



セルフサービスパスワードリセット **1.1.x**

Contents

セルフサービスパスワードリセット 1.1.x	2
新機能	2
解決された問題	4
既知の問題	5
システム要件	8
インストールと構成	11
安全な構成	28
Single Sign-On 中央ストアからのデータの移行	34
セキュリティ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	36

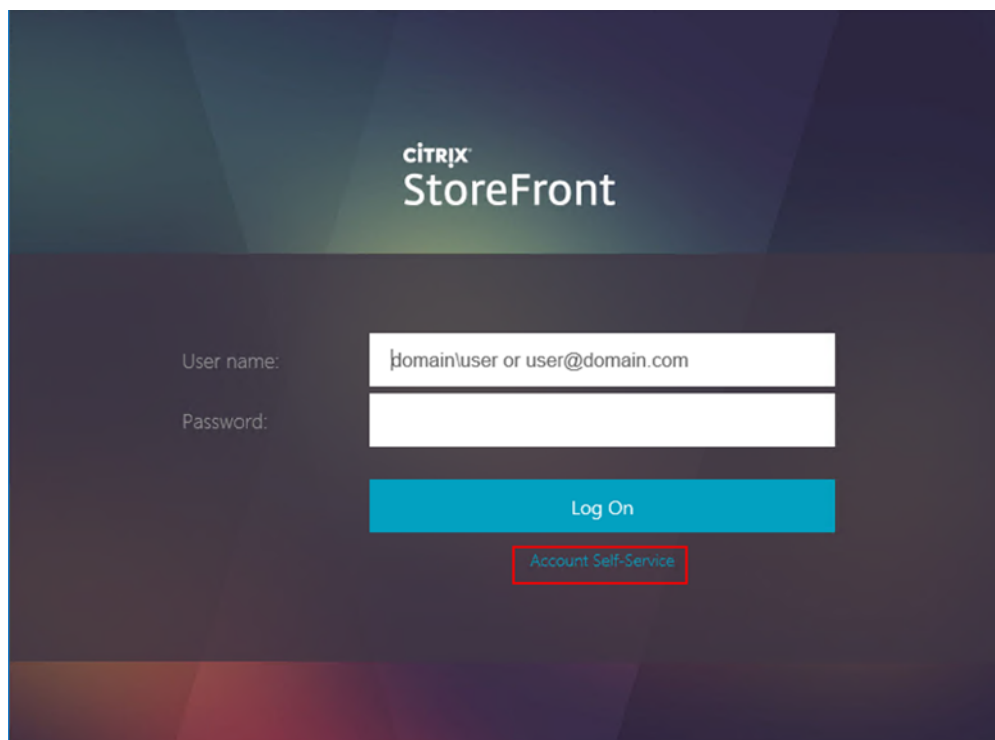
セルフサービスパスワードリセット **1.1.x**

April 4, 2024

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。セルフサービスパスワードリセットが構成されると、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。

ヒント:

「アカウントセルフサービス」リンクは StoreFront のログオンページに表示され、ユーザーはパスワードのロック解除とリセットを行うことができます。



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。

新機能

June 28, 2022

バージョン **1.1.20** の新機能

セルフサービスパスワードリセットサービスに接続できる IP アドレスを設定できます。IP アドレスを入力しないと、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

このリリースではいくつかの問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

バージョン **1.1** の新機能

このバージョンの Profile management では、次の機能が強化されています。

- 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の質問に使用できるようになりました。

セルフサービスパスワードリセットには次の 3 つのコンポーネントが含まれます。

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

セルフサービスパスワードリセット構成コンソール

- [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、セルフサービスパスワードリセットアカウントなど、セルフサービスパスワードリセット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。
 - [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、Citrix Virtual Apps または Citrix Virtual Desktops 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、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 へのセキュリティの質問の登録 StoreFront を使用すると、セキュリティ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、「[認証サービスの構成]」 ([/en-us/storefront/current-release/configure-authentication-and-delegation/configure-authentication-service.html](https://en-us/storefront/current-release/configure-authentication-and-delegation/configure-authentication-service.html)) で「セルフサービスパスワードリセットのセキュリティの質問」を参照してください。

解決された問題

June 28, 2022

バージョン 1.1.20

このリリースでは、解決された問題はありません。

バージョン 1.1.10

このリリースでは、次の問題が解決されています。

- セルフサービスパスワードリセットサーバーで TLS 1.0 を無効にした後、サーバー URL をウィザードに追加すると、次のエラーメッセージが表示されることがあります：

「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て、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機能しないことがあります。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

June 28, 2022

バージョン **1.1.20**

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う失敗し、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またはアンインストール、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またはアンインストール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。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またはアンインストールします。

[DNA-22761]

バージョン 1.1.10

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う失敗し、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またはアンインストール、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またはアンインストール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。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またはアンインストールします。

[DNA-22761]

バージョン 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う失敗し、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またはアンインストール、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またはアンインストール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。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またはアンインストールします。

[DNA-22761]

バージョン 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]

- Mac 向け Citrix Workspace アプリ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. Mac 向け Citrix Workspace アプリ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の質問を移行すると、[更新] をクリックした後も、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: セキュリティの質問に & を含めないようにしてください。

- .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またはアンインストール、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またはアンインストール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。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またはアンインストールします。

[DNA-22761]

システム要件

June 28, 2022

重要

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は Citrix で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、セルフサービスパスワードリセット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** 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)
- インターネットインフォメーションサービス (**Internet Information Services: IIS**) - 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。
 - IIS 10.0 (Windows 2016)
 - IIS 8.5 (Windows 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に必要です。

最初のインストールでは、<https://www.microsoft.com/en-us/download/details.aspx?id=26368> から vccredist_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 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

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、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手に入るか、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。

セルフサービスパスワードリセット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できます。または、モジュールごとにカスタマイズされた異なる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書き用のアクセス権を所有している。詳しくは、「[インストールと構成]」([/en-us/self-service-password-reset/current-release/install-configure.html](https://en-us/self-service-password-reset/current-release/install-configure.html)) の「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 以降

Citrix Workspace アプリ

サポート対象：

- Web 向け Citrix Workspace アプリ
- Windows 向け Citrix Workspace アプリ
- Linux 向け Citrix Workspace アプリ
- Mac 向け Citrix Workspace アプリ（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（Web 向け Citrix Workspace アプリを使用しない場合も含む）

Citrix Gateway の外部使用

サポートされません

インストールと構成

June 28, 2022

インストールチェックリスト

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：

☑	手順
	セルフサービスパスワードリセットをインストールするコンピューターを決定し、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。 セルフサービスパスワードリセットサービスに必要な 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。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

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

1. 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。
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。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。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。

中央ストアの作成

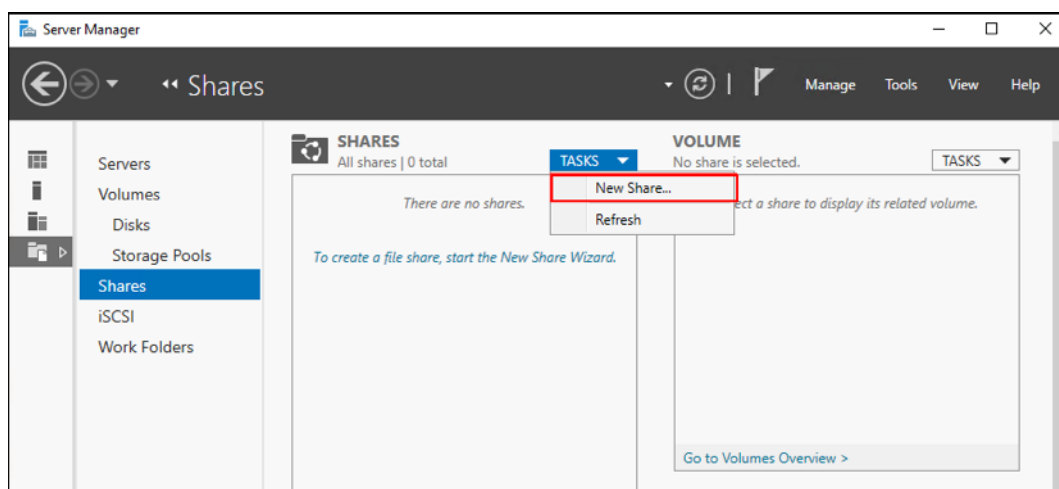
セキュリティ上の理由から、セルフサービスパスワードリセットサービスを実行しているマシンで直接中央ストアを作成することをお勧めします。複数のセルフサービスパスワードリセットサーバーを展開する必要がある場合、セルフサービスパスワードリセットサーバーおよびリモートネットワーク共有をホストするサーバーの両方が SMB 暗号化をサポートしているのであれば、リモートネットワーク共有で中央ストアをホストすることができます。

この機能は、Windows Server 2012 R2 または Windows Server 2016 でのみ使用できます。

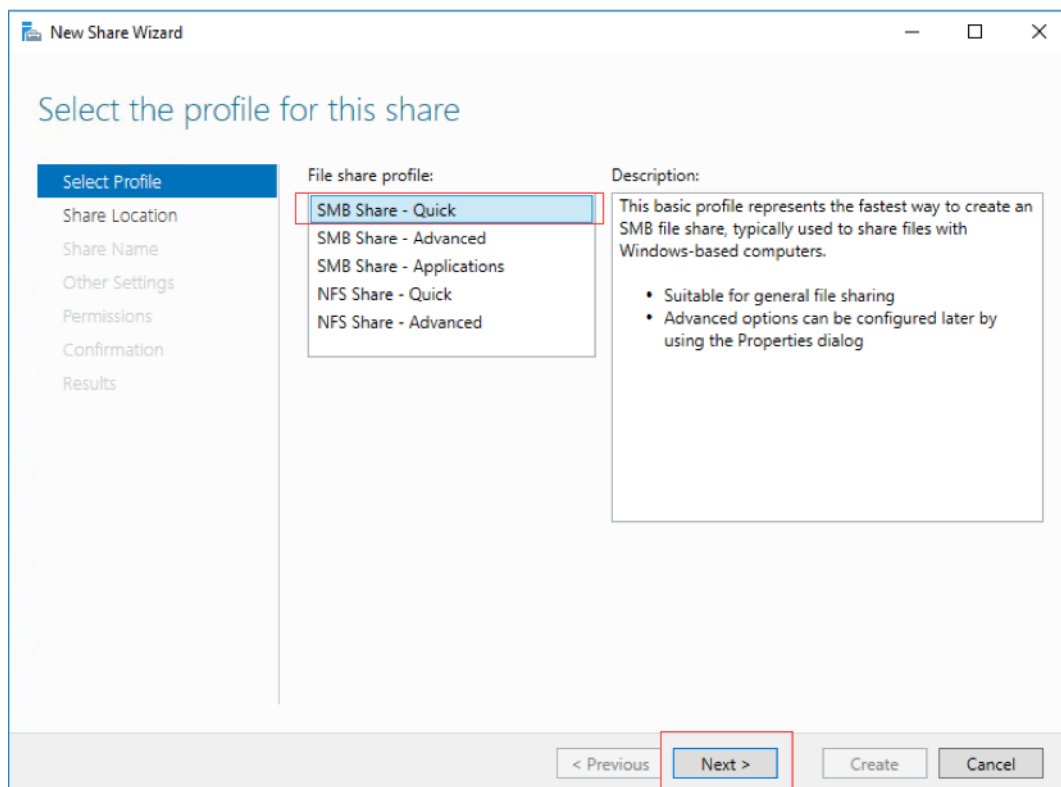
データプロキシ用アカウントの作成 データプロキシ用のアカウントとして通常使用する、ドメインユーザーを作成します。ドメイン管理者グループまたはローカル管理者グループのユーザーを、データプロキシ用のアカウントとして設定しないようにします。

