セルフサービスパスワードリセット 1.1

Dec 08, 2016

Self-Service Password Resetについて

Dec 08, 2016

Self-Service Password Resetにより、エンドユーザーは自身のユーザーアカウントをこれまで以上に制御できるようになります。 Self-Service Password Resetが構成されると、エンドユーザーは、システムへのログオンで問題がある場合にいくつかのセキュリティ用の質問に答えることによって、自身のアカウントのロックを解除するか、パスワードをリセットして新しいパスワードを設定することができます。

パスワードのリセットは、本質的にセキュリティ上の注意が必要なプロセスです。 「安全な構成」を参照して、展開が適切に構成されているか確認することをお勧めします。

バージョン1.1の新機能

このバージョンには、次の強化機能があります。

- ブラックリスト設定のサポート - IT管理者はユーザーおよびグループをブラックリストに追加できます。 ブラックリストのユーザーおよびグループは、セルフサービスパスワードリセットの機能を使用することはできません。
- 簡体中国語のサポート - 英語に加えて、日本語、フランス語、スペイン語、簡体中国をセキュリティ用の質問に使用できるようになりました。

Self-Service Password Resetには次の3つのコンポーネントが含まれます。

- Self-Service Password Reset構成コンソール
- セルフサービスパスワードリセットサービス
- StoreFrontへのセキュリティ用の質問の登録

Self-Service Password Reset構成コンソール

- **［サービス設定］**：中央ストアのアドレス、データプロキシアカウント、Self-Service Password Resetアカウントなど、Self-Service Password Resetサービスの設定を行います。
  - ［中央ストアのアドレス］：セルフサービスパスワードリセットの強力なデータを保管するネットワーク共有の場所。
  - ［データプロキシアカウント］：中央ストアとの通信に使用します。 アカウントには、中央ストアへの読み書き用のアクセス権が必要です。
  - ［Self-Service Password Resetアカウント］：アカウントのロック解除およびパスワードのリセットに使用します。
- **［ユーザー設定］**：セルフサービスパスワードリセット機能を使用可能なユーザー/グループ/OU（Organizational Unit：組織単位）の設定を行い、ライセンスサーバーのアドレスとデフォルトのサービスアドレスを指定します。
  - ［ユーザー設定の名前］：セルフサービスパスワードリセットサービスの対象ユーザーグループ（Active Directoryのユーザー/グループ/OUを含む）を定義します。
  - ［ライセンスサーバーのアドレス］：セルフサービスパスワードリセットは、XenAppまたはXenDesktop Platinum Editionでのみ使用できます。 ライセンスサーバーのバージョンは、11.13.1以上である必要があります。
  - **ロック解除**機能と**リセット**機能をオンまたはオフにします。
  - ［デフォルトのサービスアドレス］：セルフサービスパスワードリセットサービスのURLを指定します。
- **［ユーザー識別処理］**：登録およびパスワードのロック解除とリセットに使用する質問リストを設定します。
  - 質問またはグループを、質問リストを生成する質問ストアに追加します。
  - 質問ストアから、登録に使用する質問リストを選択します。
  - セキュリティ用の質問またはグループをエクスポート/インポートします。

セルフサービスパスワードリセットサービス

Self-Service Password ResetサービスはWebサーバー上で実行され、このサービスにより、ユーザーは自分のWindowsパスワードのリセットおよびWindowsアカウントのロック解除を実行できるようになります。 エンドユーザーのリクエストは、StoreFrontを経由してこのサービスに送信されます。

StoreFrontへのセキュリティ用の質問の登録

StoreFrontを使用すると、セキュリティ用の質問に対する回答の登録をユーザーに許可できます。 ユーザーは、登録されると、ドメインパスワードのリセットおよびドメインアカウントのロック解除を実行できるようになります。 詳しくは、StoreFrontのドキュメントの「セルフサービスパスワードリセット」を参照してください。

既知の問題

Dec 08, 2016

Version 1.1

このバージョンの既知の問題は次のとおりです。

- ユーザー設定ウィザードでユーザーグループを追加しようとすると失敗し、ユーザーグループがブラックリストに追加されているというメッセージが表示されることがあります。 これは、誤ったメッセージです。 試行が失敗したのは、このグループが既に追加済みであるためです。

  [#665520]

- 設定ウィザードで削除処理を完了しウィザードを閉じるまで、ウィザードから削除したユーザーやユーザーグループを追加することはできません。 この手順を経ていない場合、ユーザーまたはグループがブラックリストに追加されているという不正確なエラーメッセージが表示されます。 この問題を解決するには、削除処理を完了しウィザードを閉じてから、ウィザードを再度開いてユーザーやグループを追加し直します。

  [#665352]

- セルフサービスパスワードリセットでバージョン1.0コンソールが開いている間、バージョン1.1にアップグレードすると、対応していない、バージョン1.0の開いているコンソールを使用できません。

  [#664390]

- .Net Framework 4.5のみがインストールされているWindows Server 2012でのアップグレード、および.Net Framework 4.6のみがインストールされているWindows Server 2016でのアップグレードが失敗することがあります。 これが失敗するのは、Windows Server 2012およびWindows Server 2016のインプレースアップグレードが.Net Framework 3.5に依存しているためです。 この問題を解決するには、.NET Framework 3.5をインストールしてからアップグレードします。

  [DNA-22761]

Version 1.0

このバージョンの既知の問題は次のとおりです。

- セルフサービスパスワードリセットコンソールを開いた後、タスクバーをピン留めできないことがあります。

  [#646300]

  回避策： **[スタート]** メニューのショートカットからタスクバーをコンソールにピン留めしてください。

- これは、Windows 2016の既知の問題であるため、Windows 2016でセルフサービスパスワードリセットコンソールを検索することはできません。

  [#648939]

  回避策： **[スタート]** メニューを使用して、セルフサービスパスワードリセットを検索してください。

- デフォルトのドメインポリシーでパスワードポリシーのパスワードの変更禁止期間がデフォルト（1日）に設定され、ユーザーがパスワードをリセットしようとして失敗する場合（パスワードの複雑さの要件を満たしていないなど）、［パスワードのリセット］ウィザードを終了しても、24時間以内に再度パスワードをリセットすることはできません。

[#653221]

- Citrix Receiver for Macを使用している場合、StoreFrontへの最初のログオンで、登録用のタスクボタンが表示されます。StoreFrontからログオフして、再度ログオンすると、このタスクボタンは表示されません。

  [#657263]

  回避方法：
  1. StoreFrontストアの右上にあるユーザー名をクリックします。
  2. ドロップダウンメニューで **[アプリの更新]** ボタンをクリックします。
  3. Citrix Receiver for Macを終了して再起動すると、タスクボタンが表示されます。

- Single Sign-onの［ユーザー識別処理］からセルフサービスパスワードリセットにセキュリティ用の質問を移行すると、 **[更新]** をクリックした後でも、セルフサービスパスワードリセットコンソールに質問が表示されないことがあります。

  [#657277]

  回避策：コンソールを終了して再起動します。

- 質問リストのセキュリティ用の質問にアンパサンド（**&**）が含まれている場合は、StoreFrontの登録中に表示されません。

  [#654913]

  回避策：セキュリティ用の質問に**&**を含めないようにしてください。

システム要件

Dec 08, 2016

> **Important**
>
> ドメインコントローラーへのSelf-Service Password Resetコンポーネントのインストールはサポートされません。 専用サーバーでセルフサービスパスワードリセットのコンポーネントをインストールします。

ここでは、Self-Service Password Reset環境に必要なハードウェアおよびソフトウェアの要件について説明します。 各コンピューターが、インストールされているオペレーティングシステムの最小ハードウェア要件を満たしていることを前提としています。

ソフトウェア

Self-Service Password Resetを使用するには、以下のシステムソフトウェアが必要です。

- **Windows 2016、Windows 2012 R2、Windows 2008 R2**（ローカルファイル共有と適切な追加ロックダウンには、Windows 2008 R2のみの使用をお勧めします。 詳しくは、「中央ストアの作成」を参照してください。） - セルフサービスパスワードリセットサーバーに必要です。
- **Microsoft Windows Installer 2.0以降** - すべてのコンポーネントに必要です。
- **Microsoft .NET Framework** - Self-Service Password Resetサーバーに必要です。
  - 4.6（Windows 2016）
  - 4.5.2（Windows 2012 R2）
  - 3.5.1（Windows 2008 R2）
- **インターネットインフォメーションサービス（Internet Information Services：IIS）** - Self-Service Password Resetサーバーに必要です。
  - IIS 10.0（Windows 2016）
  - IIS 8.5（Windows 2012 R2）
  - IIS 7.5（Windows 2008 R2）

Self-Service Password Resetサーバー

- Self-Service Password Resetコンポーネント - 中央ストア
- サポートされる環境 - SMBファイル共有
- ハードウェア要件 - ユーザーあたり30KBのディスク空き容量

ASP.NET 3.5/4.Xの要件

お使いのWindows Server上のNET Frameworkのバージョンに対応したASP.NETコンポーネント。

セキュリティおよびアカウントの要件

Self-Service Password Resetサービスをインストールする前に、このサービスに必要なアカウントとコンポーネントを用意します。 また、セルフサービスパスワードリセットサービスはセキュアなHTTP（HTTPS）を使用するため、StoreFrontとのTLS（Transport Layer Security）通信のサーバー認証証明書が必要です。

サーバー認証の要件：

セルフサービスパスワードリセットサービスをインストールする前に、CA（Certificate Authority：証明機関）からTLS通信のサーバー認証証明書を入手するか、利用可能な場合、内部PKI（Public Key Infrastructure：公開キー基盤）を入手します。

サービスモジュールに必要なアカウント：

注：どちらのアカウントにも有効期限がないことを確認してください。

Self-Service Password Resetサービスを実行するには、データの読み書き用に以下の種類のアカウントが必要です。

- データプロキシ用アカウント
- セルフサービス用アカウント

複数のモジュールで同じ種類のアカウントが必要な場合は、同じアカウントを複数のモジュールに使用したり、モジュールごとに専用のアカウントを指定したりできます。

- **データプロキシ用アカウント**

  中央ストアへの読み書き用のアクセス権を所有している。 詳しくは、 中央ストアの作成」を参照してください。

- **セルフサービス用アカウント**

  ユーザー設定で関連ユーザーのパスワードをロック解除およびリセットするための権限が設定されている必要があります。 詳しくは、「安全な構成」を参照してください。

StoreFront

- StoreFront 3.7
- StoreFront 3.8

Citrix Receiver

サポート対象：

- Citrix Receiver for Web
- Citrix Receiver for Windows
- Citrix Receiver for Linux
- Citrix Receiver for Mac（StoreFront 3.8が必要です）

