Self-Service-Kennwortzurücksetzung

Contents

Self-Service-Kennwortzurücksetzung 1.1.x

October 29, 2018

Mit Self-Service-Kennwortzurücksetzung haben die Benutzer mehr Kontrolle über ihre Benutzerkonten. Wenn Self-Service-Kennwortzurücksetzung konfiguriert ist, können Benutzer, die Probleme mit der Anmeldung haben, ihr Konto entsperren oder ihr Kennwort ändern, nachdem sie einige Sicherheitsfragen korrekt beantwortet haben.

Das Zurücksetzen von Benutzerkennwörtern ist grundsätzlich ein sicherheitstechnisch sensibler Vorgang. Stellen Sie anhand des Artikels Sichere Konfiguration sicher, dass Ihre Bereitstellung richtig konfiguriert ist.

Neue Features

October 29, 2018

Neue Features in Version 1.1.20

Sie können IP-Adressen konfigurieren, die eine Verbindung zum Self-Service-Kennwortzurücksetzungsdienst herstellen dürfen. Wenn Sie keine IP-Adresse eingeben, werden alle IP-Adressen auf die Positivliste gesetzt, dürfen also eine Verbindung herstellen.

Neue Features in Version 1.1.10

In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Neue Features in Version 1.1

Diese Version enthält die folgenden bedeutenden Verbesserungen:

- Unterstützung für Sperrlistenkonfiguration: IT-Administratoren können Benutzer und Gruppen einer Sperrliste hinzufügen. Die der Sperrliste hinzugefügten Benutzer und Gruppen können keine Features von Self-Service-Kennwortzurücksetzung verwenden.
- Unterstützung für vereinfachtes Chinesisch: Neben Englisch, Französisch, Japanisch und Spanisch ist nun auch vereinfachtes Chinesisch zum Definieren von Sicherheitsfragen verfügbar.

Self-Service-Kennwortzurücksetzung enthält drei Komponenten:

- Konfigurationskonsole von Self-Service-Kennwortzurücksetzung
- Self-Service-Kennwortzurücksetzung
- Sicherheitsfragenregistrierung in StoreFront

Konfigurationskonsole von Self-Service-Kennwortzurücksetzung

- **Dienstkonfiguration:** Konfiguration von Self-Service-Kennwortzurücksetzung, einschließlich der Adresse des zentralen Speichers, dem Datenproxykonto und dem Self-Service-Kennwortzurücksetzungsk
  - Adresse des zentralen Speichers: Netzwerkfreigabeort zum Speichern der Daten von Self-Service-Kennwortzurücksetzung.
  - Datenproxykonto: Kommuniziert mit dem zentralen Speicher. Das Konto muss Lese- und Schreibzugriff auf den zentralen Speicher haben.
  - Self-Service-Kennwortzurücksetzungskonto: Zum Entsperren des Kontos und Zurücksetzen des Kennworts.
- **Benutzerkonfiguration:** Konfiguration der Benutzer/Gruppen/Organisationseinheit, die Self-Service-Kennwortzurücksetzung verwenden, sowie Angabe der Lizenzserveradresse und Standarddienstadresse.
  - Benutzerkonfiguration benennen: Definieren der Zielbenutzergruppen für den Self-Service-Kennwortzurücksetzungsdienst. Benutzer/Gruppen/Organisationseinheiten aus Active Directory können eingeschlossen werden.
  - Lizenzserveradresse: Sie können Self-Service-Kennwortzurücksetzung nur mit XenApp oder XenDesktop Platinum Edition verwenden.Die Lizenzserverversion muss mindestens 11.13.1 oder höher sein.
  - Aktivieren oder deaktivieren Sie die Features **Entsperren** und **Zurücksetzen**.
  - Standarddienstadresse: Geben Sie die URL für den Self-Service-Kennwortzurücksetzungsdienst an.
- **Identitätsprüfung:** Konfiguration des Fragebogens, der für die Registrierung und zum Entsperren oder Zurücksetzen des Kennworts verwendet wird.
  - Fügen Sie eine Frage oder Fragengruppe zum Fragenspeicher hinzu. Damit werden dann Fragenkataloge erstellt.
  - Wählen Sie für die Registrierung eine Fragenliste aus dem Fragenspeicher aus.
  - Exportieren und importieren Sie Sicherheitsfragen oder Fragengruppen.

Self-Service-Kennwortzurücksetzung

Der Self-Service-Kennwortzurücksetzungsdienst wird auf einem Webserver ausgeführt und ermöglicht Benutzern, Windows-Kennwörter zurückzusetzen und die Sperrung von Windows-Konten aufzuheben. Die Anforderungen von Endbenutzern werden über StoreFront an den Dienst gesendet.

Sicherheitsfragenregistrierung in StoreFront

Mit StoreFront können Benutzer Antworten auf Sicherheitsfragen registrieren. Wenn sie sich registriert haben, können sie Domänenkennwörter zurücksetzen und die Sperrung von Domänenkonten aufheben. Weitere Informationen finden Sie im Abschnitt "Sicherheitsfragen bei Self-Service-Kennwortzurücksetzung" von Konfigurieren des Authentifizierungsdiensts.

Behobene Probleme

October 29, 2018

Version 1.1.20

In diesem Release wurden keine Probleme behoben.

Version 1.1.10

Die folgenden Probleme wurden in dieser Version behoben.

- Wenn Sie TLS 1.0 auf dem **Self-Service-Kennwortzurücksetzungsserver** deaktiviert haben, wird möglicherweise die folgende Fehlermeldung angezeigt, wenn Sie dem Assistenten die Server-URL hinzufügen:

  "Auf die Serveradresse kann nicht zugegriffen werden." [#LC7741]

- Wenn Sie die Funktion zum Zurücksetzen des Kennworts aktivieren und benutzerdefinierte Kennwortfilter auf dem Domänencontroller anwenden, funktioniert die Funktion zum Zurücksetzen des Kennworts möglicherweise nicht. Die folgende Fehlermeldung wird angezeigt:

  "Das angegebene Kennwort ist ungültig." [#LC7570]

Bekannte Probleme

October 29, 2018

Version 1.1.20

In dieser Version gibt es die folgenden bekannten Probleme.

- Das Hinzufügen einer Benutzergruppe im Benutzerkonfigurationsassistenten kann mit der Meldung fehlschlagen, dass die Benutzergruppe auf einer Sperrliste steht. Diese Meldung ist falsch. Das Hinzufügen ist fehlgeschlagen, weil die Benutzergruppe bereits vorhanden ist.

[#665520]

- Sie können keine Benutzer und Benutzergruppen hinzufügen, die Sie mit dem Konfigurationsassistenten gerade entfernt haben, bis der Entfernungsvorgang abgeschlossen ist und Sie den Assistenten schließen. Andernfalls wird eine falsche Fehlermeldung mit der Information angezeigt, dass die Benutzer oder Gruppen auf einer Sperrliste sind. Beenden Sie den Entfernungsvorgang und schließen Sie den Assistenten. Öffnen Sie den Assistenten dann erneut und fügen Sie die Benutzer oder Gruppen wieder hinzu.

[#665352]

- Wenn Sie ein Upgrade von Self-Service-Kennwortzurücksetzung auf Version 1.1 durchführen, während die Konsole der Version 1.0 geöffnet ist, erfolgt keine Reaktion und die offene Konsole der Version 1.0 kann nicht verwendet werden.

[# 664390]

- Ein Fehler kann auftreten, wenn Sie versuchen, unter Windows Server 2012 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.5 installiert ist, oder unter Windows Server 2016 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.6 installiert ist. Die Versuche schlagen fehl, weil beim direkten Upgrade oder bei der Deinstallation unter Windows Server 2012 und unter Windows Server 2016 eine Abhängigkeit von .Net Framework 3.5 besteht. Installieren Sie als Workaround .Net Framework 3.5, bevor Sie das Upgrade oder die Deinstallation durchführen.

[DNA-22761]

Version 1.1.10

In dieser Version gibt es die folgenden bekannten Probleme.

- Das Hinzufügen einer Benutzergruppe im Benutzerkonfigurationsassistenten kann mit der Meldung fehlschlagen, dass die Benutzergruppe auf einer Sperrliste steht. Diese Meldung ist falsch. Das Hinzufügen ist fehlgeschlagen, weil die Benutzergruppe bereits vorhanden ist.

