このリリースについて

新機能

-
-
-
-
-
-
-
-
-
  -
  -
  -
-

-
-

このリリースで解決された問題について

このリリースの既知の問題について

Citrix Receiver for Windows 4.2で解決された問題

Receiver for Windows 4.2.100

-
-
-
-
  -

-
-
  -
  -
  -
-
-
-
-
  -
  -
-
-

-
-
-
-
-
-
-
-
-

-
-

Receiver for Windows 4.2

-
-

-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
  -
  -
-

-
-
-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -

-
-
-
-
-

Citrix Receiver for Windows 4.2の既知の問題

既知の問題

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-

-
-
-

システム要件

デバイス

オペレーティングシステム

-
-
-
-
-
-
-
-
-
-

ハードウェア

-
-
-

タッチ操作可能なデバイス

Citrixサーバー

-
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
  -

Webブラウザー

Connectivity

-
  -
  -
  -
  -
  -

セキュリティが保護された接続と証明書について

認証

アップグレード

Other

-
  -
  -
  -
-
-
  -

-

Receiver for Windowsのインストール

-
  -
-
  -
  -
-
  -
-
  -

Receiver for Windowsの手動アップグレード

-
-
-
-

アップグレード時の注意事項

Version 3.4から4.2.100へのアップグレードの重要な注意事項

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

Receiver for Windowsの削除

-
  -
  -
-
  -
  -

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

-
-
-
-

-
  -
  -
  -
  -
  -
  -

-
-

-
-
-
-
-
-

-
  -
  -
  -
  -
  -
    エレメントからURLをコピーします。
  -
  -
  -
  -
  -

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"

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

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

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 for Windowsの展開

-
-

サンプルスクリプトを変更するには

- set DesiredVersion= 3.3.0.<XXXX>
-
-
-

コンピューター単位のスタートアップスクリプトを追加するには

Receiverをコンピューター単位で展開するには

Receiverをコンピューター単位で削除するには

ユーザー単位のスタートアップスクリプトを設定するには

-
-

Receiverをユーザー単位で展開するには

Receiverをユーザー単位で削除するには

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

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

Receiver for Windowsの構成

-
-
-
  -
  -
  -
-
-

セルフサービスモードの構成

-
-

StoreFrontの構成

アプリケーション配信の構成

-
-
-

セルフサービスモードの構成

-
-
-

アプリケーションショートカットの場所のカスタマイズ

SelfServiceMode true SelfServiceMode false

- SelfServiceMode false
-
-
-
- UseCategoryAsStartMenuPath
- [/DESKTOPDIR="Dir_name"] CategoryPath
- AutoReInstallModifiedApps

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

-
-
-
-
-
-
-

アプリケーションショートカットをカスタマイズするためのレジストリキーの使用

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

-
-
-

-
-

-
-
-

XenAppおよびXenDesktop 7.xのアプリケーションごとの設定を使ったアプリケーションショートカットの場所のカスタマイズ

XenAppのアプリケーションごとの設定を使った、アプリケーションショートカットの場所のカスタマイズ

列挙遅延またはアプリケーションスタブデジタル署名の削減

ユースケースの例

ローカルアプリケーションアクセスのアプリケーションの構成

-

- -

-

-

-

XenDesktop環境の構成

XenDesktopおよびXenApp接続のUSBサポートの構成

USBサポートのしくみ

マスストレージデバイス

デフォルトで許可されるUSBデバイスのクラス

-

-
-
-
-
  -
  -
  -
  -
  -
  -
  -
-
-
-
-

デフォルトで拒否されるUSBデバイスのクラス

-
-
-
-
-
-

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

Bloombergキーボードの構成

-
-

非アクティブなDesktop Viewerウィンドウの減光を無効にするには

-
-

-
-

複数のユーザーおよびデバイスの設定を構成するには

-
-
-

StoreFrontの構成

StoreFrontを構成するには

グループポリシーオブジェクトテンプレートによるReceiverの構成

-
-
-
-

SalesStore;https://sales.example.com/Citrix/Store/discovery;On;営業スタッフ用のストア

ユーザーへのアカウント情報の提供

-
-
-

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

-
-
  -
  -

<NetScalerGatewayFQDN>?<MyStoreName>

Receiver環境の最適化

アプリケーションの起動時間の短縮

-
-

-
-

HKEY_LOCAL_MACHINE値

HKEY_CURRENT_USER値

クライアント側デバイスのマッピング

-
-
-

デバイスマッピングを無効にする

クライアントフォルダーのリダイレクト

クライアントドライブをホスト側のドライブ文字にマップする

HDX Plug-n-Play USBデバイスリダイレクト

クライアントのCOMポートをサーバーのCOMポートにマップするには

DNS名前解決をサポートする

特定のユーザーデバイスのDNSアドレス解決を無効にするには

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。

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。

Receiverでは、最大で8つのモニターがサポートされます。

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］、［ディスプレイの設定の変更］の順に選択して確認します。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。

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。

Windowsタブレットから仮想アプリケーションおよびデスクトップへのタッチ操作によるアクセスを有効にするため、テキスト入力フィールドがアクティブになったり、デバイスがテントまたはタブレットモードになったりすると、Receiverによって自動的にスクリーンキーボードが表示されます。

一部のデバイスおよび一部の環境下では、Receiverがデバイスのモードを正確に検出できず、必要時にスクリーンキーボードが表示されないことがあります。

変換可能なデバイス（取り外し可能なキーボード付タブレット）を使っている場合にスクリーンキーボードの表示を抑制するには、REG_DWORD値DisableKeyboardPopup in HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiverを作成し、値を1に設定します。
注：x64マシンでは、HKLM\SOFTWARE\Wow6432Node\ Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiverに値を作成します

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。

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。

企業組織にはそれぞれ異なるニーズがあります。ユーザーが仮想デスクトップにアクセスする方法の要件は、ユーザーによって、そして企業ニーズが展開するにつれて変化する可能性があります。ユーザーが仮想デスクトップに接続したり接続を構成したりするときの手順は、管理者によるReceiver for Windowsのセットアップ方法によって異なります。

ユーザーが仮想デスクトップを操作する必要がある場合は、**Desktop Viewer**を使用します。ユーザーの仮想デスクトップは公開仮想デスクトップにすることができ、または共有デスクトップや専用デスクトップにもすることができます。このアクセスシナリオでは、Desktop Viewerツールバー機能により、ユーザーが仮想デスクトップをローカルデスクトップ上のウィンドウ内に開いて、必要に応じて仮想デスクトップの表示領域や表示サイズを変更できます。ユーザーは必要に応じて設定を変更でき、同じユーザーデバイス上で複数のXenDesktop接続を使用して複数の仮想デスクトップを実行できます。

注：仮想デスクトップの解像度を変更する場合は、Citrix Receiverを使用する必要があります。Windowsコントロールパネルで解像度を変更することはできません。