サポート対象外：

- Citrix Receiver for Chrome
- モバイルデバイス（Receiver for Webを使用しない場合も含む）

NetScaler Gatewayの外部使用

サポートされていません

インストールと構成

Dec 08, 2016

この記事には、以下のセクションがあります。

インストールと構成のチェックリスト

インストールを始める前に、以下のリストに記載されている作業を行います。

✓	作業
	Self-Service Password Resetをインストールするコンピュータを決定し、インストールの用意をします。 「システム要件」を参照してください。
	Self-Service Password Resetサービスに必要なTLS証明書とアカウントをインストールします。 「システム要件」のセキュリティおよびアカウントの要件を参照してください。
	ライセンスサーバーをインストールします。ライセンスサーバーのドキュメントを参照してください。
	中央ストアを作成します。 「中央ストアの作成」を参照してください。
	Self-Service Password Resetをインストールします。 「Self-Service Password Resetのインストールと構成」を参照してください。
	コンソールを使用してSelf-Service Password Resetを構成します。 「Self-Service Password Resetのインストールと構成」を参照してください。
	StoreFrontでSelf-Service Password Resetを構成します。 「StoreFrontの構成」を参照してください。
	セルフサービスパスワードリセット構成が安全に、確実に構成されるようにします。 安全な構成」を参照してください。

Self-Service Password Resetサービスに必要なSSL証明書とアカウントをインストールします。「セキュリティおよびアカウントの要件」を参照してください。

Self-Service Password Resetサービスに必要なSSL証明書とアカウントをインストールします。「セキュリティおよびアカウントの要件」を参照してください。

StoreFrontでSelf-Service Password Resetを構成します。 「StoreFrontの構成」を参照してください。

インストールと構成の順序

セルフサービスパスワードリセットサービスをインストールするには、ログオンアカウントがドメインユーザーであり、サーバーのローカル管理者グループに属している必要があります。

Self-Service Password Resetのインストールは、次の順序で行うことをお勧めします。

1. ライセンスサーバーのバージョン11.13.1.2以上をインストールするか、このバージョン以上にアップグレードします。 ライセンスサーバーはhttps://www.citrix.com/downloads/licensing.htmlからダウンロードできます。
2. 中央ストアの作成」をクリックします。
3. Self-Service Password Resetをインストールします。
4. コンソールでSelf-Service Password Resetを構成します。
5. Self-Service Password Resetサーバーのアドレスを使用してStoreFrontを構成します。

中央ストアの作成

セキュリティ上の理由から、セルフサービスパスワードリセットサービスを実行しているマシンで直接中央ストアを作成することをお勧めします。 複数のセルフサービスパスワードリセットサーバーを展開する必要がある場合、セルフサービスパスワードリセットサーバーおよびリモートネットワーク共有をホストするサーバーの両方がSMB暗号化をサポートしているのであれば、リモートネットワーク共有で中央ストアをホストすることができます。

この機能は、Windows Server 2012 R2またはWindows Server 2016でのみ利用できます。そのため、中央ストアのリモートファイル共有を使用している時、Windows Server 2008 R2はサポートされません。

データプロキシ用アカウントの作成

データプロキシ用のアカウントとして通常使用する、ドメインユーザーを作成します。 ドメイン管理者グループまたはローカル管理者グループのユーザーを、データプロキシ用のアカウントとして設定しないようにします。

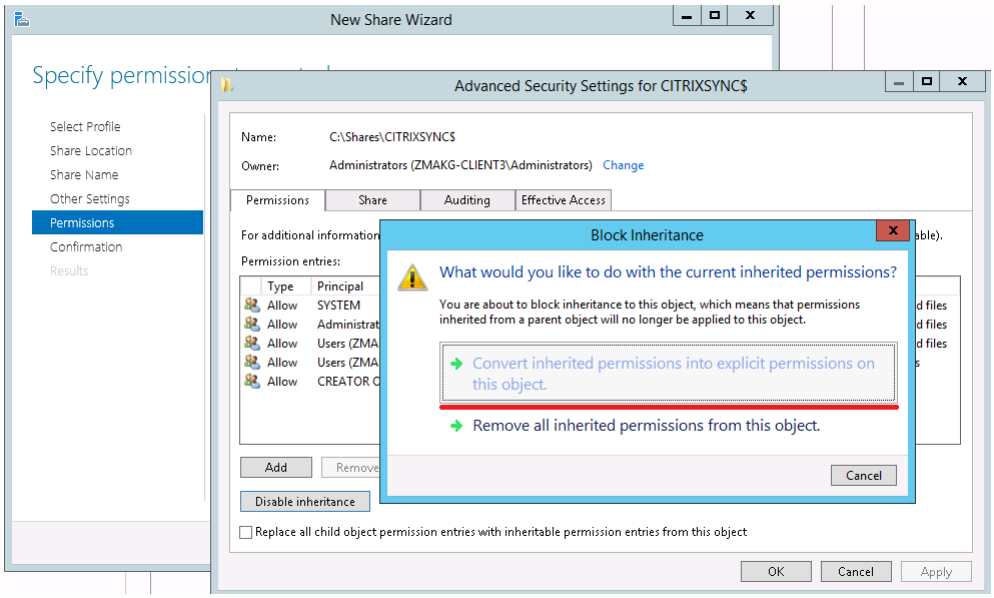
Windows Server 2012 R2またはWindows Server 2016用の中央ストアの作成

セルフサービスパスワードリセットサーバーおよび中央ストアの両方にWindows Server 2012 R2またはWindows Server 2016を使用する場合、ここで説明するように構成すると、リモートネットワーク共有を使用できます。 **[データアクセスの暗号化]** が選択され、「安全な構成」で説明された手順が確実に適用されるようにします。

1. **[新しい共有]** ウィザードを開始するには、サーバーマネージャーを開きます。 **[ファイルサービスおよびストレージサービス]** の詳細ページから、左ペインで **[共有]** を選択して、 **[タス**

ク] > [新しい共有] をクリックします。

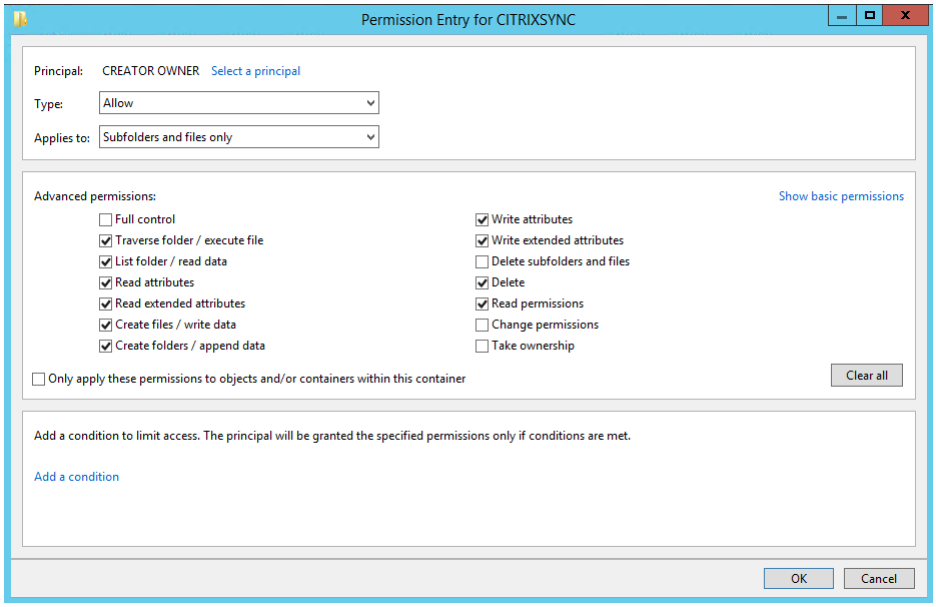
2. 左ペインで [プロファイルの選択] をクリックして [SMB共有 – 簡易] を選択し、 [次へ] をクリックします。
3. 左ペインで [共有の場所] をクリックします。 一覧から、新しい共有を作成するサーバーと新しい共有フォルダーを作成するボリュームを選択し、[次へ] をクリックします。
4. 左ペインで [共有名] をクリックし、新しい共有の名前（例 : **CITRIXSYNC$**）を入力して [次へ] をクリックします。
5. 左ペインで [他の設定] をクリックし、 [データの暗号化] をオンにして [共有のキャッシュ化を許可する] をオフにし、 [次へ] をクリックします。
6. 共有アクセス許可をカスタマイズするには、左ペインで[アクセス許可] を選択して、 [アクセス許可のカスタマイズ] > [共有] をクリックします。
   - o **Everyone**を削除
   - o **データプロキシ用のアカウント**にフルコントロールを追加
   - o **Local Administrators**にフルコントロールを追加
   - o **Domain Admins**にフルコントロールを追加
7. NTFSアクセス許可をカスタマイズするには、左ペインの[アクセス許可] で、 [アクセス許可のカスタマイズ] 、 [継承の無効化] をクリックし、 [継承されたアクセス許可をこのオブジェクトの明示的なアクセス許可に変換します] を選択します。



8. **Creator owner/Local Administrators/SYSTEM**以外のすべてのユーザーを削除するには、 [アクセス許可のカスタマイズ] > [アクセス許可] で [削除] をクリックします。

9. [Creator owner] > [権限の設定 (詳細)] を変更するには、 [編集] をクリックして、以下のチェックボックスをオフにします。

   - o フルコントロール
   - o サブフォルダとファイルの削除
   - o アクセス許可の変更
   - o 所有権の取得



10. **データプロキシ用のアカウント**にフルコントロールを追加します。

11. ［新しい共有］ウィザードの左ペインで [確認] をクリックし、現在選択している共有設定を確認します。 [作成] をクリックして、新しいフォルダーの作成プロセスを開始してから、 [閉じる] をクリックします。

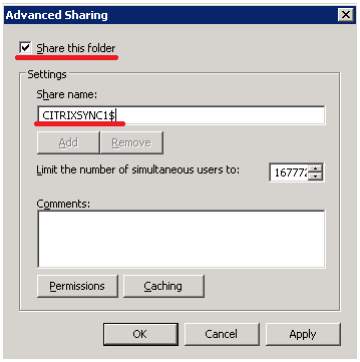
12. **CITRIXSYNC$**共有フォルダーの下に、**CentralStoreRoot**および**People**という2つのサブフォルダーを作成します。

重要：データプロキシ用のアカウントにこれらのサブフォルダーの**フルコントロール**があることを確認してください。

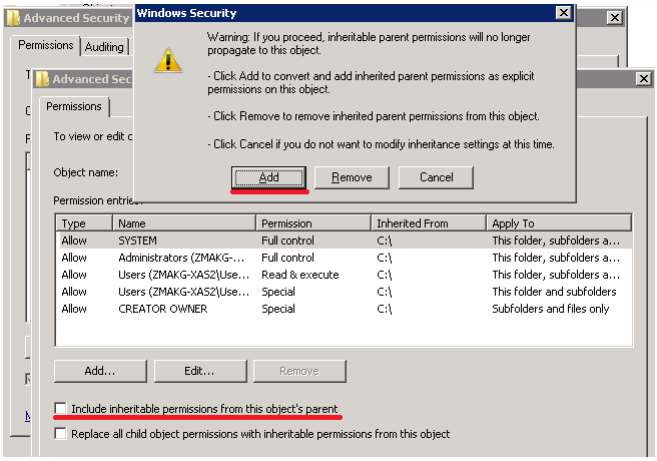
Windows Server 2008 R2の中央ストアの作成

セルフサービスパスワードリセットサービスと同じサーバーに中央ストアが作成されることを確認してから、リモートアクセスを阻止するようにWindowsファイアウォールを構成します。

