CITRIX

Citrix Receiver for Windows 4.12

Contents

新機能

January 9, 2019

4.12 の新機能

暗号キットの更新

このリリースには、TLS/DTLS セキュア通信プロトコルに関する次の 2 つの重要な変更が含まれています。**DTLS** バージョン **1.2** のサポート、および Forward Secrecy を提供しない TLS/DTLS 暗号の組み合わせの廃止。

DTLS バージョン 1.2 は、UDP トランスポートプロトコルをサポートし、TCP トランスポートプロトコル用の TLS バージョン 1.2 に相当する機能を提供します。Receiver for Windows の以前のバージョンでは、既に TLS バージョン 1.2 がサポートされていました。

接頭辞が **TLS_RSA_** の暗号の組み合わせは、Forward Secrecy を提供しません。これらの暗号の組み合わせは現在業界では推奨されていません。ただし、以前のバージョンの XenApp および XenDesktop との後方互換性をサポートするために、Receiver for Windows ではこれらの暗号の組み合わせを利用できます。

非推奨の暗号の組み合わせを使用できるように、新しいグループポリシーオブジェクト管理用テンプレートが作成されました。Receiver for Windows バージョン 4.12 では、このポリシーはデフォルトで有効になっていますが、AES または 3DES アルゴリズムを使用した場合、デフォルトでこれらの非推奨の暗号の組み合わせを適用することはありませんただし、このポリシーを変更して使用することにより、非推奨をより厳密に適用することができます。

以下は、非推奨の暗号の組み合わせの一覧です:

1. TLS_RSA_AES256_GCM_SHA384
2. TLS_RSA_AES128_GCM_SHA256
3. TLS_RSA_AES256_CBC_SHA256
4. TLS_RSA_AES256_CBC_SHA
5. TLS_RSA_AES128_CBC_SHA
6. TLS_RSA_3DES_CBC_EDE_SHA
7. TLS_RSA_WITH_RC4_128_MD5
8. TLS_RSA_WITH_RC4_128_SHA

> 注
>
> 最後の 2 つの暗号の組み合わせは RC4 アルゴリズムを使用しますが、安全ではないため推奨されていません。また、**TLS_RSA_3DES_CBC_EDE_SHA** 暗号の組み合わせを非推奨にすることも検討してください。このポリシーを使用して、これらすべての非推奨を適用することができます。

DTLS v1.2 を構成する方法について詳しくは、「アダプティブトランスポート」のドキュメントを参照してください。

非推奨の暗号の組み合わせの構成については、「廃止された暗号の組み合わせの構成」を参照してください。

バッテリーアイコンの通知

セッションのホスト通知領域にバッテリーが表示され、クライアントのバッテリー情報が表示されます。

この機能は、バージョン 7.18 以降で動作する VDA にのみ適用されます。

高速スマートカード

スマートカードを高遅延の WAN シナリオで使用すると、高速スマートカードのパフォーマンスが向上します。高速スマートカードは、Windows Server 2012、Windows Server 2016、または Windows 10 以降を実行しているホストではデフォルトで有効になっています。クライアント側で高速スマートカードを有効にするには、default.ica ファイルに **SmartCardCryptographicRedirection** パラメーターを構成します。

Web カメラのプラグアンドプレイ

アプリケーションは、クライアント上で Web カメラが接続または接続解除されたことを動的に検出します。ユーザーは、これらの変更を検出するためにアプリケーションを再起動する必要はありません。

Citrix Analytics のサポート

Citrix Receiver for Windows アプリには、ログを Citrix Analytics に安全に送信するための機能があります。有効になっている場合、ログは分析され、Citrix Analytics 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。

解決された問題

February 21, 2019

Citrix Receiver for Windows 4.12

修正前のバージョン：Citrix Receiver for Windows 4.11

HDX MediaStream Flash リダイレクト

- HDX MediaStream Flash リダイレクトの設定を有効にすると、セッションを切断した時 PseudoContainer2.exe プロセスが予期せず終了することがあります。[#LC8802]

キーボード

- StoreFront からダウンロードされた APPSRV.INI または ICA ファイルを使用して、サーバーのデフォルトまたは選択したキーボードレイアウトを使用しようとすると、失敗することがあります。

  以下は、このシナリオの制限事項です。

  - 以前にレイアウトを設定した場合でも、最初に設定する時には、コントロールパネルからセッションで手動でキーボードレイアウトを設定する必要があります。
  - キーボードレイアウトの同期を、［高度な設定］ で ［いいえ］ に設定する必要があります。レイアウトを ［はい］ に設定すると、ローカル IME がリダイレクトされます。[#LC9593]

セッション/接続

- Microsoft Internet Explorer 11 を使用してデスクトップを起動しようとすると、次のエラーメッセージが表示されることがあります:

  「The connection to <published_desktop> failed with status (Unknown client error 0).」[#LC8841]

- StoreFront の 2 つのサイト間でアグリゲーションをセットアップすると、起動前セッションは作成されません。[#LC8847]
- 特定の DVD ビデオは、マップされたクライアントドライブを経由するとセッション内で再生されないことがあります。[#LC8912]
- 第 1 ホップが VDA for Desktop OS、第 2 ホップが VDA 内で起動されるアプリケーションのダブルホップ環境では、VDA for Desktop OS を実行している最初のホップに再接続すると、数秒間画面がちらつくことがあります。[#LC9071]
- 双方向コンテンツを VDA にリダイレクトすると、ブラウザーが既に開いている場合、2 番目の URL が新しいブラウザーで開きます。[#LC9157]
- アプリケーションを起動すると、Citrix Receiver for Windows が「接続中です...」と表示して起動できないことがあります。次のエラーメッセージが表示されます:

  「The published resource is not available currently. Contact your system administrator for assistance.」[#LC9170]

- Citrix Receiver for Windows を使用してウィンドウモードおよび非シームレスモードでセッションを開始すると、灰色の画面が表示されることがあります。この問題は、ICA ファイルの解像度がクライアントのエンドポイントの解像度よりも大きい場合に発生します。[#LC9266]
- Citrix Receiver for Mac からアプリケーションを起動できないことがあります。この問題は、クライアントライセンス（LicenseRequestClientLicense）を取得できない場合に発生します。[#LC9286]
- Citrix Receiver for Windows を使用してデスクトップを起動しようとすると失敗することがあります。StoreFront を使用して **LaunchTimeoutMs** で起動時間を長く設定した場合でも、この問題が発生します。[#LC9369]

- VDA for Server OS 上で実行されている公開アプリケーションでクリップボードのクリアまたは削除を選択すると、VDA クリップボードはクリアされますが、テキストはエンドポイントのクリップボードに残ります。[#LC9434]
- System Center Configuration Manager（SCCM）を使用して Citrix Receiver for Windows をアップグレードすると、Receiver for Windows がシステムの再起動を要求することがあります。[#LC9706]
- System Center Configuration Manager（SCCM）または PSExec 経由で Citrix Receiver for Windows をインストールすると、無人インストールが行われることがあります。[#RFWIN-8188]

スマートカード

- スマートカード認証を使用して公開デスクトップを全画面モードで起動しようとすると、Desktop Viewer に PIN プロンプトが表示されないことがあります。[#LC8579]

システムの例外：

- タッチ操作可能なデバイスを使用して VDA に接続すると、wfica32 プロセスが断続的に終了することがあります。[#LC9228]
- wfica32.exe プロセスが断続的に終了することがあります。[#LC9397]

ユーザーエクスペリエンス：

- グラフィックのハードウェアアクセラレーションを有効にして公開デスクトップを起動すると、Desktop Viewer の灰色のプレビューがツールバーに表示されることがあります。[#LC8545]
- デスクトップの起動後すぐにデスクトップが非表示になることがあります。この問題は、Citrix Receiver for Windows から送信された TLS パケットが重複しているため発生します。[#LC8724]
- Citrix Receiver for Windows 内のアプリケーションを更新すると、［スタート］メニューとタスクバーアイコンがちらついて表示されることがあります。[#LC8890]
- H.265 ビデオコーデックを使用して公開デスクトップを起動すると、公開デスクトップの画面に緑色が表示されます。[#LC9083]
- Citrix Receiver for Windows を Citrix XenApp Services サイトとともに使用すると、アプリケーションとアイコンがファイルの種類に部分的に関連付けられることがあります。[#LC9402]
- ［キーボードと言語バー］ ページで ［いいえ。サーバーのキーボードレイアウトを使用します。］ を選択すると、キーボードレイアウトの同期が動的にサポートされないことがあります。［はい］ を選択すると、キーボードレイアウトの同期が動的にサポートされます。ただし、キーボードレイアウトは、どちらの場合でも最初の接続時には同期されます。[#RFWIN-7999]
- 64 ビットマシンで、%ProgramFiles% のレジストリエントリがあるアプリケーションの 32 ビットインスタンスを起動すると、エントリは C:\Program File に展開されますが、C:\Program Files (X86)\には展開されません。その結果、アプリケーションの 32 ビットインスタンスの起動がサーバーインスタンスの起動にフォールバックし、アプリケーションの vPrefer が失敗します。[#RFWIN-8025]

その他

- この修正では、Enlightened Data Transport（EDT）のパフォーマンスおよび品質のマイナーな強化に対応しています。[#LC9417]

注：このバージョンの Citrix Receiver for Windows には、4.11、4.10.1、4.10、4.9、4.8、4.7、4.6、4.5、4.4の各バージョンに含まれるすべての修正も入っています。

既知の問題

January 9, 2019

Citrix Receiver for Windows 4.12 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。

Citrix Receiver for Windows 4.12 には、バージョン4.5、4.6、4.7、4.8、4.9、4.10、4.11に存在していた既知の問題の一部が含まれています。

サードパーティ製品についての通知

November 12, 2018

Citrix Receiver for Windows 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。

Citrix Receiver for Windows のサードパーティ製品についての通知

システム要件と互換性

March 18, 2019

要件

- このバージョンの Citrix Receiver for Windows では、少なくとも 500MB のディスク空き容量と 1GB の RAM が必要です。

- .NET Framework の最小要件
  - Self-Service plug-in には、.NET 3.5 Service Pack 1 が必要です。これにより、Receiver 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ケーション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を使用した Receiver for Windows の構成とインストール」を参照してください。
  - .NET 2.0 Service Pack 1。

互換性マトリックス

Citrix Receiver for Windows は、以下の Windows オペレーティングシステムおよび Web ブラウザーと互換性があります。また、シトリックス製品ライフサイクルマトリックスの一覧にある、XenApp、XenDesktop、NetScaler Gateway の最新のサポート対象バージョンとも互換性があります。

> 注
>
> NetScaler Gateway End Point Analysis Plugin（EPA）はネイティブの Citrix Receiver for Windows をサポートしません。

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（Embedded エディションを含む）
Windows 7 32 ビット版および 64 ビット版（Embedded エディションを含む）
Windows Thin PC
Windows Server 2016
Windows Server 2012 R2、Standard および Datacenter エディション
Windows Server 2008 R2（64 ビット版）
Windows Server 2019
Windows 10 Enterprise 2016 LTSB 1607

*Windows 10 バージョン 1607、1703、1709、1803 をサポート。

Web ブラウザー

Web ブラウザー
Internet Explorer
最新版の Google Chrome（StoreFront 必須）

Web ブラウザー
最新版の Mozilla Firefox
Microsoft Edge

サポートに関するマトリックス

タッチデバイスでサポートされるオペレーティングシステム	VDA でサポートされるオペレーティングシステム
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2
	Windows Server 2016
	Windows 2008 R2

接続、証明書、認証

April 2, 2019

接続

- HTTP ストア
- HTTPS ストア
- NetScaler Gateway 10.5 以降
- Web Interface 5.4

証明書

- 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、アプリケーションの一覧が表示されますが、アプリケーションの起動に失敗することがあります。

ルート証明書のインストール

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 Receiver for Windows はワイルドカード証明書をサポートしますが、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を考慮することがあります。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 NetScaler 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、Configuring Intermediate Certificatesを参照してください。

認証

StoreFront での認証

	ブラウザーを使った **Receiver for Web**	**StoreFront** サービスサイト（ネイティブ）	**StoreFront XenApp** および **XenDesktop** サイト（ネイティブ）	**NetScaler** から **Receiver for Web**（ブラウザー）	**NetScaler** から **StoreFront Services** サイト（ネイティブ）
匿名	はい	はい			
ドメイン	はい	はい	はい	はい *	はい *
ドメインパススルー	はい	はい	はい		
セキュリティトークン				はい *	はい *
2 要素認証（ドメイン + セキュリティトークン）				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（NetScaler のプラグイン）	はい（NetScaler のプラグイン）

* デバイスへの NetScaler プラグインのインストールは不問。

> 注
>
> Citrix Receiver for Windows は、NetScaler 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。

Web Interface での認証

Citrix Receiver for Windows は次の認証方法をサポートします（Web Interface ではドメインおよびセキュリティトークン認証に明示的という用語を使用します）：

	Web Interface（ブラウザー）	**Web Interface XenApp** および **XenDesktop** サイト	**NetScaler** から **Web Interface**（ブラウザー）	**NetScaler** から **Web Interface XenApp** および **XenDesktop** サイト
匿名	はい			
ドメイン	はい	はい	はい *	
ドメインパススルー	はい	はい		
セキュリティトークン			はい *	
2 要素認証（ドメイン + セキュリティトークン）			はい *	
SMS			はい *	
スマートカード	はい	はい		
ユーザー証明書			はい（NetScaler のプラグイン）	

* NetScaler Gateway が動作する環境でのみ使用できます（デバイスへのゲートウェイプラグインソフトウェアのインストールは不要）。

認証については、NetScaler Gateway のドキュメントで「Configuring Authentication and Authorization」、StoreFront のドキュメントで「管理」のトピックを参照してください。

Web Interface でサポートされる認証方法については、Web Interface に関するドキュメントを参照してください。

インストール

January 9, 2019

CitrixReceiver.exe のインストールパッケージは、以下のどの方法でもインストールできます。

- Citrix.com または管理者が作成したダウンロードサイトからのインストール
  - 初めて使用するユーザーが Citrix Receiver for Windows のインストールファイルを Citrix.com などのダウンロードサイトから入手した場合は、サーバー URL の代わりにメールアドレスを入力してアカ

ウントをセットアップできます。これにより、メールアドレスに関連付けられた NetScaler Gateway や StoreFront サーバーが識別され、ログオン用のメッセージが表示されてインストールを続行します。この機能は、「メールアドレスによるアカウント検出」と呼ばれます。
注：初めて使用するユーザーとは、デバイスに Citrix Receiver for Windows をインストールしていないユーザーを指します。
注：Citrix.com 以外の場所（Receiver for Web サイトなど）から Citrix Receiver for Windows をダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。
  - Citrix Receiver for Windows の構成が必要な環境では、ほかの方法で Receiver をユーザーに配布してください。
- Receiver for WebサイトまたはWeb Interface のログイン画面からの自動インストール
  - 初めて使用するユーザーがアカウントをセットアップするには、サーバーの URL を入力するかプロビジョニング（CR）ファイルをダウンロードします。
- ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールによるインストール
  - 初めて使用するユーザーがアカウントをセットアップする場合、サーバーの URL を入力するかプロビジョニングファイルを開く必要があります。

パススルー認証を使用しない場合、Citrix Receiver for Windows のインストールに管理者権限は不要です。

Citrix Receiver for Windows の整合性の確認

Citrix Receiver for Windows 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。

管理者権限と非管理者権限によるインストール

管理者が実行した Citrix Receiver for Windows のインストールと、（管理者以外の）ユーザーが実行したインストールの間には、次の相違点があります。

	管理者	ユーザー
インストールフォルダー	C:\Program Files (x86)\Citrix\ICA Client	%USERPROFILE%\AppData\Local\Citrix\ICA Client
インストールの種類	システムごとのインストール	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 Receiver for Windows インスタンスがシステム上に存在し、管理者が Citrix Receiver for Windows を同じシステムにインストールすると、競合が発生します。Citrix Receiver for Windows を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 Receiver

> for Windows インスタンスをアンインストールすることをお勧めします。

Citrix Receiver for Windows の手動アップグレード

StoreFront 環境:

- BYOD（Bring Your Own Device）ユーザー（私的デバイス活用ユーザー）のベストプラクティスについては、製品ドキュメントのサイトでドキュメントを参照しながら最新バージョンの NetScaler Gateway および StoreFront を構成してください。StoreFront により作成されたプロビジョニングファイルをメールに添付して、アップグレード方法および Citrix Receiver for Windows のインストール後にプロビジョニングファイルを開く方法をユーザーに通知します。
- プロビジョニングファイルをユーザーに送信できない場合は、NetScaler Gateway の URL を入力するように指示します。また、StoreFront のドキュメントで説明されているメールアドレスによるアカウント検出を構成済みの場合は、自分のメールアドレスを入力するようにユーザーに指示します。
- また、Citrix Receiver for Web サイトを構成（StoreFront のドキュメントを参照）し、「Citrix Receiver for Web サイトからの Citrix Receiver for Windows の配布」の説明に従って構成を完了する方法もあります。Citrix Receiver for Windows のアップグレード方法、Citrix Receiver for Web サイトへのアクセス方法、Citrix Receiver for Web サイトからのプロビジョニングファイルのダウンロード方法（ユーザー名をクリックして［アクティブ化］をクリック）をユーザーに通知します。

Web Interface で展開する場合

- Citrix Receiver for Windows で Web Interface サイトをアップグレードし、「Web Interface のログオン画面からの Citrix Receiver for Windows の配布」で説明されている構成を完了します。Citrix Receiver for Windows のアップグレード方法をユーザーに通知します。たとえば、ユーザーが Citrix Receiver インストーラーを入手するためのダウンロードサイトを作成して、そこに名前を変更したインストーラーを配置します。

アップグレード時の注意事項

Citrix Receiver for Windows をアップグレードする前の考慮事項については、Knowledge Center のCTX135933を参照してください。

HDX RealTime Media Engine（RTME）

単一のインストーラーでは、最新の Citrix Receiver for Windows と HDX RTME インストーラーが結合されています。実行可能ファイル（.exe）を使用して Citrix Receiver をインストールすると、HDX RTME もインストールされます。

HDX RealTime Media Engine がインストールされていて、Citrix Receiver for Windows をアンインストールして、再インストールする場合、HDX RTME のインストールと同じモードを使用するようにしてください。

> 注
>
> RTME サポートが統合された最新バージョンの Citrix Receiver のインストールには、ホストマシンの管理者権限が必要です。

Citrix Receiver for Windows をインストールまたはアップグレードする場合は、HDX RTME に関して次の点のご注意ください。

- 最新バージョンの Citrix ReceiverPlusRTME には HDX RTME が含まれているため、別途 RTME をインストールする必要はありません。
- 前バージョンの Citrix Receiver for Windows から最新のバンドルバージョン (RTME を含む Citrix Receiver) へのアップグレードに対応しています。以前インストールされた RTME のバージョンは、最新バージョンに上書きされます。同じ Citrix Receiver for Windows のバージョンから最新のバンドルバージョンへのアップグレード（例: Receiver 4.7 から RTME がバンドルされた Receiver 4.7）はサポートしていません。
- 以前のバージョンの RTME をお持ちの場合、最新バージョンの Citrix Receiver for Windows をインストールすることにより、クライアントデバイスの RTME も自動的に更新されます。
- 最新バージョンの RTME がインストール済みであれば、インストーラーはそのバージョンを保持します。

> 重要
>
> HDME RealTime Connector は、新しい RTME パッケージとの互換性のために、バージョン 2.0.0.417 以降である必要があります。つまり、1.8 RTME Connector で RTME 2.0 を使用することはできません。

コマンドラインパラメーターを使用した構成とインストール

April 2, 2019

コマンドラインオプションを指定して、Citrix Receiver for Windows のインストーラーをカスタマイズします。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ユーザー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。

システム要件について詳しくは、「システム要件」を参照してください。

コマンドプロンプトから Citrix Receiver for Windows をインストールするには、次の構文を使用します:

CitrixReceiver.exe [<options>]

Receiver の更新

オプション	/AutoUpdateCheck = auto/manual/disabled
説明	Citrix Receiver for Windows が、利用可能な更新を検出したことを示します。**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てください。**Disabled** - 自動更新を無効にします。
使用サンプル	CitrixReceiver.exe /AutoUpdateCheck = auto、CitrixReceiver.exe /AutoUpdateCheck = manual、CitrixReceiver.exe /AutoUpdateCheck = disabled

オプション	/AutoUpdateStream= LTSR/Current
説明	Citrix Receiver for Windows のリリースの種類を示します。**LTSR** - リリースが長期サービスリリースであることを示します。**Current** - リリースが Citrix Receiver for Windows の最新バージョンであることを示します。
使用サンプル	CitrixReceiver.exe /AutoUpdateStream= LTSR 、CitrixReceiver.exe /AutoUpdateStream= Current

オプション	/DeferUpdateCount
説明	Citrix Receiver for Windows のリリースの種類を示します。**-1** - 任意の回数通知を保留できます（デフォルト値 =-1）。**0** - ［後で通知する］オプションは表示されません。その他の数字 - この回数分、［後で通知する］オプションが表示されます。たとえば、値を 10 に設定すると、［後で通知する］オプションが 10 回表示されます。
使用サンプル	CitrixReceiver.exe /DeferUpdateCount=-1 、CitrixReceiver.exe /DeferUpdateCount=-0、CitrixReceiver.exe /DeferUpdateCount=** その他の数字 >

オプション	/AURolloutPriority
説明	ロールアウトを行うことができるタイミングを示します。**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。
使用サンプル	CitrixReceiver.exe /AURolloutPriority=Fast 、CitrixReceiver.exe /AURolloutPriority=Medium、CitrixReceiver.exe /AURolloutPriority=Slow

コンテンツの双方向リダイレクトの有効化

> 注
>
> デフォルトで、サーバーにコンテンツの双方向リダイレクトのコンポーネントが既にインストールされている場合、Citrix Receiver for Windows はそれらをインストールしません。クライアントマシンとして XenDesktop を使用している場合、/FORCE_LAA スイッチを使用して Citrix Receiver for Windows をインストールすることでコンテンツの双方向リダイレクトのコンポーネントをインストールする必要があります。ただし、この機能は、サーバーとクライアントの両方で構成されている必要があります。

オプション	ALLOW_BIDIRCONTENTREDIRECTION=1
説明	「クライアントからホスト」と「ホストからクライアント」の間でのコンテンツの双方向リダイレクトを有効化します。
使用サンプル	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

設定オプションの非表示

オプション	/DisableSetting
説明	［高度な設定］ダイアログボックスで［設定オプション］が表示されないようにします。
使用サンプル	CitrixReceiver.exe /DisableSetting=3

［設定オプション］に［アプリケーションの表示］と［再接続オプション］の両方を表示するには	CitrixReceiver.exe /DisableSetting=0 と入力する
［高度な設定］ダイアログボックスで［設定オプション］を非表示にするには	CitrixReceiver.exe /DisableSetting=3 と入力する
［設定オプション］に［アプリケーションの表示］のみを表示するには	CitrixReceiver.exe /DisableSetting=2 と入力する
［設定オプション］に［再接続オプション］のみを表示するには	CitrixReceiver.exe /DisableSetting=1 と入力する

ローカルアプリアクセスの有効化

オプション	FORCE_LAA=1
説明	デフォルトで、サーバーに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既にインストールされている場合、Citrix Receiver for Windows はそれらのコンポーネントをインストールしません。Citrix Receiver 上に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を強制的にインストールするには、FORCE_LAA コマンドラインスイッチを使用します。この手順を実行するには管理者レベルの権限が必要です。ローカルアプリアクセスについては、XenApp および XenDesktop のドキュメントで「ローカルアプリアクセス」を参照してください。
使用サンプル	CitrixReceiver.exe /FORCE_LAA =1

使用方法情報の表示

オプション	/? または/help
説明	使用方法情報を表示します
使用サンプル	CitrixReceiver.exe /?、CitrixReceiver.exe /help

UI インストール時の再起動の抑制

オプション	/noreboot
説明	UI インストール時に再起動を抑制します。サイレントインストールを行う場合、このオプションを指定する必要ありません。再起動されないようにする場合、Citrix Receiver for Windows のインストール時に一時停止状態だった USB デバイスは、ユーザーデバイスを再起動するまで Citrix Receiver for Windows で認識できません。
使用サンプル	CitrixReceiver.exe /noreboot

サイレントインストール

オプション	/silent
説明	エラーメッセージや進行状況を示すダイアログボックスが開かなくなり、完全なサイレントインストールを実行できます。
使用サンプル	CitrixReceiver.exe /silent

認証時のシングルサインオンの有効化

オプション	/includeSSON
説明	Citrix Receiver for Windows 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。コマンドラインで/includeSSON を指定すると、関連のオプション ENABLE_SSON が有効になります。ADDLOCAL= で機能を指定してシングルサインオン機能をインストールする場合は、値として SSON も指定する必要があります。ユーザーデバイスに対してパススルー認証を有効にするには、/includeSSON オプションを指定したコマンドラインからローカルの管理者権限で Citrix Receiver for Windows をインストールする必要があります。詳しくは、「手動でパススルー認証のためのインストールおよび構成 Citrix Receiver をする方法」を参照してください。注：スマートカード、Kerberos とローカルユーザー名、およびパスワードポリシーは相互依存しています。重要なのは、構成の順序です。最初に必要のないポリシーを無効にしてから、次に必要なポリシーを有効にすることをお勧めします。その結果について慎重に検証してください。
使用サンプル	CitrixReceiver.exe /includeSSON

/includeSSON の指定時にシングルサインオンを有効化

オプション	ENABLE_SSON={Yes、No}
説明	/includeSSON の指定時にシングルサインオンを有効にします。デフォルト値は Yes です。スマートカードによるシングルサインオンを有効にするには、このプロパティを指定する必要があります。有効にしたシングルサインオン認証は、インストール後にユーザーがデバイスにログオンし直すまで使用できません。管理者権限が必要です。
使用サンプル	CitrixReceiver.exe ENABLE_SSON=Yes

常時トレース

オプション	/EnableTracing={true、false}
説明	デフォルトでは、この機能は true に設定されています。このプロパティを使用して、常時トレース機能を有効化または無効化します。常時トレースは、接続時間に関する重大なログの収集に役立ちます。これらのログは断続的な接続の問題のトラブルシューティングに役立つことがあります。常時トレースポリシーによりこの設定は上書きされます。
使用サンプル	CitrixReceiver.exe /EnableTracing=true

カスタマーエクスペリエンス向上プログラム（**CEIP**）の使用

オプション	EnableCEIP={true、false}
説明	Citrix のカスタマーエクスペリエンス向上プログラム（CEIP）への参加を有効にすると、匿名の統計および使用状況情報が、シトリックス製品の品質およびパフォーマンスを向上させる目的で送信されます。
使用サンプル	CitrixReceiver.exe EnableCEIP=true

インストールディレクトリの指定

オプション	INSTALLDIR=** インストールディレクトリ >
説明	ほとんどの Citrix Receiver ソフトウェアがインストールされるインストールパスを指定します。デフォルト値は、C:\Program Files\Citrix\Receiver です。次の Receiver コンポーネントは C:\Program Files\Citrix にインストールされます: **Authentication Manager**、**Citrix Receiver**、**Self-service Plug-in** このオプションでを指定する場合は、\Receiver ディレクトリに RIInstaller.msi をインストールし、にほかの MSI ファイルをインストールする必要があります。インストールディレクトリ > インストールディレクトリ >
使用サンプル	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

ユーザーデバイスの識別

オプション	CLIENT_NAME=** クライアント名 >
説明	クライアント名を指定します。ここでは、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。デフォルト値は、%COMPUTERNAME% です。クライアント名 >
使用サンプル	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

ダイナミッククライアント名

オプション	ENABLE_CLIENT_NAME=Yes、No
説明	ダイナミッククライアント名機能を有効にすると、コンピューター名がクライアント名として使用されます。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。デフォルトは Yes です。ダイナミッククライアント名機能を無効にするには、このプロパティを No に設定し、CLIENT_NAME プロパティの値を指定します。
使用サンプル	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

指定したコンポーネントのインストール

オプション	ADDLOCAL=<feature… ,>
説明	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。複数のパラメーターを指定する場合は、以下の各パラメーターをスペースなしのコンマで区切ります。大文字と小文字は区別されます。このキーを指定しない場合、すべてのコンポーネントがデフォルトでインストールされます。以下の ADDLOCAL 使用サンプルを使用することをお勧めします。使用サンプルが説明どおりに使用されない場合、予期しない動作が発生することがあります。次のコンポーネントを使用できます：ReceiverInside - Citrix Workspace アプリエクスペリエンス（Workspace アプリの操作に必要なコンポーネント）をインストールします。ICA_Client - 標準の Citrix Workspace アプリ（Workspace アプリの操作に必要なコンポーネント）をインストールします。WebHelper - WebHelper コンポーネントをインストールします。このコンポーネントは ICA ファイルを StoreFront から取得して HDX エンジンに渡します。さらに、環境パラメーターを検証し Storefront と共有します。これは ICO クライアント検出と同様です。[オプション]SSON - シングルサインオン（パススルー認証）機能をインストールします。管理者権限が必要です。AM - Authentication Manager をインストールします。SELFSERVICE - Self-service Plug-in をインストールします。コマンドラインで AM 値を指定し、ユーザーデバイスに.NET Framework 3.5 Service Pack 1 をインストールする必要があります。Self-Service Plug-in は、.NET 3.5 をサポートしない Windows Thin PC デバイスでは使用できません。Self-service Plug-in（SSP）のスクリプト、および Receiver for Windows 4.2 以降で使用できるパラメーターについて詳しくは、Knowledge Center の CTX200337 を参照してください。このセクションの「仮想デスクトップやアプリケーションをコマンドラインで起動するには」で説明されているように、ユーザーは Self-service Plug-in を使用して Citrix Workspace アプリのウィンドウまたはコマンドラインから仮想デスクトップやアプリケーションにアクセスできます。USB - USB サポートをインストールします。管理者権限が必要です。DesktopViewer - Desktop Viewer をインストールします。Flash - HDX MediaStream for Flash をインストールします。Vd3d - Windows Aero エクスペリエンスを有効にします（Aero をサポートするオペレーティングシステムが対象です）。

オプション	ADDLOCAL=<feature… ,>
使用サンプル	CitrixReceiver.exe ADDLO- CAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

ストアを手動で追加するための **Citrix Receiver for Windows** の構成

オプション	ENABLE_CLIENT_NAME=Yes、No
説明	ダイナミッククライアント名機能を有効にすると、コンピューター名がクライアント名として使用されます。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。デフォルトは Yes です。ダイナミッククライアント名機能を無効にするには、このプロパティを No に設定し、CLIENT_NAME プロパティの値を指定します。
使用サンプル	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

PNAgent プロトコルを使用してストアの資格情報をローカルで保存

オプション	ALLOWSAVEPWD={N、S、A}
説明	デフォルトの値は、実行時に PNAgent サーバーから指定される値です。ユーザーがストアの資格情報をコンピューター上に保存することを許可するかどうかを指定します。この設定は、PNAgent プロトコルを使用するストアにのみ適用されます。デフォルトは S です。次のオプションがあります：**N** - ユーザーによるパスワードの保存を許可しません。**S** -ユーザーによるパスワードの保存を許可します（HTTPS または HTTP が構成されたストア）。この機能は、レジストリキー HKEY_LOCAL_MACHINE\Software[Wow6432Node]\Citrix\Dazz で設定することもできます。注：AllowSavePwd が機能しない場合は、次のレジストリキーを手動で追加する必要があります：**1** 32 ビット OS クライアントのキー：HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager **2** 64 ビット OS クライアントのキー：HKEY_LOCAL_MACHINE\Software\wow6432node\Citrix\AuthM **3** 種類：REG_SZ **4** 値：never - ユーザーによるパスワードの保存を許可しません。secureonly - ユーザーによるパスワードの保存を許可します（HTTPS で構成されたセキュアなストアのみ）。always - ユーザーによるパスワードの保存を許可します（HTTPS または HTTP で構成されたストア）。
使用サンプル	CitrixReceiver.exe ALLOWADDSTORE=N

証明書の選択

オプション	AM_CERTIFICATESELECTIONMODE={Prompt、SmartCardDefault、LatestExpriry}
説明	このオプションを使用して証明書を選択します。デフォルト値は Prompt で、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。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）が使用されるようにしたり、長い有効期限が残っているものが使用されるようにしたりできます。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。この機能は、レジストリキー HKEY_CURRENT_USER または HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Auth Prompt | SmartCardDefault | LatestExpiry } で設定することもできます。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。
使用サンプル	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

CSP コンポーネントを使ったスマートカード **PIN** エントリの管理

オプション	AM_SMARTCARDPINENTRY=CSP
説明	CSP コンポーネントを使ってスマートカード PIN エントリを管理します。デフォルトでは、スマートカードの Cryptographic Service Provider（CSP）ではなく Citrix Receiver により 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、Receiver 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。このプロパティを設定すると、CSP コンポーネントにより PIN 入力用のメッセージが表示され、PIN が処理されます。
使用サンプル	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Kerberos の使用