[#665520]

- Sie können keine Benutzer und Benutzergruppen hinzufügen, die Sie mit dem Konfigurationsassistenten gerade entfernt haben, bis der Entfernungsvorgang abgeschlossen ist und Sie den Assistenten schließen. Andernfalls wird eine falsche Fehlermeldung mit der Information

angezeigt, dass die Benutzer oder Gruppen auf einer Sperrliste sind. Beenden Sie den Entfernungsvorgang und schließen Sie den Assistenten. Öffnen Sie den Assistenten dann erneut und fügen Sie die Benutzer oder Gruppen wieder hinzu.

[#665352]

- Wenn Sie ein Upgrade von Self-Service-Kennwortzurücksetzung auf Version 1.1 durchführen, während die Konsole der Version 1.0 geöffnet ist, erfolgt keine Reaktion und die offene Konsole der Version 1.0 kann nicht verwendet werden.

[# 664390]

- Ein Fehler kann auftreten, wenn Sie versuchen, unter Windows Server 2012 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.5 installiert ist, oder unter Windows Server 2016 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.6 installiert ist. Die Versuche schlagen fehl, weil beim direkten Upgrade oder bei der Deinstallation unter Windows Server 2012 und unter Windows Server 2016 eine Abhängigkeit von .Net Framework 3.5 besteht. Installieren Sie als Workaround .Net Framework 3.5, bevor Sie das Upgrade oder die Deinstallation durchführen.

[DNA-22761]

Version 1.1

In dieser Version gibt es die folgenden bekannten Probleme.

- Das Hinzufügen einer Benutzergruppe im Benutzerkonfigurationsassistenten kann mit der Meldung fehlschlagen, dass die Benutzergruppe auf einer Sperrliste steht. Diese Meldung ist falsch. Das Hinzufügen ist fehlgeschlagen, weil die Benutzergruppe bereits vorhanden ist.

[#665520]

- Sie können keine Benutzer und Benutzergruppen hinzufügen, die Sie mit dem Konfigurationsassistenten gerade entfernt haben, bis der Entfernungsvorgang abgeschlossen ist und Sie den Assistenten schließen. Andernfalls wird eine falsche Fehlermeldung mit der Information angezeigt, dass die Benutzer oder Gruppen auf einer Sperrliste sind. Beenden Sie den Entfernungsvorgang und schließen Sie den Assistenten. Öffnen Sie den Assistenten dann erneut und fügen Sie die Benutzer oder Gruppen wieder hinzu.

[#665352]

- Wenn Sie ein Upgrade von Self-Service-Kennwortzurücksetzung auf Version 1.1 durchführen, während die Konsole der Version 1.0 geöffnet ist, erfolgt keine Reaktion und die offene Konsole der Version 1.0 kann nicht verwendet werden.

[# 664390]

- Ein Fehler kann auftreten, wenn Sie versuchen, unter Windows Server 2012 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.5 installiert ist, oder unter Windows Server 2016 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.6 installiert ist. Die Versuche schlagen fehl, weil beim direkten Upgrade oder bei der Deinstallation unter Windows Server 2012 und unter Windows Server 2016 eine Abhängigkeit von .Net Framework 3.5 besteht. Installieren Sie als Workaround .Net Framework 3.5, bevor Sie das Upgrade oder die Deinstallation durchführen.

[DNA-22761]

Version 1.0

In dieser Version gibt es die folgenden bekannten Probleme.

- Wenn Sie die Self-Service-Kennwortzurücksetzungskonsole öffnen, können Sie sie u. U. nicht an der Taskleiste anheften.

[# 646300]

Workaround: Heften Sie die Konsole über die Verknüpfung im **Startmenü** an der Taskleiste an.

- Aufgrund eines bekannten Problems in Windows 2016 können Sie in Windows 2016 nicht nach der Self-Service-Kennwortzurücksetzungskonsole suchen.

[# 648939]

Workaround: Verwenden Sie das **Startmenü** zum Suchen von Self-Service-Kennwortzurücksetzung.

- Wenn das Mindestalter des Kennworts in der Kennwortrichtlinie in der Standarddomänenrichtlinie auf den Standardwert (1 Tag) festgelegt ist und das Zurücksetzen des Kennworts bei Benutzern fehlschlägt (z. B. wenn die Benutzer die Komplexitätsanforderung nicht erfüllen), können die Benutzer nach dem Schließen des Kennwortzurücksetzungsassistenten das Kennwort 24 Stunden lang nicht zurücksetzen.

[#653221]

- Beim Verwenden der Citrix Workspace-App für Mac wird die Schaltfläche zum Registrieren angezeigt, wenn der Benutzer sich zum ersten Mal an StoreFront anmeldet. Wenn der Benutzer sich dann von StoreFront ab- und wieder anmeldet, wird die Schaltfläche nicht mehr angezeigt.

[# 657263]

Workaround:

1. Klicken Sie auf den Benutzernamen rechts oben im StoreFront-Store.
2. Klicken Sie im Dropdownmenü auf die Schaltfläche **Apps aktualisieren**.
3. Schließen Sie die Citrix Workspace-App für Mac, öffnen Sie die Citrix Workspace-App für Mac neu und die Schaltfläche wird angezeigt.

- Beim Migrieren von Sicherheitsfragen aus der Identitätsprüfung für Single Sign-On nach Self-Service-Kennwortzurücksetzung werden die Fragen nach dem Klicken auf **Aktualisieren** u. U. nicht in der Self-Service-Kennwortzurücksetzungskonsole angezeigt.

[# 657277]

Workaround: Schließen Sie die Konsole und öffnen Sie sie wieder.

- Sicherheitsfragen im Fragenkatalog, die das Sonderzeichen **&** enthalten, werden während der Registrierung in StoreFront nicht angezeigt.

[# 654913]

Workaround: Verwenden Sie keine **&** in Sicherheitsfragen.

- Ein Fehler kann auftreten, wenn Sie versuchen, unter Windows Server 2012 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.5 installiert ist, oder unter Windows Server 2016 ein Upgrade oder eine Deinstallation durchzuführen, wenn nur .Net Framework 4.6 installiert ist. Die Versuche schlagen fehl, weil beim direkten Upgrade oder bei der Deinstallation unter Windows Server 2012 und unter Windows Server 2016 eine Abhängigkeit von .Net Framework 3.5 besteht. Installieren Sie als Workaround .Net Framework 3.5, bevor Sie das Upgrade oder die Deinstallation durchführen.

[DNA-22761]

Systemanforderungen

October 29, 2018

> **Wichtig**
>
> Citrix unterstützt nicht die Installation einer Komponente von Self-Service-Kennwortzurücksetzung auf einem Domänencontroller. Stellen Sie die Komponenten für Self-Service-Kennwortzurücksetzung auf dedizierten Servern bereit.

In diesem Abschnitt werden die Hardware- und Softwareanforderungen für die Self-Service-Kennwortzurücksetzungsumgebung beschrieben. Es wird vorausgesetzt, dass jeder Computer die hardwarebezogenen Mindestanforderungen für das installierte Betriebssystem erfüllt.

Software

Unter Umständen wird für Computer in der Self-Service-Kennwortzurücksetzungsumgebung folgende unterstützende Systemsoftware benötigt.

- **Windows 2016 und Windows 2012 R2** - Erforderlich für den Self-Service-Kennwortzurücksetzungsserver.

- **Microsoft Windows Installer 2.0 oder höher** - Erforderlich für alle.
- **Microsoft .NET Framework**: erforderlich für Self-Service-Kennwortzurücksetzungsserver.
  - 4.6.x (Windows 2016)
  - 4.5.2 (Windows 2012 R2)
- **Internetinformationsdienste (IIS)** - erforderlich für Self-Service-Kennwortzurücksetzungsserver.
  - IIS 10.0 (Windows 2016)
  - IIS 8.5 (Windows 2012 R2)
- **VC ++ 2008 SP1 Runtime** - Erforderlich für den Self-Service-Kennwortzurücksetzungsserver. Bei einer Erstinstallation müssen Sie vcredist_x86.exe von https://www.microsoft.com/en-us/download/details.aspx?id=26368 herunterladen und auf dem Self-Service-Kennwortzurücksetzungsserver installieren.

Self-Service-Kennwortzurücksetzungsserver

- Self-Service-Kennwortzurücksetzungskomponente - Zentraler Speicher
- Unterstützte Umgebung - SMB-Dateifreigabe
- Hardwareanforderung - 30 KB Speicherplatz pro Benutzer

Anforderungen von ASP.NET 3.5/4.X

Die ASP.NET-Komponente für Ihre Version von .NET Framework auf dem Windows Server-Computer.