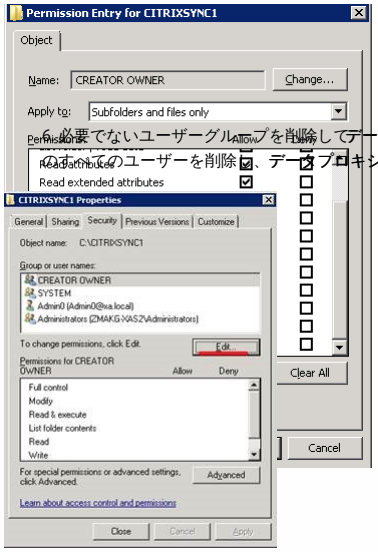
1. ローカルフォルダー（**CITRIXSYNC1**）をファイル共有のルートとして作成し、次の2つのサブフォルダーを作成します。**CentralStoreRoot**および**People**。
2. ファイル共有をセットアップし、共有アクセス権を付与します。
    a. **CITRIXSYNC1**フォルダーを右クリックし、**[プロパティ] > [共有] > [詳細な共有]**を選択します。
    b. **[このフォルダーの共有]**チェックボックスで、**[共有名]**を**CITRIXSYNC1$**に設定します。
    c. 共有アクセス権を付与するには、**[アクセス許可]**をクリックし、すべてのデフォルトのユーザーを削除し、**データ用のプロキシアカウント**、**Local Administrators**グループ、**Domain Admin**グループにそれぞれ**フルコントロール**のアクセス許可を追加します。
    d. **[キャッシュ]**をクリックして、**[共有にあるファイルやプログラムはオフラインで利用可能にしない]**チェックボックスをオンにします。



3. セキュリティのアクセス許可を付与するには、**CITRIXSYNC1**フォルダーを右クリックして、**[プロパティ] > [セキュリティ]**を選択します。
4. 継承可能なアクセス許可を無効にするには、**[詳細設定] > [アクセス許可の変更]**をクリックし、**[このオブジェクトの親からの継承可能なアクセス許可を含める]**チェックボックスをオフにしてから、警告ウィンドウで**[追加]**をクリックします。



5. **[編集]**をクリックして、**Creator owner**権限を変更し、以下のチェックボックスをオフにします。
    - フルコントロール
    - サブフォルダとファイルの削除
    - アクセス許可の変更
    - 所有権の取得



6. 必要でないユーザーグループを削除してデータプロキシ用のアカウントを追加するには、［プロパティ］画面で［編集］をクリックし、**Creator owner/SYSTEM/Local Administrators**以外のすべてのユーザーを削除し、データプロキシ用のアカウントにフルコントロールのアクセス許可を追加します。

7. SMB署名機能を有効にするには、［スタート］>［管理ツール］>［ローカルセキュリティポリシー］をクリックします。 左ペインで、［セキュリティの設定］>［ローカルポリシー］>［セキュリティオプション］を選択します。

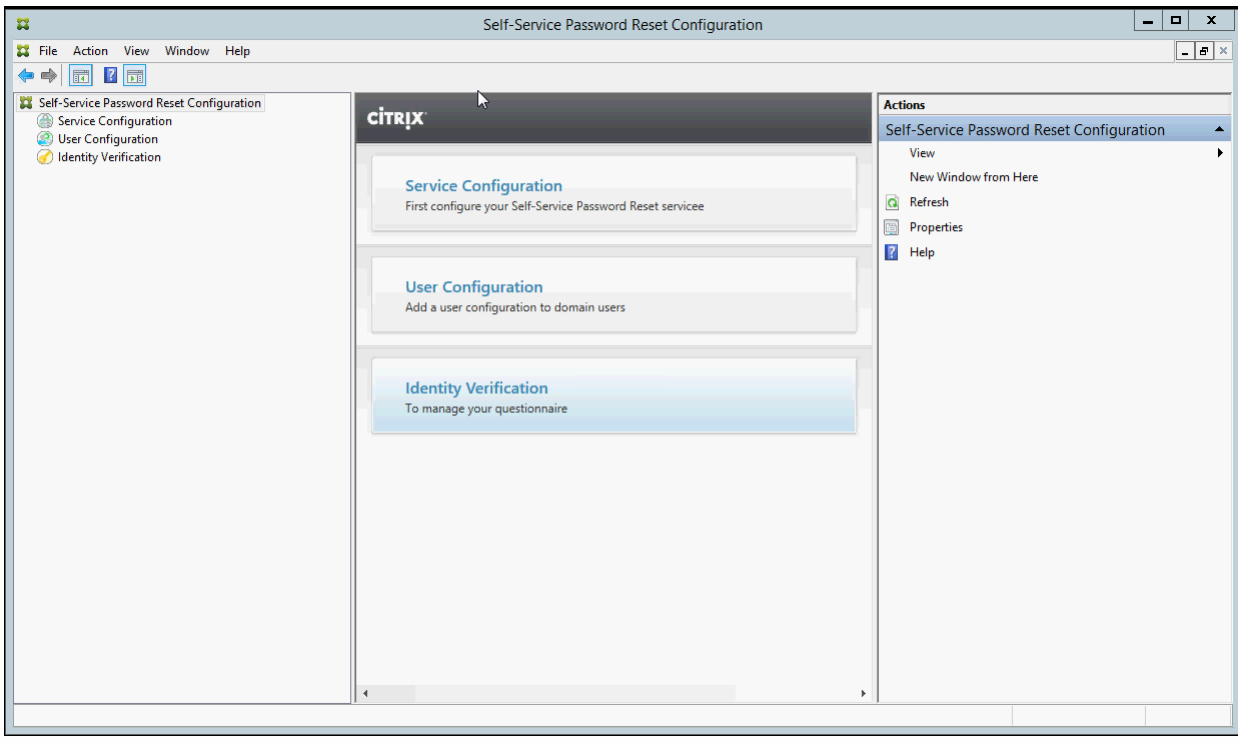
8. ［**Microsoftネットワーククライアント:サーバーが同意すれば、通信にデジタル署名を行う**]および［**Microsoftネットワークサーバー:クライアントが同意すれば、通信にデジタル署名を行う**］を有効にします。

9. ローカルの中央ストアへのリモートアクセスを阻止するには、Windowsファイアウォールの構成を終了します。 詳しくは、「ファイアウォール設定の構成」を参照してください。

Self-Service Password Resetのインストールと構成

インストールパッケージは、XenAppおよびXenDesktopのインストールメディアに含まれています。

1. Self-Service Password Resetインストールウィザードを開始してウィザードの手順を実行します。
2. ［**スタート**］>［**すべてのプログラム**］>［**Citrix**］>［**Citrixセルフサービスパスワードリセットの設定**]の順にクリックして、Citrixセルフサービスパスワードリセットサービスを構成します。
3. コンソールが表示されたら、以下の3つの基本手順に従ってサービスを構成します。



サービス設定

サービスを構成する前に、中央ストア、データプロキシ用のアカウント、セルフサービス用アカウントが作成されていることを確認します。

1. 中央ペインで［**サービス設定**］を選択し、右ペインで［**新しいサービス設定**］をクリックします。
2. ［**中央ストアの場所**］画面で中央ストアの場所を指定して、［**次へ**］をクリックします。
3. ［**ドメインの設定**］画面でドメインを選択し、［**プロパティ**］をクリックします。
4. **データプロキシアカウント**および**セルフサービスアカウント**のユーザー名とパスワードをそれぞれ指定して、［**OK**］、［**次へ**］、［**完了**］の順にクリックします。

ユーザー設定

1. 左ペインで **[ユーザー設定]** を選択し、右ペインで **[新しいユーザー設定]** をクリックします。
2. **[ユーザー設定の名前]** 画面で、セルフサービスパスワードサービスの対象ユーザーグループを定義し、Active Directoryからユーザー/グループ/組織単位を追加してから、**[次へ]** をクリックします。
3. **[ラインセンスの設定]** 画面で、ライセンスサーバーを指定して **[次へ]** をクリックします。
4. **[パスワードリセットの設定]** 画面で、Windowsパスワードのリセットおよびドメインアカウントのロック解除を管理者の介入なしで実行可能なユーザーを、チェックボックスを使用して指定します。次に、サービスのポートおよびアドレスを指定して **[作成]** をクリックします。

ユーザー設定の管理について詳しくは、「ユーザー設定の管理」を参照してください。

ユーザー識別処理

1. 左ペインで **[ユーザー識別処理]** ノードを選択し、右ペインで **[質問の管理]** をクリックします。
2. **[質問ベースの認証]** 画面で、デフォルトの言語を選択し、チェックボックスを使用してセキュリティ用の質問に対するユーザー回答の保護をオンまたはオフにして、**[次へ]** をクリックします。
3. **[セキュリティ用の質問]** 画面で、 **[質問の追加]** をクリックして、テキストボックスに質問を入力して **[OK]** をクリックし、 **[次へ]** をクリックします。
4. **[質問リスト]** 画面で **[追加]** をクリックし、質問を選択します。 **[上に移動]** および **[下に移動]** を使用して、質問とグループの順番を変更できます。 このページの設定が終わったら、**[作成]** 、 **[次へ]** の順にクリックします。

ユーザー識別用の質問の管理について詳しくは、「ユーザー識別用の質問の管理」を参照してください。

Manage user configurations

ユーザー設定の内容により、ユーザーがStoreFrontにログインしたときのSelf-Service Password Resetの動作やユーザーインターフェイスが制御されます。 ユーザー設定の作成は、環境内のユーザーにSelf-Service Password Resetを配布する直前に行います。 ただし、既存のユーザー設定の編集は、いつでも行うことができます。

ユーザー設定はユーザー固有の設定を定義したもので、Active Directory階層に関連付けられたユーザー（組織単位［OU］または個々のユーザー）またはActive Directoryグループに適用されます。

ユーザー構成は、以下の要素で構成されています。

- Active Directoryドメイン階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループ。

重要：Active Directory混在モードの配布グループとドメインローカルグループはサポートされていません。

- ライセンスサーバー
- セルフサービス機能（アカウントのロック解除とパスワードのリセット）

ユーザー構成を作成する前に、以下を作成または定義しておく必要があります。

- 中央ストア
- サービス設定

ユーザー構成を作成するには

1. **[スタート]** > **[すべてのプログラム]** > **[Citrix]** > **[Citrixセルフサービスパスワードリセットの設定]** の順にクリックします。
2. 左ペインで **[ユーザー設定]** ノードを選択します。
3. **[操作]** メニューから、 **[ユーザー設定の追加]** を選択します。

ユーザー、OU、グループを追加する

[ユーザー設定] ウィザードの **[ユーザー設定の名前]** ページで、ユーザー設定を割り当てるユーザーを指定できます。

ユーザー設定の割り当て：

ユーザー構成は、Active Directory階層に関連付けられたユーザー（組織単位または個々のユーザー）またはActive Directoryグループに割り当てることができます。 必要に応じて、**[操作]** メニューから **[ユーザー設定の編集]** を選択して、ユーザー構成を別の階層やグループに割り当てることができます。