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。

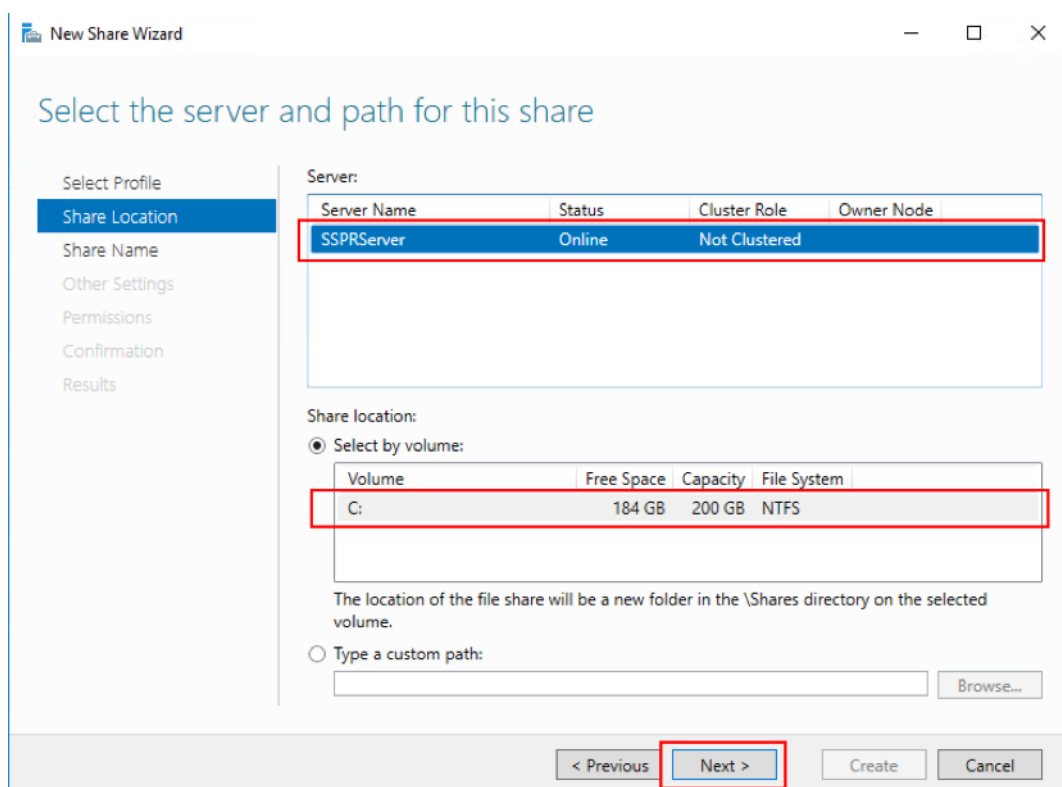
1. [新しい共有] ウィザードを開始するには、サーバーマネージャーを開きます。[ファイルサービスおよびストレージサービス] の詳細ページから、左ペインで [共有] を選択して、[タスク] > [新しい共有] をクリックします。



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。



New Share Wizard

Select the server and path for this share

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Server:

Server Name	Status	Cluster Role	Owner Node
SSPRServer	Online	Not Clustered	

Share location:

☒ Select by volume:

Volume	Free Space	Capacity	File System
C:	184 GB	200 GB	NTFS

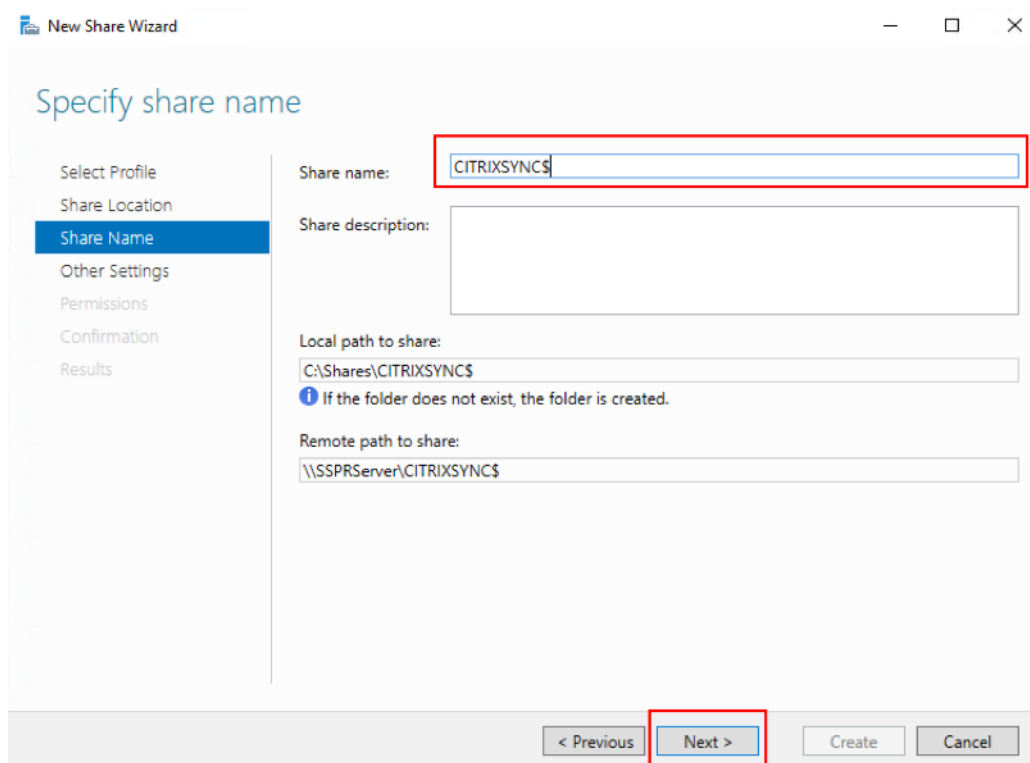
The location of the file share will be a new folder in the \Shares directory on the selected volume.

☐ Type a custom path:

Browse...

< Previous Next > Create Cancel

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。



New Share Wizard

Specify share name

Select Profile

Share Location

Share Name

Other Settings

Permissions

Confirmation

Results

Share name: CITRIXSYNC\$

Share description:

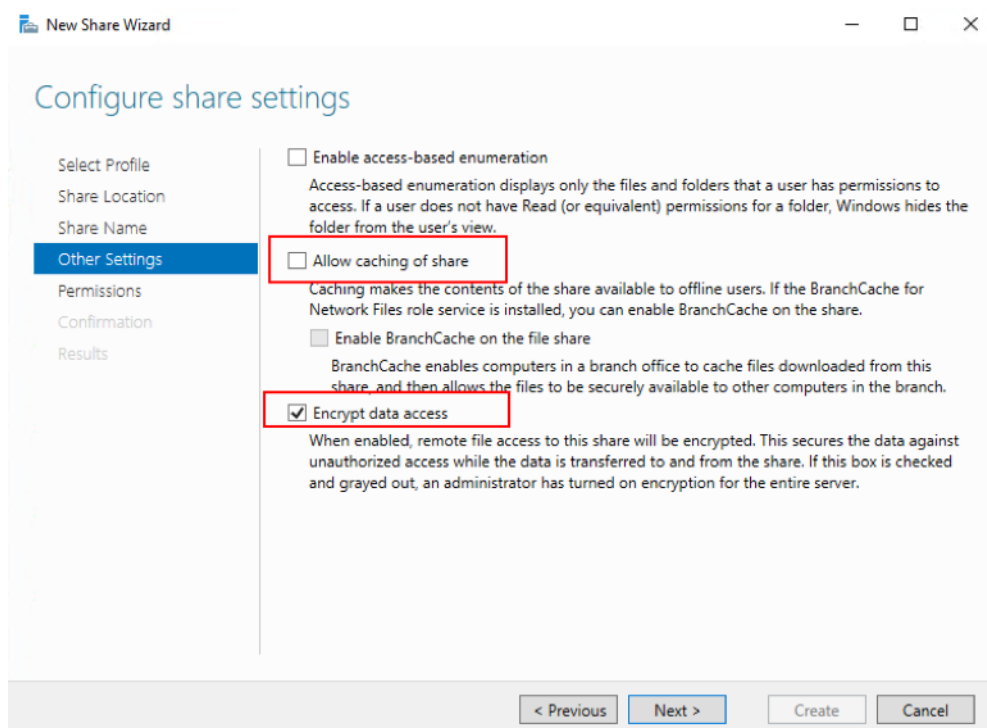
Local path to share: C:\Shares\CITRIXSYNC\$

i If the folder does not exist, the folder is created.

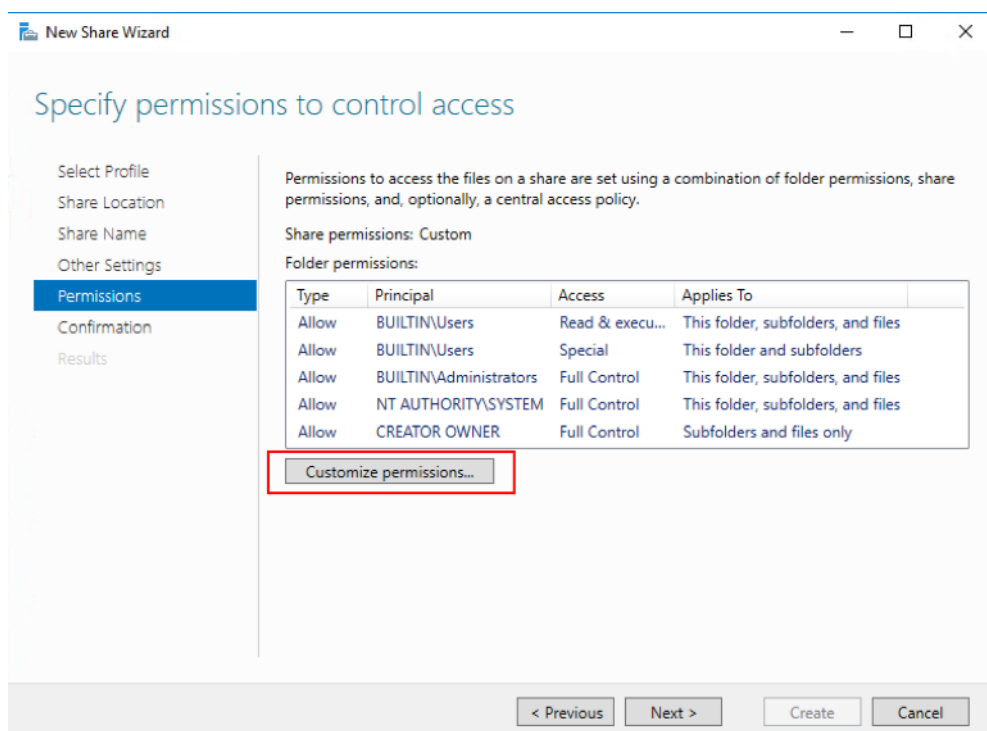
Remote path to share: \\SSPRServer\CITRIXSYNC\$

