Citrix Receiver for Windows 4.6について

Dec 08, 2016

Citrix Receiver for Windowsを使用して、ユーザーはXenAppサーバーやXenDesktopサーバーで公開されている仮想デスクトップやアプリケーションに安全にアクセスできます。

キーボードレイアウトの同期

このリリースから、Citrix Receiver for WindowsはセッションのクライアントおよびVDAでキーボードレイアウトを動的に同期できます。 ユーザーは、クライアントデバイスの優先キーボードレイアウトを切り替えることができ、たとえば、タッチキーボードのレイアウトを英語からスペイン語に変更するときに、一貫したユーザーエクスペリエンスを提供します。 ユーザーがレイアウトを切り替えると、同期の進行中、一時的にメッセージが表示されます。 その後、新しいキーボードレイアウトで作業を続けることができます。

キーボードレイアウトについて詳しくは、「キーボードレイアウト」を参照してください。

SNI（Server Name Indication）のサポート

このリリースから、Citrix Receiver for Windowsは、SNI（Server Name Indication）を構成済みのNetScaler Gatewayをサポートします。これによって、ユーザーはデスクトップおよびアプリケーションを正常に起動できます。 SNIについて詳しくは、Knowledge CenterのCTX125798を参照してください。

Enlightened Data Transport（評価目的のみ）

Enlightened Data Transport（EDT）は、高速ネットワークでデータを転送するために使用される、高度なデータ転送プロトコルです。 EDTの利点は、TCPとデータ帯域幅を同時に共有できることです。 EDTは、WAN接続での使用をお勧めします。

このリリースから、Citrix Receiver for WindowsはEDTをサポートするため、XenAppまたはXenDesktopのThinwireディスプレイリモート処理、ファイル転送（クライアントドライブマッピング）、印刷、マルチメディアリダイレクト、その他の機能で、ユーザーエクスペリエンスが向上します。 EDTによって、サーバー間のICAトラフィックを最適化できます。 ユーザーは、オプションでReceiverとVDA間の接続の種類を選択できます。 使用できる種類は、EDTとTCPです。 これは、実稼働以外の環境の新しいポリシー設定［Receiverのトランスポート プロトコル］で有効にできます。 新しいポリシー設定を［優先］に設定すると、TCPへのフォールバックとともにEDTを使用できます（使用可能な場合）。

EDTを構成する手順について詳しくは、「Enlightened Data Transportの構成」を参照してください。

HTML5ビデオリダイレクト - 社内で制御するコンテンツ

社内WebサイトのHTML5ビデオリダイレクトは、仮想環境でHTML5ビデオコンテンツのスムーズなオーディオとビデオ表示、およびサーバースケーラビリティのバランスを最適化します。 HTML5ビデオリダイレクトは、XenAppおよびXenDesktopサーバーがHTML5マルチメディアWebコンテンツをユーザーに配信する方法を制御し、最適化します。 この機能はサーバー側で設定され、デフォルトで無効になっています。

この機能は、Microsoft Edgeではサポートされません。

次のビデオコントロールがサポートされています。

- 再生
- 一時停止

- 検索
- 繰り返し
- オーディオ
- 全画面

Citrix Receiver for Windowsでの構成は必要ありません。 Citrix Receiver for WindowsがRAVEプロトコルをサポートする場合、HTML5ビデオリダイレクトは自動的にサポートされます。

Citrix Receiver for Windowsの新しい管理用テンプレートファイル

Citrix Receiver for Windowsの新しいテンプレートファイルは、CitrixBase.admx/CitrixBase.admlという名称でこのリリースから導入されました。 通常、このファイルは<インストールディレクトリ>\ICA Client\Configurationフォルダーにあります。

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。

テンプレートファイルについて詳しくは、「Citrix Receiver for Windowsでグループポリシーオブジェクト管理用テンプレートを構成する」を参照してください。

暗号の組み合わせの拡張サポート

このリリースで、Citrix Receiver for Windowsは以下の2つの暗号の組み合わせをサポートするようになりました。

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

暗号の組み合わせについて詳しくは、「TLSおよびグループポリシー」を参照してください。

Citrix Receiver for Windows 4.6で解決された問題

Jan 24, 2017

Citrix Receiver for Windows 4.5との比較

キーボード

- Microsoft Surface Proデバイスで外部USBキーボードまたはワイヤレスキーボードを使用して文字を入力するたびに、Citrix Receiver for Windowsセッションでローカルのスクリーンキーボードが表示されることがあります。

  [#LC5093]

ローカルアプリケーションアクセス

- ローカルアプリケーションアクセスを有効にすると、全画面モードまたはウインドウモードのリモートセッションでアプリケーションを起動した場合、アプリケーションアイコンがVDAセッションのタスクバーで表示されないことがあります。 エンドポイントで、1つではなく複数のアプリケーションアイコンがタスクバーに表示されることがあります。

  [#LC4217]

- ローカルアプリケーションアクセスを使用すると、特定のソフトフォンアプリケーションやChromeが正しく表示されないことがあります。

  [#LC4327]

メモリ、CPUの最適化

- SelfServicePlugin.exeプロセスによってメモリの消費量が多くなることがあります。

  [#LC4509]

印刷

- EMFプリンタードライバーで埋め込み記号を含むフォントを使用すると、フォントの埋め込みに失敗することがあります。

  [#LC3334]

セッション/接続

- NotificationDelayレジストリ設定では、シームレス接続での接続の進行状況バーの表示遅延を管理します。 SelfService Pluginを使用してアプリケーションを起動するときに、このレジストリの設定が機能しないことがあります。 この修正により、その問題が解決されます。

  32ビットWindows：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  値の名前：NotificationDelay
  種類：REG_DWORD
  値のデータ：<遅延（ミリ秒） in milliseconds>

  64ビットWindows：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  値の名前：NotificationDelay
  種類：REG_DWORD
  値のデータ：<遅延（ミリ秒） in milliseconds>

  [#LC4969]

- Single Sign-onプロセス（SSONSvr.exe）が予期せず終了するか、資格情報がログオン画面に自動的に渡されず、資格情報の手動入力を要求するメッセージが表示されることがあります。

  [#LC5123]

- Citrix Receiver for Windowsをインストールして、レジストリエントリまたはGroup Policy Object（GPO）経由でストアを構成すると、仮想マシン（VM）の再起動後の最初のログオンで、アプリケーションが列挙できないことがあります。

  [#LC5198]

- SpeechMikeを別の音声認識アプリケーションとともに使用して口述すると、SpeechMikeが停止することがあります。

  [#LC5632]

- タッチおよびドラッグジェスチャ中、シームレスEPICアプリケーションを使用すると、マウスボタンがダウン状態のままになることがあります。 シームレスEPICアプリケーションのウインドウ外でタッチ入力を解放すると、セッションが応答しなくなることがあります。

  [#LC5644]

- HDX Engineが、予期せず終了する場合があります。

  [#LC6047]

- NetScaler Gateway 11でWyseシンクライアントから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。

  「クライアントからサーバーへの認証で問題が発生しました（Your client has experienced a problem with authentication to the server）」

  [#LC6145]

スマートカード

- Citrix Receiver for Windows 4.4をインストールすると、XenApp 6.5の公開アプリケーションがスマートカードにトランザクション要求を送り、アクティブではないトランザクションを終了することがあります。 Citrix Receiver for Windowsがこの要求に誤って応答することがあり、XenAppサーバーが応答をいつまでも、または設定されたトランザクションタイムアウト値に達するまで待機します。

  [#LC5772]

User Experience

- This fix provides improved support for sounds that play for a short period of time when using real-time mode for client audio. This fix only applies to medium quality audio.

  [#LC4941]

- File type association might not connect the type of file to the correct icon and application when using Windows 8.1 and Windows Server 2012 R2. With this fix, there are two group policies introduced under "SelfService."
  1. Enable Default FTA - To enable or disable the default behavior of FTA
  2. Enable FTA - To enable or disable the FTA feature
  To get the proper file type association icon, disable the group policy "Enable Default FTA."

  [#LC5485]

- The file type association (FTA) icon might behave like the default Citrix Receiver for Windows FTA icon when you log on to a published desktop or if you reset the Citrix Receiver for Windows configuration.

  [#LC5730]

- Desktops assigned on a client name basis are not enumerated correctly in the SelfService window. This issue occurs when using the StoreFront Unified Experience.

  [#LC5773]

ユーザーインターフェイス

- ローカルアプリケーションアクセスを有効にしてスキンモードでVLC Media Playerを使用すると、エンドポイントがタスクバーのショートカットを1つではなく複数表示することがあります。

  [#LC4744]

- XenApp 6.xで公開されているアプリを使用すると、アプリケーションがサブフォルダーに表示されることがあります。

  [#LC5880]

Version 4.6におけるその他の修正

- wfica32.exeプロセスでGDIオブジェクトが解放されない場合があります。 GDIオブジェクト数が1,000に達すると、ユーザーデバイス上でXenDesktopセッションウィンドウのグラフィカル更新が行われなくなり、グラフィックに関する問題が発生します。

  [#654723]

注：このバージョンのCitrix Receiver for Windowsには、4.5、4.4、4.3、4.2、4.1、4.0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。

Citrix Receiver for Windows 4.6の既知の問題

Jan 27, 2017

このリリースでは、以下の既知の問題が確認されています。

- Citrix Receiverを最新バージョンにアップグレードすると、クライアント自動再接続機能やセッション画面の保持機能のカスタム設定は保持されず、デフォルトの設定が復元されます。

  [#659754]

このリリースでは、以下の既知の問題が確認されています。

- 匿名ユーザーセッションに対しては、切断時のDesktop Viewerのアラートメッセージが表示されません。 これは仕様です。

  [#481561]

- システムトレイ通知がデスクトップロックモードで見られることがあります。

  [#488620]

- Citrix Receiver for Windowsは、ユーザー（非管理者）アカウントではWindows Server 2012 R2マシンにインストールできません。

  この問題を解決するには、次の手順に従います。

  1. ［スタート］をクリックして「regedit」と入力し、Enterキーを押します。
  2. 次の設定を見つけます。

  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

  Create: DisableMSI Type: REG_DWORD value = 0（0に設定するとインストールできます）

  [#492508]

- Desktop Lockクライアントのログオン画面に言語バーが表示されません。 解決策として、浮動言語バーを使用します。

  [#502678]

- セッションをウィンドウモードで開くと、Citrix Desktop Viewerの **[ショートカット]** オプションが機能しません。

  [#510529]

- 7.0よりも前のバージョンのXenAppおよびXenDesktop、またはWindow 2008 R2上のXenAppおよびXenDesktop 7.0以降を介してリモート操作されるアプリケーションでは、ピンチおよびズームジャスチャーは機能しません。

  [#517877]

- 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。

  [#534790]

- Citrix Receiver for WindowsをインストールしたWindows 10 RTM Version 1511にMicrosoft Windows 10 Anniversary Update（Version 1607）を適用すると、Single Sign-Onプロセス（SSONSvr.exe）でエラーが発生する場合があります。

  [#540988]

- RAVEとの互換性の問題のため、セッション内のRealTimes（Real Player）でボリュームコントロールが機能しないことがあります。

  [#573549]

- HDX 3D Proを有効にしたセッションを50以上のFPSで実行すると、Desktop Viewer（CDViewer.exe）が予期せず終了し、ユーザーセッションが応答しなくなることがあります。

  [#597875]

- Citrix Receiver for Windowsでは、ファイル名に奇数バイトのUTF-8文字が含まれている場合に、ファイルタイプの関連付けで問題が生じることがあります。

  [#602107]

- Windows 10 Surface Proデバイス上でホストされているアプリケーションの方向を変更すると、「全画面モードを終了している」ことを示すツールチップ画面が表示されます。 この問題を回避するには、以下のレジストリキーを設定してヒントダイアログメッセージを無効にします。

  HKEY_CURRENT_USER/softwareHKCU/software/citrix/ica client/keyboard mappings/tips

  値を1にするとヒントが無効になり、0にすると有効になります。このレジストリキー値を1に設定してすべてにヒントを無効にします。

  [#608346]

- クライアントでハードウェアデコードが有効な場合にH.264 GraphicsモードでWindows 2008 R2 VDAに接続すると、パフォーマンスが低下します。 この問題を避けるには、VDAでレガシーグラフィックモードを使用することをお勧めします。

  [#609292、#611580]

- StoreFront側で［統合エクスペリエンスの構成］オプションを有効にしている場合、Self-Service Plug-inに自動更新時に更新できないことがあります。 また、最近Desktop Delivery Controller側から追加または削除したアプリケーションの列挙も、ユーザーデバイス上では手動で更新しないと更新されないことがあります。

  [#623041]

- 通知領域のCitrix Receiver for Windowsアイコンを右クリックしたときに、［スタート］メニューオプションにある［スタートメニューでアプリケーションを表示します］が灰色表示されないことがあります。 この問題は、XenApp Servicesサイトにログオンしている場合に発生します。

  [#639947]

- Microsoft Windows VistaでXenAppセッションを起動できないことがあります。 この問題を回避する方法について詳しくは、Knowledge CenterのCTX216607を参照してください。

  [#653135]

- Citrix Receiver for Windowsのバージョンを4.2.100から4.5へアップグレード後に追加したアカウントが表示されないことがあります。 同じアカウントを追加しようとすると、そのアカウントは既に存在することを示すメッセージが表示されます。 この問題は管理者以外のユーザーで発生します。

  [#654017]

サードパーティ製品についての通知

Dec 08, 2016

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

Dec 08, 2016

オペレーティングシステム

Citrix Receiver for Windows	サポートされるオペレーティングシステム
4.6	Windows 10 [1]
	Windows Server 2016
	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 Vista 32ビット版および64ビット版
	Windows Thin PC
	Windows Server 2012 R2、Standard、およびDatacenterエディション。
	Windows Server 2012、Standard、およびDatacenterエディション。
	Windows Server 2008 R2 64ビット版
	Windows Server 2008 32ビット版および64ビット版

[1] Windows 10 Anniversary Updateもサポートされます。

ハードウェア

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。

Citrix Receiver for Windows 4.6は、XenAppおよびXenDesktop 7以降がインストールされたWindows 7および8.1が動作するタッチ操作可能なラップトップ、タブレット、およびモニター、ならびにVirtual Desktop Agentがインストールされた Windows 7、8、および2012が動作するコンピューターで使用できます。

Citrix Receiver for Windows Version 4.6には、次のCitrix製品の現在サポートされているバージョンすべてと互換性があります。 Citrix製品のライフサイクル、および製品のバージョンごとのサポートが停止される時期について詳しくは、Citrix製品マトリクスを参照してください。

互換性のあるCitrix製品：

- StoreFront
- XenApp
- XenDesktop
- Web Interface

- Internet Explorer
  Citrix Receiver for WebまたはWeb Interfaceへの接続は、32ビットモードのInternet Explorerをサポートします。 サポートされるInternet Explorerのバージョンについては、「StoreFrontのシステム要件」および「Web Interfaceのシステム要件」を参照してください。
- 最新版のGoogle Chrome（StoreFront必須）
- 最新版のMozilla Firefox

Citrix Receiver for Windowsでは、以下の構成のいずれかを介して、HTTP、HTTPS、およびICA-over-TLS接続を確立できます。

- LAN接続の場合：
  - StoreFront ServicesサイトまたはCitrix Receiver for Webサイトを使用するStoreFront。
  - Web InterfaceサイトまたはXenApp Serviceサイトを使用するWeb Interface 5.4 for Windows。

  デバイスがドメインに属している場合と属していない場合について詳しくは、XenDesktop 7のドキュメントを参照してください。
- セキュリティ保護されたリモートまたはローカルの接続の場合：
  - Citrix NetScaler Gateway 11.x
  - Citrix NetScaler Gateway 10.5

  Windowsドメイン参加、管理されたデバイス（ローカルおよびリモート、VPNありまたはなし）およびドメイン非参加デバイス（VPNありまたはなし）がサポートされます。

  StoreFrontでサポートされるNetScaler GatewayおよびAccess Gatewayのバージョンについては、「StoreFrontのシステム要件」を参照してください。

セキュリティが保護された接続と証明書について

> ### 注意
>
> セキュリティ証明書については、「セキュリティで保護された接続」および「セキュリティで保護された通信」を参照してください。

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は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、Citrix Receiver for Windowsを使用してCitrixリソースにアクセスできません。

> **注意**
>
> 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します。

ユーザーデバイスへのルート証明書のインストール、およびWeb Interfaceでの証明書設定については、 「Receiver通信のセキュリティ保護」を参照してください。

ワイルドカード証明書は、同一ドメイン内の任意のサーバーで個別のサーバー証明書の代わりに使用します。 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）拡張内のサーバー名の一覧に含まれている証明書などのワイルドカード証明書に代わるものを考慮が必要なことがあります。 こういった証明書は、私的証明機関および公的証明機関の両方が発行できます。

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、「中間証明書の構成」を参照してください。

StoreFrontへの接続については、Citrix Receiver for Windowsでは以下の認証方法がサポートされます。

	ブラウザーを使ったReceiver for Web	StoreFront Servicesサイト（ネイティブ）	StoreFront XenApp Services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（セキュリティトークンがあるドメイン）*				はい *	はい *

SMS スマートカード	ブラウザーを使ったReceiver for Web はい	StoreFront Servicesサイト（ネイティブ） はい	StoreFront XenApp Servicesサイト（ネイティブ） いいえ	はい* NetScalerからReceiver for Web（ブラウザー） はい	はい* NetScalerからStoreFront Servicesサイト（ネイティブ） 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。

> ### 注意
> Citrix Receiver for Windows 4.6は、NetScaler GatewayからStoreFrontネイティブサービスを通じて2FA（ドメイン+セキュリティトークン）をサポートします。

Web Interface 5.4に接続するため、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のため「指定ユーザー」という用語を使用します）：

	Web Interface（ブラウザー）	Web Interface XenApp Servicesサイト	NetScalerからWeb Interface（ブラウザー）	NetScalerからWeb Interface XenApp Services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（セキュリティトークンがあるドメイン）*			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、eDocsのNetScaler Gatewayのドキュメントの「Configuring Authentication and Authorization」と、StoreFrontのドキュメントで管理に関する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の認証方法の構成」を参照してください。