Sicherheits- und Kontoanforderungen

Stellen Sie vor der Installation des Self-Service-Kennwortzurücksetzungsdienstes sicher, dass die entsprechenden Konten und Komponenten für die Unterstützung des Dienstes verfügbar sind. Da der Dienst sicheres HTTP (HTTPS) verwendet, wird ein Serverauthentifizierungszertifikat für die Kommunikation per TLS (Transport Layer Security) mit StoreFront benötigt.

Anforderungen für die Serverauthentifizierung:

Vor dem Installieren des Dienstes müssen Sie sich für die TLS-Kommunikation ein Serverauthentifizierungszertifikat bei einer Zertifizierungsstelle (CA) oder ggf. bei Ihrer internen PKI (Public Key Infrastructure) besorgen.

Für die Dienstmodule erforderliche Konten:

Hinweis: Stellen Sie sicher, dass für die Konten kein Ablaufdatum konfiguriert ist.

Die Konten für den Self-Service-Kennwortzurücksetzungsdienst müssen über Lese- und Schreibberechtigungen für Daten in Ihrer Umgebung verfügen.

- Konto für Datenproxy

- Self-Service-Konto

Wenn für unterschiedliche Module derselbe Kontotyp benötigt wird, können Sie dasselbe Konto für mehrere Module verwenden. Sie können auch für jedes Modul eigene benutzerdefinierte Konten angeben.

- **Konto für Datenproxy**

Konto benötigt Lese- und Schreibzugriff auf den zentralen Speicher. Weitere Informationen finden Sie im Abschnitt **Erstellen eines zentralen Speichers** von Installation und Konfiguration.

- **Self-Service-Konto**

Erfordert die Privilegien zum Entsperren und Zurücksetzen des Kennworts der relevanten Benutzer in "Benutzerkonfiguration". Weitere Informationen finden Sie unter Sichere Konfiguration.

StoreFront

- StoreFront 3.7
- StoreFront 3.8 oder höher

Citrix Workspace-App

Unterstützt:

- Citrix Workspace-App für Web
- Citrix Workspace-App für Windows
- Citrix Workspace-App für Linux
- Citrix Workspace-App für Mac (erfordert StoreFront 3.8)

Nicht unterstützt:

- Citrix Workspace-App für Chrome
- Mobile Geräte (nicht einmal mit der Citrix Workspace-App für Web)

Externe Verwendung mit Citrix Gateway

Nicht unterstützt

Installation und Konfiguration

October 29, 2018

Installations- und Konfigurationsprüfliste

Stellen Sie vor der Installation sicher, dass Sie die in dieser Liste aufgeführten Schritte abgeschlossen haben:

☒	Schritt
	Legen Sie fest, auf welchen Computern in der Umgebung die Software installiert wird und bereiten Sie die Computer für die Installation vor. Siehe Systemanforderungen.
	Installieren Sie das TLS-Zertifikat und die für den Dienst erforderlichen Konten. Siehe **Sicherheits- und Kontoanforderungen** unter Systemanforderungen.
	Installieren Sie den Lizenzserver. Siehe Lizenzserverdokumentation.
	Erstellen Sie einen zentralen Speicher. Siehe Erstellen eines zentralen Speichers.
	Installieren Sie Self-Service-Kennwortzurücksetzung. Siehe Installation und Konfiguration von Self-Service-Kennwortzurücksetzung.
	Konfigurieren Sie Self-Service-Kennwortzurücksetzung mit der Konsole. Siehe Installation und Konfiguration von Self-Service-Kennwortzurücksetzung.

☒	Schritt
	Konfigurieren Sie Self-Service-Kennwortzurücksetzung auf StoreFront. Siehe Konfigurieren von StoreFront.
	Stellen Sie sicher, dass Self-Service-Kennwortzurücksetzung sicher konfiguriert wurde. Siehe Sichere Konfiguration.
	Installieren Sie das SSL-Zertifikat und die für den Dienst erforderlichen Konten. Siehe **Sicherheits- und Kontoanforderungen** unter Systemanforderungen.
	Konfigurieren Sie Self-Service-Kennwortzurücksetzung in StoreFront. Siehe Konfigurieren von StoreFront.

Installations- und Konfigurationsreihenfolge

Damit Sie den Dienst installieren und den Assistenten für die Dienstkonfiguration ausführen können, muss das Konto, mit dem Sie sich anmelden, zur Gruppe der lokalen Administratoren auf dem Server gehören.

Es wird empfohlen, Self-Service-Kennwortzurücksetzung in der folgenden Reihenfolge zu installieren:

1. Installieren oder aktualisieren Sie den Lizenzserver mindestens auf Version 11.13.1.2.Laden Sie die aktuelle Lizenzserverversion herunter: https://www.citrix.com/downloads/licensing.html.
2. Erstellen Sie den zentralen Speicher.
3. Installieren Sie Self-Service-Kennwortzurücksetzung.
4. Konfigurieren Sie Self-Service-Kennwortzurücksetzung in der Konsole.
5. Konfigurieren Sie StoreFront mit der Adresse des Self-Service-Kennwortzurücksetzungsservers.

Erstellen eines zentralen Speichers

Zur Sicherheit empfiehlt es sich, den zentralen Speicher direkt auf der Maschine zu erstellen, auf der der Self-Service-Kennwortzurücksetzungsdienst ausgeführt wird. In Bereitstellungen, in denen mehr als ein Self-Service-Kennwortzurücksetzungsserver erforderlich ist, können Sie den zentralen Speicher auf einer Remotenetzwerkfreigabe hosten, wenn der Self-Service-Kennwortzurücksetzungsserver und der Server, der die Freigabe hostet, beide SMB-Verschlüsselung unterstützen.

Dieses Feature steht nur unter Windows Server 2012 R2 oder Windows Server 2016 zur Verfügung.

Erstellen eines Datenproxykontos

Erstellen Sie einen normalen Domänenbenutzer zum Verwenden als Datenproxykonto.Machen Sie keinen Benutzer der Gruppe “Domänenadministrator/Lokaler Administrator” zum Datenproxykonto.

Erstellen eines zentralen Speichers für Windows Server 2012 R2 oder Windows Server 2016

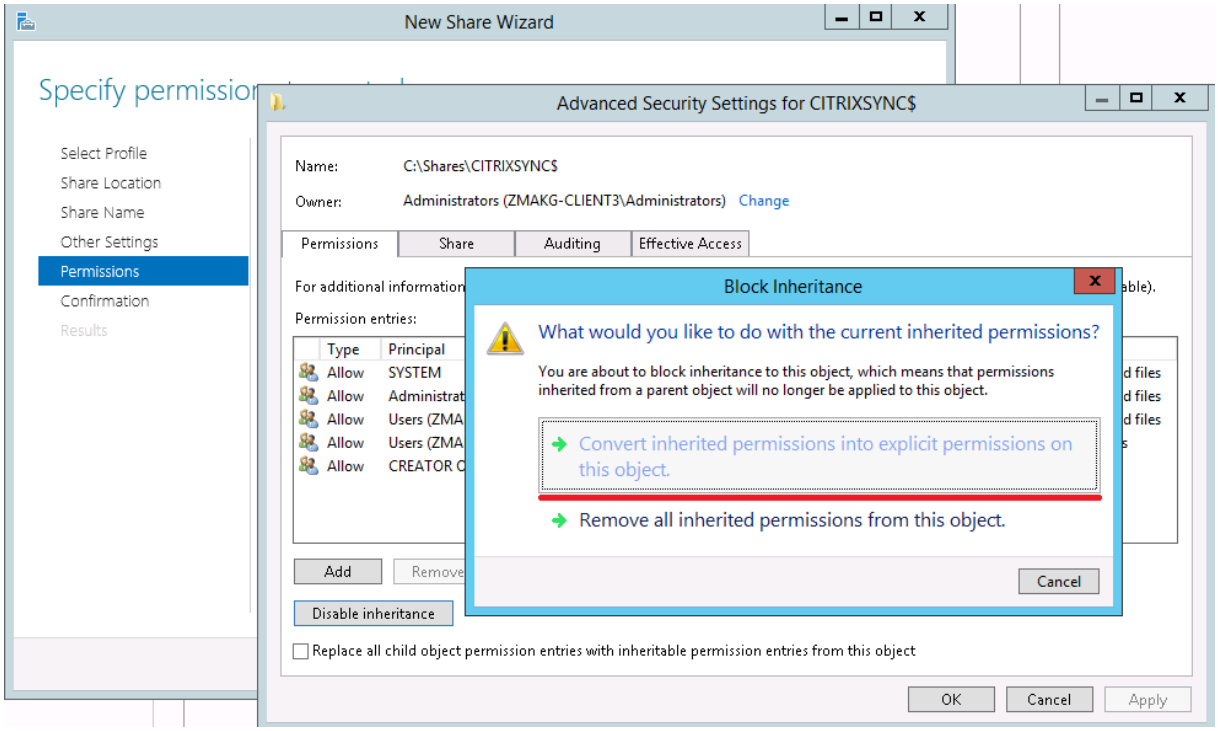
Wenn Sie Windows Server 2012 R2 oder Windows Server 2016 für den Self-Service-Kennwortzurücksetzungsserver und den zentralen Speicher verwenden, können Sie ggf. eine konfigurierte Remotenetzwerkfreigabe verwenden, wie in diesem Abschnitt beschrieben. Stellen Sie sicher, dass **Datenzugriff verschlüsseln** aktiviert ist und verfahren Sie entsprechend den Richtlinien unter Sichere Konfiguration.

