Citrix Receiver for Windows 4.9 LTSR

Contents

4.9 LTSR の新機能

June 24, 2019

Citrix Receiver に関する重要なお知らせ

Citrix Cloud の TLS バージョンの廃止

Citrix Cloud への接続時のセキュリティを向上させるため、2019 年 3 月 15 日以降、Transport Layer Security（TLS）1.0 および 1.1 を介した通信をブロックすることになりました。ただし、Citrx Receiver for Windows 4.9 LTSR トラックを利用するユーザーは、今回のバージョン廃止の影響を受けません。詳しくは、TLS バージョンの廃止を参照してください。

累積更新プログラム 7 が利用可能になりました

Citrix Receiver for Windows 4.9 LTSR 累積更新プログラム 7（CU7）は、2019 年 6 月 21 日にリリースされました。お客様から報告された問題が多数修正されたため、この LTSR バージョンはさらに使いやすく安定した機能を提供します。Citrix Receiver for Windows 4.9 CU7 にはまた、CU6 から 10 件の修正、CU5 および CU4 からそれぞれ 12 件以上の修正、CU3 から 20 件以上の修正、CU2 から 18 件以上の修正、CU1 から 15 件以上の修正が含まれています。CU7 は、シトリックスのダウンロードページからダウンロードできます。

インストーラーのサイズを縮小

このリリースでは、Citrix Receiver for Windows インストーラーのサイズが 39.9MB に縮小されました。前回のリリースから 15% の削減です。

StoreFront アカウントの新しい外部ビーコン

StoreFront アカウントで、www.citrix.com 外部ビーコンの代わりに ping.citrix.com が使用されます。

Citrix Receiver for Windows バージョン 4.9 からは、ユーザーが構成を変更する必要はありません。

Citrix Receiver for Windows の以前のバージョンを使用している場合、www.citrix.com 外部ビーコンを ping.citrix.com に置き換えてください。

外部ビーコンについて詳しくは、Knowledge Center のCTX218708を参照してください。

StoreFront の外部ビーコンの構成について詳しくは、「ビーコンポイントの構成」を参照してください。

> 注
>
> StoreFront アカウントでwww.citrix.comが外部ビーコンとして構成されていない場合、この情報は無視してください。

解決された問題

June 24, 2019

Citrix Receiver for Windows 4.9 LTSR CU7

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU6 Hotfix 1（4.9.6001）

インストール、アンインストール、アップグレード

- マシン上にサードパーティアプリケーションがインストールされ、カスタム仮想チャネルが使用されている場合、Citrix Receiver for Windows をアップグレードすると、Receiver からアプリケーションを起動できないことがあります。次のエラーメッセージが表示されます：

  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。

  サードパーティアプリケーションのドライバーに関する詳細がアップグレード時に引き継がれない場合、問題が発生します。[LD0831]

キーボード

- ローカル IME 機能を有効にしている場合、大易輸入法または行列輸入法で Shift キーを使用して英語と中国語を切り替えると、Shift キーが押されたままになることがあります。[LD1039]

Secure Gateway

- Citrix Gateway を使用して外部ネットワークからストアを追加しようとすると、`https://citrix.com` を外部ビーコンとして構成している場合に失敗することがあります。[LD0913]
- Citrix Receiver for Windows は、https アドレスで指定された場合、プロキシ自動設定（PAC）（proxy.pac）ファイルを使用しないことがあります。[LD1460]

セッション/接続

- 特定のサードパーティアプリケーションが Citrix ICA クライアントオブジェクト（ICO）を使用して ICA ホストに接続したとき、接続に失敗することがあります。[LD0266]
- 接続に頻繁に失敗すると、Citrix Director にログインすることがあります。これは、ユーザーセッションを開始したときに発生することがある問題です。[LD0519]
- デュアルモニターを使用し **Desktop Viewer** が無効になっている場合にユーザーセッションを実行すると、セッションが反応しなくなることがあります。モニタケーブルを取り外すとこの問題が発生します。[LD0999]
- Citrix Receiver for Windows を実行しているクライアントマシンに Desktop Lock をインストールすると、ログオフされることがあります。この問題は、Citrix StoreFront がオフラインになったときに発生します。[LD1021]
- 切断されたセッションの公開アプリケーションに再接続しようとすると、時間がかかることがあります。[LD1381]

ユーザーエクスペリエンス

- Citrix Receiver for Windows は、マシンの代わりの IP アドレスを StoreFront に送信することがあります。この問題は、Citrix Receiver for Windows が最新の IP アドレスかどうかに関係なく、IP アドレス一覧から最後に使用した IP アドレスを選択したときに発生します。その結果、デリバリーグループの ExcludedClientIPFilter 設定は使用できなくなります。[LC9497]
- **Desktop Lock** とローカルアプリアクセスを有効にすると、ローカルアプリケーションを最小化したときに正しく表示されないことがあります。[LD0787]
- 複数のアプリケーションの実行中にアプリケーションアイコンの上にマウスポインタ — を合わせると、タスクバーのプレビューにアクティブなウィンドウのコンテンツだけが表示されることがあります。[LD1030]

  > 注:
  >
  > クライアントが Flash または Windows Media リダイレクトをレンダリングしている場合、タスクバーのプレビューが正しく機能しないことがあります。

- Citrix Receiver for Windows を使用している場合、別のストアがあるときにストアを追加すると、既存のユーザーに対してショートカットが作成されないことがあります。[LD1125]

Citrix Receiver for Windows 4.9 LTSR CU6 Hotfix 1 (4.9.6001)

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU6

セキュリティの問題

- この修正により、セキュリティ上の問題が 1 件解決されます。詳しくは、Knowledge Center のCTX251986を参照してください。[LD1518]

Citrix Receiver for Windows 4.9 LTSR CU6

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU5

HDX MediaStream Windows Media リダイレクト

- Windows Media リダイレクトのクライアント側でのコンテンツ取得に失敗することがあります。この問題は、スクリプトストリームを含むマルチメディアファイル（Web 上のライブストリームからアーカイブされたもの）を再生する場合に発生します。[LC7948]

インストール、アンインストール、アップグレード

- Citrix Receiver for Windows をバージョン 4.9 LTSR にアップグレードすると、カスタム仮想チャネルに必要な特定のレジストリキーが保持されないことがあります。[LD0633]

キーボード

- ローカル **IME** またはローカルキーボードレイアウト同期を有効にすると、右 Ctrl キーまたは右 Shift キーを含むキーの組み合わせを使用した場合、Shift キーが押されたままになることがあります。[LD0585]
- [はい。リモートサーバーで提供されるキーボードレイアウトではなく、ローカルキーボードレイアウトを使用します] オプションをオンにすると、最後の入力文字が正しく処理されないことがあります。この問題は、右 Alt キーをクリックして韓国語から英語に切り替えると発生します。この修正を適用した後、マウスを使用すると問題が引き続き発生する場合があります。[LD0825]

セッション/接続

- 一部のサードパーティ製のアプリケーションを使用中、ホストからクライアントへのリダイレクトが機能しないことがあります。この問題は、これらのアプリケーションが HTTPS および HTTP アドレスを含む特殊な Web URL を使用する場合に発生します。[LD0484]
- 残留アプリが構成されている場合、セッションの切断後に公開アプリケーションが既存のファイルを再度開くことができないことがあります。[LD0742]

- Windows 7 で標準テーマを設定し、ユーザーデバイス上でハードウェアアクセラレーション（GDI モード）を無効にしている場合に、ローカルと公開のシームレスアプリケーションを切り替えると、表示の問題が発生する可能性があります。[LD0853]
- VDA で NVIDIA GPU を使用し、GPU で最新の NvENC を最適化している場合、h.264 DXVA デコーディングで破損が発生する可能性があります。

  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：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRender

  名前：MaxNumRefFrames

  種類：DWORD

  値：2 ～ 8 [LD0943]

ユーザーエクスペリエンス

- 非シームレスアプリケーションのウィンドウを最大化すると、アプリケーションウィンドウが破損しています。[LD0755]
- Windows 7 の公開デスクトップを起動した場合、Citrix Receiver for Windows セッション内でマウスカーソルをドラッグするときに遅延が生じることがあります。[LD0923]

Citrix Receiver for Windows 4.9 LTSR CU5

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU4

コンテンツリダイレクト

- 初めてファイルタイプの関連付けを有効にした拡張子を起動するときにデフォルトのプログラムウィンドウをキャンセルすると、以降、この拡張子のファイルを起動するとこのエラーメッセージが表示されることがあります：

  Windows が指定されたデバイス、パス、またはファイルにアクセスできません。これらの項目にアクセスするための適切なアクセス許可がない可能性があります。 [LD0026]

キーボード

- バーコードリーダーを使用すると、大量のデータと送信するときに一部が失われることがあります。[LD0243]

セッション/接続

- Citrix Receiver for Windows をバージョン 4.9.1000 にアップグレードすると、ログオフ時に CDViewer が灰色の画面を表示することがあります。[LC9290]
- アプリケーションを起動できず、次のエラーメッセージが表示されます:

  アプリケーションを起動できません。ヘルプデスクに連絡して、次の情報を提供してください:**Citrix Receiver** を開くことができません。

  - この問題を解決するには、管理者が次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\Engine

    名前:EngineTimeout

    種類:DWORD

    値:20 秒以上

  - この問題を解決するには、ユーザーが次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\Engine

    名前:EngineTimeout

    種類:DWORD

    値:20 秒以上。例:EngineTimeout=20 [LC9771]

- ホストされる共有デスクトップで複数アプリケーションを起動します。クライアント間で切り替えた場合、または切断か再接続操作を実行した場合、次のエラーメッセージが表示されることがあります:

  Citrix HDX Engine has stopped working.
  Exception caused the program to stop working correctly. Please close the program. [LC9772]

- Citrix Receiver for Windows を使用して起動したアプリケーションは、セカンダリモニターにミラーリングされることがあります。[LC9893]
- シームレスアプリケーションが最小化されると、アプリケーションの縮小バージョンが表示されますが、最小化されたウィドウとして表示されるか、ツールバー上に表示される必要があります。[LD0034]
- NVIDIA グラフィックカードを GPU と使用すると、一部のサードパーティ製アプリケーションの公開インスタンスが透過アプリケーションとして開くことがあります。[LD0175]
- コントロールパネルのアイコンから作成されたローカルアプリケーションのショートカットは、Citrix Studio で構成された **KEYWORDS:Prefer** からは起動できません。[LD0288]
- グループポリシーオブジェクト(GPO)管理用テンプレートを使用して 2 番目のストアを追加しようとすると、ビーコンやその他の情報が 2 番目のストアに追加されないことがあります。[LD0413]

システムの例外

- コンテンツの双方向リダイレクトポリシーを有効にした場合、ローカルの Webb ブラウザーで Web ページを開こうとすると、Redirector.exe プロセスが予期せず終了することがあります。その結果、コンテンツの双方向リダイレクトが機能せず、次のエラーメッセージが表示されます：

  Citrix FTA, URL Redirector stopped working. [LD0420]

- wfica32.exe プロセスが、予期せずに終了する場合があります。プロキシ設定が構成されている場合に、Citrix Receiver for Web で新しいセッションを開始しようとすると問題が発生します。[LD0548]

ユーザーインターフェイス

- リモートセッションでマウスのクリックが機能しないことがあります。この問題は、Desktop Viewer ツールバーで ［基本設定］ ウィンドウを開いて、**MouseTimer** 設定をデフォルト値以外の値に構成する場合に発生することがあります。[LD0260]
- **Receiver** のリセットオプションを選択すると、Citrix Receiver for Windows によって Microsoft Windows 10 に.Net Framework 3.5 をインストールするよう要求される場合があります。[LD0690]

Citrix Receiver for Windows 4.9 LTSR CU4

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU3

クライアントデバイスの問題

- ［キーボードの自動表示］ ポリシーを有効に設定しても、セッションで自動ソフトキーボードのポップアップが機能しないことがあります。[LC9925]

HDX MediaStream Windows Media リダイレクト

- 埋め込みスクリプトを含むリダイレクトされたマルチキャストストリームは、クライアントからコンテンツを取得できないことがあります。ビデオの代わりに黒い画面が表示されます。[LC9775]

キーボード

- この修正が導入される前は、Bloomberg モデル 4 Starboard キーボードは PC モードのみをサポートしていました。この修正により、Bloomberg モデル 4 Starboard キーボードは PC モードと KVM モードをサポートするようになりました。[LC9984]

ログオン/認証

- Citrix Receiver for Windows を使用してアカウントを追加するときにストア URL を入力すると、次のエラーメッセージが表示されることがあります：認証サービスにアクセスできませんでした。この問題は、StoreFront URL が「citrix.com」で始まる場合に発生します。[LC9631]

セッション/接続

- Citrix Studio で「KEYWORDS:Prefer」を構成すると、ローカルユーザーデバイスのアプリケーションショートカットに記載されているコマンドラインスイッチまたは引数が適用されない可能性があります。[LD0060]
- この修正により、以下の変更が行われます。
  - edtMSS と OutBufLength をカスタマイズすると、edtMSS が OutBufLength を上書きします。
  - All_regions.ini ファイル、defaulit.ica ファイル、およびレジストリで、パラメーター名を udt* から edt* に変更します。

  注：
  管理者としてアップグレードすると、レジストリキー HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT で、ユーザーレジストリキーとエントリの名前が udt * から edt * に変更されません。さらに、パラメーター値も保持されません。[LD0098]
- グループポリシーオブジェクト（GPO）を使用して追加したストアは、GPO でストアを更新または削除しても削除されないことがあります。[LD0147]

システムの例外

- ストアにログオンすると、Citrix Receiver for Windows が予期せず終了することがあります。[LC8271]
- Citrix Receiver for Windows が予期せず終了し、次のエラーメッセージが表示されることがあります：「**CitrixHDX Engine has stopped working**」（**Citrix HDX Engine** が動作を停止しました）

  この問題は、グラフィックモジュールにトラップがある場合に発生します。[LC9466]
- システムからログオフすると、wfica32.exe プロセスが予期せず終了する場合があります。[LC9892]

TWAIN

- Citrix Receiver for Windows 4.7 以降のバージョンでは、スキャナーのリダイレクトに失敗することがあります。この問題は、Twain 2.0 ドライバーがユーザーデバイス上に存在しない場合に発生します。[LC8215]

ユーザーエクスペリエンス

- 特定のサードパーティ製アプリケーションを使用して VPN 接続を確立すると、Citrix Receiver for Windows は約 15 分間使用できない状態になることがあります。[LC9302]
- Citrix Receiver for Windows から Linux VDA 7.17 以降のバージョンに接続すると、Citrix HDX Engine の GPU 使用率が高くなることがあります。[LC9506]
- IME（Input Method Editor）を使用し、シームレスモードのアプリケーションでテキストを入力すると、テキストが表示されないことがあります。この問題は、テキストのフォントサイズが小さい場合に発生します。

  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* ビットシステムの場合：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client

    名前：DisableD3DRenderWidthHeightCheck

    種類：REG_DWORD

    値：1
  - *64* ビットシステムの場合：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow 6432Node\Citrix\ICA Client

    名前：DisableD3DRenderWidthHeightCheck

    種類：REG_DWORD

    値：1 [LC9882]

ユーザーインターフェイス

- シングルサインオン構成を検証する構成チェッカーは、検証プロセスを完了できず、シングルサインオンプロセスの検証が停止することがあります。[LC9625]

Citrix Receiver for Windows 4.9 LTSR CU3

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU2

クライアントデバイスの問題

- 特定の DVD ビデオは、マップされたクライアントドライブを経由するとセッション内で再生されないことがあります。[LC8912]

コンテンツリダイレクト

- 双方向コンテンツを VDA にリダイレクトすると、ブラウザーが既に開いている場合、2 番目の URL が新しいブラウザーで開きます。[LC9157]
- Citrix Receiver for Windows を Citrix XenApp Services サイトとともに使用すると、アプリケーションとアイコンがファイルの種類に部分的に関連付けられることがあります。[LC9402]

インストール、アンインストール、アップグレード

- System Center Configuration Manager（SCCM）を使用して Citrix Receiver for Windows をアップグレードすると、Receiver for Windows がシステムの再起動を要求することがあります。[LC9706]

キーボード

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

  以下は、このシナリオの制限事項です。

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

ログオン/認証

- AuthManSvr.exe プロセスの再起動後、Citrix Receiver for Windows からのログオフに失敗します。[LC7981]

印刷

- 印刷設定で PDF ライターを使用して大きな文書を印刷しようとすると、プリンターが応答しなくなるか、次のエラーメッセージが表示されることがあります:

  「Emf viewer has stopped working.」[LC8882]

セッション/接続

- デスクトップの起動後すぐにデスクトップが非表示になることがあります。この問題は、Citrix Receiver for Windows から送信された TLS パケットが重複しているため発生します。[LC8724]

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

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

- StoreFront の 2 つのサイト間でアグリゲーションをセットアップすると、起動前セッションは作成されません。[LC8847]
- 第 1 ホップが VDA for Desktop OS、第 2 ホップが VDA 内で起動されるアプリケーションのダブルホップ環境では、VDA for Desktop OS を実行している最初のホップに再接続すると、数秒間画面がちらつくことがあります。[LC9071]
- Citrix Receiver for Windows を使用してデスクトップを起動しようとすると、しばらくしてタイムアウトになり失敗することがあります。StoreFront の **LaunchTimeoutMs** で起動タイムアウト値を長く設定した場合でも、この問題が発生します。[LC9369]
- StoreFront で内部ビーコンポイントを変更した後、Citrix Receiver for Windows を再起動するまで、Receiver for Windows からアプリケーションを起動できないことがあります。[LC9442]
- Win+Tab キーまたは Alt+Tab キーを使用して複数の公開アプリケーションを切り替えると、クライアント上で GDI オブジェクトが増加し、アプリケーションが応答しなくなり黒いピクセルが表示されることがあります。[LC9655]

スマートカード

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

システムの例外

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

ユーザーエクスペリエンス

- Citrix Receiver for Windows アプリケーションウィンドウは、アプリケーションを開いていなくても自動的に表示されることがあります。この問題は、管理者が公開アプリケーションを Citrix Studio から削除または無効にした場合に発生します。[LC8176]
- Citrix Receiver for Windows 内のアプリケーションを更新すると、［スタート］メニューとタスクバーアイコンがちらついて表示されることがあります。[LC8890]

- Citrix Receiver for Windows セッションでマウスカーソルが表示されない、または小さく表示されます。これは、Microsoft Windows 10 を実行しているエンドポイントで異なる DPI を持つ複数のモニターを使用している場合に発生する可能性があります。[LC8915]
- Citrix Receiver for Windows セッションでマウスカーソルが通常より小さく表示されることがあります。この問題は、Microsoft Windows 10 以降のバージョン 1607 を実行しているエンドポイントで高解像度ディスプレイを使用している場合に発生することがあります。

  以下は、このシナリオの制限事項です。

  - リバースシームレスモードで左クリックすると、マウスポインタが小さく表示されます。クリックを解除すると正常なサイズに戻ります。
  - Windows 10 バージョン 1607 および Windows Server 2016 より前のバージョンの VDA for Desktop OS および VDA for Server OS で実行すると、低解像度でマウスポインタがわずかに拡大されます。
  - マルチモニター環境では、モニターの DPI が異なるとマウスポインタが正しく表示されません。この問題は、モニター間でウィンドウを移動した時に発生し、アプリケーションウィンドウのサイズを変更することで修正できます。
  - マウスポインタは、起動したデスクトップの Desktop Viewer では小さく表示されたままです。[LC9221]
- この修正では、Enlightened Data Transport（EDT）のパフォーマンスおよび品質のマイナーな強化に対応しています。[LC9417]

Citrix Receiver for Windows 4.9 LTSR CU2

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR CU1

クライアントデバイスの問題

- Voice over Internet Protocol（VOIP）通話中に、user1 が公開された録音アプリケーションを起動して録音を開始すると、user1 のマイクの音声は通話中に聞こえなくなります。user2 の音声は user1 に聞こえます。[LC8713]

HDX MediaStream Flash リダイレクト

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

HDX MediaStream Windows Media リダイレクト

- 特定のサードパーティ製アプリケーションを使用してメッセージを送信する時に、通知アラートが聞こえなくなります。この修正により、短時間再生されるサウンドのサポートが強化されます。[LC8468]

HDX シームレスローカルアプリケーション

- 起動時に設定する必要がある 64 ビットアプリケーションでローカルアプリアクセス機能「**"KEYWORDS:prefer="*pattern*""**」を使用すると、アプリケーションの起動に失敗することがあります。[LC8580]

インストール、アンインストール、アップグレード

- Citrix Receiver for Windows をアップグレードすると、カスタム仮想チャネルに必要な特定のレジストリキーが削除されることがあります。[LC8414]
- Citrix Receiver for Windows の自動更新インストール後、自動更新インストールのコマンドラインスイッチが保持されないことがあります。その結果、自動更新構成がデフォルトのオプションに設定されます。[LC9103]

セッション/接続

- セッションの起動に失敗して、次のエラーメッセージが表示されることがありました。

  「ICA ファイルに無効な署名のないパラメーターが含まれています。」

  新しい ADMX ファイルをアップグレードするか、置き換える前に、ICA ファイルの署名関連ポリシー［ICA ファイルの署名を有効にします］を［構成されていません］に設定します。

  注: 参照番号 LC5338 は、StoreFront 3.0.4000、StoreFront 3.9 以降のバージョンで機能します。[LC5338]
- VDA for Server OS の最初のホップで Citrix Receiver for Windows から selfservice.exe プロセスを起動する場合、最初のホップを切断すると、特定のサードパーティ製アプリケーションまたは Windows タスクスケジューラが「SelfService.exe -disconnectapps」を実行して、最初のホップの切断時に 2 番目のホップを切断します。最初のホップに再接続すると、「SelfService.exe - reconnectapps」が実行され、最初のホップの再接続時に 2 番目のホップに再接続します。このシナリオでは、Citrix Receiver for Windows がバックグラウンドで表示されずにフォアグラウンドで表示され、再接続されたアプリケーションがバックグラウンドで表示されることがあります。[LC8224]

システムの例外

- Mobile Receiver 仮想チャネルを使用すると、wfica32 プロセスが断続的に終了することがあります。[LC8526]

- Bloomberg キーボードの生体認証を使用すると、ユーザーセッションが予期せず終了することがあります。[LC8766]
- USB リダイレクトによってリダイレクトされるセッション内で Bloomberg キーボードの指紋スキャナーを使用すると、ユーザーセッションが予期せず終了することがあります。[LC8928]

ユーザーエクスペリエンス

- IME（Input Method Editor）言語バーでカスタマイズされたフレーズ機能を使用すると、ユーザーセッションで特定の文字がランダムに失われることがあります。[LC6155]
- デスクトップとタスクバーで手動で作成されたストリーム配信アプリケーションのショートカットが削除されます。[LC7500]
- Citrix Receiver for Windows を起動する時、Receiver Self-Service ウィンドウでサブスクライブしたアプリケーションに bpp=4 のアイコンが含まれている場合、スタートメニューとデスクトップショートカットがちらつくことがあります。[LC8480]
- 特定のサードパーティ製アプリケーションが、HDX シームレスアプリケーションを有効にしたセッションに多数の文字を送信しようとすると、一部の文字しかアプリケーションに送信されないことがあります。[LC8560]
- 公開デスクトップを Windows 7 クライアントマシンから全画面モードで起動した場合、リダイレクトされた Flash ビデオを再生すると、［常に手前に表示］ に設定されているアプリケーションが Desktop Viewer ウィンドウの前に表示されることがあります。この修正はデフォルトでは、無効になっています。

  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* ビットシステムの場合：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenDesktop\DesktopViewer

    名前：PreventAlwaysOnTopWindowPopover

    種類：DWORD

    値：2。修正プログラムを無効にするには、レジストリキーの値を 0 に設定するか、レジストリキーを削除します。

  - *64* ビットシステムの場合：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenDesktop\DesktopViewer

    名前：PreventAlwaysOnTopWindowPopover

    種類：DWORD

    値：2。修正プログラムを無効にするには、レジストリキーの値を 0 に設定するか、レジストリキーを削除します。[LC8616]
- Citrix Receiver for Windows でアプリケーションを更新すると、手動でタスクバーに固定された Microsoft Outlook アプリケーションアイコンが消えることがあります。[LC8785]

ユーザーインターフェイス

- Citrix Receiver for Windows で ［設定］オプションを変更し、StoreFront でストアを ［ユーザーのサブスクリプションの無効化（必須ストア）］ 設定で構成すると、アプリケーションが［スタート］メニューに表示されないことがあります。[LC8648]

Citrix Receiver for Windows 4.9 LTSR CU1

修正前のバージョン：Citrix Receiver for Windows 4.9 LTSR

クライアントデバイスの問題

- ドッキングステーションまたは USB ハブに接続されたキーボード、マウス、モニターなどのデバイスは使用できません。この問題は、ユーザーセッションが全画面モードである場合、またはセッションウィンドウにフォーカスがある場合、およびユーザーセッションを開始した後にドッキングステーションまたはハブをクライアントマシンに接続した場合に発生します。[LC8295]

コンテンツリダイレクト

- 移動プロファイルを使用して Citrix Receiver for Windows にログオンすると、ファイルタイプの関連付けが機能しないことがあります。[LC8042]

HDX RealTime

- VDA 上に同じモデルの複数の Web カメラがインストールされている環境で、最新の Web カメラだけがセッションから認識されマップされることがあります。この修正により、同じモデルの複数の Web カメラを、セッション内の任意のビデオ会議アプリケーションで使用できます。

  > 注:
  >
  > – 参照番号 LC5008 がインストールされていると、［基本設定］タブから Web カメラを切り替えることができない場合があります。
  > – この問題を解決するには、サーバー側にも参照番号 LC5008 に対する修正をインストールする必要があります。[LC5008]

セッション/接続

- 「Run As」コマンドを使用し、システムで Redirector.exe プロセスを実行している場合、現在ログインしているユーザーとは別のユーザーとして Microsoft Internet Explorer を起動しようとすると、ブラウザーは起動することがありますが、コンテンツの読み込みに約 20 ～ 30 秒かかります。[LC5227]

- Mozilla Firefox を使用してデスクトップを起動しようとすると、失敗することがあります。この問題は、Desktop Viewer が Internet Explorer の一時ディレクトリから以前作成した ICA ファイルを削除できない場合に発生します。これにより、新しいセッションを開始する時に ICA ファイルのコピーを妨げる「アクセス拒否」エラーが発生します。[LC7883]
- ［スタート］メニューまたはデスクトップショートカットからアプリケーションを起動すると、アプリケーションは起動することがありますが、次のエラーメッセージが表示されます。

  「このファイルが見つかりません。パスとファイル名が正しいかどうか確認してください。」[LC8253]
- Citrix Receiver for Windows 4.8 がインストールされていると、従業員 Web ポータルの特定の機能が正しく機能しないことがあります。ただし、Microsoft Internet Explorer で Citrix ICA クライアントの ActiveX コントロールが無効になっている場合、Web サイトは正常に機能します。[LC8428]

システムの例外

- 以下のメッセージが表示され、Citrix Receiver for Windows が予期せず終了することがあります。

  「Citrix HDX Engine has stopped working」（Citrix HDX Engine が動作を停止しました）[LC8040]
- Citrix Receiver for Windows 4.8 でブルースクリーンエラーが発生することがあります。この問題は、特定の多機能キーボードモデルを使用してシステムを再起動し、キーボードの接続と接続解除を繰り返すと発生します。[LC8182]
- オーディオファイルの再生中にユーザーデバイスからヘッドフォンを取り外した後、セッションを切断して再接続するまで、セッションが応答しなくなることがあります。[LC8243]
- シームレスな公開アプリケーションでキーボードショートカット「Alt+Enter」を使用すると、wfica32.exe プロセスが予期せず終了することがあります。[LC8317]
- ダブルホップシナリオでは、クライアント間でセッションを切り替えると、wfica32.exe プロセスが予期せず終了することがあります。[LC8354]

ユーザーエクスペリエンス

- オーディオ品質を高品質に設定してサウンドを録音すると、録音品質が低下することがあります。[LC8241]
- マルチモニター環境でシームレスウィンドウを全画面から元のサイズに復元し、アプリケーション全体を表示するために元のモニターにドラッグすると、ウィンドウが正しく切り取られないことがあります。その結果、ウィンドウの一部のみが表示されます。この問題は、モニターよりも大きなサイズの、一部が画面外にあるシームレスウィンドウで発生します。[LC8325]
- ストアの web.config ファイルでショートカットオプションを設定すると、公開アプリケーションのショートカットが［スタート］メニューおよびデスクトップから消えることがあります。

  注： この修正により、参照番号 LC7577 の完全な修正が提供されます。[LC8391]

- Epic Hyperspace を使用中にシームレスモードでセッションを起動すると、エンドポイントのローカルで実行中のその他のアプリケーションをフォアグラウンドに表示できず、Epic Hyperspace アプリケーションのフォーカスは、アプリケーションを最小化するまでフォアグラウンドに表示され続けることがあります。[LC8462]
- 公開デスクトップに接続すると、ウィンドウのサイズを変更すると変更される空白の領域がデスクトップに表示されることがあります。このエラーは、従来のグラフィックモードを使用している場合に発生します。[LC8518]

Citrix Receiver for Windows 4.9 LTSR

修正前のバージョン：Citrix Receiver for Windows 4.8

HDX 3D Pro

- HDX 3D Pro を有効にした VDA で特定のサードパーティ製アプリケーションを使用すると、VDA が切断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。

  - *32* ビット *Windows*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

    Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

    名前：Tw2IgnoreValidationErrors

    種類：REG_SZ

    値：TRUE

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

    Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

    名前：Tw2IgnoreExecutionErrors

    種類：REG_SZ

    値：TRUE
  - *64* ビット *Windows*

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

    名前：Tw2IgnoreValidationErrors

    種類：REG_SZ

    値：TRUE

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

名前：Tw2IgnoreExecutionErrors

種類：REG_SZ

値：TRUE [LC7655]

サーバー/サイトの管理

- ユーザーパスワードの有効期限が切れると、［パスワードの変更］の入力フォームが反応しなくなることがあります。この問題は、新しいパスワードが要件を満たしていない場合に発生します。[LC7943]

セッション/接続

- Knowledge Center のCTX128232の手順どおりにデスクトップグループを外部クライアント IP アドレスに割り当てた場合、NetScaler Gateway 経由で公開デスクトップを起動できないことがあります。次のエラーメッセージが表示されます。

  「アプリケーションを起動できません」[LC5932]