ユーザー構成のグループへの割り当ては、Active Directory認証を使用するActive Directoryドメインでのみサポートされています。

（ユーザー設定の追加ウィザードまたはユーザー設定の編集ウィザードの） **[ユーザー設定の名前]** ページで、組織単位、ユーザー、グループを選択します。

注：セルフサービス パスワード リセット アカウントがパスワードをリセットできるユーザーグループには、特権が付与されているアカウント（ローカル管理者やドメイン管理者など）を含めないとをお勧めします。 新しい専用グループを使用します。

ライセンスを設定するには

ユーザー設定ウィザードの **[ラインセンスの設定]** ページで、Self-service Password Resetサービスで使用するライセンスサーバーの設定を行うことができます。

注：ロック解除機能およびリセット機能を使用できるのは、XenAppまたはXenDesktop Platinum Edition がある場合のみです。

（ユーザー設定の追加ウィザードまたはユーザー設定の編集ウィザードの） **[ラインセンスの設定]** ページで、ライセンスサーバーの名前とポート番号を入力します。

ロック解除機能およびリセット機能を有効化するには

Self-Service Password Reset により、ユーザーは、自分のWindowsパスワードのリセットおよびドメインアカウントのロック解除を管理者の介入なしで実行できるようになります。**[セルフサービスパスワードリセットの有効化]** ページで、有効化する機能を選択できます。

（ユーザー設定の追加ウィザードまたはユーザー設定の編集ウィザードの） **[セルフサービスパスワードリセットの有効化]** ページで、**ロック解除**機能と**リセット**機能から、ユーザーが使用可能な機能を選択します。

ブラックリストを構成するには

IT管理者は、ユーザーとグループをブラックリストに追加できます。 ブラックリストのユーザーおよびグループは、登録、アカウントのロック解除、パスワードリセットなどを含むセルフサービスパスワードリセットの機能を使用することはできません。 また、ブラックリストのユーザーは、ログオン後、Citrix Receiverの **[タスク]** ボタンを表示できません。

ブラックリストを構成するには

1. **[スタート]** > **[すべてのプログラム]** > **[Citrix]** > **[Citrixセルフサービスパスワードリセットの設定]**の順にクリックします。

2. 左ペインで **[ユーザー設定]** を選択し、右ペインで **[ブラックリスト設定]** をクリックします。
3. **[追加]** および **[削除]** ボタンを使用して、ユーザーやグループをブラックリストに追加したり、ブラックリストから削除できます。

ユーザー識別用の質問の管理

Citrix Self-Service Password Reset構成コンソールの［ユーザー識別処理］では、ユーザー識別処理、セルフサービスパスワードリセット、およびアカウントのロック解除機能に関連付けるすべてのセキュリティ用の質問を一元的に管理できます。 デフォルトの質問リストに独自のセキュリティ用の質問を追加したり、質問グループを作成したりすることができます。

- ユーザーがデフォルトの質問に対して回答を登録した後で、管理者が質問文を変更する場合は、その内容について考慮してください。 質問の内容を変えずに質問文を編集した場合は、回答の再登録をユーザーに要求する必要はありません。ただし、編集後もユーザーが同じ回答を入力できるように配慮する必要があります。
- ユーザーがセキュリティ用の質問に対する回答を登録した後で、質問リストの質問を追加、削除、または編集すると、ユーザーが登録済みの回答を入力できなくなる場合があります。 質問リストの質問が変更された場合、ユーザーはCitrix Receiverでタスクを開くときに新しい質問リストに回答する必要があります。
- 同じ質問を複数の質問グループに追加することができます。 質問グループに追加可能な質問の一覧には、既にほかのグループに追加されている質問も含め、すべての質問が表示されます。

以降で参照されている設定にアクセスするには、次の手順に従います。

1. **［スタート］ボタン**> **[すべてのプログラム]** > **[Citrix]** > **[Citrixセルフサービスパスワードリセットの設定]** の順にクリックします。
2. 左ペインで、 **[ユーザー識別処理]** ノードを選択します。
3. **[操作]** メニューから、 **[質問の管理]** を選択します。

デフォルトの言語を設定するには

通常、セキュリティ用の質問は、ユーザーが回答を登録したときのユーザープロファイルで設定されている言語で表示されます。 プロファイルで言語が設定されていない場合は、管理者が設定したデフォルトの言語で表示されます。

1. **［スタート］ボタン**> **[すべてのプログラム]** > **[Citrix]** > **[Citrixセルフサービスパスワードリセットの設定]** の順にクリックします。
2. 左ペインで、 **[ユーザー識別処理]** ノードを選択します。
3. **[操作]** メニューから、 **[質問の管理]** を選択します。
4. **[質問ベースの認証]** ページの **[デフォルトの言語]** ボックスの一覧で、デフォルトの言語を選択します。

回答入力時のセキュリティを有効にするには

セキュリティ用の質問を使用したユーザー認証をより安全にするために、ユーザーがテキストボックスに入力する回答の文字列を、アスタリスク（*）で隠すことができます。 この機能を有効にすると、ユーザーの入力した回答が表示されなくなります。 ユーザーは、セキュリティ用の質問に対する回答を登録するときに、誤入力を避けるために同じ回答を2回入力する必要があります。 ユーザーが同一性を証明するために再認証を受けるときは、回答を2回入力する必要はありません。入力した回答に誤りがある場合は、再入力を求めるメッセージが表示されます。

[質問ベースの認証] ページで **[ユーザーの回答の文字列を表示しない]** チェックボックスをオンにします。

セキュリティ用の質問を作成するには

管理者は、異なる言語を使用して、複数の質問を作成できます。 また、同じ質問に対して、各国語の翻訳を追加することもできます。 Citrix Receiverへの登録時には、そのユーザーのプロファイルで設定されている言語に応じた質問が表示されます。 プロファイルで言語が設定されていない場合は、デフォルトの言語で表示されます。

注：管理者は、異なる言語を使用して、複数の質問を作成できます。また、同じ質問に対して、各国語の翻訳を追加することもできます。セルフサービスパスワードリセットでは、そのユーザーのプロファイルで構成されている言語に応じた質問が表示されます。 プロファイルで設定されている言語の質問がない場合は、［質問ベースの認証］ページで設定するデフォルトの言語で表示されます。

1. **［セキュリティ用の質問］** ページの **［言語］** ボックスの一覧から言語を選択して、 **[質問の追加]** をクリックします。 ［セキュリティ用の質問］ダイアログボックスが開きます。
2. **［セキュリティ用の質問］** ダイアログボックスで、質問を作成します。

重要：既存の質問に翻訳を追加する場合は、［質問の追加］ではなく **[編集]** をクリックすることに注意してください。 **[質問の追加]** をクリックすると新しい質問が追加され、既存の質問とは関連付けられません。

既存の質問を編集したり翻訳を追加したりするには

ユーザーがセキュリティ用の質問に対する回答を登録した後で、質問リストの質問を追加、削除、または編集すると、ユーザーが登録済みの回答を入力できなくなる場合があります。 質問リストの質問が変更された場合、ユーザーはCitrix Receiverでタスクを開くときに新しい質問リストに回答する必要があります。 質問を編集しても、強制的にユーザーの再登録が実行されることはありません。

重要：既存の質問を編集する場合は、質問の意味を変更しないように注意してください。 質問の意味を変更すると、既存のユーザーが再認証を受けるときに正しい回答を入力できなくなる可能性があります。 ［編集］をクリックすると、これに対する注意を促すメッセージが表示されます。

1. **［セキュリティ用の質問］** ページの **［言語］** ボックスの一覧から言語を選択します。
2. 編集または翻訳する質問を選択して、 **[編集]** をクリックします。
3. **［セキュリティ用の質問］** ダイアログボックスで、質問を編集または翻訳します。

セキュリティ用の質問グループを作成するには

必要に応じて、多くのセキュリティ用の質問を作成して、ユーザーに回答させることができます。 管理者が質問リストに追加したすべての質問に対して、ユーザーは回答を入力する必要があります。 ただし、複数の質問をグループ化して、セキュリティ用の質問グループを作成すると、ユーザーがグループ内の質問を自由に選択して回答を登録できるようになります。この場合、ユーザーが回答しなければならない質問の数は、管理者が指定します。

たとえば、6つの質問で構成される質問グループを作成し、ユーザーが回答しなければならない質問の数を3に設定して、それを質問リストに追加します。ユーザーは、これら6つの質問から3つを自由に選択して、回答を登録します。 以降、ユーザーの同一性の検証が必要な状況になると、ユーザーが選択した3つの質問が再提示されます。

1. **［セキュリティ用の質問］** ページで **[グループの追加]** をクリックします。
2. **［セキュリティ用の質問グループ］** ダイアログボックスで、グループ名、使用する質問、およびユーザーが回答しなければならない質問の数を指定します。

セキュリティ用の質問グループを作成するには

一覧から編集する質問グループを選択して、 **[セキュリティ用の質問]** ページで **[編集]** をクリックします。 ［セキュリティ用の質問］ダイアログボックスが開き、グループに追加可能な質問の一覧が表示されます。 グループに追加済みの質問はチェックボックスがオンになっています。 ここでは、グループ名を変更したり、グループに含まれる質問を追加または削除したり、ユーザーが回答しなければならない質問の数を変更したりできます。

質問リストを追加または削除するには

質問リストでは、セキュリティ用の質問と質問グループを追加または削除できます。 また、ユーザーに表示される質問の順序を入れ替えることもできます。 質問リストの変更後、ユーザーに対して
StoreFrontへのログイン後に再登録タスクを行うように通知する必要があります。

1. 質問リストに質問またはグループを追加するには、**[質問リスト]** ページで **[追加]** をクリックします。
2. 質問リストから質問を削除するには **[削除]** をクリックします。
3. 質問の表示順序を変更するには、 **[上に移動]** または **[下に移動]** をクリックします。

ユーザー識別処理の管理

セルフサービスパスワードリセットでは、以下の操作を行うことができます。

- セキュリティ用の質問をインポートまたはエクスポートする
- ユーザーの回答を削除する

セキュリティ用の質問をインポートまたはエクスポートするには

セキュリティ用の質問およびグループのデータをインポートまたはエクスポートすることができます。

1. **[スタート]** > **[すべてのプログラム]** > **[Citrix]** > **[Citrixセルフサービスパスワードリセットの設定]** の順にクリックします。
2. 左ペインで、 **[ユーザー識別処理]** ノードを選択します。
3. **[操作]** メニューで、以下のいずれかを選択します。