Desktop Viewerセッションでは、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。

ドメインパススルー認証の構成

Nov 19, 2015

このトピックでは、XenDesktopまたはXenAppでCitrix Receiverのドメインパススルー認証を有効にする方法について説明します。

注：この例では、Receiverのインストール、コンピューターポリシーのアプリケーション、およびクライアントオペレーティングシステム上の信頼されているサイトの構成は手動で実行されます。グループポリシーオブジェクト（GPO）テンプレートをいったん構築したら、それをReceiverがインストールされているいずれのドメインクライアントマシンにも適用できます。

1. Citrix Receiver 4.2を/includeSSONスイッチでインストールします。
    1. 1つまたは複数のStoreFrontストアをインストールします。この手順は後で完了することができます。StoreFrontストアをインストールしても、ドメインパススルー認証のセットアップの前提条件とはなりません。1つまたは複数のStoreFrontストアを追加するための構文については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。
    2. Citrix Receiverの起動によりパススルー認証が有効となっているかチェックし、**ssonsvr.exe**処理が実行中かを確認します。
2. ICAクライアントGPO管理テンプレートをユーザーのローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方のローカルコンピューターポリシーに追加します。
    1. **gpedit.msc**を開きます。
       注：グループポリシーエディタースナップインのgpedit.mscは、Windows 7およびWindows 8のProfessional、Enterprise、およびUltimateエディションで利用できます。
    2. ［コンピューターの構成］、［管理用テンプレート］の順にアクセスして右クリックし、［テンプレートの追加と削除］を選択します。
    3. **C:\Program Files\Citrix\ICA Client\Configuration\icaclient.adm**テンプレートを追加します。
3. ユーザーのローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方で次のローカルコンピューターGPOを有効にします。
    1. ［Localuser nameand password］を選択します。
    2. ［有効］をクリックします。
    3. ［Enable pass-through authentication］チェックボックスをオンにします。
    4. ［Allow pass-through authentication for all ICA connections］チェックボックスをオンにします。
    5. ［OK］をクリックします。
    6. VDAデスクトップゴールドイメージを再起動します。
4. Delivery Controllerにログオンし、Windows PowerShellを開いて次のコマンドを実行し、Delivery ControllerがStoreFrontから送信されるXML要求を信頼できるようにします。
    1. Citrixコマンドレットが読み込まれていない場合は、「asnpCitrix*」と入力してこれを読み込みます（Citrix*のあとにはピリオド「.」を含めてください）。
    2. Enterキーを押します。
    3. 次のコマンドを入力します：Add-PSSnapin citrix.broker.admin.v2Enterキーを押します。
    4. 次のコマンドを入力します：Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $TrueEnterキーを押します。
    5. PowerShellを閉じます。
5. ローカルマシンまたはVDAデスクトップゴールドイメージ、あるいはその両方でInternet Explorerを開きます。
6. ［インターネットオプション］、［セキュリティ］、［信頼済みサイト］の順に選択し、ストアパスのないStoreFrontサーバーの完全修飾名を一覧に追加します。例。https://storefront.example.com
   注：またMicrosoft GPOを使って、StoreFrontサーバーを信頼済みサイトに追加することもできます。GPOはゾーンの割り当て一覧へのサイトと呼ばれ、［コンピューターの構成］、［管理用テンプレート］、［Windowsコンポーネント］、［Internet Explorer］、［インターネットコントロールパネル］、［セキュリティページ］の順に選択してアクセスできま

す。

7. いったんログオフしてから、再度Receiverにログオンします。

Citrix Receiverを開くと、現在のユーザーがドメインにログオンしている場合は、ユーザーの資格情報がStoreFrontにパススルーされ、ユーザーの［スタート］メニューに加えてCitrix Receiver内にアプリやデスクトップが列挙されます。ユーザーがアイコンをクリックすると、Receiverがユーザーのドメイン資格情報をDelivery Controllerにパススルーし、アプリまたはデスクトップが開きます。

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には

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、DisableCtrlAltDelをfalseに設定します。
  注：すべてのクライアントマシンでReceiver for Windows 4.2以降を実行している場合には、この手順は必要がありません。
- StoreFrontサーバーの認証サービスを構成するときに、［ドメインパススルー］チェックボックスをオンにします。これにより、統合Windows認証が有効になります。［スマートカード］チェックボックスは、スマートカードを使用してStoreFrontに接続する非ドメイン参加のクライアントをサポートする場合のみオンにします。

StoreFrontでスマートカードを使用する場合は、StoreFrontドキュメントの「認証サービスの構成」を参照してください。

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。これを実行できるようにするには、スマートカードを許可するためDisableCtrlAltDelメソッドをFalseに設定して、サイトごとに専用ストアをセットアップする必要があります。2モード認証にはStoreFront構成が必要です。NetScaler Gatewayが解決策にある場合、構成する必要もあります。
  また2モード認証により、StoreFront管理者はStoreFrontコンソールで選択して同じストアにエンドユーザーにユーザー名とパスワードの両方とスマートカード認証を提供できます。StoreFrontのドキュメントを参照してください。

- **複数の証明書** – 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。ユーザーがスマートカードをリーダーに挿入すると、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はユーザー証明書を保存しませんが、構成時にPINを格納できます。PINはユーザーセッションの間

に非ページ化メモリにのみキャッシュされ、ディスク内にはどの時点においても格納されません。
- 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。
- 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\

または、Kerberosの代わりにStorefrontに対してスマートカード認証を有効にできます。Kerberosの代わりにStorefrontに対してスマートカード認証を有効にするには、次のコマンドラインオプションでReceiverをインストールします。これには管理者権限が必要です。マシンをドメインに参加させる必要はありません。

- /includeSSONを指定すると、シングルサインオン認証（パススルー認証）がインストールされます。資格情報のキャッシュおよびパススルードメインベース認証の使用を有効にします。
- Receiverのスマートカード認証とは別の方法（ユーザー名とパスワードなど）でユーザーがエンドポイントにログオンしている場合、コマンドラインは次のようになります。
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  これによりログオン時に資格情報がキャプチャされるのを防ぎ、Receiverへのログオン時にPINを格納することができます。

- グループポリシーエディターで、［コンピューターの構成］、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［User authentication］、［Local user name and password］の順に選択します。
  Enable pass-through authentication。構成およびセキュリティ設定によっては、パススルー認証を実行するために［Allow pass-through authentication for all ICA］チェックボックスをオンにする必要があります。

StoreFrontを以下のように構成します。

- 認証サービスを構成する場合、［Smart card］チェックボックスをオンにします。

StoreFrontでスマートカードを使用する場合は、StoreFrontドキュメントの「認証サービスの構成」を参照してください。

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、TLSハンドシェイク時にサーバーから送信される、許可される識別名（DN）の1つに合致している。

