Nov 19, 2015

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。また、Windows、Web、およびSaaS（Software as a Service）アプリケーションへのオンデマンドアクセスも提供されます。ユーザーは、Citrix StoreFrontで管理されるストア、または従来のWeb InterfaceのWebページからアプリケーションにアクセスします。

Receiver for Windows 4.1.200には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、および4.1.100で追加された修正に加えて、Microsoft Lync 2013 VDI Plug-in for Windowsに関連する修正が含まれています。また、HDX MediaStream、印刷、サーバーファーム管理、セッション接続、システム例外、およびユーザーエクスペリエンスに関する新しい修正も含まれています。これらの修正について詳しくは、CTX138197を参照してください。

CitrixのReceiver for Windows 4.1は、Windows 8.1およびWindows Server 2012 R2をサポートし、「Citrix Receiver 4.x - Issues Fixed in This Release」で説明されているような問題が修正されています。

Citrix Receiver for Windows 4.0で追加されたり強化されたりした機能は以下のとおりです。

- **XenDesktop 7機能のサポート** – Receiverでは、XenDesktop 7で提供されるWindows Mediaのクライアント側でのコンテンツ取得、マルチキャストのサポート、クライアントフォルダーのリダイレクト、ローカルアプリケーションアクセス、IPv6接続のサポートなどの多くの拡張がサポートされます。
- **StoreFront 2.0機能のサポート** - Receiverでは、StoreFront 2.0で提供されるスマートカード認証やIPv6接続のサポートなどの多くの拡張がサポートされます。
- **スマートカード認証の統合** – ReceiverでStoreFrontに接続するときのスマートカード認証として、以下の機能がサポートされます。
  - パススルー認証（シングルサインオン）。ドメインに属しているデバイスのユーザーは、スマートカード用の資格情報でReceiverにログオンします。この場合、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。
  - 2モード認証。ユーザーは、スマートカードを使用したりユーザー名とパスワードを入力したりできます。これにより、ユーザーの資格情報の有効期限が切れたり、スマートカードを所持していなかったりする場合でもログオンできるようになります。
  - 複数の証明書。ユーザーがスマートカードをリーダーに挿入すると、必要な証明書がReceiverにより選択され、複数のカードの複数の証明書を使用できます。
  - ダブルホップセッション。ユーザーは、仮想デスクトップ上にインストールされたReceiverを起動して、ほかのデリバリーグループのアプリケーションを使用できます。
  - スマートカード対応のアプリケーション。仮想デスクトップやアプリケーションのセッションで、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。

  詳しくは、「スマートカード認証の構成」を参照してください。システム要件、スマートカード展開の計画、および関連Citrixコンポーネントの構成については、最新のXenDesktopおよびStoreFrontのドキュメントを参照してください。

- **ユーザーエクスペリエンスの向上**
  - アップデートのインストールが完了したときにメッセージが表示されるようになりました。
  - セッション画面の保持機能により切断セッションの画面表示が保持されるときに、その画面が暗くなるようになりました。
- **H.264デコード** – XenDesktop 7でH.264エンコードが使用される場合、専門的なグラフィック処理アプリケーションをWANネットワークで使用する場合でも高いパフォーマンスが提供されます。

- **HDX Insightのサポート** – HDX Insightにより、EdgeSightのネットワーク分析およびパフォーマンス管理機能がDirectorに統合されます。これにより、XenDesktop管理者はReceiverのヘルス状態に関するパフォーマンス測定値をチェックできます。この機能を使用するために特別な構成を行う必要はありません。
- **COMポートおよびLPTポートのマッピング機能の変更**– XenDesktop 7環境では、COMポートおよびLPTポートのマッピングがデフォルトで無効になります。これらのポートのマッピングは、ポートリダイレクトのポリシーを使用して制御します。

Dec 24, 2015

Citrix Receiver for Windows 4.1.100との比較

Receiver for Windows 4.1.200には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトが有効な特定のWebサイトを参照すると、Internet Explorerが応答不能になる場合があります。

  この修正を有効にするには、VDA/HDX Mediastream for Flashの参照番号#LA4151の修正もインストールし、VDA/XenAppサーバーで以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  名前：SupportedUrlHeads
  種類：REG_MULTI_SZ
  データ：<個別の行での値ごと、null区切り：>
  http://
  https://
  file://

  [RcvrForWin4.1_14.1.200から][#LA5255]

- セッションで、Flashインテリジェントフォールバックを無効にすると、Internet Explorerが応答不能になる場合があります。

  [RcvrForWin4.1_14.1.200から][#LA5404]

印刷

- Citrixプリンタードライバー（UPD）では、バーコードフォントは印刷されません。Citrixプリンタードライバー（cpviewer.exe）またはバーコードプリンターを使用して、ドキュメントを印刷するときには、フォントが黒いスペースまたはランダム文字として表示されます。

  [RcvrForWin4.1_14.1.200から][#LC0141]

サーバー/ファームの管理

- ［ファイルリダイレクトの最大帯域幅］および［セッション全体の最大帯域幅］ポリシーが設定されている場合、セッションが予期せずに終了することがあります。

  この問題に対応するには、参照番号#LA5925の修正を含む更新をサーバーとReceiverの両方にインストールして、サーバーで以下のレジストリキーを設定する必要があります。

  - 以下のレジストリキーを作成します。
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    名前：DisableHighThroughput
    種類：DWORD
    値：1
  - 以下のレジストリキーを変更します。
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    名前：MaxNetCommands
    種類：DWORD
    値：小さい値に設定

  [RcvrForWin4.1_14.1.200から][#LA5925]

セッション/接続

- VDAへのネットワーク接続が切断されて、再接続された場合、マウスのクリックに失敗します。

  [RcvrForWin4.1_14.1.200から][#LA5743]

- COMポートリダイレクトが失敗して以下のエラーメッセージが表示されることがあります。

  「OpenPortでのエラー：COMポート「COM4」」

  [RcvrForWin4.1_14.1.200から][#LC0434]

- VDAに接続されているエンドポイントがスリープ状態から再開すると、VDAセッションでマウスとキーボードが動作しなくなります。

  [RcvrForWin4.1_14.1.200から][#LC0085]

- フォアグラウンドで実行中のWindowsセッションが、予期せずにフォアグラウンドのフォーカスを失う場合があります。

  [RcvrForWin4.1_14.1.200から][#LA5489]

システムの例外

- パススルーセッションのMedia Playerでビデオを再生すると、セッションが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.200から][#LC0553]

ユーザーエクスペリエンス

- フルスクリーンのシームレスなアプリケーションをいろいろな場所に移動させると、スムーズに移動せずにジッターの状態になり、境界上でデスクトップバックグラウンドが表示される場合があります。

  [RcvrForWin4.1_14.1.200から][#LC0696]

- ワイヤレスネットワークにおいて、セッションウィンドウが一時的に、無地の灰色に変わる場合があります。

[RcvrForWin4.1_14.1.200から][#LC0530]

- セッションの音質が［高音質（低パフォーマンス）］（［詳細構成］＞［プロパティ］＞［Client devices］＞［Resources］＞［Audio］＞［Sound quality］＞［高音質（低パフォーマンス）］）に設定されているポリシーが管理するユーザーセッションでは、音声は聞こえません。

  [RcvrForWin4.1_14.1.200から][#LC0329]

- RDSデスクトップセッションで、マルチメディアファイルをループ処理すると、1時間以上経過後にファイルがループ処理された後、音声とビデオストリームが停止します。

  [RcvrForWin4.1_14.1.200から][#LC0641]

- セッションの事前起動は、構成時ではなく、最初にReceiver for Windowsが起動されたときにのみ動作します。

  [RcvrForWin4.1_14.1.200から][#LC0701]

Citrix Receiver for Windows 4.1との比較

Receiver for Windows 4.1.100には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX 3D Pro

- H264コーデックおよびテキストトラッキングを無効にしてHDX 3D Proを使用すると、数時間の使用後に、wfica32.exeプロセスがCPUを100%消費している場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5554]

HDX MediaStream

- Internet Explorerなどの公開Webブラウザーを使用して、ストリーミングビデオを表示しようとすると、HDX MediaStrear Flashリダイレクトでの障害により、動作しない場合があります。

  この修正を有効にするには、以下のレジストリキーを設定します。

- *32ビットWindowsの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0
- *64ビットWindowsの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0

[RcvrForWin4.1_14.1.100から][#LA5278]

- HDX Mediastream for Flash Version 1.0（第1世代のFlashリダイレクト）を有効にすると、Adobe Flash Player 11.8以降のインストール時に、Microsoft Internet Explorerが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5421]

HDX Plug-n-Play

- Windows XP SP3にReceiver for Windows 4.0をインストールすると、ドッキングステーションのUSBポートがリダイレクトされなくなる場合があります。

  [RcvrForWin4.1_14.1.100から][#LA4582]

HDX RealTime

- HDX RealTime Webカメラビデオ圧縮リダイレクトが、Quarter Video Graphics Array（QVGA）ディスプレイ解像度（320x240）に対応できなくなり、wfica32.exeプロセスが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5232]

インストール、アンインストール、アップグレード

- インターネットに接続せずに、Receiver for Windowsの最新バージョンにアップグレードすると、以前のバージョンが完全にはアンインストールされず、最新バージョンのインストールに失敗します。

  [RcvrForWin4.1_14.1.100から][#LA4896]

印刷

- これは、ユニバーサルプリンタードライバーを構成するときに、両面印刷が失敗する問題に対応する修正で、代わりに手動で実行する必要があります。

  [RcvrForWin4.1_14.1.100から][#261552]

- Internet Explorer 9を使用して、HTMLドキュメントを印刷しようとすると、Citrix Print Viewer（cpviewer.exe）での出力が文字化けし、特定の種類のフォントで印刷される場合があります。

  [RcvrForWin4.1_14.1.100から][#LA3962]

サーバー/ファームの管理

- StoreFrontが認証不要なストアで構成されている場合、Receiver for Windowsの使用時に、アカウント検出が失敗すること

があります。

[RcvrForWin4.1_14.1.100から][#LC0004]

- この機能拡張では、優先テンプレートディレクトリを使用した、優先アプリケーションのショートカットの自動作成がサポートされています。これらのアプリケーションでは、既存の優先規則のほかに、Self Service Plug-inが、優先テンプレートディレクトリでショートカットを検索します。このショートカットが優先規則に一致している場合、このショートカットをユーザーの［スタート］メニューにコピーします。

  デフォルトでは、このディレクトリは以下のいずれかです。

  - %systemdrive%:\Program Files\Citrix\shortcuts
  - %systemdrive%:\Program Files (x86)\Citrix\shortcuts（ユーザーデバイスのインストールごと）および
  - %systemdrive%:\Users\<ユーザー名>\AppData\Local\Citrix\SelfService\shortcuts（ユーザーインストールごと）。

  デフォルトの優先テンプレートディレクトリの場所は、レジストリで指定できます。

  HKEY_LOCAL_MACHINE\Software\Citrix\DazzleまたはHKEY_CURRENT_USER\Software\Citrix\Dazzle
  名前：PreferTemplateDirectory
  種類：REG_SZ
  データ：任意のパス（たとえば、「%systemroot%:\Shortcuts」など）

  その後、アプリケーションがストアからサブスクリプションを解除されるか、または削除された場合、優先ディレクトリからコピーされたショートカットは削除されます。

  [RcvrForWin4.1_14.1.100から][#LC0005]

セッション/接続

- 仮想デスクトップセッション内でCitrix Receiverを使用すると、XenAppの公開アプリケーションの起動に失敗し、以下のエラーメッセージが表示されます。

  「このバージョンのCitrix Receiverは、選択された暗号化をサポートしていません。管理者に連絡してください。[エラー1029：無効なDLL読み込み]。」

  [RcvrForWin4.1_14.1.100から][#LA4743]

- Receiver for Windows 13.4 Cumulative Update 2において、シームレスなアプリケーションがフォーカスを持った場合、Alt+Tabキーを押してアクティブなウィンドウに切り替えたときに、言語バーの入力言語が変更されます。

  [RcvrForWin4.1_14.1.100から][#LA4963]

- Windows XPシステム上のタスクバーおよび［スタート］メニューのプロパティで、［Group similar taskbar buttons］オプションを選択した場合、アプリケーションの起動が遅くなることがあります。

  [RcvrForWin4.1_14.1.100から][#LA4191]

- Citrix Online Plug-in Version 12.2から、Citrix Receiver for Windows Version 3.xにアップグレードすると、外部Webサイトへのプロキシ接続が、NTLMプロキシ認証を有効にして起動することに失敗する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA3781]

- ユーザーデバイスが、Webカメラに接続されていない場合、Microsoft Lync 2010の公開インスタンスを起動すると、最終的な接続を確立してアプリケーションを起動する前に、アプリケーションが数回、接続と切断を繰り返すことがあります。これが発生するのは、Motorola Bluetoothパッケージなど、ほかのWebカメラがインストールされていないときに、Web

カメラをインストールしたアプリケーションをインストールする場合です。

[RcvrForWin4.1_14.1.100から][#LA4867]

- 公開アプリケーションまたはデスクトップを起動するときに、IPv4ネットワーク上でパススルー認証を使用すると、Kerberos認証が動作しない場合があります。このリリースではIPv4ネットワークの問題のみが修正されます。

  [RcvrForWin4.1_14.1.100から][#LA5026]

- この修正は、Microsoft Lync 2013 VDI Plug-in for Windowsに関連する音声またはビデオの問題に対応しています。この修正により、Lyncユーザーのユーザーエクスペリエンスが向上します。詳しくは、Knowledge CenterのCTX138408を参照してください。

  [RcvrForWin4.1_14.1.100から][#LA5314]

- CANcaseXL USBネットワークアダプターを仮想デスクトップにリダイレクトする場合、Windowsのデバイスマネージャーが正しく動作していないように見えます。このUSBデバイスは、Citrix USBリダイレクトドライバーをサポートしていません。適切に動作させるには、VDAで参照番号#LA5022の修正をインストールする必要があります。

  [RcvrForWin4.1_14.1.100から][#LA5022]

- この修正は、参照番号#LA1257の修正が適用されていますが、以下の問題に完全に対応することはできません。

  Desktop Viewerを無効にすると、フルスクリーンのクライアントセッションで、エンドポイントの画面解像度の変更に応じて、Virtual Desktop Agentの画面解像度を調整できません。

  [RcvrForWin4.1_14.1.100から][#LA4000]

- セッション画面の保持機能のタイムアウト時間を超えたときに、XenDesktopセッションへの接続が切断された場合、DesktopViewerは無制限に画面上に残ります。セッション画面の保持機能のタイムアウト後は、セッション自体が、コネクションセンターに正常に表示されなくなります。

  [RcvrForWin4.1_14.1.100から][#LA4856]

システムの例外

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [RcvrForWin4.1_14.1.100から][#LA3964]

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [RcvrForWin4.1_14.1.100から][#LA4695]

- XenApp 6.5デスクトップからXenApp 4.5公開アプリケーションへのパススルーセッションの起動時に、wfica32.exeプロセスが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5193]

- マルチストリームポリシーが有効な場合、COMポートにアクセスすると、アプリケーションが応答不能になることがあります。

[RcvrForWin4.1_14.1.100から][#LA5543]

- ダブルホップのシナリオでは、Microsoft OutlookまたはCommunicatorを起動すると、Receiver for Windowsが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA4813]

ユーザーエクスペリエンス

- XenApp for Unixでホストされているセッションに接続または再接続すると、90秒間画面の更新が行われません。

  [RcvrForWin4.1_14.1.100から][#LA5244]

ユーザーインターフェイス

- Online Plug-in Version 12.1で導入された変更により、シームレスな接続で接続の進行状況バーの表示が遅延しています。ただし、低速なサーバーに接続するセッションでは、この動作は必ずしも適切であるとは限りません。この機能拡張では、遅延時間を構成できる、以下のレジストリキーをサポートしています。

  32ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：NotificationDelay
  種類：REG_DWORD
  データ：<ミリ秒単位の遅延時間>

  64ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  名前：NotificationDelay
  種類：REG_DWORD
  データ：<ミリ秒単位の遅延時間>

  [RcvrForWin4.1_14.1.100から][#LA0678]

- デスクトップの配色を、デフォルトの青色からほかの色（たとえば、オリーブグリーンやシルバーなど）に変更すると（**[デスクトップ]** > **[プロパティ]** > **[デザイン]** タブ> **[Color scheme]**）、Self-service Plug-inのテキストとバックグラウンドの色が同じになり、メニュー項目を読み取ることができなくなります。

  [RcvrForWin4.1_14.1.100から][#LA5121]

その他

- メールによる検出を使用するときに、DNS側で作成されたSRVレコードに443以外のポートが含まれている場合、ReceiverはSRVレコードで指定されたポートを無視し、引き続きポート443を使用して、Access/NetScaler Gateway URLに接続します。

  [RcvrForWin4.1_14.1.100から][#LA4491]

Citrix Receiver for Windows 4.1との比較

Receiver for Windows 4.1.2には、Receiver for Windows 4.0、4.0.1、4.1に含まれていたすべての修正に加えて、以下の新しい

修正が含まれています。

Microsoft Lync 2013 VDI Plug-in	インストール、アンインストール、アップグレード

Microsoft Lync 2013 VDI Plug-in

- Lyncの会話ウィンドウをセカンダリモニターに移動させると、ビデオが表示されなくなることがあります。

  [#LA5314、#399447]

