください。

### Citrix Analytics

Citrix Workspace アプリには、Citrix Analytics にログをセキュアに送信するための機能があります。この機能が有効になっていると、ログは分析され、Citrix Analytics サーバーに保存されます。Citrix Analytics について詳しくは、[Citrix Analytics](#) ドキュメントを参照してください。

### 相対マウス

相対マウス機能は、ウィンドウまたは画面内の最後のフレームからマウスが移動した距離を判断します。

相対マウスは、マウス移動の距離にピクセルデルタを使用します。たとえば、マウスコントロールを使用してカメラの方向を変更する場合、この機能が役立ちます。またアプリでは、3D オブジェクトやシーンの操作時に画面座標に対するマウスカーソルの位置は関係ないため、カーソルが隠されることがよくあります。

相対マウスのサポートでは、マウスの絶対位置ではなく相対位置を読み取るオプションを提供します。この機能は、マウスの絶対位置ではなく相対位置の入力を必要とするアプリケーションに必要です。

ユーザー単位とセッション単位の両方で相対マウス機能を構成できます。これにより、より細かく機能を制御できます。

#### 注

この機能を適用できるのは、公開デスクトップセッションのみです。

レジストリエディターまたは `default.ica` ファイルを使用してこの機能を構成すると、セッションが終了した後も設定は保持されます。

### レジストリエディターを使用した相対マウスの構成

この機能を構成するには、次のレジストリキーが適用されるよう設定し、セッションを再起動して変更を有効にします：

この機能をセッション単位で使用できるようにする場合：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

この機能をユーザー単位で使用できるようにする場合：

```
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