< Previous Next > Create Cancel

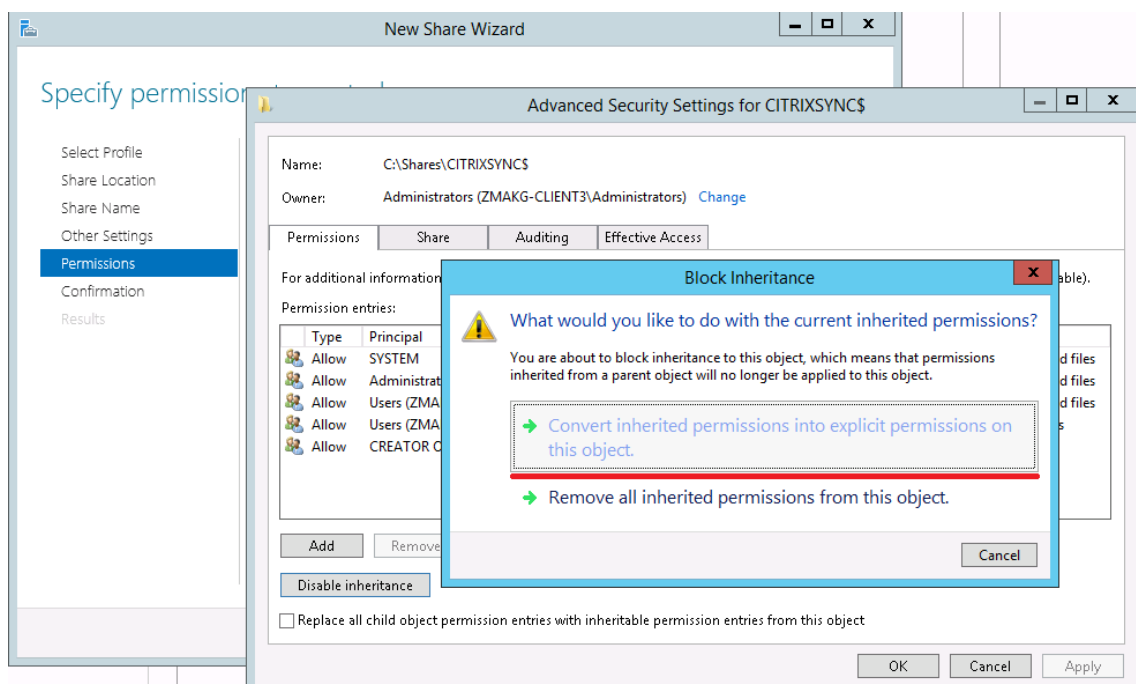
5. 左ペインで [他の設定] をクリックし、[データの暗号化] をオンにして [共有のキャッシュ化を許可する] をオフにし、[次へ] をクリックします。



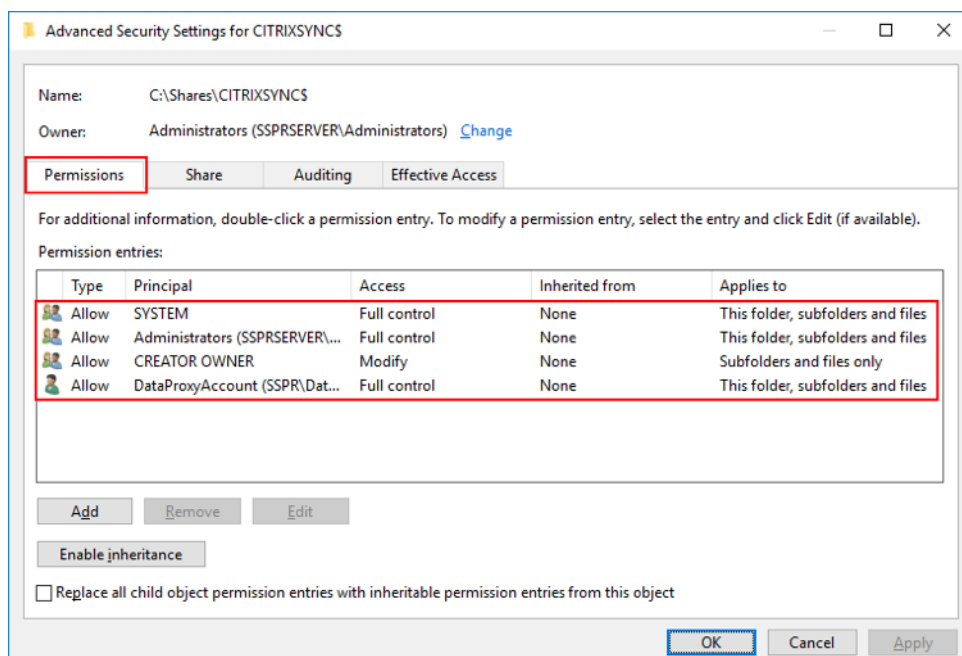
6. 共有 アクセス許可をカスタマイズするには、左ペインで [アクセス許可] を選択して、[アクセス許可のカスタマイズ] > [共有] をクリックします。



7. NTFS アクセス許可をカスタマイズするには、[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。



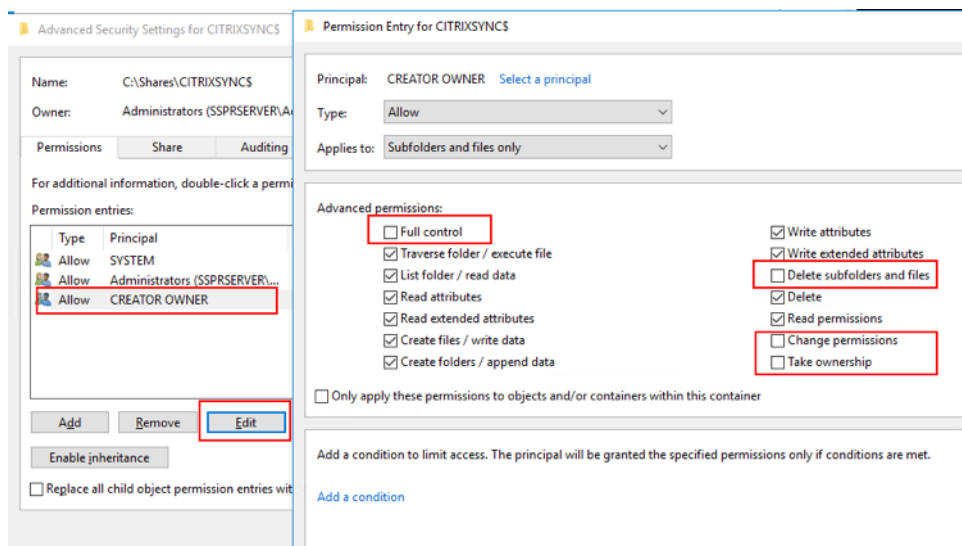
8. [アクセス許可] タブをクリックして **CREATOR OWNER**、**Local Administrators**、**SYSTEM** 以外のすべてのユーザーを削除し、フルコントロールのアクセス許可を指定して作成されたデータプロキシアカウントを追加します。



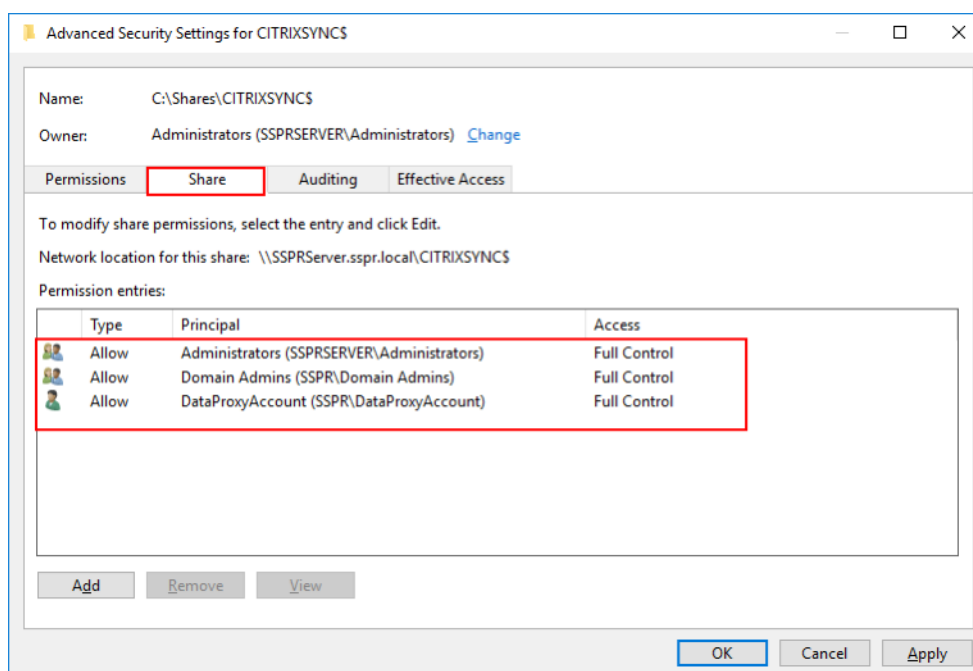
9. **CREATOR OWNER** を選択して、[編集] をクリックして以下のアクセス許可のチェックをオフにします：

- フルコントロール

- サブフォルダーとファイルの削除
- アクセス許可の変更
- 所有権の取得



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



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. **CITRIXSYNCS** 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。