セキュリティ用の質問のインポート
ファイルの場所を指定して、セキュリティ用の質問およびグループのデータをインポートします。

セキュリティ用の質問のエクスポート
ファイルの場所を指定して、セキュリティ用の質問およびグループのデータをエクスポートします。

安全な構成

Dec 08, 2016

ここでは、セルフサービスパスワードリセットのコンポーネントを安全に展開し、構成するために必要な手順について説明します。

- ユーザーパスワードのリセットおよびユーザーアカウントのアクセス権のロック解除を行うドメインユーザーアカウントの作成
- ファイアウォール設定の構成

セルフサービスアカウントの作成

セルフサービスパスワードリセットのパスワードリセット機能とアカウントロック解除機能を使用する場合は、サービスの設定時に、パスワードリセットとアカウントロック解除の実行でセルフサービスモジュールが使用するアカウントを指定します。 アカウントには適切な特権が必要ですが、実稼働環境でのDomain Adminsグループアカウントの使用はお勧めしません。推奨されるアカウント特権は次のとおりです。

- 同じドメインに属している
- 関連するドメインユーザーに対するパスワードリセットとアカウントロック解除の権限がある

[Active Directoryユーザーとコンピューター] で、ユーザーパスワードのリセットとユーザーアカウントのロック解除を行う権限を付与するグループまたはユーザーアカウントを作成します。

1. **[Active Directoryユーザーとコンピューター]** でドメインを右クリックして、メニューの **[制御の委任]** をクリックします。
2. **制御の委任**ウィザードが開きます。 **[ウィザードの開始]** ダイアログボックスで **[次へ]** をクリックします。
3. **[ローカルユーザーとグループ]** ダイアログボックスで、 **[追加]** をクリックします。 一覧からアカウントのロック解除権限を付与するグループを選択して、 **[OK]** をクリックします。 **[ユーザーとグループ]** ダイアログボックスで、 **[次へ]** をクリックします。
4. **[委任するタスク]** ダイアログボックスで、 **[委任するカスタムタスクを作成する]** 、 **[次へ]** の順にクリックします。
5. **[Active Directoryオブジェクトの種類]** ダイアログボックスで、［フォルダー内の次のオブジェクトのみ］の［ユーザーオブジェクト］をクリックして、 **[次へ]** をクリックします。
6. **[アクセス許可]** ダイアログボックスで、 **[全般]** チェックボックスと **[プロパティ固有]** チェックボックスをオンにします。 **[アクセス許可]** の一覧で、 **[lockoutTimeの読み取り]** 、 **[lockoutTimeの書き込み]** 、 **[パスワードのリセット]** 、 **[パスワードの変更]** 、 **[userAccountControlの読み取り]** 、 **[userAccountControlの書き込み]** 、 **[pwdLastSetの読み取り]** 、 **[pwdLastSetの書き込み]** の各チェックボックスをオンにして、 **[次へ]** をクリックします。
7. **[オブジェクト制御の委任ウィザードの完了]** ダイアログボックスで **[完了]** をクリックします。

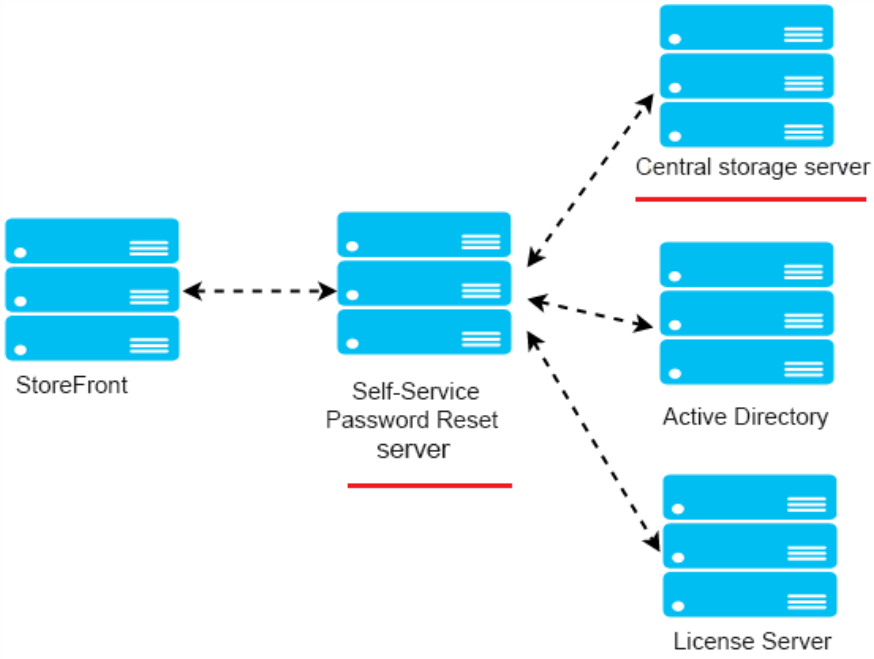
ファイアウォール設定の構成

セルフサービスパスワードリセットサーバーおよび中央ストレージサーバーのコンポーネントはユーザーのパスワードを管理するため、これらのコンポーネントを信頼できるネットワークに展開し、特定の信頼できるコンポーネントのみがアクセスできるようにすることを強くお勧めします。 ここでは、これらのサーバー用にWindowsファイアウォールを正しく構成するために必要な手順について説明します。 また、これらのサーバーが信頼できないネットワークトラフィックから確実に隔離されるように既存のネットワークインフラストラクチャを構成することもお勧めします。

展開環境で以下の構成を行うと、セルフサービスパスワードリセット中央ストアサーバーへのアクセスが、メッセージブロ

ク（Server Message Block：SMB）を使用したサーバーのみに制限されます。また、セルフサービスパスワードリセットサーバーへのアクセスは、HTTPS接続を使用したStoreFrontサーバーのみに制限されます。

Windows 2012 R2のリモートファイル共有の展開



環境

- 専用サーバーでセルフサービスパスワードリセットのコンポーネントをインストールします。 既存のStoreFrontまたはDelivery Controllerコンポーネントと同じサーバーに展開しないでください。同じサーバーに展開した場合、以下に示したファイアウォールの構成がStoreFrontまたはDelivery Controllerのトラフィックをブロックすることがあります。
- StoreFrontとSelf-Service Password Resetサーバーの間には、非透過HTTP/HTTPSプロキシは設定しないでください。

  非透過プロキシをStoreFrontとSelf-Service Password Resetサーバーの間に設定する場合は、Self-Service Password Resetサーバーへのアクセスを、ファイアウォール規則に含まれるプロキシサーバーに対してのみ許可するように構成してください。

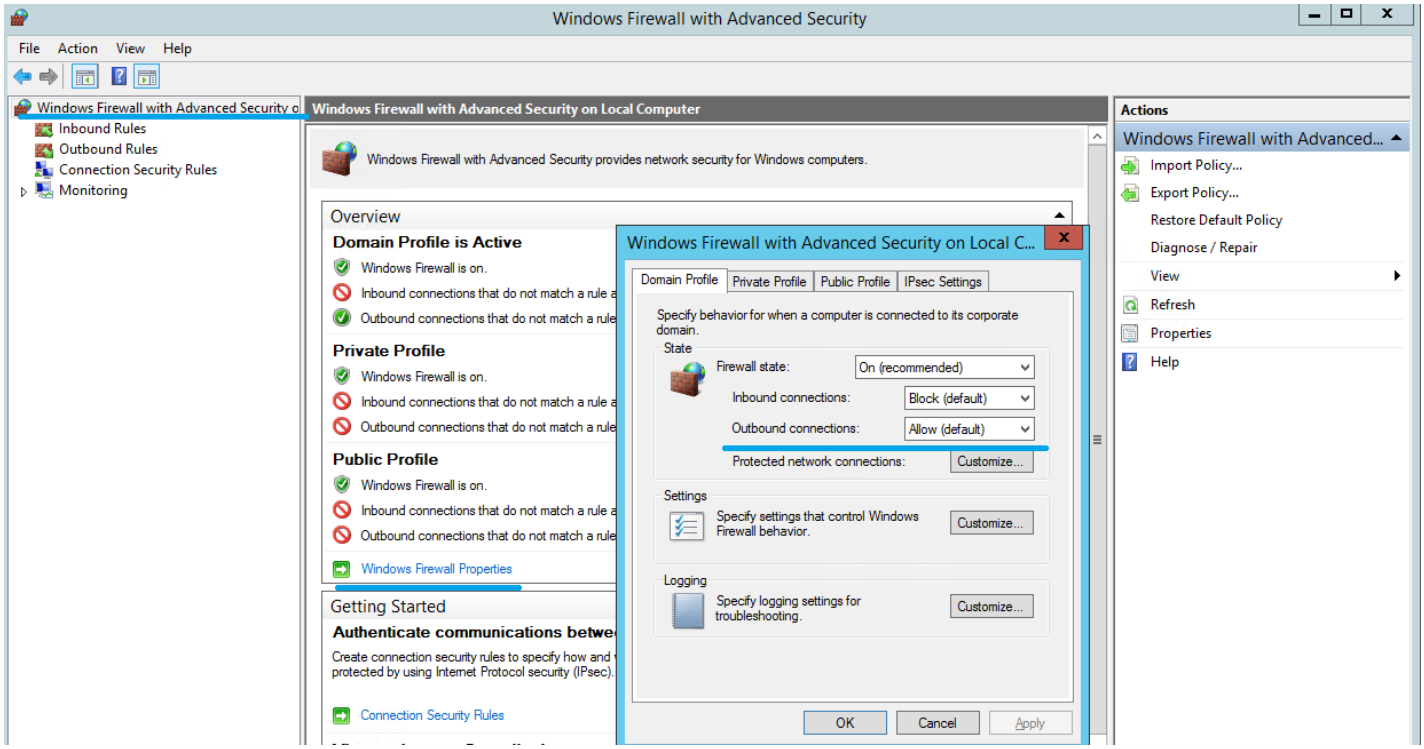
- 以下の手順の構成は、デフォルトのWindowsファイアウォールの規則に基いています。

Self-Service Password Reset中央ストアのファイアウォールを構成する

構成を完了すると、Self-Service Password Reset中央ストアから提供されるSMBサービスには、受信接続のSelf-Service Password Resetサーバーのみがアクセスできるようになります。また、Self-Service Password Reset中央ストアサーバーは、送信接続でのみ社内ネットワーク上のサービスにアクセスできるようになります。