1. Starten Sie den Assistenten **Neue Freigabe**, indem Sie den Server-Manager öffnen. Wählen Sie auf der Detailseite **Datei- und Speicherdienste** im linken Bereich **Freigaben** und klicken Sie dann auf **Aufgaben > Neue Freigabe**.
2. Wählen Sie im linken Bereich **Profil auswählen**, dann **SMB-Freigabe - Schnell** und klicken Sie auf **Weiter**.
3. Wählen Sie im linken Bereich **Freigabeort**. Wählen Sie aus der Liste den Server aus, auf dem die neue Freigabe erstellt wird, sowie das Volume, auf dem der neue freigegebene Ordner erstellt wird, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im linken Bereich **Freigabename**, geben Sie den Namen der neuen Freigabe ein, z. B. **CITRIXSYNC$**, und klicken Sie auf **Weiter**.
5. Wählen Sie im linken Bereich **Andere Einstellungen**, klicken Sie auf **Daten verschlüsseln**, deaktivieren Sie **Zwischenspeichern der Freigabe zulassen** und klicken Sie auf **Weiter**.
6. Passen Sie die Berechtigungen für **Freigabe** an, indem Sie im linken Bereich **Berechtigungen** und dann **Berechtigungen anpassen > Freigabe** auswählen.

   o Entfernen Sie **Alle**

- Fügen Sie ein **Datenproxykonto** mit Vollzugriff hinzu
- Fügen Sie **Lokale Administratoren** mit Vollzugriff hinzu
- Fügen Sie **Domänenadministratoren** mit Vollzugriff hinzu

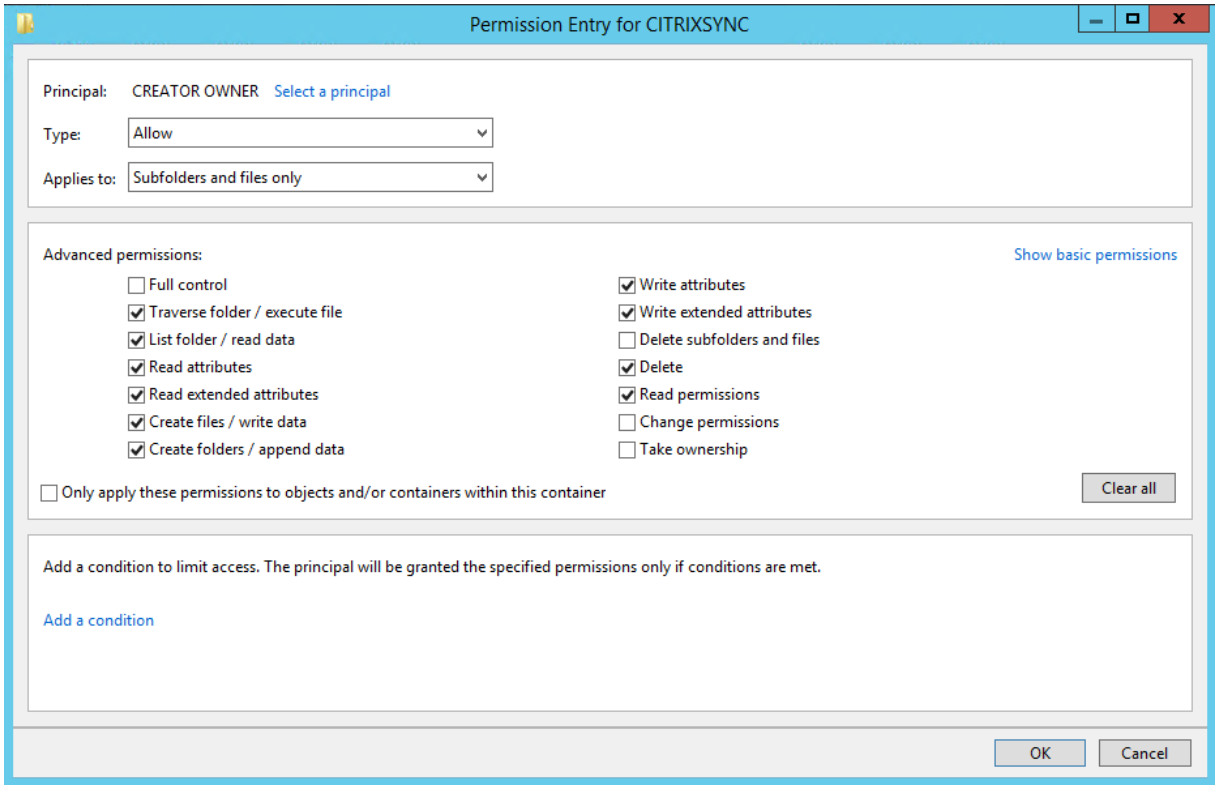
7. Wählen Sie zum Anpassen der NTFS-Berechtigungen im linken Bereich **Berechtigungen**, dann **Berechtigungen anpassen**, klicken Sie auf **Vererbung deaktivieren** und wählen Sie **Vererbte Berechtigungen in explizite Berechtigungen für dieses Objekt konvertieren**.



8. Entfernen Sie alle Benutzer außer **Ersteller-Besitzer/Lokale Administratoren/SYSTEM**, indem Sie unter **Berechtigungen anpassen** > **Berechtigungen** auf **Entfernen** klicken.

9. Sie ändern die Berechtigungen, indem Sie für **Ersteller-Besitzer** > **Erweiterte Berechtigungen** auf **Bearbeiten** klicken und die Auswahl folgender Optionen aufheben:

- Vollzugriff
- Unterordner und Dateien löschen
- Berechtigungen ändern
- Besitz übernehmen



10.Fügen Sie ein **Datenproxykonto** mit Vollzugriff hinzu.

11. Wählen Sie im linken Bereich des Assistenten für neue Freigaben **Bestätigung**, überprüfen Sie die ausgewählten Freigabeeinstellungen und klicken Sie auf **Erstellen**, um mit dem Erstellen des neuen Ordners zu beginnen. Klicken Sie dann auf **Schließen**.

12. Erstellen Sie im Freigabeordner **CITRIXSYNC$** zwei Unterordner: **CentralStoreRoot** und **People**.

Wichtig: Stellen Sie sicher, dass das Datenproxykonto **Vollzugriff** für die beiden Unterordner hat.