```
1 - Name: RelativeMouse
2 - Type: REG_SZ
3 - Value: True
```

#### 注：

- レジストリエディターで設定した値は、ICA ファイルの設定よりも優先されます。
- HKEY\_LOCAL\_MACHINE と HKEY\_CURRENT\_USER は同じ値を設定する必要があります。これらの値が異なると、競合が発生する可能性があります。

### デフォルトの `.ica` ファイルを使用した相対マウスの構成

1. `default.ica` ファイルを開きます。このファイルは通常 `C:\inetpub\wwwroot\Citrix\\conf\default.ica` にあります。ここで、`site name` はストアの作成時に指定した名前です。

す。StoreFront ユーザーの場合、default.ica ファイルは通常、`C:\inetpub\wwwroot\Citrix\  
Storename>\App_Data\default.ica`にあります。ここで、storenameはストアの作成時に指定した名前です。

2. WFClient セクションに「RelativeMouse」という名前で新しいキーを追加し、そのデータ値を JSON オブジェクトとして同じ構成に設定します。
3. 必要に応じて値を設定します。
  - true – 相対マウスを有効にする
  - false – 相対マウスを無効にする
4. 変更を保存するには、セッションを再起動します。

注:

レジストリエディターで設定した値は、ICA ファイルの設定よりも優先されます。

### Desktop Viewer から相対マウスを有効にする

1. Citrix Workspace アプリにログオンします。
2. 公開デスクトップセッションを開始します。
3. Desktop Viewer のツールバーで [基本設定] をクリックします。  
[Citrix Workspace - 基本設定] ウィンドウが開きます。
4. [接続] をクリックします。
5. [相対マウスの設定] で [相対マウスを使用する] をオンにします。
6. [適用]、[OK] の順にクリックします。

注:

Desktop Viewer から相対マウスを構成すると、セッション単位のみで適用されます。

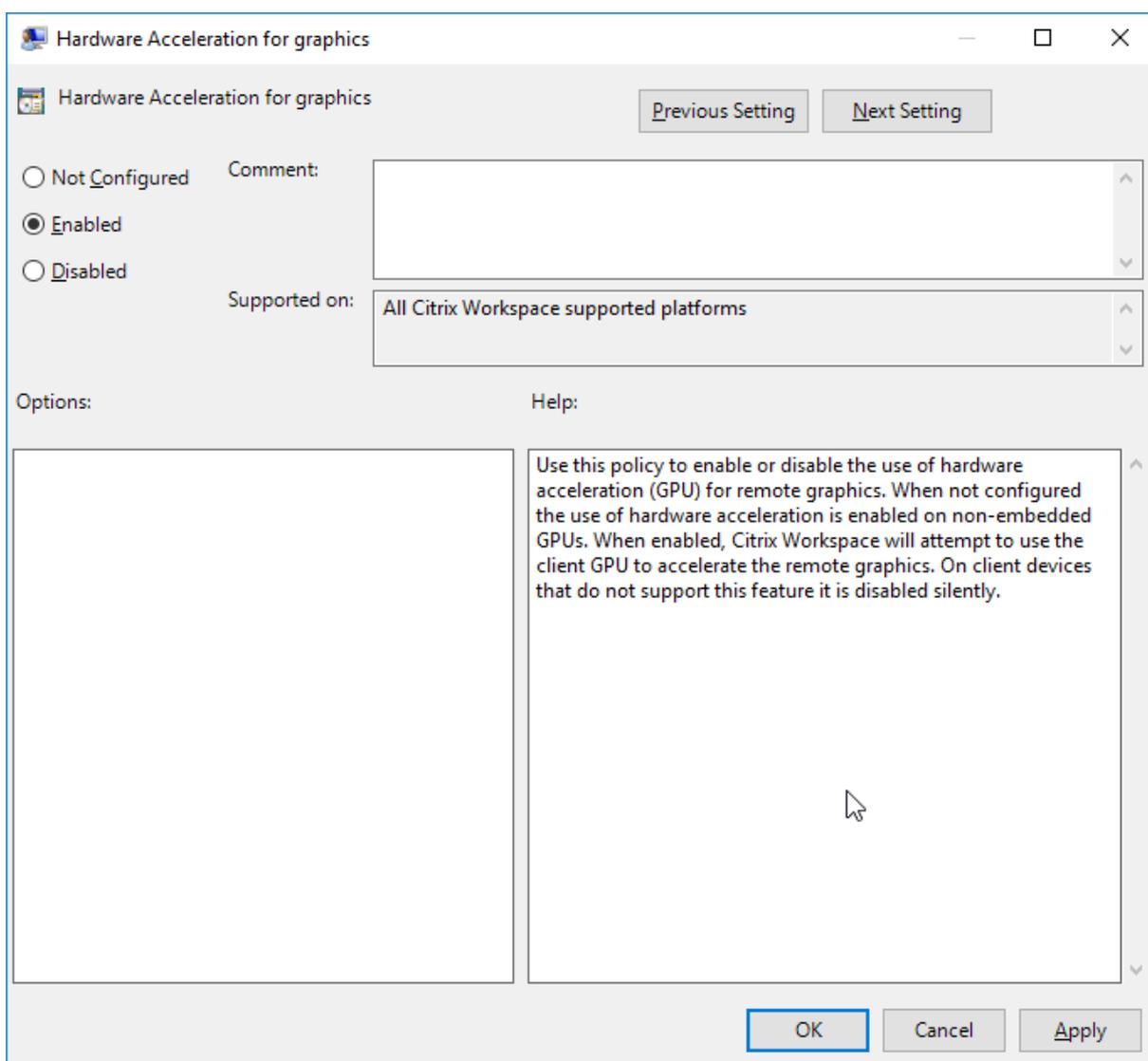
### ハードウェアのデコード

Citrix Workspace アプリ (HDX Engine 14.4 を含む) を使用する場合、クライアントで利用できる場合にはいつでも H.264 デコードに GPU を使用できます。GPU デコードで使用される API レイヤーは DirectX Video Acceleration です。

**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使用してハードウェアのデコードを有効にするには:

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 Workspace]、[ユーザーエクスペリエンス] の順に移動します。

3. [グラフィックのハードウェアアクセラレーション] を選択します。
4. [有効] を選択して、[適用] および [OK] をクリックします。



ポリシーが適用され、ハードウェアアクセラレーションがアクティブな ICA セッションで使用されているかを確認するには、次のレジストリキーを確認します。

レジストリのパス: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`

#### ヒント

**Graphics\_GfxRender\_Decoder** および **Graphics\_GfxRender\_Renderer** は 2 である必要があります。値が 1 の場合、CPU ベースのデコードが使用されています。

ハードウェアデコード機能が使用されている場合、次の制限事項を考慮してください。

- クライアントに GPU が 2 つあり、モニターの 1 つが 2 つ目の GPU でアクティブな場合、CPU デコードが使

用されます。

- Windows Server 2008 R2 が動作する Citrix Virtual Apps 7.x サーバーに接続する場合、ユーザーの Windows デバイスではハードウェアデコードを使用しないことをお勧めします。これが有効な場合、文字列を強調表示する場合のパフォーマンスの低下やちらつきの問題が発生します。

### マイク入力

Citrix Workspace アプリは、クライアント側の複数のマイク入力をサポートします。ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

- ソフトフォンでの通話や Web 会議などのリアルタイムのアクティビティ。
- ホストされている録音アプリケーション（ディクテーションプログラムなど）の使用。
- 録画と録音。

Citrix Workspace アプリのユーザーは、コネクションセンターを使用して、デバイスに付属しているマイクを使用するかどうか選択することができます。Citrix Virtual Apps and Desktops ユーザーも、ビューアの [基本設定] ダイアログボックスを使用してマイクおよび Web カメラを無効にできます。

### クライアントドライブマッピング

クライアントドライブマッピングで、データをホストとクライアントの間でストリームとして転送できます。ファイル転送は、ネットワークスループットの状態の変化に適應できます。また、使用可能な追加の帯域幅を使用して、データ転送速度を高めることもできます。

この機能は、デフォルトで有効になります。

この機能を無効にするには、次のレジストリキーを設定し、サーバーを再起動します：

パス：`HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`

名前：`DisableFullStreamWrite`

種類：`REG_DWORD`

値：

`0x01` - 無効、

`0` または削除 - 有効

### マルチモニターサポート

Windows 向け Citrix Workspace アプリで最大 8 台のモニターを使用できます。

マルチモニター環境では、各モニターの製造元により解像度が異なる場合があります。また、セッション中にモニターの解像度や向きが変更されることもあります。

セッションを複数のモニター上に表示する場合、以下の 2 つのモードがあります。

- 全画面モード。セッションはマルチモニター全体に表示されます。ローカルでの場合と同様に、アプリケーションウィンドウが表示領域全体に最大化されます。

**Citrix Virtual Apps and Desktops:** Desktop Viewer ウィンドウをマルチモニターのいずれかの矩形表示領域内に表示するには、隣接するモニターにかかるようにウィンドウのサイズを変更して [最大化] をクリックします。

- ウィンドウモード。単一のモニターがセッション用に使用されます。アプリケーションウィンドウは個々のモニター上に最大表示されません。

**Citrix Virtual Apps and Desktops:** 同じ割り当て (デスクトップグループ) に含まれるデスクトップを続けて起動すると、ウィンドウ設定が保持され、デスクトップが同じモニターに表示されます。矩形配置構成のマルチモニター環境では、複数の仮想デスクトップを 1 つのデバイス上で表示できます。デバイスのプライマリモニターを Citrix Virtual Apps and Desktops セッションで使用する場合は、セッションでもそのモニターがプライマリモニターになります。そうでない場合は、セッション内の最も小さい番号のモニターがプライマリモニターになります。

マルチモニター環境をサポートするには、次の条件を満たしている必要があります。

- ユーザーデバイスの構成でマルチモニターがサポートされている。
- オペレーティングシステムが各モニターを検出できる。Windows プラットフォームでモニターを検出できるかどうかは、[設定] > [システム] に移動し、[ディスプレイ] をクリックして、各モニターが別々に表示されていることを確認します。
- モニターが検出された後は、次の作業を行います。
  - **Citrix Virtual Desktops:** Citrix マシンポリシーの [表示メモリの制限] 設定を使用して、グラフィックメモリの制限を構成します。
  - **Citrix Virtual Apps:** インストールした Citrix Virtual Apps サーバーのバージョンに応じて、以下の操作を行います:
    - \* Citrix ポリシーの [表示メモリの制限] 設定を使用して、グラフィックメモリの制限を構成します。
    - \* Citrix Virtual Apps サーバー用 Citrix 管理コンソールの左ペインでサーバーファームを選択し、タスクペインで [サーバーファームのプロパティの変更]、[すべてのプロパティの変更]、[サーバーのデフォルト設定]、[HDX Broadcast]、[表示設定] の順に選択します (または [サーバーファームのプロパティの変更]、[すべてのプロパティの変更]、[サーバーのデフォルト設定]、[ICA]、[表示設定] の順に選択します)。そして、[各セッションのグラフィックで使用する最大メモリ] を設定します。

この値を、グラフィックメモリを提供するのに十分なサイズに設定します (単位はキロバイト)。このボックスの値が必要なサイズに満たないと、公開リソースが一部のモニター上でしか表示されません。

**Citrix Virtual Desktops** をデュアルモニターで使用する:

1. Desktop Viewer を選択し、下向き矢印をクリックします。
2. [ウィンドウ] を選択します。
3. Citrix Virtual Desktops の画面を 2 つのモニターの間にドラッグします。各モニターに画面の約半分が表示されていることを確認してください。

#### 4. Citrix Virtual Desktops のツールバーで、[フルスクリーン] を選択します。

画面が両方のモニターに拡張されます。

Citrix Virtual Apps and Desktops のセッションのグラフィックメモリ要件の計算については、Knowledge Center の[CTX115637](#)を参照してください。

### プリンター

ユーザーがプリンター設定を上書きするには

1. ユーザーデバイス上で、アプリケーションの [印刷] ダイアログボックスを開き、[プロパティ] をクリックします。
2. [クライアント設定] タブで [高度な最適化] をクリックし、[イメージ圧縮] および [イメージおよびフォント キャッシュ] オプションの設定を変更します。

### スクリーンキーボードの制御

Windows タブレットから仮想アプリケーションおよびデスクトップへのタッチ操作によるアクセスを有効にするため、テキスト入力フィールドがアクティブになったり、デバイスがテントまたはタブレットモードになったりすると、Citrix Workspace アプリによって自動的にスクリーンキーボードが表示されます。

一部のデバイスおよび一部の環境下では、Citrix Workspace アプリがデバイスのモードを正確に検出できず、必要時にスクリーンキーボードが表示されないことがあります。

変換可能なデバイスを使っている場合にスクリーンキーボードの表示を抑制するには、REG\_DWORD 値の `DisableKeyboardPopup` を `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Mod` で作成し、値を 1 に設定します。

注:

x64 マシンでは、`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Adv` に値を作成します。

キーは以下のような異なる 3 種のモードに設定できます。

- 自動: `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0`
- 常にポップアップ (スクリーンキーボード): `AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0`
- ポップアップしない (スクリーンキーボード): `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1`

### キーボードショートカット

Citrix Workspace アプリで特定の機能を実行するキーの組み合わせを構成できます。キーボードショートカットのポリシーが有効な場合、Citrix ショートカットキーのマッピング、Windows ショートカットキーの動作、およびセッションでのキーボードの種類を指定できます。

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] > [ユーザーエクスペリエンス] の順に移動します。
3. キーボードショートカットポリシーを選択します。
4. [有効] と目的のオプションを選択します。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

### Citrix Workspace アプリの 32 ビットカラーアイコンのサポート:

Citrix Workspace アプリでは 32 ビット High Color アイコンがサポートされ、コネクションセンターに表示されるアプリケーションのアイコンに適した色数が自動的に選択されます。シームレスアプリケーションを実行しているときに [スタート] メニューとタスクバーに表示されるアプリケーションのアイコンも、同様に処理されます。

#### 注意

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

優先する深さを設定するには、`TWIDesiredIconColor` という文字列レジストリキーを `HKEY\\_LOCAL\\_MACHINE\\SOFTWARE\\Wow6432Node\\Citrix\\ICA Client\\Engine\\Lockdown Profiles\\All Regions\\Preferences` に追加して、必要な値に設定します。定義できるアイコンの色数は、4、8、16、24、および 32 ビット/ピクセルです。ネットワーク接続が低速な場合は、ユーザーはより少ない色数を選択できます。

## Desktop Viewer

企業組織にはそれぞれ異なるニーズがあります。ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーによって、そして企業ニーズが展開するにつれて変化する可能性があります。ユーザーが仮想デスクトップに接続したり接続を構成したりするときの手順は、管理者による Windows 向け Citrix Workspace アプリのセットアップ方法によって異なります。

ユーザーが仮想デスクトップを操作する必要がある場合は、**Desktop Viewer** を使用します。ユーザーの仮想デスクトップには公開仮想デスクトップを使用でき、共有または専用デスクトップのいずれでも可能です。このアクセスシナリオでは、**Desktop Viewer** ツールバー機能により、ユーザーが仮想デスクトップをローカルデスクトップ上のウィンドウ内に開いて、必要に応じて仮想デスクトップの表示領域や表示サイズを変更できます。ユーザーは必要に応じて設定を変更でき、同じユーザーデバイス上で複数の Citrix Virtual Apps and Desktops 接続を使用して複数の仮想デスクトップを実行できます。

#### 注:

仮想デスクトップの解像度を変更する場合は、Citrix Workspace アプリを使用します。Windows コントロ

ールパネルで解像度を変更することはできません。

### Desktop Viewer でのキーボード入力

Desktop Viewer セッションでは、**Windows** ロゴ + L キーはローカルコンピューターに送信されます。

Ctrl+Alt+Del キーは、ローカルコンピューターに送信されます。

通常、Microsoft 社のユーザー補助機能である固定キー、フィルターキー、および切り替えキー機能を有効にするキーはローカルコンピューターに送信されます。

Desktop Viewer のユーザー補助機能として、Ctrl + Alt + Break キーを押すと、ポップアップウィンドウで **Desktop Viewer** ツールバーが開きます。

Ctrl + Esc キーは、リモートの仮想デスクトップに送信されます。

#### 注:

デフォルトでは、Desktop Viewer を最大化した場合は Alt + Tab キーを押すとセッション内のウィンドウ間でフォーカスが切り替わります。Desktop Viewer をウィンドウ内に表示している場合は、Alt + Tab キーを押すとセッション外のウィンドウ間でフォーカスが切り替わります。

ホットキーシーケンスは、Citrix により設計されたキーの組み合わせです。たとえば、Ctrl + F1 シーケンスは Ctrl + Alt + Del キーを再現し、Shift + F2 はアプリケーションの全画面モードとウィンドウモードを切り替えます。Desktop Viewer で表示されている仮想デスクトップ（つまり、Citrix Virtual Apps and Desktops セッション）ではホットキーシーケンスを使用できませんが、公開アプリケーション（つまり、Citrix Virtual Apps and Desktops セッション）ではこれを使用できます。

### 仮想デスクトップ

仮想デスクトップセッション内から同じ仮想デスクトップに接続することはできません。これを行うと、既存のデスクトップセッションが切断されます。そのため、Citrix では次のことをお勧めします：

- 管理者は、仮想デスクトップ上のクライアントが、同じデスクトップを公開しているサイトに接続するように構成しない。
- ユーザーは、同じデスクトップをホストしているサイトを参照しない（自動的に既存のセッションに再接続するようサイトが構成されている場合）。
- ユーザーは、同じデスクトップをホストしているサイトを参照したりそのデスクトップを起動したりしない。

仮想デスクトップとして動作するコンピューターにローカルでログオンするユーザーは、そのデスクトップへの接続がブロックされます。

ユーザーが仮想デスクトップ内から（Citrix Virtual Apps で公開された）仮想アプリケーションに接続し、別の管理者が Citrix Virtual Apps を管理している環境では、ローカルのデバイスが仮想デスクトップセッションおよび公開アプリケーションセッションで同様にマップされるように、Citrix Virtual Apps 管理者と共同してデバイスマッピングを定義することをお勧めします。仮想デスクトップセッションではローカルドライブがネットワークドライブと

して表示されるため、Citrix Virtual Apps 管理者がドライブマッピングポリシーでネットワークドライブ（リモートドライブ）のマッピングを許可する必要があります。

### 状態インジケータのタイムアウト

ユーザーがセッションを起動しているときに状態インジケータが表示される時間を変更できます。

タイムアウト期間を変更するには、次の手順を実行します：

1. レジストリエディターを起動します。
2. 次のパスに移動します：
  - 64 ビットの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine`
  - 32ビットの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\`
3. 次のようにレジストリキーを作成します：
  - 種類：REG\_DWORD
  - 値の名前：`SI_INACTIVE_MS`
  - 値：状態インジケータをすぐに非表示にしたい場合は、4 に設定します。

このキーを構成すると、状態インジケータが頻繁に、表示されてから非表示になることがあります。これは、正常な動作です。状態インジケータが表示されないようにするには、次の手順を実行します：

1. レジストリエディターを起動します。
2. 次のパスに移動します：
  - 64 ビットの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\`
  - 32ビットの場合：`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\`
3. 次のようにレジストリキーを作成します：
  - 種類：REG\_DWORD
  - 値の名前：`NotificationDelay`
  - 値：ミリ秒単位の任意の値（たとえば、120000）

### Workspace セッションの無操作状態によるタイムアウト

管理者は、無操作状態によるタイムアウト値を構成して、ユーザーが Citrix Workspace アプリセッションから自動的にサインアウトされるまでのアイドル時間を指定できます。指定された時間内にマウス、キーボード、またはタッチによるアクティビティがない場合は、自動的に Workspace からサインアウトされます。無操作状態によるタイムアウトは、すでに実行中の Citrix Virtual Apps and Desktops セッションまたは Citrix StoreFront ストアには影響しません。

無操作状態によるタイムアウト値は、最小1分から最大1,440分まで設定できます。デフォルトでは、無操作状態によるタイムアウトは構成されていません。管理者は、PowerShell モジュールを使用して `inactivityTimeoutInMinutes`

プロパティを構成できます。Citrix Workspace 構成のための PowerShell モジュールをダウンロードするには、[こちら](#)をクリックしてください。

エンドユーザーエクスペリエンスは次のとおりです：

- サインアウトの 3 分前にセッションウィンドウに通知が表示され、サインインしたままにするか、サインアウトするかを選択できます。
- この通知は、設定された無操作状態によるタイムアウト値が 5 分以上の場合にのみ表示されます。
- ユーザーは [サインイン状態を維持] をクリックして通知を閉じ、アプリの使用を続行できます。その場合、無通信タイマーは構成された値にリセットされます。または、[サインアウト] をクリックして、現在のストアのセッションを終了することもできます。

注：

管理者は、Workspace (クラウド) セッションに対してのみ無操作状態によるタイムアウトを構成できます。

### カスタマーエクスペリエンス向上プログラム (CEIP)

| 収集データ        | 説明                                                                                                                                      | 使用目的                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| 構成および使用状況データ | Citrix カスタマーエクスペリエンス向上プログラム (CEIP) では、Windows 向け Citrix Workspace アプリの構成および使用に関するデータが収集され、そのデータが Citrix と Google Analytics に自動的に送信されます。 | このデータは、Citrix Workspace アプリの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。 |

#### 追加情報

Citrix は、お客様のデータを Citrix との契約条件に従って取り扱い、[Citrix Trust Center](#)で利用できる [Citrix Services Security Exhibit](#) において指定されているとおりにお客様のデータを保護します。

また、CEIP の一環として、Google Analytics を使用して Citrix Workspace アプリから特定のデータを収集します。[Google Analytics のために収集されたデータ](#)の Google の取り扱い方法について確認してください。

次の方法で、Citrix および Google Analytics への CEIP データの送信をオフにすることができます (ただし、以下の 2 番目の表で \* が付けられた 2 つデータ要素は除きます)：

- システムトレイの Citrix Workspace アプリアイコンを右クリックします。
- [高度な設定] を選択します。  
[高度な設定] ダイアログボックスが表示されます。
- [データ収集] を選択します。

4. [いいえ] を選択して CEIP を無効にするか、参加を見送ります。
5. [保存] をクリックします。

または、次のレジストリエントリに移動し、推奨されている値を設定します：

パス： `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

キー： `Enable_CEIP`

値： `False`

注：

データ収集ダイアログで **[No Thanks]** を選択するか、`Enable_CEIP` キーを `False` に設定したあと、Google Analytics によって収集された最後の 2 つの CEIP データ要素（オペレーティングシステムのバージョンと Workspace アプリのバージョン）の送信を無効にする場合は、次のレジストリエントリに移動し、推奨されている値を設定します：

パス： `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

キー： `DisableHeartbeat`

値： `True`

Citrix が収集する特定の CEIP データ要素は次のとおりです：

|                         |                    |                   |         |
|-------------------------|--------------------|-------------------|---------|
| オペレーティングシステムバージョン       | Workspace アプリバージョン | 接続されている外部デバイス     | 画面解像度   |
| Flash のバージョン            | Desktop Lock 構成    | タッチ対応             | 認証構成    |
| セッションの起動方法              | グラフィック構成           | Desktop Viewer 構成 | 印刷      |
| 接続エラー                   | 起動時間               | Workspace アプリの言語  | VDA 情報  |
| SSON の状態                | インストーラーの状態         | インストール時間          | 接続プロトコル |
| Internet Explorer バージョン |                    |                   |         |

Google Analytics が収集する特定の CEIP データ要素は次のとおりです：

|                     |                      |         |                  |
|---------------------|----------------------|---------|------------------|
| オペレーティングシステムバージョン * | Workspace アプリバージョン * | 認証構成    | Workspace アプリの言語 |
| セッションの起動方法          | 接続エラー                | 接続プロトコル | VDA 情報           |

| インストーラー構成 | インストーラーの状態          | クライアントのキーボード<br>ドレアウト | ストア構成                |
|-----------|---------------------|-----------------------|----------------------|
| 自動更新の設定   | コネクションセンターの<br>使用状況 | アプリ保護構成               | オフラインバナーが表示<br>される理由 |

## 地域の設定

Citrix Workspace アプリは、ブラウザーまたはエンドポイントデバイスのロケールに基づいて、日付、時刻、および番号を表示します。

Citrix Workspace アプリ 2106 リリース以降では、地域設定を使用して地域の日付、時刻、および数値形式をカスタマイズできます。これらの設定で行われた変更は、個々のユーザー別に保存され、すべてのデバイスに適用されます。

### 注:

このオプションはクラウド展開でのみ使用できます。

詳しくは、「[地域の設定](#)」を参照してください。

## 認証

### October 22, 2021

環境のセキュリティを最大限に高めるには、Citrix Workspace アプリと公開リソースの間の接続を保護する必要があります。Citrix Workspace アプリで、ドメインパススルー、スマートカード、Kerberos パススルーなど、さまざまな種類の認証を構成できます。

### ドメインパススルー認証

シングルサインオンを使用すると、ドメインに対して認証することで、Citrix Virtual Apps and Desktops を再認証する必要なく使用できます。

Citrix Workspace アプリにログオンすると、スタートメニューの設定を含め、列挙されたアプリケーションやデスクトップとともに資格情報が StoreFront にパススルーされます。シングルサインオンの構成後、資格情報を複数回入力することなく、Citrix Workspace アプリにログオンして Citrix Virtual Apps and Desktops セッションを開始できます。

すべての Web ブラウザーで、グループポリシーオブジェクト (GPO) 管理用テンプレートを使用してシングルサインオンを構成する必要があります。グループポリシーオブジェクト管理用テンプレートを使用したシングルサインオンの構成について詳しくは、「[Citrix Gateway でのシングルサインオンの構成](#)」を参照してください。

新規インストールまたはアップグレードの両方で次のいずれかのオプションを使用して、シングルサインオンを構成できます：

- コマンドラインインターフェイス
- GUI

#### 新規インストール中のシングルサインオンの構成

新規インストールでシングルサインオンを構成するには、次の手順を実行します：

1. StoreFront で構成します。
2. Delivery Controller で XML 信頼サービスを構成します。
3. Internet Explorer の設定を変更します。
4. Citrix Workspace アプリのインストールでシングルサインオンを構成します。

#### StoreFront でのシングルサインオンの構成

シングルサインオンを使用すると、ドメインに対して認証することで、そのドメインで提供されている Citrix Virtual Apps and Desktops を再認証する必要なく使用できます。Storebrowse ユーティリティでストアを追加すると、スタートメニューの設定を含め、列挙されたアプリケーションやデスクトップとともに資格情報が Citrix Gateway サーバーにパススルーされます。シングルサインオンの構成後、資格情報を何度も入力しなくても、ストアを追加したり、アプリやデスクトップを列挙したり、必要なリソースを起動することができます。

Citrix Virtual Apps and Desktops 展開によって、StoreFront で管理コンソールを使用してシングルサインオン認証を構成できます。

以下の表で異なる使用例とそれぞれの構成を参照します：

| 使用例                     | 構成の詳細                                                                        | 追加情報                                                                                                  |
|-------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| StoreFront での構成         | Citrix Studio を起動して、[ストア] > [認証方法の管理] に移動して [ドメインパススルー] を有効にします。             | Citrix Workspace アプリでシングルサインオンが構成されていない場合、認証方法は自動的に [ドメインパススルー] から [ユーザー名とパスワード] に切り替えられます (利用可能な場合)。 |
| Web 向け Workspace が必要な場合 | [ストア] > [ <b>Workspace for Websites</b> ] > [認証方法の管理] で [ドメインパススルー] を有効にします。 | Citrix Workspace アプリでシングルサインオンが構成されていない場合、認証方法は自動的に [ドメインパススルー] から [ユーザー名とパスワード] に切り替えられます (利用可能な場合)。 |

## Citrix Gateway でのシングルサインオンの構成

GPO 管理用テンプレートを使用して Citrix Gateway でシングルサインオンを有効にします。

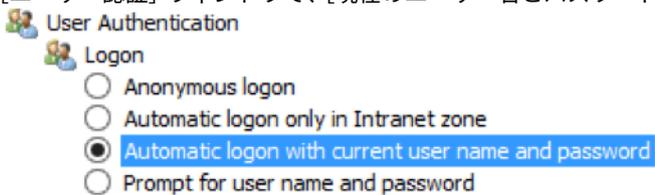
1. `gpedit.msc` を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. [コンピューターの構成] ノードで、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザー認証] の順に移動します。
3. **Citrix Gateway** のシングルサインオンポリシーを選択します。
4. [有効] をクリックします。
5. [適用]、[OK] の順にクリックします。
6. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

## Delivery Controller で XML 信頼サービスを構成

Citrix Virtual Apps and Desktops の Delivery Controller で管理者として次の PowerShell コマンドを実行します：