- ホワイトボードウィンドウを別のユーザーに移動させると、そのユーザーのビデオ映像が会話ウィンドウに表示されなくなることがあります。

  [#LA5314、#399465]

- Receiverが、マルチパーティビデオ呼び出し時またはビデオ会議の終了時に、予期せずに終了する場合があります。

  [#LA5314、#426035]

- 一部のクライアントデバイスでは、フルスクリーンVDAモードのビデオ呼び出しで、ビデオが断続的に使用できなくなります。

  [#LA5314、#418675]

- ビデオ会議ウィンドウを移動すると、ビデオが歪む場合があります。

  [#LA5314、#419898]

インストール、アンインストール、アップグレード

- インターネットに接続せずに、Receiver for Windowsの最新バージョンにアップグレードすると、以前のバージョンが完全にはアンインストールされず、最新バージョンのインストールに失敗します。

  [#LA4896]

Citrix Receiver for Windows 4.0.1との比較

Receiver for Windows 4.1には、Receiver for Windows 4.0、4.0.1に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX MediaStream Flashリダイレクト	印刷
HDX MediaStream Windows Mediaリダイレクト	セッション/接続
HDX Plug-n-Play	システムの例外
インストール、アンインストール、アップグレード	ユーザーエクスペリエンス

キーボード | 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 | その他
ログオン/認証

HDX MediaStream Flashリダイレクト

- いくつかのマルチメディアファイルを、http://www.youtube.com/でHDX MediaStream Flashリダイレクトを有効にして次々に再生すると、PseudoContainer2.exeプロセスが予期せずに終了する場合があります。

  [#LA3846]

HDX MediaStream Windows Mediaリダイレクト

- Receiver for Windows Version 3.4で、HDX MediaStream Windows Mediaリダイレクトを有効にすると、マルチメディアファイルがストリーミングを開始するまでに、最大10秒の遅延が発生する場合があります。

  [#LA4141]

HDX Plug-n-Play

- Desktop Viewer内で［デバイス］をクリックし、HDX Plug-n-PlayのUSBデバイスリダイレクトを使用して削除するUSBデバイスを選択すると、Desktop Viewerが応答不能になる場合があります。

  [#LA3348]

インストール、アンインストール、アップグレード

- 管理者以外のユーザーが、Receiver for Windowsをアップグレードしようとしたとき、Receiverが管理者によってインストールされていた場合、Receiverが部分的にしかインストールされないことがあります。

  この修正により、管理者以外のユーザーが、管理者がインストールしたReceiverをアップグレードしようとしたときには、エラーメッセージを受信し、インストールプロセスが終了されます。

  [#LA3425]

キーボード

- Receiver for Windows Version 3.3を使用しているときに、Altキーを押すと、キーがダウン状態のままになる場合があります。結果として、その後に「E」キーを押すと、Windowsエクスプローラーを起動できます。

  [#LA3288]

- フルスクリーンモードでWindowsキーを押して、Desktop Viewerのツールバーをクリックすると、キーがダウン状態のままになる場合があります。結果として、その後にEキーを押すと、Windowsエクスプローラーを起動できます。

  [#LA3349]

- この修正により、ICAセッションにおいて、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。この修正により、新しいパラメーターが導入されています。このパラメーターは、クライアントとサーバーの間でキーボードのLEDの状態を強制的に同期させます。このオプションを有効にするには、ローカルユーザープロファイルのある場所のappsrv.iniファイル、または対応するWeb Interfaceサイトのdefault.icaファイルの[WFClient]セ

クションに「KeyboardForceLEDUpdate = On」を追加します。

[#LA3682]

- この修正により、クライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある、LED同期の問題に対応しています。

  [#LA4293]

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が有効な場合、Desktop Viewerをクリックすると、クライアントのローカルタスクバーが不必要に表示されることがあります。

  [#LA3049]

ログオン/認証

- Windows Server 2008 R2にXenDesktop 7 VDAをインストールすると、パススルー認証が動作しないことがあります。この問題は、ssonsvr.exeプロセスが開始できないことが原因で発生します。

  [#LA4685]

印刷

- 複数のAdobe Acrobat印刷ジョブをセッションプリンターに送信したとき、ランダムなページまたは印刷ジョブ全体が失われる場合があります。

  [#LA3643]

- セッションプリンター列挙に、長い時間を要することがあります。

  [#LA3951]

セッション/接続

- クライアントデバイスが、長時間アクティブなXenDesktopセッションを実行中で、スリープまたは休止状態のときに再開すると、セッションが正常に再接続されず、再接続フェーズでスタックしてしまい、セッションウィンドウを手動で閉じることが必要になる場合があります。

  この修正は、クライアントデバイスを再開するときに、再接続に失敗した場合、セッションウィンドウを正常に閉じる問題に対応しています。

  [#LA2748]

- 公開アプリケーションをシームレスモードで起動するときに、進行状況バーウィンドウがバックグラウンドに残されたままになります。

  修正を有効にするには、クライアント側で以下のレジストリキーを設定します。

  - *Windows 32ビットシステムの場合：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名前：ForegroundProgressBar
    種類：DWORD
    データ：1

- *Windows 64ビットシステムの場合：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名前：ForegroundProgressBar
  種類：DWORD
  データ：1

[#LA3491]

- Desktop Lockとともに使用したReceiverが、ハードウェア障害が発生するたびに、またはVMがハイパーバイザーから強制的にシャットダウンさせられた場合に灰色の画面を表示します。

  [#LA3499]

- クライアントデバイスで、タスクバーでのグループ化を有効にすると、wfica32.exe内のTaskbarGrpXpVista.dllが、クライアントデバイスに対して、セッションで実行中の公開アプリケーションに関する情報を不必要に照会します。たとえば、cmd.exeの公開インスタンスを実行中に、TaskbarGrpXpVista.dllは、実行可能ファイルに関する情報をC:\windows\system32\cmd.exeに照会します。公開アプリケーションがリモート共有から実行されているシナリオの場合、これにより、不適切な帯域幅の消費を引き起こすことがあります。

  [#LA3661]

- GPO設定がタスクバーでのグループ化を回避するように指定されている場合、Windows XPおよびVistaクライアントデバイス上のタスクバーアイコンをクリックすると、関連するウィンドウへのフォーカスの切り替えに失敗します。

  [#LA3889]

- ［Citrix Receiver – Device Access］ダイアログボックスが表示されているときに、Desktop Viewerツールバーの［Devices］ボタンをクリックすると、Receiverが応答不能になる場合があります。このダイアログボックスは、デバイスのアクセス設定が、デフォルトの［何もしない］ではなく、［毎回確認する］に構成されている場合に表示されます。

  [#LA3899]

- Desktop Viewer（CDViewer.exe）およびwfica32.exeプロセスが、仮想デスクトップセッションに再接続中に、予期せずに終了する場合があります。

  [#LA3944]

- この修正により、IsReconnectInProgress() APIが、Citrix Fast Connect 2.0に統合されています。この機能は、クライアントの自動接続機能が有効である場合に、再接続プロセスが進行中であるかどうかを判別します。

  [#LA4080]

- この修正により、パススルーアプリケーションが再接続できるようになり、パススルーアプリケーションのワークスペースコントロールが有効になります。

  この修正を有効にするには、以下のレジストリキーを設定する必要があります。

  パススルーモードでワークスペースコントロールを有効にするには、以下のように設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
  名前：ForceEnableWSC
  種類：DWORD
  データ = 1

パススルーアプリケーションの再接続を有効にするには、以下のように設定します。

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
名前：BypassPassThruMode
種類：DWORD
データ = 1

注：この修正は、以下の条件でのみ機能します。

- 同一のXenApp Servicesサイトまたはファーム内で、2つまたは複数の接続ホップが実行できない場合があります。つまり、エンドポイントのReceiverが、XenApp ServicesサイトAで公開されているXenDesktop VDAに接続できるときに、そのVDA上のパススルークライアントは、*別の*XenApp ServicesサイトBの公開アプリケーションまたはデスクトップに接続できます。
- 2番目の接続ホップは、XenAppターミナルセッションにする必要があります。XenDesktop VDAにすることはできません。

[#LA4206]

- クライアント画面のパーセンテージが奇数（偶数ではない）として公開されているデスクトップ（たとえば、95%）で、リモートアシスタンスソフトウェアを使用しているときに、リモートアシスタンスセッションが歪んでいるように見える場合があります。

  [#LA4313]

- この互換性機能拡張により、別のUSBデバイスへのHDX Plug-n-Play USBデバイスリダイレクトが拡張されます。

  [#LA4335]

- wfcrun32.exeのデッドロックにより、新規セッションが正常に起動しないことがあります。

  [#LA4344]

- Citrixクイックアクセスバーツール、または「HTTPBrowserAddress=ServerName_Or_IP:Port」（たとえば、「HTTPBrowserAddress=192.168.1.10:8080」）と指定した静的なICAファイルを使用して、XenAppサーバーにアクセスしようとすると、失敗する場合があります。

  [#LA4585]

システムの例外

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [#LA3412]

- wfica32.exeプロセスで、アクセス違反が発生して、予期せずに終了する場合があります。

  [#LA3639]

- wfica32.exeプロセスが、予期せずに終了する場合があります。

  [#LA4208]

ユーザーエクスペリエンス

- この修正では、Receiver 4.0をStoreFrontとともに使用しているときに、不必要なログオンプロンプトが表示されるのを回避します。

  [#LA4652]

ユーザーインターフェイス

- 公開アプリケーションのアプリケーション名と表示名の間に不一致が存在する場合、アプリケーションの起動に失敗します。

  [#LA3891]

その他

- このリリースには、SSLSDKの最新バージョンであるVersion 12.1.13が含まれています。

  [#LA3804]

- この修正では、一部の展開における、Receiver for WindowsのTerminateUser関数の機能が改善されています。

  [#LA3881]

Citrix Receiver for Windows 4.0との比較

Receiver for Windows 4.0.1には、Receiver for Windows 4.0に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- この修正では、Receiver 4.0をStoreFrontとともに使用しているときに、不必要なログオンプロンプトが表示されるのを回避します。

  [#LA4652]

Citrix Receiver for Windows 3.4との比較

Receiver for Windows 4.0には、Citrix Receiver for Windows 3.4と比較して、以下の修正が含まれています。

HDX MediaStream Flashリダイレクト

HDX Plug-n-Play

インストール、アンインストール、アップグレード

キーボード

印刷

シームレスウィンドウ

セッション/接続

システムの例外

ユーザーエクスペリエンス

ユーザーインターフェイス

その他

HDX MediaStream Flashリダイレクト

- ビデオファイルのレンダリング中に、ビデオウィンドウのすべてまたは一部を画面外に移動させると、画面上に暗い領域が残されたままになることがあります。この暗い領域は、ビデオウィンドウを元に戻した後でも残されたままです。

  [#LA0599]

- **重要**：クライアントデバイスにこの修正を適用する前に、Knowledge CenterのCTX126817を参照して、Dynamic Blacklist機能がクライアント側のFlashリダイレクトに与える影響に関する重要な情報を確認してください。

  サーバー上で *[サーバー側のコンテンツの取得を有効にする]* ポリシーを有効にし、クライアント上でFlashリダイレクトポリシーに *[Flashサーバー側でのコンテンツ取得URLリスト]* 設定を構成しているシナリオでは、コンテンツへのURLに2バイト文字/Unicode文字（アジア言語では一般的です）が含まれている場合、Flashコンテンツの再生に失敗します。

  この修正自体を有効にするには、参照番号#LA1621の修正を含むクライアントHotfixと以下のHotfixの両方をインストールする必要があります。

  - *XenAppの場合*：参照番号#LA1621の修正を含むHDX FlashのHotfix
  - *XenDesktの場合*：参照番号#LA1621の修正を含むVirtual Desktop AgentのHotfix

  注：この修正では、クライアントとサーバーの両方にインストールされる、対応する言語コードページも必要になります。このコードページは、Windowsオペレーティングシステムでは、デフォルトでインストールされます。たとえば、Windows 7の日本語版配布では、デフォルトで、日本語コードページがインストールされます。ただし、Windows 7の英語版配布で日本語文字を含むURLを使用する場合、日本語コードページを明示的にインストールする必要があります。サーバー側コンテンツの取得が有効なとき、URLはクライアントからサーバーに転送されるので、これはクライアントとサーバーの両方に適用されます。

  [#LA1621]

- ボタンのクリックなど、Flashコンテンツでの特定のユーザー操作により、Pseudocontainer2.exeが予期せずに終了する場合があります。

  [#LA1948]

- クライアント側でのコンテンツリダイレクトが、特定の種類のFlashコンテンツで失敗し、サーバー側のレンダリングに戻る場合があります。以下のようなケースが含まれます。

  1. Flashコンテンツが、存在しないまたは見つけられない別のFlashファイルのダウンロードを試みた場合
  2. Adobe Captiveで作成されたFlashコンテンツが、クライアント側のコンテンツリダイレクト機能の論理チェックに失敗した場合
  3. Flashコンテンツが、サポートされていないサーバーへのリモートインターフェイスに対して、クライアント側のコンテンツリダイレクト機能を実行した場合
  4. URLがServerContentFetching URLブラックリストで構成されている場合でも、クライアントがFlashコンテンツの取得を試みた場合

  この修正を有効にするには、参照番号#LA2198の修正を含む、HDX FlashとReceiver for Windows Hotfixの両方をインストールする必要があります。上記の問題#1でこの修正を有効にするには、クライアント上で以下のレジストリキーも設定する必要があります。

  - *32ビットWindowsの場合：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名前：FallbackIfFlashNotExist

種類：REG_DWORD
データ：0

- *64ビットWindowsの場合：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0

[#LA2198]

- フォーカスをFlashウィンドウ（シームレスウィンドウを実行中のWebブラウザーの子ウィンドウ）からローカルウィンドウに切り替え、またフォーカスをシームレスなブラウザーウィンドウのアドレスバーに戻したときに、ブラウザーのアドスバーへの入力に失敗する場合があります。

  [#LA2685]

- 重要：クライアントデバイスにこの修正を適用する前に、Knowledge CenterのCTX126817を参照して、Dynamic Blacklist機能がクライアント側のFlashリダイレクトに与える影響に関する重要な情報を確認してください。

  HDX MediaStream Flashリダイレクト機能が、Dailymotionビデオ（http://www.dailymotion.com）ではエラーが発生して、動作に失敗することがあります。この問題が発生するのは、クライアントとサーバーが、別の地理的場所に配置されている場合です。

  この修正を有効にするには、以下のレジストリキーを作成する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
  名前：DisableRegionFiltering
  種類：REG_DWORD
  データ：1

  [#LA3134]

HDX Plug-n-Play

- この機能拡張では、デフォルトのUSBリダイレクト動作が、以下のように変更されます。
  - Desktop Viewerが有効な場合、ユーザーはUSBデバイスを手動でリダイレクトできます。
  - Desktop Viewerが有効ではない場合、USBデバイスは自動的にリダイレクトされます。

  [#LA0108]

- 特定のUSBデバイスを、仮想デスクトップセッションにマップできなかった場合、エンドポイントを再起動するまで、デバイスマネージャーにデバイスが表示されません。

  [#LA0954]

- Desktop Viewer内で［デバイス］をクリックし、HDX Plug-n-PlayのUSBデバイスリダイレクトを使用して削除するUSBデバイスを選択すると、Desktop Viewerが応答不能になる場合があります。

  [#LA3348]

インストール、アンインストール、アップグレード

- Receiver 3.*x*へのアップグレード後、公開アプリケーションを起動することができず、以下のエラーメッセージが表示されます。

「このバージョンのCitrix Receiverは、選択された暗号化をサポートしていません。管理者に連絡してください。エラー1046：仮想ドライバーが読み込まれていません。」

[#LA3120]

キーボード

- Desktop Viewerの［ホーム］をクリックして、仮想デスクトップセッションを最小化すると、セッションが切断されるまで、エンドポイントでTabキーが断続的に動作を停止する場合があります。

  [#LA2925]

- Receiver for Windows　Version 3.0の時点では、KeyboardTimerの以下の設定値は動作しません。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard。この修正により、機能が再度有効になります。

  [#LA2949]

- この修正により、フォアグラウンドで実行中のパススルーセッションのクライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。

  [#LA3288]

- この修正により、バックグラウンドで実行中のパススルーセッションのクライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。

  [#LA3310]

印刷

- **［クライアント設定］**タブで **［ローカルプリンター設定］**をクリックして、UPDプリンターの **［プロパティ］**シートを開きます。次に、設定ダイアログボックスを閉じると、 **［プロパティ］**シートが応答不能になることがあります。

  [#259485]

シームレスウィンドウ

- コネクションセンターまたはWeb Interfaceを使用して、データを保存せずにシームレスなセッションからログオフすると、画面が黒くなり、以下のようなメッセージが表示されます。

  「プログラムを閉じる必要があります。2つのオプション［ログオフを強制する］または［キャンセル］から選択してください。」このときに、［キャンセル］オプションが動作しません。

  この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。［キャンセル］ボタンの利用後は、これ以上パフォーマンスを低下させないために、データを保存して、セッションからログアウトすることをお勧めします。

  [#LA0318]

セッション/接続

- 仮想デスクトップセッションから切断して再接続すると、セッション内からの音声の記録に失敗することがあります。この問題を解決するには、サーバー側にも参照番号#LA0821に対する修正をインストールする必要があります。

  [#LA0821]

