citrix

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。

	сіткіх: StoreFront
User name:	þomain\user or user@domain.com
Password.	Log On Account Self-Service

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/currentrelease/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 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。

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/selfservice-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、 <mark>https:</mark>
//www.citrix.com/downloads/licensing.htmlກຣ
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。
- 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。

[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。

눰 New Share Wizard		– 🗆 ×
New Share Wizard Select the profile for Select Profile Share Location Share Name Other Settings Permissions Confirmation Beauty	File share profile: SMB Share - Quick SMB Share - Advanced SMB Share - Applications NFS Share - Quick NFS Share - Advanced	 — — ×
	< P	revious Next > Create Cancel

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。

Server Frome	Server:				
Share Location	Server Name	Status	Cluster Role	Owner Node	
Share Name	SSPRServer	Online	Not Clustered		
Permissions					
	Share location:				
	Select by volume:				
	Volume	Free Space	Capacity File Sys	tem	
	C:	184 GB	200 GB NTFS		
	The location of the f	ile share will be a new fo	lder in the \Shares d	irectory on the sel	acted
	volume.				
	volume.				

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	– 🗆 X
Specify share nam	e
Select Profile	Share name:
Share Location Share Name	Share description:
Other Settings Permissions	
Confirmation	Local path to share:
Results	C:\Shares\CITRIXSYNC\$ I fi 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。

📥 New Share Wizard	- 🗆 X
Configure share s	Enable access-based enumeration
Share Location Share Name Other Settings	access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.
Permissions Confirmation	Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.
	BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.
	When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.
	< Previous Next > Create Cancel

 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。

눰 New Share Wizard				-		×
Specify permission	ns to co	ontrol access				
Select Profile Share Location	Permission permission	s to access the files on a sha is, and, optionally, a central a	are are set using a access policy.	combination of folder per	missions,	share
Share Name	Share pern	nissions: Custom				
Other Settings	Folder per	missions:				
Permissions	Туре	Principal	Access	Applies To		
Confirmation	Allow	BUILTIN\Users	Read & execu	This folder, subfolders, a	nd files	
	Allow	BUILTIN\Users	Special	This folder and subfolder	rs	
	Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, a	nd files	
	Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, a	nd files	
	Allow	CREATOR OWNER	Full Control	Subfolders and files only		
	Custom	ize permissions				
		< F	Previous	xt > Create	Ca	ncel

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。

New Share Wizard Specify permission Select Profile Share Location Share Name Other Settings Permissions Confirmation Results For additional information Permission entries: Type Principal Allow SystEM Allow SystEM Allow Users (ZMAKG-CLIENT3\Administrators) Change Value Auditing Effective Access Volume about to block Inheritance Volume about to block Inheritance to this object, which means that permissions inherited permissions inherited permissions inherited permissions inherited permissions inherited permissions inherited permissions on this object.		
Specify permission Select Profile Share Location Share Name Other Settings	Advanced Security Settings for CITRIXSYNC\$ Name: C:\Shares\CITRIXSYNC\$ Owner: Administrators (ZMAKG-CLIENT3\Administrators) Change Permissions Share Auditing Effective Access	
Share Name Other Settings Permissions Confirmation Results	For additional information Block Inheritance Permission entries: Type Principal Allow Principal Mainistrat Allow Administrat Tinherited from a parent object will no longer be applied to this object. Allow Users (ZMA CREATOR C Allow CREATOR C Remove all inherited permissions from this object.	ted permissions? hat permissions d files bject. d files ermissions on s bbject.
	Add Remove Disable inheritance Replace all child object permission entries with inheritable permission entries from this object	Cancel K Cancel Apply

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。

ame:	C:\Shares\CITRIXSYNC\$			
wner:	Administrators (SSPRSERV	ER\Administrators) <u>C</u> han	ge	
ermissio	ns Share Aud	iting Effective Access	5	
mission Type	entries: Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (SSPRSERVER	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Modify	None	Subfolders and files only
Allow	DataProxyAccount (SSPR\Da	t Full control	None	This folder, subfolders and files
A <u>d</u> d	<u>R</u> emove <u>E</u> dit			
Enable j Replace	nheritance all child object permission entrie	es with inheritable permiss	ion entries from this object	