```
asnps Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

## Internet Explorer 設定の変更

1. Internet Explorer を使用して信頼済みサイトの一覧に StoreFront サーバーを追加します。これを行うには、次の操作を行います。
  - a) [コントロール] パネルで [インターネットオプション] を起動します。
  - b) [セキュリティ] > [ローカルイントラネット] を選択し、[サイト] をクリックします。  
[ローカルイントラネット] ウィンドウが開きます。
  - c) [詳細設定] を選択します。
  - d) 適切な HTTP または HTTPS プロトコルを使用して、StoreFront の FQDN の URL を追加します。
  - e) [適用]、[OK] の順にクリックします。
2. **Internet Explorer** で [ユーザー認証] の設定を変更します。これを行うには、次の操作を行います。
  - a) [コントロール] パネルで [インターネットオプション] を起動します。
  - b) [セキュリティ] タブ > [信頼済みサイト] を選択します。
  - c) [レベルのカスタマイズ] をクリックします。[セキュリティ設定 - 信頼されたゾーン] ウィンドウが開きます。
  - d) [ユーザー認証] ウィンドウで、[現在のユーザー名とパスワードで自動的にログオンする] を選択します。

User Authentication

Logon

    - Anonymous logon
    - Automatic logon only in Intranet zone
    - Automatic logon with current user name and password
    - Prompt for user name and password
  - e) [適用]、[OK] の順にクリックします。

コマンドラインインターフェイスを使用したシングルサインオンの構成

`/includeSSON`スイッチを使用して Citrix Workspace アプリをインストールし、再起動して変更を有効にします。

注:

Windows 向け Citrix Workspace アプリがシングルサインオンコンポーネントなしでインストールされている場合、`/includeSSON`スイッチを使用して最新バージョンにアップグレードすることはできません。

グラフィカルユーザーインターフェイスを使用したシングルサインオンの構成

1. Citrix Workspace アプリインストールファイル (`CitrixWorkspaceApp.exe`) を検索します。
2. `CitrixWorkspaceApp.exe`をダブルクリックしてインストーラーを起動します。
3. [シングルサインオンを有効化] ウィザードで、[シングルサインオンを有効化] オプションを選択します。
4. [次へ] をクリックし、ウィザードの指示に従ってインストールを完了します。

Citrix Workspace アプリを使用してユーザー資格情報を指定することなく既存のストア（または構成した新しいストア）にログオンできるようになりました。

### Web 向け Workspace でのシングルサインオンの構成

グループポリシーオブジェクト管理用テンプレートを使用して、Web 向け Workspace のシングルサインオンを構成できます。

1. `gpedit.msc` を実行して、Web 向け Workspace の GPO 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] > [ユーザー認証] の順に移動します。
3. [ローカルユーザー名とパスワード] ポリシーを選択して [有効] に設定します。
4. [パススルー認証を有効にします] をクリックします。このオプションを使用すると、Web 向け Workspace はリモートサーバーでの認証にログイン資格情報を使用できます。
5. [すべての ICA 接続にパススルー認証を許可します] をクリックします。このオプションは、すべての認証制限を省略し、すべての接続で資格情報のパススルーを許可します。
6. [適用]、[OK] の順にクリックします。
7. Web 向け Workspace のセッションを再起動して、この変更を適用します。

シングルサインオンが有効になっていることを確認するには、タスクマネージャを起動し、`ssonsvr.exe` プロセスが実行中であることを確認します。

### Active Directory を使用したシングルサインオンの構成

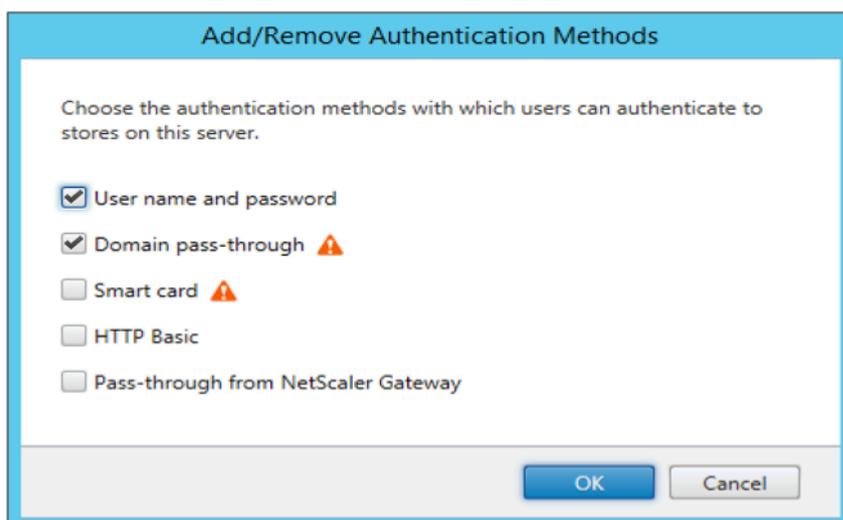
次の手順を完了し、Active Directory グループポリシーを使用して Citrix Workspace アプリでパススルー認証を構成します。このシナリオでは、Microsoft System Center Configuration Manager などのエンタープライズソフトウェア展開ツールを使用することなくシングルサインオン認証を構成できます。

1. Citrix Workspace アプリインストールファイル (**CitrixWorkspaceApp.exe**) をダウンロードして適切なネットワーク共有に配置します。Citrix Workspace アプリをインストールする対象マシンからアクセス可能であることが必要です。
2. [Windows 向け Citrix Workspace アプリのダウンロード](#) ページから **CheckAndDeployWorkspacePerMachineStartupScript.bat** テンプレートを入手します。
3. **CitrixWorkspaceApp.exe** の場所およびバージョンが反映されるようコンテンツを編集します。
4. **Active Directory** のグループポリシー管理コンソールで **CheckAndDeployWorkspacePerMachineStartupScript.bat** をスタートアップスクリプトとして入力します。スタートアップスクリプトの展開について詳しくは、「[Active Directory](#)」のセクションを参照してください。
5. [コンピューターの構成] ノードで [管理用テンプレート] > [テンプレートの追加と削除] に移動して **receiver.adml** ファイルを追加します。
6. **receiver.adml** テンプレートの追加後、[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**] > [ユーザー認証] に移動します。テンプレートファイルの追加について詳しくは、「[グループポリシーオブジェクト管理用テンプレート](#)」を参照してください。
7. [ローカルユーザー名とパスワード] ポリシーを選択して [有効] に設定します。
8. [パススルー認証を有効にします] チェックボックスをオンにして [適用] を選択します。
9. 変更を保存するには、マシンを再起動します。

### StoreFront でのシングルサインオンの構成

#### StoreFront の構成

**Citrix Studio** を StoreFront サーバーで開いて [認証] > [認証方法の追加と削除] の順に選択します。[ドメインパススルー] を選択します。



### 認証トークン

認証トークンは暗号化されローカルディスクに保存されるため、システムやセッションの再起動時に資格情報を再入力する必要はありません。Citrix Workspace アプリは、ローカルディスクへの認証トークンの保存を無効にするオプションを提供します。

セキュリティを強化するために、認証トークンストレージを構成するためのグループポリシーオブジェクト (GPO) ポリシーが提供されるようになりました。

#### 注:

この構成は、クラウド展開でのみ適用されます。

グループポリシーオブジェクト (**GPO**) ポリシーを使用して認証トークンの保存を無効にするには:

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] > [SelfService] に移動します。
3. 認証トークンを保存しますポリシーで、次のいずれかを選択します:
  - 有効: 認証トークンがディスクに保存されていることを示します。これはデフォルトのオプションです。
  - 無効: 認証トークンがディスクに保存されていないことを示します。システムまたはセッションを再起動するときに、資格情報を再入力する必要があります。
4. [適用]、[OK] の順にクリックします。

バージョン 2106 以降、Citrix Workspace アプリは、ローカルディスクへの認証トークンの保存を無効にする追加のオプションを提供します。既存の GPO 構成に加えて、Global App Configuration Service を使用してローカルディスクへの認証トークンの保存を無効にすることもできます。

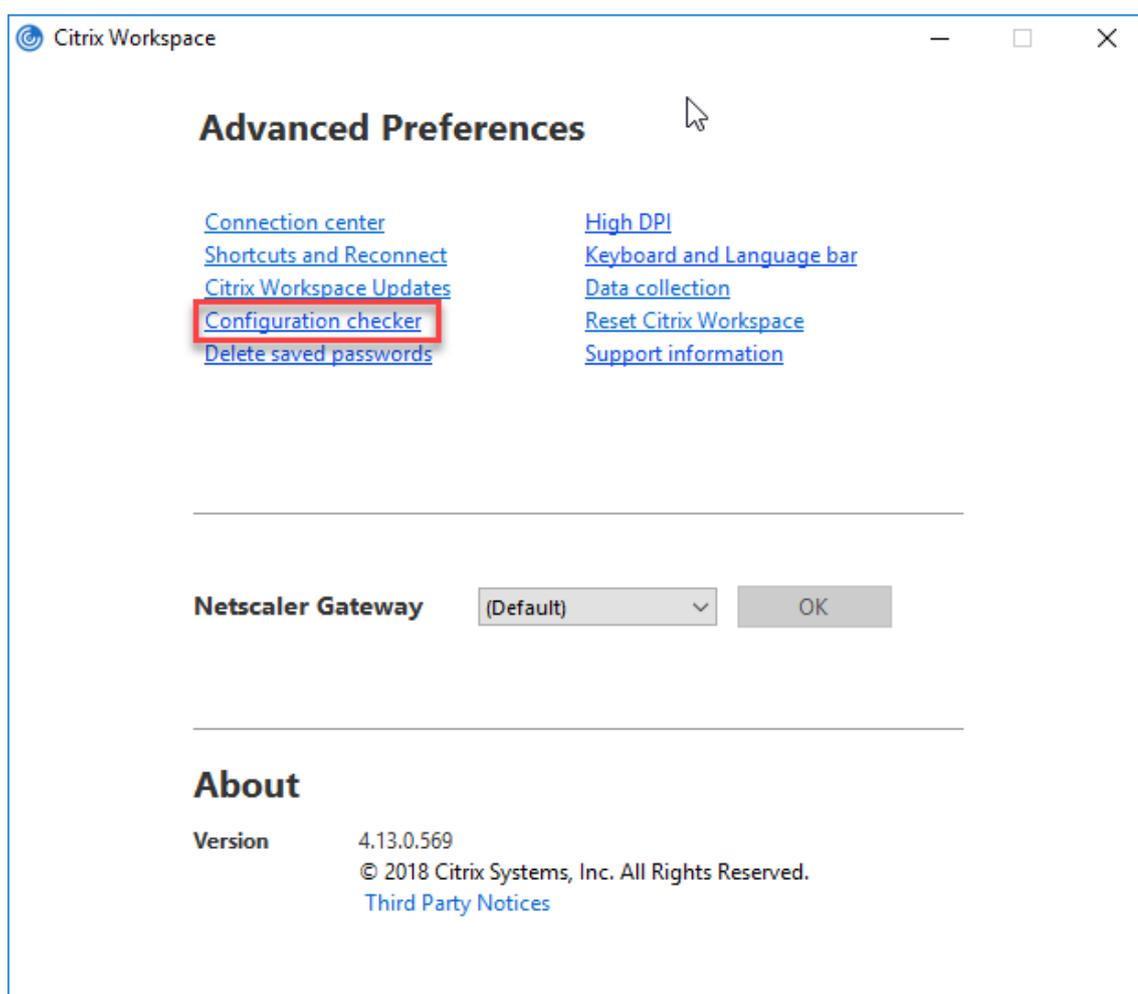
Global App Configuration Service で、`Store Authentication Tokens`属性を`False`に設定します。

詳しくは、「[Global App Configuration Service](#)」のドキュメントを参照してください。

### 構成チェッカー

構成チェッカーで、シングルサインオンが正しく構成されていることを確認するためのテストを実行できます。テストはシングルサインオン構成の各チェックポイントに対して実行され、構成結果を表示します。

1. 通知領域で Citrix Workspace アプリアイコンを右クリックし、[高度な設定] をクリックします。  
[高度な設定] ダイアログボックスが表示されます。
2. [構成チェッカー] をクリックします。  
[Citrix 構成チェッカー] ウィンドウが開きます。



3. [選択] ペインで **[SSONChecker]** チェックボックスをオンにします。
4. [実行] をクリックします。テストの状態を示す進捗状況バーが表示されます。

[構成チェッカー] ウィンドウには次の列があります：

1. 状態：特定のチェックポイントでのテスト結果が表示されます。
  - 緑色のチェックマークは、チェックポイントが適切に構成されていることを示します。
  - 青色の I は、チェックポイントに関する情報を示します。
  - 赤色の X は、チェックポイントが適切に構成されていないことを示します。
2. **Provider**：テストが実行されているモジュールの名前が表示されます。この場合は、シングルサインオンになります。
3. **Suite**：テストのカテゴリを示します。例：「インストール」。
4. テスト：実行中のテストの名前を示します。
5. **Details**：テスト結果にかかわらず、そのテストの詳細が表示されます。

各チェックポイントおよび対応する結果の詳細を確認することができます。

以下のテストが実施されます：

1. シングルサインオンとともにインストール済み。
2. ログオン資格情報のキャプチャ。
3. ネットワークプロバイダーの登録： ネットワークプロバイダーの登録のテスト結果で緑色のチェックマークが表示されるのは、ネットワークプロバイダーの一覧で「Citrix Single Sign-on」が先頭に設定されている場合のみです。「Citrix Single Sign-On」が一覧の先頭以外の場所に表示されている場合、ネットワークプロバイダーの登録のテスト結果では青色の | と詳細情報が表示されます。
4. シングルサインオンプロセスが実行されている。
5. グループポリシー： デフォルトでは、このポリシーはクライアントで構成されます。
6. Internet Explorer のセキュリティゾーンの設定： [インターネットオプション] のセキュリティゾーンの一覧に Store/XenApp サービスの URL を追加していることを確認してください。  
セキュリティゾーンをグループポリシー経由で構成しており、そのポリシーを変更した場合、変更を有効にしてテストの正確な状態が表示されるようにするために、[高度な設定] ウィンドウを開き直す必要があります。
7. StoreFront の認証方法。

