セルフサービスパスワードリセット 1.1.x

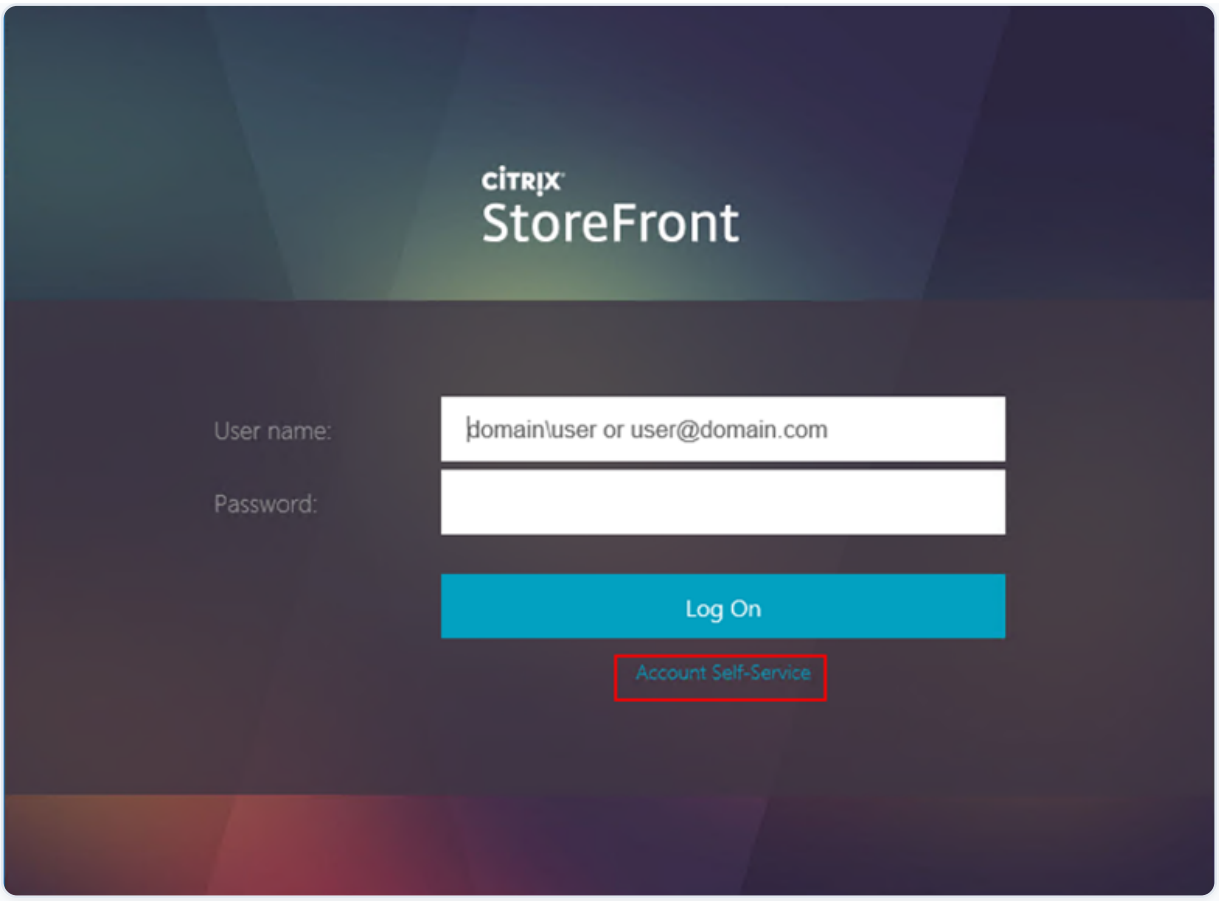
注：

セルフサービスパスワードリセットは非推奨であり、Citrix Virtual Apps and Desktops™ 2006以降のバージョンでは利用できません。

セルフサービスパスワードリセットにより、エンドユーザーは自分のユーザーアカウントをより詳細に制御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が構成されている場合、エンドユーザーがシステムへのログオンに問題がある場合でも、いくつかのセキュリティの質問に正しく答えることによって、アカウントのロックを解除したり、パスワードを新しいものにリセットしたりできます。

ヒント:

StoreFront™のログオンページには、ユーザーがパスワードのロック解除とリセットを行うための**Account Self-Service**リンクが表示されます。



ユーザーパスワードのリセットは、本質的にセキュリティ上機密性の高いプロセスです。展開が正しく構成されていることを確認するために、Secure configurationの記事を参照することをお勧めします。

新機能

バージョン 1.1.20 の新機能

Self-Service Password Reset サービスへの接続を許可する IP アドレスを設定できます。IP アドレスを入力しない場合、すべての IP アドレスがホワイトリストに登録され、接続が許可されます。

バージョン 1.1.10 の新機能

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

バージョン 1.1 の新機能

このバージョンには、次の主要な機能強化が含まれています。

- ブラックリスト構成のサポート - 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。ブラックリスト内のユーザーとグループは、Self-Service Password Reset のどの機能も使用できません。
- 簡体字中国語のサポート - 英語、フランス語、日本語、スペイン語に加えて、セキュリティの質問を定義するために簡体字中国語が利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ています。

- 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™ でのセキュリティの質問の登録

Self-Service Password Reset 構成コンソール

- **サービス構成。** 中央ストアアドレス、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 サービスを構成します。
    - 中央ストアアドレス: Self-Service Password Reset データを保存するためのネットワーク共有の場所。

  - データプロキシアカウント: 中央ストアと通信します。このアカウントには、中央ストアへの読み取り/書き込みアクセスが必要です。
  - セルフサービスパスワードリセットアカウント: アカウントのロック解除とパスワードのリセットに使用されます。

- **ユーザー構成。** セルフサービスパスワードリセット機能を使用できるユーザー/グループ/OUを構成し、ライセンスサーバー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。
  - ユーザー構成の名前: セルフサービスパスワードサービスのターゲットユーザーグループを定義します。これにはActive Directoryのユーザー/グループ/OUを含めることができます。
  - ライセンスサーバーアドレス: セルフサービスパスワードリセットは、Citrix Virtual AppsまたはCitrix Virtual Desktops Platinumエディションでのみ使用できます。最小ライセンスサーバーバージョンは11.13.1以降である必要があります。
  - **ロック解除**機能と**リセット**機能を選択または選択解除します。
  - 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。

- **ID検証。** 登録、アカウントのロック解除、またはパスワードのリセットに使用されるアンケートを構成します。
  - 質問またはグループを、アンケートが生成される質問ストアに追加します。
  - 登録に使用される質問ストアから質問リストを選択します。
  - セキュリティ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

セルフサービスパスワードリセットサービスはWebサーバー上で実行され、ユーザーがWindowsパスワードをリセットし、Windowsアカウントのロックを解除できるようにします。エンドユーザーのリクエストは、StoreFrontを介してこのサービスに送信されます。

StoreFrontでのセキュリティ質問の登録

StoreFrontを使用して、ユーザーがセキュリティの質問に対する回答を登録できるようにします。登録されると、ドメインパスワードをリセットし、ドメインアカウントのロックを解除できます。詳細については、「認証サービスの構成」の「セルフサービスパスワードリセットのセキュリティ質問」セクションを参照してください。

修正された問題

バージョン 1.1.20

このリリースには、修正された問題はありません。

バージョン 1.1.10

このバージョンでは、以下の問題が解決されています。

- **Self-Service Password Reset** サーバーで TLS 1.0 を無効にした後、ウィザードにサーバー URL を追加すると、このエラーメッセージが表示されることがあります。

  「サーバーアドレスにアクセスできません。」\[#LC7741\]

- パスワードリセット機能を有効にし、ドメインコントローラーにカスタマイズされたパスワードフィルターを適用すると、パスワードリセット機能が動作しない場合があります。このエラーメッセージが表示されます。

  「指定されたパスワードが無効です。」\[#LC7570\]

既知の問題

バージョン 1.1.20

このバージョンには以下の既知の問題があります。

- ユーザー構成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登録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。このメッセージは正しくありません。この試行は、このグループをすでに登録しているために失敗しました。

  \[#665520\]

- 構成ウィザードから削除したばかりのユーザーやユーザーグループは、削除プロセスを完了してウィザードを閉じるまで追加できません。そうしないと、ユーザーまたはグループがブラックリストに登録されているという誤ったエラーメッセージが表示されます。回避策として、削除プロセスを完了してウィザードを閉じ、その後ウィザードを再度開いてユーザーまたはグループを再度追加してください。

  \[#665352\]

- Self-Service Password Reset をバージョン 1.1 にアップグレードする際に、バージョン 1.0 のコンソールが開いていると、対応するものがなく、バージョン 1.0 の開いているコンソールは使用できません。

  \[#664390\]

- .Net Framework 4.5 のみがインストールされている Windows Server 2012 でアップグレードまたはアンインストールしようとすると、および .Net Framework 4.6 のみがインストールされている Windows Server 2016 でアップグレードまたはアンインストールしようとすると、失敗することがあります。これらの試行は、Windows Server 2012 および Windows Server 2016 でのインプレースアップグレードまたはアンインストールが .Net Framework 3.5 に依存しているために失敗します。回避策として、アップグレード前およびアンインストール前に .Net Framework 3.5 をインストールしてください。

  \[DNA-22761\]

バージョン 1.1.10

このバージョンには以下の既知の問題があります。

- ユーザー構成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登録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。このメッセージは正しくありません。この試行は、このグループをすでに登録しているために失敗しました。

  \[#665520\]

- 構成ウィザードから削除したばかりのユーザーやユーザーグループは、削除プロセスを完了してウィザードを閉じるまで追加できません。そうしないと、ユーザーまたはグループがブラックリストに登録されているという誤ったエラーメッセージが表示されます。回避策として、削除プロセスを完了してウィザードを閉じ、その後ウィザードを再度開いてユーザーまたはグループを再度追加してください。

  \[#665352\]

- 「セルフサービスパスワードリセット」をバージョン1.1にアップグレードする際にバージョン1.0コンソールが開いている場合、対応するバージョン1.0の開いているコンソールは使用できません。

  \[#664390\]

- .Net Framework 4.5のみがインストールされているWindows Server 2012、および.Net Framework 4.6のみがインストールされているWindows Server 2016でアップグレードまたはアンインストールを実行しようとすると、失敗する可能性があります。これらの試行が失敗す

るのは、Windows Server 2012およびWindows Server 2016でのインプレースアップグレードまたはアンインストールが.Net Framework 3.5に依存しているためです。回避策として、アップグレードおよびアンインストールの前に.Net Framework 3.5をインストールしてください。

\[DNA-22761\]

バージョン1.1

このバージョンには、以下の既知の問題があります。

- ユーザー構成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登録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。このメッセージは誤りです。この試行が失敗したのは、このグループが既に追加されているためです。

  \[#665520\]
- 構成ウィザードから削除したばかりのユーザーやユーザーグループは、削除プロセスを完了してウィザードを閉じるまで追加できません。そうしないと、ユーザーまたはグループがブラックリストに登録されているという誤ったエラーメッセージが表示されます。回避策として、削除プロセスを完了してウィザードを閉じ、ウィザードを再度開いてユーザーまたはグループを再度追加してください。

  \[#665352\]
- 「セルフサービスパスワードリセット」をバージョン1.1にアップグレードする際にバージョン1.0コンソールが開いている場合、対応するバージョン1.0の開いているコンソールは使用できません。

  \[#664390\]
- .Net Framework 4.5のみがインストールされているWindows Server 2012、および.Net Framework 4.6のみがインストールされているWindows Server 2016でアップグレードまたはアンインストールを実行しようとすると、失敗する可能性があります。これらの試行が失敗するのは、Windows Server 2012およびWindows Server 2016でのインプレースアップグレードまたはアンインストールが.Net Framework 3.5に依存しているためです。回避策として、アップグレードおよびアンインストールの前に.Net Framework 3.5をインストールしてください。

  \[DNA-22761\]

バージョン 1.0

このバージョンには、以下の既知の問題があります。

- Self-Service Password Reset コンソールを開いた後、タスクバーにピン留めできない場合があります。

  回避策: **スタート**メニューのショートカットからコンソールをタスクバーにピン留めします。

- Windows 2016の既知の問題により、Windows 2016でSelf-Service Password Resetコンソールを検索できません。

  > 回避策: **スタート**メニューを使用してSelf-Service Password Resetを見つけます。

- デフォルトドメインポリシーのパスワードポリシーでパスワードの最小有効期間がデフォルト（1日）に設定されており、ユーザーがパスワードのリセットを試みたもののリセットに失敗した場合（たとえば、複雑さの要件を満たさない場合など）、パスワードリセットウィザードを閉じると、24時間パスワードを再度リセットできません。

- Mac版Citrix Workspace™アプリを使用している場合、登録用のタスクボタンはユーザーがStoreFrontに初めてログオンしたときに表示されます。StoreFrontからログオフして再度ログオンすると、タスクボタンは表示されません。

回避策: 1\. StoreFrontストアの右上隅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の**Refresh Apps**ボタンをクリックします。 3\. Mac版Citrix Workspaceアプリを閉じて再度開くと、タスクボタンが表示されます。

- Single Sign-on Identity VerificationからSelf-Service Password Resetにセキュリティの質問を移行する際、**更新**をクリックしてもSelf-Service Password Resetコンソールに質問が表示されない場合があります。

  > 回避策: コンソールを閉じてから再度開きます。

- アンケートのセキュリティの質問に特殊文字 **&** が含まれている場合、StoreFront への登録中に表示されません。

  \[#654913\]

  > 回避策: セキュリティの質問に **&** を含めないでください。

- Windows Server 2012 に .Net Framework 4.5 のみがインストールされている環境でのアップグレードまたはアンインストール、および Windows Server 2016 に .Net Framework 4.6 のみがインストールされている環境でのアップグレードまたはアンインストールは失敗する可能性

があります。これは、Windows Server 2012 および Windows Server 2016 でのインプレースアップグレードまたはアンインストールが .Net Framework 3.5 に依存しているためです。回避策として、アップグレードまたはアンインストールの前に .Net Framework 3.5 をインストールしてください。

\[DNA-22761\]

システム要件

重要

Citrix® は、ドメインコントローラーへのセルフサービスパスワードリセットコンポーネントのインストールをサポートしていません。セルフサービスパスワードリセットコンポーネントは専用サーバーに展開してください。

この記事では、セルフサービスパスワードリセット環境のハードウェアおよびソフトウェア要件について説明します。この記事は、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

セルフサービスパスワードリセット環境のコンピューターには、以下のサポートシステムソフトウェアが必要になる場合があります。

- **Windows 2016 および Windows 2012 R2** - セルフサービスパスワードリセットサーバーで必要です。
- **Microsoft Windows Installer 2.0 以降** - すべてで必要です。
- **Microsoft .NET Framework** - セルフサービスパスワードリセットサーバーで必要です。
  - 4.6.x (ウィンドウズ 2016)
  - 4.5.2 (ウィンドウズ 2012 R2)
- **Internet Information Services (IIS)** - セルフサービスパスワードリセットサーバーで必要です。
  - IIS 10.0 (ウィンドウズ 2016)
  - IIS 8.5 (ウィンドウズ 2012 R2)
- **VC++ 2008 SP1 ランタイム** - セルフサービスパスワードリセットサーバーで必要です。

初回インストールの場合、`<https://www.microsoft.com/ja-jp/download/details.aspx?id=26368>` から vcredist_x86.exe をダウンロードし、セルフサービスパスワードリセットサーバーにインストールする必要があります。

セルフサービスパスワードリセットサーバー

- セルフサービスパスワードリセットコンポーネント - 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30 KBのディスク容量