- クライアントセッションでファイルの転送に要する時間が、RDPセッションの場合より長くなることがあります。

  この問題を解決するには、サーバー側にも参照番号#LA1263に対する修正をインストールする必要があります。

  [#LA1263]

- 特定の条件下では、仮想デスクトップセッションの解像度を変更した後で、セッションが予期せずに切断されると（ネットワーク障害などによる）、再接続した後にセッション解像度が予期していた設定とは異なっていることがあります。

  [#LA1377]

- シリアルポートバーコードスキャナーは、512バイトを越えるサイズのラベルデータを処理できません。この修正を有効にするには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：CommBufferSize
  種類：REG_DWORD
  データ：512（最小）～2048（最大）の範囲の値

  [#LA1695]

- Knowledge CenterのCTX131577の説明に従って、Network List ServiceまたはNetwork Location Awarenessサービスを無効にすると、Online Plug-in Version 12.3が切断されます。

  [#LA2024]

- 狭帯域幅の接続を介して、UNCパスに公開されているシームレスなアプリケーションを起動しようとすると、完了するまで2分を超えてしまう場合があります。

  [#LA2170]

- Ctrl+Shiftキーをクリックして、シームレスなセッションの入力方法を起動させると、クライアント側のローカルの入力方法も変更されることがあります。この問題を回避するには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：Showlocallanguagebar
  種類：REG_DWORD
  データ：1 <*ローカル言語バーを表示する*>、0 <*ローカル言語バーを非表示にする*>

  [#LA2180]

- 自動クライアントリダイレクトを有効にすると、休止状態を選択した後、クライアントが自動的に閉じられたときに、再接続に失敗することがあります。

  この修正により、システムはUSBデバイスリダイレクトにより、一時停止するかまたは休止状態モードに移行し、システムがスタンバイモードから復帰した後に、自動的に再接続することができます。

  [#LA3061]

- Citrix Receiver for Windows 3.xで、ICA圧縮が「OFF」に設定されている場合、公開アプリケーションが起動に失敗することがあります。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off。

[#LA3072]

- マルチモニター環境では、フルスクリーンモードでディスプレイを2番目のモニターに切り替えている間、Desktop Viewe ツールバーが表示されなくなることがあります。

  [#LA3083]

- 2つのモニターがVirtual Desktop Agentに接続されており、プライマリモニターがラップトップであるデュアルモニター構成では、ラップトップのディスプレイをオフにしてまたオンに戻すと、その後のセッションはプライマリモニターのディスプレイのみで行われます。

  [#LA3202]

- Internet Explorer 8を実行中のWindows XPワークステーションで、Receiver for Windows Version 3.3またはVersion 3.4 Cumulative Update 1を使用すると、Web Interfaceから最初のアプリケーションの起動に失敗することがあります。

  [#LA3234]

- Receiver for Linuxを使用して、切断されている仮想デスクトップセッションに再接続しようとすると、コンソールおよびXenDesktopの両方のセッションが応答不能になることがあります（［ようこそ］画面でのスタック）。この問題が発生するのは、Virtual Desktop AgentでWDDMドライバーが有効にされており、セッション内で別の仮想デスクトップセッションが実行されている場合です。

  [#LA3241]

- Windows 7でクライアントの［地域と言語のオプション］が［Kazakh（Kazakhstan）］に設定されている場合、Receiver for Windows Version 3.4が起動に失敗することがあります。

  [#LA3517]

システムの例外

- EdgeSight for Load Testingが展開されている環境では、wfica32.exeプロセスが予期せずに終了する場合があります。

  [#LA0289]

- HP LoadRunnerが展開されている環境では、wfcrun.exeプロセスが予期せずに終了する場合があります。

  [#LA0859]

- オーディオポリシーが高品位オーディオに設定されている場合、公開デスクトップの［サウンド］コントロールパネルでランダムにサンプルサウンドファイルを再生すると、wfica32.exeプロセスが予期せずに終了することがあります。

  [#LA1000]

- Microsoft Excel 2007スプレッドシートが開かれている状態で、Web Interfaceサイトからセッションを切断すると、Online Plug-in Version 12.3が予期せずに終了する場合があります。

  [#LA2274]

- ローカルアプリケーションアクセスが有効で、Virtual Desktop Agentで法的通知が構成されている場合、Virtual Desktop Agentへの接続に失敗することがあります。

  [#LA2351]

- セッションへの再接続時に、Pnamain.exeプロセスが予期せずに終了する場合があります。

  [#LA2704]

- 単一モニターで実行中のセッションでは、Aeroが有効なWindowsクライアントデバイスが予期せずに切断される場合があります。この問題が発生するのは、動的ウィンドウプレビュー機能の一部として、クライアントにプレビューが送信された場合です。その時点で、twi3.dllスレッドがWinlogon.exeプロセスを終了し、次にセッションが切断されることがあります。

  この問題を解決するには、サーバー側にも参照番号#LA2858に対する修正をインストールする必要があります。

  [#LA2858]

- wfica32.exeプロセスが、予期せずに終了する場合があります。この問題は、無効なメモリ逆参照によるものです。

  [#LA2860]

- 特定のダブルホップシナリオでの印刷中に、以下のエラーメッセージが表示され、Wfica32.exeプロセスが予期せずに終了します。「Citrix HDX Engineが動作を停止しました。」この問題は、ポート名の長さが260文字を超えていることによるものです。

  この問題に対応するには、参照番号#LA3009の修正を含む、サーバーHotfixおよびReceiver Hotfixの両方をインストールする必要があります（XA650R01W2K8R2X64056; RcvrForWin3.3_13.3.104、またはその置き換えHotfix）。

  [#LA3009]

- Citrix Receiverが、selfserviceplugin.exeプロセスの複数のインスタンスを生成し、システムのメモリが不足することがあります。

  [#LA3460]

- ログオフ時、Desktop Viewerが予期せずに終了する場合があります。

  [#LA3567]

- Online Plug-inをパススルークライアントとして使用しているときに、PNMain.exeが予期せずに終了する場合があります。

  [#LA0785]

ユーザーエクスペリエンス

- USBリダイレクトの使用時、数時間後にUSB SpaceMouseデバイスが、仮想デスクトップセッションに表示されなくなることがあります。

  [#LA2256]

- Receiver for Windows Version 3.4のこの機能拡張では、ユーザーがネットワーク接続を切り替えたときに表示される、VPN ログインに対する以下の認証メッセージの表示を抑制できます。

  メッセージが表示されないようにするには、以下のレジストリキーを作成します。

  - *32ビットWindowsの場合*：
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    名前：AutoSecureConnection
    種類：REG_DWORD

値：0（VPnプロントを無効化）

- *64ビットWindowsの場合*：
  HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
  名前：AutoSecureConnection
  種類：REG_DWORD
  値：0（VPnプロントを無効化）

[#LA3772]

ユーザーインターフェイス

- この修正では、具体的には、Desktop Viewerツールバーの［ホームデスクトップ］アイコンタイトルの韓国語表示を修正します。

  [#232198]

- エンドポイントでデスクトップグループショートカットの実行中に表示される、認証ダイアログボックス**[キャンセル]**をクリックすると、以下の不正確で不適切なエラーメッセージが表示されます。

  参照されているアプリケーションが見つかりません。ネットワーク接続を確認してください

  [#259081]

- 最大化されたセッションウィンドウで、［セッション/接続］画面が表示されなくなった**後**、USBMultiInsertDialogueダイアログボックスの*［接続］*をクリックすると、Desktop Viewerツールバーが、適切に表示されない場合があります。

  [#260390]

- icaclient.admの［クライアント側ドライブのマッピング］の［ヘルプ］トピックでは、「ポリシーはユーザーの選択を上書きしない」と誤って記述されています。ポリシーはユーザーの選択を上書きします。

  [#LA0398]

- 特定のカスタムアプリケーションでは、SpeedScreen機能のローカルテキストエコー編集ボックスに入力中、黒いバーが表示されます。

  [#LA0544]

- Merchandising Serverからの最初の配信に成功した後、「ようこそ」または補完メッセージが表示されません。

  [#LA2277]

- 公開アプリケーションの起動時に、Windowsタスクバーの通知領域のTivoli Access Manager for Enterprise Single Sign-On（TAM ESSO）アイコンが、予期せずに表示されなくなる場合があります。

  [#LA3190]

- ローカルタスクバーが、自動的に隠すように設定されており、その後に画面のデフォルトの場所から上部、左側、または右側に移動された場合は、アクセスできなくなります。

  [#LA3400]

その他

- UDPオーディオストリームの再生時に、wfica32.exeプロセスのハンドル数が大幅に増加する場合があります。

[#LA3094]

- この修正により、Receiver for Web 3.3ではProgram Neighborhood Web Interface 5.4サイトは1つであるという制限が削除されます。

  [#LA3142]

Nov 19, 2015

ここでは、次の内容について説明します。

- インストールおよびアップグレードに関する問題
- 一般的な問題
- 既知の問題 - デスクトップ接続
- Microsoft Lync 2013 VDI Plug-inの問題

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。

- citrix.comでReceiver for Windows 3.4をアップグレードする場合、一部の保留アップデートが完了しない場合があります。この問題を回避するには、Receiverを手作業でアップグレードしてください。[#396558]
- citrix.comでReceiver for Windows 3.3にアップグレードできないという問題があります。この問題を回避するには、Receiverを手作業でアップグレードしてください。[#393294]
- .NET 3.5がインストールされていないWindows 8コンピューターでは、Receiver for Windowsが正しくインストールされません。この場合、Receiver for Windowsのインストール時に.NET 3.5のダウンロードを確認するメッセージが表示されます。.NETをダウンロードしてインストールするとReceiverのインストールが開始されますが、正しく完了しません。Receiverをインストールするには、コントロールパネルの［プログラムと機能］でReceiverをアンインストールし、再度インストールしてください。[#352779]
- Windows 8コンピュータで.NET 3.5がインストールされていない、またはこれが有効になっていない場合、Receiverのインストール時に.NET 3.5のインストールを確認するメッセージが表示されます。ここでインストールをキャンセルすると、Receiverを正しくアンインストールできなくなります。この問題が発生した場合は、.NET 3.5をインストールするか有効にしてからReceiverをアンインストールしてください。Windows 8コンピューターで.NET 3.5を有効にするには、［コントロールパネル］、［プログラムと機能］、［Windowsの機能の有効化または無効化］の順に選択して［.Net Framework 3.5］を選択します。[#354996]
- Merchandising Serverを使用してReceiverをWindows 8コンピューター上にインストールする場合、タスクバーにReceiverアイコンが表示されなくなることがあります。この問題を解決するには、ユーザーデバイスを再起動してください。または、Receiverのインストール先フォルダーからReceiver.exeを起動してください。[#381529]
- Windows 8コンピューターにReceiverをサイレントインストールする場合、Receiverのインストールに成功しても無制限に待機状態になることがあります。この問題を避けるため、PowerShellコマンドラインで-waitパラメーターを使用しないでください。[#354627]
- Merchandising Serverを使用してReceiverをWindows 8コンピューター上にインストールする場合、タスクバーにReceiverアイコンが表示されなくなることがあります。この問題を解決するには、Receiverのインストール先フォルダーからReceiver.exeを起動してください。[#381529]
- App Controller 2.0環境で、ログオン済みのユーザーの状態がReceiverに反映されない場合があります。この問題が発生すると、Receiverメニューに［ログオン］コマンドが表示され、Receiverウィンドウにユーザー名が表示されません。この場合、Receiverのほかの機能は正しく動作します。この問題を回避するには、ユーザーがReceiverをアップグレードする前に、App Controller 2.5にアップグレードしてください。[#353789]
- Merchandising Serverによる展開環境では、Receiver Updater for Windows 3.4にアップグレードしないとReceiver for Windowsをアンインストールできなくなります。さらに、Receiverの再起動後に表示されるメッセージに、ユーザーが［後

で再起動］をクリックするように指示してください。ユーザーが［再起動］をクリックすると、Receiverがアンインストールされません。[#346341]

- 以前のバージョンのOnline Plug-inを使用するユーザーが Internet Explorer 10でReceiver for Webサイトに接続する場合、最新のReceiver for Windowsにアップグレードできません。この問題を回避するには、ほかのWebブラウザーを使用するか、Online Plug-inをアンインストールしておく必要があります。[#393929]
- ユーザーがコントロールパネルを使ってプラグインをアンインストールしてコンピューターを再起動すると、Receiverアイコンを右クリックして［バージョン情報］を選択し［詳細情報］をクリックしたときに表示される一覧がプラグインにより引き続き表示されます。この問題は、ReceiverをCitrix.comまたは自分のダウンロードサイトからインストールした場合にのみ発生します。[#320277]
- 64ビット版のWindows XP上でプラグインを更新すると失敗します。この問題を回避するには、http://support.microsoft.com/kb/968730/en-usからHotfixを入手してインストールしてください。[#328081]
- Receiver for WindowsをWindows XP Embeddedシンクライアントデバイスにインストールする場合は、事前にデバイスのRAMディスク制限を100MBに増やしてください。[#266384]

- サポートされない機能については、『Citrix Receiver feature matrix（英文）』を参照してください。
- Receiverでアプリケーションを起動するときに、スマートカード認証用のダイアログボックスにフォーカスが設定されず、認証できなくなることがありました。この問題は、シングルサインオンが無効な場合に発生します。ユーザーは、セッションを再起動してこの問題を解決する必要があります。この問題を回避するには、以下のレジストリキーでTWISeamlessFlagを1に設定します。[#379878]
  32ビットシステム：HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

  64ビットシステム：HKEY_LOCAL_MACHINE\Software\ Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\WFClient

- SaaSアプリケーションのアイコンが48x48よりも大きい場合、Receiverでサブスクライブできません。[#353794]
- ［バージョン情報］ダイアログボックスの［更新］をクリックして［詳細設定］を展開すると、「Receiverのリセット］リンクが表示されなくなります。この問題を解決するには、［バージョン情報］ダイアログボックスを閉じてから再度開いてください。[#383110]
- Windows Server 2008 R2が動作するサーバー上のReceiverを工場出荷時の設定にリセットすると、［スタート］メニューからReceiverを起動できなくなり、Receiverメニューに［開く］コマンドが表示されなくなります。この問題を解決するには、設定をリセットした後でReceiverを再起動してください（Receiverの設定をリセットするには、Receiverアイコンを右クリックして［バージョン情報］を選択し、［詳細設定］の［Receiverのリセット］を選択します）。[#355092]
- 複数のストアを構成すると、Receiverで適切なゲートウェイに接続できなくなることがあります。この場合、不正なアプリケーションがユーザーに提供されます。この問題を回避するには、単一のストアのみを構成してください。[#263165]
- ReceiverでWeb Interfaceサイトに接続する場合、Receiverでの自動再接続に問題が生じることがあります。この問題は、default.icaファイルにSessionReliabilityTTL=60というエントリがあると発生します。この問題を解決するには、default.icaファイルを編集してSessionReliabilityTTLを削除する（これによりデフォルトの180が適用されます）か、SessionReliabilityTTL=180に変更してください。[#373506]
- Web Interface接続でユーザーがアプリケーションを起動した場合に、コネクションセンターにセッションが列挙されなくなることがあります。[#261177]
- Access Gateway用にフィルター設定された仮想アプリケーションをユーザーが起動すると、ほかの仮想アプリケーションが起動しなくなります。[#263003]
- タッチキーボードをサポートするWindows 8デバイスで仮想アプリケーションに日本語などのアジア言語を入力するには、ローカルのIME（Input Method Editor）を有効にする必要があります。これを行うには、コマンドプロンプトで以下のコマンドを実行してください。[#350071]

32ビットシステム：%PROGRAMFILES%/Citrix/ICA client/wfica32 /localime:on

64ビットシステム：%PROGRAMFILES(X86)%/Citrix/ICA client/wfica32 /localime:on

- 繁体中国語、韓国語またはロシア語版のReceiverをAccess Gateway Standard Editionと統合する場合は、Access Gateway Standard Edition側の言語の制限のため、Receiverのログオン画面に英語が表示されます。[#263442]
- ユーザーデバイス上のインターネットオプションで証明書失効一覧（CRL）に関する設定が無効になっていると、ReceiverのCertificateRevocationCheckレジストリ設定が上書きされます。このため、有効な資格情報を持たないWebサイトにユーザーがアクセスできることがあります。この問題を回避するには、［設定］、［コントロールパネル］、［インターネットオプション］、［詳細設定］の順に選択して、［サーバーの証明書失効を確認する］チェックボックスをオンにします。[#32682]
- ReceiverはAccess Gateway ClientChoicesモードのVPNキーワードをサポートしません。[#274828]
- ユーザーがサブスクライブした後にVPNキーワードがアプリケーションから削除されると、Receiverはアプリケーションに対するAccess Gateway接続を続行しようとします。この問題を回避するには、ユーザーがそのアプリケーションのサブスクリプションを解除してから再度サブスクライブする必要があります。これにより、VPNキーワードがReceiverから削除されます。[#298387]
- XenApp 5.0以前のバージョンで公開されたアプリケーションをユーザーが起動すると、タスクバーにアプリケーションアイコンの代わりにReceiverアイコンが表示されます。[#310366]
- Internet ExplorerでSharePointにアクセスしてMicrosoft Officeのドキュメントを編集モードで開こうとすると、「アクセスが拒否されました」というMicrosoft Officeのメッセージが表示される可能性があります。この問題を回避するには、SharePointサイトでドキュメントをチェックアウトして編集し、そのファイルをSharePointにチェックインします。[#258725]