- 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

Name:	C:\Shares\CITRIXS	SYNC\$	Principal:	CREATOR OWNER Select a principal		
Owner:	Administrators (SS	SPRSERVER\A	Туре:	Allow	~	
Permissions	Share	Auditing	Applies to:	Subfolders and files only	~	
For additional	l information, double	-click a permi				
Permission en	ntries:		Advanced p	permissions:		
Туре	Principal		L	Full control		Write attributes
Allow	SYSTEM			Traverse folder / execute file		Write extended attributes
🚨 Allow	Administrators (SSP)	RSERVER\		List folder / read data		Delete subfolders and files
🚨 Allow	CREATOR OWNER			Read attributes		✓ Delete
				Read extended attributes		Read permissions
				Create files / write data		Change permissions
				Create folders / append data		Take ownership
			Only app	ly these permissions to objects and/or container	s within this contai	ner
A <u>d</u> d	Remove	<u>E</u> dit				
Enable jnh	eritance		Add a cond	ition to limit access. The principal will be granted	d the specified perr	nissions only if conditions are met.
Replace all	child object permissi	on entries wit	Add a cond	ition		

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。

lame	e:	C:\Shares\CITRIX	SYNC\$				
)wne	er:	Administrators (S	SPRSERVER\Ad	ministrators) <u>C</u> hange			
Pern	nissions	Share	Auditing	Effective Access			
o m letw erm	odify shai ork locati ission ent	re permissions, sele on for this share: \' ries:	ct the entry and	i click Edit. r.local\CITRIXSYNC\$			
	Туре	Principal			Access		
92	Allow	Administrators (SSPRSERVER\Administrators)			Full Control		
2	Allow	Domain Adm	nins (SSPR\Dom	ain Admins)	Full Control		
2	Allow	DataProxyAc	count (SSPR\Da	taProxyAccount)	Full Control		

- 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。

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。

Delivery Controller Virtual Delivery Agent for Windows Server OS Start here. Select and install the Delivery Controller and other essential services like License Server and StoreFront. Install this agent to deliver applications and desktops from se based VMs or physical machines. Extend Deployment Citrix Studio Solf Service Descuered Paget	Get Started			Prepare Machines and Images			
Start here. Select and install the Delivery Controller and other essential services like License Server and StoreFront. Extend Deployment Citrix Director	Delivery Controller		Virtual Delivery Agent for Windows Server OS				
Extend Deployment	Start here. Select and install the Delivery Controller and other essential services like License Server and StoreFront.		Install this agent to deliver applications and desktops from server based VMs or physical machines.			rver-	
Citrix Director I Citrix Studio I Solf Service Descuard Paget	end Deployment						
Citità Director Sen-Service Password Reset	rix Director		Citrix Studio			Self-Service Password Reset	(
Citrix License Server (i) Universal Print Server (i) Session Recording	rix License Server		Universal Print Server			Session Recording	i
Citrix StoreFront i Federated Authentication Service i			Federated Authentication Servi				

- 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。

Create Self-Service Password Reset Service

#	Self-Service Password Reset Configuration	_ D X
I File Action View Window Help		- 6 ×
Self-Service Password Reset Configuration	CITRIX *	Actions
Service Configuration Configuration Configuration Configuration	Service Configuration First configure your Self-Service Password Reset servicee User Configuration Add a user configuration to domain users	Self-Service Password Reset Configuration
	Identity Verification To manage your questionnaire	

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。

Password Reset	Central Store Location
	Identify your central store location.
✓ Welcome Central Store Location	Set Store Location(NTFS) NTFS network share
Domain Configurations	Enter the UNC path to the central store of your Self-Service Password Reset environment \\SSPRSERVER.sspr.local\CITRIXSYNC\$
Apply Settings	
	Back Next Cancel

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。

e self-selfice Passiford Reset sel	ince		
Password Reset	Domain Configuration	ns	summer on that down in Theo select one
Welcome	domain and click Propert	ties to open the Edit Configurati	on wizard.
Welcome	Domain Name	Data Proxy Account	Self-Service Account
Central Store Location	sspr.local		
Domain Configurations			
	Properties	Remove	