ASP.NET 3.5/4.X の要件

Windows Server コンピューター上の .NET Framework のバージョンに対応する ASP.NET コンポーネント。

セキュリティとアカウントの要件

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、サービスをサポートするために適切なアカウントとコンポーネントが利用可能であることを確認してください。また、このサービスはセキュアHTTP (HTTPS) を使用するため、StoreFront との Transport Layer Security (TLS) 通信にはサーバー認証証明書が必要です。

サーバー認証の要件:

サービスをインストールする前に、利用可能な場合は、証明機関 (CA) または社内の公開鍵インフラストラクチャ (PKI) から TLS 通信用のサーバー認証証明書を取得してください。

サービスモジュールに必要なアカウント:

注: 両方のアカウントが期限切れにならないようにしてください。

セルフサービスパスワードリセットサービスは、環境内で動作する際にデータを読み書きするために、次のアカウントタイプを必要とします。

- データプロキシアカウント
- セルフサービスアカウント

異なるモジュールが同じタイプのアカウントを必要とする場合、複数のモジュールで同じアカウントを使用できます。または、各モジュールに異なるカスタマイズされたアカウントを指定することもできます。

- **データプロキシアカウント**

中央ストアへの読み取りおよび書き込みアクセスが必要です。詳細については、「インストールと構成」の「**中央ストアの作成**」セクションを参照してください。

- **セルフサービスアカウント**

ユーザー構成で関連するユーザーのパスワードのロック解除とリセットを行うための十分な権限が必要です。詳細については、セキュアな構成を参照してください。

StoreFront

- StoreFront 3.7〜1912

シトリックス ワークスペース™ アプリ

サポート対象:

- Citrix Workspace アプリ Web用
- Windows版 Citrix Workspaceアプリ
- Linux向け Citrix Workspace アプリ
- Citrix Workspaceアプリ for Mac (StoreFront 3.8が必要です)

サポート対象外:

- Chrome向けCitrix Workspaceアプリ
- モバイルデバイス (Citrix Workspaceアプリ for Webを使用してもサポートされません)

Citrix Gatewayとの外部での使用

サポートされていません

インストールと構成

インストールチェックリスト

インストールを開始する前に、次のリストを完了してください。

✓	ステップ
	ソフトウェアをインストールする環境内のコンピューターを選択し、インストール用に準備します。「システム要件」を参照してください。
	TLS証明書とサービスに必要なアカウントをインストールします。「システム要件」の「**セキュリティとアカウントの要件**」を参照してください。
	ライセンスサーバーをバージョン11.13.1.2以降にインストールまたは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>`からダウンロードしてください。詳しくは、「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。

インストールと構成の順序

Citrix®では、セルフサービスパスワードリセットを次の順序でインストールすることをお勧めします。

1. セントラルストアを作成します。「セントラルストアの作成」を参照してください。
2. セルフサービスパスワードリセットをインストールします。サービスをインストールしてサービス構成ウィザードを実行するには、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。詳しくは、「セルフサービスパスワードリセットのインストールと構成」を参照してください。

3. コンソールを使用してセルフサービスパスワードリセットを構成します。「セルフサービスパスワードリセットのインストールと構成」を参照してください。
4. StoreFrontでセルフサービスパスワードリセットを構成します。「StoreFrontの構成」を参照してください。
5. セルフサービスパスワードリセットの構成が安全に設定されていることを確認します。「安全な構成」を参照してください。

セントラルストアを作成する

セキュリティ上の理由から、セントラルストアは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に直接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が必要な展開では、セルフサービスパスワードリセットサーバーと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場合、セントラルストアをリモートネットワーク共有でホストできます。

この機能は、Windows Server 2012 R2 または Windows Server 2016 でのみ利用可能です。

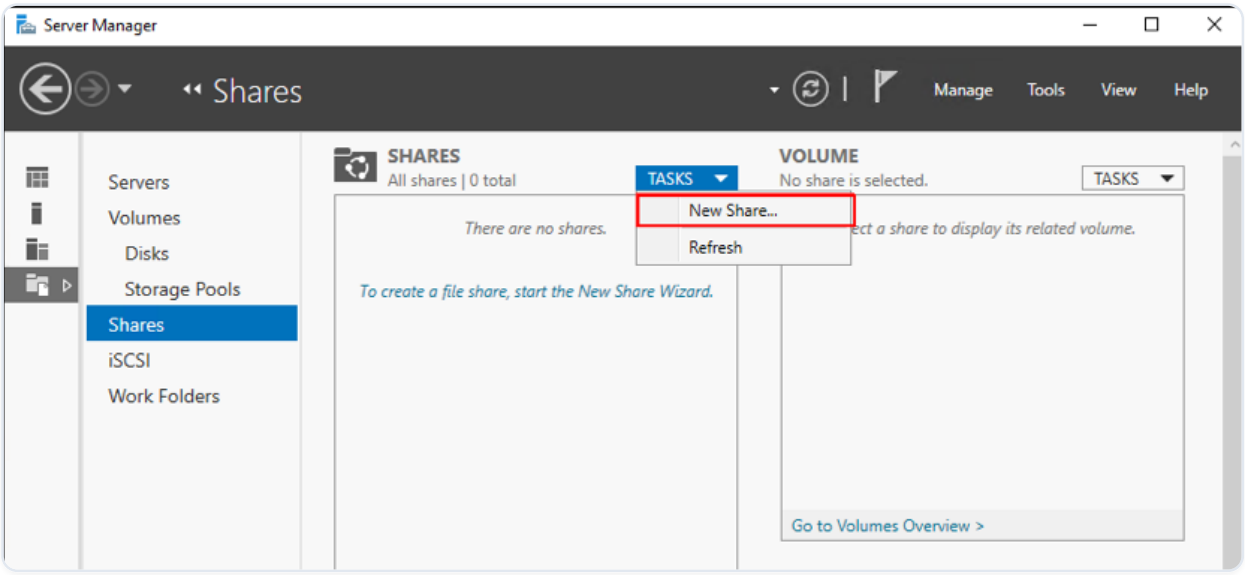
データプロキシアカウントの作成

データプロキシアカウントとして使用する通常のドメインユーザーを作成します。ドメイン管理者/ローカル管理者グループのユーザーをデータプロキシアカウントとして設定しないでください。

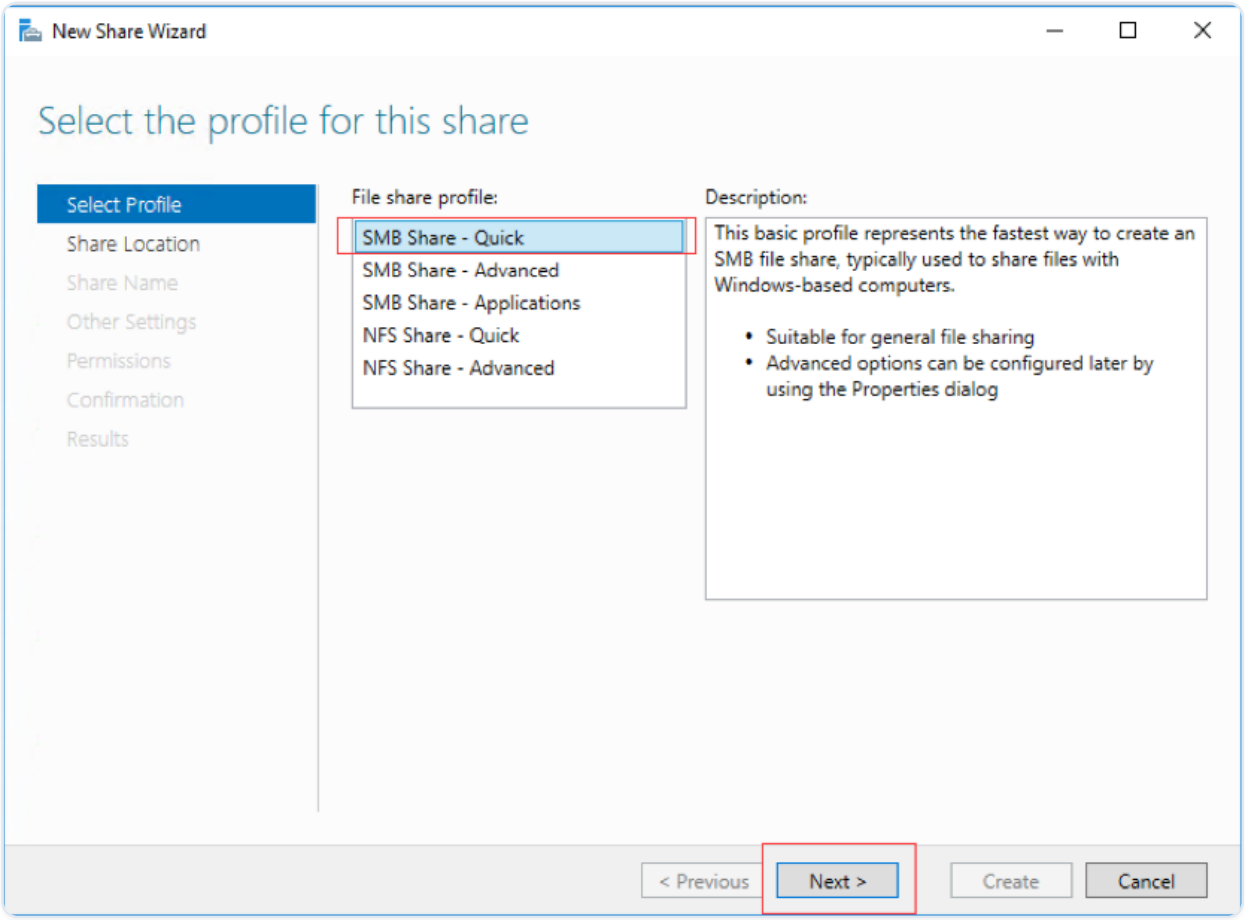
Windows Server 2012 R2 または Windows Server 2016 用のセントラルストアを作成する

セルフサービスパスワードリセットサーバーとセントラルストアの両方にWindows Server 2012 R2またはWindows Server 2016を使用する場合、このセクションで説明されているように構成されていれば、リモートネットワーク共有を使用できます。**データアクセスを暗号化**が選択されていることを確認し、セキュアな構成で示されているガイダンスを適用してください。

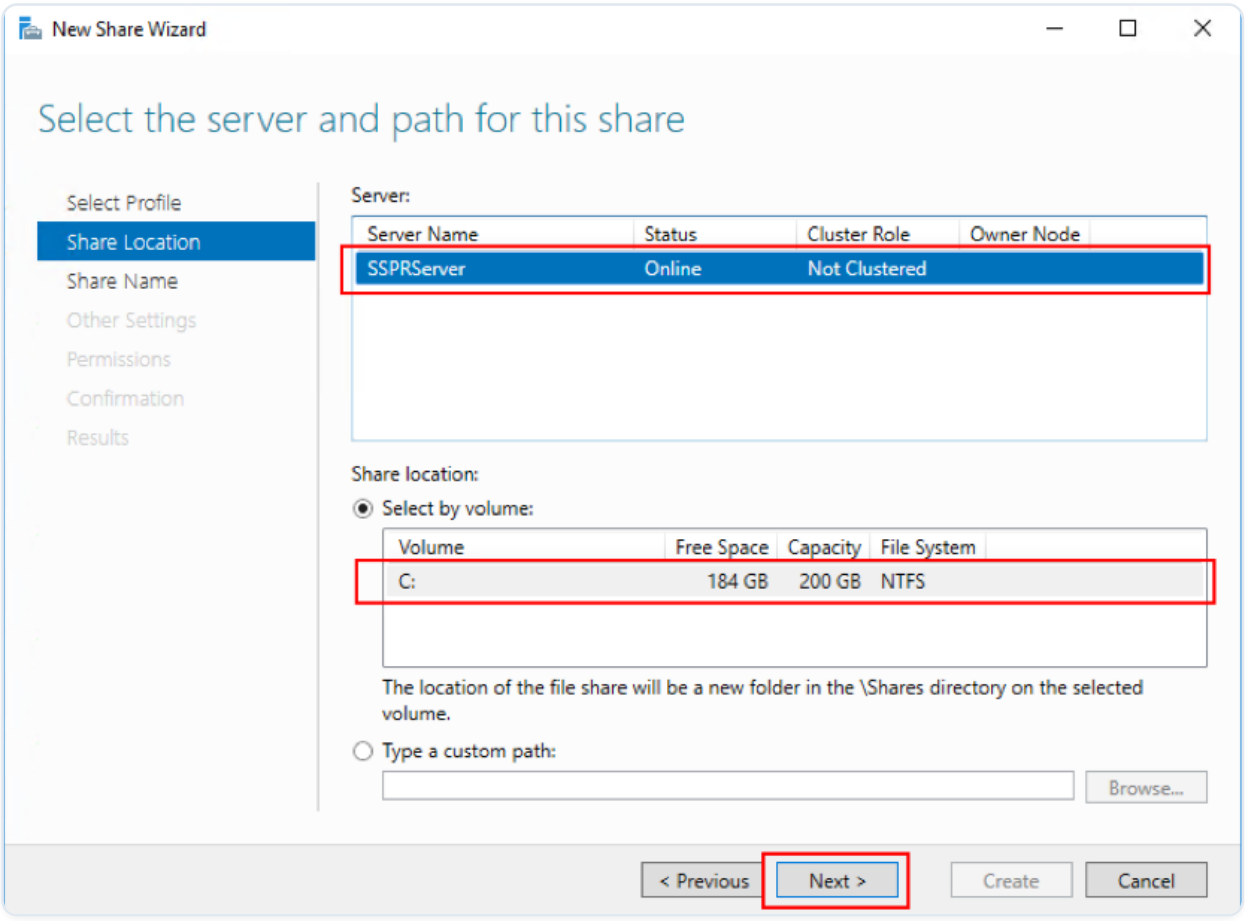
1. **新しい共有**ウィザードを開始するには、サーバーマネージャーを開きます。**ファイルサービスと記憶域サービス**の詳細ページから、左ペインで**共有**を選択し、**タスク \> 新しい共有**をクリックします。



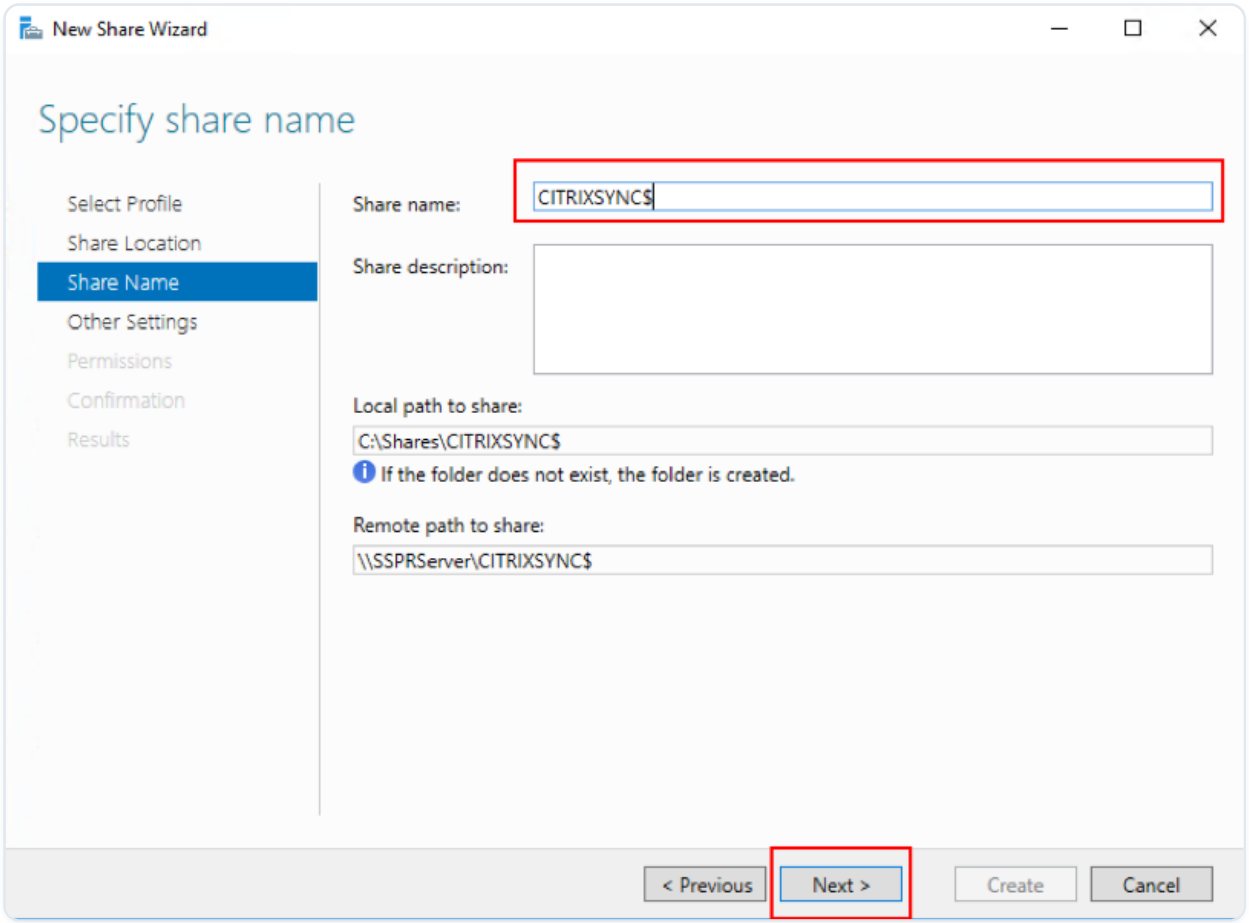
2. 左ペインで**プロファイルの選択**を選択し、**SMB 共有 - クイック**を選択して、**次へ**をクリックします。