Citrix Receiver for Windowsのアップグレード方法について詳しくは、Knowledge CenterのCTX135933を参照してください。

- **.NET Frameworkの最小要件**
  - Self-Service Plug-inでは.NET 3.5 Service Pack 1が必要となります。ユーザーはこのプラグインを使って、Receiver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へのサブスクライブを実行して起動できます。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。
  - Receiverアイコンを問題なく表示するには、.NET 2.0 Service Pack 1およびMicrosoft Visual C++ 2005 Service Pack 1再頒布可能パッケージが必要です。 Microsoft Visual C++ 2005 Service Pack 1パッケージは、.NET 2.0 Service Pack 1、.NET 3.5、および.NET 3.5 Service Pack 1に含まれており、単独で入手することもできます。
  - XenDesktop接続の場合：Desktop Viewerを使用するには.NET Framework 2.0 Service Pack 1以降が必要です。 インターネットにアクセスできない場合は証明書失効チェックにより接続の起動時間が長くなるため、このバージョンが必要です。 このバージョンのFrameworkではチェックを無効にして起動時間を短縮できますが、.NET 2.0ではできません。
- Microsoft Lync Server 2013およびMicrosoft Lync 2013 VDI Plug-in for Windowsとの併用については、「XenDesktop、XenApp、およびCitrix ReceiverでのMicrosoft Lync 2013 VDI Plug-inのサポート」を参照してください。
- **サポートされる接続方法とネットワークトランスポート：**
  - TCP/IP+HTTP
    必要となることがある追加の値については、CTX 134341を参照してください。
  - TLS+HTTPS

インストール

Jan 27, 2017

CitrixReceiver.exeのインストールパッケージは、以下の方法で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
  - Receiverを初めて使用するユーザーがReceiver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（またはAccess 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ます。ユーザーは、ログオンしてインストールを完了します。 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Receiverをインストールしていないユーザーを指します。
  - Citrix.com以外の場所（Receiver for Webサイトなど）からReceiver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。
  - Receiver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のログオン画面からの自動インストール
  - Receiverを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
  - Receiverを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、Receiverのインストールに管理者権限は不要です。

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。 このバージョンのCitrix Receiverをインストールすると、HDX RTMEが実行可能ファイル（.exe）に含まれます。

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 RealTime Media Engine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。

> **注意**
>
> 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Receiver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Receiver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 4.6からRTMEがバンドルされたReceiver 4.6)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Receiver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。

> **Important**
>
> XenApp/XenDesktopサーバー上のHDX RealTime Connectorを最新バージョンの2.0.0.417（GAリリース）にして新しいRTMEパッケージと互換性を持たせる必要があります。RTME 2.0は1.8 RTME Connectorとは使用できません。

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 4.xでは、Citrix Receiver for Windows 3.xと、Citrix Online Plug-in 12.xをアップグレードできます。

Citrix Receiver for Windows 3.xまたはOnline Plug-inがマシン単位でインストールされている場合、管理権限のないユーザーによるユーザー単位のアップグレードはサポートされません。

Citrix Receiver for Windows 3.xまたはOnline Plug-inがユーザー単位でインストールされている場合、マシン単位でのアップグレードはサポートされません。

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

Dec 08, 2016

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。

> **Important**
>
> Citrix Receiver for Windows 4.xでは、パススルー認証（Single Sign-On）の構成プロセスが変わりました。 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/includeSSONの説明を参照してください。

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。

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Citrix Receiver for Windowsがアンインストールされても、receiver.adm/receiver.admlまたはreceiver.admxにより作成されたCitrix Receiver for Windowsのカスタム設定レジストリキーは、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せぬ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。

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

Jan 20, 2017

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。 セットアッププログラムが起動する前にインストーラーパッケージはユーザーの一時フォルダーに自己展開されるため、**%temp%**フォルダーにはおおよそ57.8 MBの空き領域が必要です。 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。

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>]

Option	FORCE_LAA=1
Description	By default, Citrix Receiver for Windows does not install the client side Local App Access components if the components are already installed on the server. To force the client side Local App Access components on the Citrix Receiver, use FORCE_LAA command line switch. Requires administrator rights. For more information on Local App Access, see Local App Access in XenApp and XenDesktop documentation.
Sample usage	CitrixReceiver.exe FORCE_LAA =1

オプション	/? または/help
説明	この切り替えにより使用方法情報が表示されます。
使用サンプル	CitrixReceiver.exe /? CitrixReceiver.exe /help

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

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

オプション	/includeSSON
説明	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。 スマートカードでシングルサインオンする場合は、このオプションを指定する必要があります。 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。 またユーザーデバイスで、［管理者テンプレート］、［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］の順に選択して、これらのポリシーを有効にする必要もあります。 ● ローカルユーザー名とパスワード ● パススルー認証の有効化 ● すべてのICAに対してパススルー認証を有効にします（Web Interface構成およびセキュリティ設定により必要／不必要が異なる）。 変更が完了したら、ユーザーデバイスを再起動します。 詳しくは、『How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication」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

Option	ENABLE_SSON={Yes | No}
Description	Enable Single Sign-on when /includeSSON is specified. The default value is Yes. Enables Single Sign-on when /includeSSON is also specified. This property is required for smart card Single Sign-on. Note that users must log off and log back on to their devices after an installation with Single Sign-on authentication enabled. Requires administrator rights.
Sample usage	CitrixReceiver.exe /ENABLE_SSON=Yes

オプション	/EnableTracing={true | false}
説明	この機能はデフォルトで有効になっています。 このプロパティを使用して、常時トレース機能を明示的に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

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、Citrix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

オプション	INSTALLDIR=<Installation Directory>
	インストールパスを指定します。ここでInstallation Directoryは、ほとんどのCitrix Receiverソフトウェアがインストールされる場所です。 デフォルト値は、C:\Program Files\Citrix\Receiverです。 ただし、Citrix Receiverの一部の

説明	コンポーネント（Authentication Manager、Receiver、およびSelf-Service Plug-in）はC:\Program Files\Citrixにインストールされます。 このオプションで<Installation directory>を指定する場合は、<Installation directory>\Receiverディレクトリに RIInstaller.msiをインストールし、<Installation directory>ディレクトリにほかのMSIファイルをインストールする必要があります。
使用サンプル	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

オプション	CLIENT_NAME=<*ClientName*>
説明	クライアント名を指定します。ここでClientNameは、サーバーファーム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。
使用サンプル	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

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 DYNAMIC_NAME=Yes

オプション	ADDLOCAL=<feature... ,>
	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。

説明	次のコンポーネントがあります。 ● ReceiverInside – Citrix Receiverエクスペリエンスをインストールします（Receiverの操作に必要なコンポーネント）。 ● ICA_Client – 標準のCitrix Receiver（Receiverの操作に必要なコンポーネント）。 ● 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。 AM値はコマンドラインで指定し、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を使ってReceiver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）。
使用サンプル	CitrixReceiver.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,usb,WebHelper

オプション	ALLOWADDSTORE={N | S | A}
説明	Merchandising Serverの配信により構成されなかったストアをユーザーが追加および削除できるかどうかを指定します。ユーザーは、Merchandising Serverの配信により構成されたストアを有効または無効にできますが、そのようなストアを削除したり、名前やURLを変更したりすることはできません。デフォルトはSです。 次のオプションがあります。 ● N – ユーザーによるストアの追加や削除を許可しません。 ● S – ユーザーによるストアの追加や削除を許可します（HTTPSで構成されたセキュアなストアのみ）。 ● A – ユーザーによるストアの追加や削除を許可します（HTTPSまたはHTTPで構成されたストア）。 Citrix Receiverをユーザー単位でインストールする場合には適用されません。 この機能は、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStoreで設定することもできます。

	注：デフォルトでは、HTTPSによるセキュアなストアのみが許可されます。実稼働環境では、このデフォルト設定の使用をお勧めします。 テスト環境でHTTPストア接続を使用するには、以下の構成を行います。 1. HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStoreにAを設定すると、HTTPによる非セキュアなストアをユーザーが追加できるようになります。 2. HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwdにAを設定すると、非セキュアなストアでユーザーがパスワードを保存できるようになります。 3. StoreFrontで構成された［TransportType］が［HTTP］のストアを追加するには、HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManagerに値ConnectionSecurityMode（REG_SZ）を追加して、Anyを設定します。 4. Citrix Receiverの終了と再起動
使用サンプル	CitrixReceiver.exe ALLOWADDSTORE=N

オプション	ALLOWSAVEPWD={N | S | A}
説明	Merchandising Serverの配信により構成されなかったストアをユーザーが追加および削除できるかどうかを指定します。ユーザーは、Merchandising Serverの配信により構成されたストアを有効または無効にできますが、そのようなストアを削除したり、名前やURLを変更したりすることはできません。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で構成されたセキュアなストアのみ）。 ● A – 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）。 この機能は、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd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。 ● 32ビットOSクライアントのキー：HKLM\Software\Citrix\AuthManager ● 64ビットOSクライアントのキー：HKLM\Software\wow6432node\Citrix\AuthManager ● 種類：REG_SZ ● 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 ALLOWSAVEPWD=N

オプション	AM_CERTIFICATESELECTIONMODE={Prompt | SmartCardDefault | LatestExpiry}
説明	このオプションを使っ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のSoftware\[Wow6432Node\]Citrix\AuthManagerのCertificateSelectionMode={ 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

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

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

オプション	LEGACYFTAICONS={False | True}
説明	レガシ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

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

オプション	STARTMENUDIR={Directory Name}
	デフォルトでは、［スタート］>［すべてのプログラム］の下にアプリケーションのショートカットが追加されます。 ユーザーがサブスクライブしたアプリケーションの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。 ユーザーは、必要に応じてこのフォルダー名を変更したりフォルダーを移動したりできます。 以下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 c 」を入力します。 場所： HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\Dazzle 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

説明	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 8/8.1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。 例 ● ［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。 ● また、［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。
使用サンプル	CitrixReceiver.exe STARTMENUDIR=\Office

オプション	STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On | 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。 値のデータ： ● 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"

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「ローカルアプリケーションアクセス」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

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

オプション	DESKTOPDIR=<Directory Name>
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CategoryPath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

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

インストールが完了したら、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]** 画面が開きます。 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。

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、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。

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

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。

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

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。

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Citrix Receiver for Windowsの展開

Dec 08, 2016

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奨めします。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。

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。 例： set DesiredVersion= 3.3.0.<XXXX> に、展開するバージョンの番号を指定します。「3.3.0」などバージョン番号の一部を指定すると、その番号で始まるすべてのバージョン（「3.3.0.1111」や「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。

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. ［スタートアップのプロパティ］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。

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。

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。

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。ただし、Citrix Receiver for Windowsをユーザーごとに構成する必要がある場合は、ユーザー単位のスタートアップスクリプトを使用できます。XenDesktopおよびXenAppのメディアのCitrix Receiver for Windows and Plug-ins\Windows\Receiver\Startup_Logon_Scriptsフォルダーには、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設定するには

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. ［ログオンのプロパティ］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

Dec 08, 2016

ReceiverをReceiver for Webサイトからユーザーに配布すると、Webブラウザーからアプリケーションにアクセスするユーザーに確実にReceiverをインストールさせることができます。 Citrix Receiver for Webサイトを使用すると、ユーザーは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. 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。

Web InterfaceのログオンからのCitrix Receiver for Windowsの配布

Dec 08, 2016

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とき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。

詳しくは、Web Interfaceのドキュメントの「クライアント展開の構成」を参照してください。

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、XenAppまたはXenDesktopのインストールメディアで提供されている名前でCitrix Receiver for Windowsのインストールファイルが検索されます。
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。

Citrix Receiver for Windowsの構成

Dec 08, 2016

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。 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。
- ショートカットのみのモードを構成します。これには以下の方法が含まれます。
  - グループポリシーオブジェクトテンプレートを使ったショートカットの構成
  - ショートカットカスタマイズ用のレジストリキー。
  - StoreFrontアカウント設定をベースにしたショートカットの構成
- ユーザーにアカウント情報を提供します。 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。

- 外部から接続するユーザー（遠隔地からまたはインターネット経由で接続するユーザーなど）にアクセスを提供するには、NetScaler Gatewayを使用した認証を構成します。 詳しくは、Netscaler Gatewayのドキュメントを参照してください。

アプリケーション配信の構成

Dec 08, 2016

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、ストアのアプリケーションにアクセスするユーザーの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 4.4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するだけです。 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。 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、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。

- 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、ユーザーは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ム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アプリケーションの作成」を参照してください。

注：デリバリーグループのアプリケーションにわかりやすい説明を入力します。 Webアクセスまたはセルフサービスモードを使う場合、Citrix Receiver for Windowsのユーザーにはこの説明が表示されます。
［スタート］メニュー内またはデスクトップ上でショートカットを構成する方法について詳しくは、「ショートカットのみのモードの構成」を参照してください。

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の構成では、グループポリシーオブジェクトを使う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。

GPOを介してNetScaler Gatewayを追加または指定するには

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。
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］の順に開き、［NetScaler Gateway URL\StoreFront アカウント一覧］を選択します。

3. 設定を編集します。

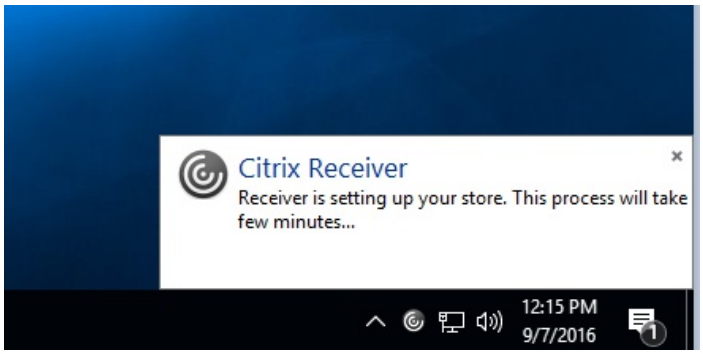
- ［ストア名］ – ストアの表示名を指定します。
- ［ストア URL］ – ストアのURLを指定します。
- ［#Store name］ – NetScaler Gatewayの後ろにあるストアの名前を指定します。
- ［ストアの有効/無効］ – ストアの状態をOnまたはOffで指定します。
- ［ストアの説明］ - ストアの説明を入力します。

4. 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;https://dtls.blrwinrx.com#Store name;On;人事部用ストア*

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を経由してNetScaler Gatwayを追加してからCitrix Receiver for Windowsを起動すると、通知領域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。

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。

> ## 注意
>
> 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。

管理者として、グループポリシーを使ってショートカットを構成できます。

1. 単一のコンピューターにポリシーを適用する場合に［スタート］メニューからgpedit.mscを実行して、またはドメインポリシーを適用する場合にグループポリシー管理コンソールを使用して、グループポリシーエディターを開きます。
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］を選択し、ReceiverのConfigurationフォルダーを参照してからreceiver.admx（またはreceiver.adml）を選択します。
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 Components］、［Citrix Receiver］、［Self Service］の順に開きます。
7. ［SelfServiceModeを管理します］を選択し、セルフサービスモードのReceiverユーザーインターフェイスを有効または無効にします。
8. ［Manage App Shortcut］を選択して、次のことを有効または無効にします。

- Shortcuts on Desktop
- Shortcuts in Start menu
- Desktop Directory
- Start menu Directory
- Category path for Shortcuts
- Remove apps on logoff
- Remove apps on exit

9. ［ユーザーにアカウントの追加/削除を許可します］を選択して、アカウントを追加または削除する権限をユーザーに付与します。

［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）。
- 以前にはストアー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は、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" />

Important

複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。 展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。 変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

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。

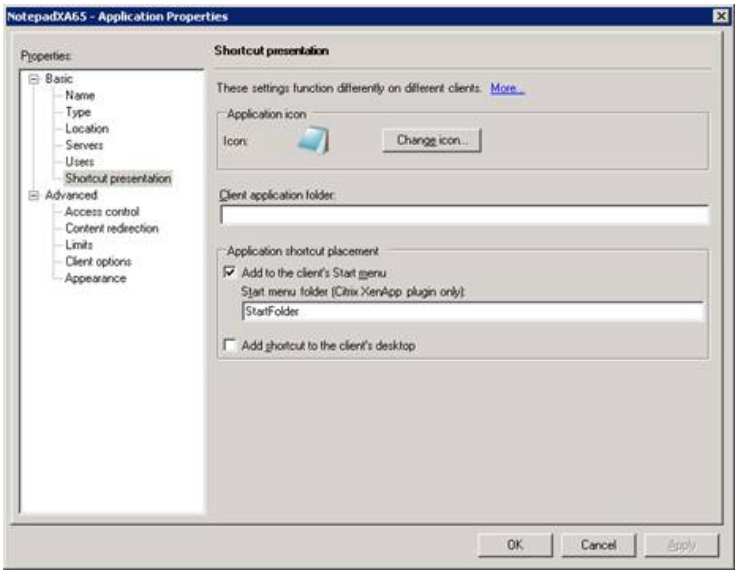
セルフサービスモードか、または［スタート］メニューモードかには関係なく、アプリケーションごとの設定によりアプリケーションを配置する場所を決定する場合は、	Receiverで**PutShortcutsInStartMenu=false**と構成して、アプリケーションごとの設定を有効にします。 注：この設定は、Web Interfaceサイトにのみ適用されます。