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。

Create Self-Service Password Reset Ser	rvice	Self-Service Password Reset Service Domain Configuration
Password Reset	Domain Configurations	Provide the data proxy with an account that has read and write access to the central store. Data Proxy Account(Domain)Account) User Name Servi DataProxyAccount
✔ Welcome	Select the check box next domain and click Propertie	Password *******
Central Store Location	Domain Name	Confirm
Apply Settings		Provide account credentials for the Self-Service module. The account requires sufficient privileges to reset user domain passwords and to unlock domain user accounts.
		Self-Service Account(Domain\Account) User Name sspr\SelfServiceAccount
		Password ******** Confirm ******
	Properties	OK Cancel
	I	Back Next Cancel

5. [次へ]をクリックして、すべての設定内容を適用します。

Password Reset	Domain Configuratio	ns	
	Select the check box new domain and click Proper	t to a domain to enable service supp ties to open the Edit Configuration w	ort on that domain. Then select on vizard.
Welcome	Domain Name	Data Proxy Account	Self-Service Account
Central Store Location	sspr.local	sspr.local\DataProxyAccount	sspr.local\SelfServiceAccount

6. [終了] をクリックして、構成を完了します。

Password Reset	Apply Settings			
	Status			
✔ Welcome	A Don't close this wizard until applying settings is finished!			
Central Store Location				
 Domain Configurations 	Details			
Apply Settings	Creating performance counters	-		
	Stop CSSPR Active Directory Connector COM+ application			
	Stop Self-Service Password Reset Data Proxy COM+ application			
	Import configuration templates			
	Save Self-Service Password Reset Active Directory Connector COM+ application confi			
	Saving data proxy configuration file			
	Saving data proxy event log source			
	Save Signing Certificate configuration			
	Validating signing certificate configuration			
	Creating signing certificate			
	Save Self-Service Password Reset Data Proxy COM+ application configuration			
	Saving Self-Service account configuration	-		
	Les energy and a second s			

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。

 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。

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

Password Reset	Configure Licensing
	Specify the License Server name and port number for this user configuration.
 Name User Configuration Configure Licensing 	You can use the Self-Service Password Reset feature only when you have XenApp or XenDesktop Platinum Edition.
Enable Self-Service Password Reset	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	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
✓ Name User Configuration	
Configure Licensing	Reset: Allow users to reset their primary domain password
Enable Self-Service Password Reset	Unlock: Allow users to unlock their domain account
	Please provide the service address below.
_	Service port: 443
	Https:// SSPRServer.sspr.local/MPMService/
_	
	Back Contra
	Back Create Cancel

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。
- (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。
- [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。

#	Window	s Firewall with Advanced Security	_ 🗆 X
File Action View Help			
🗢 🔿 💽 🚺			
Windows Firewall with Advanced Security o	Windows Firewall with Advanced Security on Lo	cal Computer	Actions
 Inbound Rules Outbound Rules Connection Security Rules Monitoring 	Windows Firewall with Advanced Security prov	rides network security for Windows computers.	Windows Firewall with Advanced Import Policy Export Policy
	Overview	A	Restore Default Policy
	Domain Profile is Active	Windows Firewall with Advanced Security on Local C	Diagnose / Repair
	Windows Firewall is on.	Domain Profile Private Profile Public Profile IPsec Settings	View 🕨
	Outbound connections that do not match a rule	Specify behavior for when a computer is connected to its corporate	Q Refresh
	Cubound connections that do not match a rule Private Profile Windows Frewall is on. Indown connections that do not match a rule Outbound connections that do not match a rule	domain. State	Properties
		Frewall state: On (recommended) v Inbound connections: Block (default) v Outbound connections: Allow (default) v	👔 Help
	Public Profile	Protected network connections: Customize	
S S Get Au	 Windows Firewall is on. Inbound connections that do not match a rule a Outbound connections that do not match a rule 	Settings Specify settings that control Windows Frewall behavior.	
	Windows Firewall Properties Getting Started Authenticate communications between	Logging Specify logging settings for troubleshooting.	
	Create connection security rules to specify how and protected by using Internet Protocol security (IPsec).		
	Connection Security Rules	OK Cancel Apply	