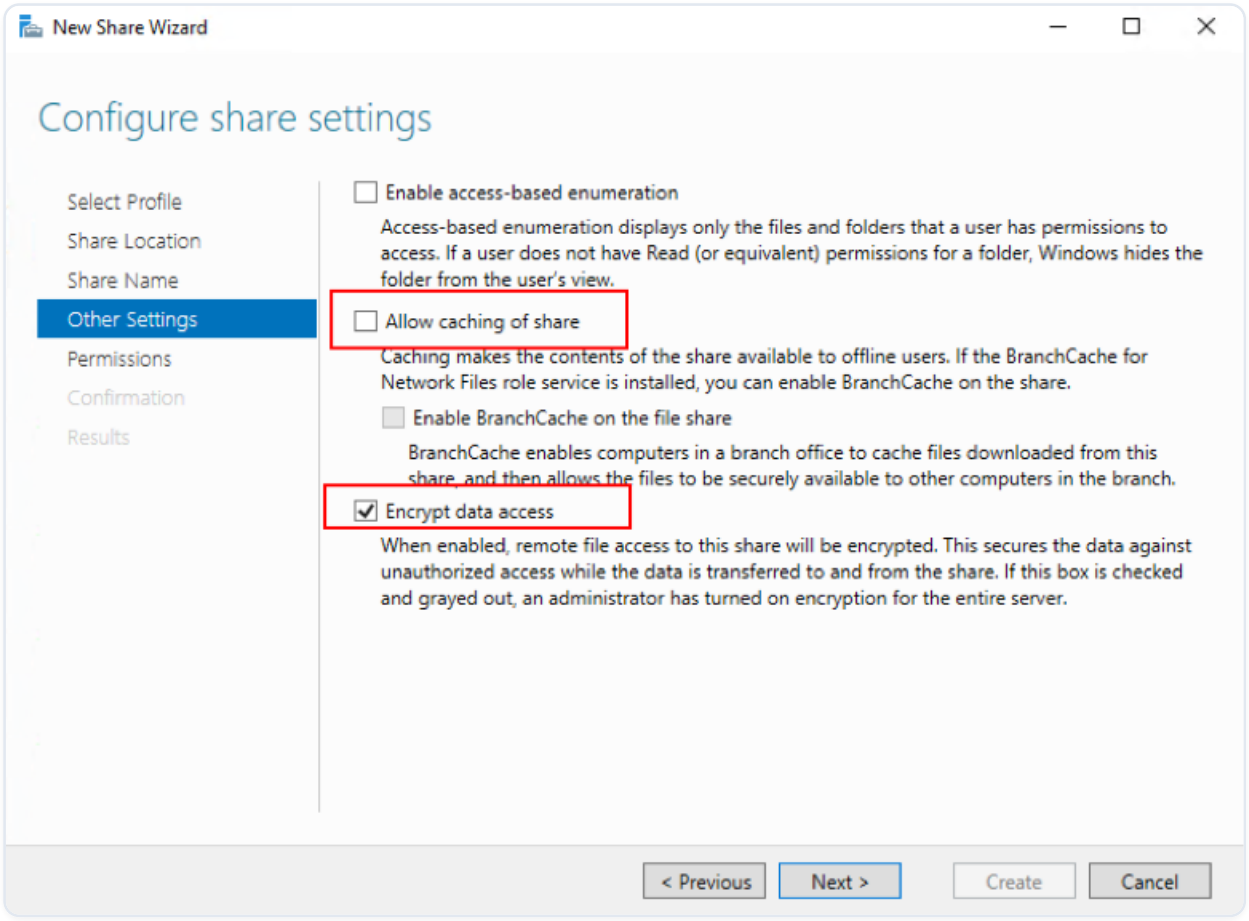
3. 左ペインで**共有の場所**を選択します。リストから、新しい共有を作成するサーバーと、新しい共有フォルダーを作成するボリュームを選択し、**次へ**をクリックします。



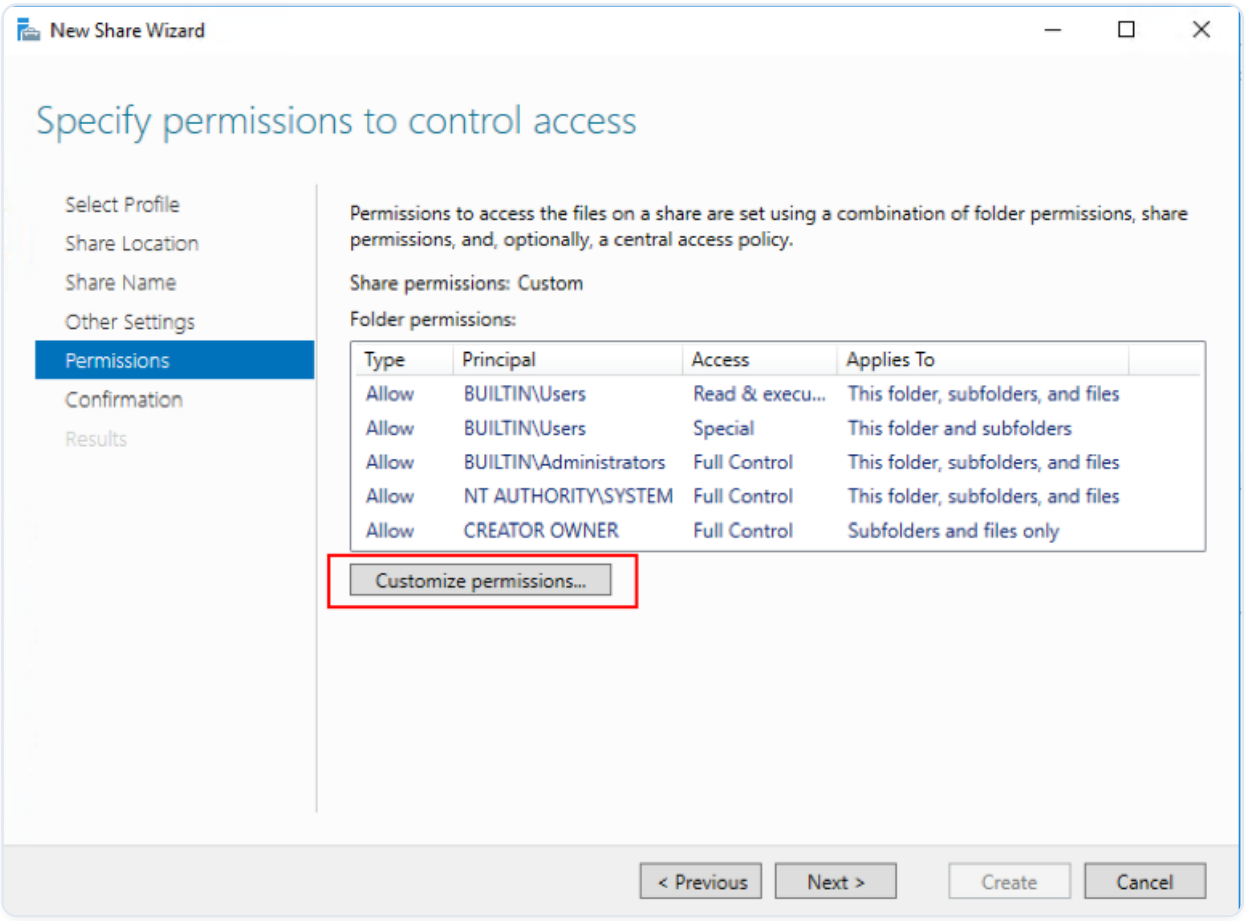
4. 左ペインで**共有名**を選択し、新しい共有名（例: **CITRIXSYNC$**）を入力して、**次へ**をクリックします。



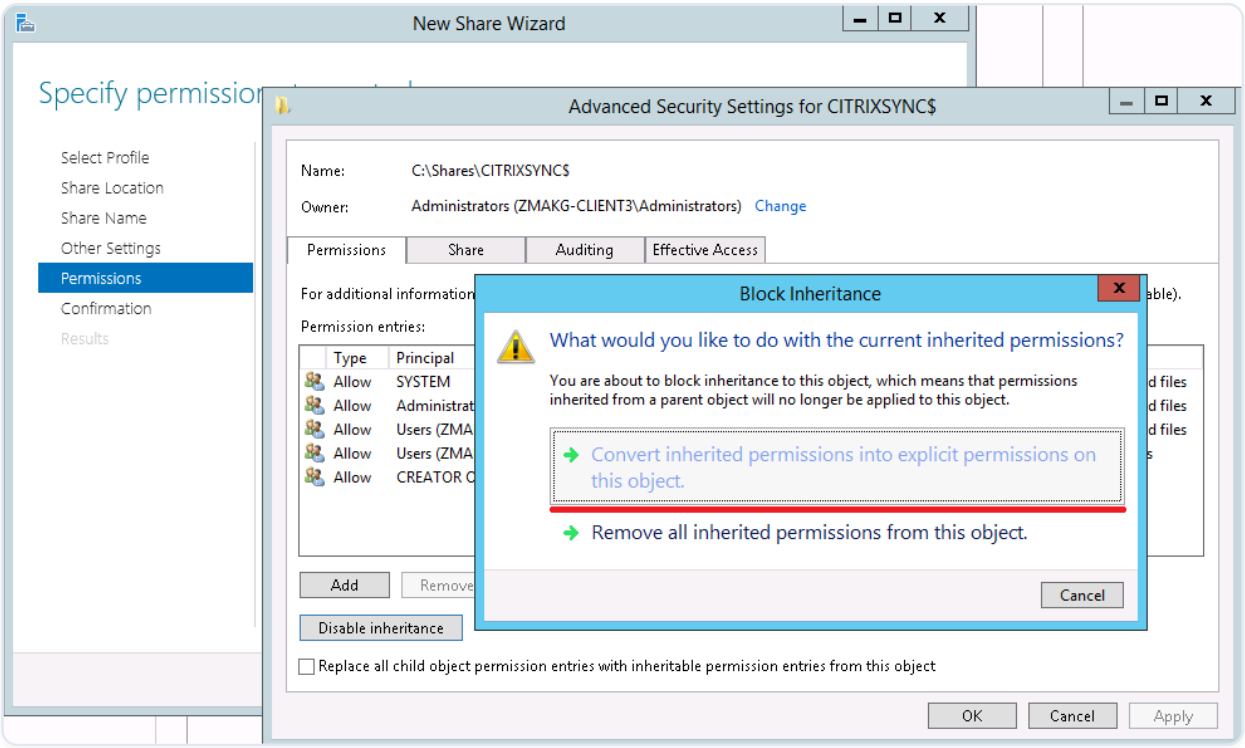
5. 左ペインで**その他の設定**を選択し、**データを暗号化**を選択し、**共有のキャッシュを許可する**の選択を解除して、**次へ**をクリックします。



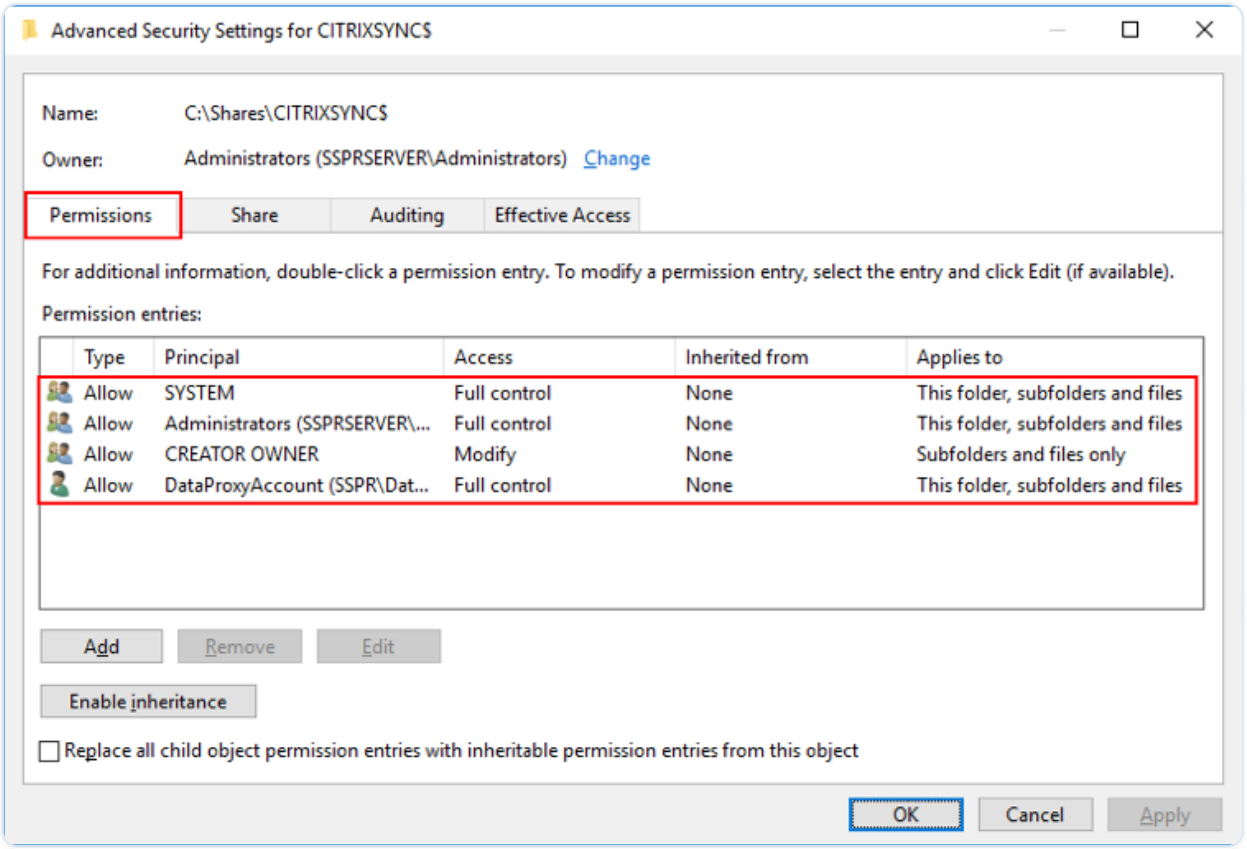
6. **共有**アクセス許可をカスタマイズするには、左ペインで**アクセス許可**を選択し、**アクセス許可のカスタマイズ \> 共有**を選択します。