注：

- Web 向け Workspace にユーザーがアクセスしている場合、テスト結果は不正確になります。
- Citrix Workspace アプリで複数のストアを構成している場合、認証方法テストはすべての構成済みストアに対して実行されます。
- テスト結果はレポートとして保存できます。デフォルトのレポート形式は.txt です。

[高度な設定] ウィンドウの [構成チェッカー] オプションを非表示にする

1. `gpedit.msc` を実行して、Citrix Workspace アプリの GPO 管理用テンプレートを開きます。
2. グループポリシーエディターで、[Citrix コンポーネント] > [Citrix Workspace] > [Self Service] > [DisableConfigChecker] の順に開きます。
3. [有効] を選択すると、[高度な設定] ウィンドウで [構成チェッカー] オプションが表示されなくなります。
4. [適用]、[OK] の順にクリックします。
5. `gpupdate /force` コマンドを実行します。

制限事項：

構成チェッカーの対象チェックポイントに、Citrix Virtual Apps and Desktops サーバー上の [Citrix XML Service への要求を信頼する] の構成は含まれません。

ビーコンテスト

Citrix Workspace アプリを使用して、構成チェッカーユーティリティの一部であるビーコンチェッカーでビーコンテストを実行できます。ビーコンテストは、ビーコン (ping.citrix.com) が到達可能かどうかを確認します。この診断テストは、リソースの列挙が遅くなる理由として考えられる原因から、ビーコンが使用できないという可能性を排除

するのに役立ちます。テストを実行するには、システムトレイの Citrix Workspace アプリを右クリックし、[高度な設定] > [構成チェッカー] を選択します。テスト一覧からビーコンチェッカーを選択して [実行] をクリックします。

テスト結果は、次のいずれかになります：

- Reachable - Citrix Workspace アプリが正常にビーコンに通信できます。
- Not reachable - Citrix Workspace アプリはビーコンに通信できません。
- Partially reachable - Citrix Workspace アプリは、断続的にビーコンに通信できます。

注：

- テスト結果は、Web 向け Workspace では適用されません。
- テスト結果はレポートとして保存できます。デフォルトのレポート形式は.txt です。

### Kerberos を使用したドメインパススルー認証

このトピックの内容は、Windows 向け Citrix Workspace アプリと StoreFront、Citrix Virtual Apps and Desktops 間の接続にのみ適用されます。

Citrix Workspace アプリでは、スマートカードを使用する展開環境での Kerberos によるドメインパススルー認証がサポートされます。Kerberos とは、統合 Windows 認証 (IWA) に含まれる認証方法の 1 つです。

これを有効にすると、認証時に Citrix Workspace アプリのパスワードが使用されません。このため、トロイの木馬型の攻撃でユーザーデバイス上のパスワードが漏えいすることを避けることができます。ユーザーは、任意の認証方法を使用してログオンし、公開リソースにアクセスできます。たとえば、指紋リーダーなどの生体認証システムなどです。

スマートカード認証が構成された Citrix Workspace アプリ、StoreFront、Citrix Virtual Apps and Desktops でスマートカードを使用してログオンすると、Citrix Workspace アプリは以下を実行します：

1. シングルサインオン中にスマートカード PIN を取得します。
2. IWA (Kerberos) を使用して StoreFront へのユーザー認証を行います。すると、使用可能な Citrix Virtual Apps and Desktops の情報を StoreFront が Workspace アプリに提供します。

注

追加の PIN プロンプトが表示されるのを回避するために Kerberos を有効にします。Citrix Workspace アプリで Kerberos 認証を使用しない場合、StoreFront への認証にはスマートカード資格情報が使用されます。

3. HDX エンジン (従来「ICA クライアント」と呼ばれていたもの) がスマートカードの PIN を VDA に渡します。これにより、ユーザーが Citrix Workspace アプリセッションにログオンできます。Citrix Virtual Apps and Desktops が、要求されたリソースを配信します。

Citrix Workspace アプリで Kerberos 認証を使用する場合は、以下のように構成する必要があります。

- Kerberos を使用するには、サーバーと Citrix Workspace アプリを、同じまたは信頼されている Windows Server ドメイン内に設置する必要があります。さらに、管理タスクを割り当てられるように、[Active Directory ユーザーとコンピューター] を使ってサーバーの信頼関係を構成する必要があります。
- ドメイン、および Citrix Virtual Apps and Desktops の両方で Kerberos が有効になっている必要があります。セキュリティを強化するには、Kerberos 以外の IWA オプションを無効にして、ドメインで必ず Kerberos が使用されるようにします。
- リモートデスクトップサービス接続で、基本認証や保存されたログオン情報の使用、または常にユーザーにパスワードを入力させたりする場合、Kerberos によるログオンは使用できません。

### 警告

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があります。Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

スマートカードを使用する環境で **Kerberos** によるドメインパススルー認証

Citrix Virtual Apps and Desktops ドキュメントの「[展開環境の保護](#)」セクションでスマートカード情報を参照してください。

Windows 向け Citrix Workspace アプリのインストール時に、以下のコマンドラインオプションを指定します。

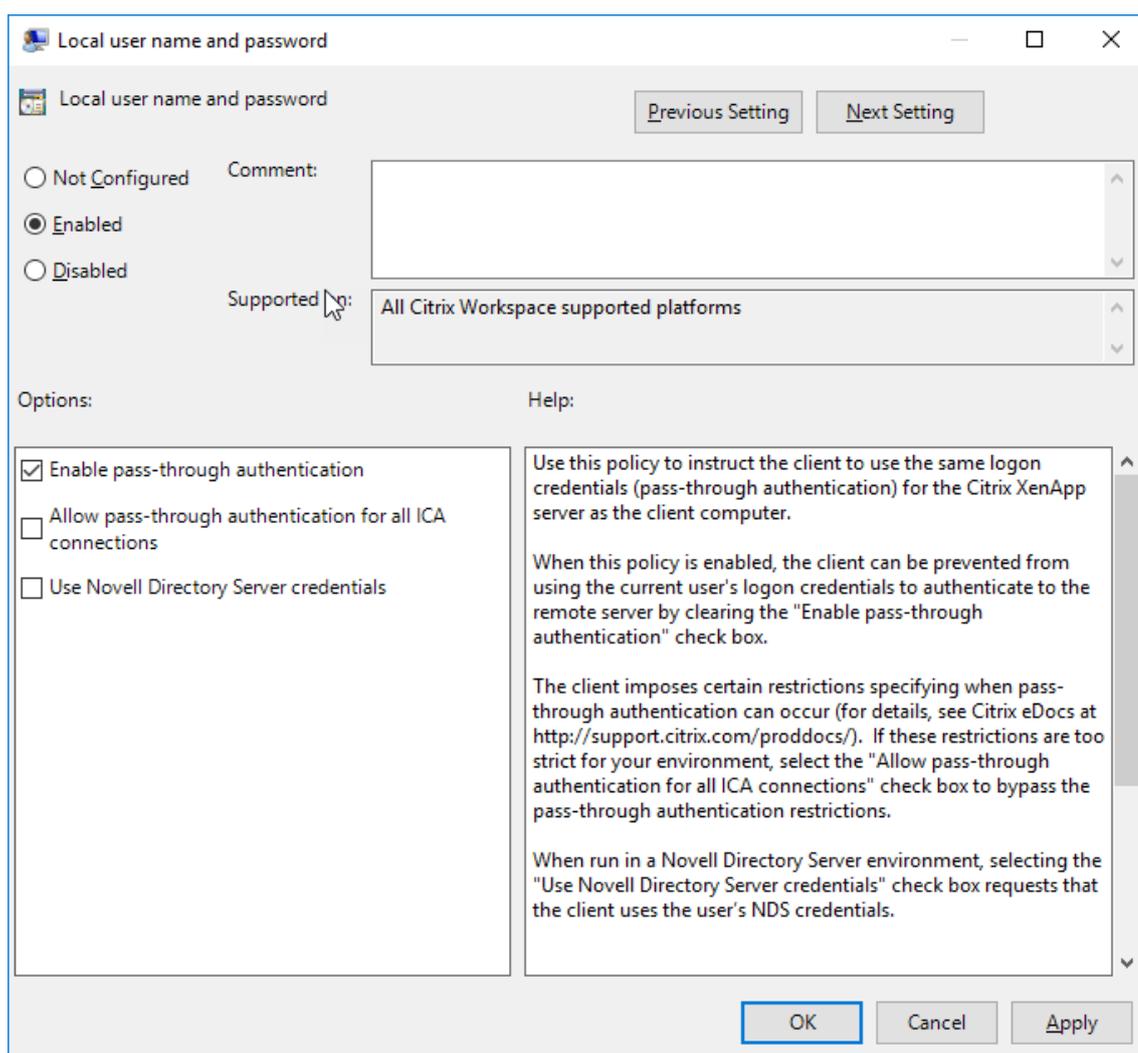
- `/includeSSON`

これにより、ドメインに参加しているコンピューターにシングルサインオンコンポーネントがインストールされ、ワークスペースの IWA (Kerberos) による StoreFront への認証が有効になります。シングルサインオンコンポーネントは、スマートカードの PIN を格納します。次に、HDX エンジンがこの PIN を使用して、Citrix Virtual Apps and Desktops がスマートカードハードウェアと資格情報にアクセスできるようにします。Citrix Virtual Apps and Desktops は、自動的にスマートカードから証明書を選択して、HDX エンジンから PIN を取得します。

関連オプション「`ENABLE_SSON`」は、デフォルトで有効になっています。

セキュリティポリシーにより、デバイスでシングルサインオンを有効にできない場合は、グループポリシーオブジェクト管理用テンプレートを使用して Citrix Workspace アプリを構成します。

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. [管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザー認証] > [ローカルユーザー名とパスワード] を選択します。
3. [パススルー認証を有効にします] チェックボックスをオンにします。
4. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。



**StoreFront** を構成するには:

StoreFront サーバーの認証サービスを構成するときに、[ドメインパススルー] オプションをオンにします。これにより、統合 Windows 認証が有効になります。[スマートカード] オプションは、スマートカードを使用して StoreFront に接続する非ドメイン参加のクライアントをサポートする場合のみオンにします。

StoreFront でスマートカードを使用する場合は、StoreFront ドキュメントの「[認証サービスの構成](#)」を参照してください。

### **Azure Active Directory** での条件付きアクセスのサポート

条件付きアクセスは、Azure Active Directory が組織のポリシーを適用するために使用するツールです。ワークスペース管理者は、Citrix Workspace アプリへの認証を行うユーザーに対して、Azure Active Directory の条件付きアクセスポリシーを構成および適用できます。Workspace アプリを実行する Windows マシンには、Microsoft Edge WebView2 ランタイムバージョン 92 以降がインストールされている必要があります。

Azure Active Directory を使用して条件付きアクセスポリシーを構成する方法の詳細と手順については、「**Azure**

**AD** の条件付きアクセスのドキュメント」 ([Docs.microsoft.com/en-us/azure/active-directory/conditional-access/](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/)) を参照してください。

注:

この機能は、Workspace (Cloud) のみでサポートされます。

## Citrix Workspace への認証を行う他の方法

Citrix Workspace アプリを使用して、次の認証メカニズムを構成できます。次の認証メカニズムが想定どおりに機能するには、Workspace アプリを実行する Windows マシンに、Microsoft Edge WebView2 ランタイムバージョン 92 以降がインストールされている必要があります。

1. Windows Hello ベースの認証 - Windows Hello ベースの認証の設定手順については、「**ビジネス Windows Hello** 設定の構成 - 証明書の信頼」([Docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings)) を参照してください。
2. FIDO2 セキュリティキーベースの認証 - FIDO2 セキュリティキーは、企業の従業員がユーザー名やパスワードを入力せずに認証するためのシームレスな方法を提供します。Citrix Workspace への FIDO2 セキュリティキーベースの認証を構成できます。ユーザーが FIDO2 セキュリティキーを使用して Azure AD アカウントで Citrix Workspace に対して認証を行うようにする場合は、「パスワードなしのセキュリティキーサインインを有効にする」([Docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key)) を参照してください。
3. ID プロバイダーとして Microsoft Azure Active Directory (AAD) を使用し、AAD 参加済みのマシンから Citrix Workspace アプリへのシングルサインオンを構成することもできます。Azure Active Directory Domain Services の構成について詳しくは、「**Azure Active Directory Domain Services** とは」([Docs.microsoft.com/en-us/azure/active-directory-domain-services/overview](https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview)) を参照してください。Azure Active Directory を Citrix Cloud に接続する方法については、「[Azure Active Directory を Citrix Cloud に接続する](#)」を参照してください。

## スマートカード

Windows 向け Citrix Workspace アプリでは、以下のスマートカード認証がサポートされます:

- パススルー認証 (シングルサインオン) - ユーザーが Citrix Workspace アプリにログオンするときに使用するスマートカードの資格情報を取得します。取得した資格情報は以下のように使用されます:
  - ドメインに属しているデバイスのユーザーがスマートカードで Citrix Workspace アプリにログオンした場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要はありません。
  - ドメインに属していないデバイスで実行している Citrix Workspace アプリがスマートカードの資格情報を使用している場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要があります。

パススルー認証を使用するには、StoreFront および Citrix Workspace アプリ両方での構成が必要です。

- **2 モード認証** - 認証方法として、スマートカードと、ユーザー名およびパスワードの入力を選択できます。この機能は、スマートカードを使用できない場合に有効です。たとえば、ログオン証明書が期限切れになった場合などです。これを実行できるようにするには、スマートカードを許可するため **False** に設定した **DisableCtrlAltDel** メソッドを使って、サイトごとに専用ストアをセットアップする必要があります。2 モード認証には StoreFront 構成が必要です。

また 2 モード認証により、StoreFront 管理者はユーザーが StoreFront コンソールでユーザー名とパスワード、およびスマートカード認証の両方を選択して同じストアで使用できるようにします。StoreFront のドキュメントを参照してください。

- **複数の証明書** - 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。ユーザーがスマートカードをリーダーに挿入すると、ユーザーデバイス上で実行する、Citrix Workspace アプリを含むすべてのアプリケーションで複数の証明書を適用できるようになります。
- **クライアント証明書による認証** - この機能を使用するには、Citrix Gateway および StoreFront での構成が必要です。
  - Citrix Gateway を使って StoreFront にアクセスする場合、ユーザーがスマートカードを取り外した後で再認証が必要です。
  - Citrix Gateway の SSL 構成で常にクライアント証明書による認証が使用されるようにすると、より安全になります。ただし、この構成では 2 モード認証を使用できません。
- **ダブルホップセッション** - ダブルホップセッションでは、Citrix Workspace アプリとユーザーの仮想デスクトップとの間に接続が確立されます。
- **スマートカード対応のアプリケーション** - Microsoft Outlook や Microsoft Office などのスマートカード対応アプリケーションでは、Citrix Virtual Apps and Desktops セッションでドキュメントにデジタル署名を追加したりファイルを暗号化したりできます。