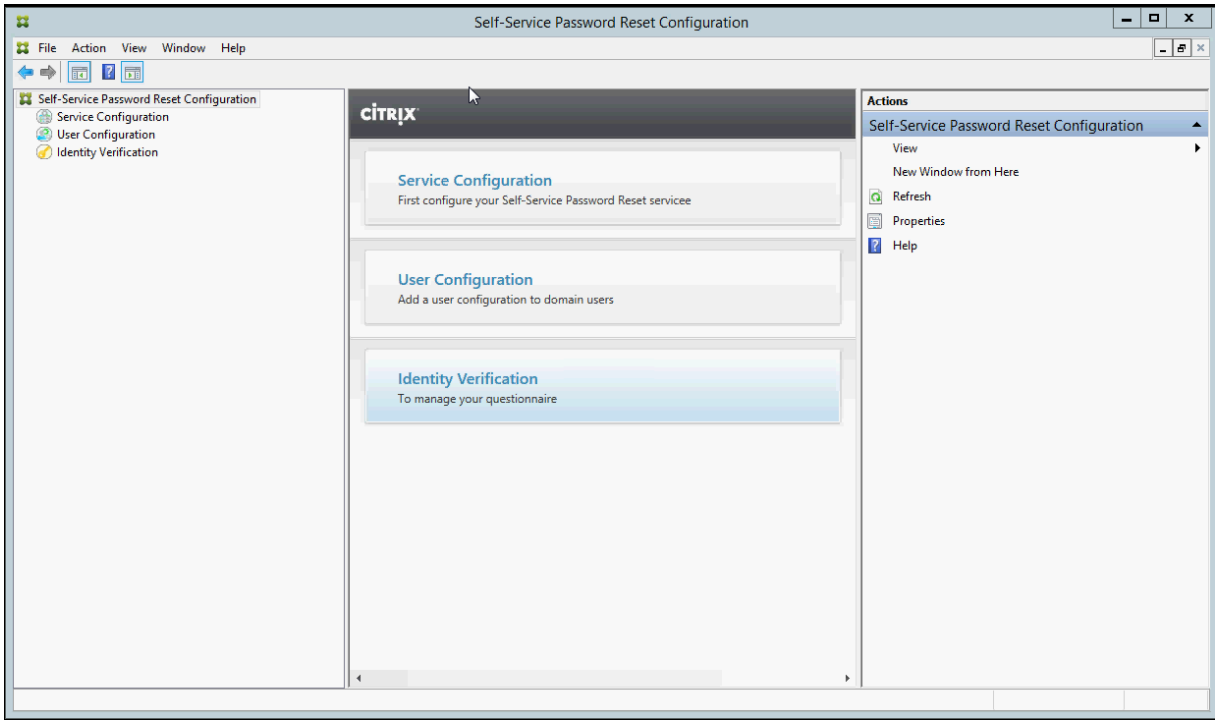
Sie müssen EncryptData, RejectUnencryptedAccess und RequireSecuritySignature für den zentralen Speicher der Self-Service-Kennwortzurücksetzung konfigurieren. Weitere Informationen zur Konfiguration finden Sie in den folgenden Microsoft-Artikeln:
https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbserverconfiguration
https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbshare

Installation und Konfiguration von Self-Service-Kennwortzurücksetzung

Das Installationspaket ist auf den Installationsmedien von Citrix Virtual Apps und Citrix Virtual Desktops.

1. Starten Sie den Installationsassistenten für Self-Service-Kennwortzurücksetzung und folgen Sie den Anweisungen.

2. Klicken Sie auf **Start > Alle Programme > Citrix > Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**, um den Citrix Self-Service-Kennwortzurücksetzungsdienst zu konfigurieren.
3. Wenn die Konsole geöffnet wird, führen Sie die folgenden drei grundlegenden Vorgänge aus, um den Dienst zu konfigurieren.



Dienstkonfiguration

Stellen Sie vor dem Konfigurieren des Diensts sicher, dass Sie den zentralen Speicher, das Datenproxykonto und Self-Service-Konto erstellt haben.

1. Wählen Sie im mittleren Bereich **Dienstkonfiguration** und klicken Sie dann im rechten Bereich auf **Neue Dienstkonfiguration**.
2. Geben Sie im Bildschirm **Seitenspeicherort des zentralen Speichers** den Speicherort des zentralen Speichers an und klicken Sie auf **Weiter**.
3. Wählen Sie im Bildschirm **Domänenkonfiguration** eine Domäne aus und klicken Sie auf **Eigenschaften**.
4. Geben Sie den Benutzernamen und das Kennwort für das **Datenproxykonto** und das **Self-Service-Konto** an und klicken Sie auf **OK**.
5. Geben Sie auf dem Bildschirm **Positivliste für IP-Adressen** die IP-Adressen ein, die Sie mit dem Self-Service-Kennwortzurücksetzungsdienst verbinden möchten. Wenn Sie keine IP-Adresse eingeben, werden alle IP-Adressen auf die Positivliste gesetzt. Klicken Sie auf **Weiter** und auf **Fertig stellen**.

Benutzerkonfiguration

1. Wählen Sie im linken Bereich **Benutzerkonfiguration** und klicken Sie dann im rechten Bereich auf **Neue Benutzerkonfiguration**.
2. Definieren Sie im Bildschirm **Benutzerkonfiguration benennen** die Zielbenutzergruppen für Self-Service-Kennwortzurücksetzung, fügen Sie Benutzer/Gruppen/Organisationseinheiten aus Active Directory hinzu und klicken Sie auf **Weiter**.
3. Geben Sie im Bildschirm **Lizenzierung konfigurieren** den Lizenzserver an und klicken Sie auf **Weiter**.
4. Legen Sie im Bildschirm zum **Konfigurieren der Kennwortzurücksetzung** mit den Kontrollkästchen fest, ob Benutzer Windows-Kennwörter zurücksetzen und die Sperrung ihrer Domänenkonten ohne Intervention des Administrators aufheben können. Geben Sie den Dienstport und die Adresse an und klicken Sie auf **Erstellen**.

Weitere Informationen zum Verwalten von Benutzerkonfigurationen finden Sie unter Verwalten von Benutzerkonfigurationen.

Identitätsprüfung

1. Wählen Sie im linken Bereich **Identitätsprüfung** und klicken Sie dann im rechten Bereich auf **Fragen verwalten**.
2. Wählen Sie im Bildschirm **Fragenbasierte Authentifizierung** die Standardsprache aus, aktivieren oder deaktivieren Sie das Kontrollkästchen “Antworten auf Sicherheitsfragen maskieren” und klicken Sie auf **Weiter**.
3. Klicken Sie im Bildschirm **Sicherheitsfragen** auf **Frage hinzufügen**, geben Sie eine Frage in das Textfeld ein, klicken Sie auf **OK** und dann auf **Weiter**.
4. Klicken Sie im Bildschirm **Fragenkatalog** auf **Hinzufügen** und wählen Sie eine Frage aus. Sie können die Reihenfolge der Fragen und Gruppen mit den Schaltflächen **Nach oben** und **Nach unten** ändern. Wenn Sie fertig sind, klicken Sie auf **Erstellen** und **OK**.

Weitere Informationen zum Verwalten der Fragen zur Identitätsprüfung finden Sie unter Verwalten von Fragen zur Identitätsprüfung.

Verwalten von Benutzerkonfigurationen

Mit Benutzerkonfigurationen können Sie das Verhalten und die Darstellung der Benutzeroberfläche von StoreFront steuern. Das Erstellen einer neuen Benutzerkonfiguration ist der letzte Schritt, den Sie ausführen müssen, bevor Sie Citrix Self-Service-Kennwortzurücksetzung Benutzern in der Umgebung zur Verfügung stellen. Vorhandene Benutzerkonfigurationen können jederzeit bearbeitet werden.

Eine Benutzerkonfiguration ist eine eindeutige Zusammenstellung von Einstellungen, die Sie auf Benutzer anwenden, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind.

Eine Benutzerkonfiguration beinhaltet Folgendes:

- Benutzer, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind.

Wichtig: Verteilergruppen und lokale Gruppen der Domänen im gemischten Modus von Active Directory werden nicht unterstützt.

- Lizenzserver
- Self-Service-Features (Konto entsperren und Kennwort zurücksetzen)

Vor dem Erstellen von Benutzerkonfigurationen müssen Sie Folgendes erstellt bzw. definiert haben:

- Zentraler Speicher
- Dienstkonfiguration

Erstellen einer Benutzerkonfiguration

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**.
2. Wählen Sie im linken Bereich den Knoten **Benutzerkonfigurationen**.
3. Klicken Sie im Menü **Aktionen** auf **Neue Benutzerkonfiguration hinzufügen**.

Hinzufügen von Benutzern, Organisationseinheiten oder Gruppen

Auf der Seite **Benutzerkonfiguration benennen** des **Benutzerkonfigurationsassistenten** können Sie die Benutzerkonfiguration Benutzern zuordnen.

Benutzerkonfigurationszuordnung:

Sie haben zwei Optionen: Benutzer können entsprechend einer Active Directory-Hierarchie (Organisationseinheit oder Einzelbenutzer) oder einer Active Directory-Gruppe zugeordnet werden. Bei Bedarf können Sie die Benutzerkonfiguration später einer anderen Hierarchie oder Gruppe zuordnen, indem Sie im Menü **Aktionen** auf **Benutzerkonfiguration bearbeiten** klicken.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

Wählen Sie die Organisationseinheit, die Benutzer oder Gruppe auf der Seite **Benutzerkonfiguration benennen** (unter “Neue Benutzerkonfiguration hinzufügen” oder “Benutzerkonfiguration bearbeiten”).