証明書の選択方法を変更するには、以下のいずれかの構成を行います。

- 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には

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、TLSサーバーの暗号化認証機能が強化され、ユーザーデバイスとサーバー間のTLS接続のセキュリティが向上します。

証明書失効一覧のチェック機能には、いくつかの設定レベルが用意されています。たとえば、ローカルの証明書失効一覧だけがチェックされるように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。

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」とも呼ばれます）。プロキシサーバーでネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Receiverとサーバー間の接続を制御できます。Receiverは、SOCKSプロトコルとSecureプロキシプロトコルをサポートしています。
- XenAppまたはWeb Interface展開環境では、TLS（Transport Layer Security）プロトコルを使用するCitrix SSL Relay（XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には適用されません）。
- XenApp 7.6およびXenDesktop 7.6の場合、ユーザーとVDA間で直接SSL接続を有効にできます（XenApp 7.6またはXenDesktop 7.6に対するSSL構成については、「SSL」を参照してください）。

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

Oct 31, 2016

リモートのユーザーがNetScaler Gatewayを介して接続できるようにするには、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。

接続の構成方法については、Citrix製品ドキュメントの「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、Citrix製品ドキュメントの「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

Oct 31, 2016

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製品ドキュメントの「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、Citrix製品ドキュメントの「Configuring Access Gateway Enterprise Editior 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。

ファイア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（TLS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。

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 (SSL) Relayによる接続

Nov 19, 2015

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

ReceiverをCitrix SSL（Secure Sockets Layer）Relayサービスと一緒に使うことができます。ReceiverはTLSプロトコルをサポートします。Receiver for Windows 4.2はTLS 1.0のみをサポートします。

- 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。米国政府など、データ通信を保護するためにTLSの使用を必須としている組織もあります。このような組織では、さらにFIPS 140（Federal Information Processing Standard）などのテスト済み暗号化基準の使用を義務付けられる場合があります。FIPS 140は、暗号化の情報処理規格です。

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

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

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

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

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

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、XenDesktop 7.1、XenDesktop 7.5、またはXenApp 7.5には該当しません。

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。

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。

1. TLSでアプリケーション一覧を暗号化して、そのデータを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。

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。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、ReceiverはTLS暗号化を使用して接続します。
   - ［SSL 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。
   - ［TLS version］で［TLS v1.0］または［Detect version］を選択してTLSを有効にします。［Detect version］を選択した場合、ReceiverはTLS暗号化を使用して接続します。
   - ［SSL 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。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。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。

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。TLSを使って設定データを暗号化するには、サーバーURLを「https://<servername>」の形式で入力します。
4. ［更新］をクリックして変更を適用します。
5. ユーザーデバイス上のWebブラウザーでTLSを有効にします。詳しい設定方法については、Webブラウザーのヘルプを参照してください。

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、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。

信頼済みサイトにWeb Interfaceのサイトを追加するには

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

レジストリでクライアントリソースのアクセス許可を変更するには

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

値	説明
0	アクセスなし

値	説明
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 Desktop Lock

Nov 19, 2015

ユーザーがローカルのデスクトップを操作する必要がない場合は、Receiver Desktop Lockを使用できます。ユーザーはDesktop Viewer（有効な場合）を引き続き使用することはできますが、ツールバー上には必須オプションセットであるCtrl+Alt+Del、基本設定、デバイス、および切断しかありません。

Receiver Desktop Lockなら、SSONが有効（Single Sign-On）でストアが構成されたドメイン参加のマシンで実行できます。Program Neighborhoodエージェントサイトはサポートしません。以前のバージョンのDesktop Lockは、Receiver for Windows 4.2.xへアップグレードするとサポートされません。

Citrix Receiver for Windowsを/includeSSONフラグを使ってインストールする必要があります。admファイルまたはコマンドレットオプションのいずれかを使って、ストアおよびシングルサインオンを構成する必要があります。

次に、管理者としてcitrix.com/downloadsにあるCitrixReceiverDesktopLock.MSIを使ってReceiver Desktop Lockをインストールします。

Citrix Receiver Desktop Lockのシステム要件

- Windows XP（Embedded Edition）、Windows 7（Embedded Editionを含む）、Windows 7 Thin PC、Windows 8、およびWindows 8.1でサポートされます。
- ネイティブプロトコルのみを介してStoreFrontに接続します。
- ドメイン参加のエンドポイントです。
- ユーザーデバイスをローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）に接続する必要があります。

注：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日に終了しました。

ローカルアプリケーションアクセス

注意：ローカルアプリケーションアクセスを有効にすると、グループポリシーオブジェクトテンプレートまたは同様のポリシーでフルロックダウンが適用されていない限り、ローカルデスクトップアクセスを実行できます。詳しくは、XenAppおよびXenDesktopのドキュメントで「ローカルアプリケーションアクセスとURLリダイレクトの構成 」を参照してください。

Receiver Desktop Lockの実行

- Receiver Desktop Lockを使って次のReceiver for Windowsの機能を実行できます。
  - 3Dpro、Flash、USB、HDX Insight、Microsoft Lync 2013プラグイン、およびローカルアプリケーションアクセス
  - ドメイン、2要素、またはスマートカード認証のみ
- Receiver Desktop Lockセッションを切断するとエンドデバイスをログアウトします。
- FlashのリダイレクトはWindows 8以降では無効です。Windows 7では有効です。
- Desktop ViewerはHome、Restore、Maximize、およびDisplayプロパティがないReceiver Desktop Lockに最適化されています。
- Viewerのツールバーでは、Ctrl+Alt+Delキーの組み合わせを使用できます。
- Windows+Lキー以外のほとんどのWindowsショートカットキーをリモートセッションで実行できます。詳しくは、「リモートセッションでのWindowsショートカットキーの実行」を参照してください。
- 接続を無効にするまたはデスクトップ接続のDesktop Viewerを無効にする場合、Ctrl+F1キーを押すとCtrl+Alt+Delを押すのと同じように動作します。

Receiver Desktop Lockをインストールするには

この手順に従ってReceiver for Windowsをインストールすると、Receiver Desktop Lockで仮想デスクトップが表示されます。スマートカードを使用する展開については、「Receiver Desktop Lockを実行するデバイスでスマートカードを使用できるように構成するには」を参照してください。

1. ローカルの管理者アカウントを使用してログオンします。

2. コマンドプロンプトで次のコマンド（インストールメディアのCitrix Receiver and Plug-ins > Windows > Receiverフォルダーにあります）を実行します。
   Receiver for Windows 4.2の場合：
   CitrixReceiver.exe /includeSSON STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   コマンドの詳細については、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」でReceiver for Windowsのインストールに関する説明を参照してください。