**制限事項:**

- 証明書は、ユーザーデバイス上ではなくスマートカード上に格納されている必要があります。
- Citrix Workspace アプリはユーザー証明書の選択を保存しませんが、構成時に PIN を格納します。PIN はユーザーセッションの間にのみ非ページ化メモリにキャッシュされ、ディスク内には格納されません。
- Citrix Workspace アプリでは、スマートカードが挿入されたときに自動的に切断セッションに再接続されません。
- スマートカード認証が構成されている場合、Citrix Workspace アプリでは仮想プライベートネットワーク (VPN: Virtual Private Network) のシングルサインオンやセッションの事前起動がサポートされません。スマートカード認証で VPN を使用するには、ユーザーが Citrix Gateway Plug-in をインストールして Web ページ経由でログオンする必要があります。この場合、各手順でスマートカードと PIN による認証が必要になります。スマートカードユーザーは、Citrix Gateway Plug-in を使用した StoreFront へのパズスルー認証を使用できません。
- Citrix Workspace アプリ更新ツールと citrix.com や Merchandising Server 間の通信では、Citrix Gateway 上のスマートカード認証を使用できません。

### 警告

一部の構成では、レジストリの編集が必要です。レジストリエディターの使用を誤ると、問題が発生する可能性があります。Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

スマートカード認証のシングルサインオンを有効にするには:

Windows 向け Citrix Workspace アプリのインストール中に、以下のコマンドラインオプションを指定します:

- `ENABLE_SSON=Yes`

シングルサインオンは、「パススルー認証」と呼ばれることもあります。このオプションを指定すると、Citrix Workspace アプリで PIN を繰り返し入力する必要がなくなります。

- レジストリエディタで次のパスに移動し、シングルサインオンコンポーネントがインストールされていない場合は `SSONCheckEnabled` 文字列を `False` に設定します。

```
HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\
```

```
HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\
```

これにより、Citrix Workspace アプリの Authentication Manager でシングルサインオンコンポーネントがチェックされなくなり、Citrix Workspace アプリで StoreFront への認証が可能になります。

Kerberos の代わりに StoreFront に対してスマートカード認証を有効にするには、次のコマンドラインオプションで Windows 向け Citrix Workspace アプリをインストールします:

- `/includeSSON` を指定すると、シングルサインオン認証（パススルー認証）がインストールされます。資格情報のキャッシュおよびパススルードメインベース認証の使用を有効にします。
- Windows 向け Citrix Workspace アプリのスマートカード認証とは別の方法（ユーザー名とパスワードなど）でユーザーがエンドポイントにログオンしている場合、コマンドラインは次のようになります:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

これによりログオン時に資格情報がキャプチャされるのを防ぎ、Citrix Workspace アプリへのログオン時に PIN を格納することができます。

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. [管理用テンプレート] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザー認証] > [ローカルユーザー名とパスワード] に移動します。
3. [パススルー認証を有効にします] チェックボックスをオンにします。構成およびセキュリティ設定によっては、パススルー認証を実行するために [すべての ICA 接続にパススルー認証を許可します] チェックボックスをオンにします。

**StoreFront** を構成するには:

- 認証サービスを構成する場合、[スマートカード] チェックボックスをオンにします。

StoreFront でスマートカードを使用する場合は、StoreFront ドキュメントの「[認証サービスの構成](#)」を参照してください。

ユーザーデバイスでスマートカードを使用できるようにするには:

1. デバイスのキーストアに、証明機関のルート証明書をインポートします。
2. ベンダーが提供する暗号化ミドルウェアをインストールします。
3. Citrix Workspace アプリをインストールして構成します。

証明書の選択方法を変更するには:

複数の証明書が有効な場合、Citrix Workspace アプリではデフォルトでそれらの証明書の一覧が表示され、ユーザーは使用する証明書を選択できます。管理者は、デフォルトの証明書（スマートカードプロバイダー指定の証明書）、または有効期限が最も残っている証明書が使用されるように Citrix Workspace アプリを構成できます。有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。

有効な証明書とは、以下のものを指します:

- ローカルコンピューターの現在時刻に基づき、証明書が有効期限内である。
- サブジェクトの公開キーで RSA アルゴリズムが使用されており、キーの長さが 1024 ビット、2048 ビット、または 4096 ビットである。
- キー使用法にデジタル署名が含まれている。
- Subject Alternative Name フィールドにユーザープリンシパル名 (UPN) が含まれている。
- Enhanced Key Usage フィールドに Smart Card Logon および Client Authentication、または All Key Usages が含まれている。
- 証明書の発行者チェーンに含まれる証明機関の 1 つが、TLS ハンドシェイク時にサーバーから送信される、許可される識別名 (DN) の 1 つに合致している。

証明書の選択方法を変更するには、以下のいずれかの構成を行います:

- Citrix Workspace アプリのコマンドラインで、オプション `AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` を指定します。

デフォルト値は、Prompt です。SmartCardDefault または LatestExpiry を指定して複数の証明書が該当する場合は、Citrix Workspace アプリによりユーザーが証明書を選択するための一覧が表示されます。

- 次のキー値をレジストリキー `HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\AuthManager` に追加します: `CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }`

最適な証明書をユーザーが選択できるように、`HKEY_CURRENT_USER`での設定は、`HKEY_LOCAL_MACHINE`の設定よりも優先されます。

**CSP** の PIN 入力メッセージを使用するには:

Windows 向け Citrix Workspace アプリのデフォルトでは、スマートカードの Cryptographic Service Provider (CSP) ではなく PIN 入力用のメッセージが表示されます。PIN の入力が必要な場合、Citrix Workspace アプリがメッセージを表示して、ユーザーにより入力された PIN をスマートカードの CSP に渡します。プロセスごとやセッションごとの PIN のキャッシュが禁止されているなど、環境やスマートカードでより厳格なセキュリティが求められる場合は、CSP コンポーネントを使用して PIN 入力用のメッセージを表示して PIN を処理するように Citrix Workspace アプリを構成できます。

PIN 入力の処理方法を変更するには、以下のいずれかの構成を行います：

- Citrix Workspace アプリのコマンドラインで、オプション `AM_SMARTCARDPINENTRY=CSP` を指定します。
- 次のキー値をレジストリキー `HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager` に追加します： `SmartCardPINEntry=CSP`

### スマートカードのサポートおよび取り出しの変更

スマートカードを取り外すと Citrix Virtual Apps セッションからログオフされます。ただし、Citrix Workspace アプリの認証方法をスマートカードに設定している場合、Citrix Virtual Apps セッションからのログオフを有効にするには Windows 向け Citrix Workspace アプリで対応するポリシーを構成する必要があります。ユーザーは Citrix Workspace アプリセッションにログインしたままになります。

### 制限事項：

スマートカード認証を使用して Citrix Workspace アプリサイトにログインした場合、ユーザー名が [ログオン済み] と表示されます。

### 高速スマートカード

高速スマートカードは、既存の HDX PC/SC ベースのスマートカードリダイレクトの改良版です。遅延が大きい WAN 環境でスマートカードを使用する場合のパフォーマンスが向上しています。

高速スマートカードは、Linux VDA でのみサポートされています。

**Citrix Workspace** アプリで高速スマートカードログオンを有効にするには：

高速スマートカードログオンは VDA でデフォルトで有効になっていますが、Citrix Workspace アプリではデフォルトで無効になっています。高速スマートカードログオンを有効にするには、関連する StoreFront サイトの `default.ica` ファイルに次のパラメーターを追加します：

```
1 copy[WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

**Citrix Workspace** アプリで高速スマートカードログオンを無効にするには：

Citrix Workspace アプリで高速スマートカードログオンを無効にするには、関連する StoreFront サイトの **default.ica** ファイルから **SmartCardCryptographicRedirection** パラメーターを削除します。

詳しくは、「[スマートカード](#)」を参照してください。

### Citrix Workspace のサイレント認証

Citrix Workspace アプリでは、グループポリシーオブジェクト (GPO) ポリシーが導入され、Citrix Workspace のサイレント認証が有効になります。このポリシーにより、Citrix Workspace アプリがシステムの起動時に Citrix Workspace に自動的にログインできるようになります。このポリシーは、ドメインに参加しているデバイスの Citrix Workspace に対してドメインパススルー (シングルサインオン) が構成されている場合のみ使用してください。

このポリシーが機能するには、次の条件を満たす必要があります：

- シングルサインオンを有効にする必要があります。
- レジストリエディターで **SelfServiceMode** キーを **Off** に設定する必要があります。

サイレント認証の有効化：

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 Workspace**] > [**Self Service**] の順に移動します。
3. [**Citrix Workspace** のサイレント認証] ポリシーをクリックして、[有効] に設定します。
4. [適用]、[OK] の順にクリックします。

### セキュリティで保護された通信

May 17, 2021

以下の一連の技術を使用して安全に通信することで、Citrix Workspace アプリ接続を統合します：

- Citrix Gateway
- ファイアウォール：ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。
- 信頼されたサーバー。
- Citrix Virtual Apps 展開の場合のみ：SOCKS プロキシサーバーまたはセキュアプロキシサーバー。プロキシサーバーは、ネットワークとのアクセスを制限するのに役立ちます。また、Citrix Workspace アプリとサーバー間の接続も処理します。Citrix Workspace アプリは、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。

## 送信プロキシのサポート

SmartControl を使用すると、管理者は環境に影響を与えるポリシーを構成して適用できます。たとえば、ユーザーがドライブをリモートデスクトップにマップできないようにしたい場合があります。Citrix Gateway の SmartControl 機能を使用して、このような詳細設定を実現できます。

Citrix Workspace アプリと Citrix Gateway が別々のエンタープライズアカウントに属している場合、状況は異なります。このような場合は、クライアントドメインに Gateway が存在しないため、ドメインは SmartControl 機能を適用できません。代わりに、送信 ICA プロキシを利用できます。送信 ICA プロキシ機能を使用すると、Citrix Workspace アプリと Citrix Gateway が異なる組織に展開されている場合でも、スマートコントロール機能を使用できます。

Citrix Workspace アプリは、NetScaler LAN プロキシを使用したセッションの起動をサポートします。送信プロキシプラグインを使用して、単一の静的プロキシを構成するか、実行時にプロキシサーバーを選択します。

送信プロキシは、次の方法を使用して構成できます：

- 静的プロキシ：プロキシのホスト名とポート番号を指定してプロキシサーバーを構成します。
- 動的プロキシ：プロキシプラグイン DLL を使用して、1 つ以上のプロキシサーバーから 1 つのプロキシサーバーを選択できます。

グループポリシーオブジェクト管理用テンプレートまたはレジストリエディターを使用して、送信プロキシを構成できます。

送信プロキシについて詳しくは、Citrix Gateway のドキュメントの「[送信 ICA プロキシのサポート](#)」を参照してください。

## 送信プロキシのサポート - 構成

注：

静的プロキシと動的プロキシの両方が構成されている場合は、動的プロキシの構成が優先されます。

**GPO** 管理用テンプレートを使用した送信プロキシの構成：

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 Workspace] > [ネットワークルーティング] の順に移動します。
3. 次のいずれかのオプションを選択します：
  - 静的プロキシの場合：[NetScaler LAN プロキシを手動で構成する] ポリシーを選択します。[有効] を選択して、ホスト名とポート番号を入力します。
  - 動的プロキシの場合：[NetScaler LAN プロキシを DLL を使用して構成する] ポリシーを選択します。[有効] を選択して、DLL ファイルのフルパスを入力します。たとえば、C:\Workspace\Proxy\ProxyChooser.dll などです。
4. [適用]、[OK] の順にクリックします。

レジストリエディターを使用して、次のように送信プロキシを構成します：

- 静的プロキシの場合：
  - レジストリエディターを起動して、HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScalerに移動します。
  - DWORD 値キーを次のように作成します：

```
"StaticProxyEnabled"=dword:00000001
"ProxyHost"="testproxy1.testdomain.com
"ProxyPort"=dword:000001bb
```
- 動的プロキシの場合：
  - レジストリエディターを起動して、HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxyに移動します。
  - DWORD 値キーを次のように作成します：