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

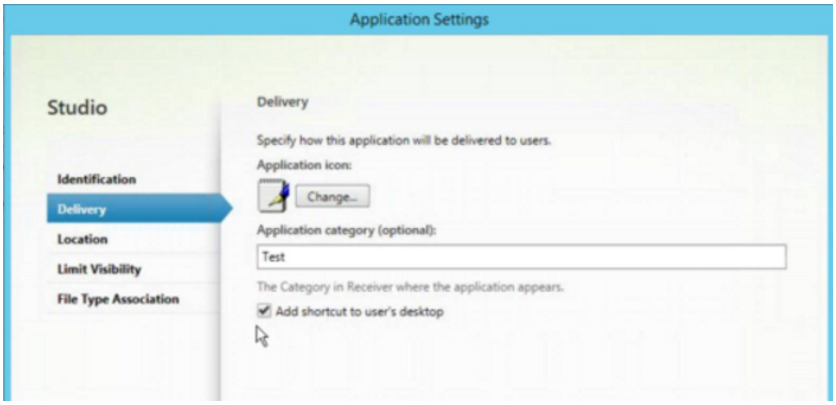
XenApp 6.5でアプリケーションごとの公開ショートカットを構成するには

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。



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copy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、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。
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。
    1. Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"
    2. Reg add HKLM\Software\Citrix\Dazzle /v
    3. 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。
    4. 設定をテストするため、Receiverを終了して再起動します。

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

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。 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。
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。

ローカルアプリケーション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、「ローカルアプリケーションアクセ

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、「ローカルアプリケーションアクセス」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	マッチするかどうか
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

KEYWORDS:prefer=	Programs配下のショートカット	マッチするかどうか
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	マッチするかどうか
"\\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	マッチするかどうか
"\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」を参照してください。

XenDesktop環境の構成

Dec 08, 2016

この記事の各トピックでは、USBサポートの構成方法、Desktop Viewerウィンドウが暗くなる機能の無効化、および複数のユーザーやデバイスのための設定について説明します。

EDTの要件

- XenAppおよびXenDesktop 7.12以降（Studioを使用して機能を有効にする必要があります）。
- StoreFront 3.8。
- IPv4 VDAのみ。 IPv6およびIPv6とIPv4混在の構成はサポートされていません。

> **注意**
>
> Enlightened Data Transportは、評価目的のみです。本番環境ではご使用にならないでください。 契約条件について詳しくは、License Agreements（EULAs）and Service Agreements（EUSAs）を参照してください。

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EDTを構成する必要があります。

新しいデータ転送レイヤー（EDT）は、デフォルトでCitrix Receiver for Windowsで許可されています。VDAのCitrixポリシーが［**優先**］に構成され、設定がVDAに適用されている場合、クライアントはデフォルトでEDTのみを使用しようとします。

特定のクライアントでEDTを無効にする場合、グループポリシーオブジェクトを使用して、EDTオプションを適切に設定します。

グループポリシーオブジェクト（GPO）でEDTを構成するには（オプション）

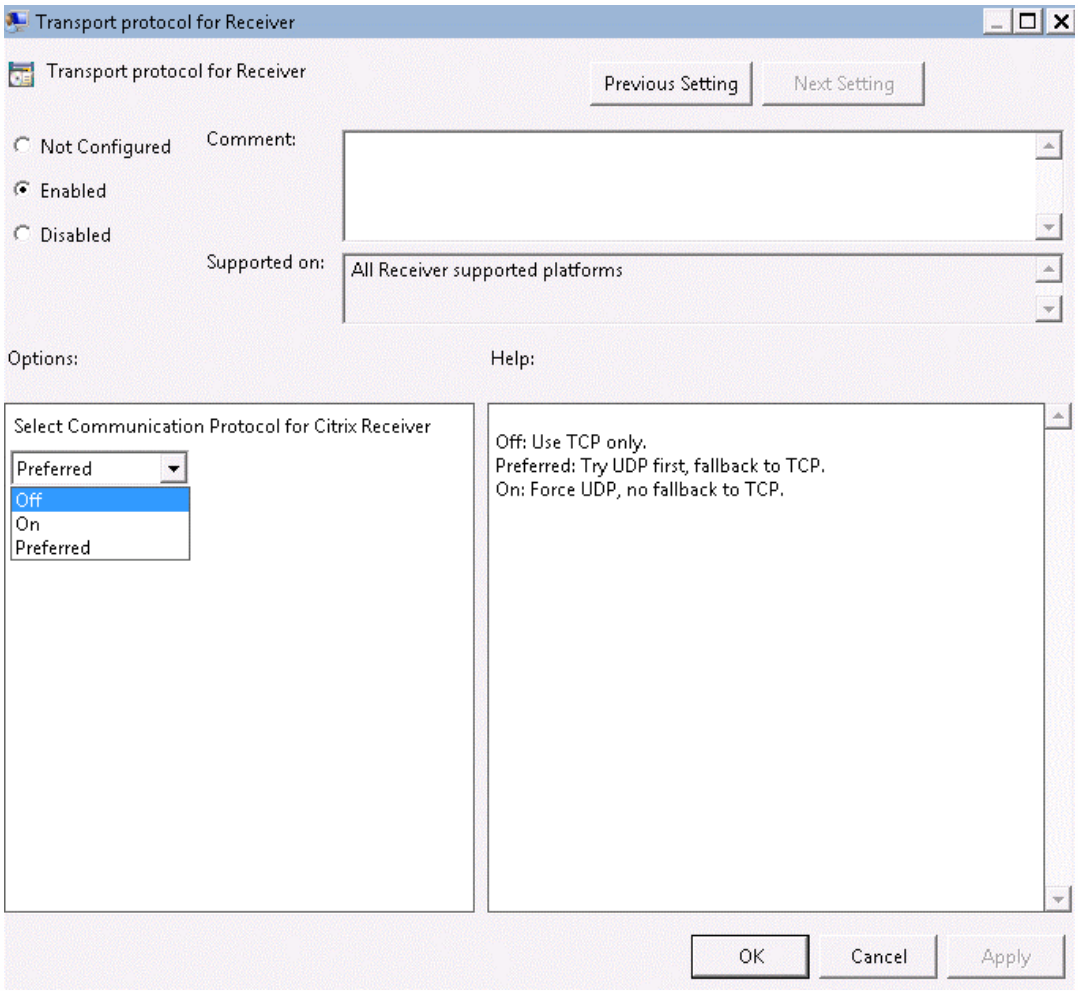
以下は、この機能を評価するために環境をカスタマイズするオプションの構成手順です。 たとえば、セキュリティ上の理由で特定のクライアントの機能を無効にできます。

> **注意**
>
> デフォルトでは、Enlightened Data Transportは無効（オフ）になっており、常にTCPが使用されます。

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。

   Citrix Receiver for Windowsの管理用テンプレートファイルをグループポリシーエディターにインポートする手順について詳しくは、「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 for Windowsの構成」を参照してください。

2. ［コンピューターの構成］ノードで、［**管理用テンプレート**］>［**Citrix 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. コマンドプロンプトを開きます。
7. gpupdate /forceコマンドを実行します。

また、EDT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。

ポリシー設定が有効になっていることを確認するには

- レジストリが更新され、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDTにHDXOverUDPキーが含まれているかを確認します。

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。 ユーザーがコンピューターに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、および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、XenDesktopおよびXenApp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3-D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CTX120292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は、 このデバイスのリモート操作はしません。 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
- マスストレージデバイス

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。

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］>［Remoting client devices］>［Client drive mapping］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（ユーザーが通知領域の［ハードウェアの安全な取り外し］をクリックする場合）

［Generic USB］と［Client drive mapping］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。

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 ほとんどのマスストレージデバイスはこのSCSIのバリエーションを使用します

  マスストレージデバイスには、クライアントドライブマッピングを介して頻繁にアクセスすることができ、USBサポートは必要ありません。

  重要：ウィルスプログラムの中には、あらゆる種類のマスストレージ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。
  注：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。

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。

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。

<ルートドライブ>:\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、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。
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、Citrix Knowledge CenterのCTX119722を参照してください。

ユーザーごとにUSBオーディオを構成する

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の構成では、グループポリシーオブジェクトのreceiver.admx/receiver.admlテンプレートファイルを使用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。

注：この機能は、XenAppサーバーでのみ使用できます。

ユーザーごとにUSBオーディオを構成するには

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Receiver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］**を選択し、ReceiverのConfigurationフォルダー（一般的に、32ビットマシンの場合はC:\Program Files\Citrix\ICA Client\Configuration、64ビットマシンの場合はC:\Program Files (x86)\Citrix\ICA Client\Configuration）を参照してreceiver.admxを選択します。
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. ［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。
7. 設定を編集します。
8. [適用]、[OK]の順にクリックします。
9. コマンドプロンプトを管理者モードで開きます。
10. 次のコマンドを実行します。
    gpupdate /force

注：ポリシーを変更した場合、変更を有効にするにはXenAppサーバーを再起動する必要があります。

Bloombergキーボードは、XenDesktopおよびXenAppセッションでサポートされます（ただしほかのUSBキーボードはサポートされません）。 プラグインをインストールすると必要なコンポーネントが自動的にインストールされますが、インストール時または後でレジストリキーを変更しなければ、この機能は有効になりません。

単一のユーザーデバイス上の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。

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、DisableDimmingという名前のREG_DWORDエントリを次のキーのどちらかに作成します。作成場所は減光を無効にする対象が現在のデバイスユーザーかデバイス自体かによって異なります。 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。

   1. HKEY_CURRENT_USER\Software\Policies\Citrix\...
   2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\...
   3. HKEY_CURRENT_USER\Software\Citrix\...
   4. HKEY_LOCAL_MACHINE\Software\Citrix\...

StoreFrontの構成

Dec 08, 2016

Citrix StoreFrontは、XenDesktop、XenApp、およびVDI-in-a-Boxのユーザーを認証し、使用可能なデスクトップおよびアプリケーションをストアに集約して、Citrix Receiver for Windowsユーザーに提供します。

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
>
> Citrix Receiver for Windowsで、すべてのストアを表示するオプションを選択すると、更新されたStoreFront UIではなく、以前のStoreFront UIが表示されることがあります。

1. 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、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。

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に対する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）

値の名前：**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）

値の名前：**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、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。 「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。

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。

> **注意**
>
> 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。

レジストリキー設定を使ってショートカットをカスタマイズできます。 レジストリキーは次の場所で設定できます。 レジストリキーを適用すると、一覧の優先順でそれが反映されます。

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、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。

注：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

レジストリ名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle

		HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle

		HKLM \SOFTWARE\Citrix\Dazzle
StartMenuDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	SelfServiceModeではTrue、NonSelfServiceModeではFalse	HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	True	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID

		+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	インストール中はレジストリが作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Policies\Citrix\Dazzle HKLM\SOFTWARE \Citrix\Dazzle

64ビットマシンのレジストリキー

レジストリ名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle

		HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle

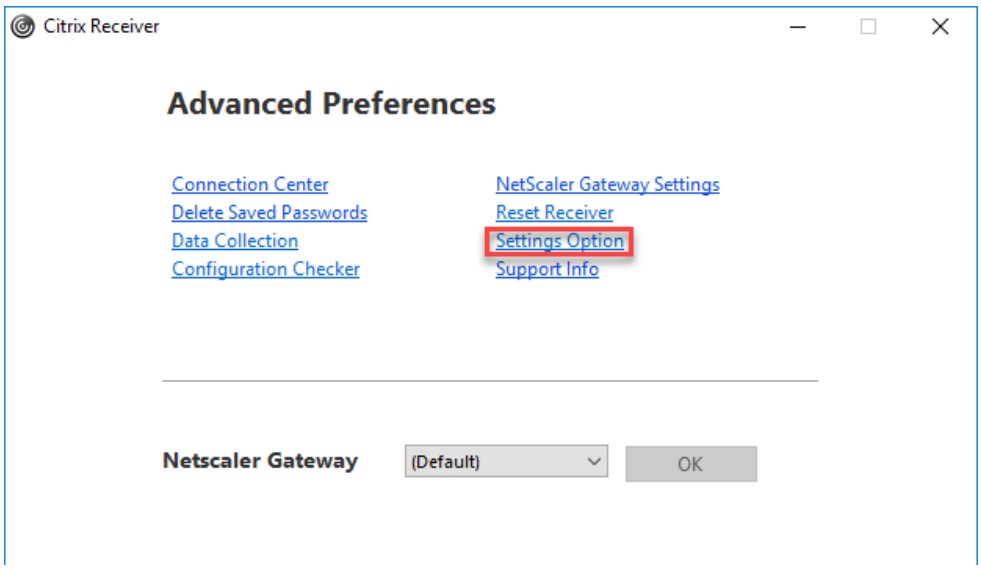
		HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	""（空）	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKEY_CURRENT_USER\Software\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
HideEditStoresDialog	SelfServiceModeではTrue、NonSelfServiceModeではFalse	HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties
WSCSupported	True	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectAll	True	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle
WSCReconnectModeUser	インストール中はレジストリが作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzle HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle

注意

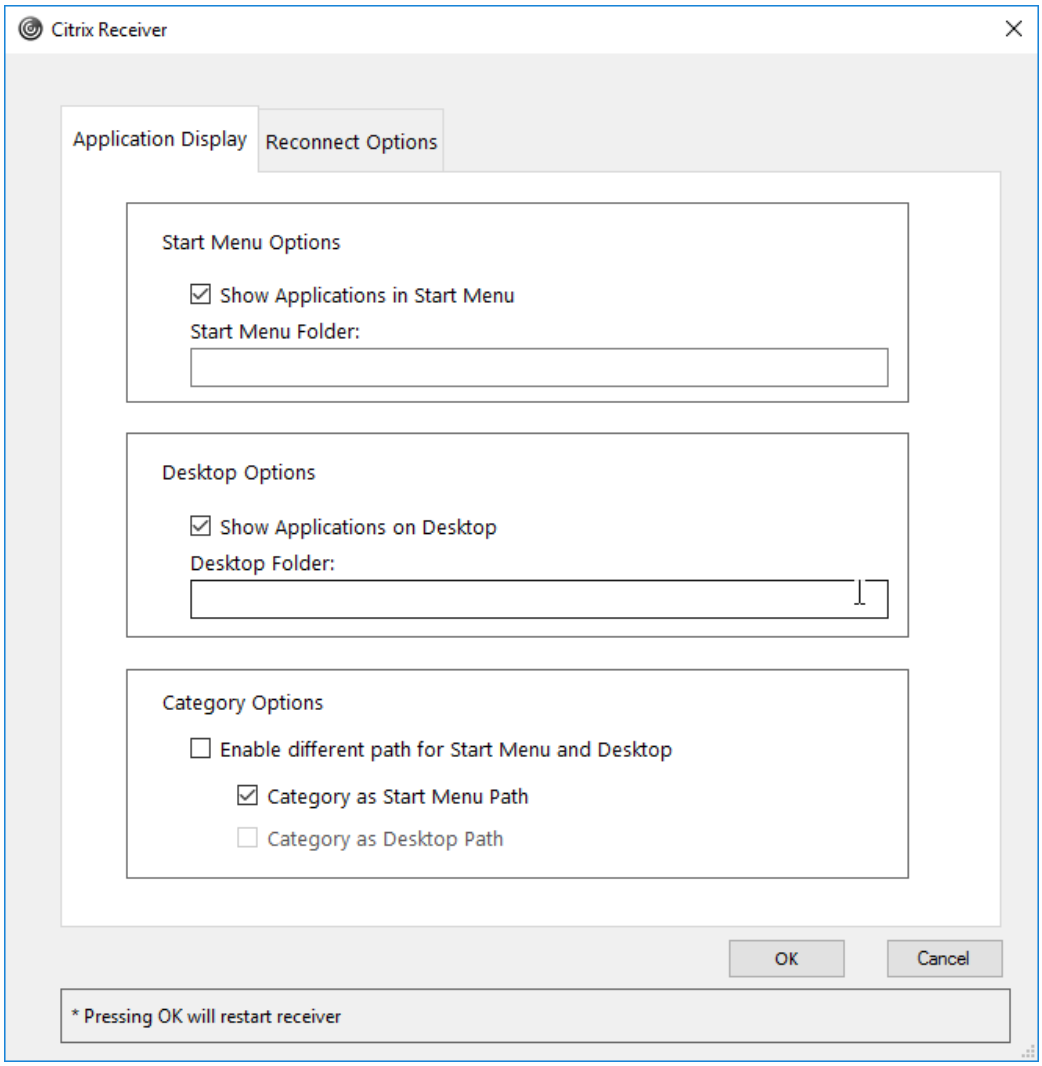
ショートカットを設定できるのは、サブスクライブ済みのアプリケーションとデスクトップに対してのみです。

1. Citrix Receiver for Windowsへのログオン
2. 通知領域のCitrix Receiver for Windowsアイコンを右クリックし、**[詳細な設定]**を選択します。
   [詳細な設定]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、アプリケーションサーバーのプロパティで定義されたとおりにアプリケーションのショートカットと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。
a. 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。
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。

5. ［OK］をクリックします。

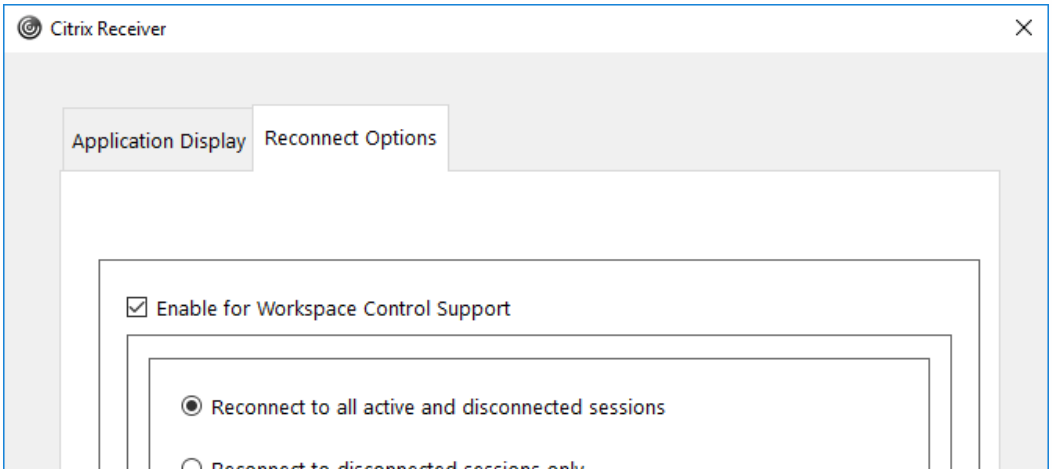
サーバーにログオンしたユーザーは、すべての自分のデスクトップやアプリケーションに一度に再接続できます。 デフォルトの再接続オプションでは、切断されているデスクトップやアプリケーションに加えて、ほかのクライアントデバイスで現在アクティブなデスクトップやアプリケーションが開かれます。 管理者は、切断されているデスクトップやアプリケーションだけが再接続されるように再接続オプションを構成することもできます。