3. インストールメディアの同じフォルダーにあるCitrixReceiverDesktopLock.MSIをダブルクリックします。Desktop Lockウィザードが開きます。画面の指示に従って操作します。
4. インストールが完了したら、ユーザーデバイスを再起動します。デスクトップへのアクセスが許可されていて、ドメインユーザーとしてログオンすると、Receiver Desktop Lockでデスクトップが表示されます。

ただし、インストールの完了後にユーザーデバイスを管理できるようにするため、CitrixReceiverDesktopLock.msiをインストールしたときのアカウントでは代替シェルが使用されません。このアカウントを削除すると、デバイスにログオンして管理することができなくなります。

Receiver Desktop Lockの**サイレントインストール**を実行するには、次のコマンドラインを使用します。msiexec /i CitrixReceiverDesktopLock.msi /qn

Receiver Desktop Lockを構成するには

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

Active Directoryポリシーを使用して、ユーザーが仮想デスクトップを休止状態にできないようにします。

Receiver Desktop Lockを構成するときは、インストール時に使用した管理者アカウントを使用します。

- icaclient.admファイルとicaclient_usb.admファイルがグループポリシーにロードされていることを確認します（ポリシーは［コンピューターの構成］または［ユーザーの構成］、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］の順に展開すると表示されます）。これらのADMファイルは、%Program Files%\Citrix\ICA Client\Configuration\にインストールされています。
- USB基本設定 — ユーザーがUSBデバイスを接続すると、そのデバイスは自動的に仮想デスクトップで使用可能になります。このとき、ユーザーが何らかの操作を行う必要はありません。USBドライブの制御と表示は、仮想デスクトップにより処理されます。
  - USBポリシー規則を有効にします。
  - ［Citrix Receiver］、［Remoting client devices］、［Generic USB Remoting］の順に選択して、Existing USB DevicesとNew USB Devicesポリシーを有効にして構成します。
- ドライブマッピング — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client drive mapping］ポリシーを有効にして構成します。
- マイク — ［Citrix Receiver］、［Remoting client devices］の順に選択して、［Client microphone］ポリシーを有効にして構成します。

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

1. StoreFrontを構成します。
   1. Citrix XML ServiceのDNSアドレス解決を有効にして、Kerberos認証を使用できるように構成します。
   2. StoreFrontサイトのHTTPSアクセスを構成して、ドメインの証明機関による署名付きのサーバー証明書を作成し、デフォルトのWebサイトにHTTPSバインドを追加します。
   3. ［スマートカードパススルー認証］が有効になっていることを確認します（デフォルトで有効になっています）。
   4. ［Kerberos］を有効にします。
   5. ［Kerberos］および［スマートカードパススルー認証］を有効にします。
   6. IISのDefault Web Siteで［匿名アクセス］を有効にして、［統合Windows認証］を使用します。
   7. IISのDefault Web SiteのSSL設定で［SSLが必要］チェックボックスがオフで、［クライアント証明書］で［無視］が選択さ

れていることを確認します。
2. グループポリシー管理コンソールを使用して、ユーザーデバイスでローカルコンピューターのポリシーを構成します。
   1. %Program Files%\Citrix\ICA Client\Configuration\からicaclient.admテンプレートをインポートします。
   2. ［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix Components］、［Citrix Receiver］、［User authentication］の順に展開します。
   3. ［Smart card authentication］を有効にします。
   4. ［Local user name and password］を有効にします。
3. Receiver Desktop Lockをインストールする前に、ユーザーデバイスを構成します。
   1. Windows Internet Explorerの信頼済みサイトの一覧に、Delivery ControllerのURLを追加します。
   2. Windows Internet Explorerの信頼済みサイトの一覧に、最初のデリバリーグループのURLを「desktop://<デリバリーグループ名>」形式で追加します。
   3. 信頼済みサイトに対するInternet Explorerの自動ログオン機能を有効にします。

Receiver Desktop Lockがユーザーデバイスにインストールされている場合、スマートカード取り出し時の動作に競合が生じないようにポリシーが適用されます。たとえば、スマートカード取り出し時の動作がデスクトップ側で［ログオフを強制する］に設定されている場合、ユーザーデバイスのWindows側の設定にかかわらず、ユーザーデバイスからも強制的にログオフされます。これにより、ユーザーデバイスの整合性が維持されます。これは、Receiver Desktop Lockがあるユーザーデバイスにのみ適用されます。

Receiver Desktop Lockをアンインストールするには

以下のコンポーネントを両方ともアンインストールする必要があります。
1. Recevier Desktop Lockのインストールと構成に使用したローカル管理者アカウントでログオンします。
2. プログラムの削除や変更を行うためのWindows機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います。
   - ［Citrix Receiver Desktop Lock］をアンインストールします。
   - Citrix Receiverをアンインストールします。

リモートセッションでのWindowsショートカットキーの実行

ほとんどのWindowsショートカットキーはリモートセッションで実行できます。このセクションでは、一般的なものについていくつか説明します。

Windows
- Win+D - すべてのウィンドウをデスクトップ上で最小化します。
- Alt+Tab - アクティブなウィンドウを変更します。
- Ctrl+Alt+Delete - Ctrl+F1およびDesktop Viewerツールバーを介します。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+すべての文字キー

Windows 8
- Win+C - チャームを開きます。
- Win+Q - チャームを検索します。
- Win+H - チャームを共有します。
- Win+K - デバイスのチャーム。
- Win+I - 設定のチャーム。
- Win+Q - アプリを検索します。
- Win+W - 設定を検索します。
- Win+F - ファイルを検索します。

Windows 8のアプリ

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

Desktop

- Win+D - デスクトップを開きます。
- Win+, - デスクトップでプレビューします。
- Win+B - デスクトップに戻ります。

Other

- Win+U - コンピューターの簡単操作センターを開きます。
- Ctrl+Esc - 画面を開始します。
- Win+Enter - Windowsナレーターを開きます。
- Win+X - システムユーティリティ設定メニューを開きます。
- Win+PrintScrn - スクリーンショットを取りピクチャに保存します。
- Win+Tab - スイッチ一覧を開きます。
- Win+T - タスクバーの開いているウィンドをプレビューします。

Citrix Receiver for Windows 4.xで解決された問題

Jan 27, 2017

Receiver for Windows 4.2.100

Citrix Receiver for Windows 4.2との比較

Receiver for Windows 4.2.100には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2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。

キーボード

- 公開Receiverセッションで、ユーザーがCtrl+Alt+Endキーを押したときに、パスワードを変更するように要求された場合、このキーの組み合わせは動作していない可能性があります。

  [RcvrForWin4.2_14.2.100から][#LC0862]

ローカルアプリケーションアクセス

- XenApp 7.5およびStoreFront 2.5のアプリケーションで、ローカルアプリケーションアクセス機能「KEYWORDS:prefer="*pattern*"」を使用している場合、Receiverに問題が発生することがあります。さらに、「優先テンフレートディレクトリ」を使用して、優先するアプリケーションのショートカットを自動で作成している間に、問題が発生する可能性があります。