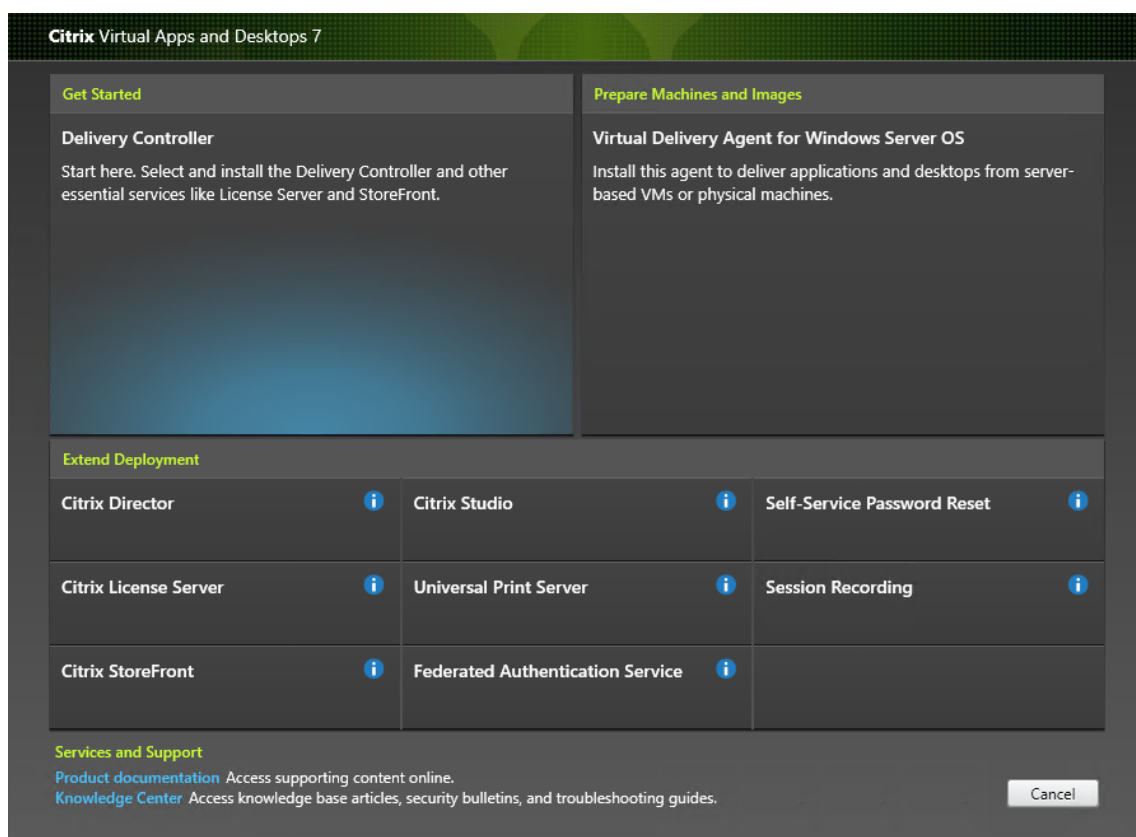
重要: データプロキシ用のアカウントにこれらのサブフォルダーのフルコントロールがあることを確認してください。

セルフサービスパスワードリセットの中央ストアの EncryptData、RejectUnencryptedAccess、RequireSecuritySignature を構成する必要があります。構成情報の詳細については、次の Microsoft の技術文書を参照してください:

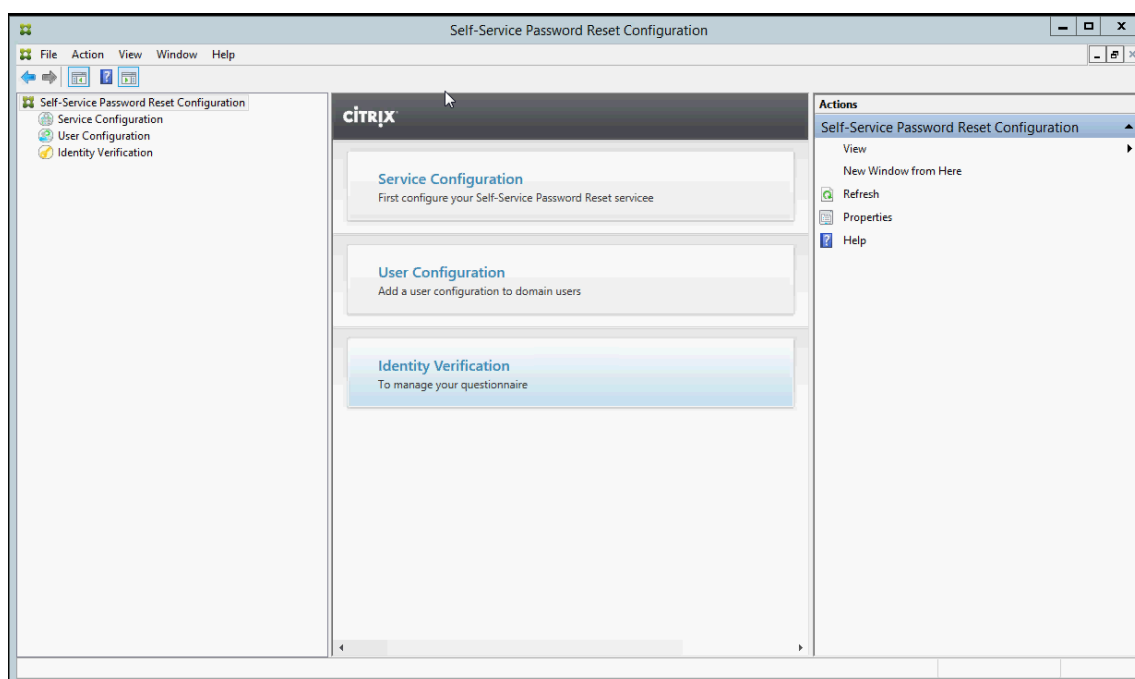
<https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbserverconfiguration>
<https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbshare>

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

1. Citrix Virtual Apps and Desktops インストーラーを使用して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。

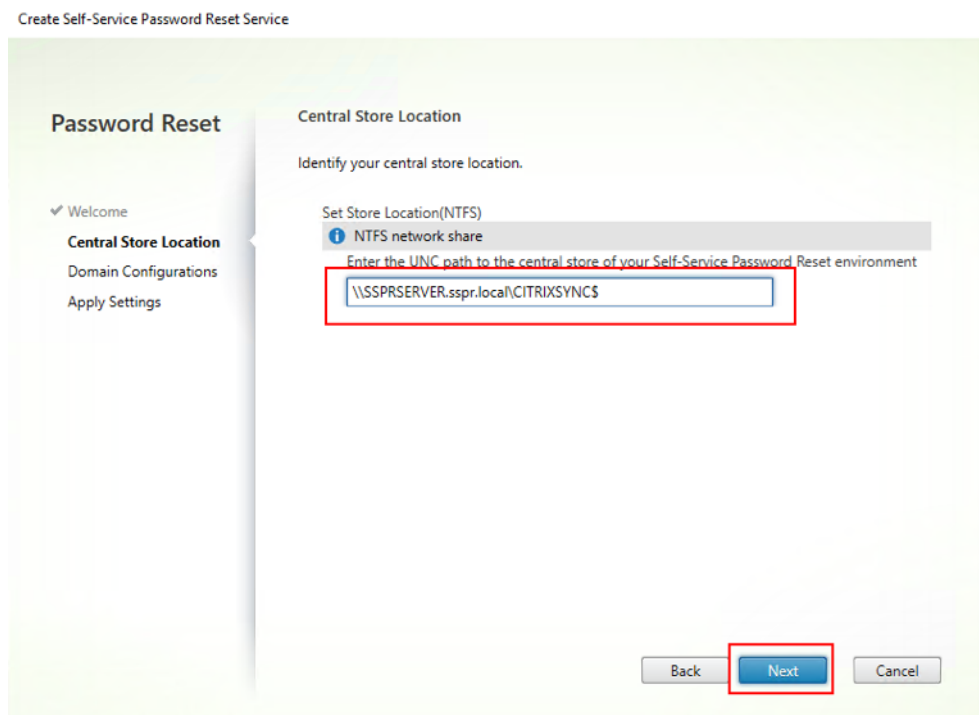


2. セルフサービスパスワードリセットのインストール後、[スタート] > [すべてのプログラム] > [Citrix] > [Citrix セルフサービスパスワードリセットの設定] の順にクリックして、Citrix セルフサービスパスワードリセットサービスを構成します。
3. コンソールが表示されたら、以下の 3 つの基本手順に従ってサービスを構成します。

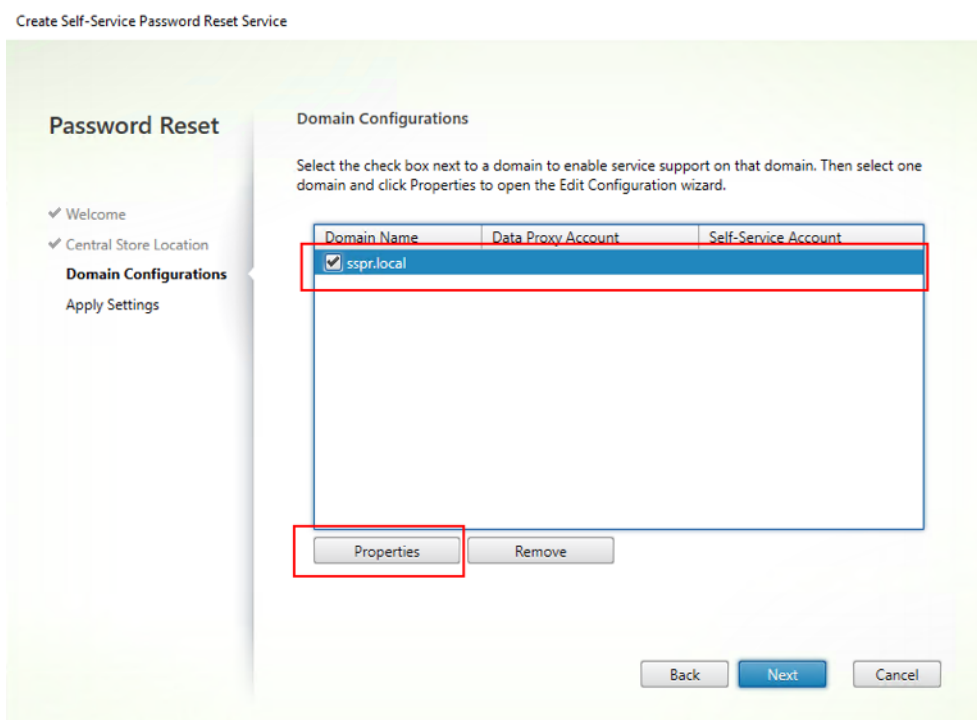


サービス設定 サービスを構成する前に、中央ストア、データプロキシ用のアカウント、セルフサービス用アカウントが作成されていることを確認します。

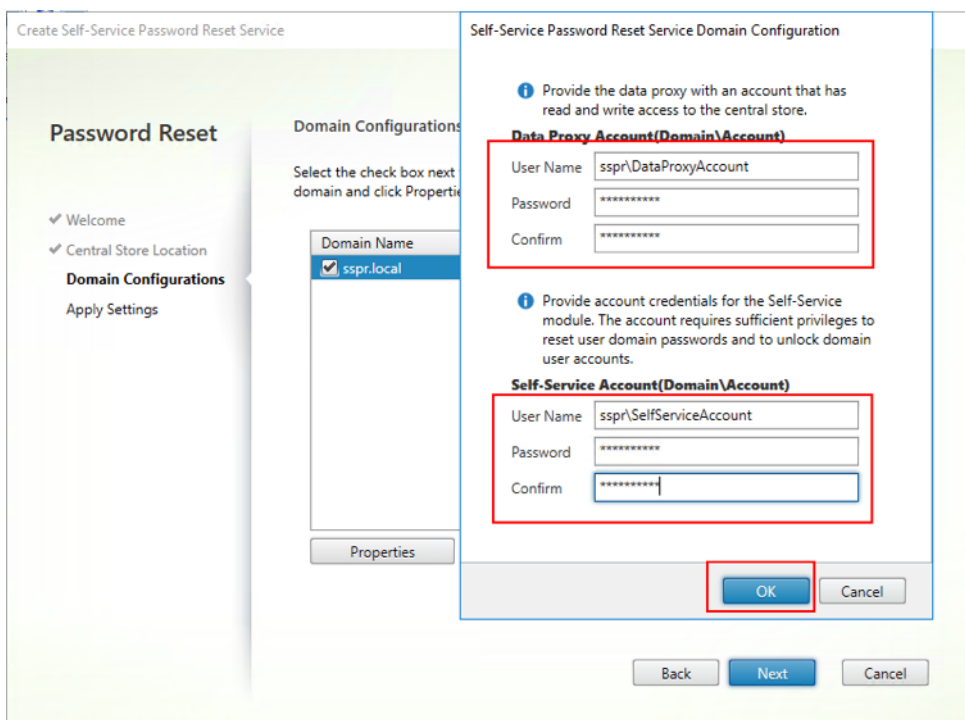
1. 中央ペインで [サービス設定] を選択し、右ペインで [新しいサービス設定] をクリックします。
2. [中央ストアの場所] 画面で中央ストアの場所を指定して、[次へ] をクリックします。