Hinweis: Es sollten keine privilegierten Konten (z. B. Lokale Administratoren oder Domänenadministratoren) in die Benutzergruppe aufgenommen werden, für die Self-Service-Kennwortzurücksetzung Kennwörter zurücksetzen kann. Verwenden Sie eine neue, dedizierte Gruppe.

Konfigurieren der Lizenzierung

Auf der Seite **Lizenzierung konfigurieren** im **Benutzerkonfigurationsassistenten** können Sie den Lizenzserver konfigurieren, den Self-Service-Kennwortzurücksetzung verwendet.

Hinweis: Sie können die Features zu Entsperren und Zurücksetzen nur verwenden, wenn Sie die Citrix Virtual Apps oder Citrix Virtual Desktops Platinum Edition haben.

Geben Sie auf der Seite **Lizenzierung konfigurieren** (unter "Neue Benutzerkonfiguration hinzufügen" oder "Benutzerkonfiguration bearbeiten") den Namen des Lizenzservers und die Portnummer ein.

Aktivieren der Features zum Entsperren und Zurücksetzen

Mit Self-Service-Kennwortzurücksetzung können Benutzer Windows-Kennwörter zurücksetzen und die Sperrung ihrer Domänenkonten ohne Eingriff des Administrators aufheben. Auf der Seite **Self-Service-Kennwortzurücksetzung aktivieren** können Sie das gewünschte Feature aktivieren.

Wählen Sie das gewünschte Feature für die Benutzer aus: **Entsperren** oder **Zurücksetzen** auf der Seite **Self-Service-Kennwortzurücksetzung aktivieren** (unter "Neue Benutzerkonfiguration hinzufügen" oder "Benutzerkonfiguration bearbeiten").

Konfigurieren einer Sperrliste

IT-Administratoren können Benutzer und Gruppen einer Sperrliste hinzufügen. Die der Sperrliste hinzugefügten Benutzer und Gruppen können keine Features von Self-Service-Kennwortzurücksetzung verwenden, auch nicht die Features zum Registrieren, Entsperren des Kontos und Zurücksetzen des Kennworts. Benutzer auf der Sperrliste können zudem nach der Anmeldung nicht die Schaltfläche **TASK** in der Citrix Workspace-App sehen.

Konfigurieren der Sperrliste

1. Klicken Sie auf **Start > Alle Programme > Citrix > Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**.
2. Wählen Sie im linken Bereich **Benutzerkonfiguration** und klicken Sie dann im rechten Bereich auf **Konfiguration der Sperrliste**.
3. Mit den Schaltflächen **Hinzufügen** und **Entfernen** können Sie Benutzer oder Gruppen der Sperrliste hinzufügen oder daraus entfernen.

Verwalten von Fragen zur Identitätsprüfung

Die Identitätsprüfung in der Konsole für die Citrix Self-Service-Kennwortzurücksetzung bietet einen zentralen Speicherort für die Verwaltung aller Sicherheitsfragen, die mit der Identitätsprüfung, der Self-Service-Kennwortzurücksetzung und dem Entsperren von Konten verbunden sind. Sie können der Liste der Standardfragen eigene Sicherheitsfragen hinzufügen sowie Fragengruppen erstellen.

- Wenn Sie die bestehenden Standardfragen ändern, nachdem Benutzer die Antworten gespeichert haben, sollten Sie die Bedeutung der bearbeiteten Fragen berücksichtigen. Durch das Bearbeiten einer Frage wird keine Neuregistrierung der Benutzer erzwungen. Wenn Sie jedoch die Bedeutung einer Frage ändern, geben Benutzer aber möglicherweise nicht die richtige Antwort ein.
- Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Aufgaben in der Citrix Workspace-App öffnen.
- Einzelne Sicherheitsfragen können zu mehreren Sicherheitsfragengruppen gehören. Wenn Sie Sicherheitsfragengruppen erstellen, können alle erstellten Fragen in jeder Sicherheitsfragengruppe verwendet werden.

Mit diesen Schritten greifen Sie auf die Einstellungen zu, die nachfolgend beschrieben werden:

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**.
2. Wählen Sie im linken Bereich den Knoten **Identitätsprüfung**.
3. Klicken Sie im Menü **Aktionen** auf **Fragen verwalten**.

Einstellen der Standardsprache

Den Benutzern werden die Sicherheitsfragen meistens in der Sprache angezeigt, die dem aktuellen Benutzerprofil zugeordnet ist. Wenn die Sprache nicht verfügbar ist, zeigt Self-Service-Kennwortzurücksetzung die Fragen in der von Ihnen gewählten Standardsprache an.

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**.
2. Wählen Sie im linken Bereich den Knoten **Identitätsprüfung**.
3. Klicken Sie im Menü **Aktionen** auf **Fragen verwalten**.
4. Wählen Sie auf der Seite **Fragenbasierte Authentifizierung** in der Dropdownliste **Standardsprache** die Standardsprache aus.

Aktivieren des Maskierens der Antworten auf Sicherheitsfragen

Das Maskieren der Antworten auf die Sicherheitsfragen bietet Benutzern zusätzliche Sicherheit, wenn sie die Antworten auf die Sicherheitsfragen registrieren oder die Antworten bei der Identitätsprüfung eingeben. Wenn dieses Feature aktiviert ist, werden die Antworten der Benutzer ausgeblendet. Bei der Registrierung der Antworten werden die Benutzer aufgefordert, die Antworten zweimal einzugeben, um Schreib- oder Rechtschreibfehler zu vermeiden. Bei der Identitätsprüfung müssen Benutzer die Antworten nur einmal eingeben, da sie bei einem Fehler zur erneuten Eingabe aufgefordert werden.

Wählen Sie **Antworten auf Sicherheitsfragen maskieren** auf der Seite **Fragenbasierte Authentifizierung**.

Erstellen neuer Sicherheitsfragen

Sie können beliebig viele Fragen erstellen und jeder Frage eine Sprache zuweisen. Sie können auch mehrere Übersetzungen einer Frage bereitstellen. Bei der Registrierung in der Citrix Workspace-App wird dem Benutzer der Fragenkatalog in der Sprache angezeigt, die den Spracheinstellungen des Benutzerprofils entspricht. Wenn die Sprache nicht verfügbar ist, zeigt Self-Service-Kennwortzurücksetzung die Fragen in der Standardsprache an.

Hinweis: Wenn Sie die Sprache für eine Sicherheitsfrage angeben, wird die Frage den Benutzern angezeigt, deren Betriebssystemeinstellungen für diese Sprache konfiguriert sind. Wenn die ausgewählten Einstellungen des Betriebssystems nicht mit den verfügbaren Fragen übereinstimmt, wird den Benutzern die ausgewählte Standardsprache angezeigt.

1. Wählen Sie auf der Seite **Sicherheitsfragen** in der der Dropdownliste **Sprache** eine Sprache aus und klicken Sie auf **Frage hinzufügen**.Das Dialogfeld “Sicherheitsfrage” wird angezeigt.
2. Erstellen Sie im Dialogfeld **Sicherheitsfragen** die neue Frage.

Wichtig: Fügen Sie den übersetzten Text bestehender Fragen mit der Schaltfläche **Bearbeiten** hinzu. Wenn Sie **Frage hinzufügen** auswählen, erstellen Sie eine neue Frage, die nicht mit der Originalfrage verknüpft ist.

Hinzufügen von Text für bestehende Fragen oder Bearbeiten von Text

Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Aufgaben in der Citrix Workspace-App öffnen. Durch das Bearbeiten einer Frage wird keine Neuregistrierung der Benutzer erzwungen.

Wichtig: Passen Sie beim Bearbeiten einer vorhandenen Frage auf, dass Sie nicht die Bedeutung einer Frage ändern. Sonst können die Antworten der Benutzer bei der erneuten Authentifizierung nicht stimmen. Ein Benutzer könnte also eine andere Antwort eingeben, die nicht mit der gespeicherten Antwort übereinstimmt.

1. Wählen Sie auf der Seite **Sicherheitsfragen** eine Sprache in der Dropdownliste **Sprache** aus.
2. Wählen Sie die Frage aus und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie die Frage im Dialogfeld **Sicherheitsfrage**.

Erstellen einer Sicherheitsfragengruppe

Sie können mehrere Sicherheitsfragen erstellen, die Benutzer beantworten, um die Identität zu bestätigen. Jede Frage, die Sie dem Fragenkatalog hinzufügen, muss von den Benutzern beantwortet werden. Sie können diese Fragen auch in einer Sicherheitsfragengruppe zusammenfassen.