[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。

					Windows Firewall with Advanced Security
File Action View H	Help				
🗢 🄿 🙍 🔜	?				
P Windows Firewall wit	Inbound Rules			Actions	
Windows Friewall with Mindows Friewall with Mindows Rules Coutbound Rules Coutbound Rules Connection Secur Monitoring Monitoring	Inbound Rules Name Core Networking - Router Advertisement (ICMPv6-In) Core Networking - Treado (UDP-In) Core Networking - Treado (UDP-In) Core Networking - Treado (UDP-In) Distributed Transaction Coordinator (RPC-IP) File and Printer Sharing (Echo Request - ICMPv6-In) File and Printer Sharing (NB-Datagram-In) File and Printer Sharing (NB-Session-In) File and Printer Sharing (Spooler Service - RPC) File Server Remote Management (DCM-In) File Server Remo	Group Core Networking Core Networking Core Networking Core Networking Core Networking Distributed Transaction Coo Distributed Transaction Coo Distributed Transaction Coo File and Printer Sharing File Server Remote Manage File Serv	Pr A AI AI AI <t< th=""><th>ictions nbound Rules New Rule ▼ Filter by Profile ▼ Filter by Group View ♥ Filter by Group View ♥ Filter by Group View ♥ Filter by Group ♥ Disable Rule ♥ Cut ♥ Cut ♥ Copy ♥ Delete ♥ Properties ♥ Help</th><th>File and Printer Sharing (SMB-In) Properties X Protocols and Ports Scope Advanced Local Principals Remote Users Ceneral Programs and Services Remote Computers With the content of the properties cannot be modified. General Name: It is a predefined rule and some of its properties cannot be modified. Description: Mane: It is an interesting (SUBE) Description: Inbound rule for File and Printer Sharing to allow Server It is bound rule for File and Printer Sharing to allow Server Image: Image: Image: Image:</th></t<>	ictions nbound Rules New Rule ▼ Filter by Profile ▼ Filter by Group View ♥ Filter by Group View ♥ Filter by Group View ♥ Filter by Group ♥ Disable Rule ♥ Cut ♥ Cut ♥ Copy ♥ Delete ♥ Properties ♥ Help	File and Printer Sharing (SMB-In) Properties X Protocols and Ports Scope Advanced Local Principals Remote Users Ceneral Programs and Services Remote Computers With the content of the properties cannot be modified. General Name: It is a predefined rule and some of its properties cannot be modified. Description: Mane: It is an interesting (SUBE) Description: Inbound rule for File and Printer Sharing to allow Server It is bound rule for File and Printer Sharing to allow Server Image: Image: Image: Image:
	Network Discovery (WSD EventsSecure-In) Network Discovery (WSD-In) Performance Logs and Alerts (DCOM-In)	Network Discovery Network Discovery Performance Logs and Alerts	Al Al Do		O Block the connection

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。



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。

@		Windows Firewall v	vith Advanced Security			– – X
File Action View H	lelp					
🗢 🄿 🙍 🔜						
Windows Firewall wit	Inbound Rules					Actions
Windows Firewall wit	Inbound Rules Name World Wide Web Services (HTTP Tra World Wide Web Services (HTTP Tra Windows R Windows F Windows R Windows R Windows R Windows P ShMP Trap SNMP Trap SNMP Trap SCW remot SCW remot SCW remot SCW remot SCW remot SCW remot Scuting an Routing an Remote Vo Remote Vo	Grou ffic-In) Worl affic-In) Secu TP-In) Winc b Services (HTTPS Traffic Scope Advanced Loca Programs and Services redefined rule and some of its pr d. e Web Services (HTTPS Traffic c events of the secure of the secure services (IIS) [TCP 443] d e connection the connection	p d Wide Web Services (HTTP) re World Wide Web Services (lows Remote Management ic-In) Properties Remote Computers Remote Computers operties cannot	HTTPS) All HTTPS) All Public In mpatiba All tion (All tion (All tion (All tion (All hent All hent All hent All hent Dom ht Dom ht Dom ht Dom ht Dom ht All ard All ard All ard All ard All All All All All All	€ ^ c a = t t t	Actions Inbound Rules ▲ Inbound Rules ▼ Intervention Filter by Profile Image: Filter by Profile ▶ Image: Filter by State ▶ Image: Filter by Group ▶ Image: Filter by Gr
	Remote Ser Remote Ser Remote Ser			All All All		
	Remote Sch			ent All		
< 111 >	Remote Sch	ОК	Cancel Apply	ent All	~	

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	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 アプリケーション定義 - サポートされません	顧客が使用する質問リスト
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	

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。

- 1. 新しい中央ストアを作成します。
- 2. 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。
- 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。
- 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。