- 仮想デスクトップセッションを経由して公開アプリケーションのWindows Media Playerでファイルを再生しているときに、Desktop Viewerウィンドウを全画面モードからウィンドウモードに変更するとビデオが表示されなくなります。この問題を回避するには、Media Playerウィンドウを最小化してから復元し、再生を一時停止してから再開するか、停止してから再開します。[#246230]
- Windows XP 32ビット版の仮想デスクトップセッションでReceiverを起動しログオンせずにいると、セッションから正常にログオフできません。Receiverのログオンダイアログボックスでの操作を完了しなければ、デスクトップからログオフできません。この問題を回避するには、ログオンダイアログボックスでの操作を完了するか、ダイアログボックスを閉じます。この問題は、ほかのオペレーティングシステムの仮想デスクトップでは発生しません。[#246516]
- ユーザーがDesktop Viewerのデバイスアイコンをクリックしても［デバイス］メニューが閉じないことがあります。また、対応するダイアログボックスを閉じても開いたままで残ることもあります。この問題が発生した場合は、デバイスアイコンをもう一度クリックします。[#262202]
- 2つのモニターを接続したWindowsユーザーデバイスの非プライマリモニターにWindows Media Playerを表示すると、期待どおりに機能しない可能性があります。これはDirectXのVMR9（Video Mixing Renderer 9：ビデオミキシングレンダラー9）フィルターが原因となる問題で、プレーヤーの進行状況バーは進みますが画面は黒くなり音声が聞こえません。この問題を修正するには、XenDesktop接続を起動するユーザーデバイスでレジストリを編集します。HKEY_CURRENT_USER\Software\Citrixサブキーに、HdxMediaStreamキーを作成します。キーの名前をDisableVMRSupportにします。種類をREG_DWORDに設定します。キーの値を3にします。[#262852]

- 仮想デスクトップセッションに再接続した後で、VDIのログオンダイアログボックスが表示されず、仮想環境内のLyncとLync VDI plug-inとの関連付けが解除されることがあります。この問題を解決するには、Lyncからサインオフして再サインオンしてください。[#399459]

- Lyncでのビデオ通話中に仮想デスクトップセッションが切断された場合に、通話が切断されず、ユーザーがLyncの会話ウィンドウを閉じるとこのウィンドウが応答不能になることがあります。[#399464]
- ユーザーが仮想デスクトップを共有する場合、Lyncの会話ウィンドウにマウスポインタが表示されなくなることがあります。[#399442]
- Lyncの会話ウィンドウをセカンダリモニターに移動させると、ビデオが表示されなくなることがあります。[#399447]
- ホワイトボードウィンドウをほかのユーザーに移動させると、そのユーザーのビデオ映像が会話ウィンドウに表示されなくなることがあります。[#399465]
- Lyncでの通話を開始したときに、Receiverによりデバイスの音量が下げられることがあります。デバイス上の音量コントロールを使って音量を上げてください。[#401519]

詳しくは、「XenDesktop 7、XenApp 6.x、およびCitrix Receiver 4.0でのMicrosoft Lync 2013 VDIプラグインのサポート」を参照してください。

Oct 31, 2016

次の要件の一覧は、サポートが限定されるエディションまたはService Packを示しています。

- Receiver for Windows 4.1の場合のみ：Windows 8.1 32ビット版および64ビット版（Embeddedを含む）
- Windows 8 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 XP Professional SP3 32ビット、およびWindows XP Professional SP2 64ビット（Embeddedエディションを含む）
  Windows XPのサポートは、Microsoft社のサポート期限である2014年4月8日に終了します。Windows XP Embeddedのサポートは継続されます。

- Windows Vista 32ビット版および64ビット版
- Windows Thin PC
  Self-Service Plug-inはサポートされません。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 for Windows 4.1の場合のみ：Windows Server 2012 R2 64ビット版
- Windows Server 2012 64ビット版
- 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
- Windows Server 2003 32ビット版および64ビット版

- VGAまたはSVGAビデオアダプターとカラーモニター
- Windows互換のサウンドカード（サウンドをサポートする場合）
- サーバーファームへのネットワーク接続用のネットワークインターフェイスカードとネットワークトランスポートソフトウェア

- XenAppの以下のバージョン：
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2
  - Citrix XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - Citrix XenApp 4 Feature Pack 1または2 for UNIX operating systems
- XenDesktopの以下のバージョン：
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
  - XenDesktop 5.6 Feature Pack 1

- XenDesktop 5.6
- XenDesktop 5.5
- XenDesktop 5
- XenDesktop 4

- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
  - VDI-in-a-Box 5.1
- Citrix Receiverは、StoreFront、App Controller、およびWeb Interfaceを使って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。
  StoreFront：
  - StoreFront 2.6（推奨）、2.5、または2.1
    StoreFrontストアへの直接アクセスを提供します。

  - Receiver for WebサイトがStoreFront
    StoreFrontストアへのWebブラウザーからのアクセスを提供します。 この場合の制限事項については、 「Receiver for Webサイト」の「重要な注意事項」を参照してください。

  App Controller 9.0および2.10：

  Windows、Web、およびサービスとしてのソフトウェア（SaaS）アプリケーションへのアクセスを提供します。 また、ShareFileアカウントのプロビジョニングとシングルサインオン機能を提供します。 App Controllerは、XenMobile App Editionのコンポーネントです。

  NetScaler VPNクライアントを使用する場合のWeb Interface：
  - Web Interface 5.4.x for WindowsのWebサイト。
    デスクトップやアプリケーションへのWebブラウザーからのアクセスを提供します。

  - Web Interface 5.4 for Windowsの従来のXenApp ServicesサイトまたはXenDesktop Webサイト。
- Receiverの展開：
  - Citrix Receiver for Webサイト（StoreFrontを使用した構成）
  - Citrix Merchandising Server 2.x
  - Citrix Web Interface 5.4
  - Microsoft System Center 2012 Configuration Manager

- Internet Explorer
  Receiver forWeb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。

- Mozilla Firefox 18.x以降
- Google Chrome 20または21（StoreFrontが必要）

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-SSL接続を確立できます。

- LAN接続の場合：

- StoreFront ServicesサイトまたはReceiver for Webサイトを使用するStoreFront。
  App Controllerで公開されたWebおよびSaaSアプリケーションへのシングルサインオンを使用するには、StoreFrontが必要です。

- Web Interfaceサイト、または従来のXenApp ServicesサイトやXenDesktop Services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 10.1
  - Citrix Access Gateway Enterprise Edition 10
  - Citrix Access Gateway Enterprise Edition 9.x
  - Citrix Access Gateway VPX
  - Citrix Access Gateway 5.0（Web Interfaceを使用する環境でのみ）
  - Citrix Secure Gateway 3.x（Web Interfaceを使用する環境でのみ）

  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。

注：このトピックに記載されているNetScaler Gatewayについての説明は、特に注記のない限りはAccess Gatewayにも該当します。

注：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。
SSLを使用してリモート接続を保護する場合、Receiverはリモートゲートウェイの SSL証明書の信頼性を、信頼されたルート証明機関のローカルストアと照合することで検証します。証明機関のルート証明書がローカルのキーストアに存在する場合は、民間の証明機関（VeriSignおよびThawteなど）が発行した証明書が自動的に検出されます。

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、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でCitrixリソースにアクセスできません。

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

ユーザーデバイスへのルート証明書のインストール

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のSSL/TLS機能の構成と有効化」を参照してください。

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内の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。Receiver for Windowsでは、ワイルドカード証明書がサポートされています。

中間証明書とNetScaler Gateway

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への接続では、Receiverで以下の認証方法がサポートされます。

- ドメイン（NetScaler Gatewayからの接続に対しては使用不可）
- ドメインパススルー
  Receiver for Webサイトでは、ドメイン資格情報のパススルー認証はサポートされません。NetScaler Gatewayからの接続に対しては使用できません。
- セキュリティトークン*
- 2要素（ドメイン+セキュリティトークン）*
- SMS*
- スマートカード（StoreFront 2.1または2.0が必要）
- ユーザー証明書*（単独で使用したりほかの認証方法と組み合わせて使用したりできます）

* Receiver for WebサイトおよびNetScaler Gatewayを含む展開に対してのみ使用できます（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）。

App Controllerへの接続では、Receiverで以下の認証方法がサポートされます。

- ドメイン
- セキュリティトークン*
- 2要素（ドメイン+セキュリティトークン）*
- SMS*

* 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）。

Web Interface 5.4への接続では、Receiverで以下の認証方法がサポートされます（Web Interfaceでは、「指定ユーザー」による認証がドメイン+セキュリティトークン認証に相当します）。

- ドメイン
- ドメインパススルー（Webブラウザーを介す接続に対してのみ利用可能）
- セキュリティトークン*
- 2要素（ドメイン+セキュリティトークン）*
- SMS*
- スマートカード
- ユーザー証明書*（単独で使用したりほかの認証方法と組み合わせて使用したりできます）

* 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」のトピックを参照してください。Web Interfaceでサポートされる認証方法については、「Web Interfaceの認証方法の構成」を参照してください。

旧バージョンからのアップグレードは、Citrix Online Plug-in 12.xおよびReceiver for Windows 3.xに対してのみサポートされています。

Receiverの機能の一部は新しいバージョンのXenDesktopおよびXenAppに接続する場合にのみ使用できます。また、最新のHotfixの適用が必要である場合があります。

- **互換性があるプラグイン**
  互換性のあるプラグインソフトウェアの一覧については、「Citrix Receiverの更新を管理するには」を参照してください。

- **.NET Frameworkの要件**
  - 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 7、XenApp 6.x、およびCitrix Receiver 4.0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
    重要：StoreFrontで構成された［Transport type］が［HTTP］のストアを使用するには、レジストリキーHKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManagerにConnectionSecurityMode=Anyを設定する必要があります。
    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。
  - SSL/TLS+HTTPS

- 以前のバージョンのPresentation Serverクライアント/Online Plug-inと現在のicaclient.admファイル。以前のバージョンのPresentation ServerクライアントとOnline Plug-inは、Receiver for Windows 4.0のicaclient.admファイルと互換性がありません。

Nov 19, 2015

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App Controller仮想アプライアンス、NetScaler Gateway（またはAccess Gateway）、または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やReceiver Updater for Windowsがインストール済みである場合は、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。
  - この場合、Receiverユーザーは Receiverのインターフェイスから手動で更新をチェックできます。
  - 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ファイルをダウンロードします。
  - XenDesktop 7はWeb Interfaceをサポートしません。
- 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。
  - 管理者は、Merchandising Serverやそのほかの方法で更新ソフトウェアを提供できます。
    アカウントセットアップの方法としてメールアドレスやサーバーURLによるアカウント検出を使用している環境では、管理者はMerchandising Serverを使用してReceiverにストアを追加できます。ただし、メールアドレスやサーバーURLによるアカウント検出で提供されているものと同じストアをMerchandising Serverで追加することはしないでください。

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」、「ユーザーによるReceiver for Windowsのインストールとアンインストール」、「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Receiverの配布」を参照してください。

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。

重要：Receiverを初めて使用するユーザーには、Receiverのインストール後にReceiverを再起動するよう指示してください。これにより、ユーザーがアカウントを追加できるようになり、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。

注：従来のVDAを使用しているサイトは、アップグレードする必要はありません。引き続きReceiver Enterpriseを使用する必要があります。
重要：Citrix Lync Optimization Packがインストール済みのエンドポイントでは、これをアンインストールしてからCitrix Receiver for Windowsをアップグレードして、その後でOptimization Packをインストールし直してください。詳しくは、CTX200340を参照してください。
StoreFront環境：

- Citrix eDocsの製品ドキュメントを参照して、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Receiver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。

App Controller 2.5以降を使用している場合は、プロビジョニングファイルが添付されたメールをReceiverユーザーに送信できます。プロビジョニングファイルには、ReceiverでApp Controllerに接続するための情報が定義されています。

- 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（またはAccess Gateway Enterprise Edition）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、Receiver for Webサイトを構成（StoreFrontのドキュメントを参照）し、「Receiver for WebサイトからのReceiverの配布」の説明に従って構成を完了する方法もあります。Receiverのアップグレード方法、Receiver for Webサイトへのアクセス方法、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環境（XenDesktop 7環境ではサポートされません）：

- App Controllerを使用している場合は、App Controllerのドキュメントの「Configuring Additional Parameters in Application Connectors」セクションを参照してコネクタを構成します。
- Receiver for Windows 4.0でWeb Interfaceサイトをアップグレードし、「Web Interfaceのログオン画面からのReceiverの配布」で説明されている構成を完了します。Receiver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。

重要：Receiver for Windows 4.xでは、パススルー認証（シングルサインオン）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。
Receiver for Windows 4.xでは、Receiver for Windows 3.xと、Citrix Online Plug-in 12.xをアップグレードできます。

Program NeighborhoodエージェントまたはCitrix Receiver（Enterprise）用に構成されたOnline Plug-in（フルバージョン）をReceiver for Windows 4.x（CitrixReceiver.exe）にアップグレードするには、最初に古いバージョンをアンインストールしてから、新しいバージョンをインストールしてください。

CitrixReceiver.exeがOnline Plug-inなし、またはOnline Plug-in（Web）と一緒にインストール済みの場合は、Receiver for Windows 4.xにアップグレードするとCitrix ReceiverへのWebベースアクセスを実行できるようになります。

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。

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。

ここでの説明は、Merchandising Serverを使用してアップデートする場合に適用されます。

プールされたマシンから配信されるデスクトップでは、そのデスクトップのマスターイメージを使ってReceiverを更新できるように、Receiverの自動更新を無効にします。

マスターイメージを準備するときに、以下の方法で自動更新を無効にします。

1. Merchandising Serverのドキュメントの「
   — To use Merchandising Server to install and set up Citrix Receiver for Windows on a shared XenDesktop image
   」の手順に従います。

2. マスターイメージで、以下のレジストリキーを設定します。
   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。
   32ビットマシンの場合：

   DWORD:00000001 HKLM\SOFTWARE\Citrix\Receiver\Inventory\NoPluginUpdates

   64ビットマシンの場合：

   DWORD:00000001 HKLM\Software\Wow6432Node\Citrix\Receiver\Inventory\NoPluginUpdates

Nov 19, 2015

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Receiver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。

インストール処理を途中でキャンセルしても、一部のコンポーネントのインストールが完了している場合があります。この場合は、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Receiverをアンインストールしてください。

重要：Receiver for Windows 4.xでは、パススルー認証（シングルサインオン）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。
社内ポリシーでEXEファイルの使用が禁止されている場合は、「How to Manually Extract, Install, and Remove Individual .msi Files」を参照してください。

Citrix Receiver Updaterを使ってReceiverをインストールした場合は、Updaterを使ってReceiverをアンインストールできます。Citrix Receiver Updaterを使わずにReceiverをインストールした場合は、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］）を使用します。

Receiver for Windowsをアンインストールしても、一部のコンポーネントファイルやレジストリエントリが削除されない場合があります。以前のバージョンのReceiverをアンインストールしてから新しいバージョンをインストールできない場合は、Receiver Clean-Up Utilityを使用して古いファイルやレジストリエントリを削除してください。

［プログラムと機能］でReceiverをアンインストールする前にReceiver関連のファイルやレジストリエントリを削除すると、アンインストールに失敗する場合があります。Microsoft Windowsインストーラー（MSI）によって修復とアンインストールが同時に試行されます。この問題が起きた場合は、Receiverを使用して自動修復を開始します。自動修復が完了したら、［プログラムと機能］でReceiverをアンインストールしてください。

Receiverに問題が起きたときには自動修復が行われます。［プログラムと機能］に［修復］オプションは表示されません。自動修復時にMSIファイルの場所を指定するダイアログボックスが開いたら、以下の場所を指定してください。

- コンピューター単位でインストールした場合：
  - オペレーティングシステム：Windows Server 2012/2008、Windows 8、Windows 7、Windows Vista
    C:\ProgramData\Citrix\Citrix Receiver\
  - オペレーティングシステム：Windows Server 2003およびWindows XP
    C:\Documents and Settings\All Users\Application Data\Citrix\Citrix Receiver\
- ユーザー単位でインストールした場合：
  - オペレーティングシステム：Windows Server 2012/2008、Windows 8、Windows 7、Windows Vista
    %USERPROFILE%\Appdata\local\Citrix\Citrix Receiver\
  - オペレーティングシステム：Windows Server 2003およびWindows XP

%USERPROFILE%\Local Settings\Application Data\Citrix\Citrix Receiver\

コマンドラインを使ってReceiver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Receiverをアンインストールすることもできます。

CitrixReceiver.exe /uninstall

ユーザーデバイスからReceiverをアンインストールした後、icaclientにより作成されたReceiverのカスタム設定レジストリキーが、HKEY_LOCAL_MACHINEおよびHKEY_LOCAL_USERの下のSoftware\Policies\Citrix\ICA Clientディレクトリに残ります。Receiver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。

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。

Nov 19, 2015
コマンドラインオプションを指定して、Receiver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、%temp%フォルダーには78.8MB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。

注意：レジストリエディタの使用を誤ると、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。
コマンドプロンプトから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>]

使用できるオプションは、次のとおりです。

- /?または/helpを指定すると、使用方法の情報が表示されます。
- /norebootを指定すると、ウィザードによるインストール時の再起動が無効になります。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、Receiver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Receiverで認識できません。
- /silentを指定すると、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。「/noreboot」も参照してください。
- /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。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Receiver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。