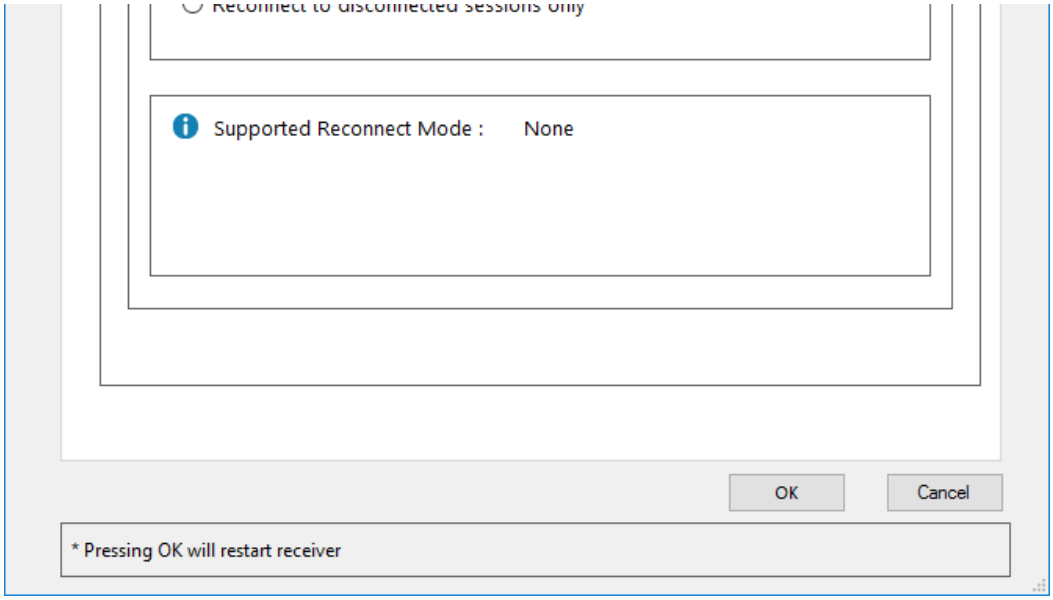
1. Citrix Receiver for Windowsにログオンします。

2. システムトレイのCitrix Receiver for Windowsアイコンを右クリックし、**[詳細な設定]** をクリックします。
［詳細な設定］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。

レジストリから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。

オプション	/DisableSetting
説明	［詳細な設定］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
［詳細な設定］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

グループポリシーオブジェクトの管理用テンプレートによるCitrix Receiver for Windowsの構成

Dec 08, 2016

Windowsグループポリシーオブジェクト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）。

> ## 注意
>
> 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。

> ## 注意
>
> .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。

> ## 注意
>
> 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、<インストールディレクトリ>\Online Plugin\Configurationです。

> ## 注意
>
> 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。

ファイルの種類	ファイルの場所
receiver.adm	<インストールディレクトリ>\ICA Client\Configuration
receiver.admx	<インストールディレクトリ>\ICA Client\Configuration

receiver.adml	<インストールディレクトリ>\ICA Client\Configuration\[MUIカルチャ]
CitrixBase.admx	<インストールディレクトリ>\ICA Client\Configuration
CitrixBase.adml	<インストールディレクトリ>\ICA Client\Configuration\[MUIカルチャ]

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. 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、テンプレートファイルの場所（<インストールディレクトリ>\ICA Client\Configuration\receiver.adm）を参照します。
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、こちらのMicrosoft MSDNの記事を参照してください。
1. Citrix Receiver for Windowsをインストールしてから、テンプレートファイルをコピーします。

admx：
コピー元：<インストールディレクトリ>\ICA Client\Configuration\receiver.admx
コピー先：%systemroot%\policyDefinitions

コピー元：<インストールディレクトリ>\ICA Client\Configuration\CitrixBase.admx
コピー先：%systemroot%\policyDefinitions

adml：
コピー元：<インストールディレクトリ>\ICA Client\Configuration\[MUIculture]receiver.adml
コピー先：%systemroot%\policyDefinitions\[MUIculture]

コピー元：<インストールディレクトリ>\ICA Client\Configuration\[MUIculture]\CitrixBase.adml
コピー先：%systemroot%\policyDefinitions\[MUIculture]

> **注意**
>
> 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）。

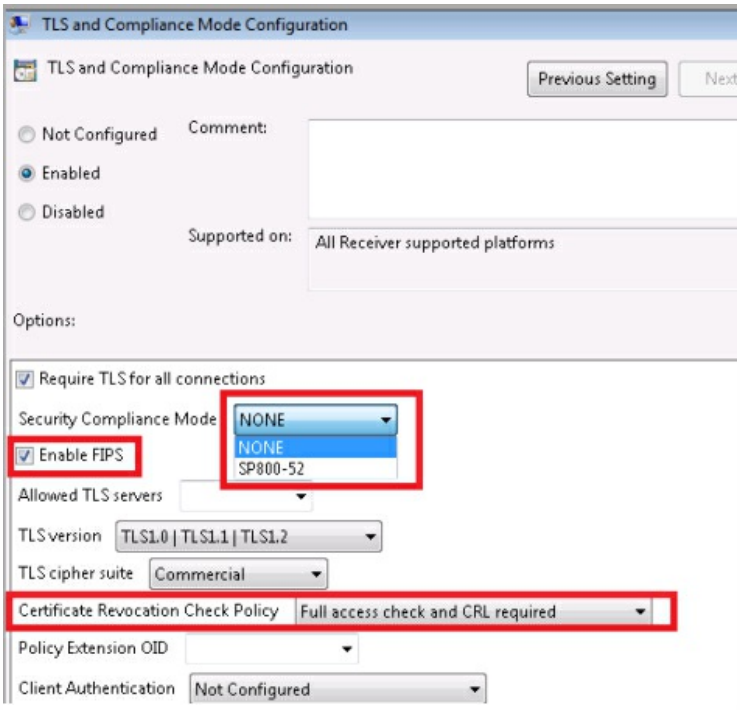
このポリシーを使用してTLSオプションを構成します。このオプションにより、Citrix Receiver for Windowsで接続先のサーバーを安全に識別して、サーバーとのすべての通信を暗号化できます。

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。
- TLSの特定の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）。

このポリシーが有効な場合、**［すべての接続でTLSが必要］**チェックボックスをオンにすることによって、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。

FIPS準拠の暗号化の使用を適用するには、**［FIPSを有効にします］**を選択します。



Important

［FIPSを有効にします］を選択する場合、Windowsセキュリティ設定 **[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。有効にしなかった場合、Citrix Receiver for Windowsは公開アプリケーションやデスクトップへの接続に失敗することがあります。

NIST SP 800-52推奨セキュリティに準拠するには、［セキュリティコンプライアンスモード］で［SP800-52］を選択します。この設定は、すべてのサーバーまたはゲートウェイがNIST SP 800-52推奨セキュリティに準拠する場合に選択してください。

Important

［セキュリティコンプライアンスモード］で［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。 また、Windowsセキュリティ設定 **[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。有効にしなかった場合、Citrix Receiver for Windowsは公開アプリケーションやデスクトップへの接続に失敗することがあります。

［セキュリティコンプライアンスモード］で［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。

［セキュリティコンプライアンスモード］で［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は、Citrix Receiver for Windowsは接続に失敗します。

特定バージョンのTLSの使用を適用するには、TLSバージョン設定を選択します。

法規制によっては、TLS 1.0の使用が禁止され、TLS 1.2の使用が優先されることがあります。 Citrix Receiverは、サーバーまたはゲートウェイでも使用できるTLSの最新バージョンを使用します。

以下から選択できます。

- TLS 1.0または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。
- TLS 1.2のみ- 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。

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。

利用可能な暗号の組み合わせは、［FIPSを有効にします］設定および［セキュリティコンプライアンスモード］設定によっても異なります。

次の表は、各セットに含まれる暗号の組み合わせの一覧です。

TLS暗号スイート		GOV	COM	すべて	GOV	COM	すべて	GOV	COM	すべて
Enable FIPS		Off	Off	Off	On	On	On	On	On	On
セキュリティコンプライアンスモードSP800-52	Off	Off	Off	Off	Off	Off	On	On	On	On
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		○		○	○		○			
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	○		○	○		○				
TLS_RSA_WITH_AES_256_GCM_SHA384		○		○	○		○	○		○
TLS_RSA_WITH_AES_128_GCM_SHA256		○	○	○	○	○	○	○	○	○
TLS_RSA_WITH_AES_256_CBC_SHA256	○		○	○		○				
TLS_RSA_WITH_AES_256_CBC_SHA		○		○	○		○	○		○
TLS_RSA_WITH_AES_128_CBC_SHA		○	○		○	○			○	○
TLS_RSA_WITH_RC4_128_SHA	○	○								
TLS_RSA_WITH_RC4_128_MD5	○	○								
TLS_RSA_WITH_3DES_EDE_CBC_SHA		○		○	○		○	○		○

Citrix Receiver for Windowsが特定のサーバーにのみ接続するように制限できます。 Citrix Receiver for Windowsでは、サーバーにより提示されるセキュリティ証明書上の名前でサーバーを識別します。 これはDNS名の形式です（例：www.citrix.com）。 **[Allowed SSL servers]** 設定でコンマ区切りの名前の一覧を指定します。 ここでワイルドカードと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元により言明されます。 Citrix Receiver for Windowsで証明書の発

行元が認識されず信頼されない場合は、接続が拒否されます。

Citrix Receiver for Windowsは、証明書失効リスト（CRL：Certificate Revocation List）を使用して、サーバー証明書が失効しているかを確認します。 証明書が失効していると、接続は拒否されます。 証明書の発行元は、サーバーが侵害されると、証明書を失効できます。

以下のように、Certificate Revocation Checkポリシー設定を選択します。

- **チェックしない**- CRLチェックなしで接続を続行する場合、このオプションを選択します。
- **ネットワークにアクセスせずにチェックします**- 最新のCRLを取得せずにCRLをチェックする場合、このオプションを選択します。
- **完全なアクセス権のチェック**- 最新のCRL（利用可能であれば）を取得してからCRLをチェックする場合、このオプションを選択します。
- **完全なアクセス権のチェックとCRLが必要です**- CRLをチェックする場合、このオプションを選択します。 最新のCRLが利用できない場合、接続は拒否されます。

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。 これは、ポリシーの拡張OIDで識別されます。 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。

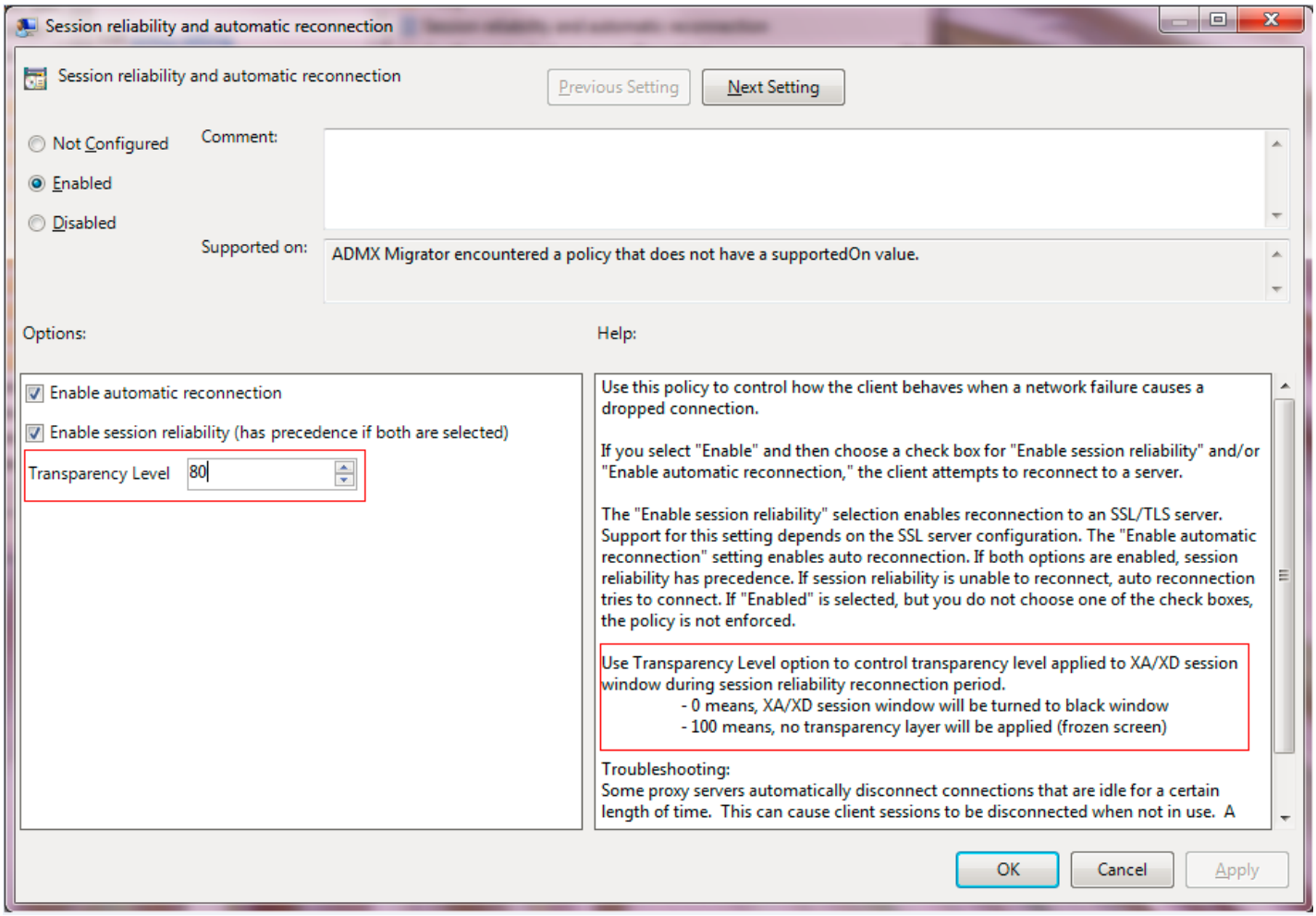
TLSで接続する場合、Citrix Receiver for Windowsにクライアント証明書の提供を要求するようにサーバーを構成できます。
以下のように **[クライアント認証]** 設定を選択します。

- **無効**- サーバーがクライアント証明書を要求するよう構成されていない場合、このオプションを選択します。 これによって、クライアント証明書の情報が誤って開示されるのを防ぎます。
- **可能な場合、自動的に選択します**- クライアント証明書を要求するようサーバーが構成されている場合、通常これが最適なオプションです。
- **証明書セレクタを表示します**- **[可能な場合、自動的に選択します]** が正しい証明書を選択しない場合、このオプションを選択します。 ユーザーにメッセージが表示されます。
- **指定された証明書を使用します**- **[可能な場合、自動的に選択します]** が正しい証明書を選択しない場合で、ユーザーにメッセージが表示されないようにするには、このオプションを選択します。 この場合、証明書の拇印を指定する必要があります。

セッション画面の保持グループポリシーを構成する場合、透過性レベルを設定します。 このオプションを使用すると、セッション画面の保持再接続期間の間に公開アプリケーション（またはデスクトップ）に適用される透過性レベルを制御できます。

透過性レベルを構成するには、**[コンピューターの構成]** > **[管理者テンプレート]** > **[Citrix Components]** > **[Network Routing]** > **[Session reliability and automatic reconnection]** > **[Transparency Level]** の順に選択します。

> ### 注意
>
> デフォルトでは、［Transparency Level］が［80］と設定されています。



ユーザーへのアカウント情報の提供

Dec 08, 2016

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

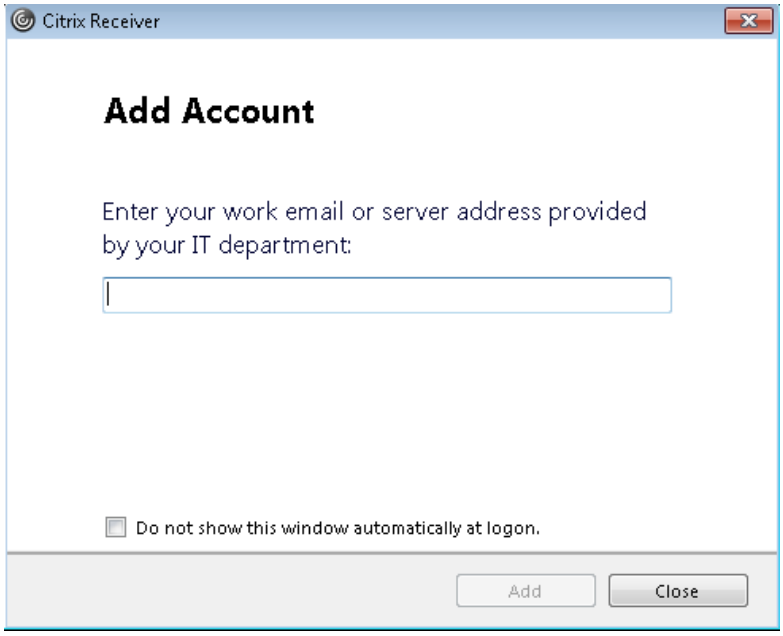
> **Important**
>
> Citrix Receiver for Windowsを初めて使用するユーザーには、Citrix Receiver for Windowsをインストール後に再起動するよう指示してください。 再起動により、ユーザーがアカウントを追加できるようになり、またCitrix Receiver for Windowsのインストール時に一時停止状態だったUSBデバイスが認識されます。