  [RcvrForWin4.2_14.2.100から][#LC2153]

セッション/接続

- FastConnectによるAPIのスクリプトを使用して、ユーザーを切り替える場合、資格情報のプロンプトは閉じません。

  [RcvrForWin4.2_14.2.100から][#LC2299]

- ユーザーがフルスクリーンモードでデスクトップセッションを開始し、Desktop Viewerが無効な場合、2番目のモニターに接続したときに、スクロールバーが表示されることがあります。

  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。

  - *Windows 32ビットシステムの場合*:
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名前：ProcessWM_SETTINGCHANGE
    種類：DWORD
    値：1（デフォルト値はゼロ）（この修正は、フルスクリーンモードで、［CDViewer Bar］および［run Desktop］を無効にしているユーザーに対してのみ適用されます）

- *Windows 64ビットシステムの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名前：ProcessWM_SETTINGCHANGE
  種類： DWORD
  値：1（デフォルト値はゼロ）（この修正は、フルスクリーンモードで、［CDViewer Bar］および［run Desktop］を無効にしているユーザーに対してのみ適用されます）

以下のレジストリキーはオプションです。デフォルトではこの値は0で、デフォルトの構成で問題が解決できない場合にのみ、必要になります。

- *Windows 32ビットシステムの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名前：MonitorLayoutUpdateDelay
  種類：DWORD
  値：0～4（デフォルト値はゼロ）
- *Windows 64ビットシステムの場合*:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名前：MonitorLayoutUpdateDelay
  種類：DWORD
  値：0～4（デフォルト値はゼロ）

[RcvrForWin4.2_14.2.100から][#LA5746]

- この機能拡張では、Receiver for Windows with XenApp 6.5の［クライアントの自動再接続］、およびユーザーがNetScaler Gatewayに接続して、CloudBridgeまたはHDX Insightを展開した場合に、VDAバージョン7.xを実行するサーバーオペレーティングシステムがサポートされています。

  注：サーバーでマルチストリームおよびマルチポートポリシーが有効にされており、以下のいずれかまたはすべてがtrueである場合、セッション画面の保持および自動再接続は動作しません。

  - NetScaler Gatewayで、セッション画面の保持機能が無効になっている場合
  - NetScalerアプライアンス上でフェールオーバーが発生した場合
  - CloudBridgeをNetScaler Gatewayとともに使用している場合

  [RcvrForWin4.2_14.2.100から][#LC1779]

- ユーザーデバイスに複数のUSBデバイスを接続して、Receiverを実行させている場合、デバイスを再起動するか、または新しいUSBデバイスを接続すると、以下のメッセージが表示されます。

  「USBハブ電源が容量を超えました」

  [RcvrForWin4.2_14.2.100から][#LC1904]

- プールされたデスクトップグループが、ユーザーごとに構成された複数のデスクトップを保持している場合、Receiver for Windowsを使用するときには、最初のデスクトップのみが起動できます。ユーザーがその他のデスクトップのアイコンをクリックすると、デスクトップに「接続中」ダイアログボックスが表示され、接続に失敗することがあります。最初のデスクトップセッションは、フォアグラウンドに表示されます。

  [RcvrForWin4.2_14.2.100から][#LC0780]

- Knowledge CenterのCTX133565の説明に従って、Client Selective Trustレジストリキーファイルをインポートし、信頼済みおよびイントラネットの両方のゾーンを構成するときに、Web InterfaceまたはStoreFrontでDesktop Viewerを有効にすると、レジストリキーが動作しないことがあります。ブラウザー内で、Web InterfaceまたはStoreFrontのURLを信頼済みゾーンとして構成した場合、クライアント側ドライブマッピング（CDM）のディレクトリにアクセスすると、ファイルセ

キュリティのプロンプトが誤って表示されます。

[RcvrForWin4.2_14.2.100から][#LC0904]

- デスクトップセッションからログオフした後に、ユーザーがWindows XP Embeddedシンクライアントからログオフしようとした場合、「プログラムconcentr.exeを終了します」というエラーメッセージが表示されます。

  [RcvrForWin4.2_14.2.100から][#LC2556]

- ユーザーがReceiver for Windowsからログオンしている場合、タイムゾーンは正しくありません。この修正を有効にするには、以下の設定が必要です。

  - ユーザーデバイスおよびサーバーには、同じMicrosoftタイムゾーンの更新Hotfixをインストールする必要があります。たとえば、Microsoft Hotfix KB2998527がユーザーデバイスにインストールされている場合は、サーバーにこのHotfixをインストールしてください。
  - サーバーのオペレーティングシステムがWindows Server 2008 R2 Service Pack 1である場合は、Microsoft Hotfix KB2870165をサーバーにインストールする必要があります。
  - 参照番号#LC1061の修正をXenAppサーバーにインストールする必要があります。

  [RcvrForWin4.2_14.2.100から][#LC1392]

- この修正により、Self-Service Plug-inと統合されていない場合でも、FastConnectによるAPIのスクリプトのサポートが有効になっています。これを有効にするには、［**ADM**］>［**Citrix Components**］>［**Citrix Receiver**］>［**FastConnect API Support**］>［**Manage FastConnectAPI support**］の下のグループポリシーを使用して、オプション［Integrate Self Service plugin with FastConnect］をオフにします。また、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Dazzleの下のレジストリーキー「FastConnectUsingSSP」を「False」に変更することもできます。

  [RcvrForWin4.2_14.2.100から][#LC2580]

- 「SelfServiceMode」を「False」に設定すると、［スタート］メニューのショートカットが、事前起動アプリケーションなどのバックグラウンドセッションで作成されます。

  [RcvrForWin4.2_14.2.100から][#LC1760]

- この修正により以下の問題が解消されます。

  - シームレスな公開アプリケーションを起動する場合には、アプリケーションが、Windowsタスクバーの後ろで開かれることがあります。
  - Windowsタスクバーをほかの場所に移動する場合、シームレスなセッションがサイズ変更に失敗し、タスクバーがシームレスなアプリケーションと重なって表示されることがあります。

  この修正を有効にするには、サーバー側の参照番号#LC1342の修正もインストールする必要があります。

  [RcvrForWin4.2_14.2.100から][#LC1645]

- Windows XP Embeddedシンクライアント上のReceiver for Windows 4.2でセッションを起動すると、エラーメッセージが表示されることがあります。

  [RcvrForWin4.2_14.2.100から][#LC1929]

- この修正で、「FastConnectAPISupportEnabled=True」と設定することにより、インストール時のFastConnectによるAPIスクリプトをサポートできるようになります。また、［Manage FastConnectAPI support］の下のグループポリシーオブジェクト［Enable FastConnect API Functionality］を介して、この設定を有効にすることもできます。

  [RcvrForWin4.2_14.2.100から][#LC2131]