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

コピー先

\\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。

citaly			Actions
CITRIX			Stores
Citricity Name Authenticated Store Yes Details - Store The store Details - Store The store Details - Store The store of the Stass Store URL: https://storefront.studio.local/Citrix/Store/PR Advertication Disability Divided Sprivices URL: https://storefront.studio.local/Citrix/Store/PR Advertication Disability Used by this store only Authentication Service: Authentication Service: https://storefront.studio.local/Citrix/StoreAuthentication Service: Store validation service: https://storefront.studio.local/Citrix/StoreAuthentication Service:	Subscription Enabled Vice	Access brand detents (orb) Manago Eleviery Controllers Configure Unitied Experience Managa Autentication Methods Configure Rendep Services Settings Configure Rendep Services Support Configure Store Settings Export Provisioning File Remove Store	Actions Stores Create Store Export Multi-Store Provisioning I Manage Citric Gleways Manage Cencons Set Default Website View Image Delivery Controllers Configure Unified Sperience Manage Delivery Controllers Configure Entroth Access Setting Configure XenApp Services Settings Export Multi-Store Foreioning File Remove Store Image Actional Store

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。

	Method	Settin	as	
	User name and password 🧃	Ö		
	SAML Authentication		Configure	Trusted Domains
	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites		Configure Manage Pa	Account Self-Service assword Options
	Smart card Can be enabled / disabled separately on Receiver for Web sites		Configure	Password Validation
	HTTP Basic			
	Pass-through from Citrix Gateway	-Q-		
ta :h	alling and uninstalling the authentication methods and the entication service settings are included in the advanced options.	Advanced	•	

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。

	Method	C-min
	User name and password 👔	Manage Password Options
	SAML Authentication	Allow was to shance persuade:
	Domain pass-through Can be enabled / disabled separately on Red	 Only when they expire
	Smart card Can be enabled / disabled separately on Red	At any time (only available when using Receiver for Web) Remind users before their passwords expire:
	HTTP Basic	Do not remind
	Pass-through from Citrix Gateway	 Use reminder settings from Active Directory group policities
Insta auth	alling and uninstalling the authentication methentication service settings are included in the	Use customized reminder setting Remind users 10 -+ Days - before expiry

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。

	Method	Settin	qs	
	User name and password 👔	0	-	
	SAML Authentication		Configu	ire Trusted Domains
	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites		Configu Manage	re Account Self-Service Password Options
	Smart card Can be enabled / disabled separately on Receiver for Web sites		Configu	ire Password Validation
	HTTP Basic			
	Pass-through from Citrix Gateway	- Q-		
nsta uth	alling and uninstalling the authentication methods and the entication service settings are included in the advanced options.	Advanced	•	

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。

elect	the methods which users will us	se to authenticate and access resources.
	Method	Settings
	SAML Authentication	Configure Account Self-Service
	Domain pass-through Can be enabled / disabled sep	Use this setting to configure user-initiated account unlock and password reset
	Smart card Can be enabled / disabled sep	Account Self Service Disabled -
	HTTP Basic	Disabled account unlock and password reset are unavailable.
	Pass-through from Citrix Gate	Citrix SSPR
Insta auth	alling and uninstalling the authe nentication service settings are in	
		OK Cancel

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)。

	Manage Authentication Methods - Stor	e	
	Select the methods which users will	use to authenticate and access resources.	
У	Method	Settings	
u	User name and password	Configure Account Self-Service	
	Domain pass-through Can be enabled / disabled se	Use this setting to configure user-initiated account unlock and password reset	
s	Smart card Can be enabled / disabled se	Account Self Service Citrix SSPR 🔻	
10	HTTP Basic	This method provides user-initiated account unlock and password reset using the self-service password reset functionality of Citrix Single Sign-	
Se M	Pass-through from Citrix Gate	On. Configure	
	Installing and uninstalling the auth authentication service settings are	Configure Citrix SSPR	
		Specify whether or not users can reset their passwords and unlock their accounts the integration with Citrix SSPR.	ough
		 Enable password reset Allow account unlock 	
		SSPR Account Service URL: https://server.fullyqualifieddomain/MPMService	
		ОК	Cancel

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。



Manage Security Questions

citrix

© 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).

© 1999–2024 Cloud Software Group, Inc. All rights reserved.