- Citrix Receiver for Windows が Juniper SSL VPN 経由で StoreFront に接続すると、接続に失敗することがあります。この問題は、StoreFront の URL の DNS 解決が失敗した場合に発生します。[LC6711]
- Citrix Receiver for Windows が Web カメラを使用中の VDA から切断されると、予期せず終了することがあります。この問題は、Web カメラの実行中に VDA から切断されると発生します。[LC6815]
- Desktop Lock が有効な場合、StoreFront セッションの期限が切れるとユーザーセッションが自動的に切断されることがあります。[LC6984]
- 医療用の音声入力に Epic Hyperspace ソフトウェアを使用している場合、ユーザーデバイスでの録音中に音声入力レコーダーが反応しなくなることがあります。[LC7435]
- Citrix ICA クライアントオブジェクト（ICO）API を使用して NetScaler 経由でクライアントセッションを起動し、グループポリシーオブジェクトで Client Selective Trust を構成すると、セッションが起動できないことがあります。[LC7575]
- レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle（32 ビット Windows）または HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle（64 ビット Windows）でレジストリ値 DisableStubCreation を true に設定すると、ファイルの種類の関連付けによって対象ドキュメントを開けないことがあります。この問題は、次のレジストリキーの関連するファイル拡張子に「%1」パラメーターがない場合に発生します。HKEY_CURRENT_USER\SOFTWARE\Classes\Dazzle.**.**.1\shell\open\command [LC7619]
  拡張子 > アプリ名 >
- ローカルアプリアクセスが有効な場合、全画面モードで起動されたデスクトップ OS セッションの VDA のサイズと位置が正しく表示されないことがあります。[LC7646]

- グループポリシー設定やコマンドラインでストアを追加して、Windows ログオン時の再接続を構成すると、Citrix Receiver for Windows が Windows ログオンで自動的に再接続されないことがあります。[LC7679]
- スリープモードから再開すると、［クライアントの自動接続］が機能しなくなり、セッションを再接続できなくなることがあります。[LC7705]
- ローカルアプリアクセスが有効な場合、wfcrun32.exe プロセスが予期せず終了することがあります。[LC7946]

スマートカード

- ポリシー［対話型ログオン：スマートカード取り出し時の動作］のローカルセキュリティ設定［ワークステーションをロックする］がユーザーセッションで設定されている時に、セッションからスマートカードリーダーを削除しても、セッションがロックされないことがあります。[LC7571]
- ユーザーセッションで SCardListReaderGroup API がサーバーから呼び出されると、Citrix Receiver for Windows がクライアント側で呼び出された API を実行しないことがあります。[LC7699]

ユーザーエクスペリエンス

- ユーザーセッションのアプリケーションで、デバイスのタッチスクリーンをダブルタップしても機能しないことがあります。[LC6698]
- シームレスセッションのサードパーティ製アプリケーションウィンドウでフォーカスを切り替えるためにタスクバーアイコンをクリックしても、アプリケーションの画面がフォアグラウンドに表示されないことがあります。[LC6709]
- マウスボタンを押したままユーザーデバイスの解像度を変更すると、マウスを離してもシームレスアプリケーションがその状態を受信できないことがあります。その結果、マウスキャプチャが失われます。[LC7419]
- ストアの web.config ファイルでショートカットオプションを設定すると、公開アプリケーションのショートカットが［スタート］メニューおよびデスクトップから消えることがあります。[LC7577]
- Epic Hyperspace を使用中にシームレスモードでセッションを起動すると、エンドポイントのローカルで実行中のその他のアプリケーションをフォアグラウンドに表示できず、Epic Hyperspace アプリケーションのフォーカスは、アプリケーションが最小化されるまでフォアグラウンドに表示され続けることがあります。[LC7906]

注：このバージョンの Citrix Receiver for Windows には、4.8、4.7、4.6、4.5、4.4、4.3、4.2、4.1、および4.0の各バージョンに含まれるすべての修正も入っています。

既知の問題

July 15, 2019

Citrix Receiver for Windows 4.9 LTSR CU7 の既知の問題

- クライアントが Flash をレンダリングした場合、または Windows Media リダイレクトが有効な場合、タスクバーのプレビューが正しく機能しないことがあります。[LCMRFWIN-2013]

Citrix Receiver for Windows 4.9 LTSR CU6 の既知の問題

このリリースで確認されている新しい問題はありません。

Citrix Receiver for Windows 4.9 LTSR CU5 の既知の問題

このリリースで確認されている新しい問題はありません。

Citrix Receiver for Windows 4.9 LTSR CU4 の既知の問題

このリリースで確認されている新しい問題はありません。

Citrix Receiver for Windows 4.9 LTSR CU3 の既知の問題

このリリースで確認されている新しい問題はありません。

Citrix Receiver for Windows 4.9 LTSR CU2 の既知の問題

このリリースで確認されている新しい問題はありません。

Citrix Receiver for Windows 4.9 LTSR CU1 の既知の問題

Citrix Receiver for Windows 4.9 には、バージョン4.5、4.6、4.7、4.8に存在していた既知の問題の一部と、以下の既知の問題が含まれています:

- Framehawk を有効にした場合、ログオンまたはログオフを何度も試みると、wfica32.exe プロセスが予期せず終了することがあります。[LCMRFWIN-704]

Citrix Receiver for Windows 4.9 の既知の問題

- Surface Pro のウィンドウモードでデスクトップセッションを起動し、デスクトップモードからタブレットモードに切り替えると、Desktop Viewer オプションが反応しなくなります。[RFWIN-5837]

サードパーティ製品についての通知

June 24, 2019

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

Citrix Receiver for Windows のサードパーティ製品についての通知（**PDF** のダウンロード）

システム要件と互換性

June 24, 2019

要件

- このバージョンの Citrix Receiver for Windows では、少なくとも 500MB のディスク空き容量と 1GB の RAM が必要です。
- .NET Framework の最小要件
  - Self-Service Plug-in 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 のユーザーインターフェイス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。
  - .NET 2.0 Service Pack 1 および Microsoft Visual C++ 2008 Service Pack 1 再頒布可能パッケージが必要です。

互換性マトリックス

Citrix Receiver for Windows バージョン 4.9 は、以下の Windows オペレーティングシステムおよび Web ブラウザーと互換性があります。また、シトリックス製品マトリクスの一覧にある、XenApp、XenDesktop、NetScaler Gateway の最新のサポート対象バージョンとも互換性があります。

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

オペレーティングシステム	Web ブラウザー
Windows 10 [1]	Internet Explorer
Windows 10 IoT Enterprise [2]	
Windows 8.1 32 ビット版および 64 ビット版（Embedded エディションを含む）	最新版の Google Chrome（StoreFront 必須）
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）	最新版の Mozilla Firefox
Windows Thin PC	Microsoft Edge
Windows Server 2016	
Windows Server 2012 R2、Standard、および Datacenter エディション。	
Windows Server 2012、Standard、および Datacenter エディション。	
Windows Server 2008 R2（64 ビット版）	

[1]Windows 10 Anniversary Update、Creators Update、Falls Creators Update、April 2018 Update（Version 1803）、および October 2018 Update（Version 1809）をサポート。
[2]Windows 10 IoT Enterprise 2015 LTSB、Windows 10 IoT Enterprise 2016 LTSB、Anniversary Update、Creators Update、Falls Creators Update、April 2018 Update（Version 1803）、および October 2018 Update（Version 1809）をサポート。

> 注
>
> - October 2018 Update（Version 1809）は、Receiver for Windows バージョン 4.9 CU5 以降でのみサポートされています。
> - April 2018 Update は、Receiver for Windows バージョン 4.9 CU3 以降でのみサポートされています。
> - Falls Creators Update は、Receiver for Windows バージョン 4.9 CU1 以降でのみサポートされています。Receiver for Windows バージョン 4.9 ではサポートされていません。

サポートに関するマトリックス

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

接続、証明書、認証

June 24, 2019

接続

1. HTTP ストア
2. HTTPS ストア
3. NetScaler Gateway 10.5 以降
4. Web Interface 5.4

Citrix Receiver for Windows を VDA に接続するか、Windows ドメイン参加マシン、管理対象デバイス（ローカルおよびリモート、VPN ありまたはなし）、ドメイン非参加マシンで ICA セッションを確立することができます。

証明書

1. プライベート（自己署名）証明書
2. ルート証明書
3. ワイルドカード証明書
4. 中間証明書

プライベート（自己署名）証明書

リモートゲートウェイにプライベート証明書がインストールされている場合は、組織の証明機関のルート証明書をユーザーデバイスにインストールしないと、Citrix Receiver for Windows を使用して Citrix リソースにアクセスできません。

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

ルート証明書のインストール

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

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

ワイルドカード証明書

ワイルドカード証明書は、同一ドメイン内のサーバーで使用されます。

Citrix Receiver for Windows はワイルドカード証明書をサポートしますが、組織のセキュリティポリシーに従って使用する必要があります。実際には、サブジェクトの別名（SAN）拡張領域内のサーバー名一覧に含まれている証明書など、ワイルドカード証明書に代わるものを考慮することがあります。このような証明書は、私的証明機関および公的証明機関の両方が発行します。

中間証明書

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

認証

StoreFront での認証

	ブラウザーを使った **Receiver for Web**	**StoreFront** サービスサイト（ネイティブ）	**StoreFront XenApp Services** サイト（ネイティブ）	**NetScaler** から **Receiver for Web**（ブラウザー）	**NetScaler** から **StoreFront Services** サイト（ネイティブ）

匿名	はい	はい			
ドメイン	はい	はい	はい	はい *	はい *
ドメインパススルー	はい	はい	はい		
セキュリティトークン				はい *	はい *
2 要素（セキュリティトークンがあるドメイン）*				はい *	はい *
SMS				はい *	はい *
スマートカード	はい	はい		はい	はい
ユーザー証明書				はい（NetScaler のプラグイン）	はい（NetScaler のプラグイン）

* デバイスへの NetScaler プラグインのインストールは不問。

> 注
>
> Citrix Receiver for Windows 4.8 は、NetScaler Gateway から StoreFront ネイティブサービスを通じて 2 要素認証（ドメイン + セキュリティトークン）をサポートします。

Web Interface での認証

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

	Web Interface（ブラウザー）	**Web Interface XenApp Services** サイト	**NetScaler** から **Web Interface**（ブラウザー）	**NetScaler** から **Web Interface XenApp Services** サイト
匿名	はい			
ドメイン	はい	はい	はい *	

ドメインパススルー	はい	はい	
セキュリティトークン			はい *
2 要素（セキュリティトークンがあるドメイン）*			はい *
SMS			はい *
スマートカード	はい	はい	
ユーザー証明書			はい（NetScaler のプラグイン）

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

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

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

インストール

June 24, 2019

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
  - 初めて使用するユーザーが Citrix Receiver for Windows のインストールファイルを Citrix.com などのダウンロードサイトから入手した場合は、サーバー URL の代わりにメールアドレスを入力してアカウントをセットアップできます。これにより、メールアドレスに関連付けられた NetScaler Gateway や StoreFront サーバーが識別され、ログオン用のメッセージが表示されてインストールを続行します。この機能は、「メールアドレスによるアカウント検出」と呼ばれます。注：初めて使用するユーザーとは、デバイスに Citrix Receiver for Windows をインストールしていないユーザーを指します。
  - Citrix.com 以外の場所（Receiver for Web サイトなど）から Citrix Receiver for Windows をダウンロードした場合は、メールアドレスによるアカウントセットアップを使用できません。
  - Citrix Receiver for Windows の構成が必要な環境では、ほかの方法で Receiver をユーザーに配布してください。

- Receiver for WebまたはWeb Interface のログオン画面からの自動インストール
  - 初めて使用するユーザーがアカウントをセットアップするには、サーバーの URL を入力するかプロビジョニング（CR）ファイルをダウンロードします。
- ESD（Electronic Software Delivery：電子ソフトウェア配信）ツールによるインストール
  - 初めて使用するユーザーがアカウントをセットアップする場合、サーバーの URL を入力するかプロビジョニングファイルを開く必要があります。

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

HDX RealTime Media Engine（RTME）

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

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

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

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

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

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

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

StoreFront 環境:

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

Web Interface で展開する場合

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

アップグレード時の注意事項

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

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

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

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

January 9, 2019

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

空きディスクスペースの検証

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

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

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

次の表に、Citrix Receiver for Windows をインストールする場合の最小必要ディスクスペースの詳細を示します。

インストールの種類	必須ディスクスペース
新規インストール	320MB
Citrix Receiver のアップグレード	206MB

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

Citrix Receiver for Windows のアンインストール

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

> 注
>
> Citrix Receiver for Windows のインストールを続行する前に、Citrix HDX RTME パッケージのアンインストールを求めるメッセージが表示されます。詳しくは、Knowledge Center のCTX200340を参照してください。

コマンドラインインターフェイスを使用して **Citrix Receiver for Windows** をアンインストールするには

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

CitrixReceiver.exe /uninstall

Citrix Receiver for Windows がアンインストールされても、receiver.adm/receiver.adml または receiver.admx により作成された Citrix Receiver for Windows のカスタム設定レジストリキーは、HKEY_LOCAL_MACHINE および HKEY_LOCAL_USER の下の Software\Policies\Citrix\ICA Client ディレクトリに残ります。

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

コマンドラインパラメーターを使用した構成とインストール

June 24, 2019

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

領域要件について詳しくは、「システム要件」を参照してください。

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

CitrixReceiver.exe [] オプション **>**

自動更新

オプション	/AutoUpdateCheck = auto/manual/disabled
説明	利用可能な更新を Citrix Receiver for Windows が検出したことを示します。**Auto** - 更新が利用可能になると通知します（デフォルト）。**Manual** - 更新が利用可能になっても通知されません。手動で更新をチェックしてください。**Disabled** - 自動更新を無効にします。

オプション	/AutoUpdateCheck = auto/manual/disabled
使用サンプル	CitrixReceiver.exe / AutoUpdateCheck = auto、CitrixReceiver.exe / AutoUpdateCheck = manual、CitrixReceiver.exe / AutoUpdateCheck = disabled

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

オプション	/DeferUpdateCount
説明	後で通知するオプションが表示される回数を示します。回数を設定して更新を保留できることを示します。**-1** - 任意の回数通知を保留できます（デフォルト値 =-1）。**0** - ［後で通知する］オプションは表示されません。**** - この回数分、［後で通知する］オプションが表示されます。たとえば、値を 10 に設定すると、後で通知するオプションが 10 回表示されます。その他の数字 >
使用サンプル	CitrixReceiver.exe /DeferUpdateCount=-1、CitrixReceiver.exe /DeferUpdateCount=-0、CitrixReceiver.exe /DeferUpdateCount= その他の数字 >

オプション	/AURolloutPriority
説明	ロールアウトを行うことができるタイミングを示します。**Fast** - 配信期間の最初に更新がロールアウトされます。**Medium** - 配信期間の中頃に更新がロールアウトされます。**Slow** - 配信期間の最後に更新がロールアウトされます。
使用サンプル	CitrixReceiver.exe /AURolloutPriority=Fast、CitrixReceiver.exe /AURolloutPriority=Medium、CitrixReceiver.exe /AURolloutPriority=Slow

コンテンツの双方向リダイレクトの有効化

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

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

ローカルアプリアクセスの有効化

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

使用方法情報の表示

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

UI インストール時の再起動の抑制

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

サイレントインストール

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

認証時のシングルサインオンの有効化

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

/includeSSON の指定時にシングルサインオンを有効化

オプション	ENABLE_SSON={Yes | No}
説明	/includeSSON の指定時にシングルサインオンを有効にします。デフォルト値は Yes です。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。
使用サンプル	CitrixReceiver.exe ENABLE_SSON=Yes

常時トレース

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

カスタマーエクスペリエンス向上プログラム（**CEIP**）の使用

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

インストールディレクトリの指定

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

ユーザーデバイスの識別

オプション	CLIENT_NAME= クライアント名 >
説明	クライアント名を指定します。ここでは、サーバーでユーザーデバイスを識別するために使用される名前です。デフォルト値は、%COMPUTERNAME% です。クライアント名 >
使用サンプル	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

ダイナミッククライアント名

オプション	ENABLE_CLIENT_NAME= Yes | No
説明	ダイナミッククライアント名機能を有効にすると、コンピューター名がクライアント名として使用されます。この場合、ユーザーがコンピューター名を変更すると、クライアント名もそれに応じて変更されます。デフォルトは Yes です。ダイナミッククライアント名機能を無効にするには、このプロパティを No に設定し、CLIENT_NAME プロパティの値を指定します。

オプション	ENABLE_CLIENT_NAME= Yes | No
使用サンプル	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

指定したコンポーネントのインストール

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

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

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

オプション	ALLOWADDSTORE={N | S | A}
説明	Merchandising Server の配信により構成されなかったストアをユーザーが追加および削除できるかどうかを指定します。ユーザーは、Merchandising Server の配信により構成されたストアを有効または無効にできますが、そのようなストアの削除や、名前や URL の変更はできません。デフォルトは S です。次のオプションがあります：N - ユーザーによるストアの追加や削除を許可しません。S - ユーザーによるストアの追加や削除を許可します（HTTPS で構成されたセキュアなストアのみ）。A - ユーザーによるストアの追加や削除を許可します（HTTPS または HTTP で構成されたストア）。Citrix Receiver をユーザー単位でインストールする場合には適用されません。この機能は、レジストリキー HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazz 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：HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazz 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。HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazz 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。［TransportType］に［HTTP］を指定して StoreFront で構成されたストアを追加するには、HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Auth に値 ConnectionSecurityMode（REG_SZ）を追加して、それを Any を設定します。Citrix Receiver を終了して再起動します。
使用サンプル	CitrixReceiver.exe ALLOWADDSTORE=N

PNAgent プロトコルを使用してストアの資格情報をローカルで保存

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

証明書の選択

オプション	AM_CERTIFICATESELECTIONMODE={Prompt |SmartCardDefault | LatestExpiry}
説明	このオプションを使用して証明書を選択します。デフォルト値は Prompt で、ユーザーが証明書を選択するための一覧が表示されます。デフォルトの証明書（スマートカードプロバイダー指定の証明書）が使用されるようにしたり、長い有効期限が残っているものが使用されるようにしたりできます。有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。このオプションを使用して証明書を選択します。デフォルト値は Prompt で、ユーザーが証明書を選択するための一覧が表示されます。デフォルトの証明書（スマートカードプロバイダー指定の証明書）が使用されるようにしたり、長い有効期限が残っているものが使用されるようにしたりできます。有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。この機能は、レジストリキー HKEY_CURRENT_USER または HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Auth Prompt | SmartCardDefault | LatestExpiry } で設定することもできます。最適な証明書をユーザーが選択できるように、HKEY_CURRENT_USER での設定は、HKEY_LOCAL_MACHINE の設定よりも優先されます。
使用サンプル	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

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

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

Kerberos の使用

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

レガシー **FTA** アイコンの表示

オプション	LEGACYFTAICONS={False | True}
説明	レガシー FTA アイコンを表示するにはこのオプションを使用します。デフォルト値は、False です。サブスクライブするアプリケーションに関連付けられているファイルタイプのドキュメントに、そのアプリケーションアイコンを表示するかどうかを指定します。この引数を False に設定すると、特定のアイコンが関連付けられていないドキュメントに Windows によるアイコンが表示されます。Windows によるアイコンは、汎用のドキュメントアイコン上にアプリケーションの小さいアイコンが重なって表示されます。Windows 7 を使用するユーザーに Microsoft Office アプリケーションを配信する場合は、このオプションを有効にすることをお勧めします。
使用サンプル	CitrixReceiver.exe LEGACYFTAICONS=False

事前起動の有効化

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

［スタート］メニューショートカット用ディレクトリの指定

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

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

ストア名の指定

オプション	STOREx=”storename;http[s]://servername.domain/IISLocatio | Off] ; [storedescription]” [STOREy=”…”]
説明	このオプションを使ってストア名を指定します。Citrix Receiver で使用するストアを 10 まで指定します。値：x および y - 0 ～ 9 の整数。storename - デフォルト値は store。これは、StoreFront サーバーで構成される名前と同じである必要があります。servername.domain - ストアをホストするサーバーの完全修飾ドメイン名。IISLocation - IIS 内のストアへのパス。このストア URL は、StoreFront プロビジョニングファイルに記述されている URL と同じである必要があります。ストア URL は、「/Citrix/store/discovery」の形式で指定します。URL を取得するには、StoreFront からプロビジョニングファイルをエクスポートしてそれをメモ帳などのテキストエディターで開き、<Address> エレメントから URL をコピーします。•On | Off – Off を指定すると、無効なストアを配信できるようになります。これにより、そのストアにアクセスするかどうかをユーザーが選択できるようになります。このオプションを指定しない場合、デフォルトの設定は On になります。storedescription - ストアの説明（任意。「HR App Store」など）。注：このリリースでは、パススルー認証が正しく実行されるように、ストア URL に「/discovery」を追加してください。
使用サンプル	CitrixReceiver.exe STORE0=”Store;https://test.xx.com/Citrix/Store/Discovery

ユーザーデバイスでの **URL** リダイレクトの有効化

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

デスクトップショートカット用ディレクトリの指定

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

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

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

インストールのトラブルシューティング

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

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

コマンドラインを使用したインストールの例:

以下のコマンドでは、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"

仮想デスクトップやアプリケーションをコマンドラインで起動するには

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

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

June 24, 2019

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

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

- CheckAndDeployReceiverPerMachineStartupScript.bat

- CheckAndRemoveReceiverPerMachineStartupScript.bat

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

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

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

サンプルスクリプトを変更する

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

- **CURRENT VERSION OF PACKAGE**（パッケージの現在のバージョン）: ここに指定するバージョン番号が検証され、そのバージョンが存在しない場合は展開（インストール）が開始されます。たとえば、DesiredVersion= 3.3.0.XXXX に、展開するバージョンの番号を指定します。バージョンの一部（たとえば 3.3.0）を指定すると、その接頭辞を持つすべてのバージョン（3.3.0.1111、3.3.0.7777 など）に一致します。
- **PACKAGE LOCATION/DEPLOYMENT DIRECTORY**（パッケージの場所/展開ディレクトリ）: パッケージを格納するネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーに Everyone の読み取りアクセス許可を設定する必要があります。
- **SCRIPT LOGGING DIRECTORY**（スクリプトのログディレクトリ）: インストールログをコピーするネットワーク共有を指定します。この共有にアクセスするための認証はスクリプトで実行しません。共有フォルダーに Everyone の読み取り/書き込みアクセス許可を設定する必要があります。
- **PACKAGE INSTALLER COMMAND LINE OPTIONS**（パッケージインストーラーのコマンドラインオプション）: インストーラーに渡すコマンドラインオプションを指定します。コマンドライン構文については、「コマンドラインパラメーターを使用した Receiver for Windows の構成とインストール」を参照してください。

コンピューター単位のスタートアップスクリプトを追加するには

1. グループポリシー管理コンソールを開きます。
2. [コンピューターの構成] > [ポリシー] > [Windows の設定] > [スクリプト（スタートアップ/シャットダウン）] の順に選択します。
3. グループポリシー管理コンソールの右ペインで [スタートアップ] を選択します。
4. [プロパティ] ダイアログボックスで [ファイルの表示] をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. [スタートアップのプロパティ] ダイアログボックスで [追加] をクリックし、[参照] をクリックして新しく作成したスクリプトを検索し追加します。

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

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

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

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

サンプルのユーザー単位のスタートアップスクリプトの使用

通常、サーバー単位のスタートアップスクリプトを使用することをお勧めします。ただし、Citrix Receiver for Windows をユーザーごとに構成する必要がある場合は、ユーザー単位のスタートアップスクリプトを使用できます。XenDesktop および XenApp のメディアの Citrix Receiver for Windows and Plugins\Windows\Receiver\Startup_Logon_Scripts フォルダーには、2 つのユーザー単位のスタートアップスクリプトが含まれています。

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

ユーザー単位のスタートアップスクリプトを設定するには

1. グループポリシー管理コンソールを開きます。
2. ［ユーザーの構成］>［ポリシー］>［Windows の設定］>［スクリプト］の順に選択します。
3. グループポリシー管理コンソールの右ペインで［ログオン］を選択します。
4. ［ログオンプロパティ］ダイアログボックスで［ファイルの表示］をクリックし、表示されるフォルダーに適切なスクリプトをコピーしてウィンドウを閉じます。
5. ［ログオンのプロパティ］ダイアログボックスで［追加］をクリックし、［参照］をクリックして新しく作成したスクリプトを検索し追加します。

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

1. 作成した組織単位に展開対象のユーザーを移動します。
2. ユーザーデバイスを再起動して特定のユーザーでログオンします。

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

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

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

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

June 24, 2019

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

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

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

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

1. CitrixReceiver.exe をローカルコンピューターにダウンロードします。
2. CitrixReceiver.exe を CitrixReceiverWeb.exe と名称変更します。
3. 名前を変更した実行可能ファイルを通常の方法で展開します。StoreFront を使用する場合は、StoreFront ドキュメントの「構成ファイルを使った Receiver for Web サイトの構成」を参照してください。

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

November 12, 2018

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

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

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

Web Interface からインストールした Citrix Receiver for Windows では、メールアドレスによるアカウント検出機能を使用できません。メールアドレスによるアカウント検出機能が構成された環境では、初めて使用するユーザーが Citrix Receiver for Windows を Citrix.com からインストールすると、メールアドレスまたはサーバーアドレスの入力が求められます。ここでユーザーがメールアドレスを入力すると、メールアドレスを使ってアカウントを追加できないという内容のエラーメッセージが表示されます。ユーザーの混乱を避けるため、サーバーアドレスの入力のみが求められるようにします:

1. CitrixReceiver.exe をローカルコンピューターにダウンロードします。
2. CitrixReceiver.exe を CitrixReceiverWeb.exe と名称変更します。
3. XenApp Web サイトの構成ファイル内の ClientIcaWin32 パラメーターに、変更したファイル名を指定します。

   この機能を使用するには、Web Interface サーバー上に Citrix Receiver for Windows のインストールファイルを配置しておく必要があります。Web Interface のデフォルトでは、XenApp または XenDesktop のインストールメディアで提供されている名前で Citrix Receiver for Windows のインストールファイルが検索されます。
4. ユーザーは、CitrixReceiverWeb.exe ファイルのダウンロードサイトを信頼済みサイトの一覧に追加しておく必要があります。
5. 名前を変更した実行可能ファイルを通常の方法で展開します。

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

June 24, 2019

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

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

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

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

Citrix Receiver for Windows を SCCM 展開環境に追加する

1. ダウンロードした Citrix Receiver の Configuration Manager サーバー上のフォルダーにコピーして、Configuration Manager コンソールを起動します。
2. ［ソフトウェアライブラリ］、［アプリケーション管理］ の順に選択します。［アプリケーション］ を右クリックして、［アプリケーションの作成］ を選択します。
   アプリケーションの作成ウィザードが開きます。
3. ［全般］ ページで ［アプリケーションの情報を手動で指定する］ をクリックし、［次へ］ をクリックします。
4. ［一般情報］ ペインで、アプリケーションの情報（名前、製造元、ソフトウェアバージョンなど）を指定します。
5. アプリケーションカタログウィザードで、追加の情報（言語、アプリケーション名、ユーザーカテゴリなど）を指定して、［次へ］ をクリックします。

   注：ここで指定された情報は、ユーザーに表示されます。
6. ［展開の種類］ ペインで、［追加］ を選択して Citrix Receiver セットアップの展開の種類を構成します。展開の種類の作成ウィザードが開きます。
7. ［全般］ ペイン：展開の種類を Windows インストーラー（*.msi ファイル）に設定し、［展開の種類の情報を手動で指定する］ を選択して、［次へ］ をクリックします。
8. ［一般情報］ ペイン：展開の種類の詳細（例：Receiver の展開）を指定して、［次へ］ をクリックします。
9. ［コンテンツ］ ペイン：
   a) Citrix Receiver セットアップファイルのある場所へのパスを指定します。例：SCCM サーバー上のツール。
   b) ［インストールプログラム］ に次のいずれかを指定します：
      - CitrixReceiver.exe / silent（デフォルトのサイレントインストール）
      - CitrixReceiver.exe /silent /includeSSON（ドメインパススルーを有効にする）
      - CitrixReceiver.exe /silent SELFSERVICEMODE=false(セルフサービスモード以外で Receiver をインストールする）
   c) ［アンインストールプログラム］ に CitrixReceiver.exe /uninstall を指定します（SCCM でのアンインストールを有効にする）。
10. ［検出方法］ ペイン：［この展開の種類のプレゼンスを検出する規則を構成する］ を選択して ［句の追加］ をクリックします。［検出方法］ダイアログボックスが開きます。
11. ［設定の種類］ をファイルシステムに設定します。

12. ［このアプリケーションを検出するためのファイルまたはフォルダーを指定してください］ で、次のように設定します：

    - 種類 - ドロップダウンリストから、［ファイル］を選択します。
    - パス – %ProgramFiles (x86)%\Citrix\ICA Client\Receiver
    - ファイル名またはフォルダー名 - Receiver.exe
    - プロパティ - ドロップダウンリストから ［バージョン］ を選択します
    - 演算子 - ドロップダウンリストから ［次の値より大きいか等しい］ を選択します
    - 値 – **4.3.0.65534** を入力します

    注：この規則の組み合わせは、Citrix Receiver for Windows のアップグレードにも適用されます。

13. ［ユーザー側の表示と操作］ ペインで、次の値を設定します：

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

    ［次へ］ をクリックします。

    注：この展開の種類には、要件や依存関係を指定しないでください。

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

    成功メッセージが表示されます。

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

16. ［次へ］ をクリックして、［閉じる］ をクリックします。

配布ポイントを追加する

1. Configuration Manager コンソールで Receiver for Windows を右クリックして、［コンテンツの配布］を選択します。
   コンテンツの配布ウィザードが開きます。

2. ［コンテンツの配布］ペインで、［追加］**>**［配布ポイント］ を選択します。［配布ポイントの追加］ダイアログボックスが開きます。

3. コンテンツが利用可能な SCCM サーバーに移動して、［**OK**］ をクリックします。［完了］ペインで、成功メッセージが表示されます。

4. ［閉じる］ をクリックします。

Receiver をソフトウェアセンターに展開する

1. Configuration Manager コンソールで Receiver for Windows を右クリックして、［展開］ を選択します。
   ソフトウェアの展開ウィザードが開きます。

2. アプリケーションを展開するコレクション（デバイスコレクションまたはユーザーコレクション）を検索して、［次へ］ をクリックします。
3. ［展開設定］ ペインで ［アクション］ を［インストール］に ［目的］ を［必須］に設定します（無人インストールを有効にする）。［次へ］ をクリックします。
4. ［スケジュール］ ペインで、対象のデバイスでソフトウェアを展開するスケジュールを指定します。
5. ［ユーザー側の表示と操作］ ペインで、［ユーザーへの通知］ 動作を設定します。［メンテナンスの期限または期間中の変更を確定する（再起動が必要）］ を選択し、［次へ］ をクリックしてソフトウェアの展開ウィザードを終了します。［完了］ペインで、成功メッセージが表示されます。

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

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

デバイスコレクションを作成する

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

> 注
>
> **MSIRESTARTMANAGERCONTROL** 属性を **False** に設定すると、SCCM を使用した Citrix Receiver for Windows の展開が失敗することがあります。
> 分析によると、Citrix Receiver for Windows はこのエラーの原因ではありません。再試行で展開が成功することがあります。