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**



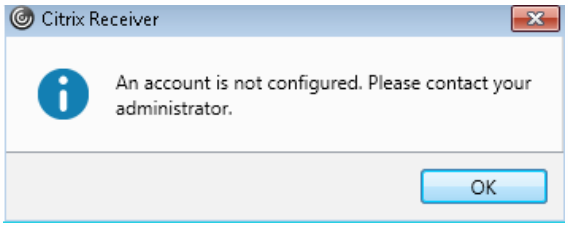
次回以降のログオン時に［アカウントの追加］ダイアログボックスがポップアップ表示されないようにするには、**[ログオン時に自動的にこのウィンドウを表示しない]**チェックボックスをオンにします。

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。

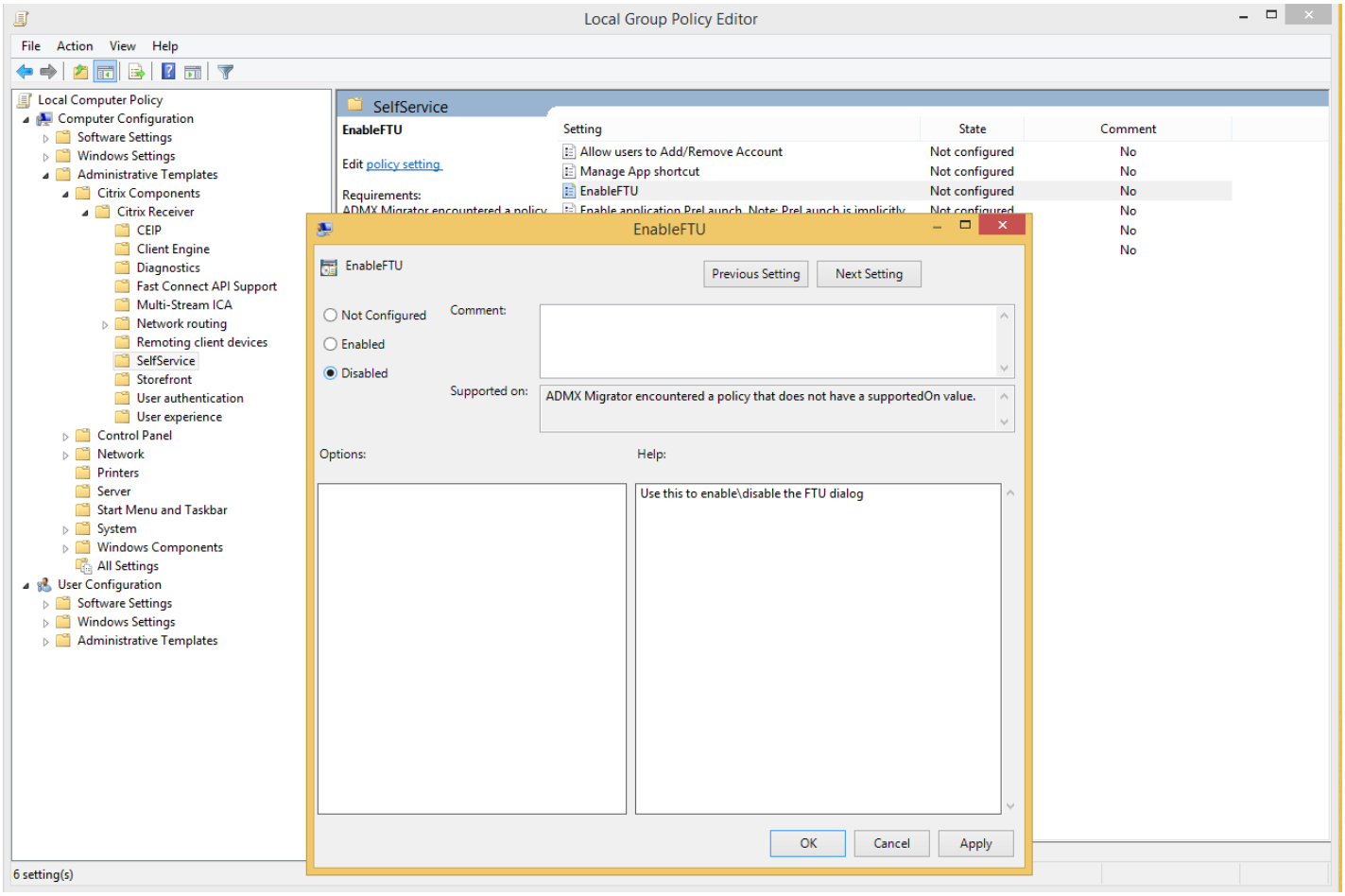
ストアが構成されていない場合は、次のメッセージが表示されます。



［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を使用する：**
  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。



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。

> ## 注意
>
> 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。

メールアドレスによるReceiverアカウントの検出機能が正しく動作するようにDNSサーバーを構成する方法については、StoreFrontのドキュメントの「メールによるアカウント検出を構成する」を参照してください。

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。

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。

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がserver1.comへのリモートアクセスが有効で、"HRApps"と言う名前のストアがserver2.comへのリモートアクセスが有効な場合、ユーザーは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。

> **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、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。

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 for Windows環境の最適化

Dec 08, 2016

管理者はReceiver環境を最適化できます。

- アプリケーションの起動時間の短縮
- デバイスから公開リソースへの接続を容易にする
- 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
- NDSユーザーのサポートを提供する
- ReceiverでXenApp for UNIXをサポートする
- 匿名アプリケーションへのアクセスを有効にする
- Single-Sign Onの構成をチェックする

そのほかの最適化オプションについては、XenDesktopのドキュメントの「セッションの継続性の維持」および「HDXによるユーザーエクスペリエンスの最適化」に関するトピック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

Dec 08, 2016

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、事前起動が午後1時45分に予定されている場合は、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。 この設定は、トラフィックの負荷が高いときに使用します。

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。

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

値のデータ：

予定事前起動を開始する、24時間形式の時刻と曜日です。入力形式は次のとおりです。

HH:MM|M:T:W:TH:F:S:SU - ここで、HHは時、MMは分です。 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|1:0:1:0:1:0:0と設定します。 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\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。

クライアント側デバイスのマッピング

Dec 08, 2016

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。

Windowsのサーバーマネージャーを使用して、クライアント側デバイスのマッピングオプション（ドライブ、プリンター、ポートなど）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。 たえば、サーバーのCドライブをMに変更し、DをNに変更しておくと、クライアントデバイスの既存のCドライブやDドライブにそのままアクセスできます。 この場合、セッションでのドライブマッピングは、次のようになります。

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

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

クライアント側デバイスの自動マッピングを無効にしない限り、ユーザーデバイスでサーバーに再接続すると、マッピングが再確立されます。 デフォルトでは、クライアント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。

Updated: 2015-01-27

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環境で、ポリシーの [クライアントCOMポートリダイレクト] 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>:

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

4. 操作を確認するには、

   net use

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

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

DNS名前解決をサポートする

Dec 08, 2016

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

Dec 08, 2016

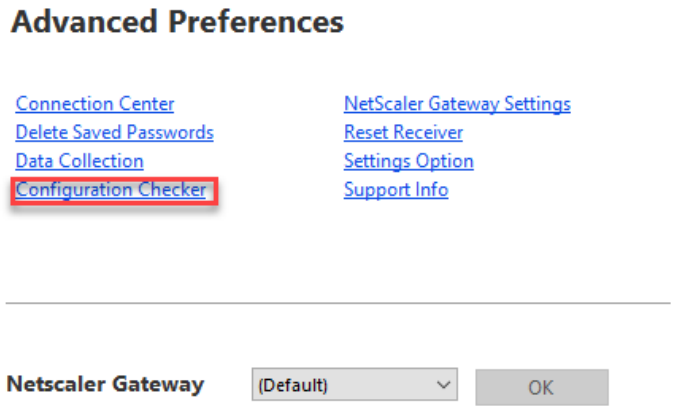
プロキシサーバーを使用しない環境でユーザーがWindows XP上のInternet Explorer 7.0を使用する場合は、Internet Explorerのプロキシ設定を変更する必要があります。 この場合、デフォルトでプロキシ設定が自動的に検出されます。 プロキシサーバーを使用しない環境でこのデフォルト設定を使用すると、プロキシ設定の検出時に不必要な遅延が発生します。 プロキシ設定の変更手順については、Internet Explorerのドキュメントを参照してください。 または、Web Interfaceを使ってプロキシ設定を変更できます。 詳しくは、Web Interfaceのドキュメントを参照してください。

構成チェッカーを使用してSingle Sign-Onの構成を検証する

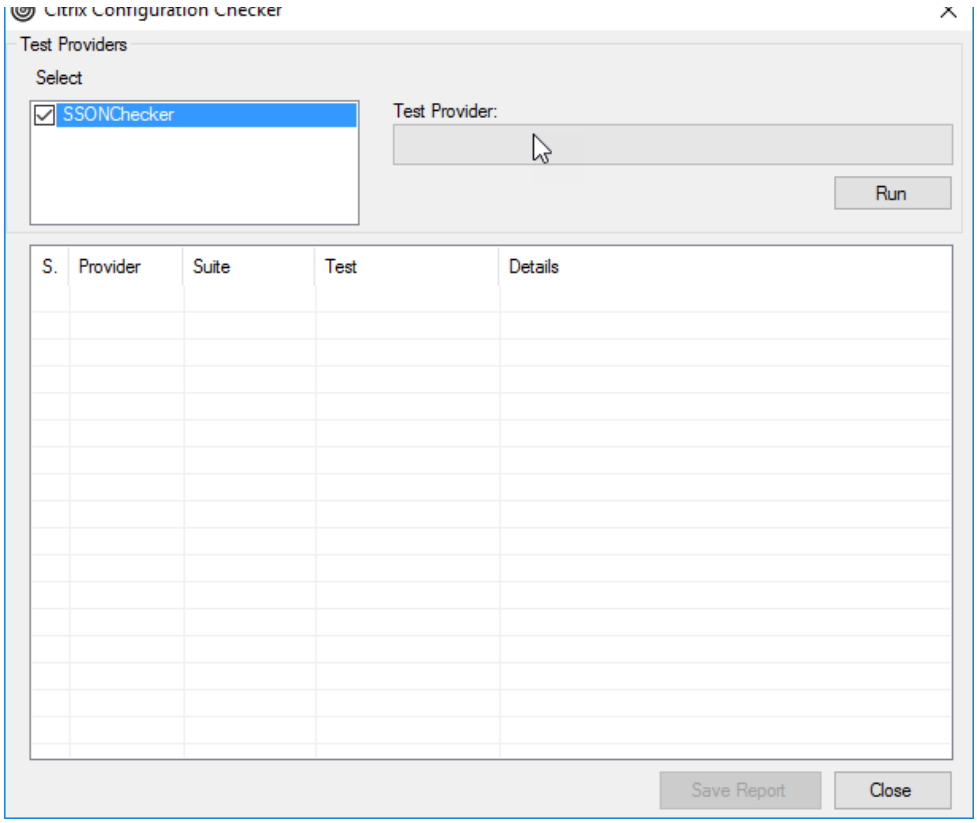
Dec 08, 2016

リリース4.5のCitrix Receiver for Windowsより、構成チェッカーを使用して、Single Sign-Onが適切に構成されていることを確認するテストを実行できるようになりました。 テストはSingle Sign-On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. Citrix Receiver for Windowsにログオンします。
2. 通知領域でCitrix Receiver for Windowsを右クリックし、 **[詳細な設定]** をクリックします。
［詳細な設定］ウィンドウが開きます。



3. **[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。



4. **[選択]** ペインで **[SSONChecker]** チェックボックスをオンにします。
5. **[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、Single Sign-On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. Single Sign-Onとともにインストール
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. Single Sign-Onプロセスの実行中
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、［詳細な設定］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。

注：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の形式は.txtです。

［詳細な設定］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. 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。

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］**をオンにします。
これにより、［詳細な設定］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/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。

ユーザーエクスペリエンスの向上

Dec 08, 2016

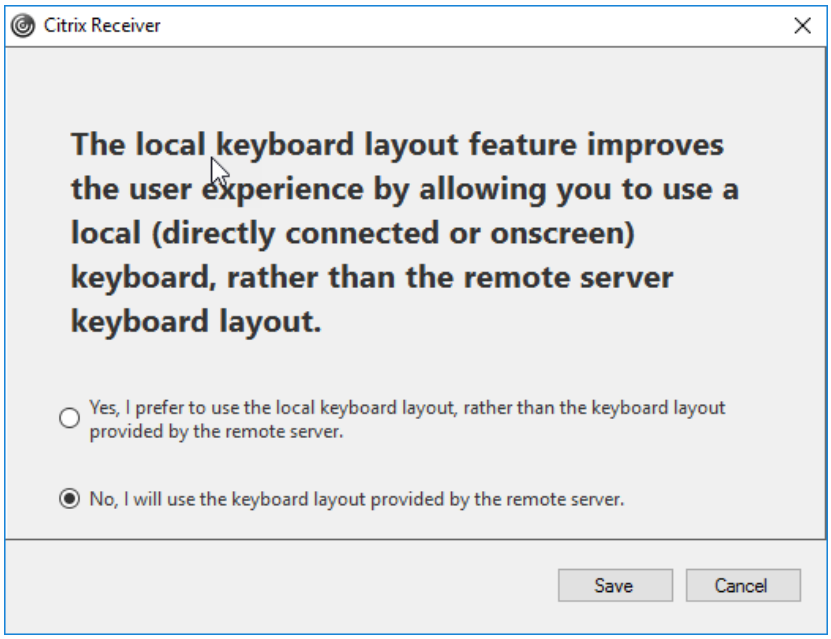
Receiverには、ユーザーエクスペリエンスを向上させるための以下の機能が用意されています。

キーボードレイアウト

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. Citrix Receiver for Windowsの通知領域アイコンで、**[詳細な設定]** > **[ローカル キーボード レイアウト設定]** > **[はい]** を選択します。



2. **[Save]** 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：HKLM\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。

> **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。 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。

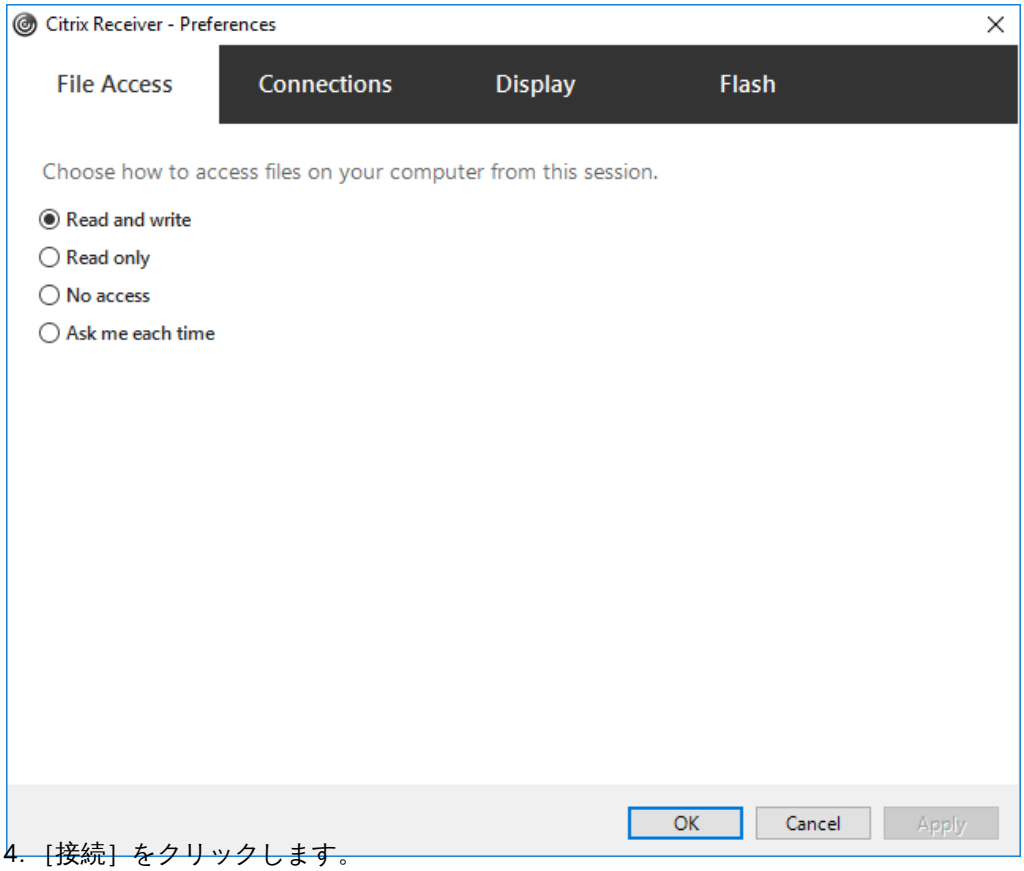
相対マウス

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。

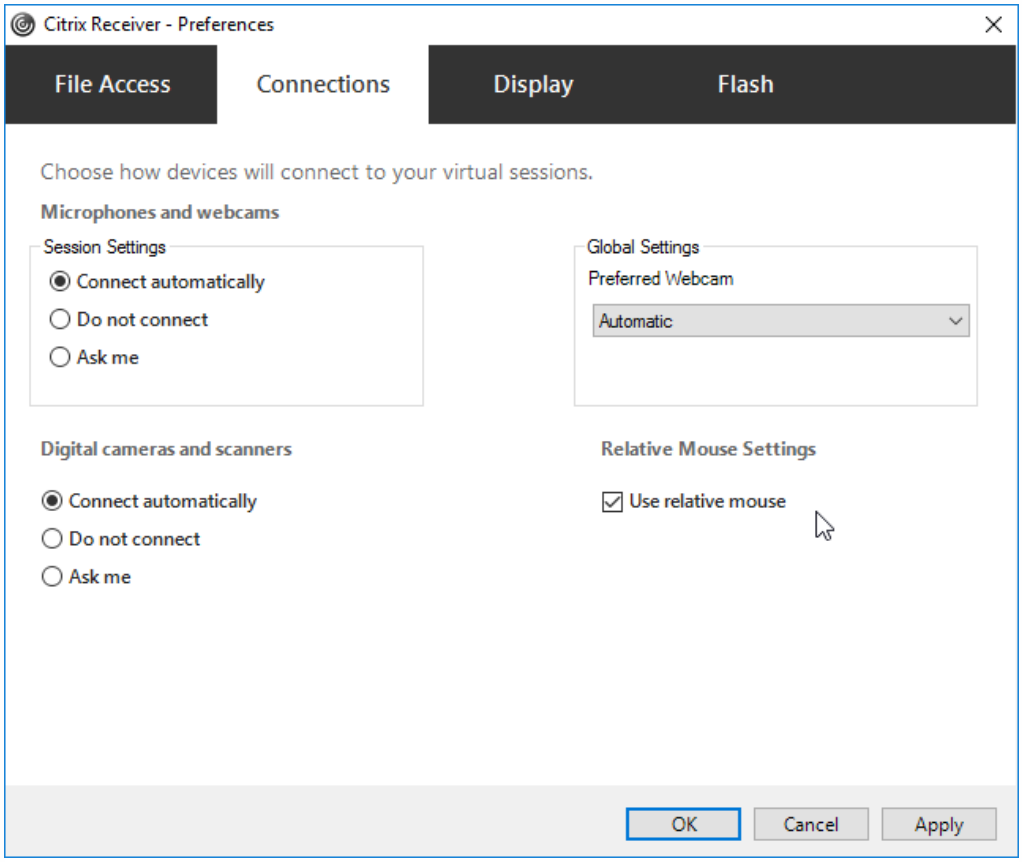
注：この機能を適用できるのは、公開デスクトップセッションのみです。

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］の下にある **[相対マウスを使用]** を有効にします。