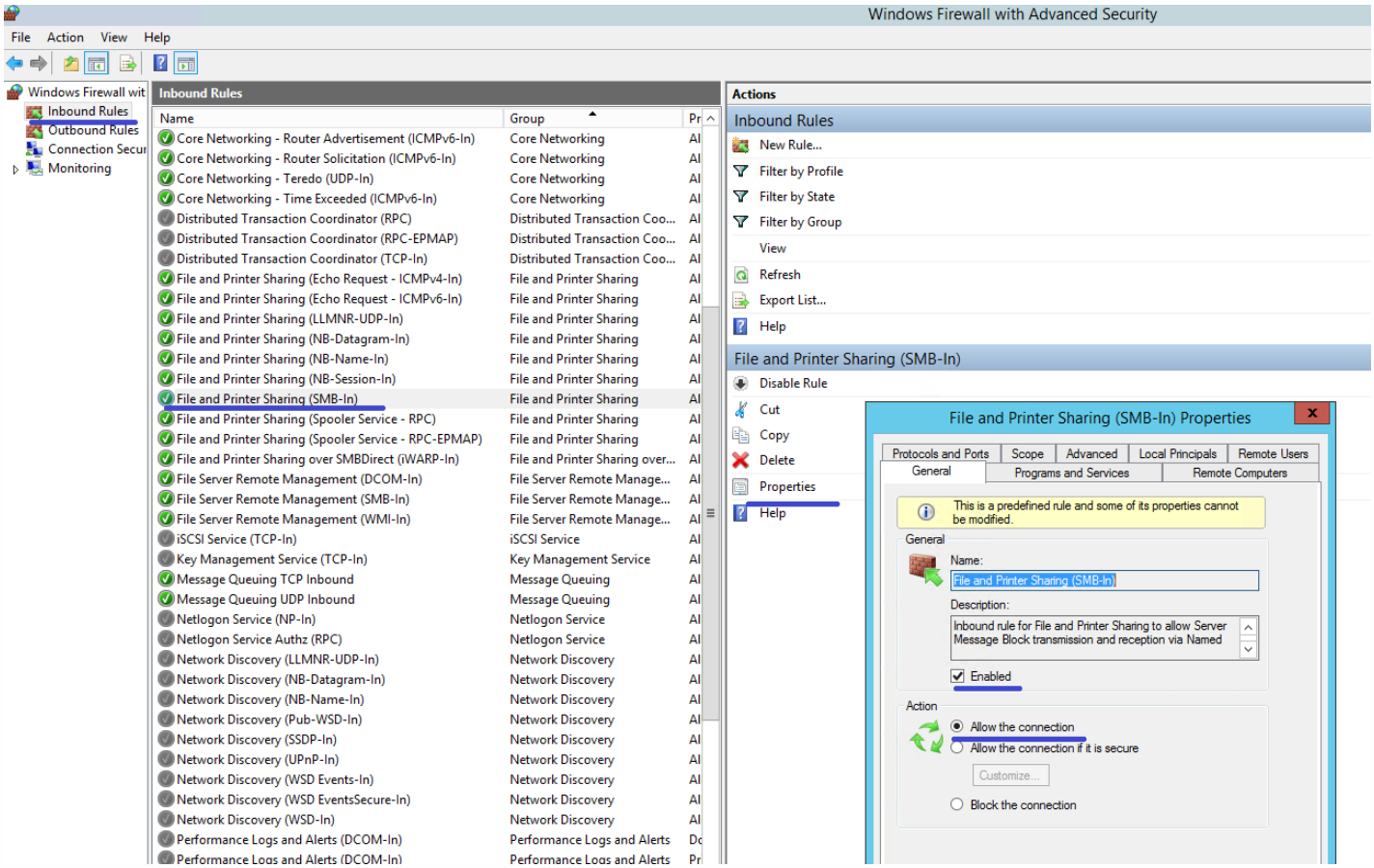
1. サーバーマネージャーを開き、上部ナビゲーションバーの **[ツール]** メニューで **[セキュリティが強化されたWindowsファイアウォール]** をクリックします。

2. **[セキュリティが強化されたWindowsファイアウォール]** ページで、中央ペインの **[Windowsファイアウォールのプロパティ]** をクリックします。 ドメイン、プライベート、パブリックの3種類のファイアウォールプロファイルがあります。 **[ドメインプロファイル]** タブを選択します。 **[ファイアウォールの状態]** を **[有効]** 、 **[受信接続]** を **[ブロック]** 、 **[送信接続]** を **[許可]** にそれぞれ設定します。



3. **[プライベートプロファイル]** タブと **[パブリックプロファイル]** タブのそれぞれで、**[ファイアウォールの状態]** を **[有効]**、**[受信接続]** と **[送信接続]** の両方を **[ブロック]** に設定します。 変更を適用して保存します。

4. **[受信の規則]** で **[ファイルとプリンターの共有（SMB受信）]** を選択して、**[有効]** をオンにして **[操作]** を **[接続を許可する]** に設定します。



5. **[ファイルとプリンターの共有（SMB受信）のプロパティ]** で **[スコープ]** タブをクリックし、 **[これらのIPアドレス]** をオンにして、一覧にすべてのSelf-Service Password Resetサーバーの IPアドレスを追加します。 例：セルフサービスパスワードリセットサーバーA（192.168.1.10）およびセルフサービスパスワードリセットサーバーB（192.168.1.11）。

6. **[ファイルとプリンターの共有（SMB受信）のプロパティ]** で **[詳細設定]** タブをクリックして、 **[ドメイン]** 、 **[プライベート]** 、 **[パブリック]** の各プロファイルをオンにして変更内容を保存します。

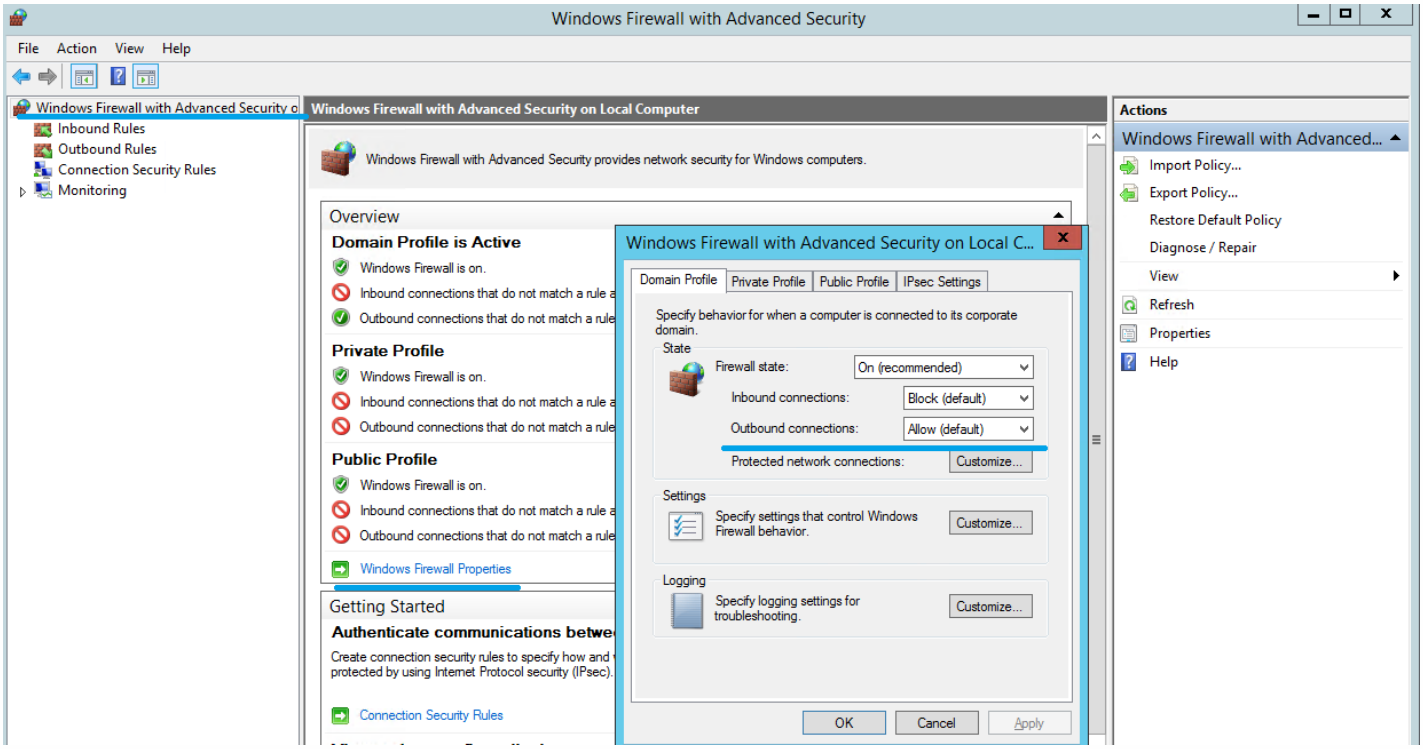
7. 上記の手順を、 **[ファイルサーバーリモート管理（SMB受信）]** と **[ファイルとプリンターの共有（NBセッション受信）]** の各受信規則に対しても実行します。

Self-Service Password Resetサーバーのファイアウォールを構成する

構成を完了すると、セルフサービスパスワードリセットサーバーから提供されるWebサービスには、HTTPSを使用したStoreFrontサーバーのみがアクセスできるようになります。また、セルフサービスパスワードリセットサーバーは、社内ネットワーク上のサービスにアクセスできるようになります。

1. サーバーマネージャーを開き、上部ナビゲーションバーの **[ツール]** メニューで **[セキュリティが強化されたWindowsファイアウォール]** をクリックします。

2. **[セキュリティが強化されたWindowsファイアウォール]** ページで、中央ペインの **[Windowsファイアウォールのプロパティ]** をクリックします。 ドメイン、プライベート、パブリックの3種類のファイアウォールプロファイルがあります。 **[ドメインプロファイル]** タブを選択します。 **[ファイアウォールの状態]** を **[有効]** 、 **[受信接続]** を **[ブロック]** 、 **[送信接続]** を **[許可]** にそれぞれ設定します。