7. NTFSアクセス許可をカスタマイズするには、**継承を無効にする**をクリックし、**このオブジェクトの継承されたアクセス許可を明示的なアクセス許可に変換する**を選択します。

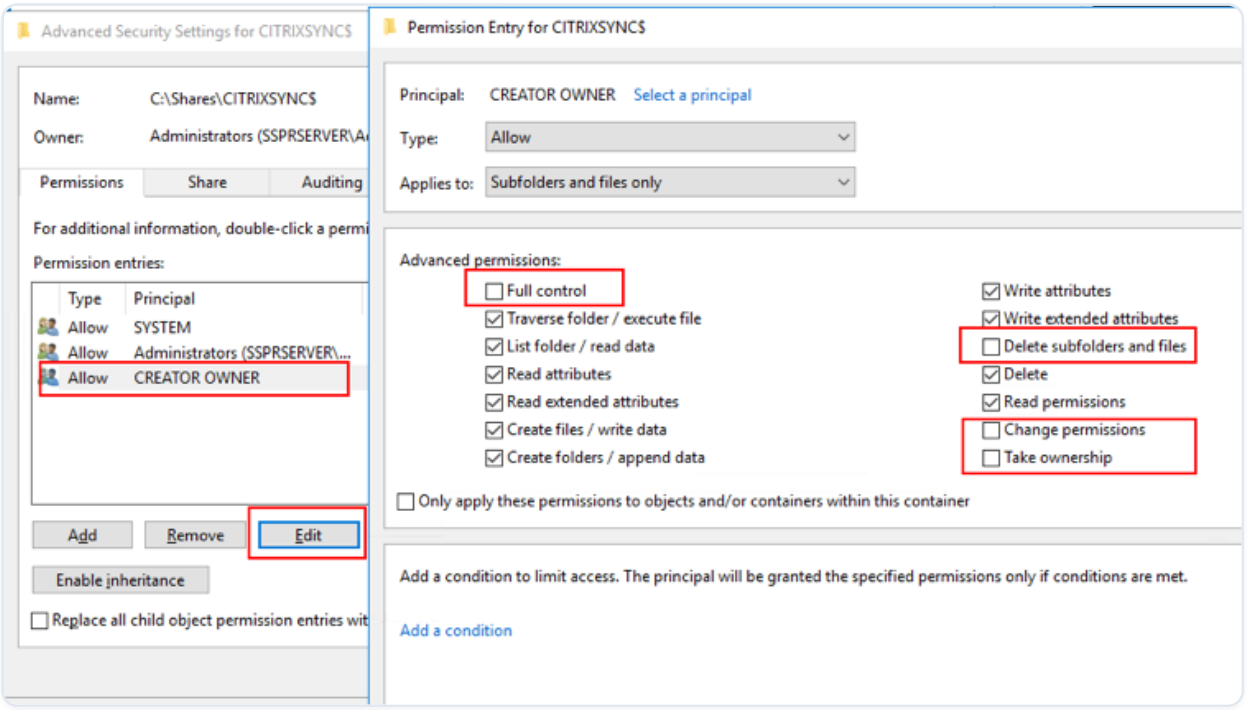


8. **アクセス許可**タブをクリックし、**CREATOR OWNER**、**ローカル管理者**、および**SYSTEM**を除くすべてのユーザーを削除して、フルコントロールアクセス許可で作成されたデータプロキシアカウントを追加します。

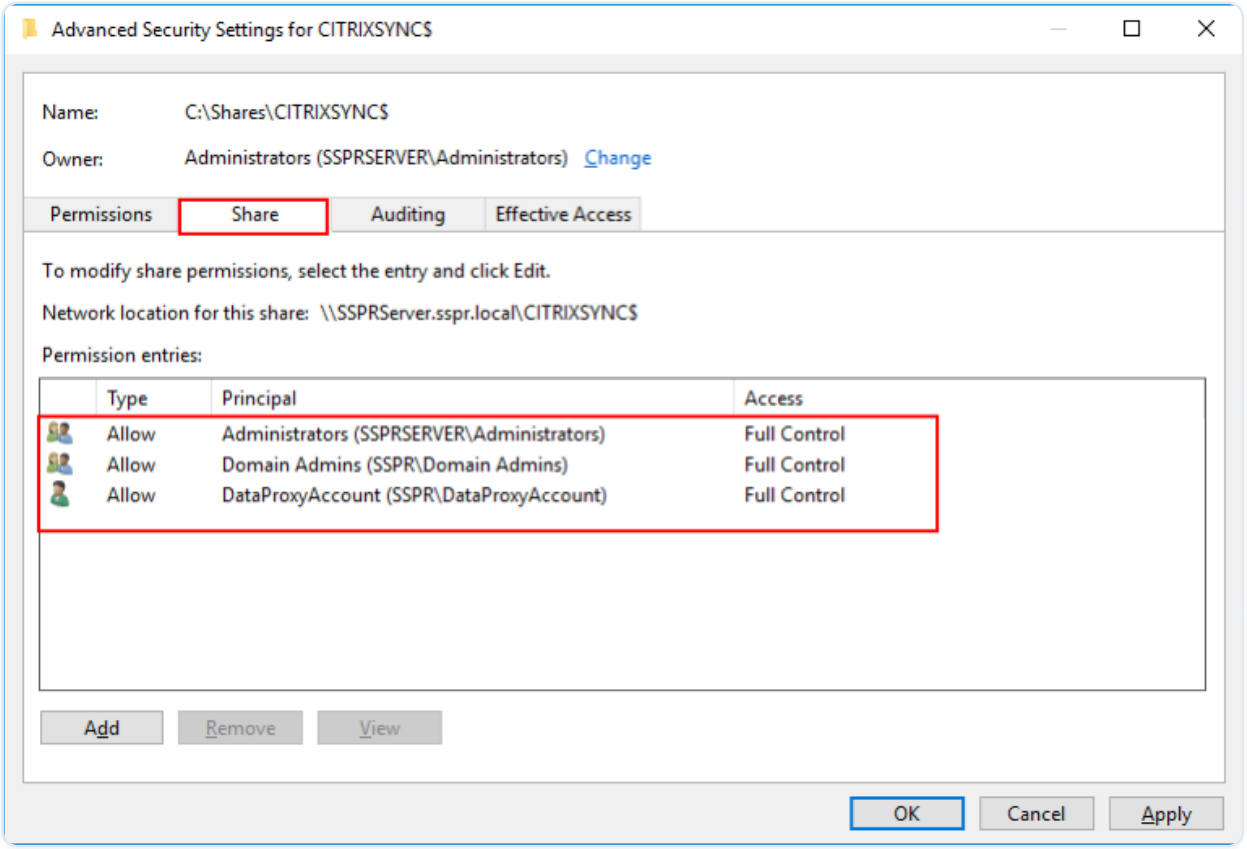


9. **CREATOR OWNER**を選択し、**編集**をクリックして、次のアクセス許可のチェックを外します。

   - フルコントロール
   - サブフォルダーとファイルを削除する
   - アクセス許可を変更する
   - 所有権を取得する



10. **共有**タブを選択し、**Everyone**を削除して、データプロキシアカウント、ローカル管理者、およびドメイン管理者をフルコントロールアクセス許可で追加します。



11. 新しい共有ウィザードの左ペインで**確認**を選択し、共有のために現在選択されている設定を確認して、**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、その後**閉じる**をクリックします。

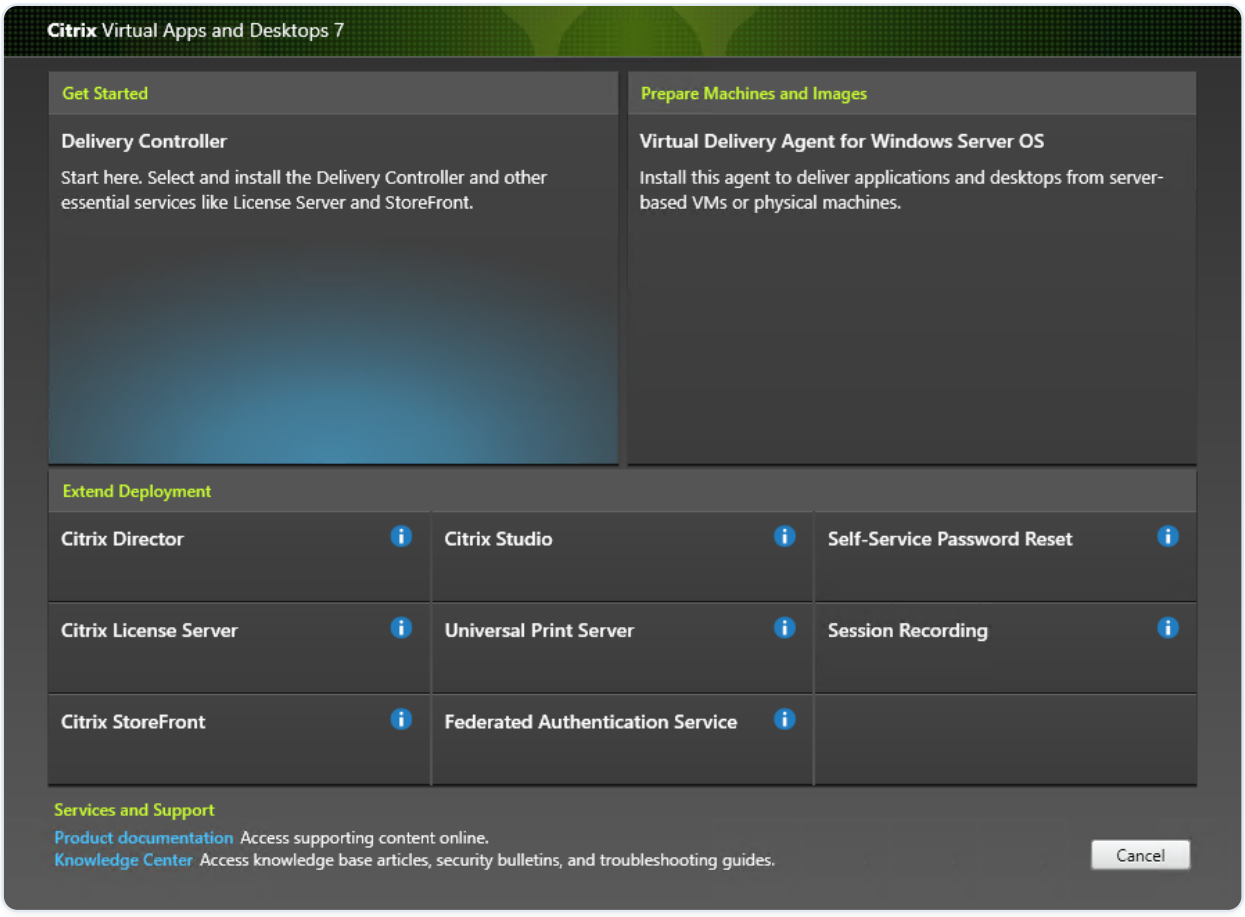
12. **CITRIXSYNC$** 共有フォルダーの下に、**CentralStoreRoot**と**People**の2つのサブフォルダーを作成します。

重要: Data Proxy Account にこれら 2 つのサブフォルダーに対する **フルコントロール** があることを確認してください。

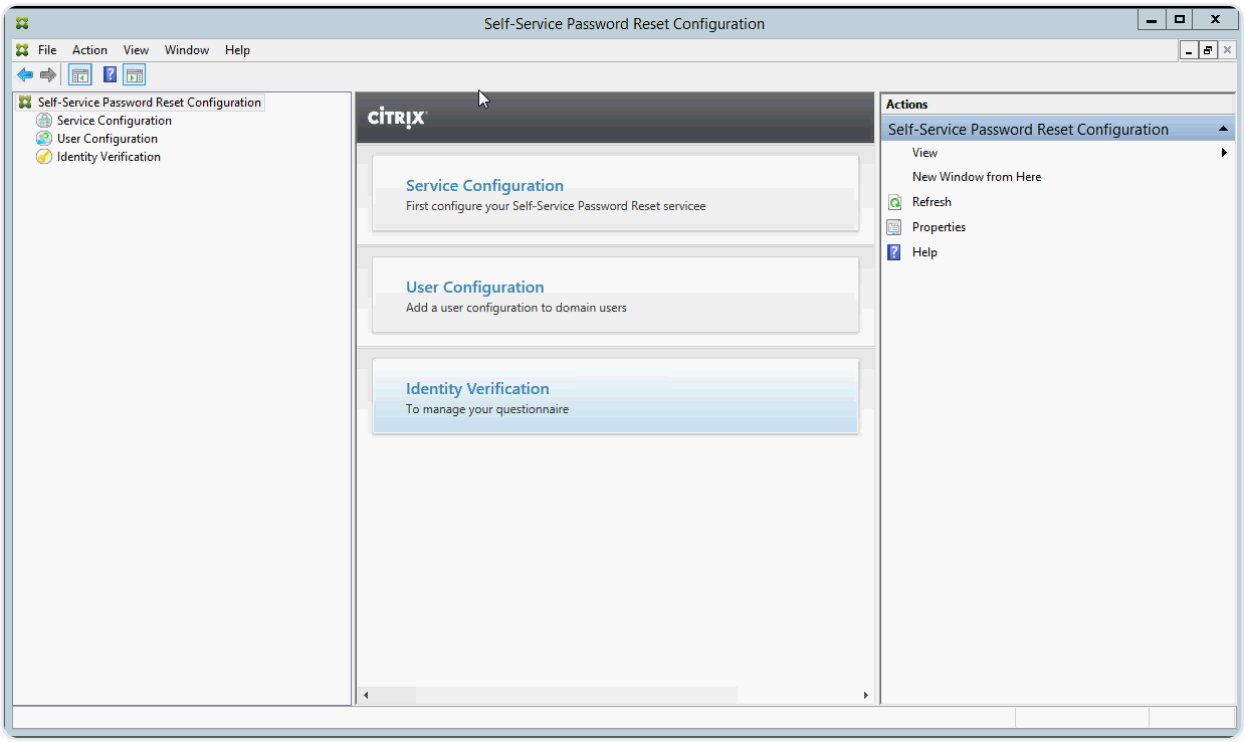
Self-Service Password Reset のセントラルストアに対して、EncryptData、RejectUnencryptedAccess、および RequireSecuritySignature を構成する必要があります。その他の構成情報については、以下の Microsoft の記事を参照してください: `<https://docs.microsoft.com/ja-jp/powershell/module/smbshare/set-smbserverconfiguration>` `<https://docs.microsoft.com/ja-jp/powershell/module/smbshare/set-smbshare>`