オプション	ENABLE_KERBEROS={Yes、No}
説明	デフォルト値は No です。HDX エンジンで Kerberos 認証を使用するかどうかを指定します。シングルサインオン（パススルー）認証が有効な場合のみ適用されます。詳しくは、「Kerberos を使用したドメインパススルー認証の構成」を参照してください。
使用サンプル	CitrixReceiver.exe ENABLE_KERBEROS=No

レガシー **FTA** アイコンの表示

オプション	LEGACYFTAICONS={False、True}
説明	レガシー FTA アイコンを表示するにはこのオプションを使用します。デフォルト値は、False です。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に、そのアプリケーションアイコンを表示するかどうかを指定します。この引数を False に設定すると、特定のアイコンが関連付けられていないドキュメントに Windows によるアイコンが表示されます。Windows によるアイコンは、汎用のドキュメント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。Windows 7 を使用するユーザーに Microsoft Office アプリケーションを配信する場合は、このオプションを有効にすることをお勧めします。
使用サンプル	CitrixReceiver.exe LEGACYFTAICONS=False

事前起動の有効化

オプション	ENABLEPRELAUNCH={False、True}
説明	デフォルト値は、False です。セッションの事前起動については、「アプリケーションの起動時間の短縮」を参照してください。
使用サンプル	CitrixReceiver.exe ENABLEPRELAUNCH=False

［スタート］メニューショートカット用ディレクトリの指定

オプション	STARTMENUDIR={ディレクトリ名}
説明	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［すべてのプログラム］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］>［Receiver］にショートカットを配置するには、STARTMENUDIR=\Receiver\と指定します。必要に応じてこのフォルダーの変更や移動ができます。次のレジストリキーを使用してこの機能を制御することもできます：StartMenuDir に REG_SZ 値を作成して、値のデータとして「RelativePath」を入力します。場所：HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazz HKEY_CURRENT_USER\Software\Citrix\Dazzle XenApp で［クライアントアプリケーションフォルダー］（「Program Neighborhood フォルダー」とも呼ばれます）を指定して公開されたアプリケーションでは、ショートカットの配置先パスにそのフォルダー名が追加されるように設定できます：これを行うには、UseCategoryAsStartMenuPath に REG_SZ 値を作成して、値のデータとして「true」を入力します。レジストリの場所は上記と同じです。注：Windows 8 および 8.1 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定義されたカテゴリサブフォルダー内ではなく、個々に、またはルートフォルダー内に表示されます。例：**1** ［クライアントアプリケーションフォルダー］に「\Office」が設定されているアプリケーションでは、UseCategoryAsStartMenuPath に true を設定して StartMenuDir を指定しない場合、［スタート］>［すべてのプログラム］>［Office］にショートカットが配置されます。**2** ［クライアントアプリケーションフォルダー］が「\Office」で、UseCategoryAsStartMenuPath に true を設定して StartMenuDir に\Receiver を指定する場合、［スタート］>［すべてのプログラム］>［Receiver］>［Office］にショートカットが配置されます。これらの設定を変更しても、配置済みのショートカットには反映されません。ショートカットに設定を反映させるには、そのアプリケーションをアンインストールしてから再インストールする必要があります。

オプション	STARTMENUDIR={ディレクトリ名}
使用サンプル	CitrixReceiver.exe STARTMENUDIR=\Office

ストア名の指定

オプション	STOREx=”storename;http[s]://servername.domain/IISLocatio Off] ; [storedescription] “[STOREy=”–”]
説明	このオプションを使ってストア名を指定します。Citrix Receiver で使用するストアを 10 まで指定します。値：**x** および **y** - 0 ～ 9 の整数。**storename** - デフォルト値は store。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」の形式で指定します。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 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どう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（任意。「HR App Store」など）。注：このリリースでは、パススルー認証が正しく実行されるように、ストア URL に「/discovery」を追加してください。
使用サンプル	CitrixReceiver.exe STORE0=”Store;https://test.xx.com/Citrix/Store/Discovery”

ユーザーデバイスでの **URL** リダイレクトの有効化

オプション	ALLOW_CLIENTHOSTEDAPPSURL=1
説明	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。管理者権限が必要です。また、Citrix Receiver をすべてのユーザー用にインストールする必要があります。URL リダイレクトについては、XenDesktop 7 のドキュメントの「ローカルアプリアクセス」のセクションを参照してください。
使用サンプル	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

セルフサービスモードの有効化

オプション	SELFSERVICEMODE={False、True}
説明	デフォルト値は、True です。管理者が SelfServiceMode フラグを false に設定すると、ユーザーはセルフサービスの Citrix Receiver 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［スタート］メニューから、および「ショートカットのみのモード」というデスクトップショートカットを介して、サブスクライブされたアプリケーションにアクセスできます。
使用サンプル	CitrixReceiver.exe SELFSERVICEMODE=False

デスクトップショートカット用ディレクトリの指定

オプション	DESKTOPDIR=** ディレクトリ名 >
説明	すべてのショートカットを単一のフォルダーにまとめます。デスクトップショートカットのため Category Path がサポートされます。注：DESKTOPDIR オプションを使用する場合、PutShortcutsOnDesktop キーを True に設定します。
使用サンプル	CitrixReceiver.exe DESKTOPDIR=\Office

サポートされていない **Citrix Receiver** バージョンからのアップグレード

> 注
>
> グラフィカルユーザーインターフェイスを使用して、Citrix Receiver バージョン 13.x Enterprise または 12.x を Citrix Receiver for Windows バージョン 4.4 以降にアップグレードすると、インストーラーはデフォルトで Receiver Clean-Up Utility を実行します。
>
> ただし、コマンドラインでアップグレードすると、ユーティリティはデフォルトでは実行されません。コマンドラインでアップグレードするには、次のコマンドを実行します:
>
> *CitrixReceiver.exe /rcu /silent*
>
> Citrix Receiver for Windows を 13.x（Enterprise 以外）から、またはバージョン 4.1 から 4.2 にアップグレードすると、/rcu スイッチは不要になり、無視されます。

オプション	/rcu
説明	サポートされていないバージョンを最新バージョンの Citrix Receiver にアップグレードできます。
使用サンプル	CitrixReceiver.exe /rcu

インストールのトラブルシューティング

インストールで問題が発生した場合は、ユーザーの%TEMP%/CTXReceiverInstallLogs ディレクトリに生成されるログファイルを確認してください。これらのログファイルの名前は、以下のように「CtxInstall-」または「TrolleyExpress- 」で始まります。次に例を示します:

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

コマンドラインを使用したインストールの例

以下のコマンドでは、**NetScaler Gateway** のストア **URL** を指定します。

CitrixReceiver.exe STORE0=";[testserver](https://testserver.com) ;<On/Off>;"\] ストア説明 > ストア名 > ストアフレンドリ名 >

注: NetScaler 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。

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。

以下のコマンドでは、シングルサインオン（パススルー認証）を指定して、**XenApp Services** サイトの **URL**を定義したストアを追加します:

仮想デスクトップやアプリケーションをコマンドラインで起動するには

Citrix Receiver for Windows により、サブスクライブ済みの各デスクトップやアプリケーションについてスタブアプリケーションが作成されます。このアプリケーションを使用して、デスクトップやアプリケーションをコマンドラインから起動できます。スタブアプリケーションは、%appdata%\Citrix\SelfService に作成されます。スタブアプリケーションの名前には、元のアプリケーションの表示名からスペースが削除されたものが設定されます。たとえば、Internet Explorer のスタブアプリケーション名は、「InternetExplorer.exe」です。

Microsoft System Center 2012 R2 Configuration Manager を使用した展開

February 21, 2019

Microsoft System Center Configuration Manager（SCCM）を使用して、Citrix Receiver for Windows を展開できます。

注 Citrix Receiver for Windows バージョン 4.5 以降のみが SCCM 展開環境をサポートします。

SCCM を使用して Citrix Receiver for Windows を展開する方法は 4 段階にわけられます。

1. Citrix Receiver for Windows を SCCM 展開環境に追加する
2. 配布ポイントを追加する
3. Receiver 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 Receiver for Windows を SCCM 展開環境に追加する

1. ダウンロードした Citrix Receiver の 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：ここで指定された情報は、ユーザーに表示されます。
6. ［展開の種類］ ペインで、［追加］ を選択して Citrix Receiver セットアップの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：Receiver 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 Receiver 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：
      - CitrixReceiver.exe / silent（デフォルトのサイレントインストール）
      - CitrixReceiver.exe /silent /includeSSON（ドメインパススルーを有効にする）
      - CitrixReceiver.exe /silent SELFSERVICEMODE=false(セルフサービスモード以外で Receiver をインストールする）
   c) ［アンインストールプログラム］ に CitrixReceiver.exe /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。
11. ［設定の種類］ をファイルシステムに設定します。
12. ［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
    - ファイル名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 ［次の値より大きいか等しい］ 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、Citrix Receiver for Windows のアップグレードにも適用されます。
13. ［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。
14. ［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。

15. ［完了］ペインの［展開の種類］一覧に新しい展開の種類（Receiver の展開）が表示されます。
16. ［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 Receiver for Windows 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。

Receiver 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 Receiver for Windows 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 Receiver for Windows 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。構成し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表示されます。［次へ］ をクリックします。
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** に設定すると、SCCM を使用した Citrix Receiver for Windows の展開が失敗することがあります。
> 分析によると、Citrix Receiver for Windows 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。

Web Interface のログオン画面からの **Citrix Receiver for Windows** の配布

November 12, 2018

この機能は、Web Interface をサポートしている XenDesktop および XenApp リリースでのみ使用できます。

Web Interface のログオン画面で Citrix Receiver for Windows をユーザーに配布すると、ユーザーが Web Interface を使用する前に確実に Receiver をインストールできます。Web Interface では、Citrix クライアントソフトウェアを検出して必要に応じてインストールするための機能が提供されます。この機能により、ユーザーは自分の環境に適したソフトウェアをインストールできます。

管理者は、ユーザーが XenApp Web サイトにアクセスした時に自動的にクライアント検出および展開処理が実行されるように構成できます。Web Interface で適切なバージョンの Citrix Receiver for Windows がインストールされていないことが検出されると、Citrix Receiver for Windows 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。

Web Interface からインストールした Citrix Receiver for Windows では、メールアドレスによるアカウント検出機能を使用できません。メールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーが Citrix Receiver for Windows を Citrix.com からインストールすると、メールアドレスまたはサーバーアドレスの入力が求められます。ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。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. CitrixReceiver.exe をローカルコンピューターにダウンロードします。
2. CitrixReceiver.exe を CitrixReceiverWeb.exe と名称変更します。
3. XenApp Web サイトの構成ファイル内の ClientIcaWin32 パラメーターに、変更したファイル名を指定します。

   この機能を使用するには、Web Interface サーバー上に Citrix Receiver for Windows のインストールファイルを配置しておく必要があります。Web Interface のデフォルトでは、Citrix Receiver for Windows のインストールファイルと XenApp または XenDesktop のインストールメディアで提供されているファイルは同じ名前であることを前提とします。
4. ユーザーは、CitrixReceiverWeb.exe ファイルのダウンロードサイトを信頼済みサイトの一覧に追加しておく必要があります。
5. 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。

ユーザーによる **Citrix Receiver for Windows** のインストールとアンインストール

January 9, 2019

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、またはコマンドラインで CitrixReceiver.exe インストーラーパッケージを手動で実行して Citrix Receiver for Windows をインストールできます。コマンドラインでのインストールパラメーターおよびスペースの要件については、「コマンドラインパラメーターを使用した Receiver for Windows の構成とインストール」を参照してください。

空きディスクスペースの検証

Citrix Receiver for Windows 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、インストールが終了し、次のダイアログが表示されます。

Citrix Receiver for Windows 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。

alt_text

次の表に、Citrix Receiver for Windows をインストールする場合の最小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	320MB
Citrix Receiver のアップグレード	206MB

> 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 Receiver for Windows のアンインストール

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 Receiver for Windows をアンインストールできます。

> 注
>
> Citrix Receiver for Windows のインストールを続行する前に、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。詳しくは、Knowledge Center のCTX200340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て **Citrix Receiver for Windows** をアンインストールするには

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 Receiver for Windows をアンインストールすることもできます。

CitrixReceiver.exe /uninstall

ユーザーデバイスから Receiver をアンインストールした後、receiver.adm/receiver.adml または receiver.admx により作成されたレジストリキーが、HKEY_LOCAL_MACHINE および HKEY_LOCAL_USER の下の Software\Policies\Citrix\ICA Client ディレクトリに残ります。

Citrix Receiver for Windows を再インストールする場合、これらのポリシーによって予期しない問題が発生することがあります。これらカスタムポリシーは、手作業で削除してください。

Receiver for Windows 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:

CitrixReceiver.exe \silent \uninstall

Active Directory とサンプルのスタートアップスクリプトを使用した展開

January 9, 2019

Active Directory のグループポリシースクリプトを使用して、Active Directory の組織構造に基づいてシステムに Citrix Receiver for Windows を事前に展開することができます。.msi ファイルを抽出するよりもスクリプトを使用することをお勧めします。スクリプトで展開すれば、インストール、アップグレード、およびアンインストールを 1 か所から実行し、［プログラムと機能］に表示される Citrix エントリを統合し、展開済みの Citrix Receiver のバージョンを簡単に検出することができます。グループポリシー管理コンソール（GPMC）の［コンピューターの構成］または［ユーザーの構成］で、［スクリプト］設定を使用します。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。

CitrixReceiver.exe のインストールとアンインストールを実行する、サンプルのコンピューター単位のスタートアップスクリプトが収録されています。スクリプトは、Citrix Receiver for Windows のダウンロードページにあります。

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Active Directory のグループポリシーを使用してコンピューターの起動時またはシャットダウン時にスクリプトを実行する場合、カスタム構成ファイルがシステムのデフォルトのユーザープロファイルに作成されることがあります。これらの構成ファイルにより、一部のユーザーが Receiver のログディレクトリにアクセスできなくなる場合があります。Citrix のサンプルスクリプトには、これらの構成ファイルを正しく削除するための機能が含まれています。

スタートアップスクリプトを使用して **Active Directory** で **Receiver** を展開するには

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。

サンプルスクリプトを変更する

各ファイルのヘッダーセクションにある次のパラメーターを編集して、スクリプトを変更します。

- **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を指定します。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 の読み取りアクセス許可を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を指定します。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を指定します。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を使用した Citrix Receiver for Windows の構成とインストール」を参照してください。

コンピューター単位の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]、[ポリシー]、[Windows の設定]、[スクリプト（スタートアップ/シャットダウン）]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［スタートアップ］を選択します。
4. ［プロパティ］ダイアログボックスで［ファイルの表示］をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. ［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。

Citrix Receiver for Windows をコンピューター単位で展開するには

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任意のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）に、新しくインストールしたパッケージが表示されていることを確認します。

Citrix Receiver for Windows をコンピューター単位で削除するには

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任意のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）から、以前にインストールしたパッケージが削除されていることを確認します。

サンプルのユーザー単位のスタートアップスクリプトの使用

通常、サーバー単位のスタートアップスクリプトを使用することをお勧めします。ユーザー単位で展開する Windows の場合は、Citrix Receiver for Windows の XenDesktop および XenApp メディアおよび Plugins\Windows\Receiver\Startup_Logon_Scripts フォルダーには、以下の 2 つのユーザー単位のスタートアップスクリプトが含まれています。

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

ユーザー単位のスタートアップスクリプトをセットアップするには

1. グループポリシー管理コンソールを開きます。
2. ［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. ［ログオンプロパティ］ダイアログボックスで［ファイルの表示］をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. ［ログオンのプロパティ］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。

Citrix Receiver for Windows をユーザー単位で展開するには

1. 作成した組織単位に展開対象のユーザーを移動します。
2. ユーザーデバイスを再起動して特定のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）に、新しくインストールしたパッケージが表示されていることを確認します。

Citrix Receiver for Windows をユーザー単位で削除するには

1. 作成した組織単位に削除対象のユーザーを移動します。
2. ユーザーデバイスを再起動して特定のユーザーでログオンします。
3. ［プログラムと機能］（以前のオペレーティングシステムでは［プログラムの追加と削除］）から、以前にインストールしたパッケージが削除されていることを確認します。

Receiver for Web サイトからの **Citrix Receiver for Windows** の配布

January 9, 2019

Citrix Receiver for Windows を Citrix Receiver for Web から展開すると、ブラウザーからアプリケーションに接続する前に、Receiver のインストールが済んでいることが保証されます。Citrix Receiver for Web サイトを使用すると、Web ページを経由して StoreFront ストアにアクセスできます。Citrix Receiver for Web サイトで適切なバージョンの Citrix Receiver for Windows がインストールされていないことが検出されると、Citrix Receiver for Windows 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。