- プログラムのデッドロックが原因で、Receiver for Windows 4.2が、ネットワークパケットの送信を停止する場合があります。この結果、以下が発生します。

  - セッションが確立できないことがある。
  - デスクトップ画面の解像度を変更すると、Citrix HDX Engineが応答不能になることがある。

  [RcvrForWin4.2_14.2.100から][#LC2105]

- この機能拡張では、Receiver for Windows 4.2 Cumulative Update 1でのTLSバージョン1.1および1.2がサポートされています。

  [RcvrForWin4.2_14.2.100から][#LC1931]

- EdgeSight AgentのICAセッション往復時間が、ファーム間のランダムセッションで長くなることがあります。

  [RcvrForWin4.2_14.2.100から][#LC1725]

- この機能拡張により、「icaclient.adm」ファイルが変更され、Fast Connectでの変更内容の処理が改善されています。

  [RcvrForWin4.2_14.2.100から][#LC2575]

- Receiverセッションを［ウィンドウに合わせる］にサイズ変更すると、セッションでマウスとキーボードが動作を中止します。

  [RcvrForWin4.2_14.2.100から][#LC2219]

- この機能拡張により、Fast Connect機能用のCitrix Diagnostic Facility（CDF）トレースログにおいて、障害が発生していない場合は報告を行わないように改善されています。

  [RcvrForWin4.2_14.2.100から][#LC2573]

- コマンドラインを使用してReceiverをインストールしたら、Receiverの停止および再起動時に、Self-Service Plug-inに新しいストアが自動的に追加されます。

  この問題が発生するのは、HKEY_CURRENT_USER\Software\Citrixの下の「Dazzle」キーに「Properties」と呼ばれるサブキーが存在する場合です。また、「RegDeleteKey」は、サブキーが含まれているレジストリキーを削除できないため、ストアキーが重複して作成されます。

  [RcvrForWin4.2_14.2.100から][#LC2154]

- ユーザーがFast ConnectによるAPIのスクリプトを使用してログオフした場合、アプリケーションのショートカットが、デスクトップのショートカットフォルダーまたは［スタート］メニューに残されたままになります。

  [RcvrForWin4.2_14.2.100から][#LC2590]

- FastConnectによるAPIのスクリプトを使用してログオフするときに、非認証の要求に対して、複数のログオンプロンプトが表示される場合があります。

  [RcvrForWin4.2_14.2.100から][#LC2300]

- Receiverをインストールする前に、Receiver関連のレジストリエントリを作成した場合、標準ユーザーはエラーなしにReceiver for Windowsをインストールできますが、アプリケーションの起動に失敗することがあります。

  [RcvrForWin4.2_14.2.100から][#LC0410]

- FastConnectによるAPIのスクリプトでは、指定ユーザー認証を実行するために、ユーザーを切り替えることができない場

合があります。

[RcvrForWin4.2_14.2.100から][#LC2127]

- この機能拡張には、［Per App shortcut management］オプションが含まれています。アプリケーションのプロパティを使用して、ユーザーのデスクトップ、および特定の公開アプリケーションの［スタート］メニューでショートカットを作成することができます。

  注：アプリケーションのプロパティの［スタート］メニューフォルダーが適用されるのは、ユーザーがStoreFrontではなくWeb Interfaceを使用して、ファームまたはデリバリーグループに接続している場合のみです。

  [RcvrForWin4.2_14.2.100から][#LC1930]

- ユーザーがFast Connectを使用してReceiverからログオフした場合、アプリケーションのサブスクリプション一覧は引き続きサイドペインに表示されます。

  [RcvrForWin4.2_14.2.100から][#LC2574]

- Receiver for Windowsがアカウントを使用して構成されていない場合、アプリケーションは、disconnect SelfServiceコマンドを使用して切断することはできません。

  [RcvrForWin4.2_14.2.100から][#LC2128]

システムの例外

- Receiverでは、アクセス違反が発生して予期せずに閉じてしまうことがあります。この場合、ユーザーがWeb Interfaceでアプリケーションのアイコンをクリックしても、セッションを開始することはできません。

  [RcvrForWin4.2_14.2.100から][#LC0650]

- ユーザーデバイスにローカルプリンターを接続して、公開アプリケーションを起動すると、Receiver for Windowsが以下のエラーメッセージを表示して、予期せずに閉じてしまうことがあります。

  「Citrix HDX Engineが動作を停止しました」

  [RcvrForWin4.2_14.2.100から][#LC1170]

ユーザーエクスペリエンス

- ユーザーがStoreFrontまたはWeb Interfaceにログオンしたときに、Receiverにおいて、アプリケーションへのデスクトップショートカットを作成するのに長い時間を要してしまうことがあります。

  [RcvrForWin4.2_14.2.100から][#LC2263]

- この修正により、セッションの構成を読み取ったときに、グループポリシーオブジェクトの優先度の設定が、プライマリストアより高く指定されます。

  [RcvrForWin4.2_14.2.100から][#LC2698]

ユーザーインターフェイス

- コマンドラインを使用して、Receiverをインストールすると、ストア名とその説明が既存のものと同じに設定されます。Receiverを再起動すると、ストア名とその説明が、自動的に別の値に変化してしまうことがあります。ただし、URLは同一のままで、接続も正常に動作します。

この問題が発生するのは、Receiverのサイトを処理したときに、レジストリからストア名が取得されないことが原因です。代わりに、ストアURLに従って、新しいストア名が生成されます。

[RcvrForWin4.2_14.2.100から][#LC1231]

- この機能拡張では、アプリケーションが公開されなくなったか、または無効にされた場合、アプリケーション一覧からアプリケーションとショートカットを削除するプロンプトが表示されなくなります。

  [RcvrForWin4.2_14.2.100から][#LC2157]

- ユーザーが、ナビゲーション領域でReceiverのアイコンメニューから［ヘルプ］をクリックしたときに、Desktop Viewerの［詳細情報を表示する］リンクが、別のセットのヘルプファイルに移動します。

  [RcvrForWin4.2_14.2.100から][#LC2066]

Receiver for Windows 4.2

Citrix Receiver for Windows 4.1.200との比較

Receiver for Windows 4.2には、Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200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。

コンテンツリダイレクト	セッション/接続
HDX MediaStream	シャドウ機能
HDX MediaStream Windows Mediaリダイレクト	スマートカード
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
ログオン/認証	ユーザーインターフェイス
印刷	その他
サーバー/ファームの管理	

コンテンツリダイレクト

- 公開アプリケーション内のURLにアクセスしたときに、サーバー/クライアント間のコンテンツリダイレクトが機能しないことがあり、サーバー側でブラウザーを開くことはできますが、クライアント側では開くことができません。

  [#LC0150]