構成

June 24, 2019

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

- アプリケーション配信の構成およびXenDesktop 環境の構成を実行します。XenApp 環境が正しく構成されていることを確認します。オプションについて理解し、ユーザーに対しわかりやすいアプリケーションについての説明を提供します。
- StoreFront アカウントを Citrix Receiver for Windows に追加して、セルフサービスモードの構成を実行します。このモードでは、ユーザーが Citrix Receiver for Windows のユーザーインターフェイスからアプリケーションをサブスクライブできます。
- グループポリシーオブジェクト管理用テンプレートによる構成
- ユーザーへのアカウント情報の提供をします。ユーザーがアカウントをセットアップするための情報を提供します。ユーザーは、このアカウントを使用して仮想デスクトップやアプリケーションにアクセスします。環境によっては、ユーザーが手作業でアカウントをセットアップする必要があります。

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

アプリケーション配信の構成

June 24, 2019

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

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

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

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

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

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

注：デリバリーグループのアプリケーションにわかりやすい説明を入力します。Web アクセスまたはセルフサービスモードを使う場合、Citrix Receiver for Windows のユーザーにはこの説明が表示されます。

NetScaler Gateway ストアの構成

グループポリシーオブジェクト管理用テンプレートを使って、ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則を構成することをお勧めします。
ドメインポリシーおよびローカルコンピューターのポリシーで receiver.admx/receiver.adml テンプレートファイルを使用することができます。ドメインポリシーの場合、グループポリシー管理コンソールを使ってテンプレートファイルをインポートします。これは、組織全体に存在する多くの異なるユーザーデバイスに Citrix Receiver for Windows の設定を適用するのに非常に有用です。単一のユーザーデバイスの場合は、デバイス上のローカルのグループポリシーエディターを使ってテンプレートをインポートします。

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

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
    - 単一のコンピューターにポリシーを適用する場合は、［スタート］メニューから起動します。
    - ドメインポリシーを適用する場合は、グループポリシー管理コンソールを使用して起動します。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］> ［従来の管理用テンプレート（ADM）］> ［Citrix コンポーネント］、［Citrix Receiver］> ［StoreFront］の順に開き、［NetScaler Gateway URL\StoreFront アカウント一覧］を選択します。

3. 設定を編集します。
    - ［ストア名］- ストアの表示名を指定します。
    - ［ストア URL］- ストアの URL を指定します。
    - ［#Store name］- NetScaler Gateway の後ろにあるストアの名前を指定します。
    - ［ストアの有効/無効］- ストアの状態を On または Off で指定します。
    - ［ストアの説明］- ストアの説明を入力します。
4. NetScaler の URL を追加または指定します。URL 名をセミコロンで区切って入力します：

> 次に例を示します：
>
> `HRStore; https://dtls.blrwinrx.com\##Store name;On; Store for HR staff`
> ここで、#Store name は NetScaler Gateway の後ろにあるストアの名前を、dtls.blrwinrx.com は NetScaler の URL を示します。
>
> GPO を使用して NetScaler Gateway を追加してから Citrix Receiver for Windows を起動すると、通知領域に以下のメッセージが表示されます。

制限事項：

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

セルフサービスモードの構成

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

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

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

デリバリーグループアプリケーションの説明に、適切なキーワードを追加します：

- 個々のアプリケーションを必須にして Citrix Receiver for Windows から削除できないようにするには、アプリケーションの説明に「KEYWORDS:Mandatory」という文字列を追加します。ユーザーが必須アプリケーションをサブスクリプション解除するための削除オプションはありません。

- アプリケーションがストアのユーザー全員に自動的にサブスクライブされるようにするには、説明に「KEYWORDS:Auto」という文字列を追加します。ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- 説明に「KEYWORDS:Featured」という文字列を追加すると、そのアプリケーションが Citrix Receiver の［おすすめ］一覧に表示され、ユーザーがそのアプリケーションを見つけやすくなります。

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

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

管理者として、グループポリシーを使ってショートカットを構成できます。

1. 単一のコンピューターにポリシーを適用する場合に［スタート］メニューから gpedit.msc を実行して、またはドメインポリシーを適用する場合にグループポリシー管理コンソールを使用して、グループポリシーエディターを開きます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、Receiver の Configuration フォルダーを参照してから receiver.admx（または receiver.adml）を選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrix コンポーネント］>［Citrix Receiver］>［Self Service］の順に開きます。
7. ［SelfServiceMode を管理します］を選択し、セルフサービスモードの Receiver ユーザーインターフェイスを有効または無効にします。
8. ［アプリのショートカットを管理します］を選択して、次のことを有効または無効にします。
    - デスクトップ上のショートカット
    - ［スタート］メニューのショートカット
    - デスクトップのディレクトリ
    - ［スタート］メニューのディレクトリ
    - ショートカットのカテゴリパス
    - ログオフ時にアプリケーションを削除
    - 終了時にアプリケーションを削除

9. ［ユーザーにアカウントの追加/削除を許可します］を選択して、1 つまたは複数のアカウントを追加または削除する権限をユーザーに付与します。

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

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

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

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

- ［スタート］メニュー内のすべてのショートカットを単一のフォルダー内に置くには、StartMenuDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- 管理者により変更されたアプリケーションが再インストールされるようにする（変更アプリケーションの自動再インストール機能）には、AutoReinstallModifiedApps を使用します。設定：”true” または”false”（デフォルトは true）。
- デスクトップ上のすべてのショートカットを単一のフォルダー内に置くには、DesktopDir を使用します。設定：文字列値、ショートカットが書き込まれるフォルダーの名前になります。
- クライアントの’add/remove programs’ でエントリを作成しないようにするには、DontCreateAddRemoveEntry を使用します。設定：”true” または”false”（デフォルトは false）。
- 以前にはストアから実行できたけど今はもう実行できないアプリケーションのショートカットや Receiver アイコンを削除するには、SilentlyUninstallRemovedResources を使用します。設定：”true” または”false”（デフォルトは false）。

web.config ファイルで、アカウントの XML セクションに変更を追加する必要があります。次の開始タグを検索し、このセクションに移動します。

<account id=… name=”Store”

このセクションは、</account> タグで終わります。

このタグ内にある、次のような最初のプロパティセクションに移動します。

<properties> <clear /> </properties>

このセクションの <clear /> タグの後ろにプロパティを追加できます。1 行ごとに名前と値を記述します。次に例を示します：

<property name=”PutShortcutsOnDesktop” value=”True” />

注：<clear /> タグの前に追加されたプロパティの要素は、無効になることがあります。プロパティ名と値の追加が任意の場合は、<clear /> タグを削除します。

プロパティの追加例：

<properties><property name=”PutShortcutsOnDesktop” value=”True” /><property name=”DesktopDir” value=”Citrix Applications” />

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

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

アプリケーションおよびデスクトップショートカットを［スタート］メニュー内に直接またはデスクトップ上に自動的に配置するよう、Citrix Receiver を構成できます。この機能は、以前にリリースされたバージョンの Citrix Receiver の機能と似ていますが、バージョン 4.2.100 では XenApp を使ってアプリケーション設定ごとにアプリケーションショートカットの配置を制御できる機能が導入されています。この機能は、終始一貫した場所に表示する必要がある一部のアプリケーションが存在する環境で有用です。

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenApp のアプリケーションごとの設定を使用します。

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

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

XenApp 7.6 のアプリケーションごとの設定を使った、アプリケーションショートカットの場所のカスタマイズ

XenApp 7.6 でアプリケーションごとの公開ショートカットを構成するには

1. Citrix Studio で、［アプリケーション設定］画面を開きます。
2. ［アプリケーション設定］画面で ［配信］ を選択します。この画面を使って、アプリケーションがユーザーにどのように配信されるかを指定できます。
3. アプリケーションの適切なアイコンを選択します。［変更］ をクリックして、必要なアイコンの場所を参照します。
4. （オプション）［アプリケーションカテゴリ］に、アプリケーションが表示される Receiver のカテゴリを指定します。たとえば、ショートカットを Microsoft Office アプリケーションに追加している場合は、「**Microsoft Office**」 と入力します。
5. ［ユーザーのデスクトップにショートカットを追加する］ チェックボックスをオンにします。
6. ［**OK**］ をクリックします。

列挙遅延またはアプリケーションスタブデジタル署名の削減

ユーザーのログオン時にアプリケーションの列挙に遅延が生じる場合、またはアプリケーションスタブにデジタル署名が必要な場合、ネットワーク共有から.EXE スタブをコピーする機能が Receiver により提供されます。

この機能を実行するには、次の複数の手順を実行します。

1. クライアントマシンにアプリケーションスタブを作成します。
2. アプリケーションスタブをネットワーク共有からアクセスできる場所にコピーします。
3. 必要な場合は、ホワイトリストを作成します（または、エンタープライズ証明書でスタブに署名します）。
4. レジストリキーを追加し、ネットワーク共有からスタブをコピーして Receiver がスタブを作成できるようにします。

RemoveappsOnLogoff および RemoveAppsonExit が有効で、ユーザーのログオン時にアプリケーション列挙に遅延が生じる場合、次の解決策により遅延を削減させます。

1. Regedit を使って、HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。
2. Regedit を使って、HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true” を追加します。HKCU は HKLM よりも優先されます。

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

ネットワーク共有に格納されている事前作成のスタブ実行可能ファイルをマシンが使用できるようにします。

1. クライアントマシン上で、すべてのアプリケーションに対するスタブ実行可能ファイルを作成します。これを実行するには、Receiver を使ってすべてのアプリケーションをマシンに追加します。Receiver は実行可能ファイルを生成します。
2. %APPDATA%\Citrix\SelfService からスタブ実行可能ファイルを取得します。必要なのは.exe ファイルだけです。
3. 実行可能ファイルをネットワーク共有にコピーします。
4. ロックダウンされる各クライアントマシンに対して次のレジストリキーを設定します。
   a) Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\ShareOne\ReceiverStub
   b) Reg add HKLM\Software\Citrix\Dazzle /v
   c) opyStubsFromCommonStubDirectory /t REG\SZ /d “true”。また、必要な場合は HKCU でこれらの設定を構成することもできます。HKCU は HKLM よりも優先されます。
   d) 設定をテストするため、Receiver を終了して再起動します。

ユースケースの例

このトピックでは、アプリケーションショートカットのユースケースについて紹介します。

［スタート］メニューに何を置くか、ユーザーが選べるようにする（セルフサービス）

数十（または数百の）アプリケーションがある場合は、ユーザーがお気に入りのアプリケーションを選択して、［スタート］メニューに追加できるようにするのが最も便利です。

［スタート］メニューに置くアプリケーションをユーザーが選べるようにするには	Citrix Receiver をセルフサービスモードに構成します。このモードでは、「自動プロビジョニング」 設定および 「必須」 アプリケーションキーワード設定も構成できます。
ユーザーが［スタート］メニューに置くアプリケーションを選べるようにして、また特定のアプリケーションショートカットをデスクトップに置くには	Citrix Receiver をオプション設定なしで構成して、デスクトップに置くアプリケーションについてアプリケーションごとの設定を使用します。必要に応じて、「自動プロビジョニング」 および 「必須」 アプリケーションを使用します。

［スタート］メニュー内にアプリケーションショートカットなし

コンピューターを家族で共有して使用していて、アプリケーションショートカットを一切置きたくないとします。このような場合、最も簡単なのはブラウザーアクセスです。いずれの構成も行わずに Citrix Receiver をインストール

し、Citrix Receiver for Web および Web interface をブラウズします。また、ショートカットをどこにも配置しないでセルフサービスアクセス用に Citrix Receiver を構成することもできます。

Citrix Receiver が［スタート］メニューに自動的にアプリケーションショートカットを配置しないようにするには	Citrix Receiver で PutShortcutsInStartMenu=False と構成します。アプリケーションごとの設定を使ってショートカットを置かない限り、セルフサービスモードであっても Citrix Receiver により［スタート］メニュー内にアプリケーションは配置されません。

［スタート］メニュー内、またはデスクトップ上にすべてにアプリケーションショートカットを置く

ユーザーが所有するアプリケーションが少ない場合は、そのすべてを［スタート］メニュー内やデスクトップ上に、あるいはデスクトップ上のフォルダー内に置くことができます。

Citrix Receiver によって［スタート］メニューにすべてのアプリケーションショートカットを自動的に配置するには	Citrix Receiver で SelfServiceMode =False と構成します。使用可能なすべてのアプリケーションが［スタート］メニュー内に表示されます。
すべてのアプリケーションショートカットをデスクトップ上に置く場合は	Citrix Receiver で PutShortcutsOnDesktop = true と構成します。使用可能なすべてのアプリケーションがデスクトップに表示されます。
すべてのショートカットをデスクトップ上のフォルダー内に置く場合は、	Citrix Receiver で DesktopDir= アプリケーションショートカットを置くデスクトップフォルダーの名前と構成します。

XenApp 6.5 または **7.x** でのアプリケーションごとの設定

ショートカットの場所を指定して、すべてのユーザーが同じ場所でそれにアクセスできるようにするには、XenApp のアプリケーションごとの設定を使用します。

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

カテゴリフォルダーまたは特定のフォルダーのアプリケーション

特定のフォルダー内にアプリケーションを表示する場合は、次のオプションを使用します。

Citrix Receiver により［スタート］メニューに置かれたアプリケーションショートカットを関連カテゴリ（フォルダー）内に表示するには	Citrix Receiver で **UseCategoryAsStartMenuPath=True** と構成します。注： Windows 8/8.1 および Windows 10 では、［スタート］メニュー内には階層分けされたフォルダーを作成できません。アプリケーションは個々に、または XexApp で定義されたカテゴリサブフォルダー内ではないルートフォルダーの下に表示されます。
Citrix Receiver により［スタート］メニューに置かれたアプリケーションを特定のフォルダー内に配置するには	Citrix Receiver で StartMenuDir=［スタート］メニューフォルダーの名前と構成します。

ログオフまたは終了時にアプリケーションを削除

エンドポイントをほかのユーザーと共有していて、自分のアプリケーションがそのユーザーには表示されないようにしたい場合は、ログオフまた終了時にアプリケーションが削除されるようにすることができます。

ログオフ時に Citrix Receiver によりすべてのアプリケーションが削除されるようにするには	Citrix Receiver で RemoveAppsOnLogoff=True と構成します。
終了時に Citrix Receiver によりアプリケーションが削除されるようにするには	Citrix Receiver で RemoveAppsOnExit=True と構成します。

ローカルアプリアクセスのアプリケーションの構成

ローカルアプリアクセスのアプリケーションを構成する場合は次のようにします。

- 説明に「KEYWORDS:prefer="<pattern>"」という文字列を追加すると、Citrix Receiver でアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

  Citrix Receiver は、ユーザーのコンピューターにアプリケーションをインストールする前に <pattern> で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Receiver はそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix Receiver からそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。

  ユーザーが Citrix Receiver を使用せずに優先アプリケーションをアンインストールすると、Citrix Receiver の次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Receiver を使用して優先アプリケーションをアンインストールすると、Citrix Receiver はそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

> 注：Citrix Receiver でアプリケーションをサブスクライブすると、キーワード prefer が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。
>
> 同じアプリケーションに対して複数回 prefer キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせて指定できます。

- 説明に「KEYWORDS:prefer="<pattern>"」という文字列を追加すると、Citrix Receiver でアクセスされるアプリケーションの代わりにローカルのアプリケーションが使用されるようになります。この機能は、「ローカルアプリアクセス」と呼ばれます。

  Citrix Receiver は、ユーザーのコンピューターにアプリケーションをインストールする前に <pattern> で指定されたパターンを検索し、そのアプリケーションがローカルにインストールされているかどうかをチェックします。アプリケーションがローカルにインストールされている場合、Citrix Receiver はそのアプリケーションをサブスクライブして、ショートカットは作成しません。ユーザーが Citrix Receiver からそのアプリケーションを起動すると、ローカルにインストールされたアプリケーション（ここでは「優先アプリケーション」と呼びます）が起動します。
  ユーザーが Citrix Receiver を使用せずに優先アプリケーションをアンインストールすると、Citrix Receiver の次回更新時にそのアプリケーションのサブスクリプションが解除されます。ユーザーが Citrix Receiver を使用して優先アプリケーションをアンインストールすると、Citrix Receiver はそのアプリケーションのサブスクリプションを解除しますが、アンインストールはしません。

> 注：Citrix Receiver でアプリケーションをサブスクライブすると、キーワード prefer が適用されます。アプリケーションをサブスクライブした後でこの文字列を追加しても、そのアプリケーションには適用されません。

同じアプリケーションに対して複数回 prefer キーワードを指定できます。この場合、指定したパターンの 1 つが一致すると、そのアプリケーションに設定が適用されます。以下のパターンを任意に組み合わせて指定できます。

- prefer="<ApplicationName>"

  ショートカットファイルに指定されているアプリケーション名にマッチします。単語または語句を指定できますが、語句の場合は引用句を使用する必要があります。単語やファイルパスの一部がマッチしても無視され、大文字/小文字も区別されません。アプリケーション名によるマッチは、管理者が手作業で設定する場合に便利です。

KEYWORDS:prefer=	**Programs** 配下のショートカット	マッチする**?**
Word	\Microsoft Office\Microsoft Word 2010	はい
“Microsoft Word”	\Microsoft Office\Microsoft Word 2010	はい
Console	\McAfee\VirusScan Console	はい
Virus	\McAfee\VirusScan Console	いいえ
McAfee	\McAfee\VirusScan Console	いいえ

- prefer="\\Folder1\Folder2…\ApplicationName"

  ［スタート］メニューのショートカットファイルの絶対パスおよびアプリケーション名にマッチします。Programs フォルダーは、［スタート］メニューディレクトリのサブフォルダーであるため、フォルダーのアプリケーションを対象にするには絶対パスに Programs フォルダーを含む必要があります。パスにスペースが含まれている場合は、引用符を使用する必要があります。また、大文字と小文字は区別されます。絶対パスによるマッチは、XenDesktop でプログラム的に優先アプリケーションを設定する場合に便利です。

***KEYWORDS:prefer=**	**Programs** 配下のショートカット	マッチする**?**
“\Programs\Microsoft Office\Microsoft Word 2010”	\Programs\Microsoft Office\Microsoft Word 2010	はい
“\Microsoft Office”	\Programs\Microsoft Office\Microsoft Word 2010	いいえ
“\Microsoft Word 2010”	\Programs\Microsoft Office\Microsoft Word 2010	いいえ
“\Programs\Microsoft Word 2010”	2010” \Programs\Microsoft Word 2010	はい

- prefer="\Folder1\Folder2…\ApplicationName"

［スタート］メニューのショートカットファイルの相対パスにマッチします。相対パスにはアプリケーション名を含める必要があり、そのショートカットの親フォルダー名を含めることもできます。ショートカットのファイルパスの末尾が、指定したパターンに一致すると、そのアプリケーションに設定が適用されます。パスにスペースが含まれている場合は、引用符を使用する必要があります。また、大文字と小文字は区別されます。相対パスによるマッチは、プログラム的に優先アプリケーションを設定する場合に便利です。

KEYWORDS:prefer=	**Programs** 配下のショートカット	マッチする**?**
“\Microsoft Office\Microsoft Word 2010”	\Microsoft Office\Microsoft Word 2010	はい
“\Microsoft Office”	\Microsoft Office\Microsoft Word 2010	いいえ
“\Microsoft Word 2010”	\Microsoft Office\Microsoft Word 2010	はい
“\Microsoft Word”	\Microsoft Word 2010	いいえ

ほかのキーワードについては、StoreFront のドキュメントの「ユーザーエクスペリエンスの最適化」を参照してください。

XenDesktop 環境の構成

June 24, 2019

ホストされているアプリケーションやデスクトップにユーザーがアクセスできるようにするには、Citrix Receiver for Windows ソフトウェアをインストールした後で、以下の構成を行う必要があります。

- アダプティブトランスポート - アダプティブトランスポートは、可能な限り、Enlightened Data Transport（EDT）と呼ばれる新しい Citrix プロトコルを TCP より優先して適用することによってデータ転送を最適化します。アダプティブトランスポートの構成について詳しくは、「アダプティブトランスポートの構成」を参照してください。
- 自動更新 - 自動更新では、更新を手動でダウンロードする必要なく、Citrix Receiver for Windows および HDX RealTime Optimization Pack を自動的に更新できます。自動更新を構成する方法について詳しくは、「自動更新の構成」を参照してください。
- コンテンツの双方向リダイレクト - コンテンツの双方向リダイレクトは、クライアントからホスト（およびホストからクライアント）への URL リダイレクトを有効または無効にできます。双方向コンテンツリダイレクトの構成について詳しくは、「コンテンツの双方向リダイレクトの構成」を参照してください。
- Bloomberg キーボード - 特殊用途の USB デバイス（Bloomberg キーボードや 3D マウスなど）では、USB サポート機能の使用を構成できます。Bloomberg キーボードの構成について詳しくは、「Bloomberg キー

ボードの構成」を参照してください。

- 複合 USB デバイス - 複合 USB デバイスは、複数の機能を実行できます。これらの各機能は異なるインターフェイスを使用します。複合 USB デバイスリダイレクトを構成する方法について詳しくは、「複合 USB デバイスの構成」を参照してください。
- USB サポート - USB サポート機能により、ユーザーが仮想デスクトップ上で作業しているときにさまざまな種類の USB デバイスを使用できるようになります。USB サポートの構成について詳しくは、「USB サポートの構成」を参照してください。

アダプティブトランスポートの構成

June 24, 2019

> 要件

- XenApp および XenDesktop 7.12 以降（Citrix Studio を使用する機能の有効化に必要）
- StoreFront 3.8。
- IPv4 VDA のみ。IPv6 および IPv6 と IPv4 の混在構成はサポートされません。
- VDA の UDP ポート 1494 および 2598 での受信トラフィックを許可するファイアウォール規則を追加します。

> 注
>
> TCP ポート 1494 および 2598 も必須で、VDA をインストールするときに自動的に開かれます。ただし、UDP ポート 1494 および 2598 は自動的に開かれません。ユーザーが有効化する必要があります。

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

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

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

特定のクライアントでアダプティブトランスポートを無効にするには、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを使用して、EDT オプションを適切に設定します。

Citrix Receiver グループポリシーオブジェクト管理用テンプレートを使用してアダプティブトランスポートを構成するには（オプション）

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

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

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   - 単一のコンピューターにポリシーを適用する場合は、［スタート］メニューから起動します。
   - ドメインにポリシーを適用する場合は、グループポリシー管理コンソールを使用して起動します。

   Citrix Receiver for Windows の管理用テンプレートファイルをグループポリシーエディターにインポートする手順について詳しくは、「グループポリシーオブジェクトテンプレートによる Citrix Receiver for Windows の構成」を参照してください。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］ > ［**Citrix Receiver**］ > ［ネットワークルーティング］ の順に移動します。
3. ［**Receiver** のトランスポートプロトコル］ ポリシーを ［有効］ に設定します。
4. 必要な場合は、**Citrix Receiver** の通信プロトコルを選択します。
   - ［オフ］： データ転送に TCP を使用することを示します。
   - ［優先］： Citrix Receiver が、UDP でサーバーに接続してから、TCP のフォールバックに切り替えることを示します。
   - ［オン］： Citrix Receiver が、UDP のみを使用してサーバーに接続することを示します。このオプションでは、TCP にフォールバックしません。
5. ［適用］、［**OK**］ の順にクリックします。
6. コマンドラインから gpupdate /force コマンドを実行します。

また、アダプティブトランスポート構成を有効にするには、Citrix Receiver Windows テンプレートファイルをポリシー定義フォルダーに追加する必要があります。admx/adml テンプレートファイルをローカル GPO に追加する方法の詳細については、グループポリシーオブジェクトテンプレートによる Citrix Receiver for Windows の構成を参照してください。

ポリシー設定の有効化を確認するには:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT に移動して、キー **HDXOverUDP** が含まれていることを確認します。

自動更新の構成

June 24, 2019

Citrix Receiver for Windows では、以下の優先順位で自動更新を構成します:

1. グループポリシーオブジェクト管理用テンプレート
2. コマンドラインインターフェイス
3. 高度な設定（ユーザーごと）

グループポリシーオブジェクト管理用テンプレートで構成する

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   - 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
   - ドメインにポリシーを適用する場合、グループポリシー管理コンソールを使用して起動します。
2. ［コンピューター構成］ノードで、［管理用テンプレート］> ［**Citrix** コンポーネント］> ［**Citrix Receiver**］> ［自動更新］ の順に移動します。
3. ［更新のチェックで遅延を設定］ ポリシーを選択します。このポリシーによって、更新をロールアウトするタイミングを選択できます。
4. ［有効］ を選択し、［遅延グループ］ ドロップダウンリストの次のオプションから選択します:
   - **Fast** - 配信期間の最初に更新がロールアウトされます。
   - **Medium** - 配信期間の中頃に更新がロールアウトされます。
   - **Slow** - 配信期間の最後に更新がロールアウトされます。
5. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。
6. 自動更新セクションで、［自動更新ポリシーを有効または無効にする］ を選択します。
7. ［有効］ を選択して必要な値を設定します:
   - ［自動更新ポリシーを有効にする］ ドロップダウンリストの次のオプションから選択します:
     - **Auto** - 更新が利用可能になると通知します（デフォルト）。
     - **Manual** – 更新が利用可能になっても通知されません。手動で更新をチェックします。
   - ［**LTSR** のみ］ を選択して LTSR の更新のみを取得します。
   - ［**auto-update-DeferUpdate-Count**］ ドロップダウンリストから、**-1** ～ **30** の値を選択します。
     - **-1** - 任意の回数通知を保留できます（デフォルト値 =-1）。
     - **0** - ［後で通知する］ オプションは表示されません。
     - その他の数字 - この回数分、［後で通知する］ オプションが表示されます。たとえば、値を 10 に設定すると、［後で通知する］ オプションが 10 回表示されます。

8.［適用］ および ［**OK**］ をクリックしてポリシーを保存します。

コマンドラインインターフェイスを使用した構成

Citrix Receiver for Windows のインストール中

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

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

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

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

例：*CitrixReceiver.exe / AutoUpdateCheck=auto*

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

Citrix Receiver for Windows のインストール後

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

コマンドラインを使用するには：

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

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

例：管理者は 4 つのオプションすべてを使用できます：

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

グラフィカルユーザーインターフェイスを使用した構成

各ユーザーが ［高度な設定］ ダイアログボックスで自動更新設定を上書きできます。このような、ユーザーごとの構成および設定は、現在のユーザーにのみ適用されます。

1. システムトレイで Citrix Receiver for Windows を右クリックします。
2. ［高度な設定］ を選択して ［自動更新］ をクリックします。

   ［自動更新］ダイアログボックスが開きます。
3. 次のいずれかのオプションを選択します：
   - はい。通知します
   - いいえ。通知しません
   - 管理者指定の設定を使用する
4. ［保存］ をクリックします。

StoreFront の自動更新を構成する

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

   例：<account id=… name=”Store”>

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

   <properties>

   <clear />
   </properties>
3. *<clear />* タグの後に、自動更新タグを追加します。

   <account>

   <clear />

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

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

   <annotatedServices>

   <clear />

   <annotatedServiceRecord serviceRef=”1__Citrix_F84Store”>

   <metadata>


```
        <plugins>
         <clear />
        </plugins>
        <trustSettings>
         <clear />
        </trustSettings>
        <properties>
         <property name=”Auto-Update-Check” value=”auto” />
         <property name=”Auto-Update-DeferUpdate-Count” value=”1” />
              <property name=”Auto-Update-LTSR-Only” value=”FALSE” />
         <property name=”Auto-Update-Rollout-Priority” value=”fast” />
             </properties>
      </metadata>
     </annotatedServiceRecord>
    </annotatedServices>
    <metadata>
     <plugins>
      <clear />
     </plugins>
     <trustSettings>
      <clear />
     </trustSettings>
     <properties>
      <clear />
     </properties>
    </metadata>
   </account>
```


auto-update-Check

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

有効な値は次のとおりです:

- Auto - 更新が利用可能になると通知します（デフォルト）。
- Manual - 更新が利用可能になっても通知されません。手動で更新をチェックします。
- Disabled – 自動更新を無効にします。

auto-update-LTSR-Only

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

有効な値は次のとおりです:

- True – 自動更新機能は Citrix Receiver for Windows の LTSR 更新のみをチェックします。
- False – 自動更新機能は Citrix Receiver for Windows の LTSR 更新以外もチェックします。

auto-update-DeferUpdate-Count

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

有効な値は次のとおりです:

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

auto-update-Rollout-Priority:

設定できるロールアウトのタイミングを示します。

有効な値は次のとおりです:

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

制限事項:

1. システムがインターネットに接続されている必要があります。
2. Receiver for Web ユーザーは、StoreFront ポリシーを自動的にダウンロードできません。
3. 送信プロキシをインターセプトするよう SSL を構成している場合、Receiver の自動更新署名サービス（`https://citrixupdates.cloud.com/`）およびダウンロード場所（`https://downloadplugins.citrix.com/`）に例外を追加する必要があります。

4. デフォルトでは、VDA で自動更新が無効になっています。リモートデスクトップのマルチユーザーサーバーマシン、VDI、リモート PC マシンでも同様です。
5. 自動更新は、Desktop Lock がインストールされたマシンでは無効になっています。

コンテンツの双方向リダイレクトの構成

January 9, 2019

次のいずれかを使用して、コンテンツの双方向リダイレクトを有効にできます。

1. グループポリシーオブジェクト管理用テンプレート
2. レジストリ

> 注
>
> - ローカルアプリアクセスが有効であるセッション上では、コンテンツの双方向リダイレクトは機能しません。
> - コンテンツの双方向リダイレクトは、サーバーとクライアントの両方で有効である必要があります。サーバーとクライアントのいずれかで無効になると、機能が無効になります。

グループポリシーオブジェクト管理用テンプレートを使用してコンテンツの双方向リダイレクトを有効化するには

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

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   - 単一のコンピューターにポリシーを適用する場合は、［スタート］メニューから起動します。
   - ドメインにポリシーを適用する場合は、グループポリシー管理コンソールを使用して起動します。
2. ［ユーザー構成］ノードで、［管理用テンプレート］>［従来の管理用テンプレート（**ADM**）］>［**Citrix** コンポーネント］>［**Citrix Receiver**］>［ユーザーエクスペリエンス］ の順に移動します。
3. ［コンテンツの双方向リダイレクト］ ポリシーを選択します。
4. 設定を編集します。

   注:
   URL を含める場合は、単一の URL か、セミコロンで区切った URL のリストを指定できます。ワイルドカード文字としてアスタリスク（*）を使用できます。
5. ［適用］、［**OK**］ の順にクリックします。
6. コマンドラインから gpupdate /force コマンドを実行します。

レジストリを使用してコンテンツの双方向リダイレクトを有効化するには

コンテンツの双方向リダイレクトを有効化するには、Citrix Receiver for Windows インストールフォルダー（C:\Program Files (x86)\Citrix\ICA Client）から、**redirector.exe /RegIE** コマンドを実行します。

制限事項:

- セッションの起動に関する問題のため、リダイレクトが失敗してもフォールバックメカニズムは存在しません。

重要:

- リダイレクトルールがループした構成になっていないことを確認してください。VDA ルールが、たとえば 1 つの URL、`https://www.my_company.com`、がクライアントにリダイレクトされるように構成され、同じ URL が VDA にリダイレクトされるように構成されている場合、ループ構成になります。
- 明示的な URL リダイレクトのみがサポートされます。つまり、Web ブラウザーのアドレスバーに表示される URL や、ブラウザー内ナビゲーションによる URL だけが正しくリダイレクトされます。
- 同じ表示名を持つ 2 つのアプリケーションが複数の StoreFront アカウントを使用するように構成されている場合、プライマリ StoreFront アカウントの表示名を使用して、アプリケーションまたはデスクトップのセッションが起動されます。
- 新しいブラウザーウィンドウが開くのは、URL がクライアントにリダイレクトされた場合だけです。URL が VDA にリダイレクトされたときにブラウザーが既に開いていた場合、リダイレクトされた URL は新しいタブで開かれます。
- ドキュメント、メール、PDF などの、ファイルに埋め込まれたリンクがサポートされます。

Bloomberg キーボードの構成

June 24, 2019

Citrix Receiver for Windows は、XenApp および XenDesktop セッションで Bloomberg キーボードをサポートします。必要なコンポーネントはプラグインとともにインストールされます。Bloomberg キーボード機能は、Citrix Receiver for Windows のインストール中またはレジストリで有効にできます。

複数のセッションで Bloomberg キーボードを使用しないでください。このキーボードは単一セッション環境でのみ正しく動作します。

Bloomberg キーボードのサポートを有効または無効にするには:

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

1. レジストリで次のキーを検索します:

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

2. 次のいずれかを行います:

    - この機能を有効にするには、種類が DWORD で名前が EnableBloombergHID の値のデータを 1 に設定します。
    - この機能を無効にするには、値のデータを 0 に設定します。

Bloomberg キーボードの構成について詳しくは、Knowledge Center でCTX122615を参照してください。

非アクティブな **Desktop Viewer** ウィンドウの減光を無効にするには

Desktop Viewer の複数のウィンドウを使用する場合、デフォルトではアクティブでないウィンドウが減光されます。この機能により、複数のデスクトップを同時に表示する必要がある場合は、非アクティブなデスクトップ上の情報が読みづらくなる可能性があります。レジストリを編集してデフォルトの設定を無効にし、Desktop Viewer ウィンドウの減光を防ぐことができます。

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

1. ユーザーデバイスで、デバイスの現在のユーザーまたはデバイス自体で減光を防止するかどうかによって、DisableDimming という REG_DWORD エントリを次のいずれかのキーで作成します。デバイスで Desktop Viewer を使用したことがある場合は、エントリが既に存在します。

    - HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
    - HKEY_LOCAL_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

    または、ユーザーまたはデバイスの設定で減光を制御する代わりに、同じ REG_WORD エントリを次のキーのどちらかに作成することによって、ローカルポリシーを定義できます。

    - HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
    - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

    通常、プラグイン管理者やユーザーではなく XenDesktop 管理者がグループポリシーを使用してポリシー設定を制御するので、これらのキーを使用するかどうかは任意です。そのため、これらのキーを使用する前に、XenDesktop 管理者がこの機能のポリシーを設定しているかどうか確認してください。

2. エントリを 1 または true のような 0 以外の値に設定します。

    エントリが未指定、または 0 に設定されている場合は、Desktop Viewer ウィンドウが減光します。複数のエントリが指定されている場合、次の方法が使用されます。次の一覧の上位のエントリの値によって、ウィンドウを減光するかどうかが決まります。

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

複合 **USB** デバイスリダイレクトの構成

January 9, 2019

グループポリシーオブジェクト管理用テンプレートで複合 **USB** リダイレクトを構成する

1. **gpedit.msc** を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   a) 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
   b) ドメインにポリシーを適用する場合、グループポリシー管理コンソールを使用して起動します。
2. ［ユーザー構成］ノード配下で、［管理用テンプレート］ > ［**Citrix** コンポーネント］ > ［**Citrix Receiver**］ > ［クライアントデバイスをリモート処理します］ > ［一般的な **USB** のリモート処理］ の順に移動します。
3. **SplitDevices** ポリシーを選択します。
4. ［有効］ を選択します。
5. ［適用］ をクリックします。
6. ［**OK**］ をクリックしてポリシーを保存します。

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

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   a) 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
   b) ドメインにポリシーを適用する場合は、グループポリシー管理コンソールを使用して起動します。
2. ［ユーザー構成］ノード配下で、［管理用テンプレート］ > ［**Citrix** コンポーネント］ > ［**Citrix Receiver**］ > ［クライアントデバイスをリモート処理します］ > ［一般的な **USB** のリモート処理］ の順に移動します。
3. **USB** デバイス規則ポリシーを選択します。
4. ［有効］ を選択します。
5. ［**USB** デバイス規則］ テキストボックスで、許可または禁止する USB デバイスを追加します。
   たとえば、*ALLOW: vid=047F pid= C039 split=01 intf=00,03 //00* および *03* インターフェイスを許可、その他を制限。
6. ［適用］、［**OK**］ の順にクリックします。

   デスクトップセッションでは、分割された USB デバイスは ［デバイス］ の Desktop Viewer で表示されます。また、［基本設定］ > ［デバイス］ から分割された USB デバイスを表示できます。

アプリケーションセッションでは、分割デバイスはコネクションセンターで表示されます。

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

インターフェイスを許可する場合**:**

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

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

インターフェイスを禁止する場合**:**

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

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

例：My_<*plantronics*> ヘッドセット

インターフェイス番号：

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

My_<*plantronics*> ヘッドセットで使用される規則例：

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

制限事項:

Web カメラのインターフェイスは分割しないことをお勧めします。代わりに、汎用 USB リダイレクトを使用してデバイスを単一のデバイスとしてリダイレクトします。パフォーマンスを向上させるには、最適化された仮想チャネルを使用してください。

USB サポートの構成

June 24, 2019

USB サポート機能により、仮想デスクトップ上で作業しているときにさまざまな種類の USB デバイスを使用できるようになります。コンピューターに USB デバイスを接続すると、仮想デスクトップ内でそのデバイスを操作できるようになります。この機能では、フラッシュドライブ、スマートフォン、PDA、プリンター、スキャナー、MP3 プレーヤー、セキュリティデバイス、およびタブレットなどの USB デバイスがサポートされます。Desktop Viewer のユーザーは、ツールバーの基本設定を使用して、仮想デスクトップで USB デバイスを使用できるようにするかどうかを制御できます。

Web カメラ、マイク、スピーカー、ヘッドセットなどの USB デバイスのアイソクロナス機能は、一般的な低遅延/高速 LAN 環境でサポートされます。これにより、Microsoft Office Communicator や Skype などのパッケージでこれらのデバイスを使用できるようになります。

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

- キーボード
- マウス
- スマートカード

注：特殊用途の USB デバイス（Bloomberg キーボードや 3D マウスなど）では、USB サポート機能が使用されるように構成できます。Bloomberg キーボードの構成について詳しくは、「Bloomberg キーボードの構成」を参照してください。そのほかの特殊用途の USB デバイスのポリシー規則の構成について詳しくは、Knowledge Center の CTX122615を参照してください。

デフォルトでは、特定の種類の USB デバイスが XenDesktop および Apps セッションで動作しないように設定されています。たとえば、内部 USB でシステムボードに装着されたネットワークインターフェイスカードの場合、このデバイスのリモート操作は適しません。次の種類の USB デバイスは、XenDesktop セッションでの使用をデフォルトでサポートしていません。

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

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

次の種類の USB デバイスは、XenApp セッションでの使用をデフォルトでサポートしていません。

- Bluetooth ドングル
- 統合ネットワークインターフェイスカード
- USB ハブ
- USB グラフィックアダプター
- オーディオデバイス
- 大容量記憶装置デバイス

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

USB サポートのしくみ

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

USB デバイスを接続すると、新しいデバイスについて知らせる通知が表示されます。ユーザーは、USB デバイスを接続するたびに、そのデバイスを仮想デスクトップで使用するかどうかを選択できます。ユーザーは、仮想デスクトップセッションの開始前、またはセッション実行中に接続した USB デバイスが、フォーカスのある仮想デスクトップで自動的に使用可能になるように設定することもできます。

大容量記憶装置デバイス

マスストレージデバイス（大容量記憶装置）の場合は、USB サポートに加え、クライアント側ドライブのマッピング機能によるリモートアクセスも可能で、これは Citrix Receiver ポリシーの［クライアントデバイスをリモート処理します］>［クライアントドライブマッピング］で設定します。このポリシーを適用すると、ユーザーのログオン時にユーザーデバイス上のドライブが自動的に仮想デスクトップ上のドライブ文字にマップされます。これらのドライブは、マップされたドライブ文字を持つ共有フォルダーとして表示されます。

クライアント側リムーバブルドライブマッピングと USB サポートの 2 つの設定の主な違いは以下のとおりです。

機能	クライアント側ドライブのマッピング	USB サポート
デフォルトで有効	はい	いいえ
読み取り専用アクセスの構成が可能	はい	いいえ

機能	クライアント側ドライブのマッピング	USB サポート
セッション中にデバイスを安全に取り外せる	いいえ	はい（ユーザーがシステムトレイの［ハードウェアの安全な取り外し］をクリックする場合）

［汎用 USB］と［クライアントドライブマッピング］の両方のポリシーが有効で、マスストレージデバイスがセッションの開始前に装着された場合は、USB サポート機能によるリダイレクトの前にクライアント側ドライブのマッピングによるリダイレクトが実行されます。マスストレージデバイスがセッションの開始後に装着された場合は、クライアント側ドライブのマッピングの前に USB サポートによるリダイレクトが実行されます。

デフォルトで許可される **USB** デバイスのクラス

以下のクラスの USB デバイスは、デフォルトの USB ポリシー規則により仮想デスクトップでの使用が許可されます。

この一覧に記載されていても、一部のクラスは構成を追加しなければ XenDesktop および XenApp セッションでリモート処理ができません。それらのクラスについては以下に記述します。

- オーディオ（クラス **01**）。このクラスのデバイスとして、オーディオ入力デバイス（マイク）、オーディオ出力デバイス、および MIDI コントローラーがあります。最近のオーディオデバイスでは一般的にアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。USB サポートを使用する XenApp でオーディオデバイスをリモート操作できないため、オーディオ（クラス 01）は XenApp に適用できません。

  注：VoIP 電話などの一部の特殊デバイスには追加の構成が必要です。詳しくは、Knowledge Center のCTX123015を参照してください。

- 物理インターフェイスデバイス（クラス **05**）。このデバイスはヒューマンインターフェイスデバイス（HID）と似ていますが、一般的に「リアルタイム」の入力またはフィードバックを提供し、フォースフィードバックジョイスティック、モーションプラットフォーム、およびフォースフィードバックエクソスケルトンなどがあります。

- 静止画（クラス **06**）。このクラスのデバイスとして、デジタルカメラおよびスキャナーがあります。ほとんどのデジタルカメラは、画像転送プロトコル（PTP）またはメディア転送プロトコル（MTP）を使ってコンピューターやほかの周辺機器にイメージを転送する静止画クラスをサポートします。また、デジタルカメラはマスストレージデバイスとして機能する場合もあり、カメラ自体のメニューを使っていずれかのクラスを使用するように構成できます。

> 注： カメラがマスストレージデバイスとして機能する場合はクライアントドライブマッピングが使用され、USB サポートは必要ありません。

- プリンター（クラス **07**）。一部のプリンターではベンダー固有のプロトコル（クラス ff）が使用されますが、一般的にはこのクラスにほとんどのプリンターが含まれます。マルチ機能プリンターの場合は、USB ハブが内蔵されていたり、混合デバイスであったりする場合があります。いずれの場合も、印刷機能では一般的にプリンタークラスが使用され、スキャナーや FAX 機能では静止画などの別のクラスが使用されます。

  プリンターは通常、USB サポートなしで適切に動作します。

> 注： このクラスのデバイス（特にスキャナー機能を持つプリンター）には追加の構成が必要です。構成手順については、Knowledge Center のCTX123015を参照してください。

- マスストレージ（クラス **08**）。最も一般的なマスストレージデバイス（大容量記憶装置）として、USB フラッシュドライブがあります。そのほかには、USB 接続のハードドライブ、CD/DVD ドライブ、および SD/MMC カードリーダーがあります。また、内部ストレージを持つさまざまなデバイスがあり、これらもこのクラスのインターフェイスを提供します。たとえば、メディアプレーヤー、デジタルカメラ、携帯電話などがあります。USB サポートを使用する XenApp でマスストレージデバイスをリモート操作できないため、マスストレージ（クラス 08）は XenApp に適用できません。既知のサブクラスには次のものが含まれます：

  - 01 制限付きフラッシュデバイス
  - 02 一般的な CD/DVD デバイス（ATAPI/MMC-2）
  - 03 一般的なテープデバイス（QIC-157）
  - 04 一般的なフロッピーディスクドライブ（UFI）
  - 05 一般的なフロッピーディスクドライブ（SFF-8070i）
  - 06 ほとんどの大容量記憶装置デバイスはこの SCSI のバリアントを使用します

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

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

- コンテンツセキュリティ（クラス **0d**）。通常、ライセンスまたはデジタル権利の管理のためのコンテンツ保護を実行します。このクラスのデバイスとして、ドングルがあります。

- ビデオ（クラス **0e**）。このクラスのデバイスとして、ビデオ、Web カメラ、デジタルカムコーダー、アナログビデオ変換機、一部のテレビチューナー、およびビデオストリーミングをサポートする一部のデジタルカメラなど、ビデオ関連の機器があります。

> 注： ほとんどのビデオストリーミングデバイスではアイソクロナス転送が使用されますが、この機能は XenDesktop 4 以降でサポートされます。動作検知機能付きの Web カメラなど、一部のビデオデバイスには追加の構成が必要です。構成手順については、Knowledge Center のCTX123015を参照してください。

- パーソナルヘルスケア（クラス **0f**）。このデバイスには、血圧センサー、心拍数モニター、万歩計、薬剤モニター、肺活量計などの個人用健康器具があります。

- アプリケーションおよびベンダー固有（クラス **fe** および **ff**）。多くのデバイスがベンダー独自のプロトコルまたは USB コンソーシアムで標準化されていないプロトコルを使用しており、これらは通常はベンダー固有

（クラス ff）として分類されます。

デフォルトで拒否される **USB** デバイスのクラス

次の USB デバイスの異なるクラスは、デフォルトの USB ポリシー規則により拒否されます。

- 通信および CDC コントロール（クラス 02 および 0a）。仮想デスクトップ自体への接続にこれらのデバイスのいずれかが使用される場合があるため、デフォルトの USB ポリシーではこれらのデバイスのリモートでの実行は許可されていません。
- ヒューマンインターフェイスデバイス（クラス 03）。さまざまな種類の入出力デバイスを含みます。一般的なヒューマンインターフェイスデバイス（HID）として、キーボード、マウス、ポインティングデバイス、グラフィックタブレット、センサー、およびゲームのコントローラー、ボタン、およびコントロール機能などがあります。

  サブクラス 01 は「起動インターフェイス」クラスとして知られ、キーボードおよびマウスで使用されます。

  デフォルトの USB ポリシーは USB キーボード（クラス 03、サブクラス 01、プロトコル 1）または USB マウス（クラス 03、サブクラス 01、プロトコル 2）を許可しません。これは、ほとんどのキーボードおよびマウスは USB サポートなしでも適切に処理され、一般に仮想デスクトップ内だけでなくローカルでも使用されるためです。
- USB ハブ（クラス 09）。USB ハブを使用すると、より多くのデバイスをローカルのコンピューターに接続できます。これらのデバイスにリモートでアクセスする必要はありません。
- スマートカード（クラス 0b）。スマートカードリーダーには、非接触型および接触型のスマートカードリーダーと、スマートカードと同等のチップを埋め込んだ USB トークンがあります。

  スマートカードリーダーは、スマートカードサポート機能によりアクセスできるため、USB サポートは必要ありません。
- ワイヤレスコントローラー（クラス e0）。これらのデバイスの中には、重要なネットワークアクセスを提供していたり、Bluetooth キーボードやマウスなどの基幹周辺装置を接続していたりするものがある場合があります。

  デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。
- そのほかのネットワークデバイス（クラス **ef**、サブクラス **04**）。これらのデバイスの一部に、重要なネットワークアクセスを提供している可能性があるものがあります。デフォルトの USB ポリシーはこれらのデバイスを許可していません。ただし、USB サポートを使ったアクセスに適したデバイスもあります。

仮想デスクトップで使用できる **USB** デバイスの一覧の変更

Citrix Receiver for Windows のテンプレートファイルを編集して、仮想デスクトップセッション内で使用できる USB デバイスの範囲を更新できます。これにより、グループポリシーを使用して Citrix Receiver for Windows に

変更を加えることができます。このファイルは、次のインストールフォルダーにあります:

:\Program Files\Citrix\ICA Client\Configuration\en

または、各ユーザーデバイスのレジストリに次のレジストリキーを追加できます:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB 種類 = 文字列名前 =”DeviceRules” 値 =

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

製品のデフォルトの規則は、次の場所に保存されています:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB 種類 = 複数行文字列値名前 =”DeviceRules” 値 =

これらのデフォルトの規則は変更しないでください。

これらの規則およびその構文については、Knowledge Center の [CTX119722](https://support.citrix.com/article/CTX119722
を参照してください。

ユーザーごとに USB オーディオを構成する

ネットワークのルーティング、プロキシサーバー、信頼されるサーバーの設定、ユーザーのルーティング、リモートユーザーデバイス、およびユーザーエクスペリエンスに関する規則の構成では、グループポリシーオブジェクトの receiver.admx/receiver.adml テンプレートファイルを使用することをお勧めします。

ドメインポリシーおよびローカルコンピューターのポリシーで receiver.admx テンプレートファイルを使用することができます。ドメインポリシーの場合、グループポリシー管理コンソールを使ってテンプレートファイルをインポートします。これは、組織全体に存在する多くの異なるユーザーデバイスに Citrix Receiver for Windows の設定を適用するのに非常に有用です。単一のユーザーデバイスの場合は、デバイス上のローカルのグループポリシーエディターを使ってテンプレートをインポートします。

** 注: ** この機能は、XenApp サーバーでのみ使用できます。

ユーザーごとに USB オーディオを構成するには

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

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

1. 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。
1. **［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。
1. **［追加］** を選択し、Receiver の Configuration フォルダー（一般的に 32 ビットマシンの場合は、C:\Program Files\Citrix\ICA Client\Configuration、64 ビットマシンの場合は、C:\Program Files (x86)\Citrix\ICA Client\Configuration）を参照し、receiver.admx を選択します。
1. **［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。
1. ［コンピューターの構成］ノードで、**［管理用テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrix

コンポーネント］>［Citrix Receiver］>［ユーザーエクスペリエンス］** の順に開き、**［一般的な USB リダイレクトによるオーディオ］** をクリックします。
1. 設定を編集します。
1. **［適用］**、**［OK］** の順にクリックします。
1. コマンドプロンプトを管理者モードで開きます。
1. 次のコマンドを実行します。
gpupdate /force
** 注：** ポリシーを変更した場合、変更を有効にするには XenApp サーバーを再起動する必要があります。
ルートドライブ >

StoreFront の構成

June 24, 2019

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

ここで説明する構成手順に加えて、リモートユーザー（インターネットを介して接続するユーザーや遠隔地のユーザーなど）が内部ネットワークにアクセスできるように NetScaler Gateway を構成する必要もあります。

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

StoreFront を構成するには

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

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

ワークスペースコントロール再接続の管理

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。これにより、たとえば病院で臨床医がほかのワークス

テーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。Citrix Receiver for Windows の場合、クライアントデバイスのワークスペースコントロールの管理はレジストリを変更して行います。これはまた、グループポリシーを使用するドメイン参加クライアントデバイスに対しても実行できます。

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

WSCReconnectModeUser を作成し、既存のレジストリキー WSCReconnectMode を Master Desktop Image または XenApp サーバーホストで変更します。公開デスクトップでは Citrix Receiver for Windows の動作を変更できます。

Citrix Receiver for Windows の WSCReconnectMode キー設定は次のとおりです。

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

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

Citrix Receiver for Windows に対してワークスペースコントロールを無効にするには、次のキーを作成します。

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

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

名前：**WSCReconnectModeUser**

種類：REG_SZ

値のデータ：0

次のキーをデフォルト値の 3 から 0 に変更

HKEY_CURRENT\USER\SOFTWARE\Wow6432Node\Citrix\Dazzle（64 ビット）

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

名前：**WSCReconnectMode**

種類：REG_SZ

値のデータ：0

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

状態インジケータータイムアウトの変更

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

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

CLI でのアプリケーションショートカットの場所のカスタマイズ

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

Citrix Receiver 管理者として、コマンドラインインストールフラグ、GPO、アカウントサービス、またはレジストリ設定を使って、通常の「セルフサービス」Citrix Receiver インターフェイスを無効にし、事前定義した［スタート］メニューと置き換えることができます。このフラグは SelfServiceMode と呼ばれ、デフォルトで true に設定されています。管理者が SelfServiceMode フラグを false に設定すると、ユーザーはセルフサービスの Citrix Receiver ユーザーインターフェイスにアクセスできなくなります。その代わり、［スタート］メニューやデスクトップのショートカットを使って、サブスクライブ済みのアプリケーションにアクセスします。これをショートカットのみのモードと呼びます。

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

ショートカットの操作

- ユーザーはアプリケーションを削除できません。SelfServiceMode フラグを false に設定（ショートカットのみのモード）すると、すべてのアプリケーションが必須アプリケーションになります。ユーザーがデスクトップからショートカットアイコンを削除しても、システムトレイの Citrix Receiver for Windows アイコンで［更新］を選択するとこれらのアイコンが再表示されます。
- ユーザーはストアを 1 つだけ構成できます。アカウントおよび基本設定オプションは使用できません。このため、ユーザーが追加のストアを構成できません。管理者はユーザーに特別な権限を付与し、これによりユーザーはグループポリシーオブジェクトテンプレートを使用して、またはクライアントマシンでレジストリキー

（HideEditStoresDialog）を手動で追加して 1 つまたは複数のアカウントを追加できます。管理者がユーザーにこの権限を付与すると、ユーザーのシステムトレイの Receiver アイコンに［基本設定］オプションが表示され、アカウントを追加および削除できるようになります。

- ユーザーは Windows のコントロールパネルを介してアプリケーションを削除することはできません。
- カスタマイズ可能なレジストリ設定を介してデスクトップショートカットを追加できます。デスクトップショートカットはデフォルトでは追加できません。レジストリ設定を変更したら、Citrix Receiver for Windows を再起動する必要があります。
- ショートカットは、［スタート］メニューにデフォルトのカテゴリパス UseCategoryAsStartMenuPath で作成されます。

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

- インストール時にフラグ [DESKTOPDIR=”Dir_name”] を指定すると、すべてのショートカットを単一のフォルダー内に配置できます。デスクトップショートカットのため CategoryPath がサポートされます。
- 変更アプリケーションの自動再インストールは、レジストリキー AutoReInstallModifiedApps を介して有効にできる機能です。AutoReInstallModifiedApps が有効な場合、管理者がサーバー上の公開アプリケーションおよび公開デスクトップの属性を変更すると、その変更がすべてクライアントマシンに反映されます。AutoReInstallModifiedApps が無効な場合、アプリケーションとデスクトップの属性は更新されず、クライアント上で削除されたショートカットも更新時に再格納されません。デフォルトでは、この AutoReInstallModifiedApps は有効です。「アプリケーションショートカットをカスタマイズするためのレジストリキーの使用」を参照してください。

レジストリでのアプリケーションショートカットの場所のカスタマイズ

> 注
>
> デフォルトでは、レジストリキーは文字列形式を使用します。

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

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

> 注：
>
> ストアを構成する前にレジストリキーに変更を加える必要があります。レジストリキーをカスタマイズする場合には管理者かユーザーかに関わらず、Receiver をリセットしてからレジストリキーを構成し、その後でストアを再構成する必要があります。

32 ビットマシンのレジストリキー

レジストリ名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKEY_CURRENT_USER\Software\Citrix\Recei HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
SelfServiceMode	True	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da

レジストリ名	デフォルト値	場所の優先順
UseCategoryAsStartMenuPath	True	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
StartMenuDir	”“（空）	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
DesktopDir	”“（空）	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
AutoReinstallModifiedApps	True	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da

レジストリ名	デフォルト値	場所の優先順
HideEditStoresDialog	SelfServiceMode では True、NonSelfServiceMode では False	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
WSCSupported	True	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID +\Properties、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
WSCReconnectAll	True	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID +\Properties、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Da
WSCReconnectModeUser	インストール中はレジストリが作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID+\Properties、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\Dazzle

64 ビットマシンのレジストリキー

レジストリ名	デフォルト値	場所の優先順
RemoveAppsOnLogoff	False	HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
RemoveAppsOnExit	False	HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
PutShortcutsInStartMenu	True	HKEY_CURRENT_USER\Software\Citrix\Recei HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
SelfServiceMode	True	HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643

レジストリ名	デフォルト値	場所の優先順
UseCategoryAsStartMenuPath	True	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
StartMenuDir	”“（空）	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
DesktopDir	”“（空）	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
AutoReinstallModifiedApps	True	HKEY_CURRENT_USER\Software\Citrix\Recei +\Properties、 HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643

レジストリ名	デフォルト値	場所の優先順
HideEditStoresDialog	SelfServiceMode では True、NonSelfServiceMode では False	HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties
WSCSupported	True	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID +\Properties、 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
WSCReconnectAll	True	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID + \Properties、 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
WSCReconnectMode	3	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID +\Properties、 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643
WSCReconnectModeUser	インストール中はレジストリが作成されません。	HKEY_CURRENT_USER\Software\Citrix\Dazzl HKEY_CURRENT_USER\Software\Citrix\Recei + primaryStoreID+\Properties、 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643 HKEY_LOCAL_MACHINE\SOFTWARE\Wow643

グラフィカルユーザーインターフェイスを使用してアプリケーションの表示を構成する

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

1. Citrix Receiver for Windows にログオンします。
2. システムトレイの Citrix Receiver for Windows アイコンを右クリックし、［高度な設定］ を選択します。

［高度な設定］ウィンドウが開きます。

3. ［設定オプション］ をクリックします。

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

4. フォルダー名を指定します。これにより、指定した［スタート］メニューのフォルダーに、すべてのサブスクライブ済みアプリケーションが移動されます。アプリケーションは、［スタート］メニューの新規フォルダーと既存フォルダーのどちらにも追加できます。この機能を有効にすると、既存のアプリケーションと新規追加されたアプリケーションの両方が指定したフォルダーに追加されます。

5. ［デスクトップオプション］ ペインの ［デスクトップにアプリケーションを表示します］ チェックボックスをオンにします。

6. フォルダー名を指定します。これにより、指定したローカルデスクトップのフォルダーに、すべてのサブスクライブ済みアプリケーションが移動されます。

7. ［カテゴリ］ オプションの ［［スタート］メニューとデスクトップのパスを有効にします］ チェックボックスをオンにします。これにより、アプリケーションプロパティサーバーで定義されたアプリケーションのショートカットおよびカテゴリフォルダーが作成されます。たとえば、IT アプリフォルダーや財務アプリフォルダーなどです。

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

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

8. ［**OK**］ をクリックします。

グラフィカルユーザーインターフェイスを使用して再接続オプションを構成する

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

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

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

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

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

コマンドラインインターフェイスで［設定オプション］を非表示にする

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

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

グループポリシーオブジェクト管理用テンプレートの構成

June 24, 2019

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

注:

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

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

注:

最新の Citrix Receiver for Windows と共に提供される GPO テンプレートファイルを使用することをお勧めします。

ファイルの種類	ファイルの場所
receiver.adm	<Installation Directory>\ICA Client\Configuration
receiver.admx	<Installation Directory>\ICA Client\Configuration
receiver.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Installation Directory>\ICA Client\Configuration

CitrixBase.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]

注:

- CitrixBase.admx\adml がローカル GPO に追加されないと、[ICA ファイルの署名を有効にします] ポリシーが失われることがあります。
- Citrix Receiver for Windows をアップグレードする場合、以下の手順に従って最新のテンプレートをローカル GPO に追加する必要があります。最新のファイルをインポートしても、以前の設定は保持されます。

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

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

1. 管理者として、[スタート] メニューから gpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。注: 既に Citrix Receiver for Windows のテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順 2. ～ 5. は省略できます。
2. グループポリシーエディターで [管理用テンプレート] を選択します。
3. [操作] メニューの [テンプレートの追加と削除] を選択します。
4. [追加] をクリックし、テンプレートファイルの場所（\ICA Client\Configuration\receiver.adm）を参照します。インストールディレクトリ >
5. [開く] をクリックしてテンプレートを追加し、[閉じる] をクリックしてグループポリシーエディターのメインウィンドウに戻ります。

ローカル GPO のパス [管理用テンプレート] **>** [従来の管理用テンプレート（**ADM**）] **>** [**Citrix** コンポーネント] **>** [**Citrix Receiver**] に、Citrix Receiver for Windows のテンプレートファイルが追加されます。

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

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

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

1. Citrix Receiver for Windows をインストールしてから、テンプレートファイルをコピーします。

   admx:

コピー元：<Installation Directory>\ICA Client\Configuration\receiver.admx

コピー先：%systemroot%\policyDefinitions

コピー元：<Installation Directory>\ICA Client\Configuration\CitrixBase.admx

コピー先：%systemroot%\policyDefinitions

adml:

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

コピー先：%systemroot%\policyDefinitions\[MUIculture]

コピー元：<Installation Directory>\ICA Client\Configuration\[MUIculture]\CitrixBase.adml

コピー先：%systemroot%\policyDefinitions\[MUIculture]

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

ユーザーへのアカウント情報の提供

June 24, 2019

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

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

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

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

［アカウントの追加］ダイアログボックスを非表示にする

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

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

［アカウントの追加］ダイアログボックスは次の方法で非表示にできます：

1. システムログオン時

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

   この設定はユーザーごとに固有であり、Citrix Receiver for Windows をリセットするとリセットされます。

2. コマンドラインを使用したインストール

   管理者として、次のスイッチを指定して Citrix Receiver for Windows をインストールします：
   CitrixReceiver.exe /ALLOWADDSTORE=N
   この設定はマシンごとであるため、動作の設定はすべてのユーザーに適用されます。

   ストアが構成されていない場合は、次のメッセージが表示されます。

［アカウントの追加］ダイアログボックスは、次の方法でも非表示にすることができます。

注： システムログオン時に設定する方法かコマンドラインインターフェイスによる方法のどちらかを使用して、［アカウントの追加］ダイアログボックスを非表示にすることをお勧めします。

- **Citrix** 実行ファイルの名前を変更する：
  ファイルの名前を **CitrixReceiver.exe** から **CitrixReceiverWeb.exe** に変えて、［アカウントの追加］ダイアログボックスの動作を変更します。これにより、［アカウントの追加］ダイアログボックスが［スタート］メニューに表示されなくなります。
  Citrix Receiver for Web について詳しくは、「Receiver for Web サイトからの Citrix Receiver for Windows の配布」を参照してください。

- グループポリシーオブジェクト：
  Citrix Receiver for Windows インストールウィザードで［アカウントの追加］ボタンが表示されないようにするには、以下のとおりにローカルグループポリシーエディターで Self-Service ノードにある **EnableFTU** ポリシーを無効にします。
  この設定はマシンごとであるため、動作の設定はすべてのユーザーに適用されます。
  テンプレートファイルの読み込みについては、「グループポリシーオブジェクトテンプレートによる Receiver の構成」を参照してください。