詳しくは、StoreFront のドキュメントの「
Receiver for Web サイト」を参照してください。

Citrix Receiver for Web サイトからインストールした Citrix Receiver for Windows では、メールアドレスによるアカウント検出機能はサポートされていませんメールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーが Citrix Receiver for Windows を Citrix.com からインストールすると、メールアドレスまたはサーバーアドレスの入力が求められます。ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。

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. CitrixReceiver.exe をローカルコンピューターにダウンロードします。
2. CitrixReceiver.exe を CitrixReceiverWeb.exe と名称変更します。
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「構成ファイルによる Receiver for Web サイトの構成」を参照してください。

構成

January 9, 2019

Citrix Receiver for Windows ソフトウェアを使用する場合、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。

- アプリケーション配信の構成およびXenDesktop 環境の構成を行います。XenApp 環境が正しく構成されていることを確認します。オプションについて理解し、ユーザーに対しわかりやすいアプリケーションについての説明を提供します。
- StoreFront アカウントを Citrix Receiver for Windows に追加して、セルフサービスモードを構成します。このモードでは、ユーザーが Citrix Receiver for Windows 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による構成

- ユーザーへのアカウント情報の提供。ユーザーがアカウントをセットアップするための情報を提供します。ユーザーは、このアカウントを使用して仮想デスクトップやアプリケーションにアクセスします。環境によっては、ユーザーが手作業でアカウントをセットアップする必要があります。

内部ネットワークの外部から接続するユーザーは、NetScaler Gateway を使用して認証を構成します。詳しくは、NetScaler Gateway ドキュメントで「認証と承認」を参照してください。

アプリケーション配信の構成

April 2, 2019

XenDesktop や XenApp でアプリケーションをユーザーに配信するときは、ユーザーエクスペリエンスを向上させるために、次のオプションについて検討します。

- Web アクセスモード - いずれの構成も行わない場合、Citrix Receiver for Windows 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。Receiver for Web または Web Interface サイトを 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 Receiver for Windows に追加するか、StoreFront サイトをポイントするように Citrix Receiver for Windows 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 Receiver for Windows 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 Receiver for Windows 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 - Citrix Receiver for Windows 管理者として、Citrix Receiver for Windows Enterprise でするのと同じように、Citrix Receiver for Windows 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。

XenApp および XenDesktop 7 を使ったアプリケーション配信については、「デリバリーグループの作成」を参照してください。

> 注
>
> Citrix Receiver for Windows 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 に追加する必要があります。

NetScaler Gateway ストアの構成

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って、ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則を構成することをお勧めします。
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。これは、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 Receiver for Windows の設定を適用するのに非常に有用です。単一のユーザーデバイスの場合は、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。

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 **NetScaler Gateway** を追加または指定するには:

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver**] > [**StoreFront**] の順に選択します。
3. NetScaler 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] - NetScaler Gateway の後ろにあるストアの名前を指定します。
    - [ストアの有効/無効] - ストアの状態を On または Off で指定します。
    - [ストアの説明] - ストアの説明を入力します。
5. NetScaler の 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: HRStore #Store name;On; Store for HR staff
ここで、#Store name は NetScaler Gateway の後ろにあるストアの名前を、dtls.blrwinrx.com は NetScaler の URL を示します。

GPO を使用して NetScaler Gateway を追加してから Citrix Receiver for Windows を起動すると、システムトレイに以下のメッセージが表示されます。

制限事項

1. NetScaler の 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。
2. 複数の NetScaler URL を入力することはできません。
3. NetScaler の URL が変更された場合、変更を有効にするには Citrix Receiver for Windows をリセットする必要があります。
4. NetScaler Gateway の URL を上記の方法で構成した場合、NetScaler Gateway の後ろにある PNA サービスはサポートされません。

セルフサービスモードの構成

StoreFront アカウントを Citrix Receiver for Windows に追加するか、StoreFront サイトをポイントするように Citrix Receiver for Windows を構成するだけで、「セルフサービスモード」 を構成できます。このモードでは、ユーザーは Citrix Receiver for Windows 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 Receiver for Windows 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 Receiver for Windows 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 Receiver の［おすすめ］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

> 注
>
> ストアを構成する前にグループポリシーに変更を加える必要があります。グループポリシーをカスタマイズする場合には、Citrix Receiver をリセットしてからグループポリシーを構成し、その後ストアを再構成する必要があります。

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver］>［Self Service］の順に選択します。
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. ［適用］、［OK］の順にクリックします。
5. ［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 Receiver］>［Self Service］の順に選択します。

6. ［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。
7. 必要に応じてオプションを選択します。
8. ［適用］、［OK］の順にクリックします。
9. Citrix Receiver for Windows 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 8/8.1 および 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 XexApp 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）。
- 以前にはストアから実行できたけど今はもう実行できないアプリケーションのショートカットや Receiver 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する必要があります。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。次に例を示します:

<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。完了したら、構成の変更をサーバーグループに反映し、展開内のほかのサーバーをアップデートします。

XenApp および **XenDesktop 7.x** 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

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 Receiver 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 Citrix Receiver の機能と似ていますが、バージョン 4.2.100 では XenApp 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。

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	Windows 向け 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。注：この設定は、Web Interface サイトにのみ適用されます。

> 注
>
> **PutShortcutsInStartMenu=false** 設定は、XenApp 6.5 と XenDesktop 7.x の両方に適用されます。

XenApp 6.5 でのアプリケーションごとの設定の構成

XenApp 6.5 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. XenApp の ［アプリケーションのプロパティ］ 画面で、［基本設定］ プロパティを展開します。
2. ［ショートカットの表示］ オプションを選択します。
3. ［ショートカットの表示］ 画面の ［アプリケーションのショートカットの追加先］ で、［クライアントのスタートメニューに追加する］ チェックボックスをオンにします。チェックボックスをオンにした後、ショートカットを置くフォルダーの名前を入力します。フォルダー名を指定しない場合は、XenApp により［スタート］メニューにフォルダーに入っていないショートカットが置かれます。
4. ［ショートカットをクライアントのデスクトップに追加するかどうかを示します］ を選択して、クライアントマシンのデスクトップにショートカットを含めます。
5. ［適用］ をクリックします。
6. ［**OK**］ をクリックします。

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. （オプション）［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 Receiver 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 Receiver 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、ホワイト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 Receiver 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、HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。
2. Regedit を使って、HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。HKCU は HKLM 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、Windows 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、Receiver 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。Receiver 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 HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\\ShareOne\ReceiverStu
    b) Reg add HKLM\Software\Citrix\Dazzle /v
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d “true”。また、必要な場合は HKCU でこれらの設定を構成することもできます。HKCU は HKLM よりも優先されます。
    d) 設定をテストするため、Receiver を終了して再起動します。

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（セルフサービス）

数十（または数百の）アプリケーションがある場合は、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 Receiver 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 Receiver 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 Receiver をインストールし、Citrix Receiver for Web および Web interface をブラウズします。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 Receiver を構成することもできます。

Citrix Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver で DesktopDir= 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 Receiver 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 Receiver 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 Receiver で UseCategoryAsStartMenuPath=True と構成します。
Citrix Receiver 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 Receiver 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 Receiver 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 Receiver で RemoveAppsOnLogoff=True と構成します。
終了時に Citrix Receiver によりアプリケーションが削除されるようにするには	Citrix Receiver で RemoveAppsOnExit=True 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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。

- 説明に「KEYWORDS:prefer="<pattern>"」という文字列を追加すると、Citrix Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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 Receiver 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
コンソール	\McAfee\VirusScan **Console**	はい
Virus	\McAfee\VirusScan Console	いいえ
McAfee	\McAfee\VirusScan Console	いいえ

- 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。絶対パスによるマッチは、XenDesktop でプログラム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、プログラム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。

StoreFront の構成

February 21, 2019

Citrix StoreFront は、XenDesktop、XenApp、および VDI-in-a-Box への接続を認証し、使用可能なデスクトップおよびアプリケーションを Citrix Receiver for Windows でアクセスできるストアに集約します。

ここで説明する構成手順に加えて、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 NetScaler Gateway を構成する必要もあります。

> ヒント
>
> 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 UI 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 Receiver for Windows を使用するには、HTTPS 接続が必要です。StoreFront サーバーで HTTP が構成されている場合は、ユーザーデバイス上のレジストリキーを設定する必要があります。詳しくは、「コマンドラインパラメーターを使用した Receiver for Windows の構成とインストール」の ALLOWADDSTORE プロパティに関する説明を参照してください。

> 注:
>
> 独自の Citrix Receiver for Windows ダウンロードサイトを作成する管理者用に、テンプレートが提供されています。

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 Receiver for Windows 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、Windows 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 XenApp サーバーホストで変更します。公開デスクトップでは Citrix Receiver for Windows の動作を変更できます。

Citrix Receiver for Windows 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 = Receiver 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

Citrix Receiver for Windows のワークスペースコントロールの無効化

Citrix Receiver for Windows に対して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_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle （64 ビット）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle （32 ビット）

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_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle （64 ビット）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle （32 ビット）

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、REG_SZ 値の 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ー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、REG_DWORD 値の SI INACTIVE MS を HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。状態インジケーターをすぐに非表示したい場合は、REG_DWORD 値を 4 に設定します。

> 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、Windows 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。

CLI での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モードにより、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 Receiver 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。

Citrix Receiver 管理者として、コマンドラインインストールフラグ、GPO、アカウントサービス、またはレジストリ設定を使って、通常の「セルフサービス」Citrix Receiver インターフェイスを無効にし、事前定義した［スタート］メニューと置き換えることができます。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、ユーザーはセルフサービスの Citrix Receiver 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、［スタート］メニューやデスクトップのショートカットを使って、サブスクライブ済みのアプリケーションにアクセスします。これをショートカットのみのモードと呼びます。

ユーザーおよび管理者は、いくつか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。ユーザーが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 Receiver for Windows アイコンで［更新］を選択するとこれらの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。レジストリ設定を変更したら、Citrix Receiver for Windows 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 8/8.1 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 XexApp 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 がサポートされます。
- 変更アプリケーションの自動再インストールは、レジストリキー AutoReInstallModifiedApps を介して有効にできる機能です。AutoReInstallModifiedApps が有効な場合、管理者がサーバー上の公開アプリケーション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、アプリケーション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再格納されません。デフォルトでは、この AutoReInstallModifiedApps は有効です。「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レジストリキーの使用」を参照してください。

レジストリでの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に変更を加える必要があります。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、Receiver 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

64 ビットマシンのレジストリキー

グラフィカルユーザーインターフェイスを使用してショートカットと再接続オプションを構成する

> 注
>
> ショートカットを設定できるのは、サブスクライブ済みのアプリケーションとデスクトップに対してのみです。
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」を参照してください。

1. Citrix Receiver for Windows にログオンします。
2. システムトレイの Citrix Receiver for Windows アイコンを右クリックし、［高度な設定］ を選択します。［高度な設定］ウィンドウが開きます。
3. ［設定オプション］ をクリックします。

> 注
>
> ［スタート］メニューでアプリケーションを表示します］ オプションは、デフォルトではオンになっています。

4. フォルダー名を指定します。これにより、指定した［スタート］メニューのフォルダーに、すべてのサブスクライブ済みアプリケーションが移動されます。アプリケーションは、［スタート］メニューの新規フォルダーと既存フォルダーのどちらにも追加できます。この機能を有効にすると、既存のアプリケーションと新規追加されたアプリケーションの両方が指定したフォルダーに追加されます。
5. ［デスクトップオプション］ ペインの ［デスクトップにアプリケーションを表示します］ チェックボックスをオンにします。
6. フォルダー名を指定します。これにより、指定したローカルデスクトップのフォルダーに、すべてのサブスクライブ済みアプリケーションが移動されます。
7. ［カテゴリ］ オプションの ［[スタート］メニューとデスクトップのパスを有効にします］ チェックボックスをオンにします。これにより、アプリケーションプロパティサーバーで定義されたアプリケーションのショートカットおよびカテゴリフォルダーが作成されます。たとえば、IT アプリフォルダーや財務アプリフォルダーなどです。

   > 注
   >
   > ［[スタート］メニューパスのカテゴリ］ オプションは、デフォルトではオンになっています。

   i. サブスクライブ済みのアプリケーションとカテゴリフォルダーをアプリケーションサーバーのプロパティで定義されたとおりに Windows の［スタート］メニューに表示するには、［[スタート］メニューパスのカテゴリ］ チェックボックスをオンにします。

   ii. サブスクライブ済みのアプリケーションとカテゴリフォルダーを、アプリケーションサーバーのプロパティで定義されたとおりにローカルデスクトップに表示するには、［デスクトップパスのカテゴリ］ チェックボックスをオンにします。
8. ［**OK**］ をクリックします。

グラフィカルユーザーインターフェイスを使用して再接続オプションを構成する

> 注
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」を参照してください。

サーバーにログオンしたユーザーは、すべての自分のデスクトップやアプリケーションに一度に再接続できます。デフォルトの再接続オプションでは、切断されているデスクトップやアプリケーションに加えて、ほかのクライアントデバイスで現在アクティブなデスクトップやアプリケーションが開かれます。管理者は、切断されているデスクトップやアプリケーションだけが再接続されるように再接続オプションを構成することもできます。

1. Citrix Receiver for Windows にログオンします。

2. システムトレイの Citrix Receiver for Windows 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］ウィンドウが開きます。
3. ［設定オプション］ をクリックします。
4. ［再接続オプション］ をクリックします。
5. ［ワークスペースコントロールのサポートを有効にします］ チェックボックスをオンにして、ユーザーが一度にすべてのデスクトップやアプリケーションに再接続できるようにします。
   a) ユーザーがアクティブなセッションと切断されたセッションの両方に接続できるようにするには、［すべてのアクティブおよび切断されたセッションに再接続します］ をクリックします。
   b) ユーザーが切断されたセッションのみに接続できるようにするには、［切断されたセッションのみに再接続します］ をクリックします。

   > 注:
   >
   > ［サポートされている再接続モード］ の値は GPO で設定されたものになります。このオプションは、［管理用テンプレート］ > ［**Citrix** コンポーネント］ > ［**Citrix Receiver**］ > ［**SelfService**］ > ［**Receiver** による既存のセッションへの再接続を制御します］ で変更できます。

   レジストリを使用してこのオプションを変更する方法については、Knowledge Center のCTX136339を参照してください。
6. ［**OK**］ をクリックします。

機能の設定

January 9, 2019

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、Receiver for Windows ソフトウェアをインストールした後で、以下の構成を行う必要があります:

- 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、可能な限り、Enlightened Data Transport（EDT）と呼ばれる新しい Citrix プロトコルを TCP より優先して適用することによってデータ転送を最適化します。アダプティブトランスポート構成について詳しくは、「アダプティブトランスポートの構成」を参照してください。
- Receiver の更新 - Receiver の更新では、更新を手動でダウンロードする必要なく、Citrix Receiver for Windows および HDX RealTime Optimization Pack を自動的に更新できます。Receiver の更新を構成する方法について詳しくは、「Receiver の更新の構成」を参照してください。
- コンテンツの双方向リダイレクト - コンテンツの双方向リダイレクトは、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または無効にできます。コンテンツの双方向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の構成」を参照してください。

- Bloomberg キーボード - 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 サポート機能の使用を構成できます。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。
- 複合 USB デバイス - 複合 USB デバイスは、複数の機能を実行します。これらの各機能は異なるインターフェイスを使用します。複合 USB デバイスリダイレクトを構成する方法について詳しくは、「複合 USB デバイスの構成」を参照してください。
- USB サポート - USB サポート機能により、ユーザーが仮想デスクトップ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。USB サポートの構成について詳しくは、「USB サポートの構成」を参照してください。

アダプティブトランスポートの構成

January 9, 2019

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。

バージョン 4.10 以降、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が 5 分ごとに EDT を検索し続けます。

要件

- XenApp および XenDesktop 7.12 以降（Citrix Studio を使用する機能の有効化に必要）
- 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 でのインバウンドトラフィックを許可するファイアウォールルールを追加します。

> 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。ユーザーが有効化する必要があります。

VDA と Citrix Receiver 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。

デフォルトでは、Citrix Receiver for Windows 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は、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、Citrix Receiver 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 Receiver 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 Receiver 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 Receiver**］ > ［ネットワークルーティング］ の順に移動します。
3. ［**Receiver** 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 Receiver** 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 Receiver 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］： Citrix Receiver 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 Receiver Windows 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する必要があります。admx/adml 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詳しくは、「グループポリシーオブジェクトテンプレートによる Citrix Receiver の構成」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、キー **HDXOverUDP** が含まれていることを確認します。