```
"DynamicProxyEnabled"=dword:00000001
"ProxyChooserDLL"="c:\Workspace\Proxy\ProxyChooser.dll"
```

## TLS

Transport Layer Security (TLS) は、Secure Sockets Layer (SSL) プロトコルに代わるものです。IETF (Internet Engineering TaskForce) が、TLS の公開標準規格の開発を Netscape Communications 社から引き継いだ時に、SSL という名前を TLS に変更しました。

TLS は、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信をセキュアに保護します。米国政府機関をはじめとする組織の中には、データ通信を保護するために TLS の使用を義務付けているところもあります。このような組織では、さらに FIPS 140 (Federal Information Processing Standard) などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140 は、暗号化の情報処理規格です。

TLS 暗号化を通信メディアとして使用するには、ユーザーデバイスと Citrix Workspace アプリを構成する必要があります。StoreFront 通信の保護については、StoreFront ドキュメントの「[セキュリティ](#)」セクションを参照してください。

前提条件：

詳しくは、「[システム要件](#)」セクションを参照してください。

以下の暗号の組み合わせを使用して、次のことができます：

- TLS の使用を適用する：インターネットを含めて、信頼されていないネットワークを介する接続で、TLS の使用をお勧めします。
- FIPS (Federal Information Processing Standards) 準拠の暗号化の使用を適用し、NIST SP 800-52 の推奨セキュリティを遵守します。デフォルトでは、これらのオプションは無効になっています。

- 特定の TLS バージョンおよび特定の TLS 暗号の組み合わせの使用を適用する：TLS 1.0、TLS 1.1、TLS 1.2 プロトコルが Citrix ではサポートされません。
- 特定のサーバーのみに接続する。
- サーバー証明書の失効を確認する。
- 特定のサーバー証明書発行ポリシーを確認する。
- 特定のクライアント証明書を選択する（サーバーが要求するよう構成されている場合）。

次の暗号の組み合わせは、セキュリティを強化するために廃止されました：

- 暗号の組み合わせ RC4 および 3DES
- 接頭辞が「TLS\_RSA\_\*」の暗号の組み合わせ
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)
- TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

Citrix Workspace アプリは以下の暗号の組み合わせのみをサポートします：

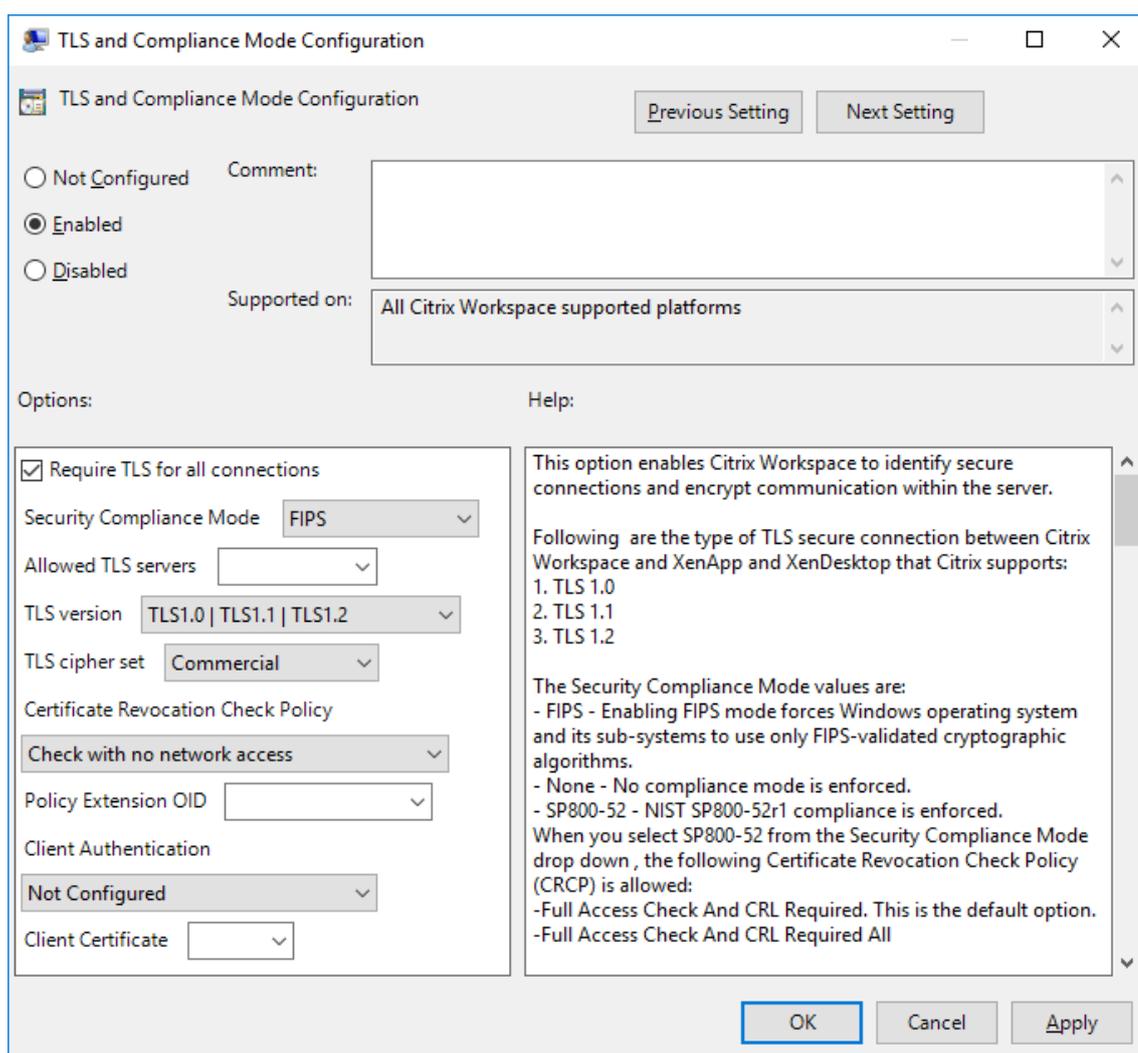
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

DTLS 1.0 ユーザーの場合、Citrix Workspace アプリは以下の暗号の組み合わせのみをサポートします：

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013)

### TLS のサポート

1. gpedit.msc を実行して、Citrix Workspace アプリの GPO 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 Workspace] > [ネットワークルーティング] の順に移動して、[TLS およびコンプライアンスモードの構成] ポリシーを選択します。



3. [有効] を選択してセキュリティで保護された接続を有効にし、サーバー上の通信を暗号化します。次のオプションを設定します。

注:

セキュリティで保護された接続で、TLS を使用することを Citrix ではお勧めします。

- a) [すべての接続で **TLS** が必要] を選択することによって、公開アプリケーションおよびデスクトップに対する Citrix Workspace アプリの通信で強制的に TLS を使用させることができます。
- b) [セキュリティコンプライアンスモード] メニューから、適切なオプションを選択します:
  - i. なし - コンプライアンスモードが適用されません。
  - ii. **SP800-52 - SP800-52** を選択して NIST SP800-52 に準拠します。このオプションは、サーバーまたはゲートウェイを NIST SP 800-52 推奨セキュリティに準拠させる場合にのみ選択してください。

注:

[**SP800-52**] を選択すると、[**FIPS** を有効にします] が選択されていない場合でも、自動的に FIPS 準拠の暗号化が使用されます。Windows セキュリティオプションの [システム暗号化: 暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う] も有効にする必要があります。有効にしない場合、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。

[**SP800-52**] を選択した場合、[証明書失効チェックのポリシー] を [完全なアクセス権のチェックと **CRL** が必要です] に設定します。

[**SP800-52**] を選択すると、Citrix Workspace アプリはサーバー証明書が NIST SP 800-52 の推奨セキュリティに準拠しているかを検証します。サーバー証明書が準拠していない場合、Citrix Workspace アプリが接続できないことがあります。

- i. **FIPS** を有効にします - FIPS 準拠の暗号化の使用を適用するには、このオプションを選択します。オペレーティングシステムのグループポリシーから Windows セキュリティオプションの [システム暗号化: 暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う] も有効にする必要があります。有効にしない場合、Citrix Workspace アプリが公開アプリケーションおよびデスクトップに接続できないことがあります。

- c) [許可された **TLS** サーバー] ドロップダウンメニューから、ポート番号を選択します。コンマ区切りの一覧を使用して、Workspace アプリが指定されたサーバーにのみ接続できるようにします。ワイルドカードおよびポート番号を指定できます。たとえば、「\*.citrix.com: 4433」により、共通名が「.citrix.com」で終わるどのサーバーともポート 4433 での接続が許可されます。セキュリティ証明書の情報の正確さは、証明書の発行者によって異なります。Citrix Workspace が証明書の発行者を認識しない、または信頼しないと、接続は拒否されます。

- d) [**TLS** バージョン] メニューから、次のいずれかのオプションを選択します:

- **TLS 1.0**、**TLS 1.1**、または **TLS 1.2** - これはデフォルトの設定です。このオプションは、業務上 TLS 1.0 との互換性が必要な場合のみお勧めします。
- **TLS 1.1** または **TLS 1.2** - このオプションで接続が TLS 1.1 または TLS 1.2 を使用するようにします。
- **TLS 1.2** - このオプションは、業務上 TLS 1.2 が必要な場合のみお勧めします。

- a) **TLS** 暗号セット - 特定の TLS 暗号セットの使用を適用するには、GOV (行政機関)、COM (営利企業)、ALL (すべて) の中から選択します。一部の Citrix Gateway 構成では、**COM** の選択が必要になることがあります。Citrix Workspace アプリは、ビット長 1024、2048 および、3072 の RSA キーをサポートします。さらに、ビット長 4096 の RSA キーを持つルート証明書がサポートされます。

注:

ビット長 1024 の RSA キーの使用は Citrix ではお勧めしません。

- 任意: 「任意」が設定されると、ポリシーは構成されず次のいずれかの暗号の組み合わせが許可されます:
  - a) TLS\_RSA\_WITH\_RC4\_128\_MD5

- b) TLS\_RSA\_WITH\_RC4\_128\_SHA
  - c) TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
  - d) TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
  - e) TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
  - f) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - g) TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- 商用: 「商用」が設定されると、次の暗号の組み合わせのみが許可されます:
    - a) TLS\_RSA\_WITH\_RC4\_128\_MD5
    - b) TLS\_RSA\_WITH\_RC4\_128\_SHA
    - c) TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
    - d) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - 自治体: 「自治体」が設定されると、暗号の組み合わせのみが許可されます:
    - a) TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
    - b) TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
    - c) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
    - d) TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- a) [証明書失効チェックのポリシー] メニューから、次の任意のオプションを選択します:
- ネットワークアクセスなしでチェックします - 証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアのみが使用されます。すべての配布ポイントが無視されます。証明書失効一覧の検索は、対象の SSL Relay/Citrix Secure Web Gateway サーバーによって提示されるサーバー証明書の検証に必須ではありません。
  - 完全なアクセス権のチェック - 証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。証明書失効一覧の検索は、対象サーバーによって提示されるサーバー証明書の検証において重大な意味を持ちません。
  - 完全なアクセス権と **CRL** のチェックが必要です - ルート証明機関を除いて証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。
  - すべてに完全なアクセス権と **CRL** のチェックが必要です - ルート CA を含めた証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。
  - チェックなし - 証明書失効一覧チェックは実行されません。
- a) [ポリシーの拡張 **OID**] を使用して、Citrix Workspace アプリが特定の証明書の発行ポリシーがあるサーバーにのみ接続するように制限できます。[ポリシーの拡張 **OID**] を選択すると、Citrix Workspace

アプリはポリシーの拡張 OID があるサーバー証明書のみを受け入れます。

b) [クライアント認証] メニューから、以下の任意のオプションを選択します：

- 無効 - クライアント認証が無効になります。
- 証明書セレクタを表示します - 常にユーザーが証明書を選択するよう求めます。
- 可能な場合、自動的に選択します - 特定する証明書に選択肢がある場合のみ、ユーザーに表示します。
- 未構成 - クライアント認証が構成されていないことを意味します。
- 指定された証明書を使用します - [クライアント証明書] オプションの設定で指定された「クライアント証明書」を使用します。

a) [クライアント証明書] 設定を使用して、識別証明書の拇印を指定します。これにより、ユーザーに不要なプロンプトを表示しないようにすることができます。

b) [適用] および [OK] をクリックしてポリシーを保存します。

次のマトリックスは、内部および外部ネットワーク接続の詳細を提供します：

| Client cipher set | VDA cipher set | Direct connections                       |      |          |           |      |          |           |      |          |
|-------------------|----------------|------------------------------------------|------|----------|-----------|------|----------|-----------|------|----------|
|                   |                | TLS                                      |      |          | DTLS v1.0 |      |          | DTLS v1.2 |      |          |
|                   |                | Open                                     | FIPS | SP800-52 | Open      | FIPS | SP800-52 | Open      | FIPS | SP800-52 |
| Any               | ANY            | Y                                        | Y    | Y        | Y         |      |          | Y         |      |          |
|                   | COM            | Y                                        | X    | X        | Y         |      |          | Y         |      |          |
|                   | GOV            | Y                                        | Y    | Y        | Y         |      |          | Y         |      |          |
| COM               | ANY            | Y                                        | X    | X        | Y         |      |          |           |      |          |
|                   | COM            | Y                                        | X    | X        | Y         |      |          |           |      |          |
|                   | GOV            | Y                                        | X    | X        | Y         |      |          |           |      |          |
| GOV               | ANY            | Y                                        | Y    | Y        | X         |      |          | Y         |      |          |
|                   | COM            | X                                        | X    | X        | X         |      |          | X         |      |          |
|                   | GOV            | Y                                        | Y    | Y        | X         |      |          | Y         |      |          |
| Client cipher set | VDA cipher set | External connections with Citrix Gateway |      |          |           |      |          |           |      |          |
|                   |                | TLS                                      |      |          | DTLS v1.0 |      |          | DTLS v1.2 |      |          |
|                   |                | Open                                     | FIPS | SP800-52 | Open      | FIPS | SP800-52 | Open      | FIPS | SP800-52 |
| Any               | ANY            | Y                                        | Y    | Y        | Y         |      |          | X         |      |          |
|                   | COM            | Y                                        | X    | X        | Y         |      |          | X         |      |          |
|                   | GOV            | Y                                        | Y    | Y        | Y         |      |          | X         |      |          |
| COM               | ANY            | Y                                        | X    | X        | Y         |      |          | X         |      |          |
|                   | COM            | Y                                        | X    | X        | Y         |      |          | X         |      |          |
|                   | GOV            | Y                                        | X    | X        | Y         |      |          | X         |      |          |
| GOV               | ANY            | Y                                        | Y    | Y        | X         |      |          | X         |      |          |
|                   | COM            | X                                        | X    | X        | X         |      |          | X         |      |          |
|                   | GOV            | Y                                        | Y    | Y        | X         |      |          | X         |      |          |

### ファイアウォール

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。ファイアウォールが使用されている場合、Windows 向け Citrix Workspace アプリと Web サーバーおよび Citrix 製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。

### 共通の Citrix 通信ポート

| 接続元                        | 種類      | ポート    | 詳細                        |
|----------------------------|---------|--------|---------------------------|
| Citrix Workspace アプリ       | TCP     | 80/443 | StoreFront との通信           |
| ICA または HDX                | TCP/UDP | 1494   | アプリケーションおよび仮想デスクトップへのアクセス |
| ICA または HDX (セッション画面の保持機能) | TCP/UDP | 2598   | アプリケーションおよび仮想デスクトップへのアクセス |
| ICA または HDX (SSL 経由)       | TCP/UDP | 443    | アプリケーションおよび仮想デスクトップへのアクセス |

ポートについて詳しくは、Knowledge Center の[CTX101810](#)を参照してください。

### プロキシサーバー

プロキシサーバーは、ネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Windows 向け Citrix Workspace アプリとサーバー間の接続を制御するために使います。Citrix Workspace アプリは、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。

Citrix Workspace アプリでサーバーと通信する場合、Web 向け Workspace を実行するサーバー上でリモートで構成されているプロキシサーバー設定が使用されます。

また、Citrix Workspace アプリが Web サーバーと通信するときは、ユーザーデバイス上でデフォルトの Web ブラウザーのインターネット設定で構成したプロキシサーバー設定が使用されます。各ユーザーデバイス上のデフォルトの Web ブラウザーで、インターネット設定を構成する必要があります。

接続中に Citrix Workspace アプリがプロキシサーバーを優先するか無視するかについて、レジストリエディターでプロキシ設定を構成します。

### 警告

レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、オペレーティングシステムの再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。

1. `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`にアクセスします。
2. **ProxyEnabled** (REG\_SZ) を設定します。
  - True – Citrix Workspace アプリは接続でプロキシサーバーを優先します。
  - False – Citrix Workspace アプリは接続でプロキシサーバーを無視します。
3. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

### 信頼されたサーバー

信頼済みサーバー構成を使用して、Citrix Workspace アプリの接続で信頼関係を識別し適用できます。

信頼済みサーバーを有効にすることで、Citrix Workspace アプリは要件を指定し、サーバーへの接続が信頼済みかどうかを判断できます。たとえば、特定のアドレス ([https://\\\*.citrix.com](https://\*.citrix.com)など) に特定の接続の種類 (TLS など) を使用して接続する Citrix Workspace アプリは、サーバーの信頼済みゾーンに接続されます。

この機能を有効にすると、接続されたサーバーは Windows の信頼済みサイトゾーンに配置されます。Windows の信頼済みサイトゾーンにサーバーを追加する手順について詳しくは、Internet Explorer のオンラインヘルプを参照してください。

グループポリシーオブジェクト管理用テンプレートを使用して信頼済みサーバーの構成を有効にするには

前提要件:

コネクションセンターなどの Citrix Workspace アプリコンポーネントを終了します。

1. `gpedit.msc` を実行して、Citrix Workspace アプリの GPO 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] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Workspace] > [ネットワークルーティング] > [信頼済みサーバーの構成を構成します] の順に選択します。
3. [有効] を選択して、Citrix Workspace アプリに領域の識別を適用します。
4. [信頼済みサーバーの構成を適用します] を選択します。これによって、クライアントに信頼済みサーバーを使用した識別を適用します。
5. [Windows インターネットゾーン] ドロップダウンメニューから、クライアントのサーバーアドレスを選択します。この設定は Windows の信頼済みサイトにのみ適用できます。
6. [アドレス] フィールドで、Windows 以外の信頼済みサイトゾーンのクライアントのサーバーアドレスを設定します。コンマ区切り一覧を使用できます。
7. [OK] および [適用] をクリックします。

## ICA ファイルの署名

ICA ファイル署名機能は、認証していないアプリケーションやデスクトップの起動を回避するために役立ちます。Citrix Workspace アプリは、信頼できるソースからアプリケーションまたはデスクトップが起動されることを管理ポリシーに基づいて検証し、信頼されていないサーバーからの起動を防ぎます。グループポリシーオブジェクトの管理用テンプレートまたは StoreFront を使用して、ICA ファイルの署名を構成できます。ICA ファイル署名はデフォルトで無効になっています。

StoreFront に対する ICA ファイル署名については、StoreFront のドキュメントの「[ICA ファイル署名の有効化](#)」を参照してください。

## ICA ファイルの署名の構成

注:

CitrixBase.admx\adml がローカル GPO に追加されないと、[ICA ファイルの署名を有効にします] ポリシーが表示されないことがあります。

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] に移動します。
3. [ICA ファイルの署名を有効にします] を選択し、必要に応じて次のいずれかのオプションを選択します。
  - a) 有効 - 署名証明書の拇印を信頼された機関からの証明書の拇印のホワイトリストに追加できます。
  - b) 信頼証明書 - [表示] をクリックして、ホワイトリストから既存の署名証明書の拇印を削除します。署名証明書のサムプリントは署名証明書のプロパティからコピーして貼り付けることができます。
  - c) セキュリティポリシー - メニューから次のいずれかのオプションを選択します。
    - i. 署名による起動のみを許可します (安全性が高い): 信頼できるサーバーからの署名されたアプリケーションまたはデスクトップの起動のみを許可します。無効な署名があると、セキュリティ警告が表示されます。認証されていないため、セッションを開始できません。
    - ii. 署名されていない起動 (安全性が低い) でユーザーにプロンプトを表示します: 署名されていないセッション、または署名が無効なセッションが開始されると、メッセージが表示されます。起動を続行するか、起動をキャンセルするか (デフォルト) を選択できます。
4. [適用] および [OK] をクリックしてポリシーを保存します。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

デジタル署名証明書を選択して配布するには:

デジタル署名証明書を選択するときは、次の一覧の上位のオプションから順にお勧めします:

1. 周知の証明機関からコード署名証明書または SSL 署名証明書を購入する。
2. 社内に証明機関がある場合はその証明機関を使用して、コード署名証明書または SSL 署名証明書を作成する。
3. 既存の SSL 証明書を使用する。
4. ルート証明書を作成して、GPO または手動インストールによりユーザーデバイスに配布する。

## ローカルセキュリティ機関 (LSA) の保護

Citrix Workspace アプリは Windows のローカルセキュリティ機関 (LSA) の保護をサポートします。この仕組みはシステムのローカルセキュリティに関するあらゆる情報を管理します。このサポートにより、ホストされるデスクトップに LSA レベルのシステム保護が提供されます。

## Storebrowse

April 19, 2021

Storebrowse は、クライアントとサーバー間の相互通信に使用されるコマンドラインユーティリティです。StoreFront 内および Citrix Gateway 内のすべての操作を認証するために使用されます。

Storebrowse ユーティリティを使用すると、管理者は以下のような操作を自動化できます：

- ストアを追加します。
- 構成済みのストアから公開アプリおよびデスクトップを列挙します。
- 公開された Citrix Virtual Apps and Desktops を選択して、ICA ファイルを手動で生成します。
- Storebrowse コマンドラインを使用して ICA ファイルを生成します。
- 公開アプリケーションを起動します。

Storebrowse ユーティリティは、Authmanager コンポーネントの一部です。Citrix Workspace アプリのインストール後、Storebrowse ユーティリティは AuthManager インストールフォルダーに格納されます。

Storebrowse ユーティリティが Authmanager コンポーネントにインストールされているかどうかは、次のレジストリパスを確認してください：

管理者が **Citrix Workspace** アプリをインストールする場合：

---

|              |                                                      |
|--------------|------------------------------------------------------|
| 32 ビットマシンの場合 | [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst |
| 64 ビットマシンの場合 | [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A    |

---

ユーザー（管理者以外）が **Citrix Workspace** アプリをインストールする場合：

---

|              |                                                     |
|--------------|-----------------------------------------------------|
| 32 ビットマシンの場合 | [HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Inst |
| 64 ビットマシンの場合 | [HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\A    |

---

### 要件

- Windows 向け Citrix Workspace アプリバージョン 1808 以降。
- 530MB 以上の空きディスクスペース。
- 2GB の RAM。

### 互換性マトリックス

Storebrowse ユーティリティは、以下のオペレーティングシステムと互換性があります：

---

#### オペレーティングシステム

---

Windows 10 32 ビット版および 64 ビット版

Windows 8.1 32 ビット版および 64 ビット版

Windows 7 SP1 32 ビット版および 64 ビット版

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2、Standard および Datacenter エディション

Windows Server 2012、Standard および Datacenter エディション

Windows Server 2008 R2 (64 ビット版)

Windows Server 2008 R2 (64 ビット版)

---

### 接続

Storebrowse ユーティリティは、以下の接続の種類をサポートします：

- HTTP ストア
- HTTPS ストア
- Citrix Gateway 11.0 以降

#### 注：

Storebrowse ユーティリティは、HTTP ストア上でコマンドラインを使用して資格情報を承認しません。

### 認証方法

#### **StoreFront** サーバー

StoreFront は、ストアにアクセスするためのさまざまな認証方法をサポートしますが、すべてが推奨されるわけではありません。セキュリティ上の理由により、ストアの作成時には一部の認証方法がデフォルトで無効になります。

- ユーザー名とパスワード：ストアにアクセスするときに、認証のために資格情報を入力します。デフォルトで、最初のストアの作成時に、指定ユーザー認証が有効になります。
- ドメインパススルー：ドメインに参加している Windows コンピューターに認証されると、ストアに自動的にログオンできます。このオプションを使用するには、Citrix Workspace アプリのインストール時にパススルー認証を有効にします。ドメインパススルーについて詳しくは、「[ドメインパススルー認証の構成](#)」を参照してください。
- **HTTP 基本**：HTTP 基本認証を有効にすると、Storebrowse ユーティリティが StoreFront サーバーと通信できます。デフォルトでは、このオプションは StoreFront サーバーで無効になっています。**HTTP 基本**認証方式を有効にする必要があります。

Storebrowse ユーティリティは、以下のいずれかの方式の認証方法をサポートします：

- Storebrowse ユーティリティに組み込みの **AuthManager** を使用します。注：Storebrowse ユーティリティを使用する場合、StoreFront で HTTP 基本認証方式を有効にする必要があります。これは、ユーザーが Storebrowse コマンドを使用して資格情報を提供する場合に適用されます。
- Windows 向け Citrix Workspace アプリに外部 **Authmanager** を含めることができます。

### Citrix Gateway でのシングルサインオン

Citrix Gateway のサポートに加えて、シングルサインオンを使用できるようになりました。ユーザー資格情報を提供することなく、ストアを追加し、公開リソースを列挙することができます。

Citrix Gateway でシングルサインオンを使用する方法については、「[Citrix Gateway でのシングルサインオンのサポート](#)」を参照してください。

注：

この機能は、Citrix Gateway でシングルサインオン認証が構成されているドメイン参加のマシンでのみサポートされます。

### 公開デスクトップまたはアプリケーションからの起動

ICA ファイルを使用せずに、ストアから直接リソースを起動できるようになりました。

### コマンドの使用方法

以下のセクションでは、Storebrowse ユーティリティで使用できるコマンドについて詳しく説明します。

#### **-a、-addstore**

説明：

新しいストアを追加します。ストアの完全な URL を返します。失敗するとエラーが表示されます。

注:

複数ストア構成は、Storebrowse ユーティリティでサポートされています。

**StoreFront** のコマンド例:

コマンド:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*  
*
```