メールアドレスによるアカウント検出を構成する

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

注:

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

NetScaler Gateway の構成について詳しくは、NetScaler Gateway ドキュメントの「Connecting to StoreFront by using email-based discovery」を参照してください。

ユーザーにプロビジョニングファイルを提供する

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

管理者は、StoreFront を使用して、接続の詳細情報を定義したプロビジョニングファイルを作成できます。作成したプロビジョニングファイルをユーザーに提供して、Citrix Receiver for Windows を自動的に構成できるようにします。Citrix Receiver for Windows をインストールした後で、提供されたファイルをユーザーが開くと Citrix Receiver for Windows が自動的に構成されます。Citrix Receiver for Web サイトを構成して、ユーザーに Citrix Receiver for Windows のプロビジョニングファイルを提供することもできます。

- 詳しくは、StoreFront のドキュメントの「ユーザー用のストアプロビジョニングファイルのエクスポート」を参照してください。

アカウント情報をユーザーに手入力させる

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

- StoreFront ストアへの接続の場合は、そのサーバーの URL を提供します。次に例を示します: `https://servername.company.com`

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

- NetScaler Gateway を介する接続の場合は、ユーザーがすべての構成済みストアを表示する必要があるのか、または特定の NetScaler Gateway に対するリモートアクセスが有効になった単一のストアだけにアクセスする必要があるのかを最初に判断します。
  - 構成済みストアをすべて表示させる場合は、ユーザーに NetScaler Gateway の完全修飾ドメイン名を提供します。

- 特定のストアへのアクセスに限定する場合は、ユーザーに NetScaler Gateway の完全修飾ドメイン名とストア名を次の形式で提供します。

  NetScalerGatewayFQDN?MyStoreName

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

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

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

複数のストアアカウントの自動的共有

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

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

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

場所: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

キー名: CurrentAccount

値: AllAccount

種類: Reg_SZ

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

場所: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

キー名: CurrentAccount

値: AllAccount

種類: REG_SZ

自動更新の構成

June 24, 2019

Citrix Receiver for Windows では、以下の優先順位で自動更新を構成します:

1. グループポリシーオブジェクト管理用テンプレート
2. コマンドラインインターフェイス
3. 高度な設定（ユーザーごと）

グループポリシーオブジェクト管理用テンプレートで構成する

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   - 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
   - ドメインにポリシーを適用する場合、グループポリシー管理コンソールを使用して起動します。
2. ［コンピューター構成］ノードで、［管理用テンプレート］> ［**Citrix** コンポーネント］> ［**Citrix Receiver**］> ［自動更新］ の順に移動します。
3. ［更新のチェックで遅延を設定］ ポリシーを選択します。このポリシーによって、更新をロールアウトするタイミングを選択できます。
4. ［有効］ を選択し、［遅延グループ］ ドロップダウンリストの次のオプションから選択します:
   - **Fast** - 配信期間の最初に更新がロールアウトされます。
   - **Medium** - 配信期間の中頃に更新がロールアウトされます。
   - **Slow** - 配信期間の最後に更新がロールアウトされます。
5. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。
6. 自動更新セクションで、［自動更新ポリシーを有効または無効にする］ を選択します。
7. ［有効］ を選択して必要な値を設定します:
   - ［自動更新ポリシーを有効にする］ ドロップダウンリストの次のオプションから選択します:
     - **Auto** - 更新が利用可能になると通知します（デフォルト）。
     - **Manual** – 更新が利用可能になっても通知されません。手動で更新をチェックします。
   - ［**LTSR** のみ］ を選択して LTSR の更新のみを取得します。
   - ［**auto-update-DeferUpdate-Count**］ ドロップダウンリストから、**-1** ～ **30** の値を選択します。
     - **-1** - 任意の回数通知を保留できます（デフォルト値 =-1）。
     - **0** - ［後で通知する］ オプションは表示されません。
     - その他の数字 - この回数分、［後で通知する］ オプションが表示されます。たとえば、値を 10 に設定すると、［後で通知する］ オプションが 10 回表示されます。

8.［適用］ および ［**OK**］ をクリックしてポリシーを保存します。

コマンドラインインターフェイスを使用した構成

Citrix Receiver for Windows のインストール中

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

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

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

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

例: *CitrixReceiver.exe / AutoUpdateCheck=auto*

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

Citrix Receiver for Windows のインストール後

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

コマンドラインを使用するには:

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

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

例: 管理者は 4 つのオプションすべてを使用できます:

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

グラフィカルユーザーインターフェイスを使用した構成

各ユーザーが ［高度な設定］ ダイアログボックスで自動更新設定を上書きできます。このような、ユーザーごとの構成および設定は、現在のユーザーにのみ適用されます。

1. システムトレイで Citrix Receiver for Windows を右クリックします。
2. ［高度な設定］ を選択して ［自動更新］ をクリックします。

   ［自動更新］ダイアログボックスが開きます。
3. 次のいずれかのオプションを選択します：
   - はい。通知します
   - いいえ。通知しません
   - 管理者指定の設定を使用する
4. ［保存］ をクリックします。

StoreFront の自動更新を構成する

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

   例：<account id=… name=”Store”>

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

   <properties>
   <clear />
   </properties>
3. *<clear />* タグの後に、自動更新タグを追加します。

```
<account>

    <clear />

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

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

      <annotatedServices>

        <clear />
```



```
12
13          <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15            <metadata>
16
17              <plugins>
18
19                <clear />
20
21              </plugins>
22
23              <trustSettings>
24
25                <clear />
26
27              </trustSettings>
28
29              <properties>
30
31                <property name="Auto-Update-Check" value="auto" />
32
33                <property name="Auto-Update-DeferUpdate-Count" value="1"
                      />
34
35                      <property name="Auto-Update-LTSR-Only" value="
                          FALSE" />
36
37                <property name="Auto-Update-Rollout-Priority" value="fast
                      " />
38
39                   </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
```



```
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

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

有効な値は次のとおりです:

- Auto - 更新が利用可能になると通知します（デフォルト）。
- Manual - 更新が利用可能になっても通知されません。手動で更新をチェックします。
- Disabled – 自動更新を無効にします。

auto-update-LTSR-Only

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

有効な値は次のとおりです:

- True – 自動更新機能は Citrix Receiver for Windows の LTSR 更新のみをチェックします。
- False – 自動更新機能は Citrix Receiver for Windows の LTSR 更新以外もチェックします。

auto-update-DeferUpdate-Count

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

有効な値は次のとおりです:

- -1 - 任意の回数通知を保留できます（デフォルト値 =-1）。
- 0 - ［後で通知する］オプションは表示されません。

- その他の数字 - この回数分、［後で通知する］オプションが表示されます。たとえば、値を 10 に設定すると、後で通知するオプションが 10 回表示されます。

auto-update-Rollout-Priority:

設定できるロールアウトのタイミングを示します。

有効な値は次のとおりです:

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

制限事項:

1. システムがインターネットに接続されている必要があります。
2. Receiver for Web ユーザーは、StoreFront ポリシーを自動的にダウンロードできません。
3. 送信プロキシをインターセプトするよう SSL を構成している場合、Receiver の自動更新署名サービス（https://citrixupdates.cloud.com）およびダウンロード場所（https://downloadplugins.citrix.com）に例外を追加する必要があります。
4. デフォルトでは、VDA で自動更新が無効になっています。リモートデスクトップのマルチユーザーサーバーマシン、VDI、リモート PC マシンでも同様です。
5. 自動更新は、Desktop Lock がインストールされたマシンでは無効になっています。

環境の最適化

November 12, 2018

管理者は Receiver 環境を最適化できます:

- アプリケーションの起動時間の短縮
- デバイスから公開リソースへの接続を容易にする
- DNS 名前解決をサポートする
- プロキシサーバーを介した XenDesktop 接続をサポートする
- 匿名アプリケーションへのアクセスを有効にする
- シングルサインオン構成のチェック

アプリケーションの起動時間の短縮

June 24, 2019

セッションの事前起動機能を使用すると、通常時および高トラフィック負荷時のアプリケーションの起動時間が短縮され、ユーザーエクスペリエンスが向上します。事前起動機能により、ユーザーが Citrix Receiver for Windows にログオンするとき、またはログオン済みの場合は予定された時間に事前起動セッションを作成できます。

この事前起動セッションにより、最初のアプリケーションの起動時間が短縮されます。ユーザーが Citrix Receiver for Windows で新しいアカウント接続を追加した後、次回のセッションまで事前起動セッションは適用されません。このセッションでは、デフォルトのアプリケーション ctxprelaunch.exe が実行されます。ただし、このアプリケーションはユーザーには表示されません。

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

セッションの事前起動機能はデフォルトでは無効になっています。この機能を有効にするには、Receiver のコマンドラインで ENABLEPRELAUNCH=true パラメーターを指定するか、レジストリキー EnablePreLaunch に true を設定します。デフォルト値（null）は、事前起動が無効であることを示します。

注：ドメインパススルー（SSON）認証をサポートするようにクライアントマシンが構成されている場合、事前起動機能が自動的に有効になります。事前起動なしでドメインパススルー（SSON）を使用する場合は、
EnablePreLaunch レジストリキーの値を
false に設定します。

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

レジストリの場所は以下のとおりです。

HHKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazzle

HKEY_CURRENT_USER\Software\Citrix\Dazzle

事前起動には 2 つの種類があります。

- 即時事前起動。トラフィック量にかかわらず、ユーザーの資格情報が認証されるとすぐに事前起動が開始されます。この設定は、通常のトラフィック負荷時に使用します。ユーザーは、Citrix Receiver for Windows を再起動することで事前起動セッションを起動できます。
- 予定事前起動。予定した時間に事前起動が開始されます。予定事前起動は、ユーザーデバイスが実行中で認証済みの場合にのみ開始されます。これら 2 つの条件が満たされない場合は、予定された事前起動時間になってもセッションが起動しません。ネットワークとサーバーの負荷を分散するため、セッションは予定された時刻を含む一定期間内に起動します。たとえば、事前起動を午後 1 時 45 分に設定すると、午後 1 時 15 分から午後 1 時 45 分の間にセッションが起動されます。この設定は、高トラフィック負荷時に使用します。

XenApp サーバーでの事前起動の構成には、事前起動アプリケーションの作成、変更、または削除と、事前起動アプリケーションを制御するユーザーポリシー設定の更新が含まれます。XenApp サーバー上でセッションの事前起動を構成する方法については、XenApp のドキュメントの「アプリケーションを事前起動するには」を参照してください。

receiver.admx ファイルで事前起動機能をカスタマイズすることはできません。ただし、Citrix Receiver for Windows のインストール時またはインストール後にレジストリ値を変更することで、事前起動構成を変更することができます。3 つの HKEY_LOCAL_MACHINE 値と 2 つの HKEY_CURRENT_USER 値を使用します。

- HKEY_LOCAL_MACHINE 値は、Receiver のインストール時に追加されます。
- HKEY_CURRENT_USER 値では、同一マシン上の特定ユーザーに HKEY_LOCAL_MACHINE とは異なる値を設定できます。ユーザーは、管理者権限がなくても HKEY_CURRENT_USER 値を変更できます。管理者は、この機能を設定するためのスクリプトをユーザーに提供できます。

HKEY_LOCAL_MACHINE の値

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

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

値の名前：UserOverride

値のデータ:

0 - HKEY_CURRENT_USER の値が存在しても、HKEY_LOCAL_MACHINE の値を使用します。

1 - 存在する場合は HKEY_CURRENT_USER の値を使用します。そうでない場合は、HKEY_LOCAL_MACHINE の値を使用します。

値の名前：State

値のデータ:

0 - 事前起動を無効にします。

1 - 即時事前起動を有効にします（ユーザーの資格情報が認証されると事前起動が開始されます）。

2 - 予定事前起動を有効にします（Schedule 値に指定した時刻に事前起動が開始されます）。

値の名前：Schedule

値:

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

HH:MM	M:T:W:TH:F:S:SU - ここで、HH は時、MM は分です。M:T:W:TH:F:S:SU は曜日です。月曜日、水曜日、および金曜日の午後 1 時 45 分に予定事前起動を有効にするには、Schedule=13:45 と設定します。	1:0:1:0:1:0:0。セッションが実際に起動するのは午後 1 時 15 分から午後 1 時 45 分の間です。

HKEY_CURRENT_USER の値

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

値については、HKEY_LOCAL_MACHINE と同じ State および Schedule 値を使用します。

クライアント側デバイスのマッピング

June 24, 2019

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

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

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

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

デバイスマッピングを無効にする

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

メントを参照してください。

クライアントフォルダーのリダイレクト

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

セッション内では、ユーザーデバイス上のすべてのファイルシステムの代わりにユーザー指定のフォルダーのみが UNC リンクとして表示されます。レジストリで UNC リンクを無効にすると、クライアントフォルダーはマップされたドライブとしてセッション内で表示されます。構成方法など、クライアントフォルダーのリダイレクトについて詳しくは XenDesktop 7 のドキュメントを参照してください。

クライアントドライブをホスト側のドライブ文字にマップする

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

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

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

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

サーバーの既存のドライブ文字をアルファベットの後ろの方の文字に変更しておくと、サーバー側のドライブ文字がクライアント側のものと競合しなくなるため、ユーザーはローカルドライブと同じドライブ文字をセッション内で使

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

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

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

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

HDX Plug-n-Play USB デバイスリダイレクト

Updated: 2015-01-27

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

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

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

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

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

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

重要：COM ポートのマッピング機能は、TAPI をサポートしません。

1. XenDesktop 7 の展開では、クライアント COM ポートリダイレクトポリシー設定を有効にします。
2. Citrix Receiver for Windows にログオンします。
3. コマンドプロンプトで、次のコマンドを実行します。

   net use com<x>: \\client\com<z>:

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

   net use

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

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

DNS 名前解決をサポートする

June 24, 2019

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

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

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

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

特定のユーザーデバイスの **DNS** アドレス解決を無効にするには

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

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

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

XenDesktop でプロキシサーバーを使用する

June 24, 2019

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

構成チェッカーを使用して **Single Sign-On** の構成を検証する

June 24, 2019

リリース 4.5 の Citrix Receiver for Windows より、構成チェッカーを使用して、Single Sign-On が適切に構成されていることを確認するテストを実行できるようになりました。テストはシングルサインオン構成の各チェックポイントに対して実行され、構成結果を表示します。

1. Citrix Receiver for Windows にログオンします。
2. 通知領域で Citrix Receiver for Windows を右クリックし、［高度な設定］ をクリックします。［高度な設定］ウィンドウが開きます。
3. ［構成チェッカー］ をクリックします。［Citrix 構成チェッカー］ダイアログボックスが開きます。
4. ［選択］ ペインで ［**SSONChecker**］ チェックボックスをオンにします。
5. ［実行］ をクリックします。テストの状態を示す進捗状況バーが表示されます。

［構成チェッカー］ウィンドウには次の列があります：

1. **Status**：特定のチェックポイントでのテスト結果が表示されます。
   - 緑色のチェックマークは、チェックポイントが適切に構成されていることを示します。
   - 青色の I は、チェックポイントに関する情報を示します。
   - 赤色の X は、チェックポイントが適切に構成されていないことを示します。
2. **Provider**：テストが実行されているモジュールの名前が表示されます。この場合は、シングルサインオンになります。
3. **Suite**：テストのカテゴリを示します。例：「インストール」。
4. **Test**：実行中のテストの名前を示します。
5. **Details**：テスト結果にかかわらず、そのテストの詳細が表示されます。各チェックポイントおよび対応する結果の詳細を確認することができます。

以下のテストが実施されます：

1. シングルサインオンとともにインストール済み
2. ログオン資格情報のキャプチャ
3. ネットワークプロバイダーの登録：ネットワークプロバイダーの登録のテスト結果で緑色のチェックマークが表示されるのは、ネットワークプロバイダーの一覧で「Citrix Single Sign-on」が先頭に設定されている場合のみです。「Citrix Single Sign-On」が一覧の先頭以外の場所に表示されている場合、ネットワークプロバイダーの登録のテスト結果では青色の I と詳細情報が表示されます。
4. シングルサインオンプロセスが実行されている
5. グループポリシー：デフォルトでは、このポリシーはクライアントで構成されます。
6. Internet Explorer のセキュリティゾーンの設定：［インターネットオプション］のセキュリティゾーンの一覧に Store/XenApp サービスの URL を追加していることを確認してください。セキュリティゾーンをグループポリシー経由で構成しており、そのポリシーを変更した場合、変更を有効にしてテストの正確な状態が表示されるようにするために、［高度な設定］ウィンドウを開き直す必要があります。

7. Web Interface/StoreFront の認証方法

注：Receiver for Web にユーザーがアクセスしている場合、テスト結果は不正確になります。
Citrix Receiver for Windows で複数のストアを構成している場合、認証方法テストはすべての構成済みストアに対して実行されます。

注：テスト結果はレポートとして保存できます。デフォルトのレポートの形式は.txt です。

［高度な設定］ダイアログボックスの［構成チェッカー］オプションを非表示にする：

1. 管理者として、［スタート］メニューから gpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
2. グループポリシーエディターで、［**Citrix** コンポーネント］>［**Citrix Receiver**］>［**Self Service**］>［**DisableConfigChecker**］ の順に開きます。
3. ［有効］ を選択します。
   これにより、［高度な設定］ ウィンドウで［構成チェッカー］オプションが表示されなくなります。
4. ［適用］、［**OK**］ の順にクリックします。
5. コマンドプロンプトを開きます。
6. gpupdate /force コマンドを実行します。

変更を有効にするには、［詳細な設定］ダイアログボックスを閉じて再度開きます。

制限事項：

構成チェッカーの対象チェックポイントに、XenApp/XenDesktop サーバー上の［Citrix XML Service への要求を信頼する］の構成は含まれません。

ユーザーエクスペリエンスの向上

June 24, 2019

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。

汎用クライアント入力システム（**IME**）の構成

コマンドラインインターフェイスを使用した汎用クライアント **IME** の構成

汎用クライアント IME を有効化するには、Citrix Receiver for Windows インストールフォルダー（C:\Program Files (x86)\Citrix\ICA Client）から **wfica32.exe /localime:on** コマンドを実行します。

> 注
>
> コマンドラインスイッチ **wfica32.exe/localime:on** を使用して、汎用クライアント IME とキーボードレイアウトの同期の両方を有効にすることができます。

汎用クライアント IME を無効化するには、Citrix Receiver for Windows インストールフォルダー（C:\Program Files (x86)\Citrix\ICA Client）から **wfica32.exe /localgenericime:off** コマンドを実行します。このコマンドは、キーボードレイアウトの同期設定に影響を及ぼしません。

コマンドラインインターフェイスを使用して汎用クライアント IME を無効にした場合、**wfica32.exe/localgenericime:on** コマンドを実行することによって、再び機能を有効化できます。

トグル:

Citrix Receiver for Windows は、この機能に対するトグルスイッチ機能をサポートしています。**wfica32.exe /localgenericime:on** コマンドを実行して、機能を有効/無効にできます。ただし、キーボードレイアウトの同期設定は、トグルスイッチより優先されます。キーボードレイアウトの同期がオフに設定されている場合、トグルしても汎用クライアント IME は有効になりません。

グラフィカルユーザーインターフェイスを使用した汎用クライアント **IME** の構成

汎用クライアント IME には VDA Version 7.13 以降が必要です。

キーボードレイアウトの同期を有効化することにより、汎用クライアント IME 機能を有効化できます。詳しくは、キーボードレイアウトの同期を参照してください。

Citrix Receiver for Windows を使用すると、汎用クライアント IME を使用するためのさまざまなオプションを構成できます。要件および使用状況に基づいて、これらのオプションのいずれかから選択できます。

1. アクティブなアプリケーションセッションで、システムトレイの Citrix Receiver アイコンを右クリックして、［コネクションセンター］ を選択します。
2. ［基本設定］ を選択し、［ローカル **IME**］ を選択します。

さまざまな IME モードをサポートするために以下のオプションを利用できます。

1. サーバー **IME** を有効にする - ローカル IME を無効にする場合にこのオプションを選択します。このオプションは、サーバー上で設定された言語のみ使用できることを意味します。
2. ローカル **IME** を高パフォーマンスモードに設定する - ローカル IME を限られた帯域幅で使用する場合にこのオプションを選択します。このオプションは、候補ウィンドウの機能を制限します。
3. ローカル **IME** を最適なエクスペリエンスモードに設定する - ローカル IME を最適なユーザーエクスペリエンスで使用する場合にこのオプションを選択します。このオプションは、高帯域を消費します。デフォルトで、汎用クライアント IME が有効の場合、このオプションが選択されます。

設定変更は、現在のセッションにのみ適用されます。

レジストリエディターを使用したホットキー構成の有効化

汎用クライアント IME が有効の場合、異なる IME モードを選択するには、**Shift+F4** ホットキーを使用できます。IME モードのさまざまなオプションがセッションの右上隅に表示されます。

デフォルトで、汎用クライアント IME のホットキーは無効です。

レジストリエディターで、HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys に移動します。

AllowHotKey を選択して、デフォルト値を 1 に変更します。

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

制限事項:

1. 汎用クライアント IME は、Search UI などの UWP（ユニバーサル Windows プラットフォーム）アプリケーションや、Windows 10 オペレーティングシステムの Edge ブラウザーをサポートしません。回避策として、代わりにサーバー IME を使用します。
2. 汎用クライアント IME は、保護モードの Internet Explorer バージョン 11 ではサポートされません。回避策として、インターネットオプションを使用して保護モードを無効にできます。そうする場合は、［セキュリティ］ をクリックして、［保護モードを有効にする］ をオフにします。

キーボードレイアウト

キーボードレイアウトの同期によって、クライアントデバイスの優先キーボードレイアウトを切り替えることができます。この機能はデフォルトでは無効になっています。

キーボードレイアウトの同期を有効にするには:

1. Citrix Receiver for Windows のシステムトレイアイコンで、［高度な設定］>［ローカルキーボードレイアウト設定］>［はい］ を選択します。
2. ［保存］ をクリックします。

この機能は、［いいえ］ で無効にできます。

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

注：ローカルキーボードレイアウトオプションで、クライアント IME（Input Method Editor）をアクティブにします。日本語、中国語、または韓国語を使用しているユーザーがサーバー IME を使用する場合、［いいえ］を選択するか、**wfica32:exe /localime:off** を実行してローカルキーボードレイアウトオプションを無効にする必要があります。次のセッションに接続すると、セッションは、リモートサーバーで指定されたキーボードレイアウトに戻します。

クライアントのキーボードレイアウトの切り替えがアクティブなセッションで有効にならないことがあります。この問題を解決するには、いったん Citrix Receiver for Windows からログオフしてから、再度ログインしてください。

制限事項:

- 管理者権限で実行しているリモートアプリケーション（例: アプリケーションアイコンを右クリックして、[管理者として実行]）は、クライアントのキーボードレイアウトと同期することはできません。この問題を解決するには、サーバー側（VDA）で手動でキーボードレイアウトを変更するか、UAC を無効にします。
- ユーザーがクライアントのキーボードレイアウトをサーバーでサポートされていないレイアウトに変更すると、キーボードレイアウトの同期機能は、セキュリティ上の理由で無効になります。認識されないキーボードレイアウトは、潜在的なセキュリティ上の脅威として扱われるためです。キーボードレイアウトの同期機能を復元するには、セッションにログオンし直す必要があります。
- RDP がアプリケーションとして展開され、ユーザーが RDP セッションで作業をしていると、キーボードレイアウトを Alt + Shift ショートカットで変更することはできません。この問題を回避するために、RDP セッションの言語バーでキーボードレイアウトを切り替えることができます。
- この機能は、パフォーマンス上のリスクの可能性があるサードパーティ製品の問題によって、Windows Server 2016 で無効になっています。これは、VDA のレジストリ設定で有効にできます: HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme で、DisableKeyboardSync という名称の新しいキーを追加し、値を 0 に設定します。

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

相対マウス

相対マウスのサポートでは、マウスの絶対位置ではなく相対位置を読み取るオプションを提供します。この機能は、マウスの絶対位置ではなく相対位置の入力を必要とするアプリケーションに必要です。

注: この機能を適用できるのは、公開デスクトップセッションのみです。

相対マウスのサポートを有効化するには

1. Citrix Receiver for Windows へのログオン
2. 公開デスクトップセッションを開始します。
3. Desktop Viewer のツールバーで ［基本設定］ をクリックします。
   ［Citrix Receiver - 基本設定］ウィンドウが開きます。
4. ［接続］をクリックします。

5. ［相対マウスの設定］で ［相対マウスを使用する］ をオンにします。
6. ［適用］、［**OK**］ の順にクリックします。

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

ハードウェアのデコード

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

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

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

ハードウェアデコードを有効にするには：

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

ポリシーが適用され、ハードウェアアクセラレーションがアクティブな ICA セッションで使用されているかを確認するには、次のレジストリキーを確認します。

レジストリパス：HKEY_CURRENT_USER\Software\Citrix\ICA Client\CEIP\Data\GfxRender\<session ID>

> ヒント
>
> **Graphics_GfxRender_Decoder** および **Graphics_GfxRender_Renderer** は 2 である必要があります。値が 1 の場合、CPU ベースのデコードが使用されています。

ハードウェアデコード機能が使用されている場合、次の制限事項を考慮してください。

- クライアントに GPU が 2 つあり、モニターの 1 つが 2 つ目の GPU でアクティブな場合、CPU デコードが使用されます。
- Windows Server 2008 R2 が動作する XenApp 7.x サーバーに接続する場合、ユーザーの Windows デバイスではハードウェアデコードを使用しないことをお勧めします。これが有効な場合、文字列を強調表示する場合のパフォーマンスの低下やちらつきの問題が発生します。

クライアント側のマイク入力

Citrix Receiver for Windows では、クライアント側の複数のマイク入力がサポートされます。ユーザーは、ローカルのマイクを使用して以下の操作を実行できます。

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

Citrix Receiver for Windows のユーザーは、コネクションセンターの設定を変更して、デバイスに付属しているマイクを使用するかどうか選択することができます。XenDesktop ユーザーも、Desktop Viewer の［基本設定］ダイアログボックスを使用してマイクおよび Web カメラを無効にできます。

マルチモニターサポート

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

マルチモニター環境では、各モニターの製造元により解像度が異なる場合があります。また、セッション中にモニターの解像度や向きが変更されることもあります。

セッションを複数のモニター上に表示する場合、以下の 2 つのモードがあります。

- 全画面モード。セッションはマルチモニター全体に表示されます。ローカルでの場合と同様に、アプリケーションウィンドウが表示領域全体に最大化されます。

  XenDesktop：Desktop Viewer ウィンドウをマルチモニターのいずれかの矩形表示領域内に表示するには、隣接するモニターにかかるようにウィンドウのサイズを変更して ［最大化］ をクリックします。

- ウィンドウモード。単一のモニターがセッション用に使用されます。アプリケーションウィンドウは個々のモニター上に最大表示されません。

XenDesktop：同じ割り当て（デスクトップグループ）に含まれるデスクトップを続けて起動すると、ウィンドウ設定が保持され、デスクトップが同じモニターに表示されます。矩形配置構成のマルチモニター環境では、複数の仮想デスクトップを 1 つのデバイス上で表示できます。デバイスのプライマリモニターを XenDesktop セッションで使用する場合は、セッションでもそのモニターがプライマリモニターになります。そうでない場合は、セッション内の最も小さい番号のモニターがプライマリモニターになります。

マルチモニター環境をサポートするには、次の条件を満たしている必要があります。

- ユーザーデバイスの構成でマルチモニターがサポートされている。
- ユーザーデバイスのオペレーティングシステムが各モニターを検出できる。Windows プラットフォームでモニターを検出できるかどうかは、［ディスプレイ］>［ディスプレイの設定の変更］で確認します。ここで、各モニターが別々に表示されていることを確認します。
- モニターが検出された後は、次の作業を行います。
  - **XenDesktop**：Citrix マシンポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。

- **XenApp**: インストールした XenApp サーバーのバージョンに応じて、次の操作を行います。
  * Citrix ポリシーの［表示メモリの制限］設定を使用して、グラフィックメモリの制限を構成します。
  * XenApp サーバー用 Citrix 管理コンソールの左ペインでサーバーファームを選択し、タスクペインで［サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［HDX Broadcast］、［表示設定］の順に選択します（または［サーバーファームのプロパティの変更］、［すべてのプロパティの変更］、［サーバーのデフォルト設定］、［ICA］、［表示設定］の順に選択します）。そして、［各セッションのグラフィックで使用する最大メモリ］を設定します。

この値を、グラフィックメモリを提供するのに十分なサイズに設定します（単位はキロバイト）。このボックスの値が必要なサイズに満たないと、公開リソースが一部のモニター上でしか表示されません。

XenApp および XenDesktop のセッションのグラフィックメモリ要件の計算については、Knowledge Center のCTX115637を参照してください。

デバイス側での印刷設定の変更

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

ユーザーがプリンター設定を上書きするには

1. ユーザーデバイス上で、アプリケーションの［印刷］ダイアログボックスを開き、［プロパティ］をクリックします。
2. ［クライアント設定］タブで［高度な最適化］をクリックし、［イメージ圧縮］および［イメージおよびフォントキャッシュ］オプションの設定を変更します。

スクリーンキーボードの制御

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

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

変換可能なデバイスを使っている場合にスクリーンキーボードの表示を抑制するには、REG_DWORD 値の DisableKeyboardPopup を HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Mod で作成し、値を 1 に設定します。

注:x64 マシンでは、HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Adva に値を作成します。

キーは以下のような異なる 3 種のモードに設定できます。

- 自動：AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0
- 常にポップアップ（スクリーンキーボード）：AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0
- ポップアップしない（スクリーンキーボード）：AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1

キーボードショートカット

Receiver で特定の機能を実行するキーの組み合わせを構成できます。キーボードショートカットのポリシーが有効な場合、Citrix ショートカットキーのマッピング、Windows ショートカットキーの動作、およびセッションでのキーボードの種類を指定できます。

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

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

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

32 ビットカラーアイコンのサポート

Citrix Receiver for Windows では 32 ビット High Color アイコンがサポートされ、Citrix コネクションセンターに表示されるアプリケーションのアイコンに適した色数が自動的に選択されます。シームレスアプリケーションを実行しているときに［スタート］メニューとタスクバーに表示されるアプリケーションのアイコンも、同様に処理されます。

注意：レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いま

せん。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

色数を設定するには、レジストリキー HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences に文字列のレジストリ値 TWIDesiredIconColor を追加し、目的の色数を値のデータとして定義します。定義できるアイコンの色数は、4、8、16、24、および 32 ビット/ピクセルです。ネットワーク接続が低速な場合は、ユーザーはより少ない色数を選択できます。

Desktop Viewer の有効化

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

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

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

Desktop Viewer セッションでのキーボード入力

Desktop Viewer セッションでは、Windows ロゴ + L キーはローカルコンピューターに送信されます。

Ctrl + Alt + Del キーは、ローカルコンピューターに送信されます。

通常、Microsoft 社のユーザー補助機能である固定キー、フィルターキー、および切り替えキー機能を有効にするキーはローカルコンピューターに送信されます。

Desktop Viewer のユーザー補助機能として、Ctrl + Alt + Break キーを押すと、ポップアップウィンドウで Desktop Viewer ツールバーが開きます。

Ctrl + Esc キーは、リモートの仮想デスクトップに送信されます。

注：デフォルトでは、Desktop Viewer を最大化した場合は Alt + Tab キーを押すとセッション内のウィンドウ間でフォーカスが切り替わります。Desktop Viewer をウィンドウ内に表示している場合は、Alt + Tab キーを押すとセッション外のウィンドウ間でフォーカスが切り替わります。

ホットキーシーケンスは、Citrix により設計されたキーの組み合わせです。たとえば、Ctrl + F1 シーケンスは Ctrl + Alt + Del キーを再現し、Shift + F2 はアプリケーションの全画面モードとウィンドウモードを切り替えます。

Desktop Viewer で表示されている仮想デスクトップ（つまり、XenDesktop セッション）ではホットキーシーケンスを使用できませんが、公開アプリケーション（つまり、XenApp セッション）ではこれを使用できます。

仮想デスクトップへの接続

仮想デスクトップセッション内から同じ仮想デスクトップに接続することはできません。これを行うと、既存のデスクトップセッションが切断されます。そのため、次のことをお勧めします:

- 管理者は、仮想デスクトップ上のクライアントが、同じデスクトップを公開しているサイトに接続するように構成しない。
- ユーザーは、同じデスクトップをホストしているサイトを参照しない（自動的に既存のセッションに再接続するようサイトが構成されている場合）。
- ユーザーは、同じデスクトップをホストしているサイトを参照したりそのデスクトップを起動したりしない。

仮想デスクトップとして動作するコンピューターにローカルでログオンするユーザーは、そのデスクトップへの接続がブロックされます。

ユーザーが仮想デスクトップ内から（XenApp で公開された）仮想アプリケーションに接続し、別の管理者が XenApp を管理している環境では、ローカルのデバイスが仮想デスクトップセッションおよび公開アプリケーションセッションで同様にマップされるように、XenApp 管理者と共同してデバイスマッピングを定義することをお勧めします。仮想デスクトップセッションではローカルドライブがネットワークドライブとして表示されるため、XenApp 管理者がドライブマッピングポリシーでネットワークドライブ（リモートドライブ）のマッピングを許可する必要があります。

状態インジケーターのタイムアウトの変更

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

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

セキュリティで保護された接続

January 9, 2019

環境のセキュリティを最大限に高めるには、Citrix Receiver for Windows と公開リソースの間の接続を保護する必要があります。Citrix Receiver for Windows では、スマートカード認証、証明書失効一覧のチェック、Kerberos 認証によるパススルー認証など、さまざまな認証方法を構成できます。

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

ドメインパススルー認証の構成

June 24, 2019

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

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

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

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

コマンドラインインターフェイスを使用したドメインパススルーの有効化

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

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

> 注
>
> 1 つ以上の StoreFront ストアを追加する構文については、コマンドラインパラメーターを使用した Receiver for Windows の構成とインストールを参照してください。

グラフィカルユーザーインターフェイスを使用したドメインパススルーの有効化

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

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

次の図は、シングルサインオンを有効にする方法を示しています。

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

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

SSON のグループポリシー設定

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

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

グループポリシーオブジェクト管理用テンプレートで **SSON** を構成する

1. **gpedit.msc** を開いて［コンピューターの構成］**>** ［管理テンプレート］**>** ［**Citrix** コンポーネント］**>** ［**Citrix Receiver**］**>** ［ユーザー認証］ の順に選択します。
2. （ユーザーのローカルマシンまたは VDA デスクトップのゴールデンイメージ、あるいはその両方で）次のローカルコンピューター GPO 設定を有効にします。
   - ［ローカルユーザー名とパスワード］を選択します。
   - ［有効］ を選択します。
   - ［パススルー認証を有効にします］ チェックボックスをオンにします。
3. （Citrix Receiver for Windows がインストールされた）エンドポイントまたは VDA デスクトップのゴールデンイメージを再起動します。

SSON グループポリシーに対する **ADM** ファイルの使用

次の手順により、ADM ファイルを使ってグループポリシー設定を構成します。

1. ［コンピューターの構成］**>** ［管理用テンプレート］**>** ［テンプレートの追加と削除］の順に選択してローカルグループポリシーエディタを開きます。

2. ［追加］ をクリックして ADM テンプレートを追加します。
3. **receiver.adm** テンプレートを問題なく追加したら、［コンピューターの構成］**>**［管理者テンプレート］**>**［従来の管理用テンプレート（**ADM**）］**>**［**Citrix** コンポーネント］**>**［**Citrix Receiver**］**>**［ユーザー認証］の順に選択します。
4. ローカルマシンまたは VDA デスクトップのゴールデンイメージ、あるいはその両方で Internet Explorer を開きます。
5. ［インターネットオプション］**>**［セキュリティ］**>**［信頼済みサイト］ の順に選択し、ストアパスのない StoreFront サーバーの完全修飾ドメイン名（FQDN）を一覧に追加します。例: `https://storefront.example.com`

   注：また Microsoft GPO を使って、StoreFront サーバーを信頼済みサイトに追加することもできます。GPO はゾーンの割り当て一覧へのサイトと呼ばれ、［コンピューターの構成］**>**［管理用テンプレート］**>**［**Windows** コンポーネント］**>**［**Internet Explorer**］**>**［インターネットコントロールパネル］**>**［セキュリティページ］ の順に選択してアクセスできます。
6. いったんログオフしてから、再度 Citrix Receiver エンドポイントにログオンします。

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

Delivery Controller で **XML** の信頼を有効にする

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

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

StoreFront および **Web Interface** での **SSON** の構成

StoreFront の構成

SSON を StoreFront および Web Interface で構成するには、Citrix Studio を StoreFront サーバーで開いて［認証］**>**［認証方法の追加と削除］ の順に選択します。［ドメインパススルー］ を選択します。

Web Interface 構成

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

Kerberos を使用したドメインパススルー認証の構成

June 24, 2019

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

Citrix Receiver for Windows では、スマートカードを使用する展開環境での Kerberos によるドメインパススルー認証がサポートされます。Kerberos とは、統合 Windows 認証（IWA）に含まれる認証方法の 1 つです。

Kerberos 認証を有効にすると、認証時に Citrix Receiver for Windows のパスワードが使用されません。このため、トロイの木馬型の攻撃でユーザーデバイス上のパスワードが漏えいすることを避けることができます。ユーザーは、指紋照合などの生体認証も含めて、さまざまな認証方式を使用してユーザーデバイスにログオンでき、公開リソースへ接続するときに資格情報を再入力する必要もありません。

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

1. Citrix Receiver for Windows のシングルサインオンサービスがスマートカードの PIN を取得します。
2. Citrix Receiver for Windows は、IWA（Kerberos）を使用して StoreFront へのユーザー認証を行います。すると、使用可能な仮想デスクトップおよびアプリケーションの情報を StoreFront が Citrix Receiver for Windows に提供します。
   注： この段階では Kerberos 認証を使用する必要はありません。Citrix Receiver for Windows での Kerberos の有効化は、PIN の再入力が求められないようにする場合のみ必要です。Citrix Receiver for Windows で Kerberos 認証を使用しない場合、StoreFront への認証にはスマートカード資格情報が使用されます。

3. HDX エンジン（従来「ICA クライアント」と呼ばれていたもの）がスマートカードの PIN を XenDesktop または XenApp に渡します。これにより、ユーザーが Windows セッションにログオンできます。最後に、XenDesktop または XenApp が、要求されたリソースを配信します。

Citrix Receiver for Windows で Kerberos 認証を使用する場合は、以下のように構成する必要があります。

- Kerberos を使用するには、サーバーと Citrix Receiver for Windows を、同じまたは信頼されている Windows Server ドメイン内に設置する必要があります。さらに、管理タスクを割り当てられるように、[Active Directory ユーザーとコンピューター] を使ってサーバーの信頼関係を構成する必要があります。
- ドメイン、および XenDesktop や XenApp で Kerberos が有効になっている必要があります。セキュリティを強化するには、Kerberos 以外の IWA オプションを無効にして、ドメインで必ず Kerberos が使用されるようにします。
- リモートデスクトップサービス接続で、基本認証や保存されたログオン情報を使用したり、常にユーザーにパスワードを入力させたりする場合、Kerberos によるログオンは使用できません。

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

> 警告
>
> このトピックの一部の構成手順では、レジストリの編集が必要です。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

スマートカードを使用する環境で **Kerberos** によるドメインパススルー認証を構成するには

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

Citrix Receiver for Windows のインストール時に、以下のコマンドラインオプションを指定します。

- /includeSSON

  これにより、ドメインに参加しているコンピューターにシングルサインオンコンポーネントがインストールされ、Citrix Receiver for Windows の IWA（Kerberos）による StoreFront への認証が有効になります。シングルサインオンコンポーネントは、スマートカードの PIN を格納します。次に、HDX エンジンがこの PIN を使用して、XenDesktop がスマートカードハードウェアと資格情報にアクセスできるようにします。XenDesktop は、自動的にスマートカードから証明書を選択して、HDX エンジンから PIN を取得します。

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

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

[管理用テンプレート] > [従来の管理用テンプレート（ADM）] > [Citrix コンポーネント] > [Citrix Receiver] > ［ユーザー認証］ > ［ローカルユーザー名とパスワード］

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

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

StoreFront を構成するには:

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

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

FastConnect API および **HTTP** 基本認証について

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

スマートカード認証の構成

June 24, 2019

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

- パススルー認証（シングルサインオン）- ユーザーが Citrix Receiver for Windows にログオンするときに使用するスマートカードの資格情報が保持されます。これにより、Citrix Receiver for Windows でのスマートカード認証が以下のように処理されます。

  - ドメインに属しているデバイスのユーザーがスマートカードの資格情報で Citrix Receiver にログオンした場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要はありません。
  - ドメインに属していないデバイスのユーザーがスマートカードの資格情報で Citrix Receiver for Windows にログオンした場合、仮想デスクトップやアプリケーションの起動時に資格情報を再入力する必要があります。

  パススルー認証を使用するには、StoreFront および Citrix Receiver for Windows での構成が必要です。

- **2** モード認証 - 認証方法として、スマートカードと、ユーザー名およびパスワードの入力を選択できます。この機能は、ユーザーがスマートカードを使用できない場合（スマートカードを自宅に忘れた場合や資格情報の有効期限が切れた場合など）に便利です。これを実行できるようにするには、スマートカードを許可するため False に設定した DisableCtrlAltDel メソッドを使って、サイトごとに専用ストアをセットアップする必要があります。2 モード認証には StoreFront 構成が必要です。NetScaler Gateway が解決策にある場合、構成する必要もあります。

  また 2 モード認証により、StoreFront 管理者は StoreFront コンソールで選択して同じストアにエンドユーザーにユーザー名とパスワードの両方とスマートカード認証を提供できます。StoreFrontのドキュメントを参照してください。

- 複数の証明書 - 単一または複数のスマートカードを使用する場合、複数の証明書を使用できます。ユーザーがスマートカードをリーダーに挿入すると、Citrix Receiver for Windows を含む、ユーザーデバイス上で実行されるすべてのアプリケーションで複数の証明書を使用できるようになります。証明書の選択方法を変更するには、Citrix Receiver for Windows を構成します。

- クライアント証明書による認証 - この機能を使用するには、NetScaler Gateway および StoreFront での構成が必要です。

  - NetScaler Gateway を使って StoreFront リソースにアクセスする場合、ユーザーがスマートカードを取り外した後で再認証が必要になることがあります。
  - NetScaler Gateway の SSL 構成で常にクライアント証明書による認証が使用されるようにすると、より安全になります。ただし、この構成では 2 モード認証を使用できません。

- ダブルホップセッション - ダブルホップセッションでは、Receiver とユーザーの仮想デスクトップとの間に追加の接続が確立されます。ダブルホップセッションをサポートする展開方法については、XenDesktop のドキュメントを参照してください。

- スマートカード対応のアプリケーション - Microsoft Outlook や Microsoft Office などのスマートカード対応アプリケーションでは、仮想デスクトップやアプリケーションセッションでドキュメントにデジタル署名を追加したりファイルを暗号化したりできます。

前提条件:

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

制限事項:

- 証明書は、ユーザーデバイス上ではなくスマートカード上に格納されている必要があります。
- Citrix Receiver for Windows はユーザー証明書を保存しませんが、構成時に PIN を格納できます。PIN はユーザーセッションの間に非ページ化メモリにのみキャッシュされ、ディスク内にはどの時点においても格納されません。
- Citrix Receiver for Windows では、スマートカードが挿入されたときに自動的には切断セッションに再接続されません。
- スマートカード認証が構成されている場合、Citrix Receiver for Windows では仮想プライベートネットワーク（VPN：Virtual Private Network）のシングルサインオンやセッションの事前起動がサポートされません。スマートカード認証で VPN トンネルを使用するには、ユーザーが NetScaler Gateway Plug-in をインストールして Web ページ経由でログオンする必要があります。この場合、各手順でスマートカードと PIN による認証が必要になります。スマートカードユーザーは、NetScaler Gateway Plug-in を使用した StoreFront へのパススルー認証を使用できません。
- Citrix Receiver for Windows Updater と citrix.com や Merchandising Server 間の通信では、NetScaler Gateway 上のスマートカード認証を使用できません。

> 警告
>
> このトピックの一部の構成手順では、レジストリの編集が必要です。レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows のインストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。レジストリエディターは、お客様の責任と判断の範囲でご使用ください。また、レジストリファイルのバックアップを作成してから、レジストリを編集してください。

スマートカード認証のシングルサインオンを有効にするには

Citrix Receiver for Windows のインストール時に、以下のコマンドラインオプションを指定します。

- ENABLE_SSON=Yes

  シングルサインオンは、「パススルー認証」と呼ばれることもあります。このオプションを指定すると、Citrix Receiver for Windows で PIN を繰り返し入力する必要がなくなります。

または、以下のポリシーおよびレジストリを設定します:

- [管理用テンプレート] > [従来の管理用テンプレート (ADM)] > [Citrix コンポーネント] > [Citrix Receiver] > [ユーザー認証] > [ローカルユーザー名とパスワード]
- シングルサインオンコンポーネントをインストールしていないデバイス上で、以下のいずれかのレジストリキーで SSONCheckEnabled に false を設定します。これにより、Citrix Receiver for Windows の Authentication Manager でシングルサインオンコンポーネントがチェックされなくなり、Citrix Receiver for Windows で StoreFront への認証が可能になります。

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

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

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

- /includeSSON を指定すると、シングルサインオン認証（パススルー認証）がインストールされます。資格情報のキャッシュおよびパススルードメインベース認証の使用を有効にします。
- Receiver のスマートカード認証とは別の方法（ユーザー名とパスワードなど）でユーザーがエンドポイントにログオンしている場合、コマンドラインは次のようになります。