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

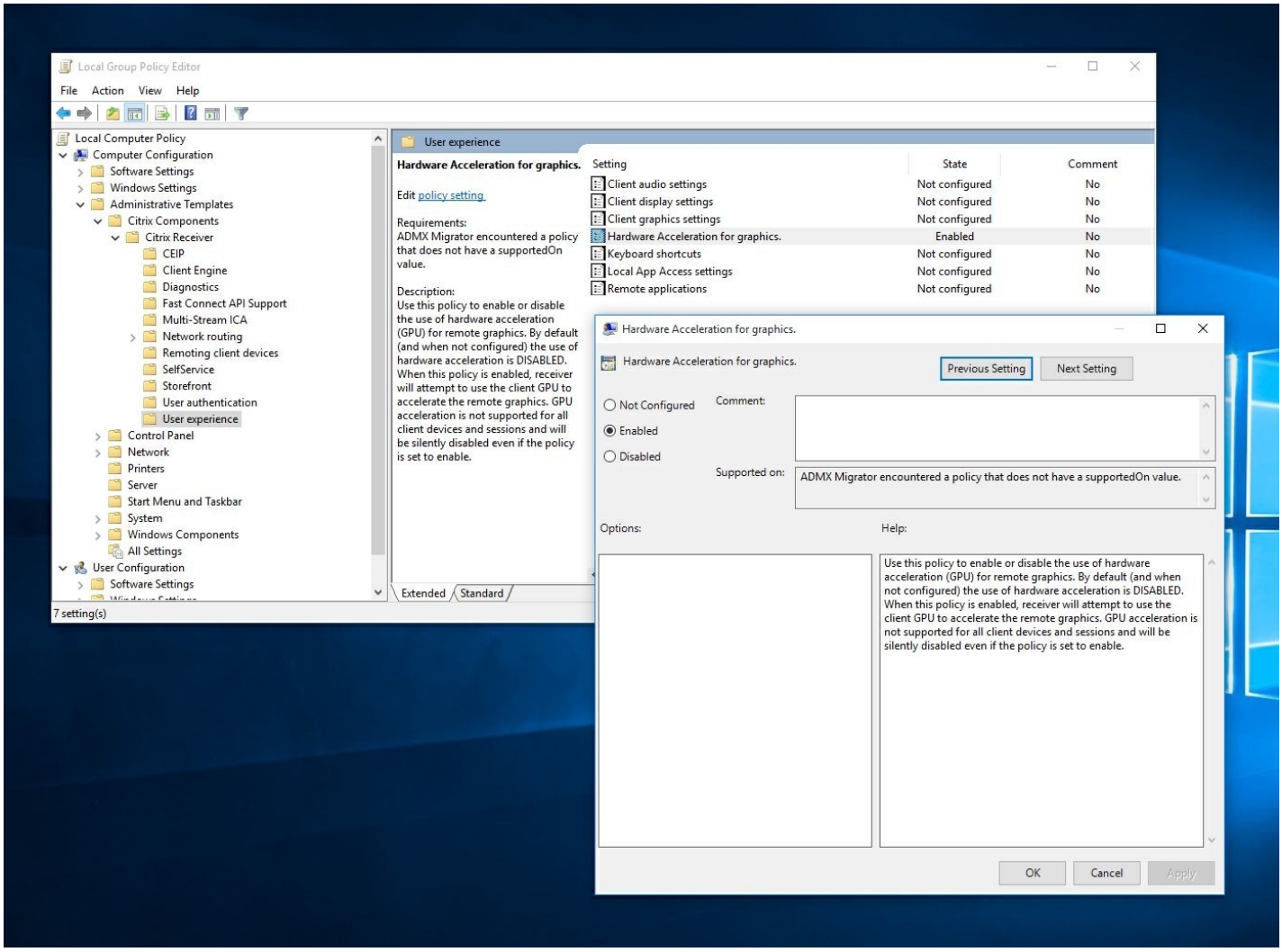
Citrix Receiver for Windows（HDX Engine 14.4含む）を使用する場合、クライアントで利用できる場合にはいつでもH.264デコードにGPUを使用できます。 GPUデコードで使用されるAPIレイヤーはDXVA（DirectX Video Acceleration）です。

詳しくは、Improved User Experience: Hardware Decoding for Citrix Windows Receiverを参照してください。

> **注意**
>
> 埋め込みGPUでは、この機能はデフォルトで無効になっています。

ハードウェアデコードを有効にするには：

1. “receiver.adml”を“root\Citrix\ICA Client\Configuration\en”から“C:\Windows\PolicyDefinitions\en-US”にコピーします。
2. “receiver.admx”を“root\Citrix\ICA Client\Configuration”から“C:\Windows\PolicyDefinitions\”にコピーします。
3. **ローカルグループポリシーエディタ**を開きます。
4. ［コンピューターの構成］>［管理用テンプレート］>［Citrix Receiver］>［User Experience］の順に選択し、**［Hardware Acceleration for graphics］**を開きます。
5. **［有効］**をクリックして**［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：HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\<session ID>

> ## 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、モニターの一つが２つめのGPUでアクティブな場合、CPUデコードがしよされます。
- 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際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。

マルチモニターのサポート

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コンピューターポリシーの［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CTX116286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\Modules\MobileReceiver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\Advanced\Modules\MobileReceiver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］の順に選択します。
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、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。
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。

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。

接続の保護

Dec 08, 2016

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。

Windowsコンピューターでは、Windows NTチャレンジ/レスポンス（NTLM）認証がデフォルトでサポートされています。

ドメインパススルー認証の構成

Dec 08, 2016

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。

シングルサインオン機能を有効にしたCitrix Receiver for Windowsのインストール

Citrix Receiver for Windowsのインストール時にドメインパススルー（SSON）を有効にするには、2通りの方法があります。

- コマンドラインインストールの使用
- グラフィカルユーザーインターフェイスの使用

コマンドラインインターフェイスを使用したドメインパススルーの有効化

コマンドラインインターフェイスを使用してドメインパススルー（SSON）を有効にするには

1. Citrix Receiver 4.xを**/includeSSON**イッチでインストールします。
   - 1つまたは複数のStoreFrontストアをインストールします（この手順は後で完了できます）。StoreFrontストアのインストールはドメインパススルー認証のセットアップに必須の条件ではありません。
   - Citrix Receiverを起動してパススルー認証が有効となっているかを確認してから、Citrix Receiverのインストール先エントポイントを再起動して、タスクマネージャーでssonsvr.exeプロセスが実行されているかを確認します。

> **注意**
>
> 1つまたは複数のStoreFrontストアを追加するための構文については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。

グラフィカルユーザーインターフェイスを使用したドメインパススルーの有効化

グラフィカルユーザーインターフェイスを使用してドメインパススルーの有効にするには

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、Single Sign-Onを有効にする方法を示しています。

注意

シングルサインオンの有効化インストールウィザードは、ドメイン参加マシンでフレッシュインストールをする場合にのみ使用できます。

Citrix Receiver for Windowsを再起動してパススルー認証が有効となっているかを確認してから、Citrix Receiver for Windowsのインストール先エンドポイントを再起動して、タスクマネージャーで**ssonsvr.exe**プロセスが実行されているかを確認します。

SSONのグループポリシー設定

このセクションの情報を使ってSSON認証用のグループポリシー設定を構成します。

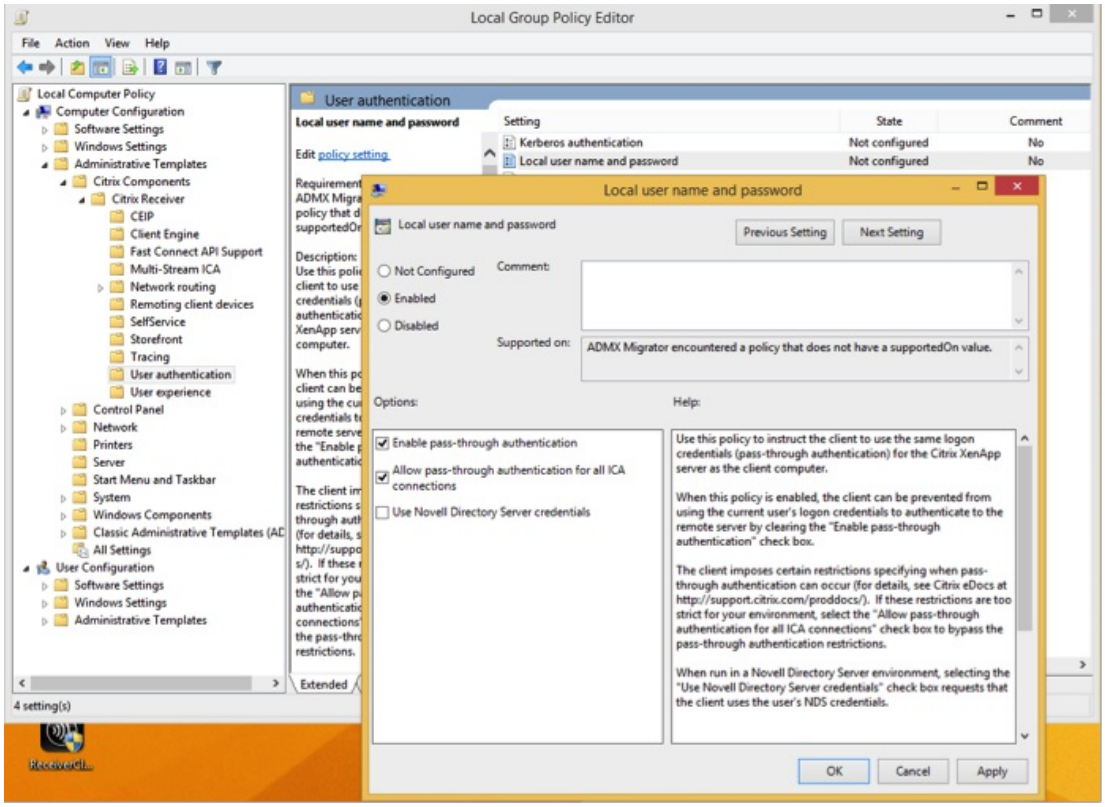
注意

SSONに関連するGPOポリシー設定のデフォルト値は **[パススルー認証を有効にします]** です。

SSONグループポリシー用のCitrix Receiver for Windowsテンプレートファイルの使用

次の手順により、ADMXファイルを使ってグループポリシー設定を構成します。

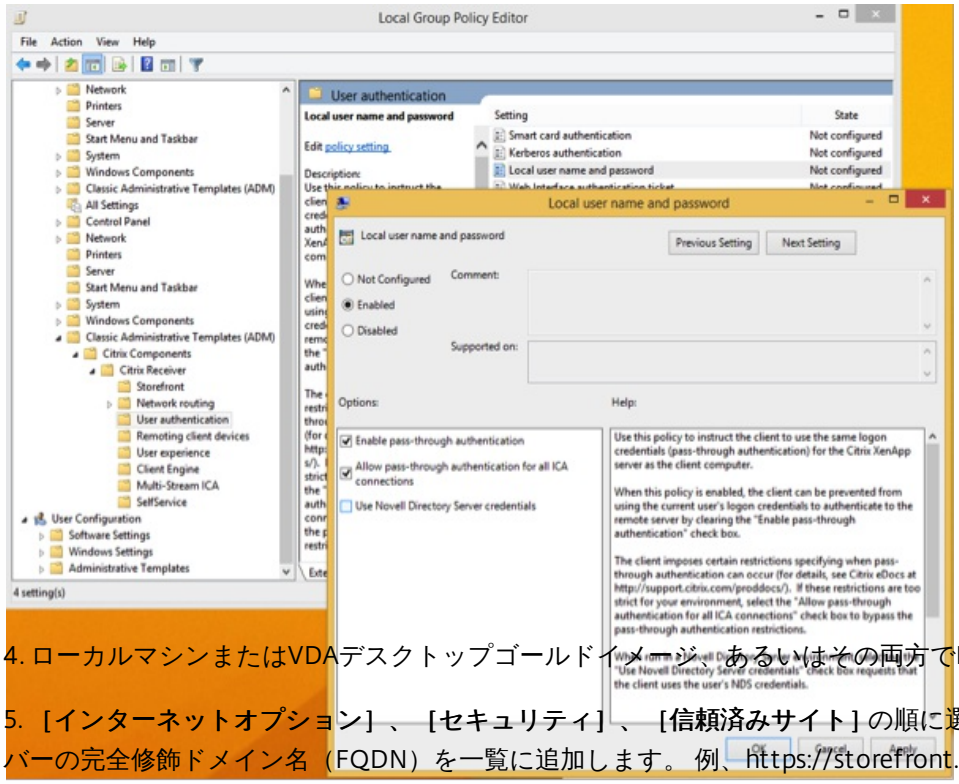
1. グループポリシーファイルを読み込みます。 Citrix Receiver for Windows4.3以降を使ったインストールでは、%SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configurationフォルダーにある**receiver.ADMX**または**receiver.ADML**を使用します。
2. **gpedit.msc**を開いて **[コンピューターの構成] > [管理テンプレート] > [Citrix Component] > [Citrix Receiver] > [User Authentication]** の順に選択します。
3. （ユーザーのローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方で）次のローカルコンピューターGPO設定を有効にします。
   - [Local user name and password] を選択します。
   - **[有効]** をクリックします。
   - **[Enable pass-through authentication]** チェックボックスをオンにします。
4. （Citrix Receiver for Windowsがインストールされた）エンドポイントまたはVDAデスクトップゴールデンイメージを再起動します。



SSONグループポリシーに対するADMファイルの使用

次の手順により、ADMファイルを使ってグループポリシー設定を構成します。

1. **[コンピューターの構成] > [管理用テンプレート] > [テンプレートの追加と削除]** の順に選択してローカルグループポリシーエディタを開きます。
2. **[Add]** をクリックしてADMテンプレートを追加します。
3. **receiver.adm**テンプレートを問題なく追加したら、**[コンピューターの構成] > [管理者テンプレート] > [従来の管理用テンプレート（ADM）] > [Citrix Components] > [Citrix Receiver] > [User authentication]** の順に選択します。



4. ローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方でInternet Explorerを開きます。

5. **［インターネットオプション］**、**［セキュリティ］**、**［信頼済みサイト］**の順に選択し、ストアパスのないStoreFrontサーバーの完全修飾ドメイン名（FQDN）を一覧に追加します。 例、https://storefront.example.com

> ## 注意
>
> またMicrosoft GPOを使って、StoreFrontサーバーを信頼済みサイトに追加することもできます。 GPOは**ゾーンの割り当て一覧へのサイト**と呼ばれ、**［コンピューターの構成］＞［管理用テンプレート］＞［Windowsコンポーネント］＞［Internet Explorer］＞［インターネットコントロールパネル］＞［セキュリティページ］**の順に選択してアクセスできます。

6. いったんログオフしてから、再度Citrix Receiverエンドポイントにログオンします。

Citrix Receiverを開くと、現在のユーザーがドメインにログオンしている場合は、ユーザーの資格情報がStoreFrontにパススルーされ、ユーザーの［スタート］メニュー設定を含む、Citrix Receiver内にアプリやデスクトップが列挙されます。 ユーザーが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、アプリまたはデスクトップが開きます。

Delivery ControllerでXMLの信頼を有効にする

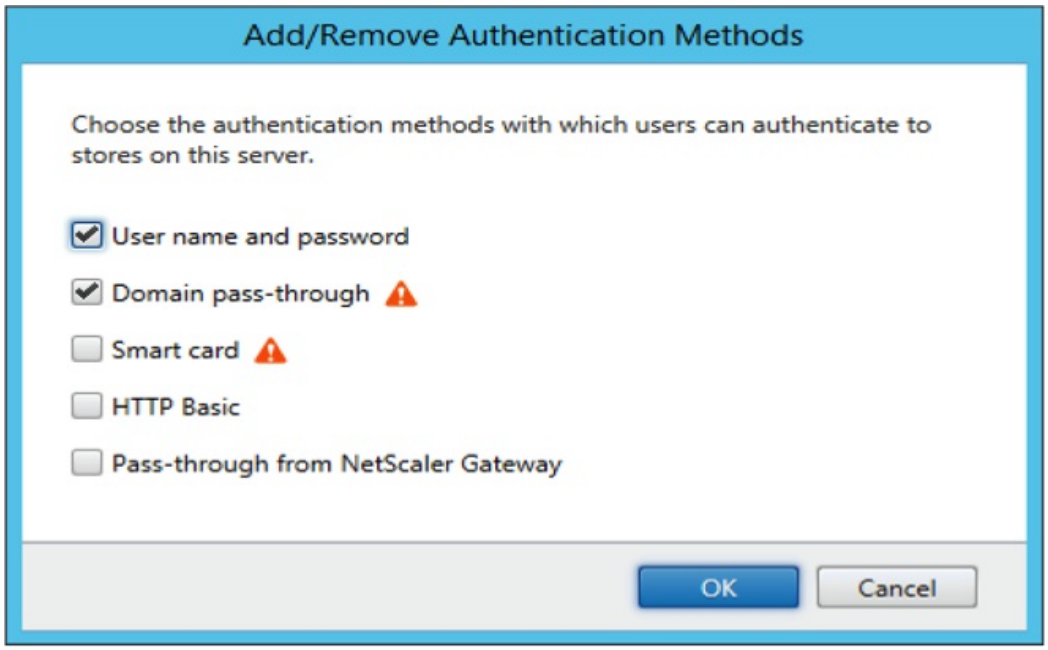
次の手順により、StoreFrontおよびWeb InterfaceでSSONを構成します