Self-Service Password Reset のインストールと構成

1. Citrix Virtual Apps and Desktops™ インストーラーを使用して Self-Service Password Reset をインストールします。



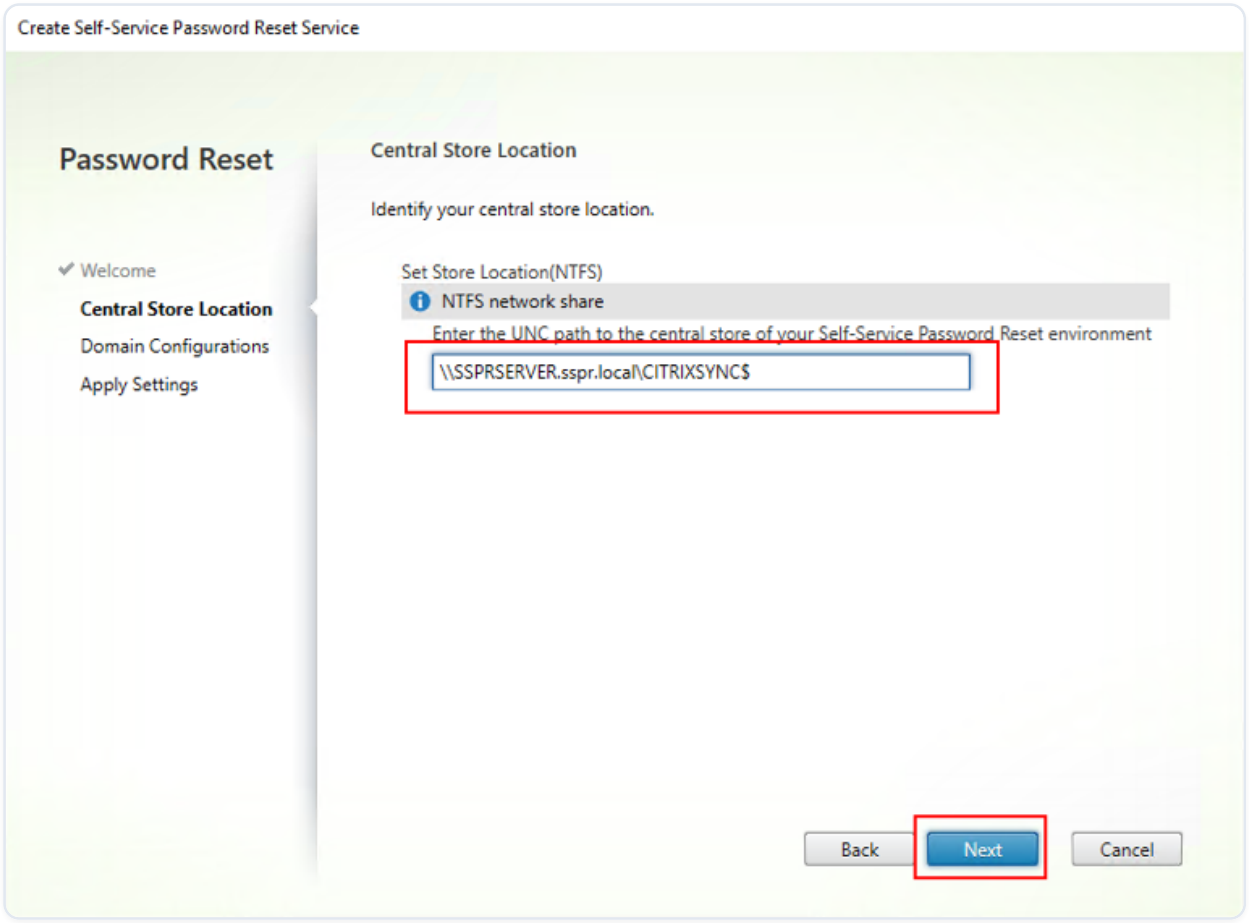
2. セルフサービスパスワードリセットのインストール後、Citrix セルフサービスパスワードリセットサービスを構成するには、**［スタート］\>［すべてのプログラム］\>［Citrix］\>［Citrix セルフサービスパスワードリセット構成］** をクリックします。
3. コンソールが開いたら、これら 3 つの基本的な手順に従ってサービスを構成します。



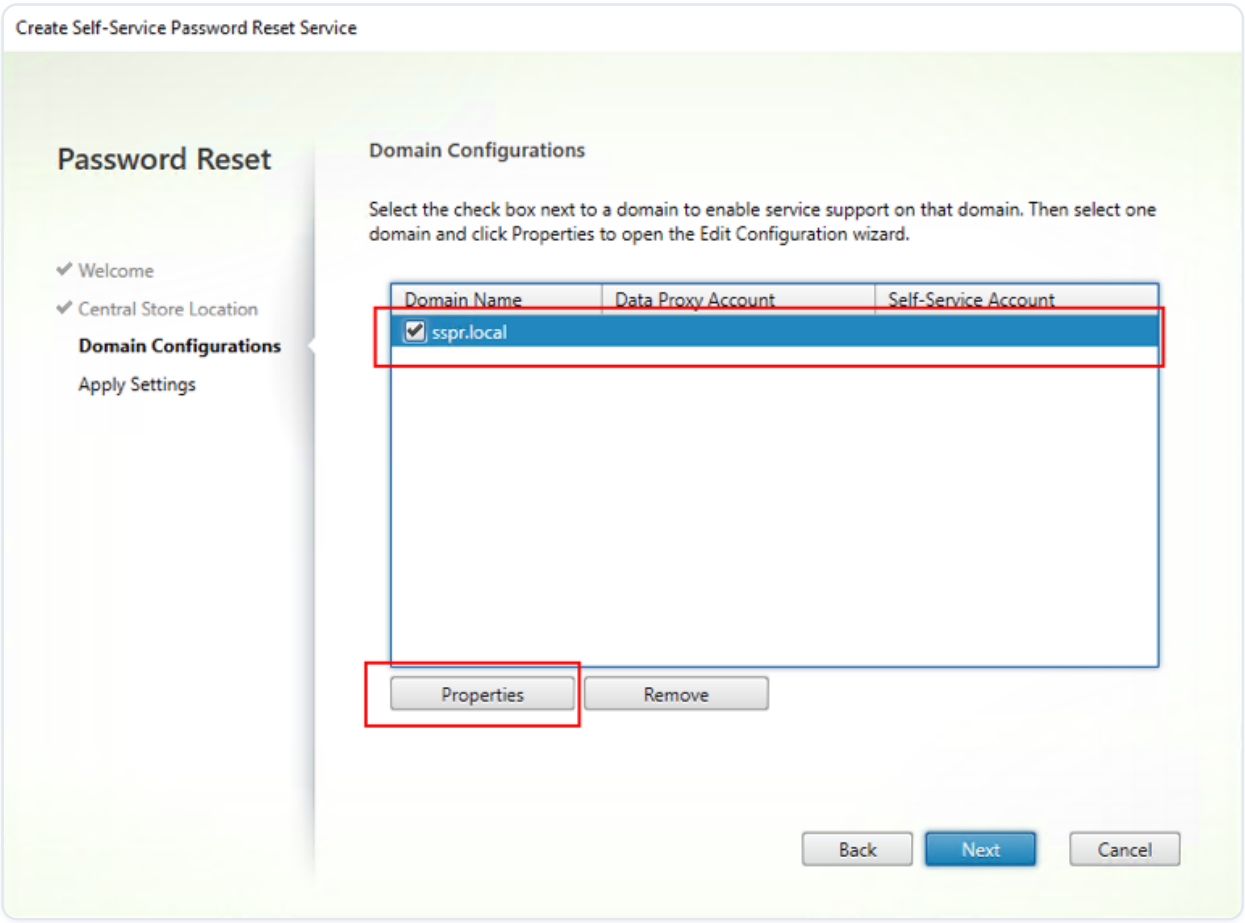
サービス構成

サービスを構成する前に、セントラルストア、Data Proxy Account、およびセルフサービスアカウントを作成していることを確認してください。

1. 中央ペインで **［サービス構成］** を選択し、右ペインで **［新しいサービス構成］** をクリックします。
2. **［セントラルストアの場所］** 画面で、セントラルストアの場所を指定し、**［次へ］** をクリックします。



3. **［ドメイン構成］** 画面で、Self-Service Password Reset サービスを有効にするドメインを選択し、**［プロパティ］** をクリックします。



4. 「**Data Proxy Account**」のユーザー名とパスワード、「**Self-Service Account**」のユーザー名とパスワードを指定し、「**OK**」をクリックします。

   ユーザー名とパスワードを指定する画像(/en-us/self-service-password-reset/current-release/media/passwords.png)

5. 「**次へ**」をクリックして、すべての設定を適用します。

   すべての設定を適用する画像(/en-us/self-service-password-reset/current-release/media/to-apply-all-the-settings.png)

6. 「**完了**」をクリックして、設定を完了します。

   完了をクリックする画像(/en-us/self-service-password-reset/current-release/media/click-finish.png)

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「**新規ユーザー設定**」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ターゲットユーザーグループを定義し、Active Directoryからユーザー/グループ/OUを追加して、「**次へ**」をクリックします。

ユーザー設定の画像(/en-us/self-service-password-reset/current-release/media/user-configuration.png)

3. 「**ライセンスの構成**」画面で、ライセンスサーバーを指定し、「**次へ**」をクリックします。

   ライセンス設定の画像(/en-us/self-service-password-reset/current-release/media/licensing-configuration.png)

4. 「**セルフサービスパスワードリセットの有効化**」画面で、チェックボックスを使用して、ユーザーが管理者の介入なしにWindowsパスワードをリセットし、ドメインアカウントのロックを解除できるかどうかを指定し、サービスポートとアドレスを指定してから、「**作成**」をクリックします。

   パスワードリセットを有効にする画像(/en-us/self-service-password-reset/current-release/media/enable-password-reset.png)

ユーザー設定の管理の詳細については、「ユーザー設定の管理」を参照してください。

ID検証

1. 左ペインで**ID検証**ノードを選択し、次に、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質問の回答のマスクを有効または無効にし、**次へ**をクリックします。
3. **セキュリティ質問**画面で、**質問の追加**をクリックし、テキストボックスに質問を入力し、**OK**をクリックし、次に**次へ**をクリックします。
4. **アンケート**画面で、**追加**をクリックし、質問を選択します。**上に移動**ボタンと**下に移動**ボタンを使用して、質問とグループを再編成できます。このページでの作業が完了したら、**作成**と**OK**をクリックします。

ID検証の質問の管理の詳細については、「ID検証の質問の管理」を参照してください。

ユーザー構成の管理

ユーザー構成を使用すると、ユーザーがStorefrontにログオンしたときのインターフェイスの動作と外観を制御できます。新しい構成を作成することは、Self-Service Password Resetを環境内のユーザーに配布する前の最後のステップです。既存のユーザー構成はいつでも編集できます。

ユーザー構成は、Active Directory階層（組織単位 \[OU\] または個々のユーザー）またはActive Directoryグループに関連付けられたユーザーに適用する、設定の一意のコレクションです。

ユーザー構成は、次の要素で構成されます。

- Active Directoryドメイン階層（OUまたは個々のユーザー）またはActive Directoryグループに関連付けられたユーザー

重要: Active Directory混合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（アカウントロック解除とパスワードリセット）

ユーザー構成を作成する前に、次のものがすでに作成または定義されていることを確認してください。

- セントラルストア
- サービス構成

ユーザー構成を作成するには：

1. **Start** > **すべてのプログラム** > **Citrix** > **Citrix Self-Service Password Reset Configuration** をクリックします。
2. 左側のペインで、**ユーザー構成**ノードを選択します。
3. **操作**メニューから、**新しいユーザー構成の追加**をクリックします。

ユーザー、OU、またはグループを追加するには：

ユーザー構成ウィザードの**ユーザー構成の名前**ページでは、ユーザー構成をユーザーに関連付けることができます。

ユーザー構成の関連付け：

Active Directory階層（OUまたは個々のユーザー）またはActive Directoryグループに従ってユーザーを関連付けるという2つの選択肢があります。必要に応じて、後で**操作**メニューの**ユーザー構成の編集**をクリックして、ユーザー構成を別の階層またはグループに関連付けることができます。

ユーザー構成をグループに関連付けることは、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。

ユーザー構成の名前ページ（新しいユーザー構成の追加またはユーザー構成の編集ウィザードから）で、OU、ユーザー、またはグループを選択します。

注： 特権アカウント（たとえば、ローカル管理者やドメイン管理者）を、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のグループに含めないことをお勧めします。新しい専用グループを使用してください。

ライセンスを構成するには：

ユーザー構成ウィザードの**ライセンスの構成**ページでは、セルフサービスパスワードリセットサービスで使用されるライセンスサーバーを構成できます。

注： ロック解除機能とリセット機能は、Citrix Virtual AppsまたはCitrix Virtual Desktops™ Platinum Editionをお持ちの場合にのみ使用できます。

「**ライセンス設定**」ページ（新規ユーザー構成の追加ウィザードまたはユーザー構成の編集ウィザードから）で、ライセンスサーバー名とポート番号を入力します。

ロック解除またはリセット機能を有効にするには：

セルフサービスパスワードリセットを使用すると、管理者の介入なしに、ユーザーはWindowsパスワードをリセットし、ドメインアカウントのロックを解除できます。「**セルフサービスパスワードリセットを有効にする**」ページから、有効にする機能を選択できます。

「**セルフサービスパスワードリセットを有効にする**」ページ（新規ユーザー構成の追加ウィザードまたはユーザー構成の編集ウィザードから）で、ユーザーに使用させる機能（**ロック解除**または**リセット**）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。ブラックリスト内のユーザーとグループは、登録、アカウントのロック解除、パスワードのリセットなど、セルフサービスパスワードリセットのどの機能も使用できません。また、ブラックリスト内のユーザーは、ログオン後にCitrix Workspace™アプリの**TASK**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 Self-Service Password Reset Configuration］** の順にクリックします。
2. 左ペインで**［ユーザー構成］** を選択し、右ペインで**［ブラックリスト構成］** をクリックします。
3. **［追加］** ボタンと**［削除］** ボタンを使用して、ユーザーまたは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したりします。

ID検証の質問を管理する

Citrix Self-Service Password Reset構成コンソールのID検証機能は、ID検証、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に関連するすべてのセキュリティの質問を管理す

るための一元的な場所を提供します。デフォルトの質問リストに独自のセキュリティの質問を追加したり、質問グループを作成したりできます。

- ユーザーが回答を登録した後に既存のデフォルトの質問を編集する場合は、編集された質問の意味を考慮してください。質問を編集しても、ユーザーの再登録は強制されません。ただし、質問の意味を変更すると、元々その質問に回答したユーザーは正しい回答を提供できなくなる可能性があります。
- ユーザーが登録された後にセキュリティの質問を追加、削除、または置き換えると、以前の質問セットを使用して登録されたすべてのユーザーは、再登録するまで認証およびパスワードのリセットができなくなります。ユーザーは、Citrix Workspaceアプリでタスクを開いたときに、新しい質問セットに回答する必要があります。
- 個々のセキュリティの質問は、複数のセキュリティの質問グループに属することができます。セキュリティの質問グループを作成すると、作成したすべての質問が任意のセキュリティの質問グループで使用できるようになります。

以下の手順で参照されている設定にアクセスするには、次の手順を使用します。

1. **スタート** > **すべてのプログラム** > **Citrix** > **Citrix Self-Service Password Reset Configuration** をクリックします。
2. 左ペインで、**Identity Verification** ノードを選択します。
3. **Actions** メニューから、**Manage Questions** をクリックします。

既定の言語を設定するには:

ほとんどの場合、ユーザーは現在のユーザープロファイルに関連付けられた言語でセキュリティの質問が表示されます。その言語が利用できない場合、Self-Service Password Reset は指定された既定の言語で質問を表示します。

1. **スタート** > **すべてのプログラム** > **Citrix** > **Citrix Self-Service Password Reset Configuration** をクリックします。
2. 左ペインで、**Identity Verification** ノードを選択します。
3. **Actions** メニューから、**Manage Questions** をクリックします。
4. **Question-Based Authentication** ページの **Default Language** ドロップダウンリストから、既定の言語を選択します。

セキュリティ回答のマスクを有効にするには:

セキュリティ回答のマスクは、ユーザーがセキュリティの質問の回答を登録するとき、または本人確認中に回答を提供するときに、セキュリティの追加レベルを提供します。この機能が有効になっ

ている場合、ユーザーの回答は非表示になります。回答登録プロセス中、これらのユーザーは入力ミスやスペルミスを避けるために回答を2回入力するように求められます。本人確認中は、エラーがあった場合に再試行を促されるため、ユーザーは回答を1回だけ入力します。