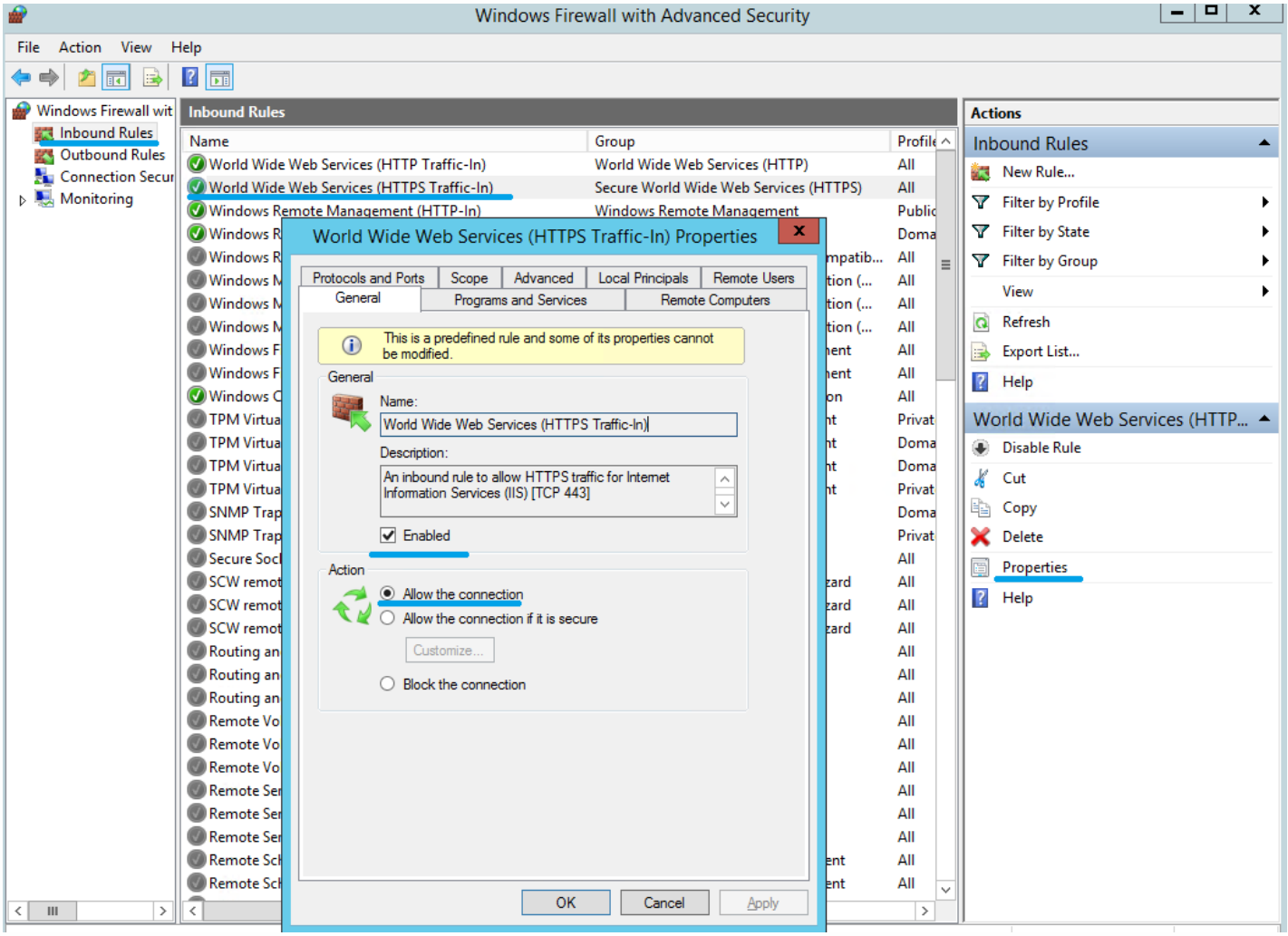


3. **[プライベートプロファイル]** タブと **[パブリックプロファイル]** タブのそれぞれで、 **[ファイアウォールの状態]** を **[有効]** 、 **[受信接続]** と **[送信接続]** の両方を **[ブロック]** に設定します。 変更を適用して保存します。

4. **[受信の規則]** で **[World Wide Webサービス（HTTPトラフィック）]** を選択して、 **[有効]** をオンにして、 **[操作]** を **[接続をブロックする]** に設定します。

5. **[World Wide Web Services（HTTPトラフィック）のプロパティ]** で **[詳細設定]** タブをクリックして、 **[ドメイン]** 、 **[プライベート]** 、 **[パブリック]** の各プロファイルをオンにして変更内容を保存します。

6. **[受信の規則]** で **[World Wide Webサービス（HTTPSトラフィック）]** を選択して、 **[有効]** をオンにして、 **[操作]** を **[接続を許可する]** に設定します。



7. **[World Wide Webサービス（HTTPSトラフィック）のプロパティ]** で［スコープ］タブをクリックし、 **[これらのIPアドレス]** をオンにして、一覧にすべてのStoreFrontサーバーのIPアドレスを追加します。 例：StoreFront A（192.168.1.50）およびStoreFront B（192.158.1.51）。

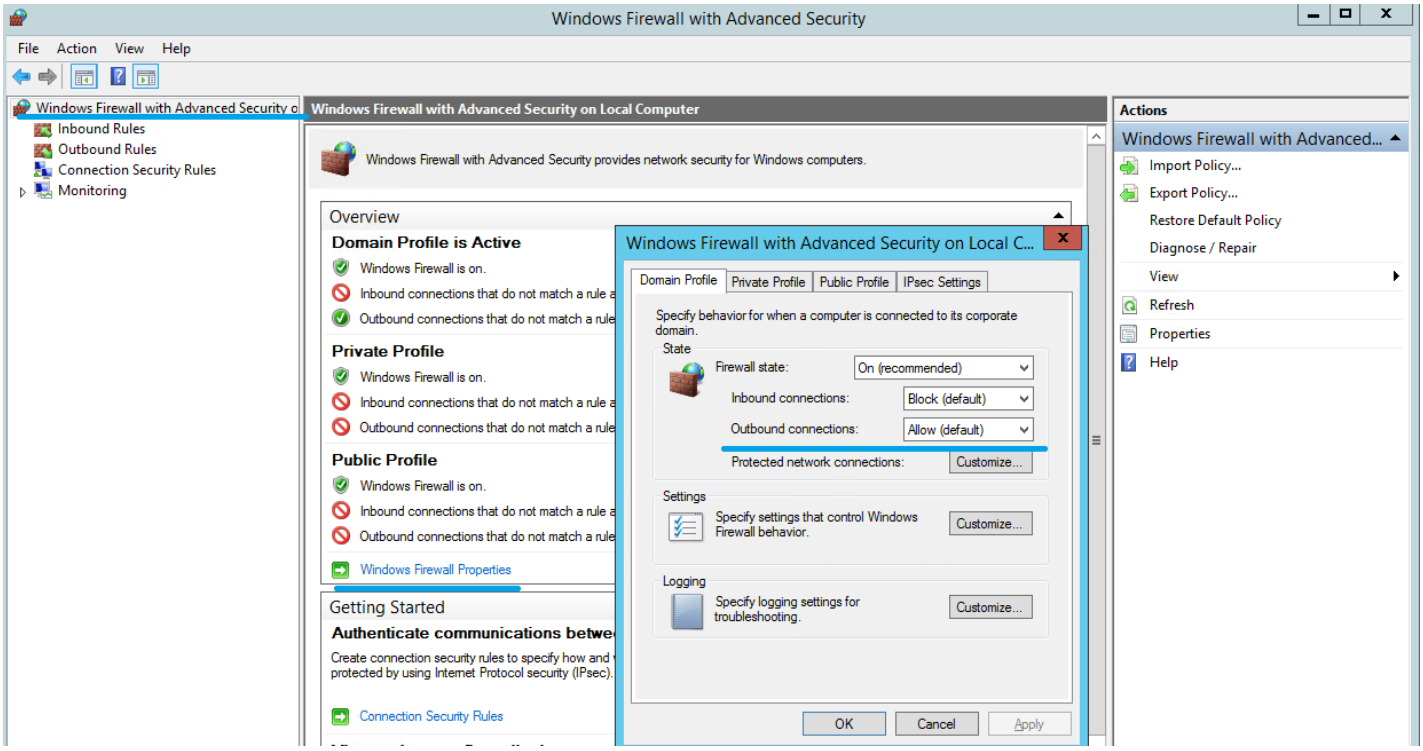
8. **[World Wide Web Services（HTTPSトラフィック）のプロパティ]** で **[詳細設定]** タブをクリックして、 **[ドメイン]** 、［プライベート］、 **[パブリック]** の各プロファイルをオンにして変更内容を保存します。

Windows 2008 R2のローカルファイル共有の展開

このトピックの説明に従って構成を完了した後、リモートクライアントのすべてのサーバーメッセージブロック（Server Message Block：SMB）アクセスがブロックされます。 SMBファイル共有には、ローカルからのみアクセスできます。また、セルフサービスパスワードリセットサービスへのアクセスは、HTTPS接続を使用したStoreFrontサーバーのみに制限されます。

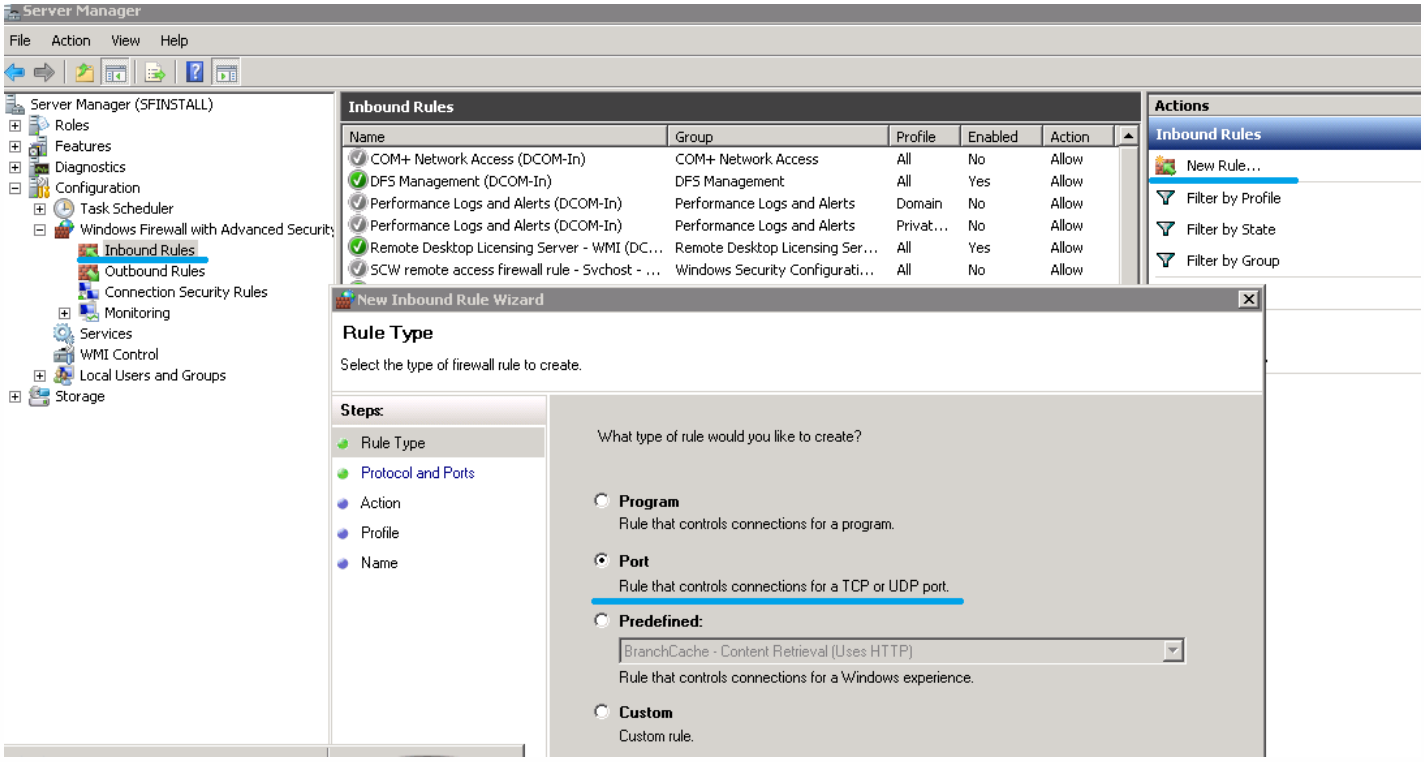
1. サーバーマネージャーを開き、上部ナビゲーションバーの **[ツール]** メニューで **[セキュリティが強化されたWindowsファイアウォール]** をクリックします。