1. 管理者としてDelivery Controllerにログオンします。
2. （管理者権限で）Windows PowerShellを開きます。 PowerShellを使うと、コマンドを実行してDelivery ControllerがStoreFrontから送信されるXML要求を信頼できるようにできます。
3. Citrixコマンドレットが読み込まれていない場合は、「**Add-PSSapin Citrix***」と入力して**Enter**キーを押します。
4. Enterキーを押します。
5. 「**Add-PSSnapin citrix.broker.admin.v2**」と入力して**Enter**キーを押します。
6. 「**Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**」と入力して**Enter**キーを押します。
7. PowerShellを閉じます。

StoreFrontおよびWeb InterfaceでのSSON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 Management] > [XenApp Sevices Sites] > [Authentication Methods]** の順に選択して **[Pass-through]** を選択します

Kerberosを使用したドメインパススルー認証の構成

Dec 08, 2016

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を以下のように構成します。

- 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。

スマートカード認証の構成

Dec 08, 2016

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 DisableCtrlAltDel メソッドを False に設定して、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、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 を false に設定します。 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、［コンピューターの構成］、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［User authentication］、［Local user name and password］の順に選択します。
  Enable pass-through authentication。 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［Allow pass-through authentication for all ICA］チェックボックスをオンにする必要があります。

StoreFrontを以下のように構成します。

- 認証サービスを構成する場合、［Smart card］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HKEY_CURRENT_USERまたはHKEY_LOCAL_MACHINEのSoftware\[Wow6432Node\]Citrix\AuthManagerのCertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }を設定する。
  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HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManagerのSmartCardPINEntry=CSPを設定する。

証明書失効一覧のチェック機能の有効化

Dec 08, 2016

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、実行中のCitrix Receiver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コンポーネントが閉じていることを確認してください。

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］を選択し、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、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］>［ネットワークルーティング］>［TLS/SSLTLS/SSLデータ暗号化およびサーバー識別］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックします。
8. ［CRL verification］の一覧からオプションを一つ選択します。
   - 無効。 証明書失効一覧をチェックしません。
   - Only check locally stored CRLs： 以前インストールまたはダウンロードされたCRLが証明書の検証に使用されます。 証明書が失効していると接続に失敗します。
   - Require CRLs for connection： CRLはローカルで、およびネットワーク上の関連の証明書発行機関からチェックされます。 証明書が失効しているか見つからないと接続に失敗します。
   - Retrieve CRLs from network： CRLは関連の証明書発行機関からチェックされます。 証明書が失効していると接続に失敗します。

   ［CRL verification］を設定しない場合、デフォルトは［Only check locally stored CRLs］となります。

Receiver通信のセキュリティ保護

Dec 08, 2016

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環境では、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 （XenApp 7.6またはXenDesktop 7.6に対するSSL構成については、「SSL」を参照してください）。

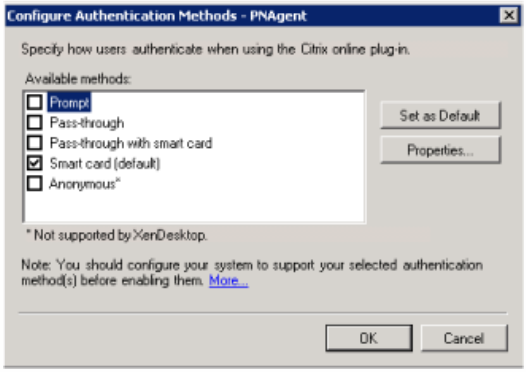
Citrix Receiver for Windowsは、Microsoft社のセキュリティ特化 - 機能制限（Specialized Security - Limited Functionality：SSLF）デスクトップセキュリティテンプレートが使用されている環境と互換性があります。 これらのテンプレートは、さまざまなWindowsプラットフォームでサポートされています。 詳しくは、Microsoft社のWebサイト（http://technet.microsoft.com）で公開されている、Windowsの『セキュリティガイド』を参照してください。

Web Interface 5.4でのスマートカード認証の構成

Dec 08, 2016

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。

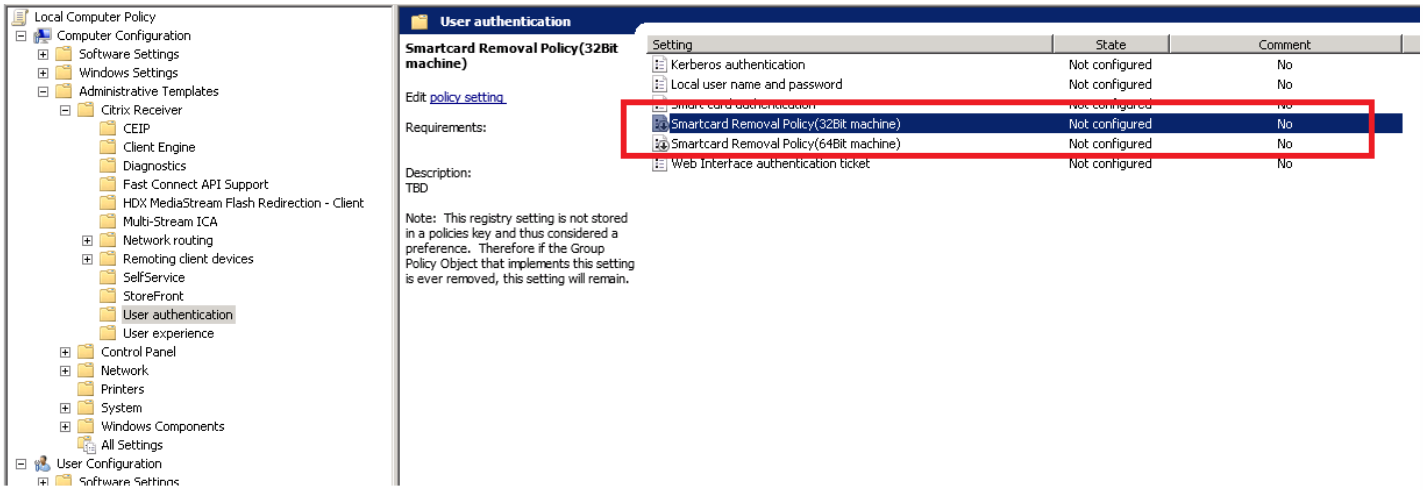
詳しくは、「How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication」を参照してください。

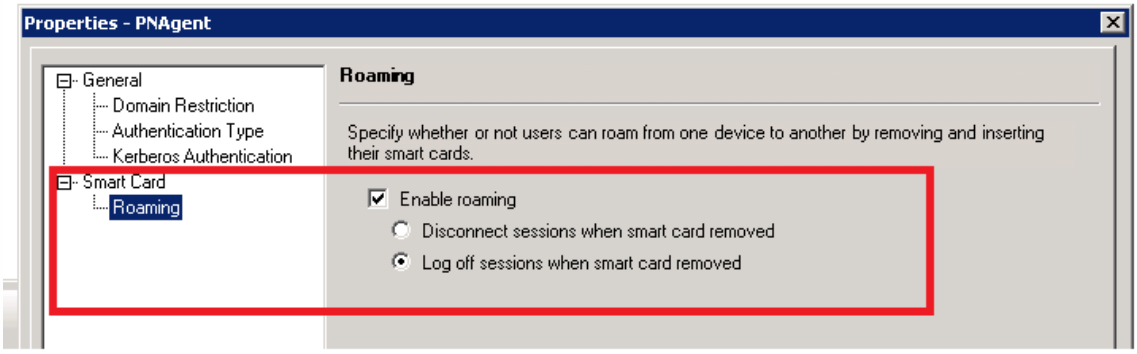


Citrix Web Interface 5.4 PNAgentサイトでユーザーが認証されている場合のスマートカードの取り出し動作を制御するには、スマートカードの取り出しポリシーを使用します。

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。

既知の問題

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。

NetScaler Gatewayによる接続

Dec 08, 2016

リモートのユーザーがNetScaler Gatewayを介して接続できるようにするには、CloudGatewayのコンポーネントであるAppControllerおよびStoreFrontと通信するようにNetScaler Gatewayを構成します。

- StoreFront環境では、NetScaler GatewayとStoreFrontを統合することで内部ユーザーやリモートユーザーがStoreFrontに接続できるようにします。 ユーザーは、StoreFrontに接続して仮想デスクトップおよびアプリケーションにアクセスします。 ユーザーは、Citrix Receiver for Windowsを使用して接続を行います。
- AppController環境では、Access GatewayとAppControllerを統合することでリモートユーザーがAppControllerに接続できるようにします。 ユーザーは、AppControllerに接続してWebアプリケーションやSaaS（Software as a Service：サービスとしてのソフトウェア）アプリケーションを取得し、ShareFile Enterpriseサービスで共有されているドキュメントにアクセスしたりします。 ユーザーは、Citrix Receiver for WindowsまたはNetScaler Gateway Plug-inを使用して接続を行います。

> **注意**
>
> 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。

接続の構成方法については、「Integrating NetScaler Gateway with XenMobile App Edition」と関連トピックを参照してください。 Citrix Receiver for Windowsでの設定については、以下のトピックを参照してください。

- Configuring Session Policies and Profiles for XenMobile App Edition
- Creating the Session Profile for Receiver for XenMobile App Edition
- Configuring Custom Clientless Access Policies for Receiver
- Configuring Session Policies and Profiles for CloudGateway
- Creating the Session Profile for Receiver for CloudGateway Enterprise
- Creating the Session Profile for Receiver for CloudGateway Express
- Configuring Custom Clientless Access Policies for Receiver

リモートのユーザーがNetScaler Gatewayを介してWeb Interface環境に接続できるようにするには、Web Interfaceと通信するようにNetScaler Gatewayを構成します。詳しくは、Citrix eDocsの「Providing Access to Published Applications and Virtual Desktops Through the Web Interface」の各トピックを参照してください。

Secure Gatewayによる接続

Dec 08, 2016

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イで保護することができます。 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ときは、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。

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。 リレーモードについて詳しくは、Secure Gatewayのトピックを参照してください。

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.x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。

- Host name
- 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。

ファイアウォールを介した接続

Dec 08, 2016

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。 ファイアウォールが使用されている環境では、Citrix Receiver for WindowsとWebサーバーおよびCitrix製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。 このためには、ユーザーデバイスとWebサーバー間のHTTPトラフィック（一般に標準HTTPポート80、またはセキュアなWebサーバーを使用している場合はポート443での通信）がファイアウォールを通過できるように設定します。 また、ReceiverとCitrix製品サーバー間の通信では、ポート1494とポート2598の受信ICAトラフィックがファイアウォールを通過できるように設定します。

ファイヤウォールによるネットワークアドレス変換（NAT：Network Address Translation）を使用している場合は、Web Interfaceを使って内部アドレスから外部アドレスおよびポートへのマッピングを定義できます。 たとえば、XenAppサーバーやXenDesktopサーバーに代替アドレスが設定されていない場合は、Web InterfaceからReceiverに代替アドレスが提供されるように設定できます。 これにより、Citrix Receiver for Windowsでのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。 詳しくは、Web Interfaceのドキュメントを参照してください。

信頼関係の適用

Dec 08, 2016

信頼済みサーバーの構成を使用して、Citrix Receiver for Windowsの接続に関連する信頼関係を識別し適用することができます。 信頼関係を設定すると、Citrix Receiver for Windows管理者とユーザーはユーザーデバイス上のデータが健全であることをさらに確実に信頼できるようになります。また、Citrix Receiver for Windows接続の悪用を防止できます。

この機能を有効にすると、Citrix Receiver for Windowsで信頼関係に必要な条件を指定し、サーバーとの接続を信頼するかどうかを決定できます。 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。

信頼済みサーバーの構成を有効にする場合は、接続先のサーバーがWindowsの信頼済みサイトゾーンに追加されている必要があります。 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。

信頼するサーバーの構成を有効にするには

ローカルのコンピューターにこの変更を適用する場合、コネクションセンターを含むすべてのCitrix Receiver for Windowsコンポーネントを終了します。

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. ［ユーザーの構成］の［管理用テンプレート］を展開します。
7. 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］>［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。
8. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックします。

昇格レベルとwfcrun32.exe

Dec 08, 2016

Windows 8、Windows 7、またはWindows Vista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）標準ユーザーとして実行するwfcrun32.exeを使用してアプリケーションを起動する場合は、Receiverなどほか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。

プロキシサーバー経由の接続

Dec 08, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

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ときは、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の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。

Secure Sockets Layer (SSL) Relayによる接続

Dec 08, 2016

このトピックの内容は、XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には該当しません。

Citrix Receiver for WindowsをSSL（Secure Sockets Layer）Relayサービスと一緒に使うことができます。 Citrix Receiver for Windowsでは、TLSプロトコルがサポートされます。

- TLS（Transport Layer Security）は、標準化されたSSLプロトコルの最新版です。 IETF（Internet Engineering TaskForce）が、SSLの公開標準規格の開発をNetscape Communications社から引き継いだときに、SSLという名前をTLSに変更しました。 TLSは、サーバーの認証、データの暗号化、メッセージの整合性の確認を行って、データ通信を保護します。 米国政府など、 データ通信を保護するためにTLSの使用を必須としている組織もあります。 このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。 FIPS 140は、暗号化の情報処理規格です。

Citrix SSL Relayを使用する接続

このトピックの内容は、XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には該当しません。

デフォルトではCitrix SSL Relayのリスナーポートとして、TLSで保護された通信の標準ポートであるXenAppサーバーのTCPポート443が使用されます。 Citrix SSL Relayは、TLS接続要求を受信すると、その要求を解読してからサーバーに転送します。ユーザーがTLS+HTTPSブラウズを選択した場合は、Citrix XML Serviceに転送します。

443以外のリスナーポートを構成する場合、プラグインに対して非標準のリスナーポート番号を指定する必要があります。

Citrix SSL Relayを使用すると、次の通信のセキュリティを保護できます。

- TLS機能が有効になっているクライアントとサーバー間の通信。 Citrixコネクションセンターでは、TLS暗号化を使用している接続に鍵のアイコンが付きます。
- サーバーファームのXenAppサーバーと、Web InterfaceのWebサーバーとの間の通信。

インストールを保護するためのSSL Relayの構成については、XenAppのドキュメントを参照してください。

ユーザーデバイスの要件

システム要件に加えて、次の条件を満たしている必要があります。

- 128ビット暗号化をサポートしている。
- サーバー証明書にあるCA（Certificate Authority：証明機関）の署名を認証するルート証明書がインストールされている。
- サーバー上のSSL Relayが使用するTCPポートの番号がCitrix Receiver for Windowsで認識されている。
- Microsoftが推奨するすべてのService Packまたはアップグレードが適用されている。

Internet Explorerをインストールしていて、システムの暗号化レベルがわからない場合は、Microsoft社のWebサイト（http://www.microsoft.com）から128ビット暗号化が含まれているサービスパックをダウンロードしてインストールしてください。

重要：Citrix Receiver for Windowsでサポートされる証明書のキーの長さは、4,096ビットまでです。 使用するルート証明書、中間証明書、およびサーバー証明書のキーの長さが4,096ビットを超えると、正しく接続できない場合があります。

すべての接続のリスナーポート番号を変更するには

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、プラグインの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］>［ネットワークルーティング］>［TLS/SSLTLS/SSLデータ暗号化およびサーバー識別］の順に選択します。
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［Allowed SSL servers］に<server:SSL relay port number>の形式で新しいポート番号を入力します。ここで、<SSL relay port number>はリスナーポートの番号です。 ワイルドカードを使用して複数のサーバーを指定できます。 たとえば、*.Test.com:<SSL relay port number>は、指定されたポートを介するTest.comへのすべての接続と一致します。

特定の接続のリスナーポート番号を変更するには

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。

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追加している場合、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］>［ネットワークルーティング］>［TLS/SSLTLS/SSLデータ暗号化およびサーバー識別］の順に選択します。
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［Allowed SSL servers］に信頼済みサーバーと新しいポート番号のコンマ区切りの一覧を「servername:SSL relay port number,servername:SSL relay port number」の形式で入力します。ここで、<SSL relay port number>はリスナーポートの番号です。 次の例のように、特定の信頼済みSSLサーバーのコンマ区切りの一覧を指定できます。
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
   これをappsrv.iniファイルの例に当てはめると次のようになります。[Word]
   SSLProxyHost=csghq.Test.com:443

   [Excel]
   SSLProxyHost=csghq.Test.com:444

   [Notepad]
   SSLProxyHost=fred.Test.com:443

TLSの構成および有効化

Dec 08, 2016

このトピックの内容は、XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には該当しません。

Citrix Receiver for Windowsで常にTLSが使用されるようにするには、Secure GatewayサーバーまたはCitrix SSL Relayサービスで TLSを指定します。 詳しくは、Secure GatewayまたはCitrix SSL Relayサービスのドキュメントのトピックを参照してください。

さらに、ユーザーデバイスがすべてのシステム要件を満たしていることを確認します。

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。 StoreFront通信の保護については、StoreFrontのドキュメントのセキュリティに関するトピックを参照してください。

ユーザーデバイスへのルート証明書のインストール

TLS機能が有効になっているCitrix Receiver for Windowsとサーバーファーム間の通信をTLSで保護するには、サーバー証明書の証明機関（CA）の署名を認証するためのルート証明書がユーザーデバイスにインストールされている必要があります。