- PROPERTY=Value
  ここで、PROPERTYはすべてが大文字の以下のいずれかの変数（キー）で、Valueにその値を指定します。

  - INSTALLDIR=<Installation directory>。<Installation directory>に、Receiverソフトウェアのインストール先フォルダーを

指定します。デフォルト値は、C:\Program Files\Citrix\Receiverです。ただし、Receiverの一部のコンポーネント（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。

- CLIENT_NAME=<ClientName>。<ClientName>に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クライアント名を指定します。デフォルト値は、%COMPUTERNAME%です。
- ENABLE_DYNAMIC_CLIENT_NAME={Yes | No}。ダイナミッククライアント名機能を有効（Yes）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。
- ADDLOCAL=<feature>[,...]。インストールするコンポーネントの種類をに指定します。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。
  注：ReceiverInsideとICA_Clientは必須であり、ほかのコンポーネントをインストールする場合でも必ずこれらを含める必要があります。
  ReceiverInside – Receiverエクスペリエンスをインストールします（Receiverの操作に必須のコンポーネント）。

  ICA_Client – 標準のReceiverをインストールします（Receiverの操作に必須のコンポーネント）。

  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で使用可能なコマンドラインパラメーターについては、http://support.citrix.com/article/CTX138514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のウイ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。Self-Service Plug-inがインストールされていない場合、ユーザーはWebページから仮想デスクトップやアプリケーションにアクセスする必要があります。

  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）。

- ALLOWADDSTORE={N | S | A} – Merchandising Serverで構成されていないストアをユーザーが追加または削除できるかどうかを指定します（ユーザーはMerchandising Serverで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。
  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）。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HKLM\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. Receiverを終了して再度起動します。

- ALLOWSAVEPWD={N | S | A} – デフォルトの値は、実行時にPNAgentサーバーから指定される値です。ユーザーがストアの資格情報をコンピューター上に保存することを許可するかどうかを指定します。この設定は、PNAgentプロトコルを使用するストアにのみ適用されます。
  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。

- ENABLE_SSON={Yes | No} – デフォルトの値は、Yesです。さらに/includeSSONを指定すると、シングルサインオンが有効になります。スマートカードによるシングルサインオンを有効にするには、このプロパティを指定する必要があります。有効にしたシングルサインオン認証は、インストール後にユーザーがデバイスにログオンし直すまで使用できません。管理者権限が必要です。
  重要：管理者が無効にしたシングルサインオン認証を後で有効にした場合、ユーザーはReceiverを再インストールする必要があります。
- AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry } – 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。

- AM_SMARTCARDPINENTRY=CSP – デフォルトでは、スマートカードのCryptographic Service Provider（CSP）ではなく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。
  この機能は、レジストリキーHKEY_LOCAL_MACHINE\Software\

[Wow6432Node\]Citrix\AuthManagerのSmartCardPINEntry=CSPで設定することもできます。

- ENABLE_KERBEROS={Yes | No} – デフォルトの値は、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。
- LEGACYFTAICONS={False | True} – デフォルトの値は、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。
- ENABLEPRELAUNCH={False | True} – 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。
- STARTMENUDIR=Text string – 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>」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。

  たとえば、［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。

- STORE<x>="<storename>;http[s]://<servername.domain>/<IISLocation>/discovery;[On | Off];[<storedescription>]"[STORE<y>="..."] – Receiverで使用するストアを最多で10個まで指定します。値のデータ：
  - <x>および<y> – 0～9の整数。
  - <storename> – ストア名。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、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。
- ALLOW_CLIENTHOSTEDAPPSURL=1 - ユーザーデバイスのURLリダイレクト機能を有効にします。管理者権限が必要です。また、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。

無人インストール時にインストール完了のメッセージが表示されるようにするには

CitrixReceiver.exeによる初回インストールを無人モードで行う場合、インストールが完了する前に［アカウントの追加］ダイアログボックスが開きます。インストールを完了するには、ユーザーが［アカウントの追加］ダイアログボックスにメールアドレスまたはサーバーアドレスを入力する必要があります。［アカウントの追加］ダイアログボックスを開く代わりにインストール完了時にアカウントセットアップ用のオプションをユーザーに表示するには、レジストリキーHKEY_CURRENT_USER\Software\Citrix\ReceiverにEnableFTU=0を指定してください。

そのコンピューターに複数のユーザーがログオンする場合は、上記の値をコンピューター全体のポリシーに追加します。

インストールの問題を解決するには

インストールで問題が発生した場合は、ユーザーの%TEMP%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、「CtxInstall-」または「TrollyExpress-」で始まります。次に例を示します。

CtxInstall-ICAWebWrapper.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"
```

Self-Service Plug-in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。

Nov 19, 2015

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Receiver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、新しいバージョンのXenAppおよびXenDesktopのインストールメディアのCitrix Receiver and Plug-ins\Windows\Receiver\Startup_Logon_Scriptsフォルダーに収録されています。

- 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既定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。たとえば、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、Receiver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 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収録されています。

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

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。

Receiverをユーザー単位で展開する

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。

Receiverをユーザー単位で削除する

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。

Nov 19, 2015

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。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。Receiver for Webサイトで適切なバージョンのReceiverがインストールされていないことが検出されると、Receiver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。

Receiver for Webからインストールしたreceiver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Receiver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の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。
   重要：CitrixReceiverWeb.exeの大文字と小文字は区別されます。
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。

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Receiver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Receiverがインストールされていないことが検出されると、Receiver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Receiver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Receiver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の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。
   重要：CitrixReceiverWeb.exeの大文字と小文字は区別されます。
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Receiver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Receiver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。

Nov 19, 2015

以下の構成手順により、ユーザーが仮想デスクトップおよびアプリケーションにアクセスできるようになります。

- アプリケーション配信およびXenDesktop環境の構成。リモートユーザーが仮想デスクトップおよびアプリケーションに安全にアクセスできるようにするには、NetScaler GatewayまたはAccess Gatewayを構成します。
- StoreFrontおよびApp Controllerの構成。XenDesktopサイト、XenAppファーム、およびApp Controllerで提供されるリソースを集約してユーザーに提供するには、ストアを作成します。
- グループポリシーオブジェクトテンプレートファイルを使ったReceiverのカスタマイズ。ルーティング、プロキシサーバー、リモートユーザーデバイスなどの規則を構成します。
- 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。

Nov 19, 2015

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、StoreFrontのストアを使って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。XenDesktop 7でのアプリケーション配信については、XenDesktop 7のドキュメントの「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。

- 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。この説明は、Receiverのユーザーに表示されます。
- 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。
  - 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。
  - 説明に「KEYWORDS:prefer="<pattern>"」という文字列を追加すると、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。
    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、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、Receiverの次回更新時までそのアプリケーションのサブスクリプションは解除されます。ユーザーが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、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：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
Console	\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。Start Menuディレクトリのサブフォルダー Programs以下の絶対パスを指定します。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。

Nov 19, 2015
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。

XenDesktopセッションでは次の種類のデバイスは直接サポートされるため、USBサポート機能は使用されません。

- キーボード
- マウス
- スマートカード

注：特殊用途のUSBデバイス（Bloombergキーボードや3Dマウスなど）では、USBサポート機能が使用されるように構成できます。Bloombergキーボードの構成について詳しくは、「Bloombergキーボードの構成」を参照してください。そのほかの特殊用途のUSBデバイスのポリシー規則の構成について詳しくは、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、リモートで動作する仮想デスクトップでの使用には適しません。次の種類のUSBデバイスは、XenDesktopセッションでの使用をデフォルトでサポートしていません。

- Bluetoothドングル
- 統合ネットワークインターフェイスカード
- USBハブ
- USBグラフィックアダプター

USBハブに接続されたデバイスは仮想デスクトップで使用できますが、USBハブ自体はリモート処理できません。

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、CTX123015を参照してください。

ユーザーがエンドポイントにUSBデバイスを接続すると、USBポリシーが照合され、許可されているデバイスであることが認識されると、仮想デスクトップ上で使用可能になります。USBポリシーで拒否されるデバイスは、ローカルのデスクトップ上でのみ使用可能になります。

ユーザーが接続する仮想デスクトップの種類により、ユーザーエクスペリエンスが異なります。

Desktop Viewerを介してアクセスするデスクトップでは、ユーザーがUSBデバイスを接続すると、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るダイアログボックスが開きます。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つの設定項目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（USB Plug-n-Play Devices）
デフォルトで有効。	はい	はい
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）

［USB Plug-n-Play Devices］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。
  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。手順については、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。
  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

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。手順については、CTX123015を参照してください。

- マスストレージ（クラス08）。最も一般的なマスストレージデバイス（大容量記憶装置）として、USBフラッシュドライブがあります。そのほかには、USB接続のハードドライブ、CD/DVDドライブ、およびSD/MMCカードリーダーがあります。また、内部ストレージを持つさまざまなデバイスがあり、これらもこのクラスのインターフェイスを提供します。たとえば、メディアプレーヤー、デジタルカメラ、携帯電話などがあります。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たはUSBサポート機能でマスストレージデバイスの使用を許可する場合は、ビジネス上の必要性があるかどうかを慎重に考慮してください。
- コンテンツセキュリティ（クラス0d）。通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。
- ビデオ（クラス0e）。このクラスのデバイスとして、ビデオ、Webカメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。
  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。手順については、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。

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。

icaclient_usb.adm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Receiver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、http://support.citrix.com/article/ctx119722/を参照してください。

Bloombergキーボードは、XenDesktop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。

Nov 19, 2015

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\...

Nov 19, 2015

Receiverのユーザーインターフェイスに表示されるオプションでの構成に加えて、グループポリシーエディターやicaclient.admテンプレートファイルを使って設定を構成できます。グループポリシーエディターでは、以下の構成を行えます。

- icaclient.admファイルを編集して、すべてのReceiver設定をicaclientテンプレートで構成する。ADMファイルの編集および特定のコンピューターに設定を適用する方法について詳しくは、Microsoft社のグループポリシーに関するドキュメントを参照してください。
- クライアントデバイスの特定のユーザーまたはすべてのユーザーに構成を適用する。
- 複数のユーザーデバイスに構成を適用する。

グループポリシーを使用してリモートからユーザーデバイスを設定することをお勧めします。ただし、必要なレジストリエントリをアップデートできるのであれば、レジストリエディターなどを使用して構成することもできます。

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icaclient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、icaclient.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. ［ユーザーの構成］または［コンピューターの構成］で、必要に応じて設定の変更を行います。

Nov 19, 2015

Citrix StoreFrontは、XenDesktop、XenApp、App Controller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、Receiver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またはAccess Gatewayを構成する必要もあります。

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します。 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Receiver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。
2. XenDesktopやXenAppでのアプリケーション配信を構成するのと同様に、App Controllerのストアを構成します。 ユーザーのReceiver側で特別な設定を行う必要はありません。 詳しくは、StoreFrontのドキュメントの「ストアの構成」を参照してください。

XenMobile App EditionのコンポーネントであるApp Controllerでは、エンタープライズレベルのWebアプリケーションやSaaS（Software-as-a-Service）アプリケーション、iOSデバイス用に開発されたアプリケーション、およびShareFileベースのデータ共有機能をReceiverユーザーに安全に配信できます。

メールアドレスによるアカウント検出機能を使用する場合は、ユーザーのメールアドレスに関連付けられているApp ControllerがReceiverにより検出されます。

メールアドレスによるアカウント検出機能を使用しない場合は、ReceiverでApp Controllerに接続するための構成が定義されたプロビジョニングファイルをユーザーに提供します。App Controllerの管理コンソールを使用すると、プロビジョニングファイル（CRファイル）をメールでユーザーに送信できます。詳しくは、App Controllerのドキュメントの「ユーザーをCitrix Receiverに接続する」を参照してください。

または、Receiver for Webサイトを構成すると、ユーザーがReceiverの [アクティブ化] をクリックしてプロビジョニングファイルを入手できるようになります。

Nov 19, 2015

グループポリシーオブジェクトの icaclient.admテンプレートを使って、ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則を構成することをお勧めします。

icaclient.admテンプレートファイルを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と一緒に使用できます。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Receiver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。

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icaclient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、icaclient.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. ［ユーザーの構成］または［コンピューターの構成］で、必要に応じて設定の変更を行います。

Nov 19, 2015

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

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

重要：Receiverを初めて使用するユーザーには、Receiverのインストール後にReceiverを再起動するよう指示してください。これにより、ユーザーがアカウントを追加できるようになり、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。

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Receiver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）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、Access Gateway、StoreFrontサーバー、またはApp Controller仮想アプライアンスが自動的に検出され、仮想デスクトップやアプリケーションにアクセスするためのログオンを求めるメッセージが表示されます。

注：メールアドレスによるアカウント検出は、Web Interface環境では使用できません。
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およびApp Controller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、ユーザーはストアやApp Controller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、Receiverを自動的に構成できるようにします。Receiver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Receiverが自動的に構成されます。Receiver for Webサイトを構成する場合は、そのサイトからユーザーにReceiver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。
- App Controllerでは、プロビジョニングファイルが添付されたメールをReceiverユーザーに送信できます。プロビジョニングファイルには、ReceiverでApp Controllerに接続するための情報が定義されています。詳しくは、App Controllerのドキュメントの「Receiver構成ファイルのダウンロード」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ストアまたはApp Controller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
  従来の展開環境の場合は、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、Receiver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。

Receiverユーザーがアカウントを管理するには、Receiver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。

Nov 19, 2015

管理者は、ユーザーが効率的に作業できるようにReceiver環境を最適化できます。

- アプリケーションの起動時間を短縮する
- 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

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。

Nov 19, 2015
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Receiver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Receiver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、Receiver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。

icaclient.adm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、Receiver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。

Nov 19, 2015

Receiver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ローカル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。

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

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

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。たとえば、サーバーのCドライブをMに変更し、DをNに変更しておくと、クライアントデバイスの既存のCドライブやDドライブにそのままアクセスできます。この場合、セッションでのドライブマッピングは、次のようになります。

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

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

クライアント側デバイスの自動マッピングを無効にしない限り、ユーザーデバイスでサーバーに再接続すると、マッピングが再確立されます。デフォルトでは、クライアント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、eDocsでXenDesktopまたはXenAppのドキュメントを参照してください。

HDX Plug-n-Play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、eDocsでXenDesktopまたはXenAppのドキュメント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、デバイス接続時にそのデバイスのリダイレクトを許可したり、拒否したり、または毎回確認のメッセージを表示したりできます。この設定は、Receiver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。

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. Receiverにログオンします。
3. コマンドプロンプトで次のように入力します。net use com<x>: \\client\com:
   ここで、<x>は、マップするクライアントCOMポートの数です。

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。
   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。TAPIデバイスをクライアントのCOMポートにマップすることはできません。

DNS名前解決をサポートする

Nov 19, 2015

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）名を要求できるように、Receiver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Receiverも、接続にCitrix XML Serviceを使用します。この場合、Receiver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、Receiver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、ReceiverがDNS名を要求するとIPアドレスが返されます。ReceiverでDNSアドレス解決を無効にする必要はありません。

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。

プロキシサーバーを介したXenDesktop接続をサポートする

Nov 19, 2015

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。

ユーザーエクスペリエンスの向上

Nov 19, 2015

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。

- クライアント側のマイク入力
- マルチモニターのサポート
- デバイス側での印刷設定の変更
- キーボードショートカット
- 32ビットカラーアイコンのサポート
- Receiverユーザーへの仮想デスクトップの提供
- Desktop Viewerセッションでのキーボード入力
- 仮想デスクトップへの接続

クライアント側のマイク入力

Nov 19, 2015

Receiverは、クライアント側の複数のマイク入力をサポートします。ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

- ソフトフォンでの通話やWeb会議などのリアルタイムのアクティビティ。
- ホストされている録音アプリケーション（ディクテーションプログラムなど）の使用。
- 録画と録音。

Receiver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

Nov 19, 2015

Receiver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］ボタンをクリックします。

- 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］の［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、CTX116286を参照してください。

デバイス側での印刷設定の変更

Nov 19, 2015

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。

キーボードショートカット

Nov 19, 2015

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icaclient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、icaclient.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 Components］、［Citrix Receiver］、［User Experience］の順に開きます。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックして必要なオプションを選択します。

32ビットカラーアイコンのサポート

Nov 19, 2015

Receiver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。

Receiverユーザーへの仮想デスクトップの提供

Nov 19, 2015

企業によって社内のニーズはさまざまであり、仮想デスクトップへのアクセス方法に対する要件も、各ユーザーの作業形態や時間の経過により変化します。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Receiver for Windowsのセットアップ方法によって異なります。仮想デスクトップへのアクセスをユーザーに提供するためのコンポーネントには、Desktop ViewerとCitrix Desktop Lockの2つがあります。

ユーザーが仮想デスクトップとローカルデスクトップの両方を操作する必要がある場合は、Desktop Viewerを使用します。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 LockはCitrixReceiverEnterprise.exeでのみサポートされます。詳しくは、Citrix eDocsのXenDesktop 7のドキュメントを参照してください。

Desktop Viewerセッションでのキーボード入力

Nov 19, 2015

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

Nov 19, 2015

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。

接続の保護

Nov 19, 2015

環境のセキュリティを最大限に高めるには、Receiverと公開リソースの間の接続を保護する必要があります。Receiver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。

スマートカード認証の構成

Nov 19, 2015

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、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Receiver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、Receiver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があります。

  パススルー認証を使用するには、StoreFrontおよびReceiver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。2モード認証を使用するには、StoreFrontおよびNetScaler Gatewayでの構成が必要です。
- **複数の証明書** – 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。ユーザーがスマートカードをリーダーに挿入すると、ユーザーデバイス上で実行する、Receiverを含む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、Receiver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/Access GatewayおよびStoreFrontでの構成が必要です。
  - NetScaler Gateway/Access 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/Access 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。
- Receiver for Windowsでは、ユーザーのPINや選択した証明書が記憶されません。
- 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、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。
- スマートカードを使用したApp Controllerへの直接認証はサポートされません。ただし、App ControllerでStoreFrontの証明書認証サービスが使用されるように構成することができます。クライアント証明書による認証を使用するWebアプリケーションでは、専用のSSL接続を確立するための個別のスマートカードログオン画面が必要です。
- 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。

注意：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。

Receiver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、Receiver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 Components］>［Citrix Receiver］>［User authentication］>［Local user name and password］
- 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、Receiver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、Receiver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\

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、Set DisableCtrlAltDelにfalseを設定します。
- 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て、［スマートカード］チェックボックスをオフにします。
  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。

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. Receiver for Windowsのインストールと構成

複数の証明書が有効な場合、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）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。

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、SSL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。

- Receiver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。

デフォルトでは、スマートカードのCryptographic Service Provider（CSP）ではなく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。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。

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

Receiverで証明書失効一覧を使用してセキュリティ保護を強化する

Nov 19, 2015

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、SSL/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SSL/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icaclient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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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。
   - Disabled：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。

サイトが信頼済みサイトまたはイントラネットのゾーンにない場合にパススルー認証を有効にする

Nov 19, 2015

ユーザーの資格情報を使用したサーバーへのパススルー認証を有効にする必要があっても、サイトを信頼済みサイトまたはイントラネットのゾーンに追加できないことがあります。この設定を有効にすると、制限付きサイト以外のすべてのサイトでパススルー認証が許可されます。

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。
   注：既にicaclient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、icaclient.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 Components］、［Citrix Receiver］、［User authentication］、［Local user name and password］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［Enable pass-through authentication］および［Allow pass-through authentication for all ICA connections］チェックボックスをオンにします。

Kerberosを使用したドメインパススルー認証の構成

Nov 19, 2015

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

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Receiver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。

Receiver、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、Receiver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. Receiver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. Receiver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Receiver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。PINの再入力が求められないようにするためだけにReceiverのKerberosを有効にします。ReceiverでKerberos認証を使用しない場合、StoreFrontへの認証に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。

Receiver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Receiver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。

注意：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。

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。

Receiver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、Receive
  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
  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る環境では、以下の
  ポリシーを使用してReceiver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 Components］>［Citrix Receiver］>［User
  authentication］>［Local user name and password］

  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Receiver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、Set DisableCtrlAltDelをfalseに設定します。
- 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。

Receiver通信のセキュリティ保護

Nov 19, 2015

XenDesktopサイトやXenAppファームとReceiver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またはAccess Gateway。詳しくは、このセクションのトピックと、NetScaler Gateway、Access 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Receiver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」、または「SSLトンネリングプロキシサーバー」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環境では、SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）プロトコルを使用するCitrix SSL Relay（XenDesktop 7環境には適用されません）。

Receiverは、Microsoft社のセキュリティ特化 - 機能制限（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、Windows XP、Windows Vista、およびWindows 7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 XP、Windows Vista、およびWindows 7の『セキュリティガイド』を参照してください。

NetScaler Gatewayによる接続

Nov 19, 2015

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、XenMobile App EditionのコンポーネントであるApp Controller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、Receiverを使用して接続を行います。
- App Controller環境では、NetScaler GatewayとApp Controllerを統合することでリモートユーザーがApp Controllerに接続できるようにします。ユーザーは、App Controllerに接続してWebアプリケーションやSaaS（Software as a Service）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、ReceiverまたはNetScaler Gateway Plug-inを使用して接続を行います。

接続の構成方法については、Citrix eDocsの「Integrating NetScaler Gateway with XenMobile App Edition」の各トピックを参照してください。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

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、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。

Access Gateway Enterprise Editionによる接続

Nov 19, 2015

リモートのユーザーがAccess 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Access Gatewayを構成します。

- StoreFront環境では、Access 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、Receiver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）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、ReceiverまたはAccess Gateway Plug-inを使用して接続を行います。

接続の構成方法については、Citrix eDocsの「Integrating Access Gateway with CloudGateway」の各トピックを参照してください。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 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Access 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Access Gatewayを構成します。詳しくは、eDocsの「Configuring Access Gateway Enterprise Edition to Communicate with 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

Nov 19, 2015

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して、Receiverとサーバーの間に保護された通信チャネルを提供できます。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、Receiverの構成は不要です。

Receiver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。Receiver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、Receiver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

Nov 19, 2015

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、Receiver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、Receiver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

Nov 19, 2015

信頼済みサーバーの構成を使用して、Receiver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、Receiver管理者とユーザーはユーザーデバイス上のデータの整合性をさらに確実に信頼することができます。また、悪意を持ったReceiver接続の使用を防止できます。

この機能を有効にすると、Receiver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しないかを決定できます。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（SSLなど）を使用して接続するReceiver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。

SSLを使用して接続する場合は、サーバー名をhttps://CN形式で追加します。ここで、CNはSSL証明書に表示される一般名を示します。SSLを使用しない場合は、Receiverが接続に使用する形式を使用します。たとえば、ReceiverがIPアドレスを使用して接続する場合は、サーバーのIPアドレスを追加します。

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、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icaclient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、icaclient.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. ［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 Components］、［Citrix Receiver］、［Network Routing］、［Configure trusted server configuration］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

Nov 19, 2015

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。

プロキシサーバーを介したReceiver接続

Nov 19, 2015

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、Receiverとサーバー間の接続を制御するために使います。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。

Receiverがサーバーファームと通信するときは、Receiver for WebまたはWeb Interfaceのサーバー上で構成されているプロキシサーバー設定が使用されます。プロキシサーバーの構成については、StoreFrontまたはWeb Interfaceのドキュメントを参照してください。

また、ReceiverがWebサーバーと通信するときは、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 Relayによる接続

Nov 19, 2015

このセクションの内容は、XenDesktop 7には適用されません。

ReceiverをCitrix SSL（Secure Sockets Layer）Relayサービスと共に使うことができます。Receiverは、SSLとTLSの両方のプロトコルをサポートしています。

- SSLは、ICAコネクションのデータを暗号化して接続を保護し、証明書を使った認証により接続先のサーバーの同一性を検証します。
- 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。技術的には、SSL Version 3.0とTLS Version 1.0の違いはわずかで、SSL用の証明書は、TLSでも使用できます。米国政府機関をはじめとする組織の中には、データ通信を保護するためにTLSの使用を義務付けているところもあります。このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140は、暗号化の情報処理規格です。

デフォルトではCitrix SSL Relayのリスナーポートとして、SSL/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、SSL/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SSL/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。

- SSL/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、SSL/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。

SSL Relayを使用したセキュリティ構成について詳しくは、XenAppのドキュメントの「サーバーとクライアント間のSSL/TLSを設定する」を参照してください。

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Receiver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：Receiver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。

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icaclient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、プラグイン構成フォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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］に以下の形式で新しいポート番号を入力します。
   server:

   ここで、<SSL relay port number>は、リスナーポート番号を示します。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。

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icaclient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は、手順2.～5.を省略できます。
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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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］に以下の形式で新しいポート番号を入力します。
   <servername>:>,<servername>:>

   ここで、<SSL relay port number>は、リスナーポート番号を示します。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
```