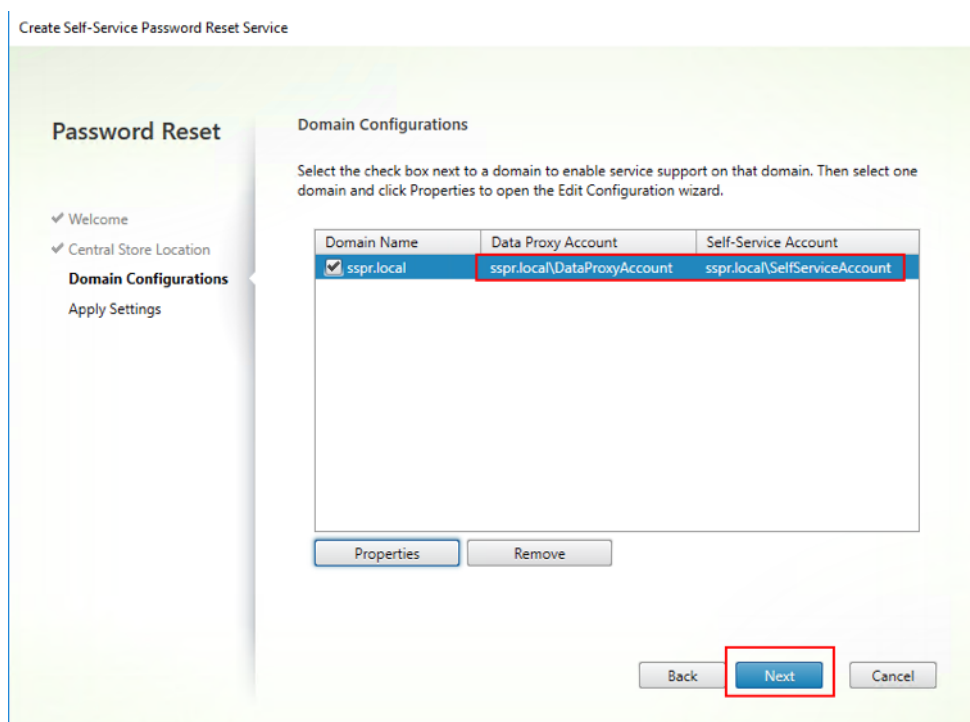
3. [ドメインの設定] 画面でセルフサービスパスワードリセットサービスを有効にするドメインを選択し、[プロパティ] をクリックします。



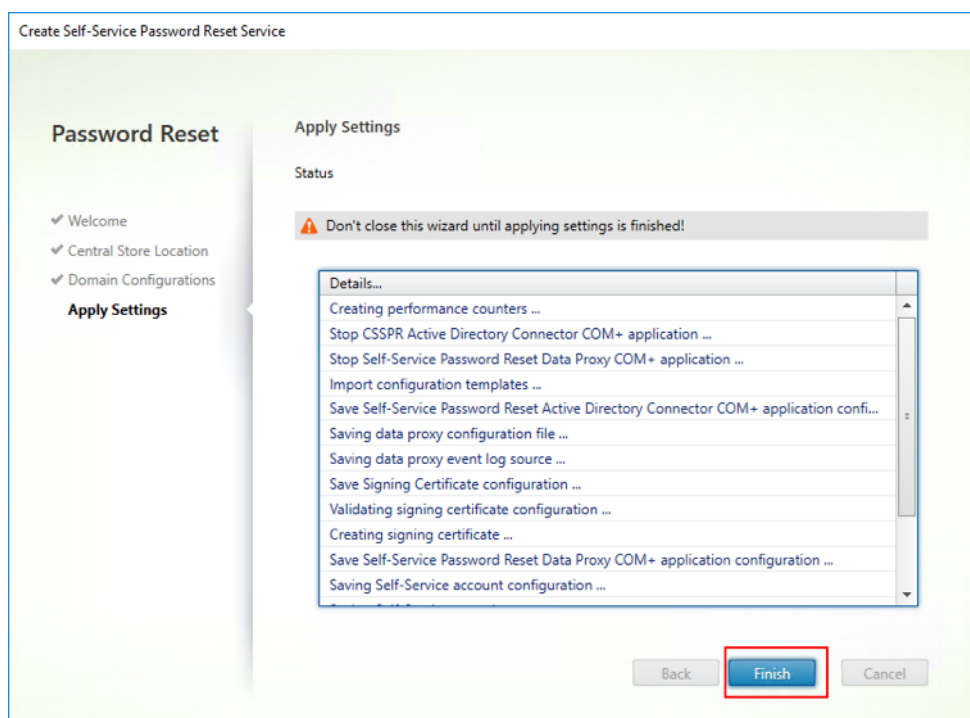
4. データプロキシアカウント および セルフサービスアカウント のユーザー名とパスワードをそれぞれ指定して、[OK] をクリックします。



5. [次へ] をクリックして、すべての設定内容を適用します。



6. [終了] をクリックして、構成を完了します。



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。

Create User Configuration

Password Reset

- Name User Configuration**
- Configure Licensing
- Enable Self-Service Password Reset

Name User Configuration

Define this user configuration and associate these settings to one or more users.

User configuration association

Active Directory Hierarchy (OU or User)

User LDAP path

LDAP://sspr.local/OU=OU1,DC=sspr,DC=local

LDAP://sspr.local/CN=User1,CN=Users,DC=sspr,DC=local

Browse

Remove

Active Directory Group

Name

SSPR\Group1

Add

Delete

Next

Cancel

3. [ライセンスの設定] 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。

Edit User Configuration

Password Reset

- ✓ Name User Configuration
- Configure Licensing**
- Enable Self-Service Password Reset

Configure Licensing

Specify the License Server name and port number for this user configuration.

You can use the Self-Service Password Reset feature only when you have XenApp or XenDesktop Platinum Edition.

License Server Name

☒ Use Default port 27000

Back

Next

Cancel

4. [セルフサービスパスワードリセットの有効化] 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。

Create User Configuration

Password Reset

- ✓ Name User Configuration
- ✓ Configure Licensing
- Enable Self-Service Password Reset**

To Configure Self-Service Password Reset Feature

Self-Service feature allow users to reset their Windows passwords and unlock their domain accounts without administrator intervention

☒ Reset: Allow users to reset their primary domain password

☒ Unlock: Allow users to unlock their domain account

Please provide the service address below.

Service port:

Https://

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。

ユーザー構成の管理 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セルフサービスパスワードリセット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セルフサービスパスワードリセット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

ユーザー設定を作成するには:

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、組織単位 (**OU**)、グループを追加するには:

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）を含めないことをお勧めします。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 [ライセンスの設定] ページで、セルフサービスパスワードリセット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、Citrix Virtual Apps または Citrix Virtual Desktops 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:

セルフサービスパスワードリセットにより、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 Workspace アプリの [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 セルフサービスパスワードリセット構成コンソールの [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 Workspace アプリ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] > [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] > [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、セキュリティの質問に対する回答を登録するときに、誤入力为了避免のために同じ回答を 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 Workspace アプリへの登録時には、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。[セキュリティの質問] ダイアログボックスが開きます。
2. [セキュリティの質問] 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、[編集] ボタンを使用してください。[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 Workspace アプリ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。

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。

セキュリティの質問グループを作成するには:

必要に応じて、セキュリティの質問を作成して、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、[セキュリティの質問] ページで [編集] をクリックします。一覧から編集する質問グループを選択して、[編集] をクリックします。[セキュリティの質問グループ] ダイアログボックスが開き、グループに追加済みの質問、および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。

セキュリティ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、次のいずれかをクリックします：
 - [セキュリティの質問のインポート]
 - セキュリティの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。
 - [セキュリティの質問のエクスポート]
 - セキュリティの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

September 25, 2020

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。

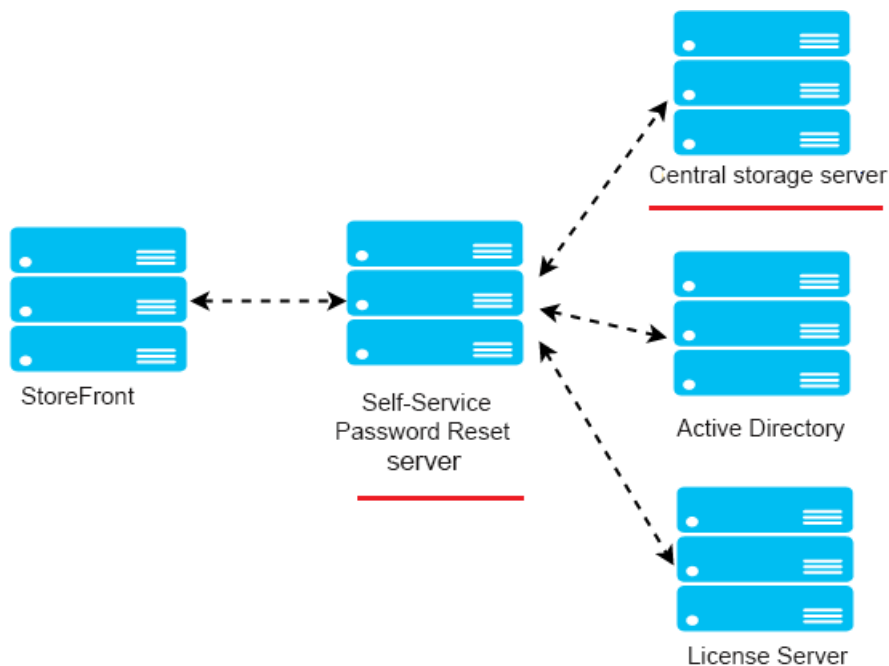
4. [委任するタスク] ダイアログボックスで、[委任するカスタムタスクを作成する]、[次へ] の順にクリックします。
5. [Active Directory オブジェクトの種類] ダイアログボックスで、[フォルダー内の次のオブジェクトのみ] の [ユーザーオブジェクト] をクリックして、[次へ] をクリックします。
6. [アクセス許可] ダイアログボックスで、[全般] チェックボックスと [プロパティ固有] チェックボックスをオンにします。[アクセス許可] の一覧で、[**lockoutTime** の読み取り]、[**lockoutTime** の書き込み]、[パスワードのリセット]、[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。