2. **[セキュリティが強化されたWindowsファイアウォール]** ページで、中央ペインの **[Windowsファイアウォールのプロパティ]** をクリックします。 ドメイン、プライベート、パブリックの3種類のファイアウォールプロファイルがあります。 **[ドメインプロファイル]** タブを選択します。 **[ファイアウォールの状態]** を **[有効]** 、 **[受信接続]** を **[ブロック]** 、 **[送信接続]** を **[許可]** にそれぞれ設定します。



3. **[プライベートプロファイル]** タブと **[パブリックプロファイル]** タブのそれぞれで、 **[ファイアウォールの状態]** を **[有効]** 、 **[受信接続]** と **[送信接続]** の両方を **[ブロック]** に設定します。 変更を適用して保存します。

4. **[受信の規則]** から **[新規の規則]** を選択し、新しい受信の規則を作成します。 **[新規の受信の規則ウィザード]** で **[規則の種類]** を選択してから、 **[ポート]** で新しい規則の種類を選択し、 **[次へ]** をクリックします。



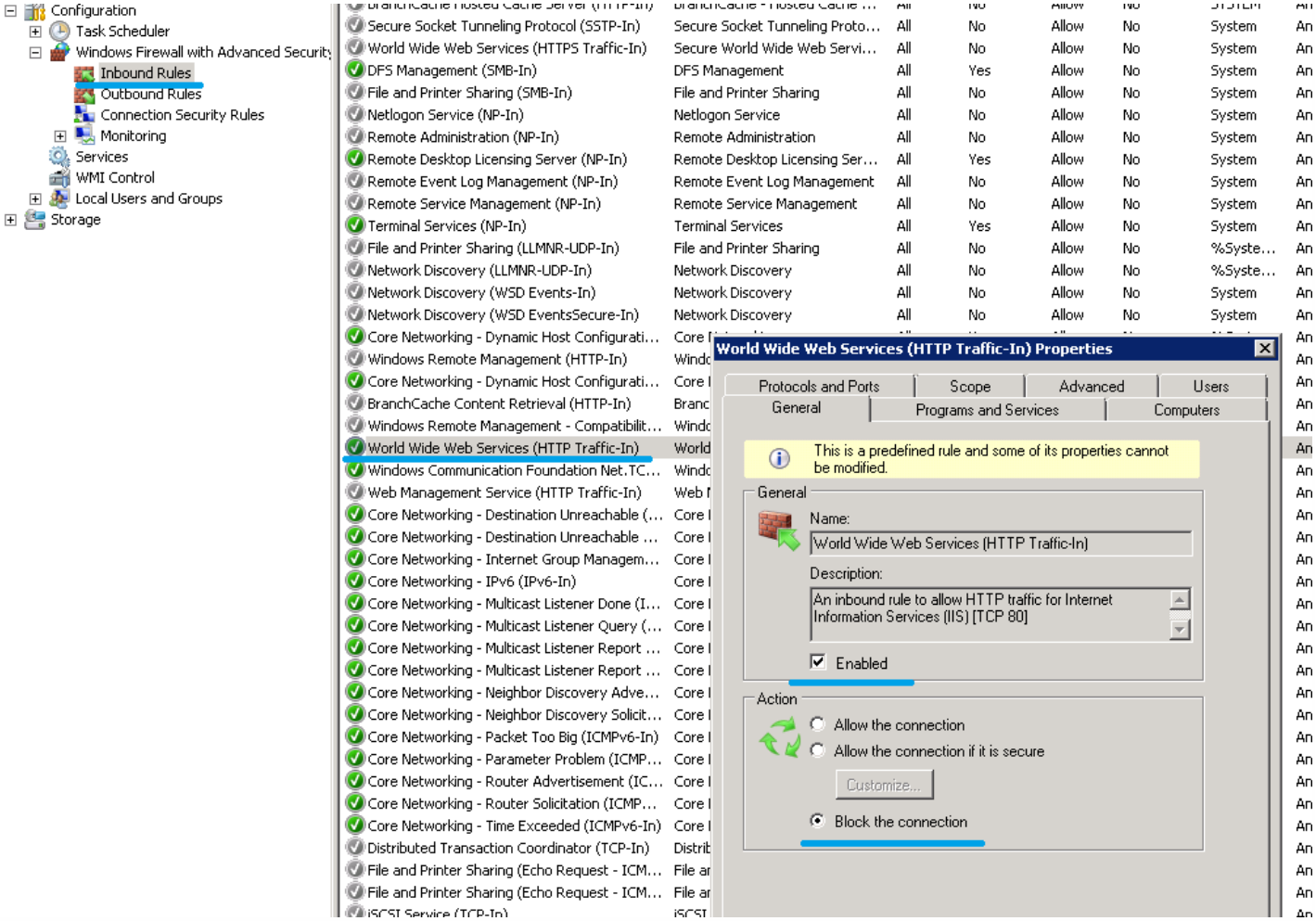
5. **[新規の受信の規則ウィザード]** で **[プロトコルおよびポート]**、**[TCP]** の順に選択し、**[特定のローカルポート]** テキストボックスに**445**を入力してから、**[次へ]** をクリックします。

6. **[新規の受信の規則ウィザード]** で、**[操作]**、**[接続をブロックする]** の順に選択し、**[次へ]** をクリックします。

7. **[新規の受信の規則ウィザード]** で、**[プロファイル]**、**[ドメイン]**、**[プライベート]** および **[パブリック]** の順に選択して、**[次へ]** をクリックします。

8. **[新規の受信の規則ウィザード]** で、**[名前]** を選択して、名前と説明を入力し、**[次へ]** をクリックします。

9. **[受信の規則]** で **[World Wide Webサービス（HTTPトラフィック）]** を選択して、**[有効]** をオンにして、**[操作]** を **[接続をブロックする]** に設定します。



10. **[World Wide Web Services（HTTPトラフィック）のプロパティ]** で **[詳細設定]** タブをクリックして、 **[ドメイン]** 、 **[プライベート]** 、 **[パブリック]** の各プロファイルをオンにして変更内容を保存します。

11. **[受信の規則]** で **[World Wide Webサービス（HTTPSトラフィック）]** を選択して、 **[有効]** をオンにして、 **[操作]** を **[接続を許可する]** に設定します。

12. **[World Wide Webサービス（HTTPSトラフィック）のプロパティ]** で **[スコープ]** タブに変更します。 **[リモートIPアドレス]** セクションで、 **[これらのIPアドレス]** をオンにして、一覧にすべてのStoreFrontサーバーのIPアドレスを追加します。 例：StoreFront A（192.168.1.13）およびStoreFront B（192.158.1.14）。

13. **[World Wide Web Services（HTTPトラフィック）のプロパティ]** で **[詳細設定]** タブをクリックして、 **[ドメイン]** 、 **[プライベート]** 、 **[パブリック]** の各プロファイルをオンにして変更内容を保存します。

Single Sign-On中央ストアからのデータの移行

Dec 08, 2016

Single Sign-on中央ストアは、Single Sign-Onによるユーザーデータや管理データを格納および管理する、集中リポジトリです。 ユーザーデータには、ログオン情報、セキュリティ用の質問と回答、およびユーザーに関するそのほかのデータがあります。 管理データには、パスワードポリシー、アプリケーション定義、セキュリティ用の質問などがあります。

データの中には、Single Sign-on中央ストアからSelf-Service Password Reset中央ストアに移行できないものがあります。 次の表に、移行可能なデータと移行できないデータを示します。

移行不可能	移行可能
パスワードポリシー - サポートされません	登録データを含むPeopleフォルダー
アプリケーションテンプレート - サポートされません	顧客が使用する質問リスト
アプリケーション定義 - サポートされません	
ユーザー設定 - Self-Service Password Resetコンソールで作成します	
アプリケーショングループ - サポートされません	
Single Sign-Onサービスのデータ - Self-Service Password Resetコンソールで作成します	

Important

- セルフサービスパスワードリセットでは、中央ストアとしてサポートされるのはネットワーク共有のみで、Active Directoryはサポートされません。
- セルフサービスパスワードリセットでは、Single Sign-On 4.8または5.0のデータのみをサポートします。

Single Sign-On中央ストアからデータを移行するには

データを移行する前に、Self-Service Password Resetのインストールと設定について把握してください。 詳しくは、「インストールと構成」を参照してください。

1. 新しい中央ストアを作成します。
2. Self-Service Password Resetのサービスおよびコンソールをインストールします。
3. コンソールで新しい中央ストアの場所を指定します。
4. 新しいユーザー設定を作成し、Single Sign-OnのSelf-Service Password Reset権限を持つユーザーを含めます。
5. Single Sign-Onの登録データとセキュリティ用の質問を新しい中央ストアにコピーします。

   注：データプロキシ用のアカウントで、すべてのコピーされたファイルに対するフルコントロールのアクセス許可があることを確認してください。

   必要なフォルダー/ファイルは2つだけです。

例

すべてのユーザーの登録データをコピーします。

\\SSO-SERVER\citrixsync$\People

を

\\SSPR-SVC\citrixsync$\People

このコマンドを使用します。
Robocopy \\SSO-SERVER\citrixsync$\People\ \\SSPR-SVC\citrixsync$\People /e /xd QBA /Log+:copylog.txt /tee

顧客に使用されているセキュリティ用の質問をコピーします。

\\SSOSERVERcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\
QuestionBasedAuthentication2

を

\\SSPRSVCcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\

このコマンドを使用します。
Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ \\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee

これで、すべてのユーザーがSingle Sign-Onの登録時の質問と回答を使用して、ロック解除およびリセットを実行できるようになりました。

セキュリティ用の質問に対する回答の登録をユーザーに許可するようにStoreFrontを構成する

Dec 08, 2016

セキュリティ用の質問に対する回答の登録をユーザーに許可するようにStoreFrontを構成します。 ユーザーは、登録されると、ドメインパスワードのリセットおよびドメインアカウントのロック解除を実行できるようになります。 詳しくは、StoreFrontのドキュメントを参照してください。

1. HTTPSに対してStoreFrontインターネットインフォメーションサービス（IIS）を構成します。
2. StoreFrontで新しい展開環境を作成します。
3. StoreFront管理コンソールの右ペインで、**[認証方法の管理] > [ユーザー名とパスワード]** の順にクリックします。 ドロップダウンの一覧から **[パスワードオプションの管理]** を選択します。
4. パスワードの変更を許可するユーザーを選択し、**[OK]** をクリックします。
5. **[ユーザー名とパスワード]** ボックスの一覧で **[アカウントセルフサービスの設定]** を選択し、**[Citrix SSPR]** を選択して **[構成]** をクリックします。
6. ユーザーに対して、Self-Service Password Resetを使用したパスワードのリセットおよびアカウントのロック解除を許可するかどうかを指定して、Password ServiceアカウントのサービスURLを追加して **[OK]** をクリックします。

注：統合エクスペリエンスを使用するようにサイトを構成する必要があります。

Citrix ReceiverまたはCitrix Receiver for Webへの次回ユーザーログオン時に、セキュリティ用の質問に対する回答を登録できるようになります。 **[開始]** をクリックすると、ユーザーが回答を登録する必要のある質問が表示されます。