Citrix Receiver for Windowsでは、Windowsオペレーティングシステムでサポートされているを CAをサポートしています。 これらのCAのルート証明書は、Windowsと一緒にインストールされ、Windowsのユーティリティを使用して管理されます。 これらのルート証明書は、Internet Explorerで使用されているものと同じです。

ほかのCAを使用する場合は、そのCAからルート証明書を取得して、各ユーザーデバイスにインストールする必要があります。 インストールされたルート証明書はMicrosoft Internet ExplorerとReceiverの両方で使用および信頼されます。

次の管理方法や配布方法を使用して、ルート証明書をインストールできる可能性があります。

- Internet Explorer管理者キット（IEAK）ウィザードおよびプロファイルマネージャーを使用する
- サードパーティ製の配布ツールを使用する

Windowsオペレーティングシステムでインストールされた証明書が、組織のセキュリティ条件を満たしていることを確認するか、所属する組織のCAによって発行された証明書を使用してください。

Citrix Receiver for WindowsでTLSを使用するようにWeb Interfaceを構成するには

1. TLSでアプリケーション一覧を暗号化して、そのデータをCitrix Receiver for WindowsとWeb Interfaceサーバー間でやり取りするには、Web Interfaceサーバーの適切な設定を構成します。 SSL/TLSのための証明書をホストする、XenAppサーバーの名前を設定する必要があります。
2. Citrix Receiver for WindowsとWeb Interfaceサーバー間でやり取りされる構成情報をセキュアHTTP（HTTPS）プロトコルで暗号化するには、サーバーのURLを「https://<servername>」の形式で入力します。 Windowsの通知領域でCitrix Receiver for Windowsアイコンを右クリックし、［基本設定］を選択します。
3. ［プラグインの状態］の［Online Plug-in］のエントリを右クリックし、［サーバーの変更］を選択します。

TLSのサポートを構成するには

ローカルのコンピューターにこの変更を適用する場合、Citrixコネクションセンターを含むすべてのReceiverコンポーネントを終了します。

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（Active Directoryを使用する場合）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］>［ネットワークルーティング］>［TLS/SSLTLS/SSLデータ暗号化およびサーバー識別］の順に選択します。
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TLS設定を選択します。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、Citrix Receiver for WindowsはTLS暗号化を使用して接続します。
   - ［SSL cipher suite］で［Detect version］を選択して、Citrix Receiver for Windowsが行政機関レベルおよび営利企業レベルの適切な暗号の組み合わせとネゴシエートするようにします。行政機関レベルまたは営利企業レベルのどちらかに暗号の組み合わせを限定できます。
   - ［CRL verification］で［Require CRLs for connection］を選択して、Citrix Receiver for Windowsが関連の証明書発行機関から証明書失効リスト（CRL：Certificate Revocation List）を取得するよう求めます。

Web Interfaceでグループポリシーテンプレートを使用してFIPS 140セキュリティ規格に準拠するには

ローカルのコンピューターにこの変更を適用する場合、コネクションセンターを含むすべてのCitrix Receiver for Windowsコンポーネントを終了します。
FIPS 140のセキュリティ規格に準拠するには、グループポリシーテンプレートを使ってパラメーターを構成するか、Web Interfaceサーバー上のDefault.icaファイルのパラメーターを含めます。Default.icaファイルについて詳しくは、Web Interfaceの情報を参照してください。

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のテンプレートファイル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3.～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］>［ネットワークルーティング］>［TLS/SSLTLS/SSLデータ暗号化およびサーバー識別］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして適切な設定を選択します。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、ReceiverはTLS暗号化を使用して接続します。
   - ［SSL暗号の組み合わせ］で［自治体］を選択します。
   - ［CRL verification］で［Require CRLs for connection］を選択します。

Citrix Receiver for Windowsとの通信にTLSを使用するようにWeb Interfaceを構成するには

Web Interfaceを使用する場合は、SSL証明書をホストするサーバーのコンピューター名を指定します。TLSを使ってCitrix Receiver for WindowsとWeb Interfaceサーバー間の通信を保護する方法について詳しくは、Web Interfaceの情報を参照してください。

1. ［設定を変更］メニューの［サーバー設定］を選択します。
2. ［プラグインとこのサイト間の通信にSSL/TLSを使用する］チェックボックスをオンにします。
3. 変更を保存します。

SSL/TLSを有効にすると、すべてのURLでHTTPSプロトコルが使用されます。

Citrix Receiver for Windowsとの通信にTLSを使用するようにXenAppを構成するには

接続時にTLSを使用するようにXenAppサーバーを構成して、Citrix Receiver for Windowsとサーバー間の通信を保護することができます。

1. XenAppサーバー用のCitrix管理コンソールを開き、セキュリティを保護する公開アプリケーションの［アプリケーションプロパティ］ダイアログボックスを開きます。
2. ダイアログボックス左側のペインで［詳細設定］>［クライアントオプション］の順に選択し、［SSLおよびTLSを有効に

する］チェックボックスをオンにします。
3. SSL/TLSプロトコルで保護するすべての公開アプリケーションで、このチェックボックスをオンにします。

Web Interfaceを使用する場合は、SSL証明書をホストするサーバーのコンピューター名を指定します。 TLSを使ってCitrix Receiver for WindowsとWeb Interfaceサーバー間の通信を保護する方法について詳しくは、Web Interfaceの情報を参照してください。

Web Interfaceサーバーとの通信にTLSを使用するようにReceiverを構成するには

TLSを使用するようにCitrix Receiver for Windowsを構成して、Citrix Receiver for WindowsとWeb Interfaceサーバー間の通信を保護することができます。

有効なルート証明書がユーザーデバイスにインストールされていることを確認します。 詳しくは、「ユーザーデバイスへのルート証明書のインストール」を参照してください。

1. Windowsの通知領域でCitrix Receiver for Windowsアイコンを右クリックし、［基本設定］を選択します。
2. ［プラグインの状態］の［Online Plug-in］のエントリを右クリックし、［サーバーの変更］を選択します。
3. ［サーバーの変更］ダイアログボックスに、現在構成されているURLが表示されます。 TLSを使って設定データを暗号化するには、サーバーURLを「https://<servername>」の形式で入力します。
4. ［更新］をクリックして変更を適用します。
5. ユーザーデバイス上のWebブラウザーでTLSを有効にします。 詳しい設定方法については、Webブラウザーのヘルプを参照してください。

TLSおよびHTML5ビデオリダイレクト

HTML5ビデオリダイレクトは、TLS（HTTPS）経由のビデオコンテンツをサポートします。 このために、カスタム証明書をVDAでコンピューターの証明書ストアに配置します。

HTML5ビデオリダイレクトはデフォルトで無効になっています。

TLS経由のビデオコンテンツにHTML5ビデオリダイレクトを使用しない場合、VDAの信頼されたルート証明書ストアで2つの証明書を削除することをお勧めします。 削除する証明書は、発行先「Citrix HDX」/発行者「Citrix HDX」の証明書と、発行先「127.0.0.1」/発行者「Citrix HDX」の証明書です。

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

Dec 08, 2016

このトピックの内容は、管理用テンプレートを使用するWeb Interface環境にのみ適用されます。

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をユーザーが起動しないようにするのに役立ちます。 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。 このアプリケーションまたはデスクトップの起動署名検証ためのCitrix Receiver for Windowsセキュリティポリシーは、グループポリシーオブジェクト、Storefront、またはCitrix Merchandising Serverを使用して構成できます。 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を使用してアプリケーションまたはデスクトップの起動署名検証を有効にし設定するには、次の手順に従います。

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ica-file-signing.adm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は、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］を選択し、Citrix Receiver for WindowsのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）を参照してica-file-signing.admを選択します。
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］の順に選択し、［ICAファイルの署名を有効にします］を開きます。
7. ［有効］をクリックすると、信頼できる証明書のサムプリントのホワイトリストに署名証明書のサムプリントを追加したり、ホワイトリストから署名証明書のサムプリントを削除したりできます。これは、［表示］をクリックして［内容の表示］ダイアログボックスを使用して行います。 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。 ［Security Policy］ボックスの一覧から［Only allow signed launches（more secure）］または［Prompt user on unsigned launches（less secure）］を選択します。

オプション	説明

オプション	説明
Only allow signed launches（more secure）	正しく署名された、信頼できるサーバーからの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。 アプリケーションまたはデスクトップの起動に無効な署名がされている場合は、Citrix Receiver for Windowsにセキュリティの警告メッセージが表示されます。 ユーザーは続行できず、承認されていない起動が禁止されます。
Prompt user on unsigned launches（less secure）	未署名または無効な署名のアプリケーションまたはデスクトップの起動が試行されるたびに、確認ダイアログボックスが開きます。 ユーザーはアプリケーションの起動を続行することも、起動を中止する（デフォルト）こともできます。

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。

シングルサインオンを有効にして信頼済みサーバーとの接続を保護するためのWebブラウザーとICAファイルの構成

Dec 08, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

シングルサインオンを使用したり、信頼済みサーバーへのセキュリティで保護された接続を管理したりするには、Citrixサーバーのサイトアドレスを Internet Explorerの［ローカルイントラネット］または［信頼済みサイト］ゾーンに追加します。これは、ユーザーデバイスのInternet Explorerで［ツール］、［インターネットオプション］、［セキュリティ］の順に選択して行います。 アドレスにはISM（Internet Security Manager）でサポートされるワイルドカード（*）を含めたり、「<protocol>://<URL>[:<port>]」のように具体的に指定する形式を使用したりできます。

ICAファイルとサイトゾーンのエントリの両方で同じ形式を使用する必要があります。 たとえば、ICAファイルで FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）を使用した場合は、サイトゾーンのエントリでもFQDNを使用する必要があります。 XenDesktop接続ではデスクトップグループ名の形式のみを使用します。

サポートされる形式（ワイルドカードを含む）

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://hostname

http[s]://fqdn.example.com

http[s]://*.example.com

http[s]://cname.*.example.com

http[s]://*.example.co.uk

desktop://group-20name

ica[s]://xaserver1

ica[s]://xaserver1.example.com

Single Sign-Onの起動またはWebサイトによる保護された接続の使用

サイトゾーンにWeb Interfaceサイトの正確なアドレスを追加します。

Webサイトのアドレスの例

https://my.company.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

Desktop ViewerでのXenDesktop接続

アドレスは「<desktop>//<Desktop Group Name>」の形式で追加します。 デスクトップグループ名（<Desktop Group Name>）にスペースが含まれる場合、各スペースを「-20」で置き換えます。

カスタムICAエントリの形式

ICAファイルでは、Citrixサーバーのサイトアドレスを次の形式で指定します。 このアドレスを同じ形式で、Internet Explore の［ローカルイントラネット］または［信頼済みサイト］ゾーンに追加します。これは、ユーザーデバイスのInternet Explorerで［ツール］、［インターネットオプション］、［セキュリティ］の順に選択して行います。

ICAファイルのHttpBrowserAddressエントリの例

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

ICAファイルのXenAppサーバーアドレスエントリの例

ICAファイルにXenAppサーバーの**Address**フィールドのみが含まれる場合、次の形式のいずれかを使用します。

icas://10.20.30.40:1494

icas://my.xenapp-server.company.com

ica://10.20.30.40

クライアントリソースのアクセス許可の設定

Dec 08, 2016

このトピックの内容は、Web Interface環境にのみ適用されます。

信頼済みサイトおよび制限付きサイトのゾーンを使用して、次の方法でクライアントリソースのアクセス許可を設定できます。

- 信頼済みサイトにWeb Interfaceのサイトを追加する
- 新しいレジストリ設定を変更する

> ### 注意
>
> Citrix Receiverの最近の機能拡張のより、以前のバージョンのプラグイン/Receiverで使用できたINIファイルによる手順は、次の手順により置き換えられました。

信頼済みサイトにWeb Interfaceのサイトを追加するには

1. Internet Explorerの［ツール］メニューで［インターネットオプション］>［セキュリティ］の順に選択します。
2. ［信頼済みサイト］アイコンをクリックし、［サイト］をクリックします。
3. ［このWebサイトをゾーンに追加する］ボックスにWeb InterfaceのサイトのURLを入力して［追加］をクリックします。
4. http://support.citrix.com/article/CTX133565からレジストリ設定をダウンロードしてレジストリを変更します。32ビット版WindowsのユーザーデバイスにはSsonRegUpx86.regを、64ビット版WindowsのユーザーデバイスにはSsonRegUpx64.regを使用します。
5. ユーザーデバイスからログオフしてログオンします。

レジストリでクライアントリソースのアクセス許可を変更するには

> ### 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。 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. http://support.citrix.com/article/CTX133565からレジストリ設定をダウンロードして各ユーザーデバイスに設定をインポートします。 32ビット版WindowsのユーザーデバイスにはSsonRegUpx86.regを、64ビット版WindowsのユーザーデバイスにはSsonRegUpx64.regを使用します。
2. レジストリエディターを開いてHKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trustに移動し、次のリソースのデフォルト値を適切なゾーンにおいて必要なアクセス値に変更します。

リソースキー	リソースの説明
FileSecurityPermission	クライアント側ドライブ
MicrophoneAndWebcamSecurityPermission	マイクおよびWebカメラ

リソースキー	リソースの説明
ScannerAndDigitalCameraSecurityPermission	USBおよびそのほかのデバイス

値	説明
0	アクセスなし
1	読み取り専用アクセス
2	フルアクセス
3	アクセスするかどうかユーザーに確認

サポートされているTLS暗号スイート

Citrix Receiver for Windowsがアプリケーションを列挙していてStorefrontと通信している場合、Windowsプラットフォーム暗号化が使用されます。

Citrix Receiver for WindowsとXenApp/XenDesktop間のTCP接続の場合、Citrix Receiver for Windowsでは次の暗号の組み合わせのTLS 1.0、1.1、および1.2がサポートされます。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

UDPベースの接続の場合、Citrix Receiver for Windowsは次の暗号の組み合わせのDTLS 1.0をサポートします。

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

SP 800-52準拠モードの有効化

［コンピューターの構成］>［管理テンプレート］>［Citrix Components］>［Network Routing］>［TLS and Compliance Mode Configuration］の下に、**[Enable FIPS]**というチェックボックスが実装されました。 このチェックボックスをオンにすると、すべてのICAコネクションに対してFIPS準拠の暗号化のみが使用されます。 デフォルトでは、このオプションは無効になっています。

新しいセキュリティ準拠モードであるSP 800-52が実装されています。 デフォルトでは、このオプションは無効になっています。 NIST SP 800-52で必要なコンプライアンスについて説明した次のリンクを参照してください。http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295

> **注意**
>
> SP800-52準拠モードはFIPSコンプライアンスを必要とします。 SP800-52が有効な場合、FIPS設定とは関係なくFIPSモードも有効になります。 Certificate Revocation Checkポリシーの値は［Full access check and CRL required］または［Full access check and CRL required All］に設定します。

TLSバージョンと暗号の組み合わせの制限

TLSバージョンと暗号の組み合わせを制限するようにCitrix Receiver for Windowsを構成できます。 ICAコネクションのTLSプロトコルを決定するための、許可されたTLSプロトコルのバージョンを選択するオプションがあります。 クライアントとサーバー間で相互に使用できる最新のTLSバージョンが選択されます。 次のオプションがあります。

- TLS 1.0 | TLS 1.1 | TLS 1.2（デフォルト）
- TLS 1.1 | TLS 1.2
- TLS 1.2

このオプションはAndroid 3.0以降で使用できます。 Citrix Receiver for Windowsは次のものを選択できます。

- 任意
- Commercial
- Government

商用暗号の組み合わせ

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

公用商用暗号の組み合わせ

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **注意**
>
> **［Require TLS for all connections］**が有効な場合、StoreFrontへの接続要求にもHTTPSが必要です。HTTPとしてのストアの追加に失敗し、非SSL VDA（XenDesktopおよびXenApp）を起動できません。

Citrix Receiver for Windows Desktop Lock

Dec 08, 2016

ユーザーが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を使用できます。 ユーザーに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 eceiver for Windows 4.2.x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 フラグを使っ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Single Sign-On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Citrix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 Download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。

ローカルアプリケーションアクセス

> **Important**
>
> ローカルアプリケーション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のドキュメントで「ローカルアプリケーションアクセスと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ケーションアクセス
  - 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、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 STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   コマンドの詳細については、「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」で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］>［Remoting client devices］>［Generic USB Remoting］の順に選択して、Existing USB DevicesとNew USB Devicesポリシーを有効にして構成します。
- ドライブマッピング — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client drive mapping］ポリシーを有効にして構成します。
- マイク — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client microphone］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。
   1. 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。
   2. 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。
   3. ［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）。
   4. ［Kerberos］を有効にします。

5. ［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。
6. 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。
7. 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。
   1. %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。
   2. ［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix Components］>［Citrix Receiver］>［User authentication］の順に展開します。
   3. ［Smart card authentication］を有効にします。
   4. ［Local user name and password］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。
   1. 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。
   2. 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://<デリバリーグループ名>」形式で追加します。
   3. 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、スマートカード取り出し時の動作がデスクトップ側で［ログオフを強制する］に設定されている場合、ユーザーデバイスのWindows側の設定にかかわらず、ユーザーデバイスからも強制的にログオフされます。 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+Delete - Ctrl+F1およびDesktop Viewerツールバーを介します。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+すべての文字キー

Windows 8

- Win+C - チャームを開きます。
- Win+Q - チャームを検索します。
- Win+H - チャームを共有します。
- Win+K - デバイスのチャーム。
- Win+I - 設定のチャーム。
- Win+Q - アプリを検索します。
- Win+W - 設定を検索します。

- Win+F - ファイルを検索します。

Windows 8のアプリ

- Win+Z - アプリのオプションを開きます。
- Win+. - アプリを左にスナップします。
- Win+Shift+. - アプリを右にスナップします。
- Ctrl+Tab - アプリ履歴を循環させます。
- Alt+F4 - アプリを閉じます。

Desktop

- 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。

Other

- 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をプレビューします。