USB サポートの構成

April 2, 2019

USB サポート機能により、仮想デスクトップ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、仮想デスクトップで 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、XenApp および XenDesktop 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

> 注
>
> 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 XenDesktop および Apps 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、XenDesktop 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、XenApp 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

ユーザーが使用できる USB デバイスの範囲を変更する方法については、「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」を参照してください。

特定の USB デバイスを自動的にリダイレクトする方法については、Knowledge Center のCTX123015を参照してください。

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 Citrix Receiver 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
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側ドライブのマッピングによるリダイレクトが実行されます。マス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、クライアント側ドライブのマッピングの前に 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 XenDesktop および XenApp 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 XenApp 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 XenApp 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（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 XenApp 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 XenApp 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 のバリアントを使用します

  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。

> 重要
>
> ウィルスプログラムの中には、あらゆる種類の大容量記憶装置デバイスを媒体にして活発に増殖するものがあります。クライアントドライブマッピングまたは USB サポート機能でマスストレージデバイスの使用を許可する場合は、ビジネス上の必要性があるかどうかを慎重に考慮してください。

- 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る場合があります。

  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。
- そのほか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に、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。

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

Citrix Receiver for Windows 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 Citrix Receiver for Windows 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：

:\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 =
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、Windows 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 = 複数行文字列値名前 =”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。
これらの規則およびその構文については、Knowledge Center の [CTX119722](https://support.citrix.com/article/CTX119722
を参照してください。
USB オーディオの構成
> ** 注 **
>
>- Citrix Receiver for Windows 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 に追加する必要があります。テンプレートファイルをローカル GPO に追加する方法の詳細については、[グループポリシーオブジェクト管理用テンプレートの構成](https://docs.citrix.com/ja-jp/receiver/windows/current-release/configure/config-gpo-template.html) 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、XenApp 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
1. gpedit.msc を実行して、Citrix Receiver 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。
1. ［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 Receiver］**、**［ユーザーエクスペリエンス］** の順に開き、**［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。
1. 設定を編集します。
1. **［適用］**、**［OK］** の順にクリックします。
1. コマンドプロンプトを管理者モードで開きます。
1. 次のコマンドを実行します:
‘gpupdate /force‘
ルートドライブ >

複合 **USB** デバイスリダイレクトの構成

January 9, 2019

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複合 **USB** リダイレクトを構成する

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver**］ > ［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］ を選択します。
5. ［適用］ をクリックします。
6. ［**OK**］ をクリックしてポリシーを保存します。

グループポリシーオブジェクト管理用テンプレートでインターフェイスを許可または禁止するには

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver**］ > ［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］ を選択します。
5. ［**USB** デバイス規則］ テキストボックスで、許可または禁止する USB デバイスを追加します。
   たとえば、*ALLOW: vid=047F pid= C039 split=01 intf=00,03 //00* および *03* インターフェイスを許可、その他を制限。
6. ［適用］、［**OK**］ の順にクリックします。

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。

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。

以下の表は、USB インターフェイスが許可または禁止される場合の動作に関する詳細です。

インターフェイスを許可する場合**:**

Split	Interface	操作（アクション）
TRUE	有効な数字 0 -n	指定のインターフェイスを許可する
TRUE	無効な数	すべてのインターフェイスを許可する
FALSE	任意の値	親デバイスの汎用 USB を許可する
指定なし	任意の値	親デバイスの汎用 USB を許可する

たとえば、SplitDevices- *true* は、すべてのデバイスが分割されることを示します。

インターフェイスを禁止する場合**:**

Split	Interface	操作（アクション）
TRUE	有効な数字 0 -n	指定のインターフェイスを禁止する
TRUE	無効な数	すべてのインターフェイスを禁止する
FALSE	任意の値	親デバイスの汎用 USB を禁止する
指定なし	任意の値	親デバイスの汎用 USB を禁止する

たとえば、SplitDevices- *false* は、デバイスが指定されたインターフェイス番号で分割されないことを示します。

例：My_<*plantronics*> headset

インターフェイス番号

- オーディオインターフェイスクラス -0
- HID インターフェイスクラス -3

My_<*plantronics*> ヘッドセットで使用される規則例：

- ALLOW: vid=047F pid= C039 split=01 intf=00,03 //00 および 03 インターフェイスを許可、その他を制限。
- DENY: vid=047F pid= C039 split=01 intf=00,03 //00 および 03 を禁止

制限事項：

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。

高度な設定シートの非表示

January 9, 2019

バージョン 4.10 以降、システムトレイの［Citrix Receiver］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

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 Receiver 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 Receiver 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 Receiver**］ > ［**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 Receiver 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 Receiver 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］シートから以下の手順で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。

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver**］ > ［**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。

［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

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
有効	設定を非表示にします
無効	設定を表示します

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 **Receiver** の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 **Receiver** の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** に移動します。
3. 新しい文字列値キー **EnableFactoryReset** を作成し、次のいずれかのオプションに設定します。
    a) True - ［高度な設定］シートで Receiver のリセットオプションが表示されます
    b) False - ［高度な設定］シートで Receiver の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［**Receiver** の更新］オプションを非表示にする

注:［Receiver の更新］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 Receiver 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. ［コンピューター構成］ ノードで、［管理用テンプレート］> ［**Citrix** コンポーネント］> ［**Citrix Receiver**］> ［**Receiver** の更新］ の順に移動します。
3. **Receiver** の更新ポリシーを選択します。
4. ［高度な設定］シートで Receiver の更新設定を非表示にするには、［無効］ を選択します。

Bloomberg キーボードの構成

November 12, 2018

Citrix Receiver for Windows は、XenApp および XenDesktop セッションで Bloomberg キーボードをサポートします。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、Citrix Receiver for Windows のインストール中またはレジストリで有効にできます。

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。このキーボードは単一セッション環境でのみ正しく動作します。

Bloomberg キーボードのサポートを有効または無効にするには

> 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、Windows 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、Citrix 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 キーボードの構成について詳しくは、Knowledge Center でCTX122615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、Windows 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、Citrix 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. 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、ユーザーまたはデバイスの設定で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

通常、プラグイン管理者やユーザーではなく XenDesktop 管理者がグループポリシーを使用してポリシー設定を制御するので、これらのキーを使用するかどうかは任意です。そのため、これらのキーを使用する前に、XenDesktop 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。

2. エントリを 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。

   a) HKEY_CURRENT_USER\Software\Policies\Citrix\…
   b) HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
   c) HKEY_CURRENT_USER\Software\Citrix\…
   d) HKEY_LOCAL_MACHINE\Software\Citrix\…

コンテンツの双方向リダイレクトの構成

April 2, 2019

次のいずれかを使用して、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

> 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。
> - 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。

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

Citrix Receiver for Windows を初めてインストールした場合は、グループポリシーオブジェクト管理用テンプレート構成を使用します。

1. gpedit.msc を実行して、Citrix Receiver 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 Receiver**］>［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。
4. 設定を編集します。

   > 注
   >
   > URL を含める場合は、単一の URL か、セミコロンで区切った URL のリストを指定できます。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。

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。

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 Receiver for Windows 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。

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。

> 重要
>
> - リダイレクトルール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 ルールが、たとえば 1 つの URL（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。

ユーザーへのアカウント情報の提供

March 18, 2019

管理者は、ユーザーにアカウントの情報を提供します。ユーザーは、この情報を使用して仮想デスクトップやアプリケーションにアクセスします。次の方法でユーザーに情報を提供できます:

- メールアドレスによるアカウント検出を構成する
- ユーザーにプロビジョニングファイルを提供する
- 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 Receiver for Windows 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 Receiver for Windows 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。このダイアログボックスでは、メールアドレスまたはサーバー URL を入力して Citrix Receiver アカウントをセットアップすることができます。

Citrix Receiver for Windows により、入力したメールアドレスに関連付けられている NetScaler Gateway、StoreFront サーバー、または AppController 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。
   この設定はユーザーごとに固有であり、Citrix Receiver for Windows をリセットするとリセットされます。

2. コマンドラインを使用したインストール

   管理者として、次のスイッチを指定して Citrix Receiver for Windows をインストールします。
   CitrixReceiver.exe /ALLOWADDSTORE=N
   この設定はマシンごとであるため、動作の設定は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、次の方法でも非表示にすることができます。

> 注
>
> システムログオン時に設定する方法かコマンドラインインターフェイスによる方法のどちらかを使用して、［ア

> カウントの追加］ダイアログボックスを非表示にすることをお勧めします。

- Citrix 実行ファイルの名前を変更する:
  ファイルの名前を **CitrixReceiver.exe** から **CitrixReceiverWeb.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。これにより、［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。
  Citrix Receiver for Web サイトについて詳しくは、「Receiver for Web サイトからの Receiver for Windows の配布」を参照してください。
- グループポリシーオブジェクト:
  Citrix Receiver for Windows インストールウィザードで［アカウントの追加］ボタンが表示されないようにするには、以下のとおりにローカルグループポリシーエディターで Self-Service ノードにある **EnableFTU** ポリシーを無効にします。
  この設定はマシンごとであるため、動作の設定はすべてのユーザーに適用されます。
  テンプレートファイルのロード方法について詳しくは、「グループポリシーオブジェクトテンプレートによる Receiver の構成」を参照してください。

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 Receiver for Windows 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。DNS（Domain Name System: ドメインネームシステム）サービス（SRV）レコードにより、そのメールアドレスに関連付けられている NetScaler Gateway または StoreFront サーバーが自動的に検出され、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。

> 注
>
> メールアドレスによるアカウント検出は、Web Interface 環境では使用できません。

NetScaler Gateway を構成する方法については、NetScaler Gateway のドキュメントの「Connecting to StoreFront by using email-based discovery」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 Receiver for Windows を自動的に構成できるようにします。Citrix Receiver for Windows をインストールした後で、提供されたファイルをユーザーが開くと Citrix Receiver for Windows が自動的に構成されます。Citrix Receiver for Web サイトを構成して、ユーザーに Citrix Receiver for Windows のプロビジョニングファイルを提供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

  Web Interface 展開環境の場合は、XenApp Services サイトの URL を提供します。

- NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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。

    NetScalerGatewayFQDN?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 Receiver for Windows 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。

Citrix Receiver ユーザーがアカウントを管理するには、Citrix Receiver for Windows のホームページで、をクリックし、［アカウント］ を選択します。

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、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 Citrix Receiver for Windows 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 Receiver for Windows を開く時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 ビットシステムの場合、「**CurrentAccount**」というキーを作成します：

場所：HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

キー名：CurrentAccount

値：AllAccount

種類：REG_SZ

64 ビットシステムの場合、「**CurrentAccount**」というキーを作成します：

場所：HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

キー名：CurrentAccount

値：AllAccount

種類：REG_SZ

Citrix Receiver の更新の構成

February 21, 2019

Citrix Receiver の更新では、以下の優先順位で Citrix Receiver の更新を構成します。

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. 高度な設定（ユーザーごと）

> 注
>
> - Citrix Receiver の更新を使用して Citrix Receiver for Windows をアップグレードすると、ログインウィンドウは表示されません。
> - このリリースでは、Citrix Receiver 更新プログラムに Windows 用の HDX RTME が含まれています。Citrix Receiver for Windows 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。

制限事項:

1. 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、Receiver 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`）に例外を追加する必要があります。
2. システムがインターネットに接続されている必要があります。
3. Receiver for Web 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。
4. デフォルトでは、VDA で Citrix Receiver 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 マシンでも同様です。
5. Citrix Receiver 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。

グループポリシーオブジェクト管理用テンプレートで構成する

1. gpedit.msc を実行して、Citrix Receiver 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. ［コンピューター構成］ノードで、［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Receiver**］>［**Receiver** の更新］ の順に移動します。
3. ［更新のチェックで遅延を設定］ ポリシーを選択します。このポリシーによって、更新をロールアウトするタイミングを選択できます。
4. ［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。
5. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。
6. Receiver の更新テンプレートセクションで、［**Receiver** の更新］ ポリシーを選択します。

   > 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［**Receiver** の更新］ オプションも非表示になります。

7. ［有効］ を選択して必要な値を設定します:
   - **Receiver** の更新ポリシーを有効にするドロップダウンリストで、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。
   - ［**LTSR** のみ］ を選択して LTSR の更新のみを取得します。
   - ［**Auto-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** - 任意の回数通知を保留できます（デフォルト値 =-1）。
     - **0** - ［後で通知する］ オプションは表示されません。
     - その他の数字 - この回数分、［後で通知する］ オプションが表示されます。たとえば、値を 10 に設定すると、［後で通知する］ オプションが 10 回表示されます。
8. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。

コマンドラインインターフェイスを使用した構成

Citrix Receiver for Windows のインストール中

Citrix Receiver のインストール中、管理者として Citrix Receiver の更新設定を構成する場合、以下のコマンドライン設定を使用できます。

- **/AutoUpdateCheck**= auto/manual/disabled

- **/AutoUpdateStream**= LTSR/Current。ここで LTSR は長期サービスリリース、Current は最新リリースを意味します。
- **/DeferUpdateCount**= -1 ～ 30 の任意の値
- **/AURolloutPriority**= auto/fast/medium/slow

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

- Citrix Receiver のインストール中、ユーザーとして Citrix Receiver の更新設定を構成する場合、以下のコマンドライン設定を使用できます。
  - **/AutoUpdateCheck=auto/manual**

次に例を示します：`CitrixReceiver.exe /AutoUpdateCheck=auto`

グループポリシーオブジェクト管理用テンプレートで Citrix Receiver の更新設定を編集すると、Citrix Receiver for Windows のインストールですべてのユーザーに適用される設定が上書きされます。

Citrix Receiver for Windows のインストール後

Citrix Receiver の更新は、Citrix Receiver for Windows のインストール後にも構成できます。

コマンドラインを使用するには：

Windows のコマンドプロンプトを開いて、**CitrixReceiverUpdater.exe** があるディレクトリに移動します。通常、CitrixReceiverUpdater.exe は`CitrixReceiverInstallLocation\Citrix\Ica Client\Receiver`にあります。

また、このバイナリで Citrix Receiver の更新のコマンドラインポリシーを設定することもできます。

たとえば、管理者は 4 つのオプションすべてを使用できます：

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

グラフィカルユーザーインターフェイスを使用した構成

> 注
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」を参照してください。

各ユーザーが ［高度な設定］ ダイアログボックスで［Citrix Receiver 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。

1. システムトレイで Citrix Receiver for Windows を右クリックします。
2. ［高度な設定］ を選択して ［**Receiver** の更新］ をクリックします。
3. 次のいずれかのオプションを選択します：

- はい。通知します
- いいえ。通知しません
- 管理者指定の設定を使用する

4. ［保存］ をクリックします。

StoreFront を使用した Citrix Receiver の更新の構成

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 ディレクトリにあります。
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）。

   例：<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：

```
<properties>
<clear />
</properties>
```

3. *<clear />* タグの後に、自動更新タグを追加します。

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"

      description="" published="true" updaterType="Citrix"
          remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />

            </plugins>

```



```
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=”1”
                      />
34
35                      <property name=”Auto-Update-LTSR-Only” value=”
                          FALSE” />
36
37                <property name=”Auto-Update-Rollout-Priority” value=”fast
                      ” />
38
39                    </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <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>
```

auto-update-Check

この属性は、Citrix Receiver for Windows が、利用可能な更新を検出したことを示します。

有効な値は次のとおりです:

- 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。
- Disabled - Citrix Receiver の更新は表示されず、更新が利用可能になっても通知されません。

auto-update-LTSR-Only

この属性は、Citrix Receiver for Windows が LTSR の更新のみを受け入れることを示します。

有効な値は次のとおりです:

- True – Citrix Receiver の更新は Citrix Receiver for Windows の LTSR 更新のみをチェックします。
- False – Citrix Receiver の更新は Citrix Receiver for Windows の LTSR 更新以外もチェックします。

auto-update-DeferUpdate-Count

この属性は、通知を保留できる回数を示します。［後で通知する］ オプションは、ここで設定された値の回数表示されます。

有効な値は次のとおりです:

- -1 – 任意の回数通知を保留できます（デフォルト値 =-1）。
- 0 – ［後で通知する］オプションは表示されません。
- その他の数字 - この回数分、［後で通知する］オプションが表示されます。たとえば、値を 10 に設定すると、後で通知するオプションが 10 回表示されます。

auto-update-Rollout-Priority

この属性は、設定できるロールアウトのタイミングを示します。

有効な値は次のとおりです:

- 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。

グループポリシーオブジェクト管理用テンプレートの構成

April 2, 2019

Windows グループポリシーオブジェクト（GPO）エディターを使用して Citrix Receiver for Windows を構成することをお勧めします。Citrix Receiver for Windows では、インストールディレクトリに管理用テンプレートファイルが含まれています（receiver.adm または receiver.admx\receiver.adml - オペレーティングシステムによって異なります）。

> 注
>
> - Citrix Receiver for Windows バージョン 4.6 以降、インストールディレクトリに CitrixBase.admx および CitrixBase.adml ファイルが含まれます。
> - グループポリシーオブジェクトエディターでオプションが正しく整理され、表示されるようにするには、CitrixBase.admx/CitrixBase.adml ファイルの使用をお勧めします。
> - .adm ファイルは、Windows XP Embedded プラットフォームでのみ使用されます。.admx/.adml ファイルは、Windows Vista/Windows Server 2008、および以降のすべての Windows バージョンで使用されます。
> - Citrix Receiver for Windows を VDA とともにインストールする場合、admx/adml ファイルはインストールディレクトリにあります。たとえば、\Online Plugin\Configuration です。インストールディレクトリ >
> - Citrix Receiver for Windows を VDA なしでインストールする場合、admx/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 Receiver for Windows 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
>
> 最新の Citrix Receiver for Windows 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。

ファイルの種類	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	\ICA Client\Configuration\\\[MUI カルチャ\] インストールディレクトリ >

> 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 Receiver for Windows をアップグレードする場合、以下の手順に従って最新のテンプレートをローカル GPO に追加する必要があります。最新のファイルをインポートしても、以前の設定は保持されます。

ローカル **GPO** に **receiver.adm** テンプレートファイルを追加するには（**Windows XP Embedded** オペレーティングシステムの場合）

> 注
>
> adm テンプレートファイルを使用して、ローカル GPO やドメインベースの GPO を構成できます。

1. gpedit.msc を実行して、Citrix Receiver 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. グループポリシーエディターで ［管理用テンプレート］ を選択します。
3. ［操作］メニューの ［テンプレートの追加と削除］ を選択します。
4. ［追加］をクリックし、テンプレートファイルの場所（\ICA Client\Configuration\receiver.adm）を参照します。インストールディレクトリ >
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
   ローカル GPO のパス ［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 Receiver**］ に、Citrix Receiver for Windows のテンプレートファイルが追加されます。

ローカル GPO に.adm テンプレートファイルが追加されると、次のメッセージが表示されます：
「strings セクションの次のエントリが長すぎるため切り詰められました。」：
［**OK**］ をクリックしてメッセージを無視します。

ローカル **GPO** に**.admx/adml** テンプレートファイルを追加するには（最近のバージョンの **Windows** オペレーティングシステムの場合）

> 注
>
> admx/adml テンプレートファイルを使用して、ローカル GPO やドメインベースの GPO を構成できます。ADMX ファイルの管理については、Microsoft MSDN の記事を参照してください。

Citrix Receiver for Windows をインストールしてから、以下の表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	インストールディレクトリ\ICA Client\Configuration\receiver.a	%systemroot%\policyDefinitions
CitrixBase.admx	インストールディレクトリ\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	インストールディレクトリ\ICA Client\Configuration\[MUIcultu	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	インストールディレクトリ\ICA Client\Configuration\[MUIculture]\CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> 注
>
> Citrix Receiver for Windows のテンプレートファイルは、[管理用テンプレート] > [Citrix コンポーネント] > [Citrix Receiver] フォルダーのローカル GPO にあります（ユーザーが CitrixBase.admx/CitrixBase.adml を\policyDefinitions フォルダーに追加する場合のみ）。

環境の最適化

November 12, 2018

管理者は Receiver 環境を最適化できます:

- ワークスペース構成のサポート
- アプリケーションの起動時間の短縮
- クライアント側デバイスのマッピング
- DNS 名前解決をサポートする
- プロキシサーバーを介した XenDesktop 接続をサポートする

DNS 名前解決をサポートする

November 12, 2018

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 Citrix Receiver for Windows 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、サーバーファームで DNS アドレス解決を有効にしないことをお勧めします。

Web Interface を使用してリモートアプリケーションに接続する Citrix Receiver for Windows も、接続に Citrix XML Service を使用します。この場合、Citrix Receiver for Windows の代わりに Web Interface サーバーが DNS 名を解決します。

DNS アドレス解決は、デフォルトでサーバーファームでは無効に、Citrix Receiver for Windows では有効に設定されています。サーバーファームで DNS アドレス解決が無効な場合、Citrix Receiver for Windows が DNS 名を要求すると IP アドレスが返されます。Citrix Receiver for Windows 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、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、Citrix 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。

XenDesktop でプロキシサーバーを使用する

February 21, 2019

プロキシサーバーを使用しない環境でユーザーが Windows XP 上の Internet Explorer 7.0 を使用する場合は、Internet Explorer のプロキシ設定を変更する必要があります。この場合、デフォルトでプロキシ設定が自動的に検出されます。プロキシサーバーを使用しない環境でこのデフォルト設定を使用すると、プロキシ設定の検出時に不必要な遅延が発生します。

プロキシ設定の変更手順については、Internet Explorer のドキュメントを参照してください。または、Web Interface を使ってプロキシ設定を変更できます。詳しくは、Web Interface のドキュメントを参照してください。

クライアント側デバイスのマッピング

January 9, 2019

Citrix Receiver for Windows 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 Receiver for Windows 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、XenDesktop または XenApp の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 XenDesktop 7 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、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。

クライアント側ドライブのマッピングは、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 XenDesktop または XenApp を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のと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

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
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、クライアント側ドライブの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、クライアント側デバイスの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 製品ドキュメントで XenDesktop または XenApp の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、XenApp および XenDesktop 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 Receiver for Windows 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、XenDesktop または XenApp のドキュメントを参照してください。

重要：COM ポートのマッピング機能は、TAPI をサポートしません。

1. XenDesktop 7 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 Receiver for Windows 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 com<x>: \\client\com<z>:

   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。

ワークスペース構成のサポート

January 9, 2019

Citrix Receiver for Windows 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のためのワークスペースを構成できるようになりました。

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。

Citrix Receiver for Windows および Receiver for Web は現在、Azure Active Directory 認証をサポートしています。
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。

アプリケーションの起動時間の短縮

November 12, 2018

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 Receiver for Windows 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 Citrix Receiver for Windows で新しいアカウント接続を追加した後、次回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。

セッションの事前起動機能は、StoreFront 環境では StoreFront 2.0 リリース以降でサポートされます。Web Interface 環境では、ログオン用の画面が表示されるのを防ぐため、Web Interface の［パスワードを保存］オプションを有効にする必要があります。セッションの事前起動機能は、XenDesktop 7 環境ではサポートされません。

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、Receiver 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。

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、Windows 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、Citrix 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すぐ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 Receiver for Windows 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にのみ開始されます。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。

XenApp 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。XenApp サーバー上でセッションの事前起動を構成する方法については、XenApp のドキュメントの「アプリケーションを事前起動するには」を参照してください。

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、Citrix Receiver for Windows 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。3 つの HKEY_LOCAL_MACHINE 値と 2 つの HKEY_CURRENT_USER 値を使用します。

- HKEY_LOCAL_MACHINE 値は、Receiver 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 の値

Windows Server 7 および 8 の 64 ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

そのほかのすべての 32 ビット Windows オペレーティングシステム:HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

値の名前：UserOverride

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

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ると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

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 です。	M:T:W:TH:F:S:SU - ここで、HH は時、MM は分です。 M:T:W:TH:F:S:SU は曜日です。 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、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 の値

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。

ユーザーエクスペリエンスの向上

May 23, 2019

以下の機能を使用して、Citrix Receiver for Windows のユーザーエクスペリエンスを向上させることができます:

- vPrefer 起動 - 公開されたデスクトップセッションで公開アプリケーションを起動する方法を制御します。
- H.265 ビデオエンコーディング - 画質や品質を犠牲にすることなく、より適切なデータ圧縮（少ない帯域幅）を実現します。
- DPI スケール - 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。
- 汎用クライアント IME - ソフトキーボードと IME を切り替えるオプションを使用できます。
- キーボードレイアウトと言語 - 優先するキーボードレイアウトを使用できます。

また、以下の機能を使用すると、より優れたユーザーエクスペリエンスを実現できます。

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。Citrix Receiver for Windows バージョン 4.10 では、モードの動的変更を含む Windows Continuum がサポートされるようになりました。

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、XenApp および XenDesktop のドキュメントの「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 Receiver は Windows Continuum 機能をサポートしていません。

詳しくは、
XenServer7.2 リリースノートを参照してください。

相対マウス

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。

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。

相対マウスのサポートを有効化するには

1. Citrix Receiver for Windows へのログオン
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 Receiver - 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：この機能はセッション単位です。切断されたセッションに再接続しても、設定は復元されません。ユーザーは、公開デスクトップに接続/再接続するたびにこの機能を有効化する必要があります。

ハードウェアのデコード

Citrix Receiver for Windows（HDX Engine 14.4 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DXVA（DirectX Video Acceleration）です。

Citrix Receiver 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 Receiver 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. ［コンピューター構成］ ノードで、［管理用テンプレート］ > ［**Citrix Receiver**］ > ［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 XenApp 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。

クライアント側のマイク入力

Citrix Receiver for Windows では、クライアント側の複数のマイク入力がサポートされます。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 Receiver for Windows のユーザーは、コネクションセンターの設定を変更して、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。XenDesktop ユーザーも、Desktop Viewer 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。

マルチモニターサポート

Citrix Receiver for Windows では、最大で 8 つのモニターがサポートされます。

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。

  XenDesktop: 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。

XenDesktop: 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 XenDesktop 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。
- ユーザーデバイスの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、［ディスプレイ］>［ディスプレイの設定の変更］で確認します。ここで、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。
  - **XenDesktop**: 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。
  - **XenApp**: インストールした XenApp サーバーのバージョンに応じて、次の操作を行います。
    * 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。
    * XenApp 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。

XenApp および XenDesktop 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。

デバイス側での印刷設定の変更

ポリシーの［ユニバーサル印刷最適化デフォルト］設定で［非管理者によるこれらの設定の変更を許可する］チェックボックスをオンにすると、ポリシーで指定されている［イメージ圧縮］および［イメージおよびフォントのキャッシュ］オプションの設定をユーザーが変更できるようになります。

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 Receiver for Windows 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 Receiver for Windows 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\Adva
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

Receiver 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. 管理者として、［スタート］メニューから gpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。

注：既に Citrix Receiver for Windows のテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順 2. ～ 5. は省略できます。

2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］をクリックし、Receiver の Configuration フォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）を参照して Citrix Receiver for Windows のテンプレートファイルを選択します。注：Windows のバージョンに応じた Citrix Receiver for Windows のテンプレートファイル（receiver.adm または receiver.admx/receiver.adml）を選択してください。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［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 Receiver］> ［ユーザーエクスペリエンス］> ［キーボードショートカット］の順に開きます。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして必要なオプションを選択します。

32 ビットカラーアイコンのサポート

Citrix Receiver for Windows では 32 ビット High Color アイコンがサポートされ、Citrix 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、Windows 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。

色数を設定するには、レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences に文字列のレジストリ値 TWIDesiredIconColor を追加し、目的の色数を値のデータとして定義します。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 の有効化

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 Citrix Receiver for Windows 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は公開仮想デスクトップにすることができ、または共有デスクトップや専用デスクトップにもすることができます。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 XenDesktop 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 Receiver for Windows を使用する必要があります。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 セッション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、XenDesktop 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、XenApp セッション）ではこれを使用できます。

仮想デスクトップへの接続

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、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（XenApp 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 XenApp 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、XenApp 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、XenApp 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。

状態インジケーターの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ー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、REG_DWORD 値の SI INACTIVE MS を HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\で作成します。状態インジケーターをすぐに非表示したい場合は、REG_DWORD 値を 4 に設定します。

カスタマーエクスペリエンス向上プログラム（**CEIP**）

> 注
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」を参照してください。

Ctrix カスタマーエクスペリエンス向上プログラム（CEIP）では、Receiver for Windows の構成および使用に関するデータが匿名で収集され、データは Citrix に自動的に送信されます。このデータは、Receiver 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。

CEIP が、ユーザーを識別できる情報を顧客環境から収集することはありません。

ヒント：CEIP に参加するかどうかは、Receiver インターフェイスで変更できます。インストール後、7 日間は CEIP を無効にできます。

CEIP を無効にする、または参加をやめるには：

1. システムトレイの Citrix Receiver アイコンを右クリックします。
2. ［高度な設定］ を選択します。
   ［高度な設定］ウィンドウが開きます。
3. ［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. ［**Save**］ をクリックします。

DPI スケール

January 9, 2019

Citrix Receiver for Windows 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。

Citrix Receiver の 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 Receiver 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. ［コンピューター構成］ノードで、［管理用テンプレート］>［**Citrix** コンポーネント］>［**Citrix Receiver**］>［**DPI**］ の順に移動します。
3. 高 **DPI** ポリシーを選択します。
4. 必要に応じて設定を変更します。
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 DPI スケールを構成するには

> 注
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」を参照してください。

1. システムトレイで Citrix Receiver for Windows 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. 必要に応じて設定を変更します。
   デフォルトでは、［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］ オプションが選択されています。
4. ［保存］ をクリックします。

Citrix Receiver for Windows のセッションを再起動して、この変更を適用します。

DPI スケールの問題のトラブルシューティングについて詳しくは、Knowledge Center のCTX230017を参照してください。

H.265 ビデオエンコーディング

January 9, 2019

Citrix Receiver for Windows 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 と Citrix Receiver for Windows の両方で機能がサポートされ、有効になっている必要があります。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。

Citrix Receiver for Windows 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 Receiver for Windows** 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 Receiver 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. ［コンピューター構成］ ノードで、［管理用テンプレート］ > ［**Citrix Receiver**］ > ［ユーザーエクスペリエンス］ の順に移動します。
3. ［**H.265 Decoding for graphics**］ ポリシーを選択します。
4. ［有効］ を選択します。
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 **Citrix Receiver for Windows** で **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 に移動します。
3. EnableH265 という名前で新しい 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 に移動します。
3. EnableH265 という名前で新しい 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
>
> - Citrix Receiver 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、[**H.265 Decoding for graphics**] 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。

vPrefer 起動

January 9, 2019

GPO 管理テンプレートを使用した **vPrefer** 起動の構成

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 Receiver 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、Receiver 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 XenApp 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 Receiver for Windows 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 Receiver for Windows 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、ホストされた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、StoreFront 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。

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 Receiver for Windows 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 に追加する必要があります。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の構成」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 Receiver GPO 管理用テンプレートを開きます。
2. ［コンピューター構成］ノードで、［管理用テンプレート］ > ［**Citrix** コンポーネント］ > ［**Citrix Receiver**］ > ［**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］ ドロップダウンリストの次のオプションから選択します。
    a) ［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 Receiver for Windows 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。
    b) 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。
    c) 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:

- Receiver for Web はこの機能をサポートしていません。

vPrefer 機能について詳しくは、Knowledge Center でCTX232210を参照してください。

汎用クライアント入力システム（**IME**）

February 21, 2019

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 を有効化するには、Citrix Receiver for Windows 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。

> 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 を無効化するには、Citrix Receiver for Windows 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 Receiver for Windows 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 Receiver for Windows 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. アクティブなアプリケーションセッションで、システムトレイの Citrix Receiver 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］ を選択し、［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 を無効にする場合にこのオプションを選択します。このオプションは、サーバー上で設定された言語のみ使用できることを意味します。
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する場合にこのオプションを選択します。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する場合にこのオプションを選択します。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。

設定変更は、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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys 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。

> 注
>
> ホットキー機能は、デスクトップセッションとアプリケーションセッションの両方でサポートされます。

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。

キーボードレイアウトと言語バー

January 9, 2019

キーボードレイアウト

> 注
>
> システムトレイの［Citrix Receiver］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、「高度な設定シートの非表示」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を有効にするには

1. システムトレイの Citrix Receiver for Windows アイコンで、［高度な設定］>［キーボードと言語バー］ を選択します。キーボードと言語バーのウィンドウが開きます。
2. ［保存］ をクリックします。

この機能は、［いいえ］ で無効にできます。

コマンドラインでキーボードレイアウトの同期を有効/無効にすることもできます。Citrix Receiver for Windows インストールフォルダー（C:\program files (x86)\Citrix\ICA Client）で **wfica32:exe /localime:on** または **wfica32:exe /localime:off** を実行します。

> 注:
>
> ローカル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 Receiver for Windows からログオフしてから、再度ログインしてください。

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の同期機能を復元するには、セッションにログオンし直す必要があります。

- RDP がアプリケーションとして展開され、ユーザーが RDP セッションで作業をしていると、キーボードレイアウトを Alt + Shift ショートカットで変更することはできません。この問題を回避するために、RDP セッションの言語バーで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、パフォーマンス上のリスクの可能性があるサードパーティ製品の問題によって、Windows Server 2016 で無効になっています。これは、VDA のレジストリ設定で有効にできます: HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme で、DisableKeyboardSync という名称の新しいキーを追加し、値を 0 に設定します。

言語バー

バージョン 4.11 から、グラフィカルユーザーインターフェイスを使用して、アプリケーションセッションでリモート言語バーを表示または非表示にすることができます。言語バーには、セッションで優先される入力言語が表示されます。以前のリリースでは、VDA のレジストリキーを使用することによってのみ、この設定を変更できました。Citrix Receiver for Windows バージョン 4.11 以降では、［高度な設定］ ダイアログを使用して変更できます。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。

リモート言語バーの表示または非表示を構成する

1. システムトレイで Citrix Receiver for Windows 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. 必要に応じて設定を変更します。

> 注
>
> - 設定の変更は直ちに有効になります。
> - 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 に移動します。
3. 新しい 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。

認証

August 7, 2018

環境のセキュリティを最大限に高めるには、Citrix Receiver for Windows 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 Receiver for Windows では、スマートカード認証、証明書失効一覧のチェック、Kerberos 認証によるパススルー認証など、さまざまな認証方法を構成できます。

ドメインパススルー認証の構成

January 9, 2019

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アプリケーションやデスクトップを再認証する必要なく使用できます。

Citrix Receiver 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設定後、資格情報を複数回入力することなく、Citrix Receiver にログオンして XenApp または XenDesktop セッションを開始できます。

ユーザーがアプリケーションアイコンをクリックすると、Citrix Receiver がユーザーのドメイン資格情報を Delivery Controller にパススルーし、アプリケーションまたはデスクトップが開きます。

次のいずれかのオプションを使用して Citrix Receiver をインストールする時に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
- グラフィカルユーザーインターフェイス

前提条件

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:
   a) Internet Explorer を起動します。
   b) ［ツール］ > ［インターネットオプション］ > ［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 または Web Interface 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:
   a) Internet Explorer を起動します。
   b) ［インターネットオプション］ > ［セキュリティ］ タブで、［信頼済みサイト］ をクリックします。

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。

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

Citrix Receiver for Windows を**/includeSSON** スイッチでインストールします。

Receiver for Windows を再起動して、この変更を適用します。

> 注
>
> Citrix Receiver 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 Citrix Receiver の最新バージョンにアップグレードすることはサポートされていません。

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 Receiver for Windows インストールファイル（CitrixReceiver.exe）を検索します。
2. **CitrixReceiver.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の有効化インストールウィザードで、シングルサインオンを有効にするチェックボックスをオンにして、Citrix Receiver for Windows で SSON 機能を有効にしてインストールします。これは、Citrix Receiver for Windows をコマンドラインスイッチの**/includeSSON** を使ってインストールするのと同じです。

次の図は、シングルサインオンを有効にする方法を示しています。

Receiver for Web 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、Receiver for Web のシングルサインオンを構成できます。

注：Citrix Receiver for Windows 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 に追加する必要があります。テンプレートファイルをローカル GPO に追加する方法の詳細については、https://docs.citrix.com/en-us/receiver/windows/current-release/configure/config-gpo-template.html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 Receiver GPO 管理用テンプレートを開きます。
2. ［コンピューター構成］ ノードで、［管理用テンプレート］ > ［**Citrix** コンポーネント］ > ［**Citrix Receiver**］ > ［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、［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、Citrix Receiver 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. Citrix Receiver for Windows for Web を再起動して、この変更を適用します。

Citrix Receiver を起動してシングルサインオンが有効になっていることを確認します。Receiver の起動後、タスクマネージャーを起動し、ssonsvr.exe プロセスが実行されているかを確認します。

StoreFront および **Web Interface** でのシングルサインオンの構成

StoreFront の構成

SSON を StoreFront および Web Interface で構成するには、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。

Web Interface 構成

SSON を Web Interface で構成するには、［**Citrix Web Interface** 管理］**>**［**XenApp Services** サイト］**>**［認証方法］ の順に選択して ［パススルー］ を選択します。