Wenn Sie beispielsweise die Fragen in einer Gruppe zusammenfassen, können Sie dem Fragenkatalog sechs Fragen hinzufügen und Benutzer können z. B. drei der sechs Fragen im Fragenkatalog beantworten. Benutzer haben dann die Flexibilität, Fragen auszuwählen und die Antworten einzugeben, die für die Prüfung der Identität verwendet werden.

1. Klicken Sie auf der Seite **Sicherheitsfragen** auf **Gruppe hinzufügen**.
2. Geben Sie im Dialogfeld **Sicherheitsfragengruppe** den Namen der Gruppe ein, wählen Sie die Fragen und legen Sie die Zahl der Antworten fest, die der Benutzer beantworten muss.

Bearbeiten einer Sicherheitsfragengruppe

Wählen Sie die Sicherheitsgruppe, die Sie bearbeiten möchten, und klicken Sie auf der Seite **Sicherheitsfragen** auf **Bearbeiten**.Das Dialogfeld “Sicherheitsfragengruppe” wird mit einer Liste von verfügbaren Sicherheitsfragen für die Gruppe angezeigt. Die Fragen, die bereits in der Gruppe eingeschlossen sind, haben ein Häkchen. In diesem Dialogfeld können Sie den Namen der Gruppe bearbeiten, der Gruppe Fragen hinzufügen und die Fragen auswählen, die Benutzer beantworten müssen.

Hinzufügen oder Entfernen im vorhandenen Fragenkatalog

Sie können Sicherheitsfragen und Fragengruppen zum Fragenkatalog hinzufügen und daraus entfernen. Sie können die Fragen nach oben und unten verschieben und so die Reihenfolge ändern, in der die Fragen Benutzern angezeigt werden. Wenn sich der Fragenkatalog geändert hat, benachrichtigen Sie die Benutzer, damit sie sich nach der Anmeldung an StoreFront neu registrieren.

1. Klicken Sie auf der Seite **Fragenkatalog** auf **Hinzufügen**, um eine Frage oder Gruppe hinzuzufügen.

2. Klicken Sie auf **Entfernen**, um eine Frage aus dem Fragenkatalog zu entfernen.
3. Klicken Sie auf **Nach oben** oder **Nach unten**, um die Anzeigereihenfolge der Fragen für Benutzer zu verwalten.

Verwalten der Identitätsprüfung

Mit Self-Service-Kennwortzurücksetzung können Sie folgende Aktionen ausführen:

- Sicherheitsfragen importieren und exportieren
- Sicherheitsfragenregistrierung für Benutzer aufheben

Importieren und Exportieren von Sicherheitsfragen

Sie können die Daten der Sicherheitsfragen und -gruppen importieren und exportieren.

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Citrix Self-Service-Kennwortzurücksetzung - Konfiguration**.
2. Wählen Sie im linken Bereich den Knoten **Identitätsprüfung**.
3. Wählen Sie im Menü **Aktion** eine der folgenden Optionen:

   Sicherheitsfragen importieren
   Geben Sie den Speicherort der Datei an, in die die Daten der Sicherheitsfragen und -gruppen exportiert werden.

   Sicherheitsfragen exportieren
   Geben Sie den Speicherort der Datei an, in die die Daten der Sicherheitsfragen und -gruppen exportiert werden.

Sichere Konfiguration

October 29, 2018

Dieser Abschnitt enthält Anleitungen um zu gewährleisten, dass die Komponenten von Self-Service-Kennwortzurücksetzung sicher bereitgestellt und konfiguriert werden.

- Erstellen eines Domänenbenutzerkontos mit Berechtigungen zum Zurücksetzen des Benutzerkennworts und Entsperren des Benutzerkontos
- Konfigurieren der Firewalleinstellungen

Erstellen eines Self-Service-Kontos

Wenn Sie die Features zum Zurücksetzen des Kennworts oder Entsperren des Kontos von Self-Service-Kennwortzurücksetzung verwenden, geben Sie bei der Dienstkonfiguration ein Self-Service-Konto an, das vom Self-Service-Modul zum Zurücksetzen und Entsperren verwendet wird. Dieses Konto muss ausreichende Privilegien haben, aber es sollte kein Konto der Domänenadministratorgruppe für Produktionsbereitstellungen sein. Empfohlene Kontoberechtigungen:

- Domänenmitglied
- Berechtigung zum Zurücksetzen des Kennworts und Entsperren des Kontos für die relevanten Domänenbenutzer

Erstellen Sie in **Active Directory-Benutzer und -Computer** eine Gruppe oder ein Benutzerkonto mit den Rechten zum Zurücksetzen des Benutzerkennworts und Entsperren von Benutzerkonten.

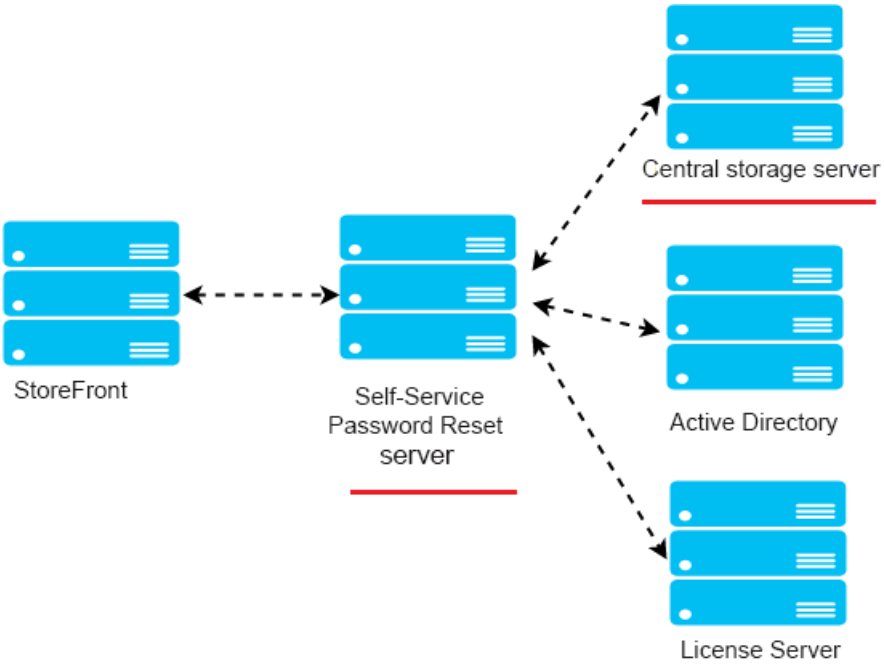
1. Klicken Sie unter **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf die Domäne und dann im Menü auf **Objektverwaltung zuweisen**.
2. Der **Assistent zum Zuweisen der Objektverwaltung** wird angezeigt. Klicken Sie im **Willkommensdialogfeld** auf **Weiter**.
3. Klicken Sie im Dialogfeld **Benutzer und Gruppen** auf **Hinzufügen**. Wählen Sie in der Liste die Gruppe aus, der Sie das Recht zum Entsperren von Konten geben möchten, und klicken Sie dann auf **OK**. Klicken Sie im Dialogfeld **Benutzer und Gruppen** auf **Weiter**.
4. Klicken Sie im Dialogfeld **Zuzuweisende Aufgaben** auf **Benutzerdefinierte Aufgaben zum Zuweisen erstellen** und klicken Sie dann auf **Weiter**.
5. Klicken Sie im Dialogfeld **Active Directory-Objekttyp** auf “Folgenden Objekten im Ordner:” > “Benutzerobjekte” und klicken Sie dann auf **Weiter**.
6. Aktivieren Sie im Dialogfeld **Berechtigungen** die Kontrollkästchen **Allgemein** und **Eigenschaftenspezifisch**. Wählen Sie in der Liste **Berechtigungen** folgende Kontrollkästchen aus: **lockoutTime lesen**, **lockoutTime schreiben**, **Kennwort zurücksetzen, Kennwort ändern, userAccountControl lesen, userAccountControl schreiben, pwdLastSet lesen sowie pwdLastSet schreiben**. Klicken Sie dann auf **Weiter**.
7. Klicken Sie im Dialogfeld **Fertigstellen des Assistenten** auf **Fertig stellen**.

Konfigurieren der Firewalleinstellungen

Da die Serverkomponenten Self-Service-Kennwortzurücksetzungsserver und zentraler Speicher Benutzerkennwörter verwalten, empfiehlt es sich, diese Komponenten auf einem vertrauenswürdigen Netzwerk bereitzustellen und den Zugriff auf bestimmte vertrauenswürdige Komponenten zu beschränken. In diesem Abschnitt werden die Schritte beschrieben, die zur richtigen Konfiguration der Windows-Firewall für diese Server erforderlich sind. Darüber hinaus sollten Sie die vorhandene Netzwerkinfrastruktur so konfigurieren, dass diese Server von nicht vertrauenswürdigem Netzwerkdatenverkehr isoliert sind.