ReceiverのSSL/TLS機能の構成と有効化

Nov 19, 2015

このトピックの内容は、XenDesktop 7には適用されません。

SSLとTLSは同じ方法で構成され、一緒に有効になり、同じ証明書が使用されます。

SSLとTLSを有効にすると、接続の開始時にまずTLS接続が試行され、接続できない場合はSSL接続が試行されます。SSLでも接続できない場合は、エラーメッセージが表示されます。

Receiver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Receiver通信をSSL/TLSで暗号化するには、ユーザーデバイス、Receiver、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。

SSL/TLS機能が有効になっているReceiverとサーバーファーム間の通信をSSL/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。

Receiver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。

1. SSL/TLSでアプリケーション一覧を暗号化して、そのデータをReceiver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. Receiver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Receiver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。

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。
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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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。
   - ［SSL/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。TLSを使った接続に失敗した場合には、ReceiverはSSLを使って接続します。
   - ［SSL cipher suite］で［Detect version］を選択して、Receiver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、Receiver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。

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。

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icaclient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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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。
   - ［SSL/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。TLSを使った接続に失敗した場合には、ReceiverはSSLを使って接続します。
- ［SSL ciphersuite］で［Government］を選択します。
- ［CRL verification］で［Require CRLs for connection］を選択します。

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。SSL/TLSを使ってReceiver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。

接続時にSSL/TLSを使用するようにXenAppサーバーを構成して、Receiver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。SSL/TLSを使ってReceiver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。

SSL/TLSを使用するようにReceiverを構成して、Receiver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。

1. Windowsの通知領域でReceiver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。SSL/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SSL/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。

ユーザーデバイスへのルート証明書のインストール

Nov 19, 2015

SSL/TLS機能が有効になっているReceiverとサーバーファーム間の通信をSSL/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。

Receiver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。

ReceiverでSSL/TLSを使用するようにWebInterfaceを構成するには

Nov 19, 2015

1. SSL/TLSでアプリケーション一覧を暗号化して、そのデータをReceiver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. Receiver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Receiver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

Nov 19, 2015

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icaclient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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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。
   - ［SSL/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。TLSを使った接続に失敗した場合には、ReceiverはSSLを使って接続します。
   - ［SSL cipher suite］で［Detect version］を選択して、Receiver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、Receiver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FIPS 140セキュリティ規格に準拠するには

Nov 19, 2015

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。

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icaclient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、icaclient.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 Components］、［Citrix Receiver］、［Network routing］、［TLS/SSL data encryption and server identification］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。
   - ［SSL/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。TLSを使った接続に失敗した場合には、ReceiverはSSLを使って接続します。
   - ［SSL ciphersuite］で［Government］を選択します。
   - ［CRL verification］で［Require CRLs for connection］を選択します。

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

Nov 19, 2015

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。SSL/TLSを使ってReceiver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との通信にSSL/TLSを使用するようにXenAppを構成するには

Nov 19, 2015

接続時にSSL/TLSを使用するようにXenAppサーバーを構成して、Receiver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。SSL/TLSを使ってReceiver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SSL/TLSを使用するようにReceiverを構成するには

Nov 19, 2015

SSL/TLSを使用するようにReceiverを構成して、Receiver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Receiver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。 SSL/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SSL/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。

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

Nov 19, 2015

このトピックの内容は、従来の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。信頼できるソースからアプリケーションを起動することをCitrix Receiverで検証し、管理ポリシーに基づいて信頼されていない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Receiver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Receiver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、ReceiverのConfigurationフォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、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 Components］、［Citrix Receiver］の順に選択し、［Enable ICA File Signing］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
Only allow	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

オプション	説明
signed launches（more secure）	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、Receiver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

Nov 19, 2015

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（Full 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。

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

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

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（）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。

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 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。

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を設定するには

Nov 19, 2015

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：Receiverの機能拡張のため、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。
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. 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。

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
PdaSecurityPermission	PDAデバイス
ScannerAndDigitalCameraSecurityPermission	USBおよびそのほかのデバイス

値	説明

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

Receiver for Windows 4.xで解決された問題

Jan 27, 2017

Citrix Receiver for Windows 4.1.100との比較

Receiver for Windows 4.1.200には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX MediaStream Flashリダイレクト

- HDX MediaStream Flashリダイレクトが有効な特定のWebサイトを参照すると、Internet Explorerが応答不能になる場合があります。

  この修正を有効にするには、VDA/HDX Mediastream for Flashの参照番号#LA4151の修正もインストールし、VDA/XenAppサーバーで以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer
  名前：SupportedUrlHeads
  種類：REG_MULTI_SZ
  データ：<個別の行での値ごと、null区切り：>
  http://
  https://
  file://

  [RcvrForWin4.1_14.1.200から][#LA5255]

- セッションで、Flashインテリジェントフォールバックを無効にすると、Internet Explorerが応答不能になる場合があります。

  [RcvrForWin4.1_14.1.200から][#LA5404]

印刷

- Citrixプリンタードライバー（UPD）では、バーコードフォントは印刷されません。Citrixプリンタードライバー（cpviewer.exe）またはバーコードプリンターを使用して、ドキュメントを印刷するときには、フォントが黒いスペースまたはランダム文字として表示されます。

  [RcvrForWin4.1_14.1.200から][#LC0141]

サーバー/ファームの管理

- ［ファイルリダイレクトの最大帯域幅］および［セッション全体の最大帯域幅］ポリシーが設定されている場合、セッションが予期せずに終了することがあります。

  この問題に対応するには、参照番号#LA5925の修正を含む更新をサーバーとReceiverの両方にインストールして、サーバーで以下のレジストリキーを設定する必要があります。

  - 以下のレジストリキーを作成します。
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    名前：DisableHighThroughput
    種類：DWORD
    値：1
  - 以下のレジストリキーを変更します。
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
    名前：MaxNetCommands
    種類：DWORD
    値：小さい値に設定

  [RcvrForWin4.1_14.1.200から][#LA5925]

セッション/接続

- VDAへのネットワーク接続が切断されて、再接続された場合、マウスのクリックに失敗します。

  [RcvrForWin4.1_14.1.200から][#LA5743]

- COMポートリダイレクトが失敗して以下のエラーメッセージが表示されることがあります。

  「OpenPortでのエラー：COMポート「COM4」」

  [RcvrForWin4.1_14.1.200から][#LC0434]

- VDAに接続されているエンドポイントがスリープ状態から再開すると、VDAセッションでマウスとキーボードが動作しなくなります。

  [RcvrForWin4.1_14.1.200から][#LC0085]

- フォアグラウンドで実行中のWindowsセッションが、予期せずにフォアグラウンドのフォーカスを失う場合があります。

  [RcvrForWin4.1_14.1.200から][#LA5489]

システムの例外

- パススルーセッションのMedia Playerでビデオを再生すると、セッションが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.200から][#LC0553]

ユーザーエクスペリエンス

- フルスクリーンのシームレスなアプリケーションをいろいろな場所に移動させると、スムーズに移動せずにジッターの状態になり、境界上でデスクトップバックグラウンドが表示される場合があります。

  [RcvrForWin4.1_14.1.200から][#LC0696]

- ワイヤレスネットワークにおいて、セッションウィンドウが一時的に、無地の灰色に変わる場合があります。

[RcvrForWin4.1_14.1.200から][#LC0530]

- セッションの音質が［高音質（低パフォーマンス）］（［詳細構成］＞［プロパティ］＞［Client devices］＞［Resources］＞［Audio］＞［Sound quality］＞［高音質（低パフォーマンス）］）に設定されているポリシーが管理するユーザーセッションでは、音声は聞こえません。

  [RcvrForWin4.1_14.1.200から][#LC0329]

- RDSデスクトップセッションで、マルチメディアファイルをループ処理すると、1時間以上経過後にファイルがループ処理された後、音声とビデオストリームが停止します。

  [RcvrForWin4.1_14.1.200から][#LC0641]

- セッションの事前起動は、構成時ではなく、最初にReceiver for Windowsが起動されたときにのみ動作します。

  [RcvrForWin4.1_14.1.200から][#LC0701]

Citrix Receiver for Windows 4.1との比較

Receiver for Windows 4.1.100には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX 3D Pro	サーバー/ファームの管理
HDX MediaStream	セッション/接続
HDX Plug-n-Play	システムの例外
HDX RealTime	ユーザーエクスペリエンス
インストール、アンインストール、アップグレード	ユーザーインターフェイス
印刷	その他

HDX 3D Pro

- H264コーデックおよびテキストトラッキングを無効にしてHDX 3D Proを使用すると、数時間の使用後に、wfica32.exeプロセスがCPUを100%消費している場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5554]

HDX MediaStream

- Internet Explorerなどの公開Webブラウザーを使用して、ストリーミングビデオを表示しようとすると、HDX MediaStrea Flashリダイレクトでの障害により、動作しない場合があります。

  この修正を有効にするには、以下のレジストリキーを設定します。

- *32ビットWindowsの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0
- *64ビットWindowsの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0

[RcvrForWin4.1_14.1.100から][#LA5278]

- HDX Mediastream for Flash Version 1.0（第1世代のFlashリダイレクト）を有効にすると、Adobe Flash Player 11.8以降のインストール時に、Microsoft Internet Explorerが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5421]

HDX Plug-n-Play

- Windows XP SP3にReceiver for Windows 4.0をインストールすると、ドッキングステーションのUSBポートがリダイレクトされなくなる場合があります。

  [RcvrForWin4.1_14.1.100から][#LA4582]

HDX RealTime

- HDX RealTime Webカメラビデオ圧縮リダイレクトが、Quarter Video Graphics Array（QVGA）ディスプレイ解像度（320x240）に対応できなくなり、wfica32.exeプロセスが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5232]

インストール、アンインストール、アップグレード

- インターネットに接続せずに、Receiver for Windowsの最新バージョンにアップグレードすると、以前のバージョンが完全にはアンインストールされず、最新バージョンのインストールに失敗します。

  [RcvrForWin4.1_14.1.100から][#LA4896]