```
1  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

  これによりログオン時に資格情報がキャプチャされるのを防ぎ、Citrix Receiver for Windows へのログオン時に PIN を格納することができます。

- グループポリシーエディターで、[管理用テンプレート] > [従来の管理用テンプレート（ADM）] > [Citrix コンポーネント] > [Citrix Receiver] > [ユーザー認証] > [ローカルユーザー名とパスワード] の順に選択します。

  パススルー認証を有効にします。構成およびセキュリティ設定によっては、パススルー認証を実行するために [すべての ICA 接続にパススルー認証を許可します] チェックボックスをオンにする必要があります。

StoreFront を構成するには:

- 認証サービスを構成する場合、[スマートカード] チェックボックスをオンにします。

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

ユーザーデバイスでスマートカードを使用できるようにするには

1. デバイスのキーストアに、証明機関のルート証明書をインポートします。
2. ご注意ください。
3. Citrix Receiver for Windows をインストールして構成します。

証明書の選択方法を変更するには

複数の証明書が有効な場合、Citrix Receiver for Windows ではデフォルトでそれらの証明書の一覧が表示され、ユーザーは使用する証明書を選択できます。管理者は、デフォルトの証明書（スマートカードプロバイダー指定の証明書）、または有効期限が最も残っている証明書が使用されるように構成できます。有効なログオン証明書がない場合はユーザーにメッセージが表示され、使用可能なほかのログオン方法が提示されます。

有効な証明書とは、以下のものを指します:

- ローカルコンピューターの現在時刻に基づき、証明書が有効期限内である。
- サブジェクトの公開キーで RSA アルゴリズムが使用されており、キーの長さが 1024、2048、または 4096 ビットである。
- Key Usage フィールドに Digital Signature が含まれている。
- Subject Alternative Name フィールドにユーザープリンシパル名（UPN）が含まれている。
- Enhanced Key Usage フィールドに Smart Card Logon および Client Authentication、または All Key Usages が含まれている。
- 証明書の発行者チェーンに含まれる証明機関の 1 つが、TLS ハンドシェイク時にサーバーから送信される、許可される識別名（DN）の 1 つに合致している。

証明書の選択方法を変更するには、以下のいずれかの構成を行います:

- Citrix Receiver for Windows のコマンドラインで、`AM\CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }` オプションを指定する。

  デフォルト値は、Prompt です。SmartCardDefault または LatestExpiry を指定して複数の証明書が該当する場合は、ユーザーが証明書を選択するための一覧が表示されます。

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

  最適な証明書をユーザーが選択できるように、HKEY_CURRENT_USER での設定は、HKEY_LOCAL_MACHINE の設定よりも優先されます。

CSP の PIN 入力メッセージを使用するには

Citrix Receiver for Windows のデフォルトでは、スマートカードの Cryptographic Service Provider（CSP）ではなく PIN 入力用のメッセージが表示されます。PIN の入力が必要な場合、Citrix Receiver for Windows がメッセージを表示して、ユーザーにより入力された PIN をスマートカードの CSP に渡します。プロセスごとやセッションごとの PIN のキャッシュが禁止されているなど、環境やスマートカードでより厳格なセキュリティが求められる場合は、CSP コンポーネントを使用して PIN 入力用のメッセージを表示して PIN を処理できます。

PIN 入力の処理方法を変更するには、以下のいずれかの構成を行います:

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

証明書失効一覧を使用してセキュリティ保護を強化

June 24, 2019

証明書失効一覧（CRL）のチェック機能を有効にすると、サーバー証明書が失効していないかどうかが Citrix Receiver によってチェックされます。強制的にこのチェックを行うことにより、TLS サーバーの暗号化認証機能が強化され、ユーザーデバイスとサーバー間の TLS 接続のセキュリティが向上します。

証明書失効一覧のチェック機能には、いくつかの設定レベルが用意されています。たとえば、ローカルの証明書失効一覧だけがチェックされるように Citrix Receiver を構成したり、ローカルおよびネットワーク上の証明書失効一覧がチェックされるように構成したりできます。さらに、すべての証明書失効一覧で証明書の有効性が検証されたときのみログオンするように構成できます。

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

1. 管理者として、［スタート］メニューから gpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既に Citrix Receiver for Windows のテンプレートをグループポリシーオブジェクトエディターにインポートしている場合、手順 2. ～ 5. は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、Receiver の Configuration フォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）に移動して、Citrix Receiver for Windows のテンプレートファイルを選択します。
   注：Windows のバージョンに応じた Citrix Receiver for Windows のテンプレートファイル（receiver.adm または receiver.admx/receiver.adml）を選択してください。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。
6. グループポリシーエディターで、［管理用テンプレート］、［従来の管理用テンプレート（ADM）］、［Citrix コンポーネント］、［Citrix Receiver］、［ネットワークルーティング］、［TLS/SSL データ暗号化およびサーバー識別］の順に選択します。
7. ［操作］メニューの［プロパティ］を選択し、［有効］をクリックします。
8. ［CRL 検証］の一覧からオプションを 1 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 検証］を設定しない場合、デフォルトは［ローカルに保存された CRL のみをチェックします］となります。

セキュリティで保護された通信

June 24, 2019

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

- Citrix NetScaler Gateway：詳しくは、このセクションのトピックと、NetScaler Gateway および StoreFront のドキュメントを参照してください。
  注：StoreFront サーバーとユーザーデバイス間の通信を保護するには、NetScaler Gateway を使用することをお勧めします。
- ファイアウォール。ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。サーバーの内部 IP アドレスを外部インターネットアドレスにマップするネットワークファイアウォール（つまり NAT（Network Address Translation：ネットワークアドレス変換））を介して Citrix Receiver for Windows を使用する場合は、外部アドレスを構成します。
- 信頼するサーバーの構成。
- XenApp または Web Interface 展開環境でのみ。XenDesktop 7 には適用されません。SOCKS プロキシサーバーまたはセキュアプロキシサーバー（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 プロトコルとセキュアプロキシプロトコルをサポートしています。
- XenApp または Web Interface 展開環境では、TLS（Transport Layer Security）プロトコルを使用する Citrix SSL Relay（XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5、または XenApp 7.5 には適用されません）。
- XenApp 7.6 および XenDesktop 7.6 の場合、ユーザーと VDA 間で直接 SSL 接続を有効にできます

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

TLS の構成および有効化

June 24, 2019

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

すべての Citrix Receiver for Windows 通信を TLS で暗号化するには、ユーザーデバイス、Citrix Receiver for Windows、および Web Interface サーバー（使用している場合）を構成します。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セクションを参照してください。詳しくは、Web Interface のドキュメントを参照してください。

前提条件:

ユーザーデバイスは、「システム要件」で指定された要件を満たす必要があります。

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

このオプションで、以下が可能になります:

- TLS の使用を適用する。インターネットを含めて、信頼されていないネットワークを介するすべての接続で、TLS の使用をお勧めします。
- FIPS（Federal Information Processing Standards）準拠の暗号化の使用を適用し、NIST SP 800-52 の推奨セキュリティへの準拠を可能にする。デフォルトでは、これらのオプションは無効になっています。
- 特定の TLS バージョンおよび特定の TLS 暗号の組み合わせの使用を適用する。Citrix Receiver for Windows と XenApp/XenDesktop 間で TLS 1.0、TLS 1.1、TLS 1.2 プロトコルがサポートされます。
- 特定のサーバーのみに接続する。
- サーバー証明書の失効を確認する。
- 特定のサーバー証明書発行ポリシーを確認する。
- 特定のクライアント証明書を選択する（サーバーが要求するよう構成されている場合）。

グループポリシーオブジェクト管理用テンプレートを使用して **TLS** サポートを構成するには

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
    - 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
    - ドメインでポリシーを適用するには、グループポリシー管理コンソールを使用して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
2. ［コンピューターの構成］ノードで、［管理用テンプレート］ > ［**Citrix Receiver**］ > ［ネットワークルーティング］ の順に移動して、［**TLS** およびコンプライアンスモードの構成］ ポリシーを選択します。
3. ［有効］ を選択してセキュリティで保護された接続を有効にし、サーバー上の通信を暗号化します。次のオプションを設定します。

    > 注：保護された接続で、TLS を使用することをお勧めします。

4. ［すべての接続で **TLS** が必要］ を選択することによって、公開アプリケーションおよびデスクトップに対する Citrix Receiver for Windows のすべての通信で強制的に TLS を使用させることができます。
5. ［セキュリティコンプライアンスモード］ ドロップダウンリストから、適切なオプションを選択します:
    - なし - コンプライアンスモードが適用されません。

- **SP800-52** - **SP800-52** を選択して NIST SP800-52 に準拠します。このオプションは、サーバーまたはゲートウェイを NIST SP 800-52 推奨セキュリティに準拠させる場合にのみ選択してください。

  注:

  ［SP800-52］を選択すると、［**FIPS** を有効にします］ が選択されていない場合でも、自動的に FIPS 準拠の暗号化が使用されます。Windows セキュリティオプションの ［システム暗号化：暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う］ も有効にする必要があります。有効にしない場合、Citrix Receiver for Windows が公開アプリケーションおよびデスクトップに接続できないことがあります。

  ［SP800-52］を選択した場合、［証明書失効チェックのポリシー］ で ［完全なアクセス権のチェック］ または ［完全なアクセス権のチェックと **CRL** が必要です］ のいずれかも選択する必要があります。

  ［SP800-52］を選択すると、Citrix Receiver for Windows はサーバー証明書が NIST SP 800-52 の推奨セキュリティに準拠しているかを検証します。サーバー証明書が準拠していない場合、Citrix Receiver for Windows が接続できないことがあります。

6. **FIPS** を有効にします - FIPS 準拠の暗号化の使用を適用するには、このオプションを選択します。オペレーティングシステムのグループポリシーから Windows セキュリティオプションの ［システム暗号化：暗号化、ハッシュ、署名のための **FIPS** 準拠アルゴリズムを使う］ も有効にする必要があります。有効にしない場合、Citrix Receiver for Windows が公開アプリケーションおよびデスクトップに接続できないことがあります。
7. ［許可された **TLS** サーバー］ ドロップダウンリストから、ポート番号を選択します。Citrix Receiver がコンマ区切りの一覧で指定されたサーバーにのみ接続できるようにします。ワイルド ― カードおよびポート番号を指定できます。たとえば、「*.citrix.com:4433」により、共通名が「.citrix.com」で終わるどのサーバーともポート 4433 での接続が許可されます。セキュリティ証明書の情報の正確さは、証明書の発行者によって異なります。Citrix Receiver が証明書の発行者を認識して信頼しないと、接続は拒否されます。
8. ［**TLS** バージョン］ ドロップダウンリストから、次のいずれかのオプションを選択します:

   - **TLS 1.0**、**TLS 1.1**、または **TLS 1.2** - これはデフォルトの設定です。このオプションは、業務上 TLS 1.0 との互換性が必要な場合のみお勧めします。
   - **TLS 1.1** または **TLS 1.2** - このオプションで ICA 接続が TLS 1.1 または TLS 1.2 を使用するようにします。
   - **TLS 1.2** - このオプションは、業務上 TLS 1.2 が必要な場合のみお勧めします。

9. **TLS** 暗号の組み合わせ - 特定の TLS 暗号の組み合わせの使用を適用するには、GOV（行政機関）、COM（営利企業）、ALL（すべて）の中から選択します。一部の NetScaler Gateway 構成では、COM の選択が必要になることがあります。

   Citrix Receiver for Windows は、ビット長 1024、2048 および、3072 の RSA キーをサポートします。さらに、ビット長 4096 の RSA キーを持つルート証明書がサポートされます。

   > 注：ビット長 1024 の RSA キーの使用はお勧めしません。

   以下は、サポートされるすべての暗号の組み合わせの一覧です。

- 任意:「任意」が設定されると、ポリシーは構成されず次のいずれかの暗号の組み合わせが許可されます。
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
- 商用:「商用」が設定されると、次の暗号の組み合わせのみが許可されます:
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
- 自治体:「自治体」が設定されると、暗号の組み合わせのみが許可されます:
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

10. [証明書失効チェックのポリシー] ドロップダウンリストから、次の任意のオプションを選択します。
    - ネットワークアクセスなしでチェックします - 証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアのみが使用されます。すべての配布ポイントが無視されます。証明書失効一覧の検索は、対象の SSL Relay/Secure Gateway サーバーによって提示されるサーバー証明書の検証に必須ではありません。
    - 完全なアクセス権のチェック - 証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。証明書失効一覧の検出は、ターゲットサーバーで提示されるサーバー証明書の検証に必要ではありません。
    - 完全なアクセス権と **CRL** のチェックが必要です - ルート CA を除いて証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。

- すべてに完全なアクセス権と **CRL** のチェックが必要です - ルート CA を含めた証明書失効一覧チェックが実行されます。ローカルの証明書失効一覧のストアおよびすべての配布ポイントが使用されます。証明書の失効情報が検出されると、接続は拒否されます。すべての必要な証明書失効一覧の検索が、検証において重大な意味を持ちます。
- チェックなし - 証明書失効一覧チェックは実行されません。

11. ［ポリシーの拡張 **OID**］ を使用して、Citrix Receiver for Windows が特定の証明書の発行ポリシーがあるサーバーにのみ接続するように制限できます。［ポリシーの拡張 **OID**］ を選択すると、Citrix Receiver for Windows はポリシーの拡張 OID があるサーバー証明書のみを受け入れます。
12. ［クライアント認証］ ドロップダウンリストから、以下の任意のオプションを選択します:
    - 無効 - クライアント認証が無効になります。
    - 証明書セレクタを表示します - 常にユーザーが証明書を選択するよう求めます。
    - 可能な場合、自動的に選択します - 特定する証明書に選択肢がある場合のみ、ユーザーに表示します。
    - 未構成 - クライアント認証が構成されていないことを意味します。
    - 指定された証明書を使用します - ［クライアント証明書］オプションの設定で指定された「クライアント証明書」を使用します。
13. ［**Client Certificate**］ 設定を使用して、識別証明書の拇印を指定します。これにより、ユーザーに不要なプロンプトを表示しないようにすることができます。
14. ［適用］ および ［**OK**］ をクリックしてポリシーを保存します。

次の表は、各セットの暗号の組み合わせを示しています:

TLS 暗号の組み合わせ	**GOV**	**COM**	**ALL**	**GOV**	**COM**	**ALL**	**GOV**	**COM**	**ALL**
FIPS を有効にします	オフ	オフ	オフ	オン	オン	オン	オン	オン	オン

セキュリティコンプライアンスモード	オフ	オフ	オフ	オフ	オフ	オフ	オン	オン	オン
SP800-52									
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384						☒			
TLS_ECD	☒		☒	☒		☒			
TLS_RSA_WITH_AES_256_GCM_SHA384				☒		☒	☒		☒
TLS_RSA	☒	☒	☒	☒	☒	☒	☒	☒	☒
TLS_RSA_WITH_AES_256_CBC_SHA256				☒		☒			
TLS_RSA	☒		☒	☒		☒	☒		☒
TLS_RSA_WITH_AES_128_CBC_SHA					☒	☒		☒	☒
TLS_RSA		☒	☒						
TLS_RSA_WITH_RC4_128_MD5									
TLS_RSA	☒		☒	☒		☒	☒		☒

Web Interface 5.4 でのスマートカード認証の構成

June 24, 2019

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

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

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

このポリシーが有効な場合、クライアントデバイスからスマートカードが取り出されるとユーザーは XenApp セッ

ションからログオフされます。ただし、ユーザーは Citrix Receiver for Windows には引き続きログインしたままになります。

このポリシーを有効にするには、Web Interface XenApp Services サイトでスマートカードの取り出しポリシーを設定する必要があります。この設定は、Web Interface 5.4 の［**XenApp Services** サイト］**>**［スマートカードパススルー認証］**>**［ローミングを有効にする］**>**［スマートカードの取り出し時にセッションをログオフする］ で行います。
スマートカードの取り出しポリシーが無効な場合、クライアントデバイスからスマートカードが取り外されるとユーザーの XenApp セッションは切断されます。Web Interface XenApp Services サイトでスマートカードを取り出しても影響はありません。
注：32 ビットクライアントと 64 ビットクライアント向けのポリシーは異なります。32 ビット向けのポリシーの名前は スマートカードの取り出しポリシー（**32** ビットマシン） であり、64 ビット向けのポリシー名は スマートカードの取り出しポリシー（**64** ビット） です。