例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a [https://  
my.firstexamplestore.net](https://my.firstexamplestore.net)
```

**Citrix Gateway** のコマンド例:

コマンド:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*  
*
```

例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://  
mysecondexample.com>
```

**/?**

説明:

Storebrowse ユーティリティの使用方法の詳細を提供します。

**(-l)、-liststore**

説明:

ユーザーが追加したストアを一覧表示します。

**StoreFront** のコマンド例:

```
.\storebrowse.exe -l
```

**Citrix Gateway** のコマンド例:

```
.\storebrowse.exe -l
```

### **(-M 0x2000 -E)**

説明:

リソースが列挙されます。

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E  
<https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E  
<https://my.secondexample.net>
```

### **-q、-quicklaunch**

説明:

Storebrowse ユーティリティを使用して、公開アプリおよび公開デスクトップの ICA ファイルを生成します。クイック起動オプションを使用するには、起動 URL とストア URL の入力が必要です。起動 URL は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。ICA ファイルは、%LocalAppData%\Citrix\Storebrowse\cache ディレクトリに生成されます。

以下のコマンドを実行して、公開されているすべてのアプリとデスクトップの起動 URL を取得できます:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/  
discovery
```

以下は、一般的な起動 URL の例です:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/  
Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_public  
apps and desktops } <https://my.firstexamplestore.net/Citrix/Store/resources  
/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix  
/Store/discovery>
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_public  
apps and desktops } <https://my.secondexamplestore.com>
```

### **-L、-launch**

説明:

Storebrowse コマンドを使用し、公開アプリおよび公開デスクトップに必要な ICA ファイルを生成します。起動オプションを使用するには、リソース名とストア URL が必要です。この名前は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。ICA ファイルは、%LocalAppData%\Citrix\Storebrowse\cache ディレクトリに生成されます。

公開アプリとデスクトップの表示名を取得するには、以下のコマンドを実行します：

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

以下は、このコマンドの結果です：

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

上記の結果で太字の名前は、起動オプションの入力パラメーターとして使用されます。

StoreFront のコマンド例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L "{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway のコマンド例：

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L { Resource_Name } https://my.seconddexamplestore.com>
```

### **-S、-sessionlaunch**

説明：

このコマンドを使用すると、ストアを追加し、公開リソースを列挙して起動できます。このオプションは、以下の情報をパラメーターとして使用します：

- ユーザー名
- パスワード
- ドメイン
- 起動するリソースの名前
- ストア URL

ただし、ユーザーが資格情報を指定しない場合、資格情報を入力するための AuthManager プロンプトが表示され、リソースが起動されます。

以下のコマンドを実行して、公開アプリや公開デスクトップのリソース名を取得できます：

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

以下は、このコマンドの結果です：

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

上記の結果で太字の名前は、-S オプションの入力パラメーターとして使用されます。

StoreFront のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S "{
Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery >
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S { Friendly_Resource_
} <https://my.secondexamplestore.com>
```

## **-f、-filefolder**

説明:

公開アプリおよびデスクトップのカスタムパスに ICA ファイルを生成します。

起動オプションを使用するには、フォルダー名とリソース名の入力が必要で、ストア URL とともに必要です。ストア URL は、StoreFront サーバーまたは Citrix Gateway URL のいずれかになります。

StoreFront のコマンド例:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```

## **-t、-traceauthentication**

説明:

AuthManager コンポーネントのログを生成します。ログは、Storebrowse ユーティリティが組み込みの AuthManager を使用している場合にのみ生成されます。localappdata%\Citrix\Storebrowse\logs ディレクトリに生成されます。

注:

このオプションを、ユーザーのコマンドラインに表示される最後のパラメーターにすることはできません。

StoreFront のコマンド例:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a {
StoreURL }
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a {  
NSG_URL }
```

#### **-d、-deletestore**

説明:

既存の StoreFront または Citrix Gateway ストアを削除します。

StoreFront のコマンド例:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Citrix Gateway のコマンド例:

```
.\storebrowse.exe -d https://my.secondexamplestore.com
```

### **Citrix Gateway** でのシングルサインオンのサポート

シングルサインオンを使用すると、ドメインに対して認証することで、そのドメインで提供されている Citrix Virtual Apps and Desktops を再認証する必要なく使用できます。ストアを追加すると、列挙された Citrix Virtual Apps and Desktops とともに資格情報とスタートメニューの設定が Citrix Gateway サーバーにパススルーされます。

この機能は、Citrix Gateway バージョン 11 以降でサポートされています。

前提条件:

Citrix Gateway のシングルサインオンを構成するための前提条件については、「[ドメインパススルー認証の構成](#)」を参照してください。

グループポリシーオブジェクト (GPO) 管理用テンプレートを使用して Citrix Gateway でシングルサインオン機能を有効にできます。

1. gpedit.msc を実行して、Citrix Workspace アプリ GPO 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] > [ユーザー認証] > [Citrix Gateway のシングルサインオン] に移動します。
3. シングルサインオンオプションで [有効] または [無効] に切り替えます。
4. [適用]、[OK] の順にクリックします。
5. Citrix Workspace アプリのセッションを再起動して、この変更を適用します。

制限事項:

- Storebrowse ユーティリティでの資格情報入力操作のために、StoreFront サーバーで **HTTP** 基本認証を有効にします。
- Citrix Virtual Apps and Desktops を列挙または起動するためにユーティリティを使用して HTTP ストアに接続しようとする場合、コマンドラインオプションを使用した資格情報の入力はサポートされません。この問題を回避するには、コマンドラインで資格情報を提供しないときに外部AuthManagerモジュールを使用します。

- Storebrowse ユーティリティは、現在、StoreFront サーバー上の Citrix Gateway で構成された単一ストアのみをサポートしています。
- Storebrowse ユーティリティの資格情報の入力、Citrix Gateway が単一要素認証で構成されている場合にのみ機能します。
- Storebrowse ユーティリティのコマンドラインオプション `Username (-U)`、`Password (-P)`、`Domain (-D)` では大文字小文字が区別され、大文字のみを使用する必要があります。

## Citrix Workspace アプリ Desktop Lock

January 18, 2021

ローカルのデスクトップを操作する必要がない場合は、Citrix Workspace アプリ Desktop Lock を使用できます。Desktop Viewer（有効な場合）を使用することはできませんが、ツールバー上には次の必須オプションしか表示されません：

- Ctrl+Alt+Del
- 基本設定
- デバイス
- 切断。

Windows 向け Citrix Workspace アプリ Desktop Lock は、SSON（Single Sign-On: シングルサインオン）が有効でありストアが構成済みのドメイン参加マシンで機能します。Program Neighborhood エージェント（PNA）サイトはサポートしません。以前のバージョンの Desktop Lock は、Citrix Receiver for Windows 4.2 以降へアップグレードするとサポートされません。

Windows 向け Citrix Workspace アプリを、`/includeSSON` フラグを使用してインストールする必要があります。adm/admx ファイルまたはコマンドレットオプションのいずれかを使って、ストアおよびシングルサインオンを構成する必要があります。詳しくは、「[インストール](#)」を参照してください。

次に、管理者として [シトリックスのダウンロードページ](#) の「`CitrixWorkspaceDesktopLock.msi`」を使って Citrix Workspace アプリ Desktop Lock をインストールします。

### システム要件

- Microsoft Visual C++ 2005 Service Pack 1 再頒布可能パッケージ。詳しくは、[Microsoft ダウンロードページ](#) を参照してください。
- Windows 7 (Embedded Edition を含む)、Windows 7 Thin PC、Windows 8、Windows 8.1、Windows 10 (Anniversary Update を含む) でサポートされます。
- ネイティブプロトコルのみを介して StoreFront に接続します。
- ドメイン参加のエンドポイントです。
- ユーザーデバイスをローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）に接続する必要があります。

### ローカルアプリアクセス

#### 重要

ローカルアプリアクセスを有効にすると、グループポリシーオブジェクトテンプレートまたは同様のポリシーでフルロックダウンが適用されていない限り、ローカルデスクトップアクセスを実行できます。詳しくは、Citrix Virtual Apps and Desktops ドキュメントの「[ローカルアプリアクセスと URL リダイレクトの構成](#)」セクションを参照してください。

### Citrix Workspace アプリ Desktop Lock の使用

- Citrix Workspace アプリ Desktop Lock では次の Citrix Workspace アプリの機能を実行できます。
  - 3Dpro、Flash、USB、HDX Insight、Microsoft Lync 2013 プラグイン、およびローカルアプリアクセス
  - ドメイン、2 要素、またはスマートカード認証のみ
- Citrix Workspace アプリ Desktop Lock セッションを切断すると、エンドデバイスがログアウトされます。
- Flash のリダイレクトは Windows 8 以降では無効です。Windows 7 では有効です。
- Desktop Viewer は Home、Restore、Maximize、および Display の各プロパティが未設定の Citrix Workspace アプリ Desktop Lock に最適化されています。
- Desktop Viewer のツールバーでは、Ctrl+Alt+Del キーの組み合わせを使用できます。
- Windows+L キー以外のほとんどの Windows ショートカットキーをリモートセッションで実行できます。
- 接続を無効にするまたはデスクトップ接続の Desktop Viewer を無効にする場合、Ctrl+F1 キーを押すと Ctrl+Alt+Del を押すのと同じように動作します。

#### 注:

Desktop Lock がインストールされ、LiveInDesktopDisconnectOnLockがレジストリパス `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` または `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` で **False** に設定されている場合、エンドポイントが休止状態またはスタンバイモードから復帰すると、アクティブなセッションが切断されます。

### Citrix Workspace アプリ Desktop Lock のインストール

この手順では、Citrix Workspace アプリ Desktop Lock を使用して仮想デスクトップが表示されるように、Windows 向け Citrix Workspace アプリをインストールします。スマートカードを使用する展開については、「[スマートカード](#)」を参照してください。

1. ローカルの管理者アカウントを使用してログオンします。
2. コマンドプロンプトで次のコマンドを実行します（インストールメディアの Citrix Workspace アプリおよびプラグイン > Windows > Citrix Workspace アプリフォルダーにあります）。

たとえば、次のようになります：

```
1 CitrixWorkspaceApp.exe
```

```
2     /includeSSON
3     STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
        discovery;on;Desktop Store"
4     <!--NeedCopy-->
```

コマンドについて詳しくは、Citrix Workspace アプリのインストールに関するドキュメント ([インストール](#)) を参照してください。

3. インストールメディアの同じフォルダーにある `CitrixWorkspaceDesktopLock.msi` をダブルクリックします。Desktop Lock ウィザードが開きます。画面の指示に従って操作します。
4. インストールが完了したら、ユーザーデバイスを再起動します。デスクトップへのアクセスが許可されていて、ドメインユーザーとしてログオンすると、Citrix Workspace アプリ Desktop Lock でデスクトップが表示されます。

ただし、インストールの完了後にユーザーデバイスを管理できるようにするため、`CitrixWorkspaceDesktopLock.msi` をインストールしたときのアカウントでは代替シェルが使用されません。このアカウントを削除すると、デバイスにログオンして管理することができなくなります。

Citrix Workspace アプリ Desktop Lock のサイレントインストールを実行するには、次のコマンドラインを使用します。

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

## Citrix Workspace アプリ Desktop Lock の構成

非管理者としてログインすると、Desktop Lock は割り当てられたデスクトップセッションを自動的に起動します。

Active Directory ポリシーを使用して、ユーザーが仮想デスクトップを休止状態にできないようにします。

Citrix Workspace アプリ Desktop Lock を構成するときは、インストール時に使用した管理者アカウントを使用します。

- `receiver.admx` (または `receiver.adml`) と `receiver_usb.admx` (`.adml`) ファイルがグループポリシーにロードされていることを確認します (ポリシーは [コンピューターの構成] または [ユーザーの構成] > [管理用テンプレート] > [従来の管理用テンプレート (ADMX)] > [Citrix コンポーネント] の順に展開すると表示されます)。これらの `.admx` ファイルは、`%Program Files%\Citrix\ICA Client\Configuration\` にインストールされています。
- **USB 基本設定** - ユーザーが USB デバイスを接続すると、そのデバイスは自動的に仮想デスクトップで使用可能になります。このとき、ユーザーが何らかの操作を行う必要はありません。USB ドライブの制御と表示は、仮想デスクトップにより処理されます。
  - USB ポリシー規則を有効にします。
  - [Citrix Workspace アプリ]、[クライアントデバイスをリモート処理します]、[一般的な USB のリモート処理] の順に選択して、Existing USB Devices と New USB Devices ポリシーを有効にして構成します。

- ドライブマッピング - [Citrix Workspace アプリ]、[クライアントデバイスをリモート処理します] の順に選択して、Client drive mapping ポリシーを有効にして構成します。
- マイク - [Citrix Workspace アプリ]、[クライアントデバイスをリモート処理します] の順に選択して、Client microphone ポリシーを有効にして構成します。

## Desktop Lock を実行する Windows デバイスでのスマートカードの使用を構成

1. StoreFront を構成します。
  - a) Citrix XML Service の DNS アドレス解決を有効にして、Kerberos 認証を使用できるように構成します。
  - b) StoreFront サイトの HTTPS アクセスを構成して、ドメインの証明機関による署名付きのサーバー証明書を作成し、デフォルトの Web サイトに HTTPS バインドを追加します。
  - c) [スマートカードパススルー認証] が有効になっていることを確認します（デフォルトで有効になっています）。
  - d) [Kerberos] を有効にします。
  - e) [Kerberos] および [スマートカードパススルー認証] を有効にします。
  - f) IIS の Default Web Site で [匿名アクセス] を有効にして、[統合 Windows 認証] を使用します。
  - g) IIS の Default Web Site の SSL 設定で [SSL が必要] チェックボックスがオフで、[クライアント証明書] で [無視] が選択されていることを確認します。
2. グループポリシー管理コンソールを使用して、ユーザーデバイスでローカルコンピューターのポリシーを構成します。
  - a) %Program Files%\Citrix\ICA Client\Configuration\ から Receiver.admx テンプレートをインポートします。
  - b) [管理用テンプレート] > [従来の管理用テンプレート (ADMX)] > [Citrix コンポーネント] > [Citrix Workspace] > [ユーザー認証] の順に展開します。
  - c) [スマートカード認証] を有効にします。
  - d) [ローカルユーザー名とパスワード] を有効にします。
3. Citrix Workspace アプリ Desktop Lock をインストールする前に、ユーザーデバイスを構成します。
  - a) Windows Internet Explorer の信頼済みサイトの一覧に、Delivery Controller の URL を追加します。
  - b) Windows Internet Explorer の信頼済みサイトの一覧に、最初のデリバリーグループの URL を「desktop://delivery-group-name」形式で追加します。
  - c) 信頼済みサイトに対する Internet Explorer の自動ログオン機能を有効にします。

Citrix Workspace アプリ Desktop Lock がユーザーデバイスにインストールされている場合、スマートカード取り出し時の動作に競合が生じないようにポリシーが適用されます。たとえば、Windows のスマートカードの取り出しポリシーがデスクトップで強制ログオフに設定されている場合、Windows のスマートカードの取り出しポリシーが設定されているかどうかにかかわらず、ユーザーはユーザーデバイスからもログオフする必要があります。これにより、ユーザーデバイスの整合性が維持されます。これは、Citrix Workspace アプリ Desktop Lock が有効なユーザーデバイスにのみ適用されます。

## Desktop Lock の削除

以下のコンポーネントを両方ともアンインストールする必要があります。

1. Citrix Workspace アプリ Desktop Lock のインストールと構成に使用したローカル管理者アカウントでログオンします。
2. プログラムの削除や変更を行うための Windows 機能（コントロールパネルの [プログラムと機能] など）を開き、以下の操作を行います：
  - Citrix Workspace アプリ Desktop Lock をアンインストールします。
  - Windows 向け Citrix Workspace アプリをアンインストールします。

## リモートセッションでの **Windows** ショートカットキーの実行

ほとんどの Windows ショートカットキーはリモートセッションで実行できます。このセクションでは、一般的なものについていくつか説明します。

## Windows

- Win+D - すべてのウィンドウをデスクトップ上で最小化します。
- Alt+Tab - アクティブなウィンドウを変更します。
- Ctrl+Alt+Delete - Ctrl+F1 および Desktop Viewer ツールバーを介します。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+ すべての文字キー

## Windows 8

- Win+C - チャームを開きます。
- Win+Q - チャームを検索します。
- Win+H - チャームを共有します。
- Win+K - デバイスのチャーム。
- Win+I - 設定のチャーム。
- Win+Q - アプリを検索します。
- Win+W - 設定を検索します。
- Win+F - ファイルを検索します。

## Windows 8 のアプリ

- Win+Z - アプリのオプションを開きます。
- Win+. - アプリを左にスナップします。

- Win+Shift+. - アプリを右にスナップします。
- Ctrl+Tab - アプリ履歴を循環させます。
- Alt+F4 - アプリを閉じます。

### デスクトップ

- Win+D - デスクトップを開きます。
- Win+, - デスクトップでプレビューします。
- Win+B - デスクトップに戻ります。

### その他

- Win+U - コンピューターの簡単操作センターを開きます。
- Ctrl+Esc - 画面を開始します。
- Win+Enter - Windows ナレーターを開きます。
- Win+X - システムユーティリティ設定メニューを開きます。
- Win+PrintScrn - スクリーンショットを取りピクチャに保存します。
- Win+Tab - スイッチ一覧を開きます。
- Win+T - タスクバーの開いているウィンドウをプレビューします。

## SDK および API

March 25, 2021

### Certificate Identity Declaration SDK

Certificate Identity Declaration SDK (CID) を使用すると、Citrix Workspace アプリがクライアントマシンにインストールされている証明書を使用して StoreFront サーバーに認証できるプラグインを開発者が作成できます。CID は、スマートカードベースの認証を実行せずに、ユーザーのスマートカード ID を StoreFront サーバーに宣言します。

CID SDK を使用すると、Citrix Workspace アプリがクライアントマシンにインストールされている証明書を使用して StoreFront サーバーに認証できるユーティリティを開発者が作成できます。

詳しくは、[Certificate Identity Declaration SDK for Citrix Workspace app for Windows](#)のドキュメントを参照してください。

## Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK は、基本的な操作をプログラマ的にやりとりして実行できるネイティブ API のセットを提供します。この SDK は、Windows 向け Citrix Workspace アプリインストールパッケージの一部であるため、別途ダウンロードする必要はありません。

注:

起動に関連する API によっては、Citrix Virtual Apps and Desktops セッションの起動プロセスの開始に ICA ファイルが必要な場合があります。

CCM SDK の機能は次のとおりです。

- セッションの起動
  - 生成された ICA ファイルを使用してアプリケーションおよびデスクトップを起動できます。
- セッションの切断
  - コネクションセンターを使用した切断と同様の操作です。切断は、すべてのセッションまたは特定のユーザーに対して行うことができます。
- セッションのログオフ
  - コネクションセンターを使用したログオフと同様の操作です。ログオフは、すべてのセッションまたは特定のユーザーに対して行うことができます。
- セッション情報
  - 起動されたセッションの接続関連情報を取得するさまざまな方法を提供します。対象となるのは、デスクトップセッション、アプリケーションセッション、リバースシームレスアプリケーションセッションなどです。

SDK のドキュメントについては、[Programmers guide to Citrix CCM SDK](#)を参照してください。

## Citrix 仮想チャネル SDK

Citrix 仮想チャネルソフトウェア開発キット (SDK) は、ICA プロトコルを使用する追加の仮想チャネルのための、サーバー側アプリケーションやクライアント側ドライバの作成をサポートします。サーバー側仮想チャネルアプリケーションは、Citrix Virtual Apps and Desktops サーバー上にあります。他のクライアントプラットフォーム用の仮想ドライバの作成については、Citrix テクニカルサポートにお問い合わせください。

仮想チャネル SDK には、以下のものが用意されています。

- Citrix Server API SDK (WFAPI SDK) の仮想チャネル機能とともに使用して新しい仮想チャネルを作成する、Citrix Virtual Driver Application Programming Interface (VD-API)。VD-API によって提供される仮想チャネルサポートは、独自の仮想チャネルを容易に作成できるように設計されています。
- 視覚的要素を強化し、ICA と統合されたサードパーティアプリケーションをサポートする Windows Monitoring API。
- プログラミングテクニックの実例となる仮想チャネルサンプルプログラムの、実際に機能するソースコード。
- 仮想チャネル SDK では、WFAPI SDK で仮想チャネルのサーバー側を作成する必要があります。

詳しくは、[Citrix Virtual Channel SDK for Citrix Workspace app for Windows](#)のドキュメントを参照してください。

### **Fast Connect 3 Credential Insertion API**

Fast Connect 3 Credential Insertion API は、Windows 向け Citrix Workspace アプリ 4.2 以降のシングルサインオン (SSO) 機能に対してユーザーの資格情報を提供するインターフェイスです。この API を使用すると、Citrix パートナーは、StoreFront を使用して仮想アプリケーションまたはデスクトップにユーザーをログオンさせ、その後でそれらのセッションからユーザーを切断する、認証や SSO にかかわる製品を提供できます。

詳しくは、[Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#)のドキュメントを参照してください。

### **ICA 設定リファレンス**

February 11, 2021

ICA 設定リファレンスファイルは、レジストリ設定および ICA ファイル設定のリストを提供し、管理者は環境に対して Citrix Workspace アプリの動作を高度にカスタマイズできます。また、ICA 設定リファレンスを使用して、予期しない Citrix Workspace アプリの動作をトラブルシューティングできます。

[ICA 設定リファレンス \(PDF のダウンロード\)](#)



**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States  
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).