実稼働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、メッセージブロック (Server Message Block: SMB) を使用したセルフサービスパスワードリセット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は、HTTPS 接続を備えた StoreFront サーバーからのみアクセスされます。

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、以下に示すファイアウォール構成では Storefront または Delivery Controller 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 とセルフサービスパスワードリセットサーバーの間に設定する場合は、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。

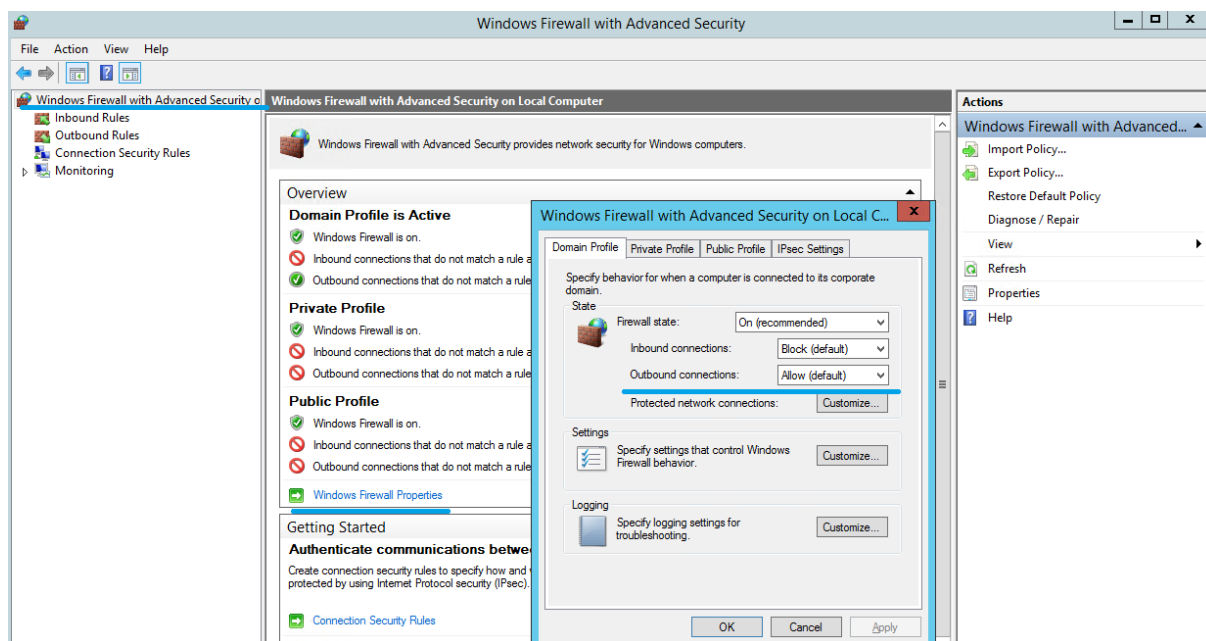
- 以下の手順の構成は、デフォルトの Windows ファイアウォールの規則に基づいています。

セルフサービスパスワードリセット中央ストアのファイアウォールを構成する

構成が完了すると、セルフサービスパスワードリセット中央ストアから提供される SMB サービスには、セルフサービスパスワードリセットサーバーのみが受信で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中央ストアサーバーは、社内ネットワークにあるサービスに送信のみでアクセスできるようになります。

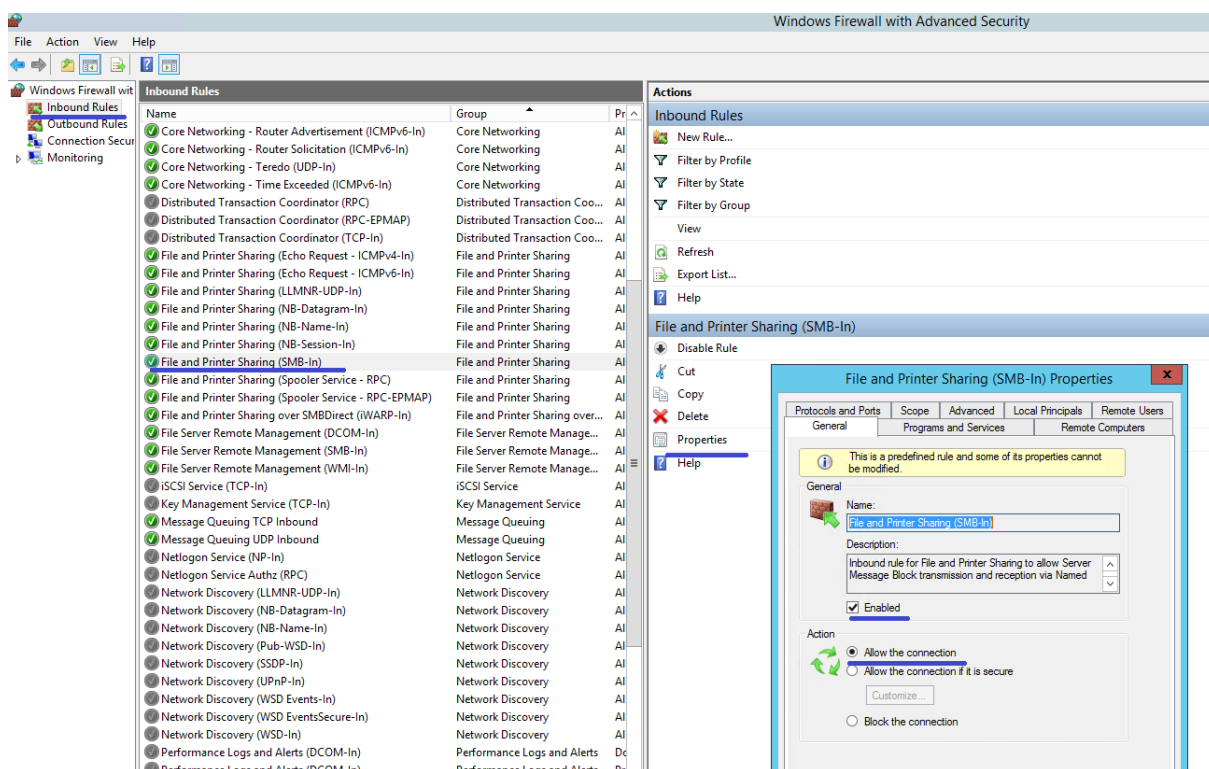
1. サーバーマネージャーを開き、上部ナビゲーションバーの [ツール] メニューで [セキュリティが強化された Windows ファイアウォール] をクリックします。

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] タブを選択します。[ファイアウォールの状態] を [有効]、[受信接続] と [送信接続] を [ブロック] にそれぞれ設定します。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、[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] タブに移動します。[これらの IP アドレス] をオンにして、一覧にすべてのセルフサービスパスワードリセットサーバーの 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。

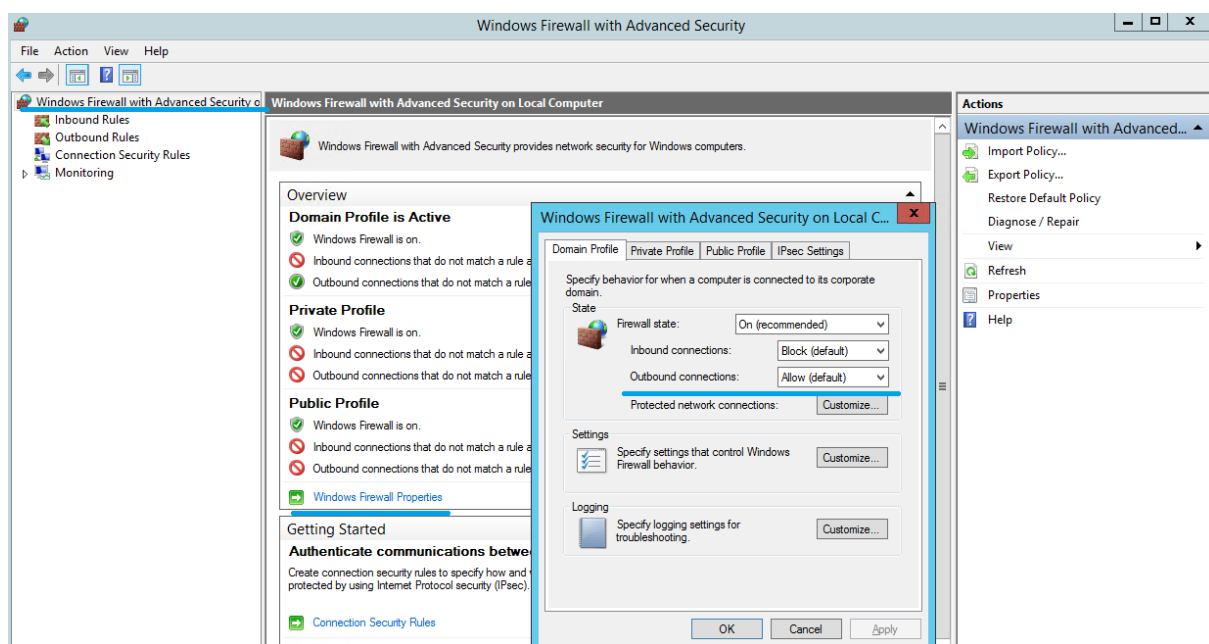
7. 上記の手順を、[ファイルサーバーリモート管理 (SMB 受信)] と [ファイルとプリンターの共有 (NB セッション 受信)] の各 受信 規則に対しても実行します。