スマートカードのサポートおよび取り出しの変更

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

- Citrix Receiver for Windows 4.5 より、PNAgent サイトへのログインでもスマートカードによるログインがサポートされるようになりました。
- PNAgent サイトでのスマートカードの取り出しポリシーは次のように変更されました。
  スマートカードを取り外すと XenApp セッションからログオフされます。ただし、PNAgent サイトの認証方法をスマートカードに設定している場合、XenApp セッションからのログオフを有効にするには Receiver for Windows で対応するポリシーを構成する必要があります。XenApp PNAgent サイトでスマートカード認証のローミングを有効にして、Receiver セッションから XenApp をログオフするスマートカードの取り出しポリシーを有効にします。ユーザーは Receiver セッションにログインしたままになります。

既知の問題

スマートカード認証を使用して PNAgent サイトにログインした場合、ユーザー名が［ログオン済み］と表示されます。

Secure Gateway による接続

November 12, 2018

このトピックの内容は、Web Interface 環境にのみ適用されます。

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

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

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

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

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

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

完全修飾ドメイン名には、以下の 3 つの要素を順に指定する必要があります:

- ホスト名
- サブドメイン名
- 最上位ドメイン名

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

ファイアウォールを介した接続

June 24, 2019

ネットワークファイアウォールは、送信先アドレスとポート番号に基づいてパケットを通過させたりブロックしたりできます。ファイアウォールが使用されている環境では、Citrix Receiver for Windows と Web サーバーおよび Citrix 製品のサーバーとの通信がファイアウォールでブロックされないように設定する必要があります。

共通の **Citrix** 通信ポート

接続元	種類	ポート	詳細
Citrix Receiver	TCP	80/443	StoreFront との通信

接続元	種類	ポート	詳細
ICA/HDX	TCP	1494	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX（セッション画面の保持機能）	TCP	2598	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX（SSL 経由）	TCP	443	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX（HTML5 Receiver）	TCP	8008	アプリケーションおよび仮想デスクトップへのアクセス
ICA/HDX オーディオ（UDP 経由）	TCP	16500 ～ 16509	ICA/HDX オーディオのポート範囲
IMA	TCP	2512	Independent Management Architecture（IMA）
管理コンソール	TCP	2513	Citrix 管理コンソールおよび *WCF サービス。注：FMA ベースのプラットフォーム 7.5 以降では、ポート 2513 は使用されません。
アプリケーション/デスクトップ要求	TCP	80/8080/443	XML Service
STA	TCP	80/8080/443	Secure Ticketing Authority（XML Service に組み込み済み）

> 注
>
> XenApp 6.5 では、ポート 2513 は WCF 経由の XenApp Command Remoting サービスに使用されます。

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、Citrix Receiver for Windows でのサーバー接続で、外部アドレスおよびポート番号が使用されるようになります。詳しくは、Web Interfaceのドキュメントを参照してください。

プロキシサーバー経由の接続

June 24, 2019

プロキシサーバーは、ネットワークから外部へのアクセスや外部からネットワークへのアクセスを制限して、Citrix Receiver for Windows とサーバー間の接続を制御するために使います。Citrix Receiver for Windows は、SOCKS プロトコルとセキュアプロキシプロトコルをサポートしています。

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

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

接続中に Citrix Receiver for Windows がプロキシサーバーを優先するか無視するかについて、レジストリエディターでプロキシ設定を構成します。

> 警告
>
> レジストリエディターの使用を誤ると、深刻な問題が発生する可能性があり、Windows の再インストールが必要になる場合もあります。レジストリエディターの誤用による障害に対して、シトリックスでは一切責任を負いません。

1. HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager に移動します。\
2. **ProxyEnabled**（REG_SZ）を設定します。
    a) True - Citrix Receiver for Windows は接続でプロキシサーバーを優先します。
    b) False - Citrix Receiver for Windows は接続でプロキシサーバーを無視します。
3. レジストリエディターを閉じます。
4. Citrix Receiver for Windows のセッションを再起動して、この変更を適用します。

信頼関係の適用

November 12, 2018

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

信頼済みサーバー機能を有効にすることで、要件を指定し、サーバーへの接続が信頼済みかどうかを判断できます。たとえば、特定のアドレス（https://*.citrix.comなど）に特定の接続の種類（TLS など）を使用して接続する Citrix Receiver for Windows は、サーバーの信頼済みゾーンに接続されます。

この機能を有効にすると、接続されたサーバーは Windows の信頼済みサイトゾーンに配置されます。Windows の信頼済みサイトゾーンにサーバーを追加する手順について詳しくは、Internet Explorer のオンラインヘルプを参照してください。

グループポリシーオブジェクト管理用テンプレートを使用して信頼済みサーバーの構成を有効にするには

前提要件:

コネクションセンターなどの Citrix Receiver for Windows コンポーネントを終了します。

1. gpedit.msc を管理者として実行して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを開きます。
   a) 1 台のコンピューターでポリシーを適用するには、［スタート］メニューから Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
   b) ドメインでポリシーを適用するには、グループポリシー管理コンソールを使用して、Citrix Receiver グループポリシーオブジェクト管理用テンプレートを起動します。
2. ［コンピューターの構成］で、［管理用テンプレート］、［従来の管理用テンプレート（**ADM**）］、［**Citrix** コンポーネント］、［**Citrix Receiver**］、［ネットワークルーティング］、［信頼済みサーバーの構成を構成します］ の順に選択します。
3. ［有効］ を選択して、Citrix Receiver for Windows に領域の識別を適用します。
4. ［信頼済みサーバーの構成を適用します］ を選択します。これによって、クライアントに信頼済みサーバーを使用した識別を適用します。
5. ［**Windows** インターネットゾーン］ ドロップダウンリストから、クライアントのサーバーアドレスを選択します。この設定は Windows の信頼済みサイトにのみ適用できます。
6. ［アドレス］ フィールドで、Windows 以外の信頼済みサイトゾーンのクライアントサーバーアドレスを設定します。コンマ区切り一覧を使用できます。
7. ［**OK**］ および ［適用］ をクリックします。

昇格レベルと **wfcrun32.exe**

August 7, 2018

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

例 **1**:

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

例 **2**:

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

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

June 24, 2019

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

ICA ファイル署名機能は、認証していないアプリケーションやデスクトップをユーザーが起動しないようにするのに役立ちます。Citrix Receiver for Windows は、信頼できるソースからアプリケーションまたはデスクトップが起動されることを管理ポリシーに基づいて検証し、信頼されていないサーバーからの起動を防ぎます。このアプリケーションまたはデスクトップの起動署名検証ための Citrix Receiver for Windows セキュリティポリシーは、グループポリシーオブジェクト、Storefront、または Citrix Merchandising Server を使用して構成できます。ICA ファイル署名はデフォルトで無効になっています。Storefront に対する ICA ファイル署名については、Storefront のドキュメントを参照してください。

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

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

グループポリシーオブジェクトを使用してアプリケーションまたはデスクトップの起動署名検証を有効にし設定するには、次の手順に従います。

1. 管理者として、［スタート］メニューから gpedit.msc を実行（単一のコンピューターにポリシーを適用する場合）するか、グループポリシー管理コンソールを使用（ドメインポリシーを適用する場合）して、グループポリシーエディターを開きます。
   注：既に ica-file-signing.adm テンプレートをグループポリシーオブジェクトエディターにインポートしている場合は、手順 2. ～ 5. は省略できます。
2. グループポリシーエディターで［管理用テンプレート］を選択します。
3. ［操作］メニューの［テンプレートの追加と削除］を選択します。
4. ［追加］を選択し、Citrix Receiver for Windows の Configuration フォルダー（通常は、C:\Program Files\Citrix\ICA Client\Configuration）を参照して ica-file-signing.adm を選択します。
5. ［開く］をクリックしてテンプレートを追加し、［閉じる］をクリックしてグループポリシーエディターのメインウィンドウに戻ります。

6. グループポリシーエディターで、［管理用テンプレート］>［従来の管理用テンプレート（ADM）］>［Citrix コンポーネント］>［Citrix Receiver］の順に選択し、［ICA ファイルの署名を有効にします］を開きます。
7. ［有効］をクリックすると、信頼できる証明書のサムプリントのホワイトリストに署名証明書のサムプリントを追加したり、ホワイトリストから署名証明書のサムプリントを削除したりできます。これは、［表示］をクリックして［内容の表示］ダイアログボックスを使用して行います。署名証明書のサムプリントは署名証明書のプロパティからコピーして貼り付けることができます。［セキュリティポリシー］ボックスの一覧から［署名による起動のみを許可します (安全性が高い)］または［署名されていない起動 (安全性が低い) でユーザーにプロンプトを表示します］を選択します。

オプション	説明
署名による起動のみを許可します（安全性が高い）	正しく署名された、信頼できるサーバーからのアプリケーションまたはデスクトップの起動のみを許可します。アプリケーションまたはデスクトップの起動に無効な署名がされている場合は、Citrix Receiver for Windows にセキュリティの警告メッセージが表示されます。ユーザーは続行できず、承認されていない起動が禁止されます。
署名されていない起動（安全性が低い）でユーザーにプロンプトを表示します	未署名または無効な署名のアプリケーションまたはデスクトップの起動が試行されるたびに、確認ダイアログボックスが開きます。ユーザーはアプリケーションの起動を続行することも、起動を中止する（デフォルト）こともできます。

デジタル署名証明書を選択して配布するには

デジタル署名証明書を選択するときは、次の一覧の上位のオプションから順にお勧めします。

1. 周知の証明機関からコード署名証明書または SSL 署名証明書を購入する。
2. 社内に証明機関がある場合はその証明機関を使用して、コード署名証明書または SSL 署名証明書を作成する。
3. Web Interface のサーバー証明書などの既存の SSL 証明書を使用する。
4. 新しいルート証明書を作成して、GPO または手動インストールによりユーザーデバイスに配布する。

Citrix Receiver for Windows のヘルプ

August 7, 2018

Citrix Receiver とは

August 7, 2018

Citrix Receiver は、任意のデバイス上に仮想デスクトップやアプリケーションへのアクセスを提供し、場所を問わずに簡単にこれらのリソースを使用できます。Receiver は、安全かつ簡単に使用でき、異なるデバイス上でも同じ方法で使用できます。

注: これらのトピックで説明している一部の機能へのアクセスが管理者により制限されている場合もあります。

アカウントの追加またはサーバーの切り替え

November 12, 2018

ヘルプデスクによりアカウントの追加を求められたり、異なる NetScaler Gateway を使用するように指示された場合は、次の手順で実行します:

Citrix Receiver for Windows アカウントを追加するには

1. Citrix Receiver for Windows ホームページで、下矢印をクリックし、［アカウント］ を選択します。
2. ［アカウントの追加］ウィンドウで［追加］をクリックして、ヘルプデスクから提供された情報を入力します。

別の **NetScaler Gateway** を使用するには

NetScaler Gateway サーバーを身元照会に使用している場合があります。

1. Citrix Receiver for Windows アイコンを右クリックして ［バージョン情報］ を選択します。
2. ［**NetScaler Gateway**］ メニューでサーバーを選択します。

デスクトップの外観と操作性の変更

January 9, 2019

仮想デスクトップはウィンドウ内に開きます。ウィンドウのツールバー上のボタンを使用して、デスクトップの移動、サイズ変更、およびファイルとデバイスのアクセス方法の制御を行います。小さなツールバーグリップがウィンドウまたは（最大化した場合は）画面の上部に表示されます。グリップをクリックするとツールバーが表示されます。

ツールバーを画面上のほかの位置に移動するには

ツールバーは、ほかのウィンドウの内容やコントロールに重ならないように、使いやすい位置に移動できます。

- ウィンドウまたは画面上部に表示されるツールバーグリップをクリックし、左または右に移動します。

ローカルファイルへのアクセスを制御するには

仮想デスクトップからローカルコンピューター上のファイルにアクセスする場合は、そのアクセス方法を制御することができます。

- ツールバーで ［基本設定］>［ファイルアクセス］ の順にクリックし、次のいずれかのオプションを選択し、［OK］をクリックします:

オプション	説明
読み取りと書き込み	仮想デスクトップからのローカルファイルの読み取りおよび書き込みを許可します。
読み取り専用	仮想デスクトップからのローカルファイルの読み取りを許可しますが、書き込みは許可しません。
アクセスなし	仮想デスクトップからのローカルファイルへのアクセスを許可しません。
毎回確認する	仮想デスクトップからローカルファイルにアクセスするたびに確認のメッセージが表示されます。

マイクまたは **Web** カメラをセットアップするには

仮想デスクトップからローカルのマイクまたは Web カメラにアクセスする方法を変更する場合は、以下の手順に従います。

- ツールバーで［基本設定］>［接続］の順にクリックし、次のいずれかのオプションを選択します。

オプション	説明
自動的に接続	仮想デスクトップでのマイクまたは Web カメラの使用を許可します。
接続しない	仮想デスクトップでのマイクまたは Web カメラの使用を許可しません。
確認する	仮想デスクトップからマイクまたは Web カメラにアクセスするたびに確認のメッセージが表示されます。

1. ［グローバル設定］で［優先 **Web** カメラ］を選択します。
2. ［OK］をクリックします。

制限事項:

- ［優先 Web カメラ］ダイアログボックスは、Desktop Delivery Controller で Windows メディアのリダイレクトポリシーが ［無効］ に設定されていても、Citrix コネクションセンターに表示されます。

Desktop Viewer でのデバイスの表示

January 9, 2019

Citrix Receiver for Windows によりコンピューターに接続しているデバイスが検出され、ホストされるデスクトップやアプリケーションで使用するデバイスを選択できます。

［基本設定］**>**［接続］の順に選択して、マイクや Web カメラといったデバイスを仮想セッションに接続するかしないかカスタマイズできます。

- ［基本設定］>［デバイス］のデバイスの一覧には、ローカルマシンに接続されたデバイスが表示されます。
- デバイスに接続しているのにデバイスの一覧にそれが表示されない場合は、［更新］をクリックします。
- 接続すると、［最適化］、［ポリシー制限］、または［汎用］としてデバイスが表示されます。

デバイス	説明
最適化済み	デバイスに Citrix 仮想チャネルがあり、自動的にリモートセッションとローカルマシンの両方において同時に使用できるようになります。最適化されたデバイスの［現在の接続］列には、ローカルマシンとリモートセッションの両方で接続されているデバイスが表示されます。［リダイレクト］チェックボックスはオンのまま変更できません。［仮想チャネル］列の切り替えボタンを使って［汎用］と［最適化］を切り替えることができます。たとえば、仮想チャネルがデバイスの機能のすべてをサポートしない場合は、［汎用に切り替え］をクリックします。
汎用	デバイスに Citrix 仮想チャネルがなく、ローカルマシンとリモートセッションで同時には使用できません。［リダイレクト］チェックボックスを使って、デバイスをリモートセッションで使うのか、ローカルマシンで使うのかを切り替えます。［現在の接続］列で、現在の接続の状態を確認できます。

デバイス	説明
ポリシー制限	この種類のデバイスを制限するため、管理者によりポリシーが設定されています。たとえば、USB マウスおよびキーボードの動作は USB をサポートしないリモートセッションで自動的に処理されるため、通常はデフォルトでこれらのポリシーが制限されています。ネットワークデバイスなどそのほかのデバイスは、セキュリティ上の理由により制限されることがあります。ポリシー制限の［現在の接続］列にはローカルマシンのみが表示されます。ポリシー制限のデバイスでは［リダイレクト］チェックボックスをオンにはできません。

パスワードの管理

June 24, 2019

Citrix Single Sign-On は、アプリケーションや Web サイトにアクセスするときに必要なログオン情報（ユーザー名やパスワードなど）を管理します。ユーザーのログオン情報は、Single Sign-On が動作するすべてのコンピューターからアクセスできる、ネットワーク上のデータベースに保管されます。つまり、組織内のほかのコンピューターからこれらのアプリケーションや Web サイトにアクセスする場合でも、Single Sign-On に登録済みの自分のログオン情報を使用して自動ログオンできます。

Single Sign-On を使用すると、ログオン操作を自動化できるだけでなく、ヘルプデスクの手を煩わせずに自分で Windows 用パスワードをリセットしたりアカウントのロックを解除したりできます。Single Sign-On では、安全なパスワードをユーザーに代わって自動生成することもできます。

管理者の設定により、ユーザーがコンピューターにログオンしたとき、またはパスワードで保護されたアプリケーションや Web サイトを初めて開いたときに、Single Sign-On が自動的に起動します。Single Sign-On が起動すると、ユーザーの情報が登録されているデータベースに接続して、ユーザーの同一性を確認します。同一性が正しく確認されると、ユーザーは、登録済みのログオン情報を使ってアプリケーションや Web サイトに自動的にログオンできるようになります。ログオン情報が登録されていないアプリケーションや Web サイトを開くと、ログオン情報を登録するかどうかを確認するメッセージが表示されます。

管理者の設定によっては、Single Sign-On を Windows の［スタート］メニューから起動することもできます。

- ［スタート］ボタンをクリックし、［(すべての) プログラム］**>** ［**Citrix**］**>** ［**Citrix Single Sign-On**］の順に選択します。

Single Sign-On を終了するには、Citrix Receiver for Windows を終了する必要があります。ただし、Citrix Receiver を終了せずに Single Sign-On だけを一時停止することができます。

重要：Single Sign-On は、管理者が環境に合わせて設定をカスタマイズできる、柔軟性に富んだ製品です。管理者の設定によっては、このドキュメントに記載されている機能の一部がユーザー側で使用できない場合があります。たとえば、パスワード文字列を表示する機能などが無効に設定されている場合があります。また、操作の手順がこのヘルプの記述と異なる場合があります。このドキュメントはユーザー側のさまざまな状況を想定して作成されていますが、一部の状況が網羅されていない場合があります。詳しい内容は、シトリックスのドキュメントで公開されています。

アカウントセルフサービスの使用

November 12, 2018

管理者がアカウントセルフサービス機能を有効に設定している場合、シングルサインオンのユーザーは次の操作を実行できます。

- Windows アカウントがロックされているというメッセージが表示された場合に、アカウントのロックを解除する。
- Windows にログオンするときのパスワード（プライマリパスワード）を忘れてコンピューターにログオンできない場合に、パスワードを再設定する。

［ユーザーの切り替え］画面（Windows Vista、Windows 7、Windows Server 2008、および Windows Server 2008 R2）、または［**Windows** へのログオン］と［コンピュータのロックの解除］ダイアログボックス（サポートされるそのほかの Windows）に［アカウントセルフサービス］ボタンが表示されます。このボタンをクリックすると、アカウントセルフサービスウィザードが起動します。

アカウントセルフサービスウィザードを使用すると、ヘルプデスクに連絡しなくても、アカウントの問題を自分で解決できます。

重要：アカウントセルフサービスウィザードを使用する場合、ユーザーの同一性を確認するために、セキュリティ用の質問に対する回答を再入力する必要があります。Windows 用パスワードをリセットしたりアカウントのロックを解除したりするときにセキュリティ用の質問に対する回答がわからない場合は、組織のサポート担当者に連絡してください。

Windows アカウントのロックを解除するには（**Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2**）

1. 画面のメッセージに従って、Ctrl + Alt + Del キーを押します。
2. 次のいずれかを行います：
   - ようこそ画面で、［ユーザーの切り替え］をクリックします。
     ［ユーザーの切り替え］画面が開きます。

- ようこそ画面で、［他の資格情報］をクリックします。
  ［ユーザーの切り替え］画面が開きます。

3. ［アカウントセルフサービス］をクリックします。［アカウントセルフサービス］画面が開きます。
4. タイトルの下の［パスワードのリセットまたはアカウントのロック解除を行うには、ここをクリックしてください。］をクリックして、アカウントセルフサービスウィザードを起動します。
5. ［アカウントセルフサービスウィザードへようこそ］ページで［アカウントのロックを解除する］をクリックして、［次へ］をクリックします。
6. ［アカウントの確認］ページで正しいユーザー名とドメインが表示されていることを確認して、［次へ］をクリックします。［アカウントのロック解除］ページが開きます。
7. ［アカウントのロック解除］ページで［次へ］をクリックします。最初のセキュリティ用の質問が表示されます。
8. ［回答］ボックスにセキュリティ用の質問の回答を入力し、［次へ］をクリックします。セキュリティ用の質問が複数ある場合は、次の質問が表示されます。
9. ［アカウントのロック解除］ ページが開くまで、手順 8. を繰り返します。
10. ［アカウントのロック解除］ページで［次へ］をクリックします。
11. ［アカウントのロック解除の完了］ページで［完了］をクリックします。

Windows アカウントのパスワードをリセットするには（**Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2**）

1. 画面のメッセージに従って、Ctrl + Alt + Del キーを押します。
2. 次のいずれかを行います：
   - ようこそ画面で、［ユーザーの切り替え］をクリックします。
     ［ユーザーの切り替え］画面が開きます。
   - ようこそ画面で、［他の資格情報］をクリックします。
     ［ユーザーの切り替え］画面が開きます。
3. ［アカウントセルフサービス］をクリックします。［アカウントセルフサービス］画面が開きます。
4. タイトルの下の ［パスワードのリセットまたはアカウントのロック解除を行うには、ここをクリックしてください。］ をクリックして、アカウントセルフサービスウィザードを起動します。
5. ［アカウントセルフサービスウィザードへようこそ］ ページで ［パスワードをリセットする］ をクリックして、［次へ］ をクリックします。
6. ［アカウントの確認］ページで正しいユーザー名とドメインが表示されていることを確認して、［次へ］をクリックします。［パスワードのリセット］ページが開きます。
7. ［パスワードのリセット］ページで［次へ］をクリックします。最初のセキュリティ用の質問が表示されます。
8. ［回答］ボックスにセキュリティ用の質問の回答を入力し、［次へ］をクリックします。
9. ［新しいパスワードの入力］ ページが開くまで、手順 8. を繰り返します。
10. ［新しいパスワードの入力］ ページで新しいパスワードを入力し、確認のためもう一度入力します。［次へ］ をクリックします。
11. ［パスワード変更の完了］ページで［完了］をクリックします。［アカウントセルフサービス］画面に戻り、ユーザーを選択して Windows にログオンできるようになります。

Windows アカウントのロックを解除するには（**Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2** 以外のシステム）

1. 次のいずれかを行います：
   - ［**Windows** へようこそ］ダイアログボックスで Ctl + Alt + Del キーを押し、必要な場合は［オプション］をクリックします。
   - ［コンピュータのロック］ダイアログボックスで、Ctl + Alt + Del キーを押し、［コンピュータのロックの解除］ダイアログボックスで［オプション］をクリックします。
2. ［アカウントセルフサービス］をクリックして、アカウントセルフサービスウィザードを起動します。
3. ［アカウントセルフサービスウィザードへようこそ］ページで［アカウントのロックを解除する］をクリックして、［次へ］をクリックします。
4. ［アカウントの確認］ページで正しいユーザー名とドメインが表示されていることを確認して、［次へ］をクリックします。［アカウントのロック解除］ページが開きます。
5. ［アカウントのロック解除］ページで［次へ］をクリックします。最初のセキュリティ用の質問が表示されます。
6. ［回答］ボックスにセキュリティ用の質問の回答を入力し、［次へ］をクリックします。セキュリティ用の質問が複数ある場合は、次の質問が表示されます。
7. ［アカウントのロック解除］ ページが開くまで、手順 6. を繰り返します。
8. ［アカウントのロック解除］ページで［次へ］をクリックします。
9. ［アカウントのロック解除の完了］ページで［完了］をクリックします。

Windows アカウントのパスワードをリセットするには（**Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2** 以外のシステム）

1. 次のいずれかを行います：
   - ［**Windows** へようこそ］ダイアログボックスで Ctl + Alt + Del キーを押し、必要な場合は［オプション］をクリックします。
   - ［コンピュータのロック］ダイアログボックスで、Ctl + Alt + Del キーを押し、［コンピュータのロックの解除］ダイアログボックスで［オプション］をクリックします。
2. ［アカウントセルフサービス］をクリックして、アカウントセルフサービスウィザードを起動します。
3. ［アカウントセルフサービスウィザードへようこそ］ ページで ［パスワードをリセットする］ をクリックして、［次へ］ をクリックします。
4. ［アカウントの確認］ページで正しいユーザー名とドメインが表示されていることを確認して、［次へ］をクリックします。［パスワードのリセット］ページが開きます。
5. ［パスワードのリセット］ページで［次へ］をクリックします。最初のセキュリティ用の質問が表示されます。
6. ［回答］ボックスにセキュリティ用の質問の回答を入力し、［次へ］をクリックします。
7. ［新しいパスワードの入力］ ページが開くまで、手順 6. を繰り返します。
8. ［新しいパスワードの入力］ページで新しいパスワードを入力し、確認のためもう一度入力します。［次へ］をクリックします。
9. ［パスワード変更の完了］ページで［完了］をクリックします。

パスワードの手動変更

November 12, 2018

1. アプリケーションまたは Web サイトのパスワードを、通常の手順に従って変更します。
2. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
3. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［編集］をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。
4. ［パスワード］ボックスに入力されている内容を削除して、手順 1. で設定した新しいパスワードを入力します。
5. ［**OK**］ をクリックします。新しいパスワードが Single Sign-On に登録されます。

一般的な問題とその解決方法

November 12, 2018

ここでは、Single Sign-On を使用するときに生じる可能性のある、以下の問題や疑問点について説明します。

パスワードの有効期限切れメッセージが表示される

パスワードを定期的に変更することで、情報管理のセキュリティを向上させることができます。管理者の設定によっては、パスワードを長期間変更せずに使用していることを警告するメッセージが表示されます。

このメッセージは、パスワードを変更するまで表示されます。

Single Sign-On を実行したくない

Single Sign-On の機能を一時的に無効にした方がよい場合があります。たとえば、アプリケーションにログオンしないでログオンページを操作しなければならない場合など、Single Sign-On の自動ログオン機能を使用したくないことがあります。

この場合、Single Sign-On の一時停止機能を使用します。一時停止機能を使用すると、Single Sign-On を起動したまま自動ログオン処理を無効にすることができます。

新しいパスワードがアプリケーションに拒否される

一部のアプリケーションで、Single Sign-On のパスワードの変更ウィザードで変更したパスワードが拒否され、ログオンできなくなることがあります。

この問題は、パスワードの変更ウィザードにより Single Sign-On に登録された新しいパスワードが、アプリケーション側で許可されない場合に発生します。この場合、Single Sign-On により送信されるパスワードが、アプリケーション側で無効なものとして認識されます。

この問題を解決するには、［以前のパスワードに戻す］機能を使用します（この機能が管理者により有効になっている場合）。

注：この機能を使用できない場合は、ヘルプデスクに連絡してください。

アプリケーションの以前のパスワードに戻すには

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［編集］をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   選択したアプリケーションのプロパティダイアログボックスが開きます。
3. ［以前のパスワードに戻す］をクリックして、［はい］をクリックします。

自分のユーザーデータにアクセスできない

コンピューターにログオンすると、Single Sign-On は Single Sign-On のユーザー情報が保存されているサーバーに接続します。接続が確立され、ユーザー情報が確認されると、Single Sign-On が動作を開始します。

接続が確立されなかったり、ユーザー情報が確認されなかったりすると、Single Sign-On は起動しません。この場合、ユーザーデータにアクセスできないというエラーメッセージが表示されます。この問題が発生した場合は、ヘルプデスクに連絡してください。

Web ブラウザー使用時に **Single Sign-On** が動作しない

Single Sign-On は、Microsoft Internet Explorer をサポートしています。Internet Explorer 以外の Web ブラウザーでは、正しく動作しない場合があります。

アプリケーションからログオフしても再ログオンされる

アプリケーションや Web サイトによっては、ログオフした後にログオン用の画面が再び開く場合があります。このとき、管理者の設定によっては、Single Sign-On がそのアプリケーションに再度ログオンしてしまうことがあります。

この問題を解決するには、次の操作を行います。

- アプリケーションからログオフする前に、Single Sign-On の一時停止機能を使用します（管理者が有効に設定している場合）。
- 一時停止機能が有効でない場合は、アプリケーションからのログオフ後、Single Sign-On が再ログオンする前にアプリケーションのウィンドウを閉じます。

注：この問題を完全に解決するには、ヘルプデスクに連絡して、アプリケーション定義の詳細な検出設定の［初回のログオンのみを自動処理する］オプションを有効にするように管理者に通知してください。

オフラインで作業する場合に必要な設定

Single Sign-On Plug-in をネットワーク上のサーバーではなくユーザーのラップトップコンピューターなどにインストールする場合、社内ネットワークに接続していないときでも Single Sign-On を使用できるようにするには、事前にライセンスを更新しておく必要があります。これにより、社内ネットワークに再接続するまで、ライセンスが正規に割り当てられます。

Single Sign-On のライセンスを更新するには

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

2. ［バージョン情報］をクリックします。

   ［**Citrix Single Sign-On** のバージョン情報］ ダイアログボックスが開きます。

3. ［ライセンス情報の更新］をクリックします。

4. ［**OK**］ をクリックします。

   ［**Citrix Single Sign-On** のバージョン情報］ ダイアログボックスが閉じます。

ワークステーションがロックされる

ユーザーが、より高いセキュリティレベルを必要とする操作を実行しようとすると、そのユーザーが本人であることを確認するためにワークステーションがロックされます。たとえば、パスワードを変更したり、パスワードの文字列を表示したりする場合に、ユーザーの同一性検証が必要になります。

ワークステーションがロックされたら、Windows アカウントのパスワードを入力して、本人であることを証明します。セキュリティ用の質問に対する回答を入力する必要がある場合もあります。これにより、本人以外のユーザーが Single Sign-On の自動ログオン機能を使って、パスワードで保護されるべき機密情報に不正にアクセスすることが避けられます。

これは煩雑な作業のように見えますが、ユーザー自身、データ、および組織のセキュリティを保護するための作業です。

パスワードの自動変更

June 24, 2019

Single Sign-On のパスワード変更ウィザードでは、アプリケーションや Web サイトのパスワードを簡単に変更できます。管理者の設定により、新しいパスワードをユーザーが作成したり、自動的に生成したりできます。

注：パスワード変更ウィザードが自動的に生成するパスワードでは、任意の文字、数字、および記号などが組み合わされるため、パスワードのセキュリティレベルを高めることができます。パスワードの自動作成機能では、ユーザーがパスワードを作成したり管理したりする必要がないため、この自動作成機能を使用することをお勧めします。

管理者の設定により、パスワード変更ウィザードは、次のどちらかの方法で起動します。

- アプリケーションからのパスワード変更要求により自動的にウィザードが起動する。
- ユーザーがウィザードを起動する。

アプリケーションや Web サイトのパスワード変更用の画面を Single Sign-On が認識できない場合は、パスワード変更ウィザードが起動しません。この場合、アプリケーションや Web サイトと Single Sign-On の両方で、登録されているパスワードを手作業で変更する必要があります。アプリケーションや Web サイト上で設定した新しいパスワードが Single Sign-On に登録されているパスワードと異なると、自動ログオンに失敗します。

パスワードの作成方法の選択

パスワード変更ウィザードでは、新しいパスワードの作成方法を選択できます（管理者が許可している場合）。パスワード変更ウィザードの［パスワードの作成方法を選択してください。］ページで、以下のいずれかのオプションを選択します。使用できるオプションは、次のとおりです：