構成チェッカーを使用したシングルサインオンの構成の検証

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. システムトレイで Citrix Receiver for Windows を右クリックし、［高度な設定］ をクリックします。
2. ［構成チェッカー］ をクリックします。
   ［Citrix 構成チェッカー］ダイアログボックスが開きます。
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. **Status**：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：Installation。
4. **Test**：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 I 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. Web Interface/StoreFront の認証方法

> 注
>
> - Receiver for Web 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 Receiver for Windows 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。
> - Receiver for Web 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 Receiver for Windows 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。
> - Receiver for Web 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 Receiver for Windows 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。
>   - Receiver for Web 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 Receiver for Windows 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。

ドメインパススルー認証の構成方法について詳しくは、Knowledge Center のCTX133982を参照してください。

［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 Receiver 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. グループポリシーエディターで、［**Citrix** コンポーネント］>［**Citrix Receiver**］>［**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. コマンドプロンプトを開きます。
6. 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、XenApp および XenDesktop 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。

スマートカード認証の構成

April 2, 2019

Citrix Receiver for Windows では、以下のスマートカード認証機能がサポートされます。XenDesktop および StoreFront での構成については、これらの製品のドキュメントを参照してください。このトピックでは、Citrix Receiver for Windows でスマートカードを使用するための構成について説明します。

- パススルー認証（シングルサインオン） - ユーザーが Citrix Receiver for Windows 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が保持されます。これにより、Citrix Receiver for Windows でのスマートカード認証が以下のように処理されます。
  - 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の資格情報で Citrix Receiver 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のユーザーがスマートカードの資格情報で Citrix Receiver for Windows 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があります。

  パススルー認証を使用するには、StoreFront および Citrix Receiver for Windows 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、ユーザーがスマートカードを使用できない場合（スマートカードを自宅に忘れた場合や資格情報の有効期限が切れた場合など）に便利です。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。NetScaler Gateway が解決策にある場合、構成する必要もあります。

また 2 モード認証により、StoreFront 管理者は StoreFront コンソールで選択して同じストアにエンドユーザーにユーザー名とパスワードの両方とスマートカード認証を提供できます。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、Citrix Receiver for Windows を含む、ユーザーデバイス上で実行されるすべてのアプリケーションで複数の証明書を使用できるようになります。証明書の選択方法を変更するには、Citrix Receiver for Windows を構成します。
- 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、NetScaler Gateway および StoreFront での構成が必要です。
  - NetScaler Gateway を使って StoreFront リソース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になることがあります。
  - NetScaler 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、Receiver とユーザーの仮想デスクトップとの間に追加の接続が確立されます。ダブルホップセッションをサポートする展開方法については、XenDesktop のドキュメントを参照してください。
- 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、仮想デスクトップやアプリケーション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。

前提条件

このトピックの内容を理解するには、XenDesktop および StoreFront のドキュメントで説明されているスマートカードについての理解が必要です。

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 Receiver for Windows はユーザー証明書を保存しませんが、構成時に PIN を格納できます。PIN はユーザーセッションの間に非ページ化メモリにのみキャッシュされ、ディスク内にはどの時点においても格納されません。
- Citrix Receiver for Windows では、スマートカードが挿入されたときに自動的には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 Receiver for Windows 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 トンネルを使用するには、ユーザーが NetScaler 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、NetScaler Gateway Plug-in を使用した StoreFront へのパススルー認証を使用できません。

- Citrix Receiver for Windows Updater と citrix.com や Merchandising Server 間の通信では、NetScaler Gateway 上のスマートカード認証を使用できません。

> 警告
>
> このトピックの一部の構成手順では、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、深刻な問題が発生する可能性があり、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。

スマートカード認証のシングルサインオンを有効にするには

Citrix Receiver for Windows 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。

- 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 Receiver for Windows で PIN を繰り返し入力する必要がなくなります。

または、以下のポリシーおよびレジストリを設定します:

- [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 Receiver] > [ユーザー認証] > [ローカルユーザー名とパスワード]
- シングルサインオンコンポーネントをインストールしていないデバイス上で、以下のいずれかのレジストリキーで SSONCheckEnabled に false を設定します。これにより、Citrix Receiver for Windows 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 Receiver for Windows で StoreFront への認証が可能になります。

  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

または、Kerberos の代わりに Storefront に対してスマートカード認証を有効にできます。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 Citrix Receiver for Windows をインストールします。これには管理者権限が必要です。マシンをドメインに参加させる必要はありません。

- /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。
- Receiver 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 Receiver for Windows へのログオン時に PIN を格納することができます。

- グループポリシーエディターで、[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 Receiver] > [ユーザー認証] > [ローカルユーザー名とパスワード] の順に選択します。

  パススルー認証を有効にします。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する必要があります。

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 Receiver for Windows 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 Receiver for Windows 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、2048、または 4096 ビットである。
- Key Usage フィールドに Digital Signature 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 Receiver for Windows のコマンドラインで、`AM\\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` オプションを指定する。

  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、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。

- レジストリキー HKCU または HKLM\Software\[Wow6432Node\]Citrix\AuthManager: `CertificateSelection ={ Prompt | SmartCardDefault | LatestExpiry }` を追加する。

  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

Citrix Receiver for Windows 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 Receiver for Windows 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 Receiver for Windows のコマンドラインで、AM_SMARTCARDPINENTRY=CSP オプションを指定する。
- レジストリキー HKLM\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP を追加する。

Kerberos を使用したドメインパススルー認証の構成

January 9, 2019

このトピックの内容は、Citrix Receiver for Windows と StoreFront、XenDesktop、または XenApp 間の接続にのみ適用されます。

Citrix Receiver for Windows 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。

Kerberos 認証を有効にすると、認証時に Citrix Receiver for Windows 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、指紋照合などの生体認証も含めて、さまざまな認証方式を使用してユーザーデバイスにログオンでき、公開リソースへ接続するときに資格情報を再入力する必要もありません。

Citrix Receiver for Windows、StoreFront、XenDesktop、および XenApp でスマートカード認証が構成されており、ユーザーがスマートカードを使用する場合、Citrix Receiver for Windows では Kerberos によるパススルー認証が以下のように処理されます。

1. Citrix Receiver for Windows のシングルサインオンサービスがスマートカードの PIN を取得します。
2. Citrix Receiver for Windows は、IWA（Kerberos）を使用して StoreFront へのユーザー認証を行います。すると、使用可能な仮想デスクトップおよびアプリケーションの情報を StoreFront が Citrix Receiver for Windows に提供します。
   注: この段階では Kerberos 認証を使用する必要はありません。Citrix Receiver for Windows での Kerberos の有効化は、PIN の再入力が求められないようにする場合のみ必要です。Citrix Receiver for Windows 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 XenDesktop または XenApp に渡します。これにより、ユーザーが Windows セッションにログオンできます。最後に、XenDesktop または XenApp が、要求されたリソースを配信します。

Citrix Receiver for Windows 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 Receiver for Windows 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 XenDesktop や XenApp 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を使用したり、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。

このトピックの以降のセクションでは、一般的な環境でのドメインパススルー認証の構成方法について説明します。カスタムの認証ソリューションを使用していた Web Interface 環境を StoreFront に移行する場合の注意事項については、Citrix のテクニカルサポート担当者に問い合わせてください。

> 警告
>
> このトピックの一部の構成手順では、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、深刻な問題が発生する可能性があり、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、Citrix 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を構成するには

XenDesktop 環境でのスマートカード展開について精通していない場合は、XenDesktop ドキュメントの「展開環境の保護」のスマートカードに関する内容を事前に理解しておくことをお勧めします。

Citrix Receiver for Windows 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、Citrix Receiver for Windows 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、XenDesktop 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。XenDesktop 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。

  関連するオプションの ENABLE_SSON はデフォルトで有効になっています。これを無効にしないでください。

  何らかのセキュリティポリシーによりデバイス上でシングルサインオンを有効にすることが禁止されている環境では、以下のポリシーを使用して Citrix Receiver for Windows を構成します。

  [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 Receiver] > [ユーザー認証] > [ローカルユーザー名とパスワード]

  > 注
  >
  > このシナリオでは、HDX エンジンで Kerberos ではなくスマートカード認証を使用しています。このため、HDX エンジンで常に Kerberos を使用するためのオプション ENABLE_KERBEROS=Yes は使用しないでください。

設定を適用するには、ユーザーデバイス上の Citrix Receiver for Windows を再起動します。

StoreFront を構成するには:

- StoreFront サーバー上の default.ica ファイルで、DisableCtrlAltDel を false に設定します。

> 注
>
> すべてのクライアントマシンで Citrix Receiver for Windows 4.2 以降を実行している場合には、この手順は必要がありません。

- 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] チェックボックスをオンにします。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] チェックボックスは、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。

FastConnect API および HTTP 基本認証について

FastConnect API は HTTP 基本認証方式を採用しています。これは、ドメインパススルー、Kerberos、および IWA に割り当てられている認証方式と頻繁に混同されます。Citrix は、StoreFront 上や ICA グループポリシーでは IWA を無効にすることをお勧めします。

証明書失効一覧を使用してセキュリティ保護を強化

January 9, 2019

証明書失効一覧（CRL）のチェック機能を有効にすると、サーバー証明書が失効していないかどうかが Citrix Receiver for Windows によってチェックされます。強制的にこ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には、いくつかの設定レベルが用意されています。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 Receiver for Windows 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。

ローカルのコンピューターにこの変更を適用する場合は、Citrix Receiver for Windows を終了してください。コネクションセンターを含むすべての Citrix Receiver for Windows コンポーネントが閉じていることを確認してください。

TLS の構成について詳しくは、「TLS の構成および有効化」を参照してください。

セキュリティで保護された通信

November 12, 2018

XenDesktop サイトや XenApp ファームと Citrix Receiver for Windows 間の通信を保護するには、以下の一連のセキュリティ技術を使用します。

- Citrix NetScaler Gateway：詳しくは、このセクションのトピックと、NetScaler Gateway および StoreFront のドキュメントを参照してください。
  注：StoreFront サーバーとユーザーデバイス間の通信を保護するには、NetScaler Gateway を使用することをお勧めします。
- 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。サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（Network Address Translation：ネットワークアドレス変換））を介して Citrix Receiver for Windows を使用する場合は、外部アドレスを構成します。
- 信頼するサーバーの構成。
- XenApp または Web Interface 展開環境でのみ。XenDesktop 7 には適用されません。SOCKS プロキシサーバーまたは Secure プロキシサーバー（セキュリティプロキシサーバー、HTTPS プロキシサーバーとも呼ばれます）。プロキシサーバーで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、Receiver とサーバー間の接続を制御できます。Receiver は、SOCKS プロトコルと Secure プロキシプロトコルをサポートしています。

- XenApp または Web Interface 展開環境では、TLS（Transport Layer Security）プロトコルを使用する Citrix SSL Relay（XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、または XenApp 7.5 には適用されません）。
- XenApp 7.6 および XenDesktop 7.6 の場合、ユーザーと VDA 間で直接 SSL 接続を有効にできます

Citrix Receiver for Windows は、Microsoft 社のセキュリティ特化 - 機能制限（Specialized Security - Limited Functionality：SSLF）デスクトップセキュリティテンプレートが使用されている環境と互換性があります。これらのテンプレートは、さまざまな Windows プラットフォームでサポートされています。
詳しくは、Microsoft 社の Web サイトhttp://technet.microsoft.comで公開されている、Windows の『セキュリティガイド』を参照してください。

信頼関係の適用

November 12, 2018

信頼済みサーバー構成を使用して、Citrix Receiver for Windows の接続で信頼関係を識別し適用できます。

信頼済みサーバー機能を有効にすることで、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/など）に特定の接続の種類（TLS など）を使用して接続する Citrix Receiver for Windows 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 Receiver for Windows コンポーネントを終了します。

1. gpedit.msc を管理者として実行して、Citrix Receiver 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。
   a) 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver 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。
   b) ドメインでポリシーを適用するには、グループポリシー管理コンソールを使用して、Citrix Receiver 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。
2. ［コンピューターの構成］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 Receiver**］、［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 Receiver for Windows 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] ドロップダウンリストから、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。

Web Interface 5.4 でのスマートカード認証の構成

January 9, 2019

Citrix Receiver for Windows を SSON コンポーネントとともにインストールすると、XenApp PNAgent サイトでスマートカードの PIN パススルー認証が有効化されていない場合でも、デフォルトでパススルー認証が有効になります。認証方法でパススルーを設定しても有効にはなりません。次の画像に、Citrix Receiver for Windows で SSON が適切に構成されている場合にスマートカードを認証方法として有効にする方法を示します。

Citrix Web Interface 5.4 PNAgent サイトでユーザーが認証されている場合のスマートカードの取り出し動作を制御するには、スマートカードの取り出しポリシーを使用します。

このポリシーが有効な場合、クライアントデバイスからスマートカードが取り出されるとユーザーは XenApp セッションからログオフされます。ただし、ユーザーは Citrix Receiver for Windows には引き続きログインしたままになります。

このポリシーを有効にするには、Web Interface XenApp Services サイトでスマートカードの取り出しポリシーを設定する必要があります。この設定は、Web Interface 5.4 の [**XenApp Services** サイト] **>** [スマートカードパススルー認証] **>** [ローミングを有効にする] **>** [スマートカードの取り出し時にセッションをログオフする] で行います。

スマートカードの取り出しポリシーが無効な場合、クライアントデバイスからスマートカードが取り外されるとユーザーの XenApp セッションは切断されます。Web Interface XenApp Services サイトでスマートカードを取り出しても影響はありません。
注：32 ビットクライアントと 64 ビットクライアント向けのポリシーは異なります。32 ビット向けのポリシーの名前は スマートカードの取り出しポリシー（**32** ビットマシン） であり、64 ビット向けのポリシー名は スマートカードの取り出しポリシー（**64** ビット） です。

スマートカードのサポートおよび取り出しの変更

XenApp 6.5 PNAgent サイトに接続する場合は次の点に注意してください。

- Citrix Receiver for Windows 4.5 より、PNAgent サイトへのログインでもスマートカードによるログインがサポートされるようになりました。

- PNAgent サイトでのスマートカードの取り出しポリシーは次のように変更されました。
  スマートカードを取り外すと XenApp セッションからログオフされます。ただし、PNAgent サイトの認証方法をスマートカードに設定している場合、XenApp セッションからのログオフを有効にするには Receiver for Windows で対応するポリシーを構成する必要があります。XenApp PNAgent サイトでスマートカード認証のローミングを有効にして、Receiver セッションから XenApp をログオフするスマートカードの取り出しポリシーを有効にします。ユーザーは Receiver 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 PNAgent 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。

プロキシサーバー経由の接続

August 7, 2018

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、Citrix Receiver for Windows とサーバー間の接続を制御するために使います。Citrix Receiver for Windows は、SOCKS プロトコルと Secure プロキシプロトコルをサポートしています。

Receiver がサーバーファームと通信する時は、Receiver for Web または Web Interface のサーバー上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。プロキシサーバーの構成については、StoreFront または Web Interface のドキュメントを参照してください。

また、Receiver が Web サーバーと通信する時は、ユーザーデバイス上のデフォルトの Web ブラウザーで構成したプロキシサーバー設定が使用されます。このため、サーバーと正しく通信できるように、事前にユーザーデバイス上の Web ブラウザーでインターネット接続を設定しておく必要があります。

接続中に Citrix Receiver for Windows 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、Windows 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、Citrix では一切責任を負いません。

1. HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\に移動します。\
2. **ProxyEnabled**（REG_SZ）を設定します。
   a) True – Citrix Receiver for Windows は接続でプロキシサーバーを優先します。
   b) False – Citrix Receiver for Windows は接続でプロキシサーバーを無視します。
3. レジストリエディターを閉じます。

4. Citrix Receiver for Windows のセッションを再起動して、この変更を適用します。

ICA ファイルに署名して信頼されていないサーバー上のアプリケーションやデスクトップが起動しないようにする

January 9, 2019

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 Receiver for Windows 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、StoreFront、または Citrix Merchandising Server 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 のドキュメントを参照してください。

Web Interface 展開の場合、Web Interface でこの機能を有効にして構成し、Citrix ICA File Signing Service を使用して起動処理中にアプリケーションまたはデスクトップの起動に署名を含めることができます。このサービスにより、コンピューターの個人証明書ストアにある証明書を使用して ICA ファイルに署名できます。

Citrix Merchandising Server と Citrix Receiver for Windows を組み合わせて、起動署名検証を有効にして構成できます。これを行うには、Citrix Merchandising Server Administrator Console の Deliveries ウィザードを使用して、信頼できる証明書の「拇印」を追加します。

グループポリシーオブジェクト管理用テンプレートで ICA ファイルの署名を構成する

> 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 Receiver 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. ［コンピューター構成］ノードで、［管理用テンプレート］、［Citrix コンポーネント］の順に移動します。
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 - 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。
        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。無効な署名の場合、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。

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. Web Interface のサーバー証明書などの既存の SSL 証明書を使用する。
4. 新しい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。

廃止された暗号の組み合わせの構成

January 9, 2019

> 注
>
> Citrix Receiver for Windows 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 に追加する必要があります。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の構成」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 Receiver 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 Receiver**］ > ［ネットワークルーティング］ の順に移動します。
3. ［廃止された暗号の組み合わせ］ ポリシーを選択します。
4. ［有効］ を選択し、次のオプションから選択します：
   a) **TLS_RSA_**：デフォルトでは、*TLS_RSA_* が選択されています。他の 2 つの暗号の組み合わせを使用するには、このオプションを選択する必要があります。このオプションを選択すると、次の暗号の組み合わせが含まれます。
      i. TLS_RSA_AES256_GCM_SHA384
      ii. TLS_RSA_AES128_GCM_SHA256
      iii. TLS_RSA_AES256_CBC_SHA256
      iv. TLS_RSA_AES256_CBC_SHA
      v. TLS_RSA_AES128_CBC_SHA
      vi. TLS_RSA_3DES_CBC_EDE_SHA

b) **TLS_RSA_WITH_RC4_128_MD5**：RC4-MD5 暗号の組み合わせを使用する場合、このオプションを選択します。
c) **TLS_RSA_WITH_RC4_128_SHA**：RC4_128_SHA 暗号の組み合わせを使用する場合、このオプションを選択します。

5. ［適用］、［**OK**］ の順にクリックします。
6. この変更を有効にするには、gpupdate /force コマンドを実行します。

次の表は、各セットの暗号の組み合わせを示しています：

TLS の構成および有効化

February 21, 2019

このトピックは、XenApp および XenDesktop のバージョン 7.6 以降に適用されます。

すべての Citrix Receiver for Windows 通信を TLS で暗号化するには、ユーザーデバイス、Citrix Receiver for Windows、および Web Interface サーバー（使用している場合）を構成します。Web Interface の保護については、Web Interface のドキュメントのセキュリティに関するセクションを参照してください。

前提条件

ユーザーデバイスは、[「システム要件」] で指定された要件を満たす必要があります。(/ja-jp/receiver/windows/current-release/system-requirements.html)

このポリシーを使用して TLS オプションを構成します。このオプションにより、Citrix Receiver for Windows で接続先のサーバーを安全に識別して、サーバーとのすべての通信を暗号化できます。

このオプションで、以下が可能になります：

- 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すべての接続で、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への準拠を可能にする。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。Citrix Receiver for Windows と XenApp/XenDesktop 間で TLS 1.0、TLS 1.1、TLS 1.2 プロトコルがサポートされます。
- 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）。

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 **TLS** サポートを構成する

1. gpedit.msc を管理者として実行して、Citrix Receiver 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。
   - 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver 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。
   - ドメインでポリシーを適用するには、グループポリシー管理コンソールを使用して、Citrix Receiver 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。
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 Receiver**］ > ［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：保護された接続で、TLS を使用することをお勧めします。

4. ［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 Receiver for Windows のすべての通信で強制的に TLS を使用させることができます。
5. ［セキュリティコンプライアンスモード］ ドロップダウンリストから、適切なオプションを選択します：
   - なし – コンプライアンスモードが適用されません。
   - **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 Receiver for Windows 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］ で ［完全なアクセス権のチェック］ または ［完全なアクセス権のチェックと **CRL** が必要です］ のいずれかも選択する必要があります。

     ［SP800-52］を選択すると、Citrix Receiver for Windows 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 Receiver for Windows が接続できないことがあります。
6. **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 Receiver for Windows 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。

7. [許可された **TLS** サーバー] ドロップダウンリストから、ポート番号を選択します。Citrix Receiver がコンマ区切りの一覧で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 Receiver が証明書の発行者を認識して信頼しないと、接続は拒否されます。

8. [**TLS** バージョン] ドロップダウンリストから、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 ICA 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。

9. **TLS** 暗号の組み合わせ - 特定の TLS 暗号の組み合わせ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 NetScaler Gateway 構成では、COM の選択が必要になることがあります。Citrix Receiver for Windows 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 キーの使用はお勧めしません。

   以下は、サポートされるすべての暗号の組み合わせの一覧です。

   - 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:
     - TLS_RSA_WITH_RC4_128_MD5
     - TLS_RSA_WITH_RC4_128_SHA
     - TLS_RSA_WITH_3DES_EDE_CBC_SHA
     - TLS_RSA_WITH_AES_128_CBC_SHA
     - TLS_RSA_WITH_AES_256_CBC_SHA
     - TLS_RSA_WITH_AES_128_GCM_SHA256
     - 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:
     - TLS_RSA_WITH_RC4_128_MD5
     - TLS_RSA_WITH_RC4_128_SHA
     - TLS_RSA_WITH_AES_128_CBC_SHA
     - 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:
     - TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

10. ［証明書失効チェックのポリシー］ ドロップダウンリストから、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/Secure 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出は、ターゲットサーバーで提示されるサーバー証明書の検証に必要ではありません。
    - 完全なアクセス権と **CRL** のチェックが必要です - ルート CA 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。
11. ［ポリシーの拡張 **OID**］ を使用して、Citrix Receiver for Windows 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 Receiver for Windows 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。
12. ［クライアント認証］ ドロップダウンリストから、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。
13. ［**Client Certificate**］ 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。
14. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。

次の表は、各セットの暗号の組み合わせを示しています:

Secure Gateway による接続

November 12, 2018

このトピックの内容は、Web Interface 環境にのみ適用されます。

Secure Gateway を通常モードまたはリレーモードのどちらかで使用すると、Citrix Receiver for Windows とサーバー間の通信チャネルをセキュリティで保護できます。Secure Gateway を通常モードで使用していて、ユーザーが Web Interface 経由で接続する場合は、Citrix Receiver for Windows の構成は不要です。

Citrix Receiver for Windows が Secure Gateway サーバーと通信する時は、リモートの Web Interface サーバーで構成されている設定が使用されます。Citrix Receiver for Windows のためにプロキシサーバー設定を構成する方法については、Web Interface のトピックを参照してください。

プロキシサーバー設定の構成について詳しくは、Web Interface のドキュメントを参照してください。

Secure Gateway Proxy がセキュリティで保護されたネットワーク内のサーバーにインストールされている場合は、Secure Gateway Proxy をリレーモードで使用できます。

ただし、リレーモードで使用する場合、Secure Gateway サーバーはプロキシサーバーとして機能するため、Citrix Receiver for Windows で次の項目を構成する必要があります。

- Secure Gateway サーバーの完全修飾ドメイン名。
- Secure Gateway サーバーのポート番号。Secure Gateway, Version 2.0 では、リレーモードはサポートされていません。

完全修飾ドメイン名には、以下の 3 つの要素を順に指定する必要があります:

- ホスト名
- サブドメイン名
- 最上位ドメイン名

たとえば、my_computer.my_company.com は完全修飾ドメイン名です。ホスト名（my_computer）、サブドメイン名（my_company）、最上位ドメイン名（com）が順に指定されています。一般的には、サブドメイン名と最上位ドメイン名の組み合わせ（my_company.com）をドメイン名といいます。

昇格レベルと **wfcrun32.exe**

November 12, 2018

Windows 10、Windows 8、または Windows7 を実行するデバイスでユーザーアカウント制御（UAC）が有効な場合は、wfcrun32.exe と同じ昇格/整合性レベルのプロセスのみが仮想アプリケーションを起動できます。

例 **1**:

（昇格されていない）標準ユーザーが wfcrun32.exe を実行してアプリケーションを起動する場合は、Receiver など他のプロセスを標準ユーザーとして実行する必要があります。

例 **2**:

wfcrun32.exe を昇格モードで実行する場合は、非昇格モードで動作する Receiver、コネクションセンター、および ICA クライアントオブジェクトを使用するサードパーティアプリケーションは wfcrun32.exe と通信できません。

Citrix Receiver for Windows Desktop Lock

April 2, 2019

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 Receiver for Windows Desktop Lock を使用できます。Desktop Viewer（有効な場合）を引き続き使用することはできますが、ツールバー上には必須オプションセットである Ctrl+Alt+Del、基本設定、デバイス、および切断しかありません。

Citrix Receiver for Windows Desktop は、SSON（Single Sign-On：シングルサインオン）が有効化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。また、SSON が有効ではない非ドメイン参加のマシンでも使用できます。Program Neighborhood エージェント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。

Citrix Receiver for Windows 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、「コマンドラインを使った Citrix Receiver のインストールと構成」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にある CitrixReceiverDesktopLock.MSI を使って Citrix Receiver for Windows Desktop Lock をインストールします。

Citrix Receiver Desktop Lock のシステム要件

- 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。
- ドメイン参加および非ドメイン参加のエンドポイント。
- 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、XenApp および XenDesktop 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」を参照してください。

Citrix Receiver for Windows Desktop Lock の使用

- Citrix Receiver for Windows Desktop Lock では次の Citrix Receiver for Windows 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 Receiver for Windows 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 の各プロパティを未設定の Citrix Receiver for Windows Desktop Lock に最適化されています。
- 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。詳しくは、「リモートセッションでの Windows ショートカットキーの実行」を参照してください。
- 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。

Citrix Receiver for Windows Desktop Lock をインストールするには

この手順に従って Citrix Receiver for Windows をインストールすると、Citrix Receiver Desktop Lock で仮想デスクトップが表示されます。スマートカードを使用する展開については、「Receiver Desktop Lock を実行するデバイスでスマートカードを使用できるように構成するには」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（インストールメディアの Citrix Receiver and Plug-ins > Windows > Citrix Receiver for Windows フォルダーにあります）を実行します。

   次に例を示します:

```
CitrixReceiver.exe
      /includeSSON
```



```
3 STORE0=”DesktopStore;https://my.storefront.server/Citrix/MyStore/
    discovery;on;Desktop Store”
```

コマンドについて詳しくは、「コマンドラインパラメーターを使用した Receiver for Windows の構成とインストール」の Citrix Receiver for Windows のインストールに関する説明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 CitrixReceiverDesktopLock.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、Receiver 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、CitrixReceiverDesktopLock.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。

Receiver 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 CitrixReceiverDesktopLock.msi /qn

Citrix Receiver for Windows Desktop Lock を構成するには

Citrix Receiver for Windows Desktop Lock を使用するユーザーには、単一の仮想デスクトップだけのアクセスを付与します。

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 Receiver for Windows 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 Receiver］>［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、［既存の USB デバイス］と［新しい USB デバイス］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 Receiver］>［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、［クライアントドライブマッピング］ポリシーを有効にして構成します。
- マイク - ［Citrix Receiver］>［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、［クライアント側マイク］ポリシーを有効にして構成します。

Citrix Receiver for Windows Desktop Lock を実行するデバイスでスマートカードを使用できるように構成するには

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 Receiver］>［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 Receiver for Windows 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://」形式で追加します。デリバリーグループ名 >
   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 Receiver for Windows 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 Receiver for Windows Desktop Lock があるユーザーデバイスにのみ適用されます。

Citrix Receiver for Windows Desktop Lock をアンインストールするには

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 Receiver for Windows 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 Receiver for Windows Desktop Lock をアンインストールします。
    - Citrix Receiver for Windows 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+Del - 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。

そのほか

- 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

November 12, 2018

Citrix Common Connection Manager SDK

Common Connection Manager（CCM）SDK は、基本的な操作をプログラム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、Citrix Receiver for Windows 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、XenApp セッションまたは XenDesktop 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
  - Receiver の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
  - Receiver の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ー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、XenApp または XenDesktop サーバー上にあります。このバージョンの SDK は、Receiver for Windows 用の新しい仮想チャネルの作成をサポートします。他のクライアントプラットフォーム用の仮想ドライバーの作成については、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（VDAPI）。VDAPI 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。

SDK のドキュメントについては、Citrix Virtual Channel SDK for Citrix Receiver for Windowsを参照してください。

Fast Connect 3 Credential Insertion API

Fast Connect 3 Credential Insertion API は、Citrix Receiver for Windows 4.2 以降のシングルサインオン（SSON）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 または Web Interface 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。

Fast Connect API については、Fast Connect 3 Credential Insertion API for Citrix Receiver for Windowsを参照してください。

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