セルフサービスパスワードリセットサーバーのファイアウォールを構成する

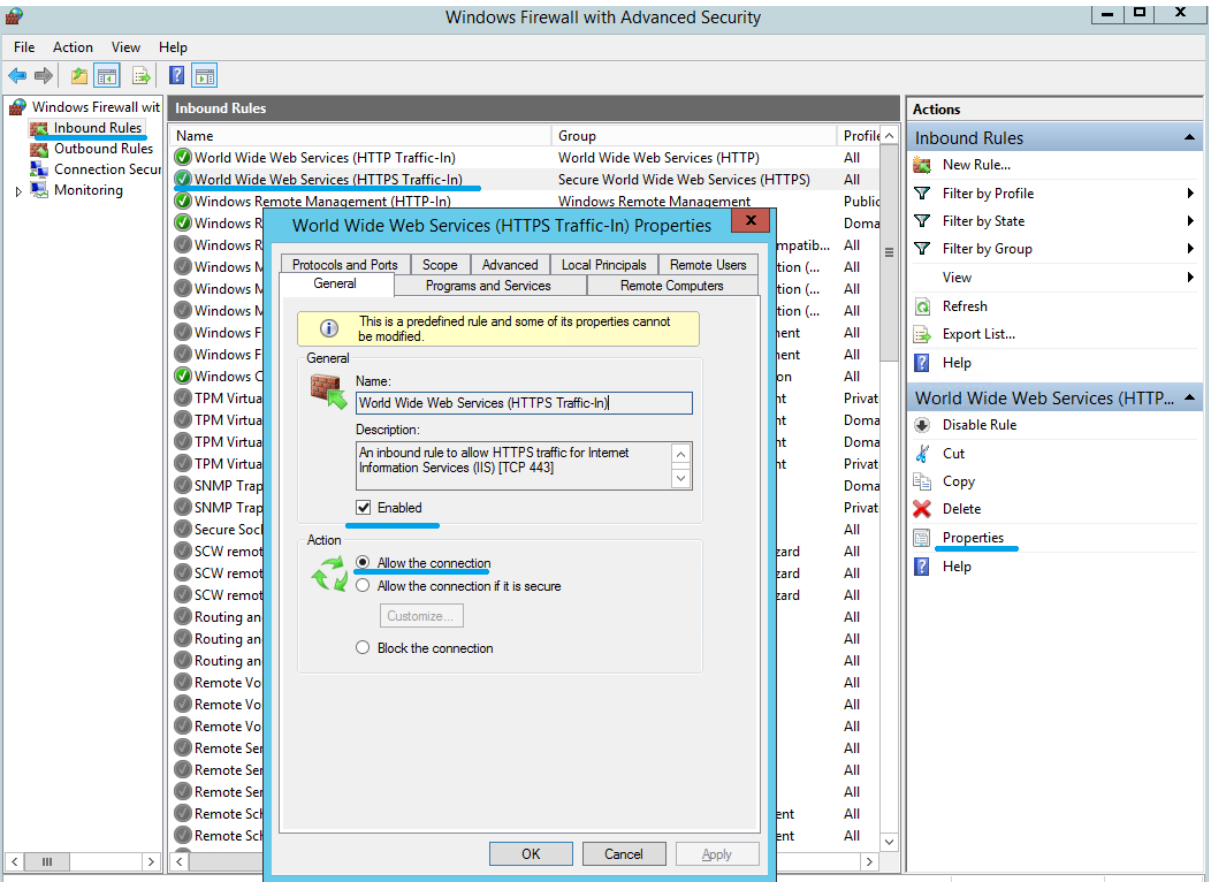
構成が完了すると、セルフサービスパスワードリセットサーバーから提供される Web サービスには、HTTPS を使用した StoreFront サーバーのみがアクセスできるようになります。また、セルフサービスパスワードリセットサーバーは、社内ネットワークにあるサービスにアクセスできるようになります。

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] に設定します。また、[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)] を選択します。この規則を [有効] 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 サービス (HTTP トラフィック) のプロパティ] で [詳細設定] タブに移動します。[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)] を選択します。この規則を [有効] 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] タブに移動します。[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 サービス (HTTPS トラフィック) のプロパティ] で [詳細設定] タブに移動します。[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

June 28, 2022

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、セキュリティの質問と回答、およびユーザーに関するその他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 中央ストアからセルフサービスパスワードリセット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

パスワードポリシー - サポートされません

アプリケーションテンプレート - サポートされません

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 - セルフサービスパスワードリセット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 - セルフサービスパスワードリセットコンソールで作成します

移行可能

登録データを含む People フォルダー

顧客が使用する質問リスト

重要

- 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、セルフサービスパスワードリセットのインストールと設定について把握しておいてください。詳しくは、「インストールと構成」を参照してください。

- 新しい中央ストアを作成します。
- セルフサービスパスワードリセットのサービスおよびコンソールをインストールします。
- コンソールで新しい中央ストアの場所を指定します。
- 新しいユーザー設定を作成し、Single Sign-On のセルフサービスパスワードリセット権限を持つユーザーを含めます。
- 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：データプロキシ用のアカウントに、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権限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

変更後は以下の通り

\\SSPR-SVC\citrixsync\$\People

次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の質問をコピーします。

****\\SSO-SERVER**citrixsync\$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\
QuestionBasedAuthentication2**

コピー先

****\\SSPR-SVC**citrixsync\$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\
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**

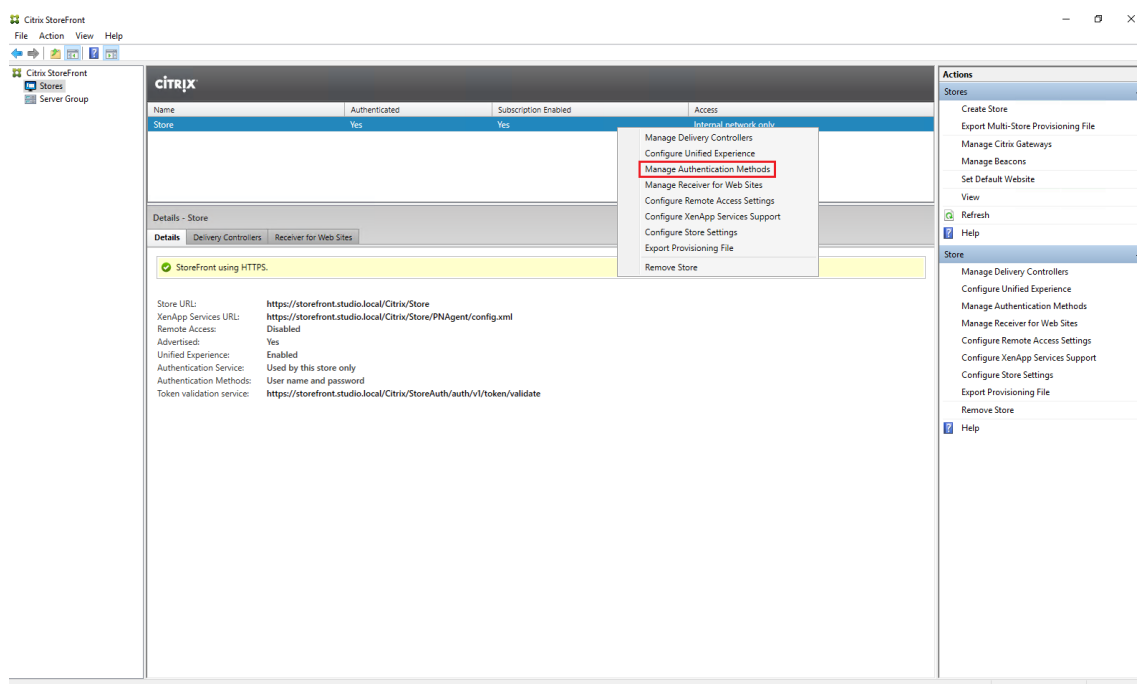
これで、すべてのユーザーが Single Sign-On の登録時の質問と回答を使用して、ロック解除およびリセットを実行できるようになりました。

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

June 29, 2022

セキュリティ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。

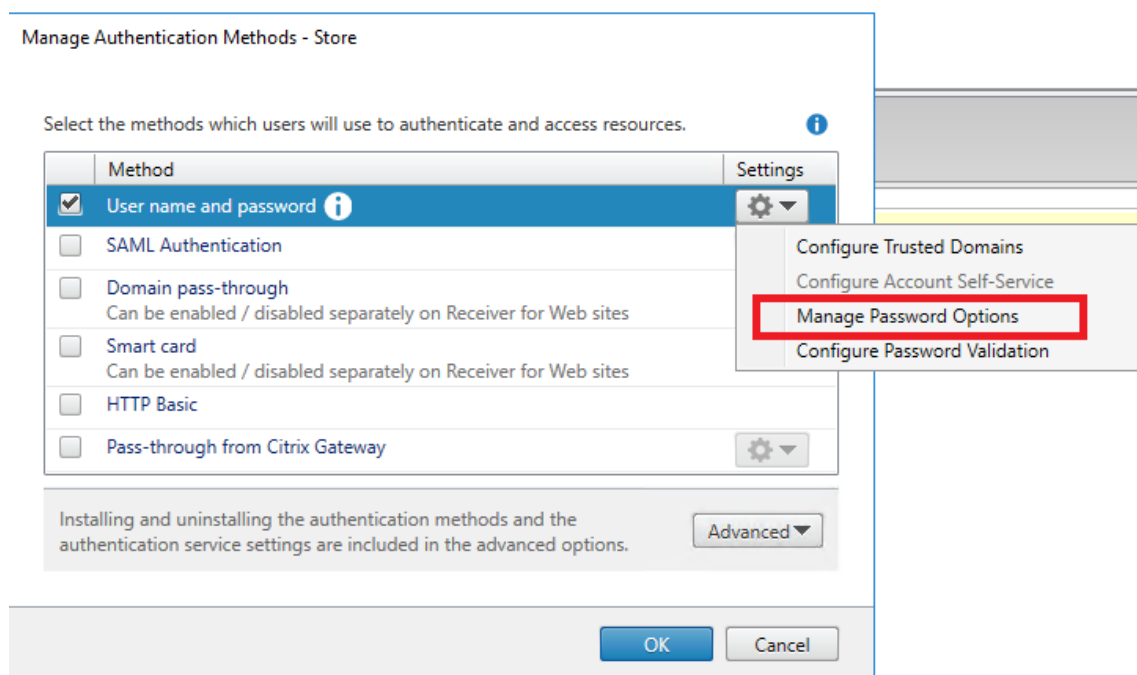
1. HTTPS に対して StoreFront インターネットインフォメーションサービス (IIS) を構成します。
2. StoreFront で展開を作成します。
3. CStoreFront 管理コンソールの右ペインで、ストアを右クリックして 「認証方法の管理」 を選択します。