- URLヘッダーに「GET」リクエストではなく「HEAD」リクエストが含まれているWebサイトにアクセスすると、WebサーバーがHEADリクエストへのアクセスに失敗したときに、そのサイトへのアクセスが失敗する場合があります。この結果、

サーバー/クライアント間のコンテンツリダイレクトが機能しません。

この修正を有効にするには、以下のレジストリキーを作成します。

HKEY_CURRENT_USER_\Software\Citrix\ICA Client\Engine
名前：SpecificSites
種類：REG_MULTI_SZ
値：Webサイト名（行ごとに1つのWebサイト）

注：値で指定したWebサイトへは、HEADリクエストではなくGETリクエストが送信されます。Webサイト名では大文字と小文字は区別され、ワイルドカード「*」が使用できます。たとえば、このレジストリ値で「*.mycompany.com」と指定した場合、ユーザーはwww.mycompany.comとsupport.mycompany.comの両方にアクセスできます。これらは「特定の」Webサイトです。

[#LC0326]

- この修正は、参照番号#LA0803の修正の拡張です。XenApp 6 Hotfix Rollup Pack 2およびXenApp 6.5 Hotfix Rollup Pack 3がインストールされているサーバーでは、公開アプリケーション内のカスタムURLにアクセスしたときに、サーバー/クライアント間のコンテンツリダイレクトが機能せず、ユーザーデバイスではなくサーバーでWebブラウザーが開きます。

  [#LC0428]

HDX MediaStream

- モニターが2つあるユーザーデバイスでは、1番目のモニターのReceiverセッションにおいて、Windows Media Playerでビデオを再生した場合、2番目のモニターでは黒いウィンドウが開きます。

  [#LC0552]

- Receiverセッションにおいて、Windows Media Playerでビデオを再生した場合、タイトルが「Citrix HDX Movie Window」の2番目の黒いウィンドウが開きます。この2番目のウィンドウを閉じても、再生中のビデオには影響を与えません。

  [#LC0818]

HDX MediaStream Windows Mediaリダイレクト

- Windows Media Playerで音声の再生時に、静的ノイズが発生することがあります。

  [#LA2911]

HDX Plug-n-Play

- セッション中に、エンドポイントからUSBデバイスを取り外すと、Receiver for Windowsが応答不能になることがあります。

  [#LA4827]

- セッションからのログオフ後に、USBデバイスが解放されず、その後のローカルセッションで、このデバイスが使用できないことがあります。

  [#LC0091]

インストール、アンインストール、アップグレード

- /includeSSONコマンドラインスイッチを使用してReceiverをインストールした後に、SSONSVR.exeプロセスが実行に失敗

します。

[#LC0138]

- Windowsのシステム管理者として、CitrixReceiver.exe /uninstallを使用してReceiverをアンインストールしようとすると、UACプロンプトが表示される場合があります。

  [#LC0977]

ログオン/認証

- クライアントのADMテンプレートで、スマート認証を有効にすると、ローカルポリシーがまだ構成されていない場合でも、ポリシー内でローカルユーザー名とパスワードが自動的に［有効］に設定されます。

  [#LC0713]

- Cumulative Update 3を適用したCitrix Receiver for Windows 3.4では、ドメインパススルー認証が断続的に失敗することがあります。

  [#LC0865]

印刷

- Internet Explorer 8で、1枚の用紙に複数のページを印刷するように［ローカルプリンター設定］を構成すると、設定が適用されないことがあります。代わりに、1枚の用紙に1ページが印刷されます。この問題が発生するのは、XenApp 6.5の公開デスクトップから、XenApp 6サーバーで公開されているInternet Explorer 8のインスタンスに接続した場合です。

  [#LA3379]

- XPSユニバーサルプリンタードライバーを使用して、［クライアントでのプレビュー］をクリックした場合、Internet Explorerに以下のエラーメッセージが表示されます。

  「Internet Explorerではこのページは表示できません。」

  [#LA5896]

- プリンターの自動作成は、1セッションにつき100に制限されています。

  [#LC0031]

- この機能拡張では、LPTマッピングクライアント側コンポーネントに、CDFトレースサポートが追加されます。

  [#LC0823]

サーバー/ファームの管理

- この修正は、基本コンポーネント内のメモリ問題に対応しています。

  [#LA5664]

- Receiver for WindowsがNetScaler Gatewayに接続され、StoreFrontへの接続を渡した場合、StoreFrontからの応答に含まれるのは、ビーコンではなくサービスURLのみです。この状態になると、ユーザーはHTTP 403エラーを受信し、自動検出機能が動作しなくなることがあります。

  [#LC0481]

- ユーザーデバイスがVDAに接続されたときに、デバイス上でユーザーが［USBルートハブ］設定を無効にし、再度デバイスマネージャーから有効にした場合、USBデバイスのリダイレクト機能は動作しません。

  [#LC0541]

セッション/接続

- Receiver for Windows Enterprise Editionがインストールされ ているWindows 7クライアントデバイスとの間でのログオンおよびログオフが、遅延することがあります。この問題が発生するのは、ログオンおよびログオフスクリプトが、GPOによって適用されている場合です。各スクリプトが、大幅な遅延を引き起こす場合があります。

  [#LA3811]

- Receiver for Windowsを使用して、XenAppまたはXenDesktopセッションに接続しているときに、スリープまたは休止状態モードからエンドポイントを再開した場合、そのエンドポイントとCitrixセッションの間のコピーまたは貼り付け動作が失敗することがあります。

  [#LA3973]

- マルチストリームが有効な場合、Desktop Lockとともに使用したReceiverが、VDAスクリーンセーバーから復元できず、VDAのロック後の再接続に失敗することがあります。

  [#LA4097]

- セッションにマップされたクライアントドライブから、読み取り専用アクセスでMicrosoft WordまたはMicrosoft Excel 2003ファイルを開こうとした場合、ファイルを開くことができないことがあります。

  [#LA4198]

- 「Hide Icon」ポリシーを有効にすると、クライアントデバイスへのログオン後に、自動的に［Citrix Receiverについて］ウィンドウが表示される場合があります。

  [#LA4513]

- カスタムの仮想ドライバーを使用してセッションを起動しようとすると、失敗する場合があります。

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

  - *32ビットWindowsの場合*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名前：VdLoadUnLoadTimeOut
    種類：REG_DWORD
    データ：秒単位の任意の値
  - *64ビットWindowsの場合*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
    名前：VdLoadUnLoadTimeOut
    種類：REG_DWORD
    データ：秒単位の任意の値

  [#LA4540]

- Huawei OpenEyeプラグインがあるHollyCRMを使用して、PVSストリームVDAからVOIP呼び出しを実行すると、2時間以上の経過後、両側でお互い同士が聞こえなくなることがあります。

[#LA4809]