印刷

- これは、ユニバーサルプリンタードライバーを構成するときに、両面印刷が失敗する問題に対応する修正で、代わりに手動で実行する必要があります。

  [RcvrForWin4.1_14.1.100から][#261552]

- Internet Explorer 9を使用して、HTMLドキュメントを印刷しようとすると、Citrix Print Viewer（cpviewer.exe）での出力が文字化けし、特定の種類のフォントで印刷される場合があります。

  [RcvrForWin4.1_14.1.100から][#LA3962]

サーバー/ファームの管理

- StoreFrontが認証不要なストアで構成されている場合、Receiver for Windowsの使用時に、アカウント検出が失敗すること

があります。

[RcvrForWin4.1_14.1.100から][#LC0004]

- この機能拡張では、優先テンプレートディレクトリを使用した、優先アプリケーションのショートカットの自動作成がサポートされています。これらのアプリケーションでは、既存の優先規則のほかに、Self Service Plug-inが、優先テンプレートディレクトリでショートカットを検索します。このショートカットが優先規則に一致している場合、このショートカットをユーザーの［スタート］メニューにコピーします。

  デフォルトでは、このディレクトリは以下のいずれかです。

  - %systemdrive%:\Program Files\Citrix\shortcuts
  - %systemdrive%:\Program Files (x86)\Citrix\shortcuts（ユーザーデバイスのインストールごと）および
  - %systemdrive%:\Users\<ユーザー名>\AppData\Local\Citrix\SelfService\shortcuts（ユーザーインストールごと）。

  デフォルトの優先テンプレートディレクトリの場所は、レジストリで指定できます。

  HKEY_LOCAL_MACHINE\Software\Citrix\DazzleまたはHKEY_CURRENT_USER\Software\Citrix\Dazzle
  名前：PreferTemplateDirectory
  種類：REG_SZ
  データ：任意のパス（たとえば、「%systemroot%:\Shortcuts」など）

  その後、アプリケーションがストアからサブスクリプションを解除されるか、または削除された場合、優先ディレクトリからコピーされたショートカットは削除されます。

  [RcvrForWin4.1_14.1.100から][#LC0005]

セッション/接続

- 仮想デスクトップセッション内でCitrix Receiverを使用すると、XenAppの公開アプリケーションの起動に失敗し、以下のエラーメッセージが表示されます。

  「このバージョンのCitrix Receiverは、選択された暗号化をサポートしていません。管理者に連絡してください。[エラー1029：無効なDLL読み込み]。」

  [RcvrForWin4.1_14.1.100から][#LA4743]

- Receiver for Windows 13.4 Cumulative Update 2において、シームレスなアプリケーションがフォーカスを持った場合、Alt+Tabキーを押してアクティブなウィンドウに切り替えたときに、言語バーの入力言語が変更されます。

  [RcvrForWin4.1_14.1.100から][#LA4963]

- Windows XPシステム上のタスクバーおよび［スタート］メニューのプロパティで、［Group similar taskbar buttons］オプションを選択した場合、アプリケーションの起動が遅くなることがあります。

  [RcvrForWin4.1_14.1.100から][#LA4191]

- Citrix Online Plug-in Version 12.2から、Citrix Receiver for Windows Version 3.xにアップグレードすると、外部Webサイトへのプロキシ接続が、NTLMプロキシ認証を有効にして起動することに失敗する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA3781]

- ユーザーデバイスが、Webカメラに接続されていない場合、Microsoft Lync 2010の公開インスタンスを起動すると、最終的な接続を確立してアプリケーションを起動する前に、アプリケーションが数回、接続と切断を繰り返すことがあります。これが発生するのは、Motorola Bluetoothパッケージなど、ほかのWebカメラがインストールされていないときに、Web

カメラをインストールしたアプリケーションをインストールする場合です。

[RcvrForWin4.1_14.1.100から][#LA4867]

- 公開アプリケーションまたはデスクトップを起動するときに、IPv4ネットワーク上でパススルー認証を使用すると、Kerberos認証が動作しない場合があります。このリリースではIPv4ネットワークの問題のみが修正されます。

  [RcvrForWin4.1_14.1.100から][#LA5026]

- この修正は、Microsoft Lync 2013 VDI Plug-in for Windowsに関連する音声またはビデオの問題に対応しています。この修正により、Lyncユーザーのユーザーエクスペリエンスが向上します。詳しくは、Knowledge CenterのCTX138408を参照してください。

  [RcvrForWin4.1_14.1.100から][#LA5314]

- CANcaseXL USBネットワークアダプターを仮想デスクトップにリダイレクトする場合、Windowsのデバイスマネージャーが正しく動作していないように見えます。このUSBデバイスは、Citrix USBリダイレクトドライバーをサポートしていません。適切に動作させるには、VDAで参照番号#LA5022の修正をインストールする必要があります。

  [RcvrForWin4.1_14.1.100から][#LA5022]

- この修正は、参照番号#LA1257の修正が適用されていますが、以下の問題に完全に対応することはできません。

  Desktop Viewerを無効にすると、フルスクリーンのクライアントセッションで、エンドポイントの画面解像度の変更に応じて、Virtual Desktop Agentの画面解像度を調整できません。

  [RcvrForWin4.1_14.1.100から][#LA4000]

- セッション画面の保持機能のタイムアウト時間を超えたときに、XenDesktopセッションへの接続が切断された場合、DesktopViewerは無制限に画面上に残ります。セッション画面の保持機能のタイムアウト後は、セッション自体が、コネクションセンターに正常に表示されなくなります。

  [RcvrForWin4.1_14.1.100から][#LA4856]

システムの例外

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [RcvrForWin4.1_14.1.100から][#LA3964]

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [RcvrForWin4.1_14.1.100から][#LA4695]

- XenApp 6.5デスクトップからXenApp 4.5公開アプリケーションへのパススルーセッションの起動時に、wfica32.exeプロセスが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA5193]

- マルチストリームポリシーが有効な場合、COMポートにアクセスすると、アプリケーションが応答不能になることがあります。

[RcvrForWin4.1_14.1.100から][#LA5543]

- ダブルホップのシナリオでは、Microsoft OutlookまたはCommunicatorを起動すると、Receiver for Windowsが予期せずに終了する場合があります。

  [RcvrForWin4.1_14.1.100から][#LA4813]

ユーザーエクスペリエンス

- XenApp for Unixでホストされているセッションに接続または再接続すると、90秒間画面の更新が行われません。

  [RcvrForWin4.1_14.1.100から][#LA5244]

ユーザーインターフェイス

- Online Plug-in Version 12.1で導入された変更により、シームレスな接続で接続の進行状況バーの表示が遅延しています。ただし、低速なサーバーに接続するセッションでは、この動作は必ずしも適切であるとは限りません。この機能拡張では、遅延時間を構成できる、以下のレジストリキーをサポートしています。

  32ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：NotificationDelay
  種類：REG_DWORD
  データ：<ミリ秒単位の遅延時間>

  64ビットWindows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
  名前：NotificationDelay
  種類：REG_DWORD
  データ：<ミリ秒単位の遅延時間>

  [RcvrForWin4.1_14.1.100から][#LA0678]

- デスクトップの配色を、デフォルトの青色からほかの色（たとえば、オリーブグリーンやシルバーなど）に変更すると（**[デスクトップ]** > **[プロパティ]** > **[デザイン]** タブ> **[Color scheme]**）、Self-service Plug-inのテキストとバックグラウンドの色が同じになり、メニュー項目を読み取ることができなくなります。

  [RcvrForWin4.1_14.1.100から][#LA5121]

その他

- メールによる検出を使用するときに、DNS側で作成されたSRVレコードに443以外のポートが含まれている場合、ReceiverはSRVレコードで指定されたポートを無視し、引き続きポート443を使用して、Access/NetScaler Gateway URLに接続します。

  [RcvrForWin4.1_14.1.100から][#LA4491]

Citrix Receiver for Windows 4.1との比較

Receiver for Windows 4.1.2には、Receiver for Windows 4.0、4.0.1、4.1に含まれていたすべての修正に加えて、以下の新しい

修正が含まれています。

Microsoft Lync 2013 VDI Plug-in	インストール、アンインストール、アップグレード

Microsoft Lync 2013 VDI Plug-in

- Lyncの会話ウィンドウをセカンダリモニターに移動させると、ビデオが表示されなくなることがあります。

  [#LA5314、#399447]

- ホワイトボードウィンドウを別のユーザーに移動させると、そのユーザーのビデオ映像が会話ウィンドウに表示されなくなることがあります。

  [#LA5314、#399465]

- Receiverが、マルチパーティビデオ呼び出し時またはビデオ会議の終了時に、予期せずに終了する場合があります。

  [#LA5314、#426035]

- 一部のクライアントデバイスでは、フルスクリーンVDAモードのビデオ呼び出しで、ビデオが断続的に使用できなくなります。

  [#LA5314、#418675]

- ビデオ会議ウィンドウを移動すると、ビデオが歪む場合があります。

  [#LA5314、#419898]

インストール、アンインストール、アップグレード

- インターネットに接続せずに、Receiver for Windowsの最新バージョンにアップグレードすると、以前のバージョンが完全にはアンインストールされず、最新バージョンのインストールに失敗します。

  [#LA4896]

Citrix Receiver for Windows 4.0.1との比較

Receiver for Windows 4.1には、Receiver for Windows 4.0、4.0.1に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

HDX MediaStream Flashリダイレクト	印刷
HDX MediaStream Windows Mediaリダイレクト	セッション/接続
HDX Plug-n-Play	システムの例外
インストール、アンインストール、アップグレード	ユーザーエクスペリエンス

キーボード | 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 | その他
ログオン/認証

HDX MediaStream Flashリダイレクト

- いくつかのマルチメディアファイルを、http://www.youtube.com/でHDX MediaStream Flashリダイレクトを有効にして次々に再生すると、PseudoContainer2.exeプロセスが予期せずに終了する場合があります。

  [#LA3846]

HDX MediaStream Windows Mediaリダイレクト

- Receiver for Windows Version 3.4で、HDX MediaStream Windows Mediaリダイレクトを有効にすると、マルチメディアファイルがストリーミングを開始するまでに、最大10秒の遅延が発生する場合があります。

  [#LA4141]

HDX Plug-n-Play

- Desktop Viewer内で［Devices］をクリックし、HDX Plug-n-PlayのUSBデバイスリダイレクトを使用して削除するUSBデバイスを選択すると、Desktop Viewerが応答不能になる場合があります。

  [#LA3348]

インストール、アンインストール、アップグレード

- 管理者以外のユーザーが、Receiver for Windowsをアップグレードしようとしたとき、Receiverが管理者によってインストールされていた場合、Receiverが部分的にしかインストールされないことがあります。

  この修正により、管理者以外のユーザーが、管理者がインストールしたReceiverをアップグレードしようとしたときには、エラーメッセージを受信し、インストールプロセスが終了されます。

  [#LA3425]

キーボード

- Receiver for Windows Version 3.3を使用しているときに、Altキーを押すと、キーがダウン状態のままになる場合があります。結果として、その後に「E」キーを押すと、Windowsエクスプローラーを起動できます。

  [#LA3288]

- フルスクリーンモードでWindowsキーを押して、Desktop Viewerのツールバーをクリックすると、キーがダウン状態のままになる場合があります。結果として、その後にEキーを押すと、Windowsエクスプローラーを起動できます。

  [#LA3349]

- この修正により、ICAセッションにおいて、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。この修正により、新しいパラメーターが導入されています。このパラメーターは、クライアントとサーバーの間でキーボードのLEDの状態を強制的に同期させます。このオプションを有効にするには、ローカルユーザープロファイルのある場所のappsrv.iniファイル、または対応するWeb Interfaceサイトのdefault.icaファイルの[WFClient]セ

クションに「KeyboardForceLEDUpdate = On」を追加します。

[#LA3682]

- この修正により、クライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある、LED同期の問題に対応しています。

  [#LA4293]

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が有効な場合、Desktop Viewerをクリックすると、クライアントのローカルタスクバーが不必要に表示されることがあります。

  [#LA3049]

ログオン/認証

- Windows Server 2008 R2にXenDesktop 7 VDAをインストールすると、パススルー認証が動作しないことがあります。この問題は、ssonsvr.exeプロセスが開始できないことが原因で発生します。

  [#LA4685]

印刷

- 複数のAdobe Acrobat印刷ジョブをセッションプリンターに送信したとき、ランダムなページまたは印刷ジョブ全体が失われる場合があります。

  [#LA3643]

- セッションプリンター列挙に、長い時間を要することがあります。

  [#LA3951]

セッション/接続

- クライアントデバイスが、長時間アクティブなXenDesktopセッションを実行中で、スリープまたは休止状態のときに再開すると、セッションが正常に再接続されず、再接続フェーズでスタックしてしまい、セッションウィンドウを手動で閉じることが必要になる場合があります。

  この修正は、クライアントデバイスを再開するときに、再接続に失敗した場合、セッションウィンドウを正常に閉じる問題に対応しています。

  [#LA2748]

- 公開アプリケーションをシームレスモードで起動するときに、進行状況バーウィンドウがバックグラウンドに残されたままになります。

  修正を有効にするには、クライアント側で以下のレジストリキーを設定します。

  - *Windows 32ビットシステムの場合：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名前：ForegroundProgressBar
    種類：DWORD
    データ：1

- *Windows 64ビットシステムの場合：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名前：ForegroundProgressBar
  種類：DWORD
  データ：1

[#LA3491]

- Desktop Lockとともに使用したReceiverが、ハードウェア障害が発生するたびに、またはVMがハイパーバイザーから強制的にシャットダウンさせられた場合に灰色の画面を表示します。

  [#LA3499]

- クライアントデバイスで、タスクバーでのグループ化を有効にすると、wfica32.exe内のTaskbarGrpXpVista.dllが、クライアントデバイスに対して、セッションで実行中の公開アプリケーションに関する情報を不必要に照会します。たとえば、cmd.exeの公開インスタンスを実行中に、TaskbarGrpXpVista.dllは、実行可能ファイルに関する情報をC:\windows\system32\cmd.exeに照会します。公開アプリケーションがリモート共有から実行されているシナリオの場合、これにより、不適切な帯域幅の消費を引き起こすことがあります。

  [#LA3661]

- GPO設定がタスクバーでのグループ化を回避するように指定されている場合、Windows XPおよびVistaクライアントデバイス上のタスクバーアイコンをクリックすると、関連するウィンドウへのフォーカスの切り替えに失敗します。

  [#LA3889]

- ［Citrix Receiver – Device Access］ダイアログボックスが表示されているときに、Desktop Viewerツールバーの［Devices］ボタンをクリックすると、Receiverが応答不能になる場合があります。このダイアログボックスは、デバイスのアクセス設定が、デフォルトの［何もしない］ではなく、［毎回確認する］に構成されている場合に表示されます。

  [#LA3899]

- Desktop Viewer（CDViewer.exe）およびwfica32.exeプロセスが、仮想デスクトップセッションに再接続中に、予期せずに終了する場合があります。

  [#LA3944]

- この修正により、IsReconnectInProgress() APIが、Citrix Fast Connect 2.0に統合されています。この機能は、クライアントの自動接続機能が有効である場合に、再接続プロセスが進行中であるかどうかを判別します。

  [#LA4080]

- この修正により、パススルーアプリケーションが再接続できるようになり、パススルーアプリケーションのワークスペースコントロールが有効になります。

  この修正を有効にするには、以下のレジストリキーを設定する必要があります。

  パススルーモードでワークスペースコントロールを有効にするには、以下のように設定します。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
  名前：ForceEnableWSC
  種類：DWORD
  データ = 1

パススルーアプリケーションの再接続を有効にするには、以下のように設定します。

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
名前：BypassPassThruMode
種類：DWORD
データ = 1

注：この修正は、以下の条件でのみ機能します。

- 同一のXenApp Servicesサイトまたはファーム内で、2つまたは複数の接続ホップが実行できない場合があります。つまり、エンドポイントのReceiverが、XenApp ServicesサイトAで公開されているXenDesktop VDAに接続できるときに、そのVDA上のパススルークライアントは、*別の*XenApp ServicesサイトBの公開アプリケーションまたはデスクトップに接続できます。
- 2番目の接続ホップは、XenAppターミナルセッションにする必要があります。XenDesktop VDAにすることはできません。

[#LA4206]

- クライアント画面のパーセンテージが奇数（偶数ではない）として公開されているデスクトップ（たとえば、95%）で、リモートアシスタンスソフトウェアを使用しているときに、リモートアシスタンスセッションが歪んでいるように見える場合があります。

  [#LA4313]

- この互換性機能拡張により、別のUSBデバイスへのHDX Plug-n-Play USBデバイスリダイレクトが拡張されます。

  [#LA4335]

- wfcrun32.exeのデッドロックにより、新規セッションが正常に起動しないことがあります。

  [#LA4344]

- Citrixクイックアクセスバーツール、または「HTTPBrowserAddress=ServerName_Or_IP:Port」（たとえば、「HTTPBrowserAddress=192.168.1.10:8080」）と指定した静的なICAファイルを使用して、XenAppサーバーにアクセスしようとすると、失敗する場合があります。

  [#LA4585]

システムの例外

- wfica32.exeプロセスが予期せずに終了し、以下のエラーメッセージが表示される場合があります。

  「Citrix HDX Engineに問題が発生しているので閉じてください。」

  [#LA3412]

- wfica32.exeプロセスで、アクセス違反が発生して、予期せずに終了する場合があります。

  [#LA3639]