「**質問ベース認証**」ページで、「**セキュリティ質問の回答をマスクする**」を選択します。

新しいセキュリティの質問を作成するには:

多数の異なる質問を作成し、各質問に言語を指定できます。また、1つの質問に対して複数の翻訳を提供することもできます。Citrix Workspace アプリでの登録では、ユーザーのプロファイルの言語設定に対応する言語でアンケートがユーザーに提示されます。その言語が利用できない場合、Self-Service Password Reset は既定の言語で質問を表示します。

注: セキュリティ質問の言語を指定すると、その指定された言語にオペレーティングシステムの設定が構成されているユーザーに質問が表示されます。選択されたオペレーティングシステムの設定が利用可能な質問のいずれとも一致しない場合、ユーザーには選択されたデフォルト言語が表示されます。

1. **セキュリティ質問**ページで、**言語**ドロップダウンリストから言語を選択し、**質問の追加**をクリックします。セキュリティ質問ダイアログボックスが表示されます。
2. **セキュリティ質問**ダイアログボックスで新しい質問を作成します。

重要: 既存の質問の翻訳されたテキストを含めるには、**編集**ボタンを使用します。**質問の追加**を選択すると、元の質問に関連付けられていない新しい質問が作成されます。

既存の質問のテキストを追加または編集するには:

ユーザーが登録された後にセキュリティ質問を追加、削除、または置き換えると、以前の質問セットを使用して登録されたすべてのユーザーは、再登録するまで認証およびパスワードのリセットができなくなります。ユーザーはCitrix Workspaceアプリでタスクを開くときに、新しい質問セットに回答する必要があります。質問を編集しても、ユーザーの再登録は強制されません。

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。これにより、再認証時にユーザーの回答が一致しなくなる可能性があります。つまり、ユーザーが保存された回答と一致しない異なる回答を提供する可能性があります。

1. **セキュリティ質問**ページで、**言語**ドロップダウンボックスから言語を選択します。
2. 質問を選択し、**編集**をクリックします。
3. **セキュリティ質問**ダイアログボックスで質問を編集します。

セキュリティ質問グループを作成するには:

ユーザーが本人確認のために回答するセキュリティ質問を作成できます。アンケートに追加する各質問には、ユーザーが回答する必要があります。ただし、これらの質問をセキュリティ質問グループにまとめることもできます。

たとえば、質問をグループにまとめることで、6つの質問のグループをアンケートに追加し、ユーザーがその質問グループから選択して、たとえば6つのうち3つに回答できるようにします。これにより、ユーザーは本人確認に使用する質問の選択と回答の提供において柔軟性が得られます。

1. **セキュリティ質問**ページで**グループの追加**をクリックします。
2. **セキュリティ質問グループ**ダイアログボックスで、グループに名前を付け、質問を選択し、ユーザーが回答する必要がある質問の数を設定します。

セキュリティ質問グループを編集するには：

編集するセキュリティグループを選択し、**セキュリティ質問**ページで**編集**をクリックします。セキュリティ質問グループダイアログボックスが表示され、グループの一部として利用可能なセキュリティ質問のリストが表示されます。現在グループに含まれている質問にはチェックマークが付いています。ここでは、グループの名前を編集したり、グループに質問を追加したり、ユーザーが回答する必要があるこのグループからの質問の数を選択したりできます。

既存のアンケートを追加または削除するには：

アンケートからセキュリティ質問と質問グループを追加または削除します。ユーザーに提示される順序で質問を上下に移動します。アンケートが変更された場合は、Storefrontにログオンした後、ユーザーに再登録タスクを実行するよう通知します。

1. **アンケート**ページで**追加**をクリックして、質問またはグループをアンケートに追加します。
2. **削除**をクリックして、アンケートから質問を削除します。
3. **上に移動**または**下に移動**をクリックして、ユーザーに提示される質問を管理します。

セキュリティ質問をインポートまたはエクスポートするには：

セキュリティ質問とグループのデータをインポートまたはエクスポートできます。

1. **スタート** \> **すべてのプログラム** \> **Citrix** \> **Citrix Self-Service Password Reset Configuration**をクリックします。
2. 左ペインで、**ID検証**ノードを選択します。
3. **アクション**メニューから、次のいずれかをクリックします。

   セキュリティ質問をインポート セキュリティ質問とグループのデータをインポートするファイルの場所を指定します。

セキュリティ質問をエクスポート セキュリティ質問とグループのデータをエクスポートするファイルの場所を指定します。

安全な構成

この記事では、セルフサービスパスワードリセットコンポーネントが安全に展開および構成され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をリセットし、ユーザーアカウントのロックを解除するためのドメインユーザーアカウントを作成する
- ファイアウォール設定を構成する

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またはアカウントロック解除機能を使用している場合は、サービス構成中にセルフサービスモジュールがパスワードリセットとアカウントロック解除を実行するために使用するセルフサービスアカウントを指定します。アカウントには十分な権限があることを確認してください。ただし、本番環境の展開では、Domain Admins グループのアカウントを使用することはお勧めしません。推奨されるアカウント権限は次のとおりです。

- ドメインのメンバー
- 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およびアカウントロック解除の権限

Active Directoryユーザーとコンピューターで、ユーザーパスワードをリセットし、ユーザーアカウントのロックを解除する権限を持つ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、メニューから**制御の委任**をクリックします。
2. **制御の委任**ウィザードが表示されます。**ようこそ**ダイアログボックスで、**次へ**をクリックします。
3. **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。アカウントのロックを解除する権限を付与したいグループをリストから選択し、**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**をクリックし、**次へ**をクリックします。

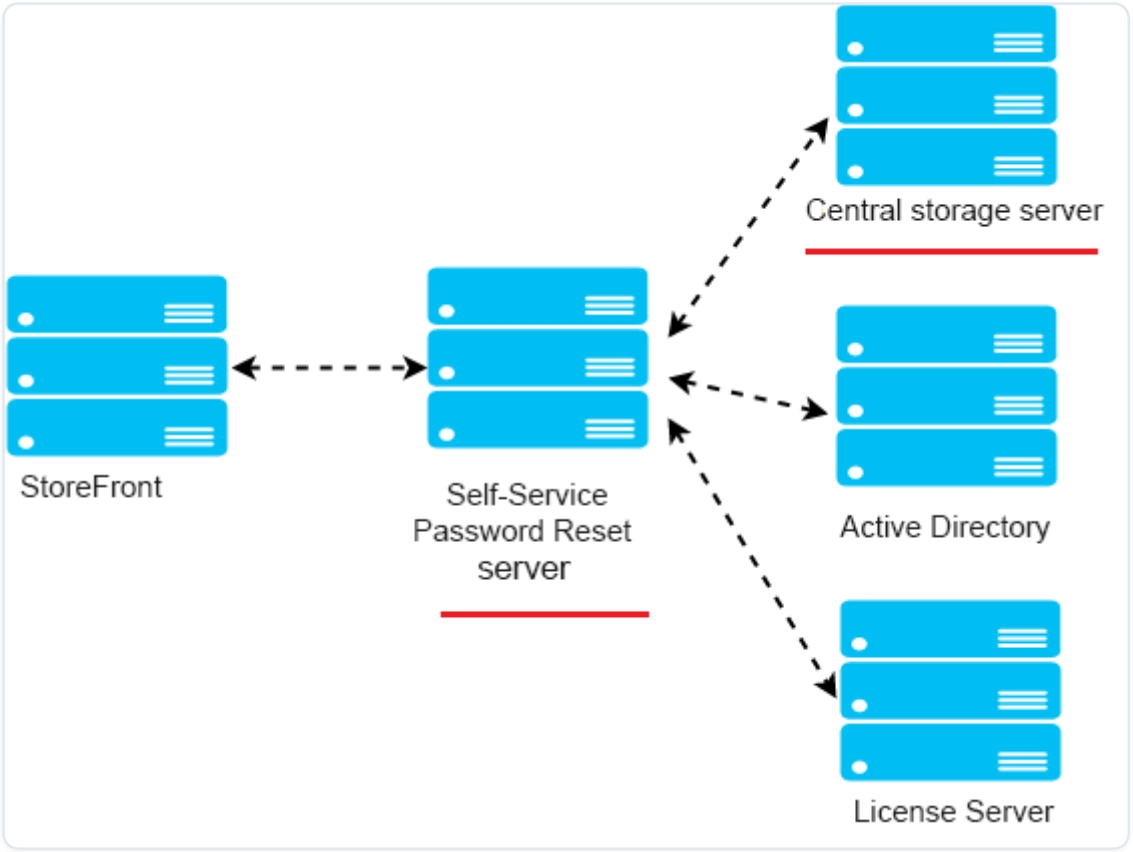
5. 「**Active Directoryオブジェクトの種類**」ダイアログボックスで、「フォルダー内の次のオブジェクトのみ \> ユーザーオブジェクト」をクリックし、**次へ**をクリックします。
6. 「**アクセス許可**」ダイアログボックスで、「**全般**」と「**プロパティ固有**」のチェックボックスをオンにします。「**アクセス許可**」リストで、「**lockoutTimeの読み取り**」、「**lockoutTimeの書き込み**」、「**パスワードのリセット、パスワードの変更、userAccountControlの読み取り、userAccountControlの書き込み、pwdLastSetの読み取り、およびpwdLastSetの書き込み**」のチェックボックスをオンにし、**次へ**をクリックします。
7. 「**Completing the Delegation of Control**」ウィザードダイアログボックスで、「**Finish**」をクリックします。

ファイアウォール設定を構成する

Self-Service Password Resetサーバーと中央ストレージサーバーコンポーネントはユーザー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されたネットワークに展開し、特定の信頼されたコンポーネントからのみアクセスできるようにすることを強くお勧めします。このセクションでは、これらのサーバーのWindowsファイアウォールを正しく構成するための手順について説明します。また、これらのサーバーが信頼されていないネットワークトラフィックから隔離されるように、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。

展開でこれらの構成を完了すると、Self-Service Password Reset中央ストアサーバーには、Server Message Block (SMB) を使用してSelf-Service Password Resetサーバーからのみアクセスできるようになります。また、Self-Service Password Resetサーバーには、HTTPS接続を使用してStoreFront™サーバーからのみアクセスできます。

Windows 2012 R2のリモートファイル共有展開



環境

- Self-Service Password Resetコンポーネントは専用サーバーに展開してください。既存のStoreFrontまたはDelivery Controller™コンポーネントと同じサーバーには展開しないでください。そうしないと、以下に示すファイアウォール構成によってStoreFrontまたはコントローラーのトラフィックがブロックされる可能性があります。
- StoreFrontとセルフサービスパスワードリセットサーバーの間に、非透過型HTTP/HTTPSプロキシが存在しないこと。

StoreFrontとSelf-Service Password Resetサーバーの間に非透過的なプロキシが存在する場合は、ファイアウォールルールでプロキシサーバーからのみSelf-Service Password Resetサーバーにアクセスできるように構成してください。

- これらの手順の構成は、Windowsのデフォルトのファイアウォールルールに基づいています。

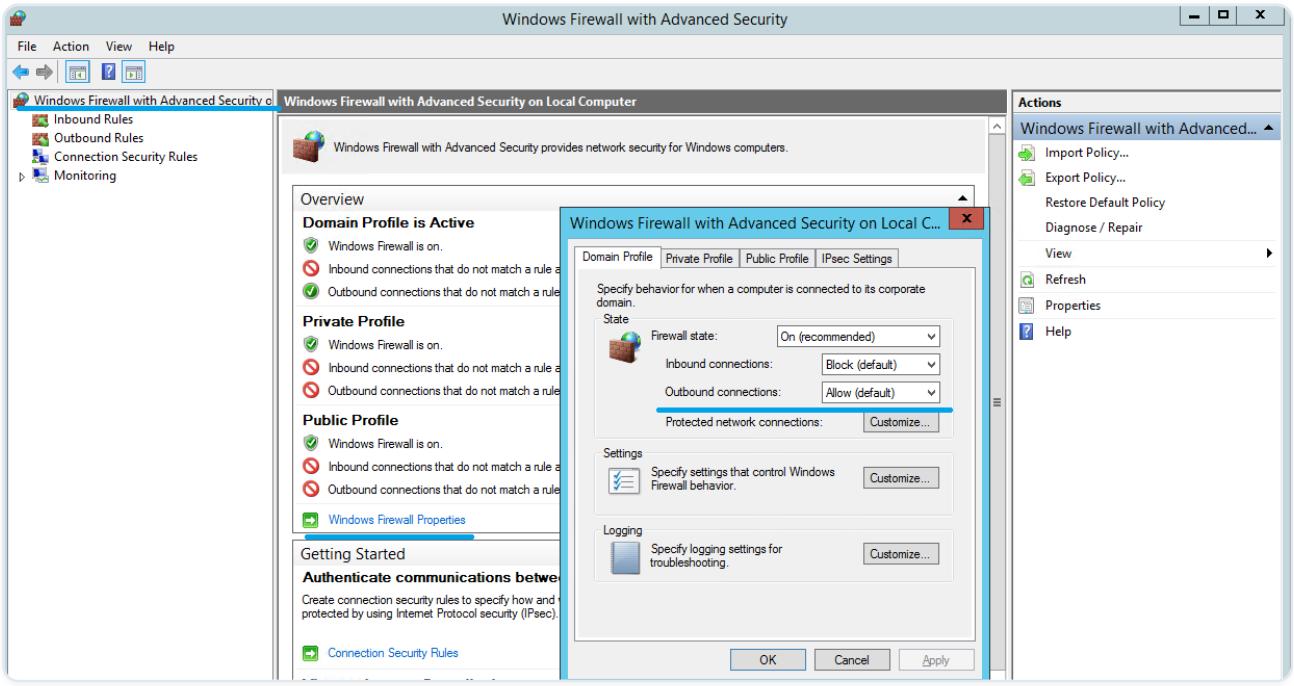
Self-Service Password Reset中央ストアのファイアウォールを構成する

構成を完了すると、Self-Service Password Reset中央ストアによって提供されるSMBサービスは、インバウンドではSelf-Service Password Resetサーバーからのみ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、アウトバウンドでは企業ネットワーク上にあるサービスにのみアクセスできます。