- Windowsキーを押すか、または［スタート］ボタンをクリックして、フォアグラウンドで実行中のシームレスなセッションウィンドウからクライアント側で［スタート］メニューを開く場合、ローカルウィンドウのタスクバーアイコンをクリックすると、ローカルウィンドウに移動せずに、フォーカスがシームレスなセッションウィンドウに残されたままになります。

  [#LA5089]

- SSL Relayを有効にすると、暗号化を利用するように構成されているアプリケーションでは、セッション画面の保持機能が動作しません。

  [#LA5476]

- XenAppの公開デスクトップセッションでパスワードを変更した後は、公開デスクトップセッション内からの公開アプリケーションに対するパススルー認証が失敗し、ユーザーはユーザー名とパスワードの入力を要求されるプロンプトを受信します。

  [#LA5587]

- Receiverは、Windows Server 2012 R2からのNetscaler Gatewayを介したStoreFrontへの接続に失敗します。

  [#LC0084]

- Receiver for Windows 4.1では、ユーザーが［Self-Service Plug-in］ウィンドウのデスクトップアイコンをクリックして、切断されたセッションに再接続しようとしたときに、2番目のデスクトップセッションが作成されます。

  [#LC0182]

- Cleanup.exeは、Receiverのリセット時に予期せずに終了する場合があります。

  [#LC0249]

- 英語以外のXenApp環境でのセッションの事前起動中に、Citrix Receiverの進行状況バーが表示され、以下のエラーメッセージで応答不能になることがあります。

  「接続は確立されましたが、機能をネゴシエーションしています」

  [#LC0306]

- Microsoft Outlookの公開インスタンスで入力を行うと、セッションがランダムに切断される場合があります。

  [#LC0323]

- TWAINデバイスでサードパーティアプリケーションを使用して、ファイルを転送しようとすると、アプリケーションが予期せずに終了する場合があります。

  [#LC0369]

- ユーザーがReceiver for Windowsを使用してWindows 7 VDAに接続したときに、Desktop Viewerを使用してSpeechMikeをリダイレクトした場合、マイクボタンを放したときにリダイレクトが失敗することがあります。

  [#LC0510]

- ファイルタイプの割り当てが構成されている場合でも、ユーザーに対して、指定したファイルを開くためのアプリケーシ

ンの選択を要求するプロンプトが表示されます。

[#LC0515]

- PACファイル経由でプロキシサーバーを介して接続しようとしても失敗します。

  [#LC0529]

- 公開SAPアプリケーションにおいて、Citrix Receiver for Windows 13.4 Cumulative Update 3が、以下のエラーメッセージで予期せずに終了する場合があります。

  「Citrix HDX Engineが動作を停止しました」

  [#LC0712]

- リダイレクトCOMポートデバイスは、Receiverセッション内では動作しません。

  [#LC0851]

- 参照番号#LC0031の修正が適用されている場合、ユーザーが切断するかまたはログオフすると、ほかのアクティブなセッションが存在するときには、2分間を超えてReceiverセッションが応答不能になります。

  [#LC0983]

シャドウ機能

- 管理者がセッションをシャドウしようとすると、初期化が必要な黒いシャドウセッションが発生し、自動的に再描画されないことがあります。この問題が発生するのは、シャドウする側とその対象となる側が同じサイズである場合です。

  [#LA2913]

スマートカード

- Citrix Receiver for Windowsが、有効なスマートカード証明書の検出に失敗し、Authentication Managerのデバッグログに、以下のエラーメッセージが表示される場合があります。

  「ERROR_WINHTTP_CLIENT_AUTH_CERT_NEEDED：不明なエラーコード「12044」」

  [#LC0783]

システムの例外

- クライアントデバイスが休止状態から再開したときに、Receiver for Windowsが応答不能になる場合があります。

  [#LA5023]

- CDViewerプロセスに関する問題が原因で画面が黒くなり、ハンドルされない.Net例外がトリガーされます。

  [#LC1038]

ユーザーエクスペリエンス

- 一部の構成では、ユーザーセッションで、マウスのちらつきが発生する場合があります。

  [#LA309]

- ［ローカルテキストエコー］を有効にすると、Internet Explorerの公開インスタンス内の入力脱字記号でちらつきが発生するか、または接続で遅延時間が長くなり、表示されなくなる場合があります。

  [#LA4762]

- 特定の環境下では、アプリケーションがバックグラウンドで起動されます。

  [#LC0050]

- ユーザーが複数のExcelブックを開いており、レジストリでExcelhookが有効な場合、最後のブックを閉じると、Excelウィンドウが開いているときでも、Excelタスクバーアイコンは表示されません。

  [#LC0062]

- Receiverをインストールしたユーザー以外のユーザーに対しては、最初にReceiverを起動したときに、［アカウントの追加］を要求するプロンプトが表示されます。

  [#LC0253]

- ［ディスプレイの電源を切る］から再開した後、セッションはモニターの左上隅に小さい画面として再描画されます。

  [#LC0319]

- ローカルWindowsタスクバーの後ろにある公開アプリケーションウィンドウを移動しようとすると、失敗する場合があります。

  [#LC0561]

- マルチモニター構成では、アプリケーションウィンドウが誤って再描画される場合があります。

  [#LC0600]

ユーザーインターフェイス

- アプリケーションの起動時に［Receiver Store］ウィンドウを閉じると、アプリケーションの起動完了後にも、進行状況バーが表示されたままになります。

  [#LC0464]

- アプリケーションまたはデスクトップの起動中には、起動ダイアログがアクティビティに関する説明なしに、数秒間空白になります。

  [#LC0624]

- この修正により、デフォルトのAdminテンプレートから、印字エラーが削除されます。

  [#LC0848]

その他

- Citrix Receiverインストーラーのログに対するこの機能拡張により、以下の処理が実行できます。

  - ログの永続的な場所への保存
  - インストールごとのインストール履歴の保存
  - 実際のインストールの開始前のユーザー環境情報の収集

- インストールログへの詳細なデバッグ情報の提供
  [#LA4615]

- 現在、CtxCredApi.dllおよびCtxCredApi(64).dllは、Citrix Receiver for Windows Enterprise MSIパッケージに付属しています。APIで64ビットがサポートされるようになりました。64ビットのアプリケーションにはCtxCredApi64.dllを使用します。

  [#LA4630]

- サーバー上のすべてのwficaプロセスのCPU使用率が、ユーザーセッションで単一のユーザーが音声を使用しているときに、約10%増加する場合があります。

  [#LA5918]

- 名前に特殊文字、特にASCII文字セットの最初の128文字以外の文字が含まれているときには、Receiverが証明書の組織名を適切に読み取ることができない場合があります。

  [#LC0801]

- 「wfica32.exe /setup」コマンドを使用するときには、wfica.ocx ActiveXアドオンが、Internet Explorerの登録に失敗します。

  [#LC0927]

注：このバージョンのCitrix Receiverには、バージョン4.1、4.0に含まれているすべての修正が入っています。