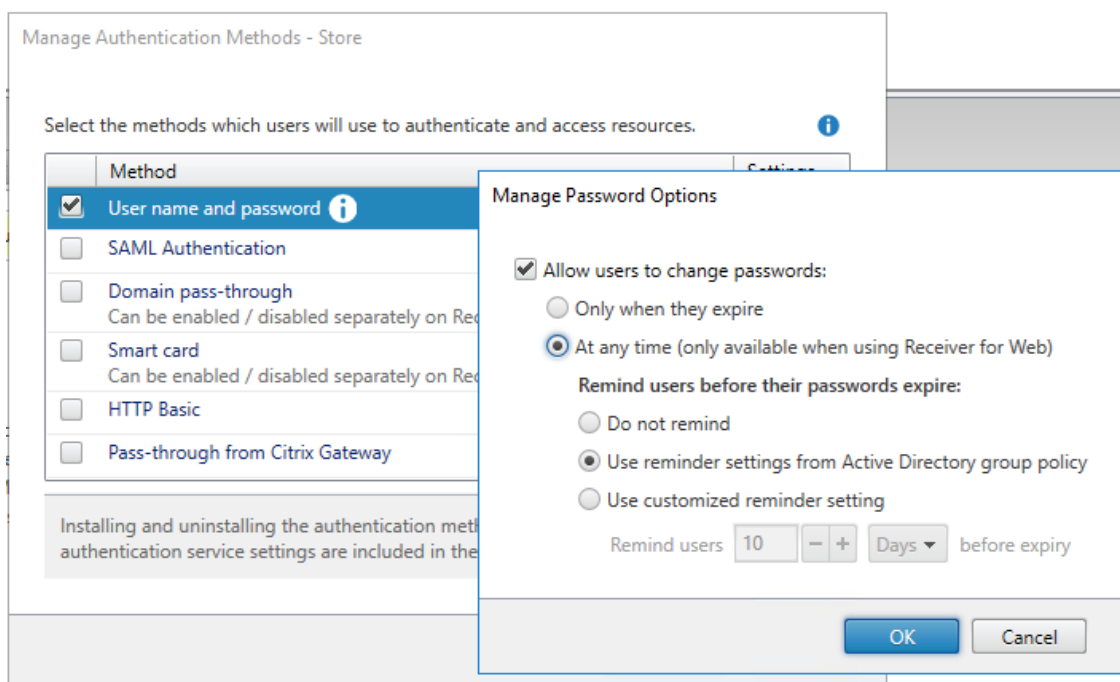
4. [ユーザー名とパスワード] の設定で、[パスワードオプションの管理] を選択します。

注:

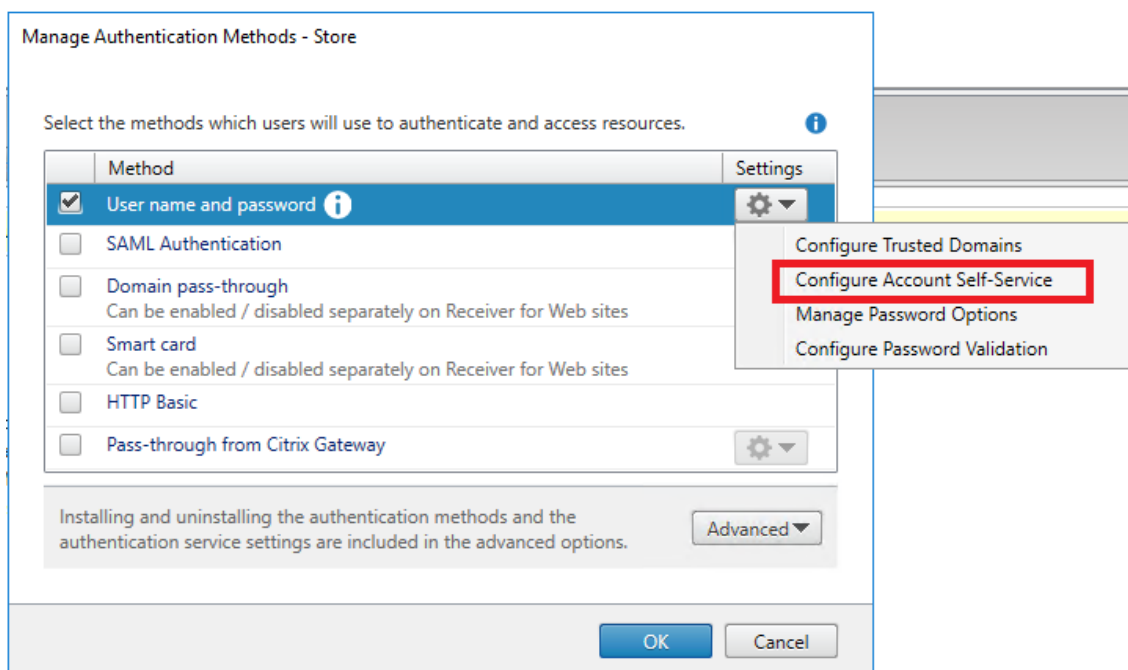
セルフサービスパスワードリセット（SSPR）では、StoreFront の認証方法として、ユーザー名とパスワードのみがサポートされます。ドメインパススルーなどの他の方法はサポートされません。



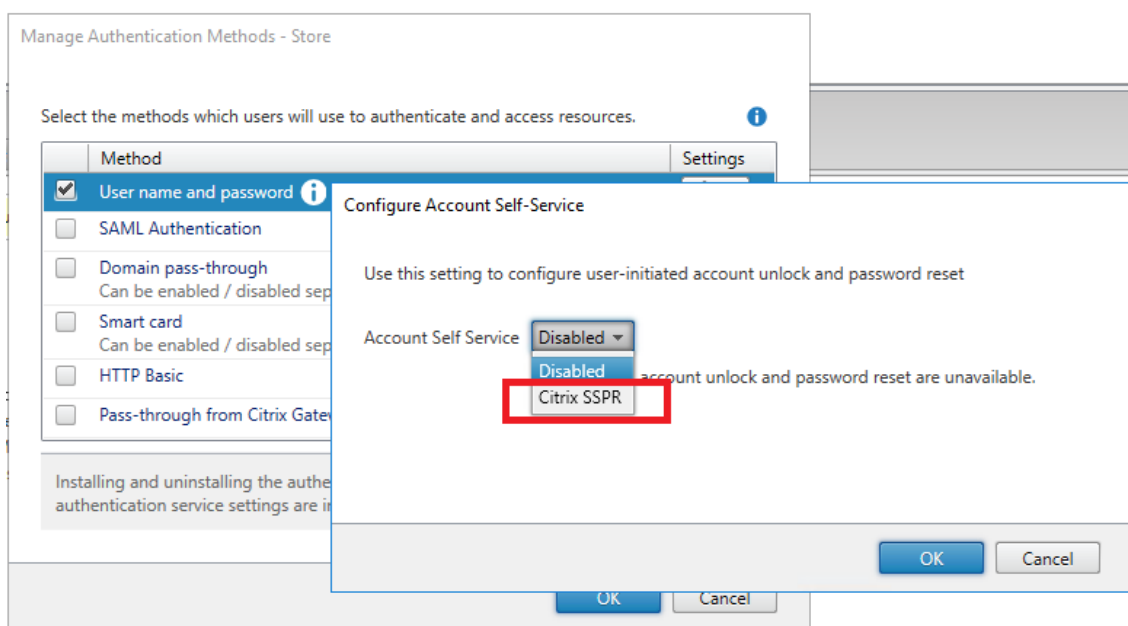
5. パスワードの変更を許可するユーザーを選択し、[OK] をクリックします。



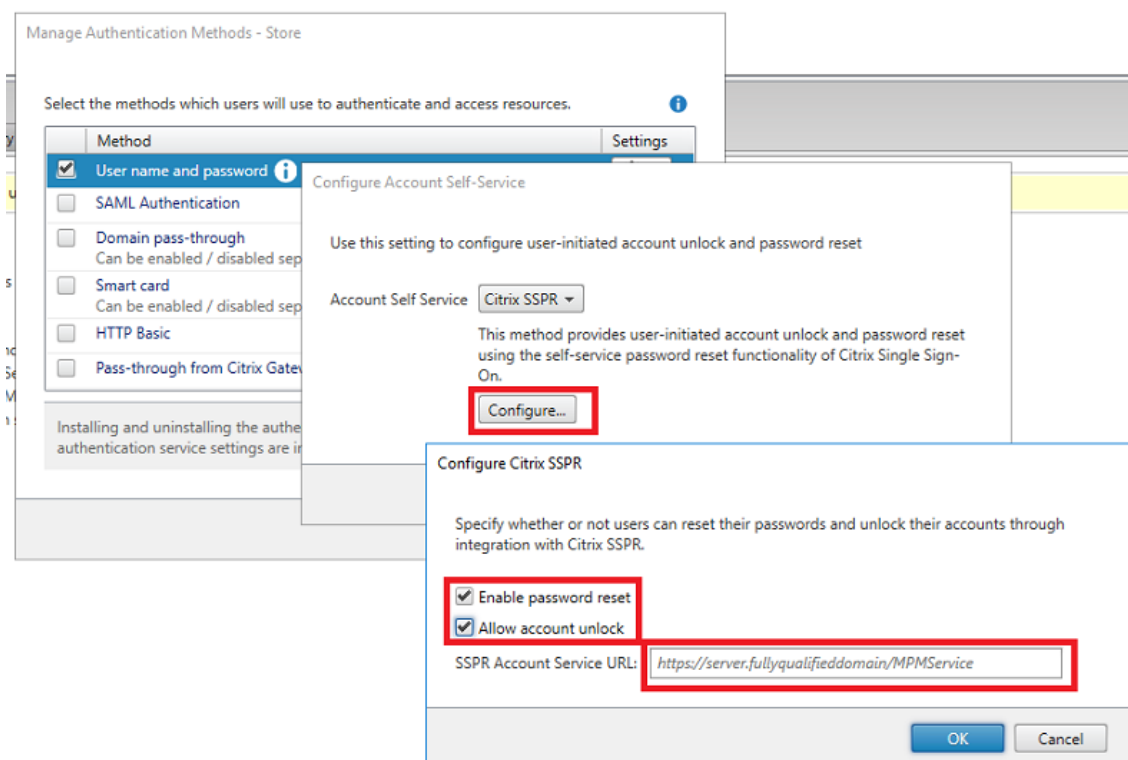
6. [ユーザー名とパスワード] の設定で、[アカウントセルフサービスの構成] を選択します。



7. [Citrix SSPR] を選択して、[アカウントセルフサービス] を有効にします。



8. [構成] をクリックして、[パスワードリセットを有効にする] と [アカウントのロック解除を許可する] のチェックボックスをオンにし、[SSPR アカウントサービス URL] を構成します (https://<FQDN of the SSPR server>/MPMService)。

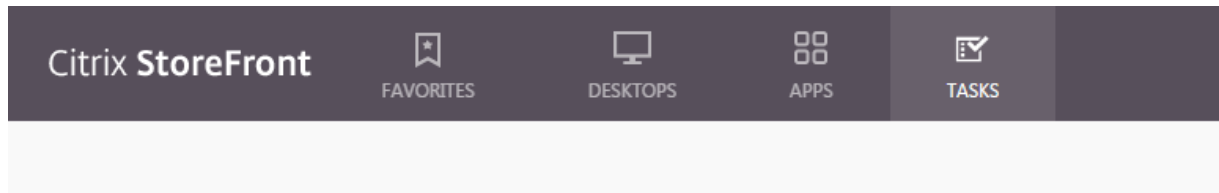


9. [OK] をクリックして、すべての設定内容を適用します。

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します。

Citrix Workspace アプリまたは Web 向け Citrix Workspace アプリへの次回ユーザーログオン時に、セキュリティの質問に対する回答を登録できるようになります。ユーザーが [開始] をクリックすると、今後のパスワードのリセットやアカウントのロック解除に使用されるセキュリティの質問に対する回答を指定できます。



[Start](#)

Manage Security Questions



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).