- wfica32.exeプロセスが、予期せずに終了する場合があります。

  [#LA4208]

ユーザーエクスペリエンス

- この修正では、Receiver 4.0をStoreFrontとともに使用しているときに、不必要なログオンプロンプトが表示されるのを回避します。

  [#LA4652]

ユーザーインターフェイス

- 公開アプリケーションのアプリケーション名と表示名の間に不一致が存在する場合、アプリケーションの起動に失敗します。

  [#LA3891]

その他

- このリリースには、SSLSDKの最新バージョンであるVersion 12.1.13が含まれています。

  [#LA3804]

- この修正では、一部の展開における、Receiver for WindowsのTerminateUser関数の機能が改善されています。

  [#LA3881]

Citrix Receiver for Windows 4.0との比較

Receiver for Windows 4.0.1には、Receiver for Windows 4.0に含まれていたすべての修正に加えて、以下の新しい修正が含まれています。

- この修正では、Receiver 4.0をStoreFrontとともに使用しているときに、不必要なログオンプロンプトが表示されるのを回避します。

  [#LA4652]

Citrix Receiver for Windows 3.4との比較

Receiver for Windows 4.0には、Citrix Receiver for Windows 3.4と比較して、以下の修正が含まれています。

HDX MediaStream Flashリダイレクト

HDX Plug-n-Play

インストール、アンインストール、アップグレード

キーボード

印刷

シームレスウィンドウ

セッション/接続

システムの例外

ユーザーエクスペリエンス

ユーザーインターフェイス

その他

HDX MediaStream Flashリダイレクト

- ビデオファイルのレンダリング中に、ビデオウィンドウのすべてまたは一部を画面外に移動させると、画面上に暗い領域が残されたままになることがあります。この暗い領域は、ビデオウィンドウを元に戻した後でも残されたままです。

  [#LA0599]

- **重要**：クライアントデバイスにこの修正を適用する前に、Knowledge CenterのCTX126817を参照して、Dynamic Blacklist機能がクライアント側のFlashリダイレクトに与える影響に関する重要な情報を確認してください。

  サーバー上で *[サーバー側のコンテンツの取得を有効にする]* ポリシーを有効にし、クライアント上でFlashリダイレクトポリシーに *[Flashサーバー側でのコンテンツ取得URLリスト]* 設定を構成しているシナリオでは、コンテンツへのURLに2バイト文字/Unicode文字（アジア言語では一般的です）が含まれている場合、Flashコンテンツの再生に失敗します。

  この修正自体を有効にするには、参照番号#LA1621の修正を含むクライアントHotfixと以下のHotfixの両方をインストールする必要があります。

  - *XenAppの場合*：参照番号#LA1621の修正を含むHDX FlashのHotfix
  - *XenDesktの場合*：参照番号#LA1621の修正を含むVirtual Desktop AgentのHotfix

  注：この修正では、クライアントとサーバーの両方にインストールされる、対応する言語コードページも必要になります。このコードページは、Windowsオペレーティングシステムでは、デフォルトでインストールされます。たとえば、Windows 7の日本語版配布では、デフォルトで、日本語コードページがインストールされます。ただし、Windows 7の英語版配布で日本語文字を含むURLを使用する場合、日本語コードページを明示的にインストールする必要があります。サーバー側コンテンツの取得が有効なとき、URLはクライアントからサーバーに転送されるので、これはクライアントとサーバーの両方に適用されます。

  [#LA1621]

- ボタンのクリックなど、Flashコンテンツでの特定のユーザー操作により、Pseudocontainer2.exeが予期せずに終了する場合があります。

  [#LA1948]

- クライアント側でのコンテンツリダイレクトが、特定の種類のFlashコンテンツで失敗し、サーバー側のレンダリングに戻る場合があります。以下のようなケースが含まれます。

  1. Flashコンテンツが、存在しないまたは見つけられない別のFlashファイルのダウンロードを試みた場合
  2. Adobe Captiveで作成されたFlashコンテンツが、クライアント側のコンテンツリダイレクト機能の論理チェックに失敗した場合
  3. Flashコンテンツが、サポートされていないサーバーへのリモートインターフェイスに対して、クライアント側のコンテンツリダイレクト機能を実行した場合
  4. URLがServerContentFetching URLブラックリストで構成されている場合でも、クライアントがFlashコンテンツの取得を試みた場合

  この修正を有効にするには、参照番号#LA2198の修正を含む、HDX FlashとReceiver for Windows Hotfixの両方をインストールする必要があります。上記の問題#1でこの修正を有効にするには、クライアント上で以下のレジストリキーも設定する必要があります。

  - *32ビットWindowsの場合：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名前：FallbackIfFlashNotExist

種類：REG_DWORD
データ：0

- *64ビットWindowsの場合：*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
  名前：FallbackIfFlashNotExist
  種類：REG_DWORD
  データ：0

[#LA2198]

- フォーカスをFlashウィンドウ（シームレスウィンドウを実行中のWebブラウザーの子ウィンドウ）からローカルウィンドウに切り替え、またフォーカスをシームレスなブラウザーウィンドウのアドレスバーに戻したときに、ブラウザーのアドスバーへの入力に失敗する場合があります。

  [#LA2685]

- 重要：クライアントデバイスにこの修正を適用する前に、Knowledge CenterのCTX126817を参照して、Dynamic Blacklist機能がクライアント側のFlashリダイレクトに与える影響に関する重要な情報を確認してください。

  HDX MediaStream Flashリダイレクト機能が、Dailymotionビデオ（http://www.dailymotion.com）ではエラーが発生して、動作に失敗することがあります。この問題が発生するのは、クライアントとサーバーが、別の地理的場所に配置されている場合です。

  この修正を有効にするには、以下のレジストリキーを作成する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
  名前：DisableRegionFiltering
  種類：REG_DWORD
  データ：1

  [#LA3134]

HDX Plug-n-Play

- この機能拡張では、デフォルトのUSBリダイレクト動作が、以下のように変更されます。
  - Desktop Viewerが有効な場合、ユーザーはUSBデバイスを手動でリダイレクトできます。
  - Desktop Viewerが有効ではない場合、USBデバイスは自動的にリダイレクトされます。

  [#LA0108]

- 特定のUSBデバイスを、仮想デスクトップセッションにマップできなかった場合、エンドポイントを再起動するまで、デバイスマネージャーにデバイスが表示されません。

  [#LA0954]

- Desktop Viewer内で［デバイス］をクリックし、HDX Plug-n-PlayのUSBデバイスリダイレクトを使用して削除するUSBデバイスを選択すると、Desktop Viewerが応答不能になる場合があります。

  [#LA3348]

インストール、アンインストール、アップグレード

- Receiver 3.*x*へのアップグレード後、公開アプリケーションを起動することができず、以下のエラーメッセージが表示されます。

「このバージョンのCitrix Receiverは、選択された暗号化をサポートしていません。管理者に連絡してください。エラー1046：仮想ドライバーが読み込まれていません。」

[#LA3120]

キーボード

- Desktop Viewerの［ホーム］をクリックして、仮想デスクトップセッションを最小化すると、セッションが切断されるまで、エンドポイントでTabキーが断続的に動作を停止する場合があります。

  [#LA2925]

- Receiver for Windows　Version 3.0の時点では、KeyboardTimerの以下の設定値は動作しません。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard。この修正により、機能が再度有効になります。

  [#LA2949]

- この修正により、フォアグラウンドで実行中のパススルーセッションのクライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。

  [#LA3288]

- この修正により、バックグラウンドで実行中のパススルーセッションのクライアントとサーバーの間で、Caps Lock、Num Lock、およびScroll Lockキーの状態の同期が乱れることがある問題に対応しています。

  [#LA3310]

印刷

- **［クライアント設定］**タブで **［ローカルプリンター設定］**をクリックして、UPDプリンターの **［プロパティ］**シートを開きます。次に、設定ダイアログボックスを閉じると、 **［プロパティ］**シートが応答不能になることがあります。

  [#259485]

シームレスウィンドウ

- コネクションセンターまたはWeb Interfaceを使用して、データを保存せずにシームレスなセッションからログオフすると、画面が黒くなり、以下のようなメッセージが表示されます。

  「プログラムを閉じる必要があります。2つのオプション［ログオフを強制する］または［キャンセル］から選択してください。」このときに、［キャンセル］オプションが動作しません。

  この修正をインストールすると、［キャンセル］オプションが正常に動作するようになります。［キャンセル］ボタンの利用後は、これ以上パフォーマンスを低下させないために、データを保存して、セッションからログアウトすることをお勧めします。

  [#LA0318]

セッション/接続

- 仮想デスクトップセッションから切断して再接続すると、セッション内からの音声の記録に失敗することがあります。この問題を解決するには、サーバー側にも参照番号#LA0821に対する修正をインストールする必要があります。

  [#LA0821]

- クライアントセッションでファイルの転送に要する時間が、RDPセッションの場合より長くなることがあります。

  この問題を解決するには、サーバー側にも参照番号#LA1263に対する修正をインストールする必要があります。

  [#LA1263]

- 特定の条件下では、仮想デスクトップセッションの解像度を変更した後で、セッションが予期せずに切断されると（ネットワーク障害などによる）、再接続した後にセッション解像度が予期していた設定とは異なっていることがあります。

  [#LA1377]

- シリアルポートバーコードスキャナーは、512バイトを越えるサイズのラベルデータを処理できません。この修正を有効にするには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：CommBufferSize
  種類：REG_DWORD
  データ：512（最小）～2048（最大）の範囲の値

  [#LA1695]

- Knowledge CenterのCTX131577の説明に従って、Network List ServiceまたはNetwork Location Awarenessサービスを無効にすると、Online Plug-in Version 12.3が切断されます。

  [#LA2024]

- 狭帯域幅の接続を介して、UNCパスに公開されているシームレスなアプリケーションを起動しようとすると、完了するまで2分を超えてしまう場合があります。

  [#LA2170]

- Ctrl+Shiftキーをクリックして、シームレスなセッションの入力方法を起動させると、クライアント側のローカルの入力方法も変更されることがあります。この問題を回避するには、以下のレジストリキーを設定する必要があります。

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：Showlocallanguagebar
  種類：REG_DWORD
  データ：1 <*ローカル言語バーを表示する*>、0 <*ローカル言語バーを非表示にする*>

  [#LA2180]

- 自動クライアントリダイレクトを有効にすると、休止状態を選択した後、クライアントが自動的に閉じられたときに、再接続に失敗することがあります。

  この修正により、システムはUSBデバイスリダイレクトにより、一時停止するかまたは休止状態モードに移行し、システムがスタンバイモードから復帰した後に、自動的に再接続することができます。

  [#LA3061]

- Citrix Receiver for Windows 3.xで、ICA圧縮が「OFF」に設定されている場合、公開アプリケーションが起動に失敗することがあります。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off。

[#LA3072]

- マルチモニター環境では、フルスクリーンモードでディスプレイを2番目のモニターに切り替えている間、Desktop Viewe ツールバーが表示されなくなることがあります。

  [#LA3083]

- 2つのモニターがVirtual Desktop Agentに接続されており、プライマリモニターがラップトップであるデュアルモニター構成では、ラップトップのディスプレイをオフにしてまたオンに戻すと、その後のセッションはプライマリモニターのディスプレイのみで行われます。

  [#LA3202]

- Internet Explorer 8を実行中のWindows XPワークステーションで、Receiver for Windows Version 3.3またはVersion 3.4 Cumulative Update 1を使用すると、Web Interfaceから最初のアプリケーションの起動に失敗することがあります。

  [#LA3234]

- Receiver for Linuxを使用して、切断されている仮想デスクトップセッションに再接続しようとすると、コンソールおよびXenDesktopの両方のセッションが応答不能になることがあります（［ようこそ］画面でのスタック）。この問題が発生するのは、Virtual Desktop AgentでWDDMドライバーが有効にされており、セッション内で別の仮想デスクトップセッションが実行されている場合です。

  [#LA3241]

- Windows 7でクライアントの［地域と言語のオプション］が［Kazakh（Kazakhstan）］に設定されている場合、Receiver for Windows Version 3.4が起動に失敗することがあります。

  [#LA3517]

システムの例外

- EdgeSight for Load Testingが展開されている環境では、wfica32.exeプロセスが予期せずに終了する場合があります。

  [#LA0289]

- HP LoadRunnerが展開されている環境では、wfcrun.exeプロセスが予期せずに終了する場合があります。

  [#LA0859]

- オーディオポリシーが高品位オーディオに設定されている場合、公開デスクトップの［サウンド］コントロールパネルでランダムにサンプルサウンドファイルを再生すると、wfica32.exeプロセスが予期せずに終了することがあります。

  [#LA1000]

- Microsoft Excel 2007スプレッドシートが開かれている状態で、Web Interfaceサイトからセッションを切断すると、Online Plug-in Version 12.3が予期せずに終了する場合があります。

  [#LA2274]

- ローカルアプリケーションアクセスが有効で、Virtual Desktop Agentで法的通知が構成されている場合、Virtual Desktop Agentへの接続に失敗することがあります。

  [#LA2351]

- セッションへの再接続時に、Pnamain.exeプロセスが予期せずに終了する場合があります。

  [#LA2704]

- 単一モニターで実行中のセッションでは、Aeroが有効なWindowsクライアントデバイスが予期せずに切断される場合があります。この問題が発生するのは、動的ウィンドウプレビュー機能の一部として、クライアントにプレビューが送信された場合です。その時点で、twi3.dllスレッドがWinlogon.exeプロセスを終了し、次にセッションが切断されることがあります。

  この問題を解決するには、サーバー側にも参照番号#LA2858に対する修正をインストールする必要があります。

  [#LA2858]

- wfica32.exeプロセスが、予期せずに終了する場合があります。この問題は、無効なメモリ逆参照によるものです。

  [#LA2860]

- 特定のダブルホップシナリオでの印刷中に、以下のエラーメッセージが表示され、Wfica32.exeプロセスが予期せずに終了します。「Citrix HDX Engineが動作を停止しました。」この問題は、ポート名の長さが260文字を超えていることによるものです。

  この問題に対応するには、参照番号#LA3009の修正を含む、サーバーHotfixおよびReceiver Hotfixの両方をインストールする必要があります（XA650R01W2K8R2X64056; RcvrForWin3.3_13.3.104、またはその置き換えHotfix）。

  [#LA3009]

- Citrix Receiverが、selfserviceplugin.exeプロセスの複数のインスタンスを生成し、システムのメモリが不足することがあります。

  [#LA3460]

- ログオフ時、Desktop Viewerが予期せずに終了する場合があります。

  [#LA3567]

- Online Plug-inをパススルークライアントとして使用しているときに、PNMain.exeが予期せずに終了する場合があります。

  [#LA0785]

ユーザーエクスペリエンス

- USBリダイレクトの使用時、数時間後にUSB SpaceMouseデバイスが、仮想デスクトップセッションに表示されなくなることがあります。

  [#LA2256]

- Receiver for Windows Version 3.4のこの機能拡張では、ユーザーがネットワーク接続を切り替えたときに表示される、VPN ログインに対する以下の認証メッセージの表示を抑制できます。

  メッセージが表示されないようにするには、以下のレジストリキーを作成します。

  - *32ビットWindowsの場合*：
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    名前：AutoSecureConnection
    種類：REG_DWORD

値：0（VPnプロントを無効化）

- *64ビットWindowsの場合*：
  HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
  名前：AutoSecureConnection
  種類：REG_DWORD
  値：0（VPnプロントを無効化）

[#LA3772]

ユーザーインターフェイス

- この修正では、具体的には、Desktop Viewerツールバーの［ホームデスクトップ］アイコンタイトルの韓国語表示を修正します。

  [#232198]

- エンドポイントでデスクトップグループショートカットの実行中に表示される、認証ダイアログボックス**[キャンセル]**をクリックすると、以下の不正確で不適切なエラーメッセージが表示されます。

  参照されているアプリケーションが見つかりません。ネットワーク接続を確認してください

  [#259081]

- 最大化されたセッションウィンドウで、［セッション/接続］画面が表示されなくなった*後*、USBMultiInsertDialogueダイアログボックスの**[接続]**をクリックすると、Desktop Viewerツールバーが、適切に表示されない場合があります。

  [#260390]

- icaclient.admの［クライアント側ドライブのマッピング］の［ヘルプ］トピックでは、「ポリシーはユーザーの選択を上書きしない」と誤って記述されています。ポリシーはユーザーの選択を上書きします。

  [#LA0398]

- 特定のカスタムアプリケーションでは、SpeedScreen機能のローカルテキストエコー編集ボックスに入力中、黒いバーが表示されます。

  [#LA0544]

- Merchandising Serverからの最初の配信に成功した後、「ようこそ」または補完メッセージが表示されません。

  [#LA2277]

- 公開アプリケーションの起動時に、Windowsタスクバーの通知領域のTivoli Access Manager for Enterprise Single Sign-On（TAM ESSO）アイコンが、予期せずに表示されなくなる場合があります。

  [#LA3190]

- ローカルタスクバーが、自動的に隠すように設定されており、その後に画面のデフォルトの場所から上部、左側、または右側に移動された場合は、アクセスできなくなります。

  [#LA3400]

その他

- UDPオーディオストリームの再生時に、wfica32.exeプロセスのハンドル数が大幅に増加する場合があります。

[#LA3094]

- この修正により、Receiver for Web 3.3ではProgram Neighborhood Web Interface 5.4サイトは1つであるという制限が削除されます。

  [#LA3142]