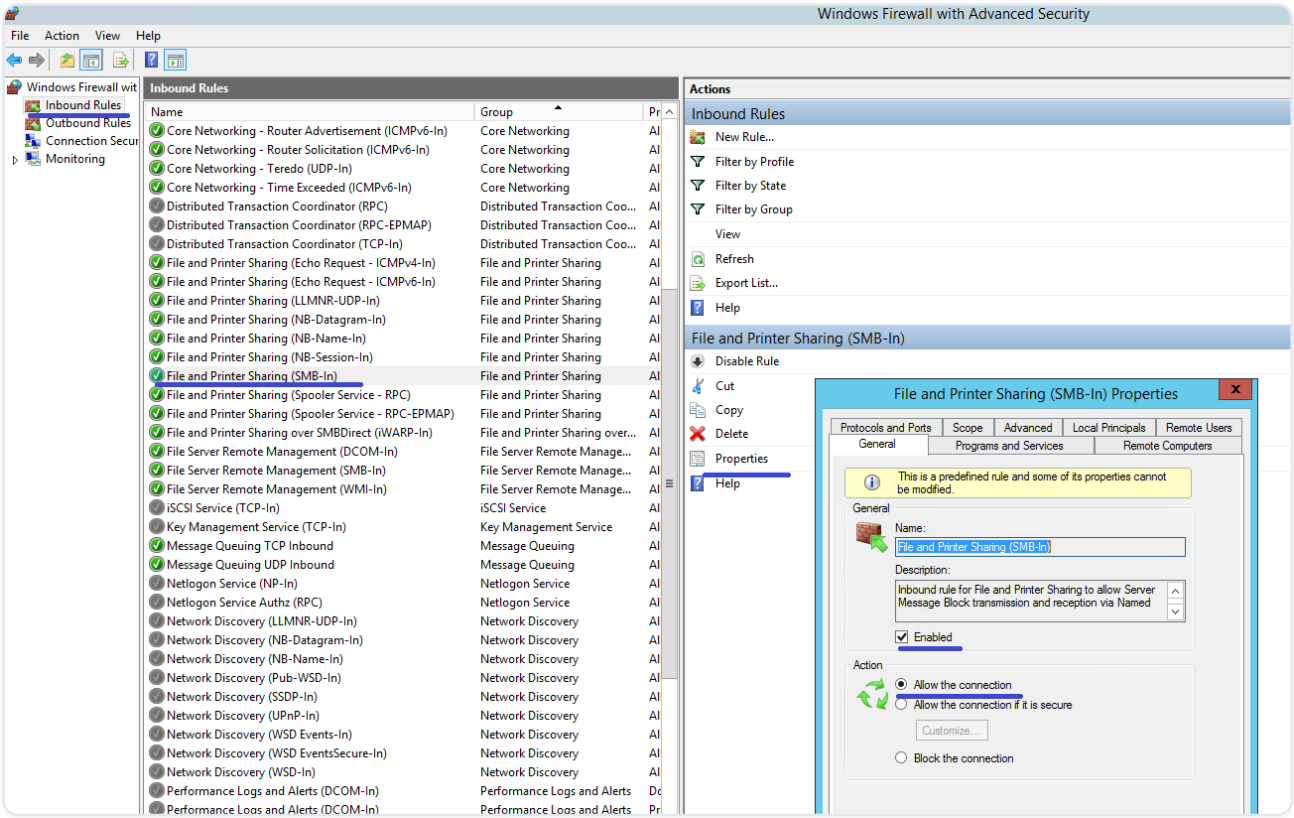
1\. Server Managerを開き、上部のナビゲーションバーにある「**Tools**」メニューから「**Windows Firewall with Advanced Security**」を選択します。

2\. 「**Windows Firewall with Advanced Security**」で、中央ペインの「**Windows Firewall Properties**」を選択します。ファイアウォールプロファイルには、Domain、Private、Publicの3つがあります。「**Domain Profile**」タブを選択します。「**Firewall state**」が「**On**」に設定され、「**Inbound connections**」が「**Block**」に設定され、「**Outbound connections**」が「**Allow**」に設定されていることを確認します。



3\. 「**Private Profile**」タブと「**Public Profile**」タブを選択します。「**Firewall state**」が「**On**」に設定され、「**Inbound connections**」と「**Outbound connections**」の両方が「**Block**」に設定されていることを確認します。変更を適用して保存します。

4\. 「**Inbound Rules**」から「**File and Printer Sharing (SMB-In)**」を選択し、このルールが「**Enabled**」であり、「**Action**」が「**Allow the connection**」に設定されていることを確認します。



5\. **ファイルとプリンターの共有 (SMB-In) のプロパティ**で、**スコープ**タブに切り替えます。**これらのIPアドレス**を選択し、すべてのSelf-Service Password ResetサーバーのIPアドレスをリストに追加します。例: Self-Service Password ResetサーバーA (192.168.1.10) およびSelf-Service Password ResetサーバーB (192.168.1.11)。

6\. **ファイルとプリンターの共有 (SMB-In) のプロパティ**で、**詳細設定**タブに切り替え、**ドメイン**、**プライベート**、**パブリック**のプロファイルを選択し、このルールの変更を保存します。

7\. **ファイルサーバーのリモート管理 (SMB-In)** および **ファイルとプリンターの共有 (NB-Session-In)** の**受信の規則**で、この手順を繰り返します。

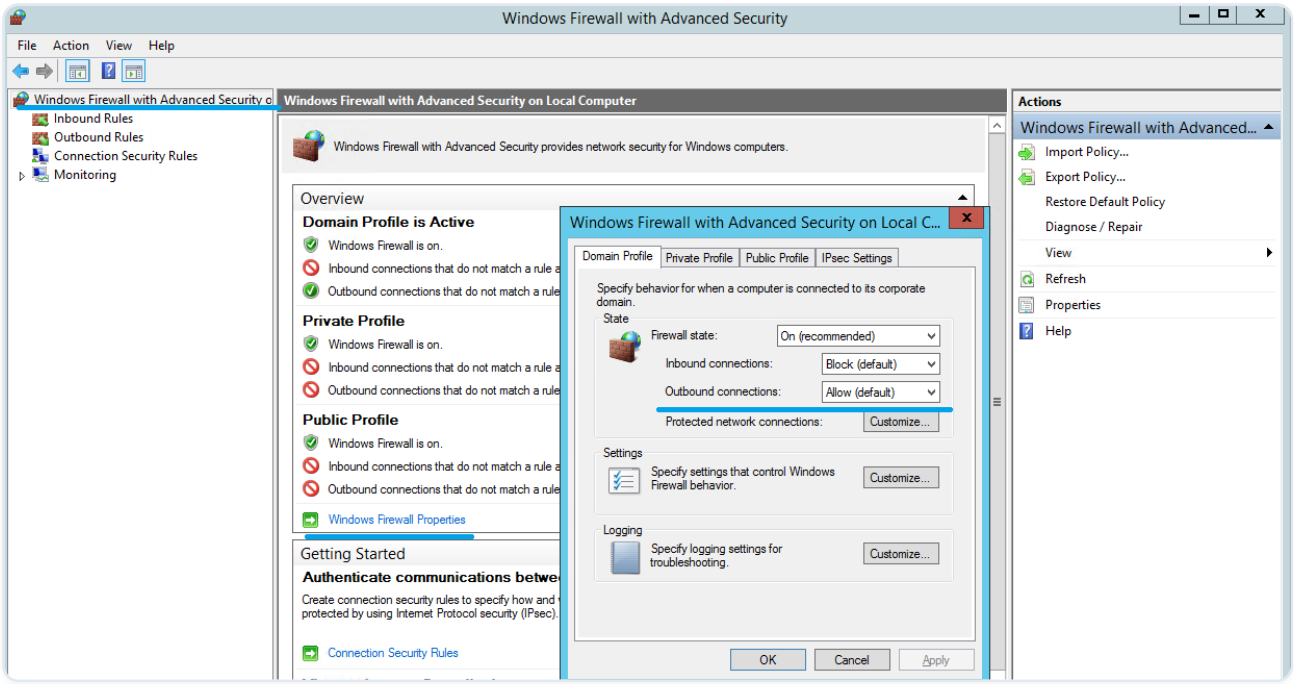
Self-Service Password Resetサーバーのファイアウォールを構成する

構成が完了すると、Self-Service Password Resetサーバーが提供するWebサービスには、HTTPSを使用してStoreFrontサーバーからのみアクセスできるようになります。また、Self-Service Password Resetサーバーは、企業ネットワーク上にあるサービスにアクセスできます。

1\. サーバーマネージャーを開き、上部のナビゲーションバーにある**ツール**メニューから、**セキュリティが強化されたWindows Defender ファイアウォール**を選択します。

2\. **セキュリティが強化されたWindows Defender ファイアウォール**で、中央のペインで**Windows Defender ファイアウォールのプロパティ**を選択します。ファイアウォールプロファイルには、ドメイン、プライベート、パブリックの3種類があります。**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**が**オン**に設定されていること、**受信接続**が**ブロック**に設定されていること、**送信接続**が**許可**に設定されていることを確認します。

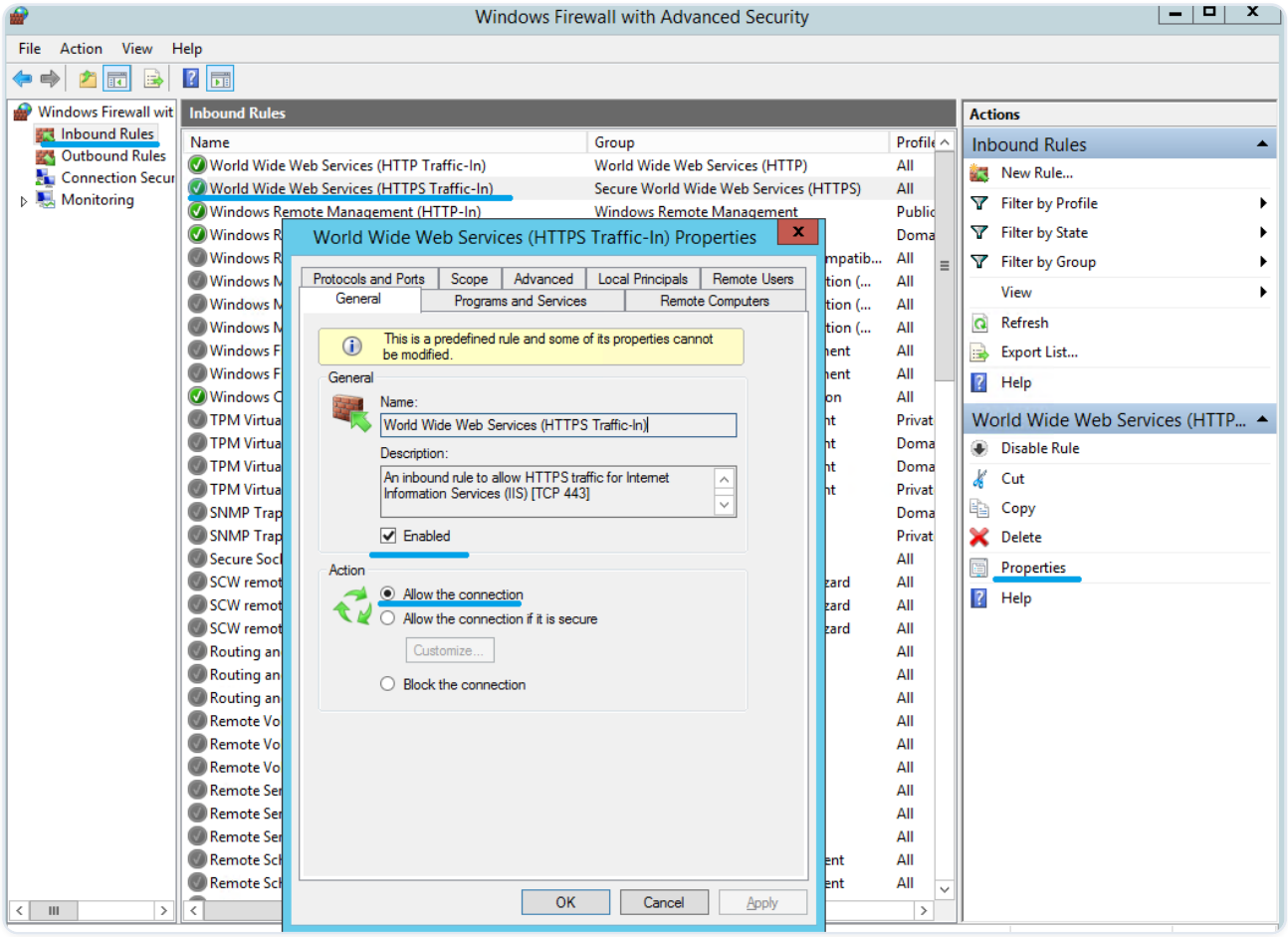


3\. **プライベートプロファイル**タブと**パブリックプロファイル**タブを選択し、**ファイアウォールの状態**が**オン**に設定されていることを確認します。**受信接続**と**送信接続**の両方が**ブロック**に設定されていることを確認します。変更を適用して保存します。

4\. **受信の規則**から、**World Wide Web サービス (HTTP 受信)を選択します。この規則が有効**になっていること、および**操作**が**接続をブロックする**に設定されていることを確認します。

5\. **World Wide Web サービス (HTTP 受信) のプロパティ**で、**詳細設定**タブに切り替えます。**ドメイン、プライベート、パブリック**のプロファイルを選択し、このルールの変更を保存します。

6\. **受信の規則**から、**World Wide Web サービス (HTTPS 受信)を選択します。この規則が有効**になっていること、および**操作**が**接続を許可する**に設定されていることを確認します。



7\. **World Wide Web サービス (HTTPS 受信) のプロパティ**で、**スコープ**タブに切り替えます。**これらのIPアドレス**を選択し、すべてのStoreFrontサーバーのIPアドレスをリストに追加します。例: StoreFront A (192.168.1.50) およびStoreFront B (192.158.1.51)。

8\. **World Wide Web サービス (HTTPS 受信) のプロパティ**で、**詳細設定**タブに切り替えます。**ドメイン**、プライベート、**パブリック**のプロファイルを選択し、このルールの変更を保存します。

Single Sign-on 中央ストアからデータを移行する

Single Sign-on 中央ストアは、Single Sign-on がユーザーデータと管理データを保存および管理するために使用する集中リポジトリです。ユーザーデータには、ユーザー資格情報、セキュリティの質問の回答、その他のユーザーに焦点を当てたデータが含まれます。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、セキュリティの質問、その他の広範囲にわたるデータが含まれます。

Single Sign-on 中央ストアから Self-Service Password Reset 中央ストアにすべてのデータを移行することはできません。この表は、移行できるデータと移行できないデータを示しています。

移行できません	移行できます
パスワードポリシー - サポートされていません	登録データを含むユーザーフォルダー
アプリケーションテンプレート - サポートされていません	顧客が使用するアンケート
アプリケーション定義 - サポートされていません	
ユーザー構成 - Self-Service Password Reset コンソールで作成	
アプリケーショングループ - サポートされていません	
Single Sign-on サービスデータ - Self-Service Password Reset コンソールで作成	

重要

- Self-Service Password Reset は、中央ストアとして Active Directory をサポートしておらず、ネットワーク共有のみをサポートしています。
- Self-Service Password Reset は、Single Sign-on 4.8 または 5.0 のデータのみをサポートしています。

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 のインストールと構成について理解しておいてください。詳細については、「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 サービスと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. 新しいユーザー構成を作成し、Single Sign-on で Self-Service Password Reset を使用している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: データプロキシアカウントが、コピーされたすべてのファイルに対するフルコントロール権限を持ってい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

へ

\\\\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**

顧客が使用するセキュリティの質問をコピーします。

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

へ

\\\\SSPRSVCcitrixsync$\\CentralStoreRoot\\AdminConsole\
\QuestionBasedAuthentication2\\