- 自動作成されたパスワードを選択する

このオプションを選択して［次へ］をクリックすると、セキュリティレベルの高いパスワードがパスワード変更ウィザードによって生成されます。生成されたパスワードは Single Sign-On で自動的に管理されるため、このウィザードでパスワードの文字列が表示されることはありません。ただし、必要な場合は、パスワード変更ウィザードが完了した後でパスワードの文字列を確認することができます（管理者が許可している場合）。

注：パスワード変更ウィザードが自動的に生成するパスワードでは、任意の文字、数字、および記号などが組み合わされるため、パスワードのセキュリティレベルを高めることができます。パスワードの自動作成機能では、ユーザーがパスワードを作成したり管理したりする必要がないため、この自動作成機能を使用することをお勧めします。

- パスワードの手動作成

  このオプションを選択して［次へ］をクリックすると、新しいパスワードをユーザーが自分で作成できます。この方法でパスワードを作成する場合、パスワードの文字数や数字を使用するかどうかなど、組織で定められているパスワードポリシーに準拠する必要があります。

パスワード変更の確認待ち

パスワードの変更処理が成功したかどうかを検出している間、パスワード変更ウィザードの［待機中］ページが開きます。

パスワード変更の結果に関するメッセージがアプリケーション側から表示されても［待機中］ページが閉じない場合は、［スキップ］をクリックして［パスワード変更の確認］ページに進みます。

パスワード変更の確認

管理者の設定によっては、パスワード変更ウィザードで新しいパスワードを作成した後で［パスワード変更の確認］ページが開きます。このページでは、パスワードの変更が成功したかどうか（新しいパスワードがアプリケーションによって受け入れられたかどうか）を指定します。次の 3 つのオプションから選択します。

はい:

処理に成功したことを示すメッセージが表示されたり、エラーメッセージが表示されなかったりした場合は、パスワードが正しく変更されています。

［はい］、［次へ］の順にクリックして、パスワードの変更が正しく完了したことをパスワード変更ウィザードに知らせます。これにより、パスワード変更ウィザードの処理が終了します。

いいえ:

パスワードの変更が失敗したことを示すメッセージが表示された場合は、パスワードが変更されていません。

［いいえ］、［次へ］の順にクリックして、新しいパスワードがアプリケーションに受け入れられなかったことをパスワード変更ウィザードに知らせます。これにより、パスワードが変更されないまま、パスワード変更ウィザードの処理が終了します。

わからない:

[わからない] を選択して [次へ] をクリックすると、パスワードの変更が成功したかどうかを確認するための説明が表示されます。

自分でパスワードを作成した場合は、Single Sign-On を一時停止し、新しいパスワードを手入力してアプリケーションにログオンできるかどうかを確認することもできます。

注: パスワード変更ウィザードのウィンドウを移動して、パスワードの変更に関するメッセージが表示されていないかどうかを確認してください。

未変更パスワードの確認

パスワード変更ウィザードでパスワード変更処理の失敗が検出された場合、またはユーザーが [パスワード変更の確認] ページで [いいえ] を選択した場合は、[パスワードは変更されていません] ページが開きます。

[パスワードは変更されていません] ページでは、次の 2 つのオプションを選択できます。

- 別のパスワードを作成する:

  アプリケーションのパスワード変更用の画面がまだ開いている場合は、このオプションを選択して新しいパスワードを再指定します。パスワード変更用の画面が閉じてからこのオプションを選択して新しいパスワードを再指定すると、アプリケーションに設定されているパスワードと Single Sign-On に登録されているパスワードに相違が生じる場合があります。

  [別のパスワードを作成する] を選択して [次へ] をクリックすると、新しいパスワードを再指定できます。管理者の設定により、パスワード変更ウィザードで次のいずれかの処理が実行されます。

  - [パスワードの作成方法を選択してください。] ページが開きます。パスワードを自動生成するか、ユーザーが自分で作成するかを選択できます。
  - [自分でパスワードを作成する] ページが開きます。
  - Single Sign-On によりパスワードが自動生成され、アプリケーションに送信されます。パスワード変更ウィザードでパスワードの変更が成功したことを確認します。

- このままウィザードを終了する:

  パスワードを変更せずにウィザードを終了します。後で必要に応じてパスワード変更ウィザードを起動して、パスワードの変更を再度試行できます。

パスワード変更に失敗した場合のウィザードの終了

パスワードの変更処理に失敗したことが検出された場合、またはユーザーが [パスワード変更の確認] ページで [いいえ]、[次へ] の順にクリックした場合、[パスワードは変更されていません] ページが開きます。

パスワード変更ウィザードでパスワードの変更に失敗した場合は、次の方法でパスワードを変更できます。

- ［パスワードは変更されていません］ページで［完了］をクリックしてウィザードを終了した後で、ウィザードを再度起動してパスワードの変更を試みます。
- アプリケーションのパスワードおよび Single Sign-On に登録済みのパスワードを手作業で変更します。
- ヘルプデスクに連絡します。

パスワード変更に成功した場合のウィザードの終了

パスワード変更ウィザードでパスワード変更処理の成功が検出された場合、またはユーザーが［パスワード変更の確認］ページで［はい］を選択した場合は、［パスワード変更の完了］ページが開きます。

これで、新しいパスワードがアプリケーションに設定され、Single Sign-On に登録されます。

新しいパスワードがアプリケーションに受け入れられたかどうかの確認

パスワード変更ウィザードの［パスワード変更の確認］ページで［わからない］を選択して［次へ］をクリックすると、パスワードの変更が成功したかどうかを確認するための説明が表示されます。

Single Sign-On を一時停止し、新しいパスワードを手入力してアプリケーションにログオンできるかどうかを確認することもできます。

このページで［次へ］をクリックすると、［パスワードの作成方法を選択してください。］ページが再度開きます。

パスワードの手動作成

パスワード変更ウィザードの［パスワードの作成方法を選択してください。］ページで［自分でパスワードを作成する］を選択すると、［自分でパスワードを作成する］ページが開きます。管理者がユーザーによるパスワードの作成を禁止している場合、このページは開きません。

新しいパスワードを正しく指定するために、［新しいパスワード］ボックスと［パスワードの確認入力］ボックスに同じパスワードを入力します。これらのボックスに入力したパスワードが一致しないと、パスワードが同一でないことを示すメッセージが表示されます。パスワードが一致すると、［次へ］をクリックできるようになります。

パスワード変更ウィザードで作成する新しいパスワードは、管理者が定義したパスワードポリシーに準拠している必要があります。たとえば、管理者は次のようなパスワードポリシーを定義できます。

- 過去に使用したことのあるパスワードを新しいパスワードとして設定できない。
- パスワードには数字とアルファベット文字を混在させる。
- パスワードに特定の文字を含めることを禁止する。
- パスワードの文字数を指定する。

Single Sign-On Plug-in の一時停止と再開

November 12, 2018

必要に応じて、Single Sign-On を一時的に無効にすることができます。たとえば、以下の状況で Single Sign-On を一時的に停止できます。

- アプリケーションや Web サイトにログオンしないでログオンページを使用する必要がある。
- ログオン情報の登録を確認するメッセージを表示させないでインターネットを使用する必要がある。

Single Sign-On を終了するのとは異なり、一時停止してもプログラムはそのまま動作を続けます。ただし、パスワードで保護されたアプリケーションや Web サイトには自動的にログオンされません。また、新しいログオン情報を登録するためのメッセージも表示されません。一時停止中の Single Sign-On は、必要に応じて再開させて、これらの機能を使用することができます。

Single Sign-On を一時停止するには

- Windows タスクバーの通知領域で Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［**Single Sign-On** の一時停止］の順に選択します。

Single Sign-On が一時停止中かどうかを確認するには

- Windows タスクバーの通知領域で Citrix Receiver のアイコンを右クリックし、［基本設定］を選択します。［Citrix Receiver - 基本設定］ダイアログボックスが開き、Citrix Single Sign-on Plug-in の状態が表示されます。

Single Sign-On を再開するには

- Windows タスクバーの通知領域で Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［**Single Sign-On** の再開］の順に選択します。

パスワード共有グループでのプログラムのグループ化

November 12, 2018

Single Sign-On の管理者が、パスワード共有グループを設定している場合があります。パスワード共有グループでは、同じパスワードを使用する複数のプログラムをグループ化して管理できます。これにより、ユーザーはそのグループに属するすべてのプログラムのパスワードを一括して変更できます。

たとえば、管理者がメール、経理、ワードプロセッサ、データ入力、および人事管理用のプログラムを含む 1 つのパスワード共有グループを定義した場合、ユーザーがメールプログラム用のパスワードを変更すると、同じグループに属するすべてのプログラムのパスワードが更新されます。

複数のアカウントを使い分ける必要があるプログラムがパスワード共有グループに含まれている場合は、そのプログラムをパスワード共有グループから除外することで、各アカウント用のパスワードを個別に管理できるようになりま

す。パスワード共有グループからプログラムを除外すると、ほかのプログラムでパスワードを変更しても、そのプログラムのパスワードは更新されません。

パスワード共有グループのパスワードを変更するには

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［編集］をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   パスワード共有グループに属するアプリケーションでは、［このパスワード共有グループのパスワードを変更する］リンクが表示されます。
3. ［このパスワード共有グループのパスワードを変更する］をクリックして、ウィザードの指示に従ってパスワードを変更します。

パスワード共有グループからプログラムを除外するには

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［編集］をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   パスワード共有グループに属するアプリケーションでは、［このアプリケーションをパスワード共有グループから除外する］リンクが表示されます。
3. ［このアプリケーションをパスワード共有グループから除外する］をクリックして、ウィザードの指示に従って操作します。

ログオン情報の登録

June 24, 2019

ログオンが必要なアプリケーションや Web サイトをユーザーが開くと、シングルサインオンがそれを検出して、登録済みのログオン情報を使って自動的にログオンします。ログオン情報（ユーザー名、パスワードなど）が登録されている場合は、シングルサインオンにより自動的にログオンされます。

シングルサインオンは、ユーザーが起動したアプリケーションや Web サイトからのログオン要求を検出し、

- ログオン情報がまだ登録されていない場合はここで登録するかどうかを確認するメッセージを表示します。
- シングルサインオンがログオン要求を検出しない場合は、ユーザーがログオン情報を手作業で登録できます。

シングルサインオンでは、次の種類のアプリケーションのログオン情報を登録できます。

- **Windows** アプリケーション：一般的に［スタート］メニューやデスクトップから起動する、Lotus Notes などのアプリケーションです。
- **Web** アプリケーションまたは **Web** サイト：Web ブラウザー上で表示したり操作したりするアプリケーションやサイトです。インターネットストアや Web ベースの教育アプリケーションなどがあります。

  重要：シングルサインオンでサポートされる Web ブラウザーは、Microsoft Internet Explorer（32 ビット版）のみです。
- ターミナルエミュレーターベースのアプリケーション：通常メインフレームコンピューターでホストされる、テキストベースのアプリケーションです。この種類のアプリケーションでは、一般的に深い緑色などの暗い色の背景に明るい同系色の文字が表示されます。

注：ログオン時に必要な情報の種類は、アプリケーションによって異なる場合があります。ほとんどの場合、ユーザー名またはユーザー ID と、パスワードの入力が必要になります。必要なログオン情報が不明な場合は、ヘルプデスクに連絡してください。

ログオン情報を自動的に登録するには

1. パスワードで保護されたアプリケーションや Web サイトを開きます。ログオン用のダイアログボックスまたは Web ページが開きます。
2. ログオン情報を登録するかどうかを確認するダイアログボックスで、［保存］をクリックします。
3. Web サイトまたは Web アプリケーションの場合は、ログオン情報用のフィールドおよび送信用のボタンの枠が強調表示されます。これらのフィールドやボタンが正しく強調表示されているかどうかを確認するダイアログボックスで、［はい］をクリックします。
4. ［新規ログオン］ダイアログボックスでログオン情報を入力し、［完了］をクリックします。［新規ログオン］ダイアログボックスが閉じ、ログオン情報がシングルサインオンに登録され、アプリケーションにログオンされます。

ログオン情報を手作業で登録するには

1. パスワードで保護されたアプリケーションや Web サイトを開きます。ログオン用のダイアログボックスまたは Web ページが開きます。
2. ログオン情報を登録するかどうかを確認するダイアログボックスが自動的に開かない場合は、ログオン情報を手作業でシングルサインオンに登録します。これを行うには、Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの送信］ の順に選択します。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。
3. ログオン情報を登録するかどうかを確認するダイアログボックスで、［保存］をクリックします。
4. Web サイトまたは Web アプリケーションの場合は、ログオン情報用のフィールドおよび送信用のボタンの枠が強調表示されます。これらのフィールドやボタンが正しく強調表示されているかどうかを確認するダイアログボックスで、［はい］をクリックします。
5. ［新規ログオン］ダイアログボックスでログオン情報を入力し、［完了］をクリックします。［新規ログオン］ダイアログボックスが閉じ、ログオン情報がシングルサインオンに登録され、アプリケーションにログオンされます。

同じアプリケーションのログオン情報を複数登録する

1 つのアプリケーションや Web サイトで複数のアカウントを使用する場合があります。次に例を示します：

- 特定の用途の電子メールアカウントと通常の電子メールアカウントを使い分けている。
- 2 つのプロジェクトで物品を購入するために、取引先の Web サイトにプロジェクトごとの個別アカウントがある。

管理者によりシングルサインオンの複数アカウント機能が有効に設定されている場合、同じアプリケーションや Web サイトに対して複数のアカウント情報を登録できます。複数のアカウント情報を登録すると、シングルサインオンではログオン情報の選択機能を使って、使用するログオン情報を選択できるようになります。

シングルサインオンに登録済みのアプリケーションや **Web** サイトにログオン情報をさらに追加するには

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、ログオンアカウントを追加するアプリケーションまたは Web サイトを選択します。

3. ［コピー］ をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   選択したアプリケーションまたは Web サイトの複製が一覧に追加されます。

4. 追加された項目を選択して、［編集］をクリックします。ダイアログボックスが開き、コピーされたログオン情報が表示されます。
5. 必要に応じて、ログオン情報を変更します。
6. ［アプリケーション名］ボックスで、複製元のアプリケーションと区別しやすい名前を設定します。
7. ［**OK**］ をクリックします。

複数のログオン情報を登録しているアプリケーションへのログオン

同じアプリケーションまたは Web サイトで複数のログオン情報を登録している場合は、シングルサインオンのログオン情報の選択機能で、使用するログオン情報を選択します。

ログオン情報を複数登録したアプリケーションまたは Web サイトにログオンするには

1. アプリケーションまたは Web サイトのログオン画面を開きます。［ログオン情報の選択］ダイアログボックスが開きます。
2. ［ログオン情報の選択］ダイアログボックスで、使用するログオンアカウントを選択し、［**OK**］をクリックします。［ログオン情報の選択］ダイアログボックスが閉じて、アプリケーションまたは Web サイトにログオンされます。

セキュリティの質問に対する回答の登録

November 12, 2018

1. ［セキュリティ用の質問の登録ウィザードへようこそ］ページで［次へ］をクリックして、最初のセキュリティ用の質問を表示します。
2. ［回答］ボックスにセキュリティ用の質問の回答を入力します。管理者の設定によっては、回答として入力した文字列が画面に表示されません。この場合は、［回答の確認入力］ボックスに同じ回答を入力する必要があります。

   注： 回答として入力する語句の大文字と小文字は区別されます。回答の登録時に大文字を使用した場合は、同一性の検証時に回答を入力するときにも大文字を使用する必要があります。たとえば、恩師の名前などで

「Ms. Takeda」という回答を登録した場合は、同一性の検証時にピリオドを含め大文字/小文字を正確に入力する必要があります。

3. ［次へ］ をクリックします。セキュリティ用の質問が複数ある場合は、次の質問が表示されます。
4. ［回答の登録］ページが開くまで、手順 2. と手順 3. を繰り返します。
5. ［回答の登録］ページで［次へ］をクリックします。
6. ［セキュリティ用の質問の登録の完了］ページで［完了］をクリックします。入力したすべての回答が Single Sign-On に登録されます。

ログオン情報の削除

June 24, 2019

ここでは、シングルサインオンで保存されているパスワードを削除する方法について説明します。Receiver でも、ログオン時に［パスワードを保存する］チェックボックスをオンにすることでパスワードを保存できます。Receiver に保存されたパスワードを削除するには、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［パスワードの削除］を選択します。

必要に応じて、シングルサインオンからログオン情報を削除できます。次に例を示します:

- アプリケーションまたは Web サイトに対して複数登録しているアカウントすべてが不要になった。
- 使用しないアプリケーションまたは Web サイトのログオン情報を登録している。

重要: 使用しているログオン情報を削除すると、そのアプリケーションまたは Web サイトに自動的にログオンできなくなります。次にそのアプリケーションを起動するとき、ログオン情報を登録するかどうかを確認するメッセージが表示されます。

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［削除］をクリックします。

   注: 管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   選択したアプリケーションのログオン情報を削除するかどうかを確認するダイアログボックスが開きます。
3. ［はい］ をクリックします。シングルサインオンからログオン情報が削除され、［パスワード管理］ダイアログボックスの一覧に表示されなくなります。

注：ログオン情報を削除したアプリケーションまたは Web サイトに再度アクセスすると、ログオン情報を登録するかどうかを確認するメッセージが表示されます。

パスワード文字列の表示

November 12, 2018

管理者により許可されている場合、Single Sign-On に登録したパスワードの内容をユーザーが確認することができます。

注：管理者の設定によっては、一部のログオン情報のパスワード文字列を表示できない場合があります。

警告：パスワードを表示するときは、他人に見られないように注意してください。パスワードを厳重に管理することは、個人のアカウントだけでなく、組織全体の情報を保護するために不可欠です。

1. Windows タスクバーのシステムトレイで Citrix Receiver のアイコンを右クリックし、［パスワード］**>**［パスワードの管理］の順に選択します。
2. ［パスワード管理］ダイアログボックスで、目的のアプリケーションまたは Web サイトを選択して［文字列の表示］をクリックします。

   注：管理者の設定によっては、ここでユーザーの同一性検証が必要になる場合があります。同一性検証用のダイアログボックスが開いた場合は、Windows にログオンするときに使用したユーザー名とパスワードを入力します。スマートカードなど、ユーザー名/パスワード以外の認証方法で Windows にログオンした場合は、その方法で同一性を検証する必要があります。

   ダイアログボックスが開き、選択したアプリケーションのパスワードが表示されます。
3. ［**OK**］をクリックして、アプリケーションのパスワードダイアログボックスを閉じます。

Single Sign-On の初回起動時設定

August 7, 2018

管理者の設定により、ユーザーがコンピューターにログオンしたとき、またはパスワードで保護されたアプリケーションや Web サイトを初めて開いたときに、Single Sign-On が自動的に起動します。

管理者の設定によっては、Single Sign-On の初回起動時に情報を入力する必要があり、このときにセキュリティ用の質問（「学生時代の恩師の名前は何ですか?」など）に対する回答が求められる場合があります。この回答は、後で本人の確認（同一性検証）が必要になったときに使用されます。

インターネットに接続していないときのアプリケーションの使用

November 12, 2018

初めてアプリケーションを開くときは、インターネットに接続している必要があります。Citrix Receiver for Windows はデバイスにいくつかのアプリケーションをインストールします。インターネットに接続していないときは、これらのアプリケーションを実行できます。このインストールには数分間かかる可能性があります。

注：オフラインアクセス機能は、必ずしもすべてのユーザーまたはすべてのアプリケーションで使用できるわけではありません。インターネットへの接続を求められる前にどのぐらいの期間オフラインでアプリケーションを使用できるかは、管理者が決定します。

デスクトップおよびアプリケーションの一覧

August 7, 2018

アクセス可能な仮想デスクトップおよびアプリケーションの一覧は、各種デバイス上にインストールされた Citrix Receiver for Windows のホームページに表示されます。

ホームページを開くには、Citrix Receiver for Windows アイコンを右クリックして ［開く］ を選択します。

アプリケーションやデスクトップは、以下の場所にも表示されます。

- Windows のスタートメニュー：Citrix Receiver for Windows でアクセスするアプリケーションやデスクトップが、Windows のスタートメニューの［(すべての) プログラム］の下のフォルダー内にも追加されます。
- デスクトップ：管理者の設定によっては、アプリケーションのショートカットがコンピューターのデスクトップ上に追加されます。ショートカットがデスクトップ上のフォルダー内に追加されることもあります。
- Web ページ：管理者により、アプリケーションやデスクトップにアクセスできる Web ページの URL が提供される場合もあります。この場合、Internet Explorer、Firefox、または Google Chrome でその URL にアクセスします。

セッションの管理

November 12, 2018

Citrix コネクションセンターには、Receiver から確立されたすべてのアクティブな接続が表示されます。

コネクションセンターを開くには、以下の手順に従います。

- Receiver アイコンを右クリックして［コネクションセンター］を選択します。

異常停止した仮想アプリケーションを終了するには

コネクションセンターでアプリケーションを選択して、［終了］をクリックします。

すべてのアクティブな仮想アプリケーションを一度に閉じるには

コネクションセンターでアプリケーションのホストサーバーを選択して、［ログオフ］をクリックします。

デスクトップとアプリケーションの表示モードを変更するには

シームレスウィンドウモードと全画面モードを切り替えることができます。

- シームレスウィンドウモード：デスクトップやアプリケーションは、セッションウィンドウ内に表示されません。ユーザーデバイス上にインストールされているローカルのデスクトップやアプリケーションと同じように、サイズ変更が可能な個別のウィンドウで表示されます。この場合、仮想アプリケーションとローカルのデスクトップを簡単に切り替えることができます。
- 全画面モード：アプリケーションは、デスクトップウィンドウに表示されます。

全画面モードに切り替えるには、コネクションセンターでホストサーバーを選択し、［全画面］をクリックして［**OK**］をクリックします。

シームレスウィンドウモードに戻るには、Shift+F2 キーを押します。

アプリケーションの更新または削除

August 7, 2018

Citrix Receiver for Windows を終了するかログオフすると、アプリは切断されます。ドロップダウンメニューから［アプリケーションを更新］ を選択するか、アプリアイコンをクリックしてセッションに再接続します。

セルフサービスモードが無効で、［スタート］メニューまたはデスクトップショートカットを介して排他的にアプリにアクセスしている場合にアプリを更新するには、通知領域にある Citrix Receiver for Windows のアイコンを右クリックして ［更新］ を選択します。

［アプリケーションを更新］ オプションを選択して StoreFront から最新の公開アプリおよびデスクトップを取得します。

アプリケーションビューからアプリケーションを削除するには、アプリケーションを右クリックして ［削除］ をクリックします。

Citrix Receiver for Windows Desktop Lock

June 24, 2019

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

Citrix Receiver for Windows Desktop は、SSON（Single Sign-On：シングルサインオン）が有効化でありストアが構成済みのドメイン参加マシンで機能します。また、SSON が有効ではない非ドメイン参加のマシンでも使用できます。Program Neighborhood エージェントサイトはサポートしません。以前のバージョンの Desktop Lock は、Citrix Receiver for Windows 4.2 以降へアップグレードするとサポートされません。

Citrix Receiver for Windows を、/includeSSON フラグを使用してインストールする必要があります。adm/admx ファイルまたはコマンドレットオプションのいずれかを使って、ストアおよびシングルサインオンを構成する必要があります。詳しくは、コマンドラインを使った Citrix Receiver のインストールと構成を参照してください。

次に、管理者としてシトリックスのダウンロードページにある CitrixReceiverDesktopLock.MSI を使って Citrix Receiver for Windows Desktop Lock をインストールします。

Citrix Receiver Desktop Lock のシステム要件

- Microsoft Visual C++ 2005 Service Pack 1 再頒布可能パッケージ。詳しくは、Microsoft ダウンロードページを参照してください。
- Windows 7 (Embedded Edition を含む)、Windows 7 Thin PC、Windows 8、Windows 8.1、Windows 10（Anniversary Update を含む）でサポートされます。
- ネイティブプロトコルのみを介して StoreFront に接続します。
- ドメイン参加および非ドメイン参加のエンドポイント。
- ユーザーデバイスをローカルエリアネットワーク（LAN）またはワイドエリアネットワーク（WAN）に接続する必要があります。

ローカルアプリアクセス

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

Citrix Receiver for Windows Desktop Lock の使用

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

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

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

1. ローカルの管理者アカウントを使用してログオンします。
2. コマンドプロンプトで次のコマンド（インストールメディアの Citrix Receiver and Plug-ins > Windows > Citrix Receiver for Windows フォルダーにあります）を実行します。

   次に例を示します:

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

   コマンドについて詳しくは、「コマンドラインパラメーターを使用した Receiver for Windows の構成とインストール」の Citrix Receiver for Windows のインストールに関する説明を参照してください。
3. インストールメディアの同じフォルダーにある CitrixReceiverDesktopLock.MSI をダブルクリックします。Desktop Lock ウィザードが開きます。画面の指示に従って操作します。

4. インストールが完了したら、ユーザーデバイスを再起動します。デスクトップへのアクセスが許可されていて、ドメインユーザーとしてログオンすると、Receiver Desktop Lock でデスクトップが表示されます。

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

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

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

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

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

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

- receiver.admx（または receiver.adml）と receiver_usb.admx（.adml）ファイルがグループポリシーにロードされていることを確認します（ポリシーは［コンピューターの構成］または［ユーザーの構成］>［管理用テンプレート］>［従来の管理用テンプレート（ADMX)］>［Citrix コンポーネント］の順に展開すると表示されます)。これらの.admx ファイルは、%Program Files%\Citrix\ICA Client\Configuration にインストールされています。
- USB 基本設定 - ユーザーが USB デバイスを接続すると、そのデバイスは自動的に仮想デスクトップで使用可能になります。このとき、ユーザーが何らかの操作を行う必要はありません。USB ドライブの制御と表示は、仮想デスクトップにより処理されます。
  - USB ポリシー規則を有効にします。
  - ［Citrix Receiver］>［クライアントデバイスをリモート処理します］>［一般的な USB のリモート処理］の順に選択して、［既存の USB デバイス］と［新しい USB デバイス］ポリシーを有効にして構成します。
- ドライブマッピング - ［Citrix Receiver］>［クライアントデバイスをリモート処理します］の順に選択して、［クライアントドライブマッピング］ポリシーを有効にして構成します。
- マイク - ［Citrix Receiver］>［クライアントデバイスをリモート処理します］の順に選択して、［クライアント側マイク］ポリシーを有効にして構成します。

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

1. StoreFront を構成します。
   a) Citrix XML Service の DNS アドレス解決を有効にして、Kerberos 認証を使用できるように構成します。

b) StoreFront サイトの HTTPS アクセスを構成して、ドメインの証明機関による署名付きのサーバー証明書を作成し、デフォルトの Web サイトに HTTPS バインドを追加します。
c) ［スマートカードパススルー認証］が有効になっていることを確認します（デフォルトで有効になっています）。
d) ［Kerberos］を有効にします。
e) ［Kerberos］および［スマートカードパススルー認証］を有効にします。
f) IIS の Default Web Site で［匿名アクセス］を有効にして、［統合 Windows 認証］を使用します。
g) IIS の Default Web Site の SSL 設定で［SSL が必要］チェックボックスがオフで、［クライアント証明書］で［無視］が選択されていることを確認します。

2. グループポリシー管理コンソールを使用して、ユーザーデバイスでローカルコンピューターのポリシーを構成します。
a) %Program Files%\Citrix\ICA Client\Configuration から Receiver.admx テンプレートをインポートします。
b) ［管理用テンプレート］>［従来の管理用テンプレート（ADMX）］>［Citrix コンポーネント］>［Citrix Receiver］>［ユーザー認証］の順に展開します。
c) ［スマートカード認証］を有効にします。
d) ［ローカルユーザー名とパスワード］を有効にします。

3. Citrix Receiver for Windows Desktop Lock をインストールする前に、ユーザーデバイスを構成します。
a) Windows Internet Explorer の信頼済みサイトの一覧に、Delivery Controller の URL を追加します。
b) Windows Internet Explorer の信頼済みサイトの一覧に、最初のデリバリーグループの URL を「desktop://」形式で追加します。デリバリーグループ名 >
c) 信頼済みサイトに対する Internet Explorer の自動ログオン機能を有効にします。

Citrix Receiver for Windows がユーザーデバイスにインストールされている場合、スマートカード取り出し時の動作に競合が生じないようにポリシーが適用されます。たとえば、Windows のスマートカードの取り出しポリシーがデスクトップで強制ログオフに設定されている場合、Windows のスマートカードの取り出しポリシーが設定されているかどうかにかかわらず、ユーザーはユーザーデバイスからもログオフする必要があります。これにより、ユーザーデバイスの整合性が維持されます。これは、Citrix Receiver for Windows Desktop Lock があるユーザーデバイスにのみ適用されます。

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

以下のコンポーネントを両方ともアンインストールする必要があります。

1. Citrix Receiver for Windows Desktop Lock のインストールと構成に使用したローカル管理者アカウントでログオンします。
2. プログラムの削除や変更を行うための Windows 機能（コントロールパネルの［プログラムと機能］など）を開き、以下の操作を行います：
   - Citrix Receiver for Windows Desktop Lock をアンインストールします。
   - Citrix Receiver for Windows をアンインストールします。

リモートセッションでの **Windows** ショートカットキーの実行

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

Windows

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

Windows 8

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

Windows 8 のアプリ

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

デスクトップ

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

そのほか

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

SDK および API

June 24, 2019

Citrix 仮想チャネル SDK

Citrix 仮想チャネルソフトウェア開発キット（SDK）は、ICA プロトコルを使用する追加の仮想チャネルのための、サーバー側アプリケーションやクライアント側ドライバーの作成をサポートします。サーバー側仮想チャネルアプリケーションは、XenApp または XenDesktop サーバー上にあります。このバージョンの SDK は、Receiver for Windows 用の新しい仮想チャネルの作成をサポートします。他のクライアントプラットフォーム用の仮想ドライバーの作成については、Citrix テクニカルサポートにお問い合わせください。

仮想チャネル SDK には、以下のものが用意されています。

- Citrix Server API SDK（WFAPI SDK）の仮想チャネル機能とともに使用して新しい仮想チャネルを作成する、Citrix Virtual Driver Application Programming Interface（VDAPI）。VDAPI によって提供される仮想チャネルサポートは、独自の仮想チャネルを容易に作成できるように設計されています。
- 視覚的要素を強化し、ICA と統合されたサードパーティアプリケーションをサポートする Windows Monitoring API。
- プログラミングテクニックの実例となる仮想チャネルサンプルプログラムの、実際に機能するソースコード。
- 仮想チャネル SDK では、WFAPI SDK で仮想チャネルのサーバー側を作成する必要があります。

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

Fast Connect 3 Credential Insertion API

Fast Connect 3 Credential Insertion API は、Citrix Receiver for Windows 4.2 以降のシングルサインオン（SSON）機能に対してユーザーの資格情報を提供するインターフェイスです。この API を使用すると、Citrix パート

ナーは、StoreFront または Web Interface を使用して仮想アプリケーションまたはデスクトップにユーザーをログオンさせ、その後でそれらのセッションからユーザーを切断する、認証や SSO にかかわる製品を提供できます。

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

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States