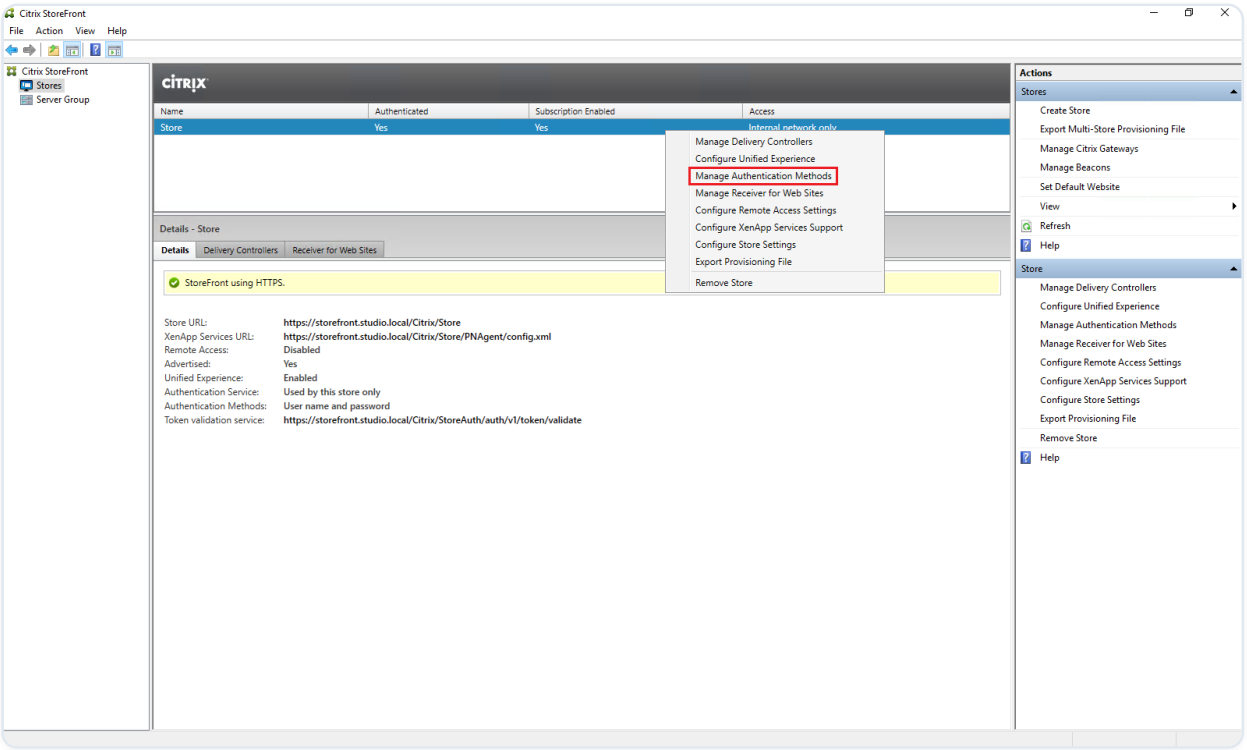
次のコマンドを使用します。 **Robocopy \\\\SSO-SERVER\\citrixsync$\\CentralStoreRoot\
\AdminConsole\\QuestionBasedAuthentication2\\ \\\\SSPR-SVC\\citrixsync$\
\CentralStoreRoot\\AdminConsole\\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee**

これで、すべてのユーザーは、シングルサインオンの登録質問と回答を使用してロック解除とリセットを行うことができます。

StoreFront™ を構成して、ユーザーがセキュリティの質問への回答を記録できるようにする

StoreFront を構成して、ユーザーがセキュリティの質問への回答を登録できるようにします。登録が完了すると、ドメインパスワードをリセットしたり、ドメインアカウントのロックを解除したりできます。詳細については、StoreFront のドキュメントを参照してください。

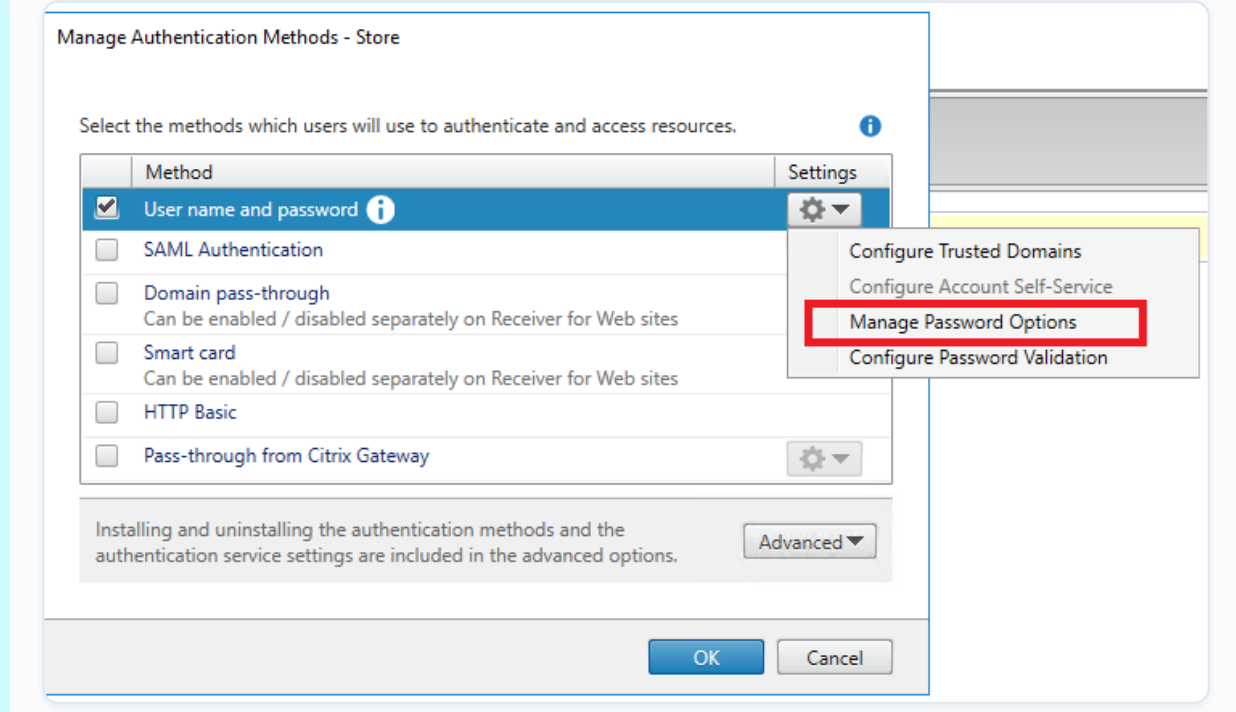
1. StoreFront の Internet Information Services (IIS) を HTTPS に構成します。
2. StoreFront で展開を作成します。
3. StoreFront 管理コンソールの右ペインで、ストアを右クリックし、 を選択します。



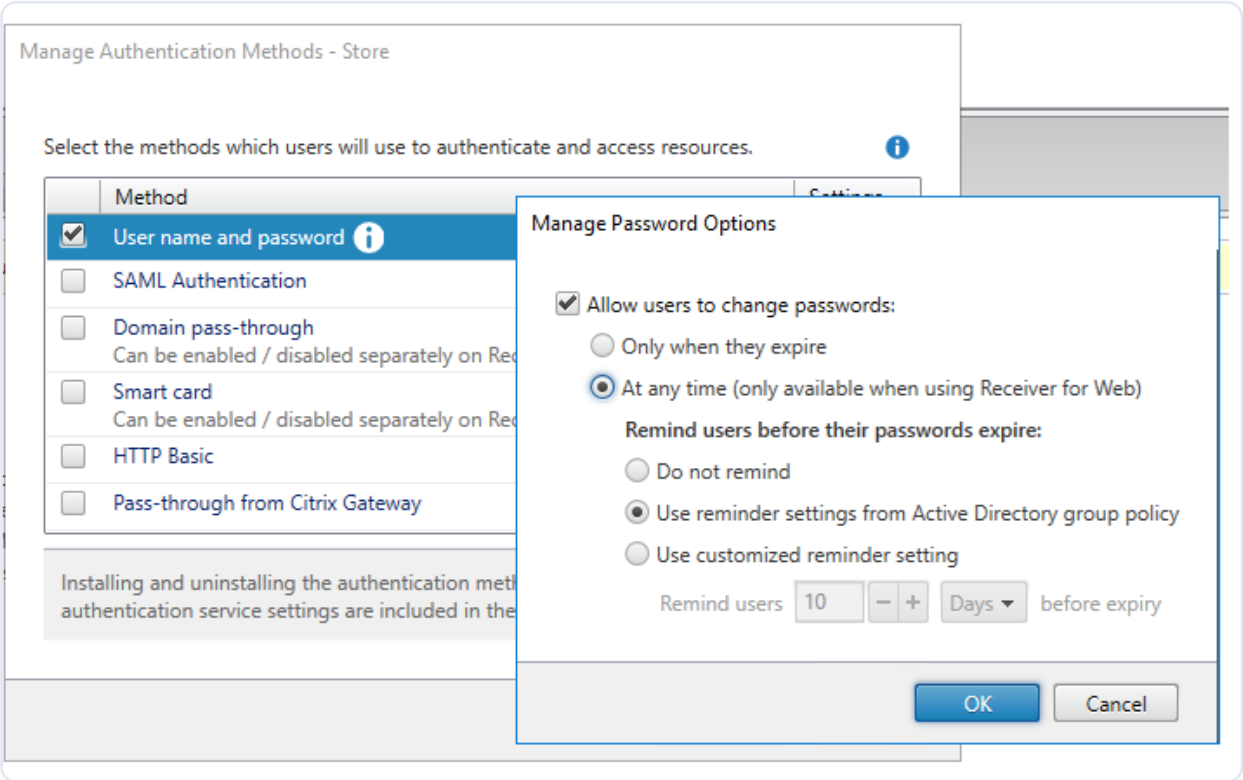
4. の設定で、 を選択します。

> **注：**

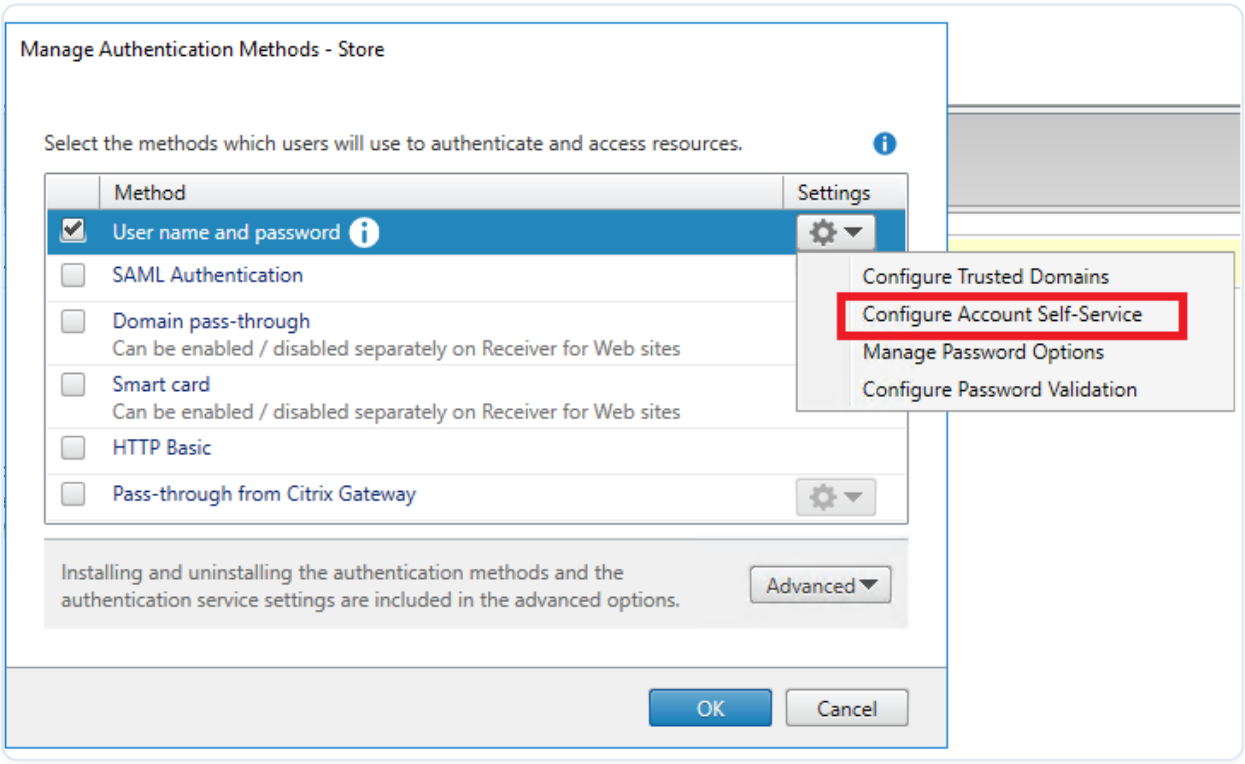
セルフサービスパスワードリセット (SSPR) は、StoreFront の 認証方法のみをサポートしています。ドメインパススルーなどの他の方法はサポートしていません。



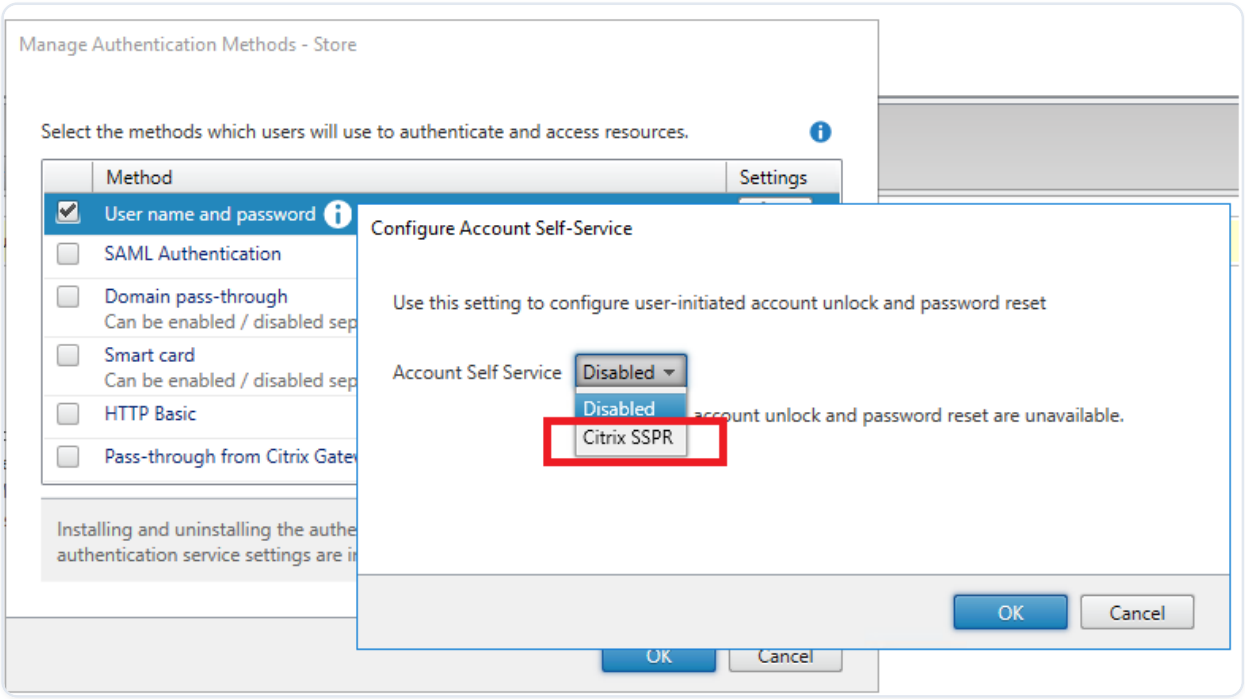
5. ユーザーにパスワードを変更させるタイミングを選択し、 をクリックします。



6. の設定で、 を選択します。



7. を有効にするには、 を選択します。



8. 「**Configure**」をクリックし、「**Enable password reset**」と「**Allow account unlock**」を選択し、「**SSPR Account Service URL**」（https://< SSPRサーバーのFQDN>/MPMService）を設定します。

   「SSPRアカウントサービスURL」(/en-us/self-service-password-reset/current-release/media/sspr-account-service-url.png)

9. すべての設定を適用するには、「**OK**」をクリックします。

> **注：**

> 統合されたエクスペリエンスを使用するようにサイトを構成します。

> ユーザーが次回Citrix Workspace™アプリまたはCitrix Workspaceアプリ for Webにログオンすると、セキュリティ登録が利用可能になります。ユーザーは **開始**をクリックして、将来のパスワードリセットまたはアカウントロック解除のためのセキュリティ質問に対する回答を指定できます。

「セキュリティ質問の管理」(/en-us/self-service-password-reset/current-release/media/manage-security-questions.png)

セルフサービスパスワードリセットのドキュメント履歴

次の表に、セルフサービスパスワードリセット1.1.xのドキュメントに対する重要な変更点を示します。これらのアップデートに関する通知を受け取るには、RSSフィードを購読してください。

日付	変更	説明
29 Aug 2018	セルフサービスパスワードリセット1.1.xのリリース	セルフサービスパスワードリセット 1.1.xの新機能