Wenn Sie diese Konfigurationen in der Bereitstellung abgeschlossen haben, kann auf die Server des zentralen Speichers von Self-Service-Kennwortzurücksetzung nur von Servern aus zugegriffen werden, die Server Message Block (SMB) verwenden. Auf die Self-Service-Kennwortzurücksetzungsserver kann nur von StoreFront-Servern aus über HTTPS-Verbindungen zugegriffen werden.

Bereitstellung einer Remotedateifreigabe für Windows 2012 R2



Umgebung

- Stellen Sie die Komponenten für Self-Service-Kennwortzurücksetzung auf dedizierten Servern bereit. Stellen Sie sie nicht auf denselben Servern wie die vorhandenen StoreFront- oder Delivery Controller-Komponenten bereit. Ansonsten blockiert möglicherweise die unten dargestellte Firewallkonfiguration den Datenverkehr von StoreFront oder vom Delivery Controller.
- Zwischen StoreFront und dem Self-Service-Kennwortzurücksetzungsserver ist kein nicht transparenter HTTP/HTTPS-Proxy.

Wenn zwischen StoreFront und dem Self-Service-Kennwortzurücksetzungsserver ein nicht transparenter Proxy ist, konfigurieren Sie die Firewallregeln so, dass auf den Self-Service-Kennwortzurücksetzungsserver nur über den Proxyserver zugegriffen wird.

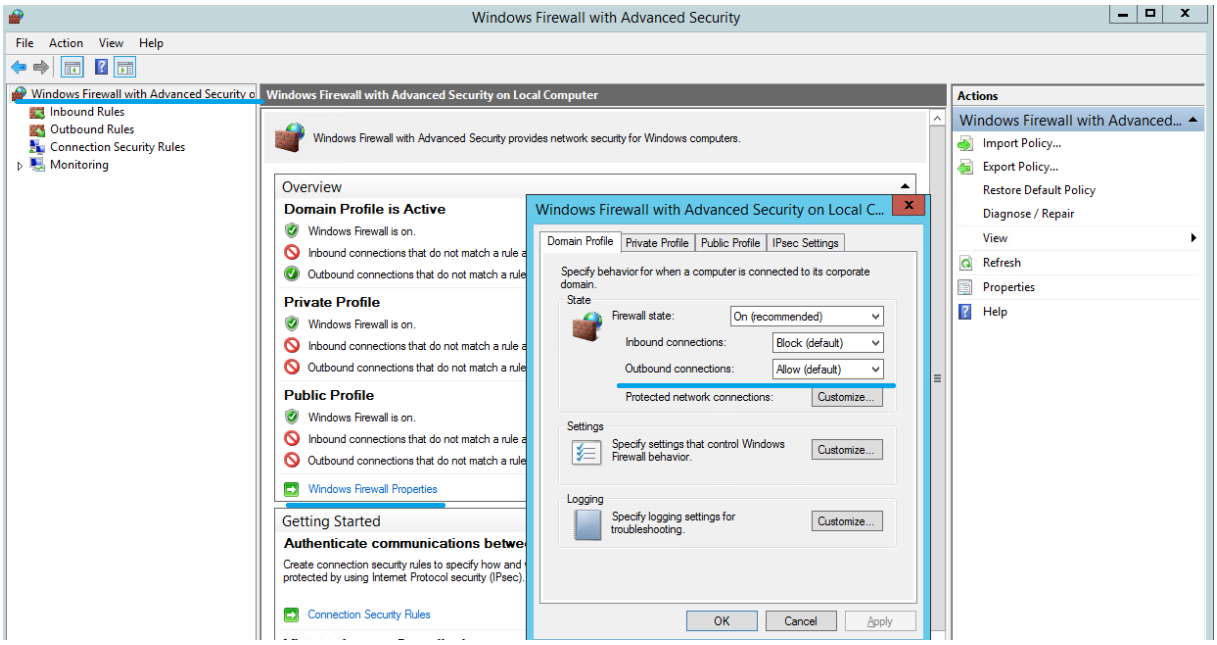
- Die Konfigurationen in diesen Schritten basieren auf den Windows-Standardfirewallregeln.

Konfigurieren der Firewall für den zentralen Speicher von Self-Service-Kennwortzurücksetzung

Nach Abschluss der Konfiguration ermöglicht der SMB-Service, der vom zentralen Speicher der Self-Service-Kennwortzurücksetzung bereitgestellt wird, nur den eingehenden Zugriff von den Self-Service-Kennwortzurücksetzungsservern. Außerdem kann der Self-Service-Kennwortzurücksetzungsserver mit dem zentralen Speicher auf den Dienst im Unternehmensnetzwerk nur ausgehend zugreifen.

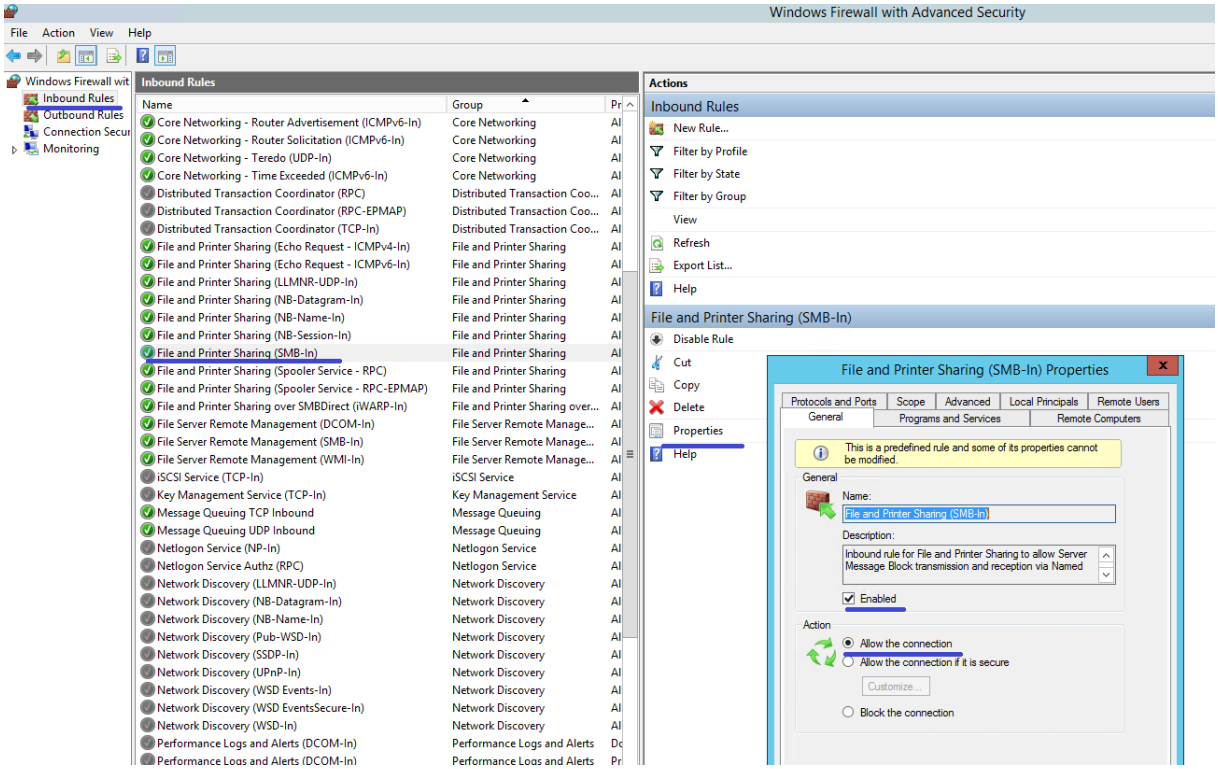
1. Öffnen Sie den Server-Manager und wählen Sie im Menü **Extras** auf der oberen Navigationsleiste die Option **Windows-Firewall mit erweiterter Sicherheit**.

2. Wählen Sie im mittleren Bereich von **Windows-Firewall mit erweiterter Sicherheit** die Option **Windows-Firewalleigenschaften**. Es gibt drei Firewallprofile: Domänenprofil, Privates Profil und Öffentliches Profil. Wählen Sie die Registerkarte **Domänenprofil**. Stellen Sie sicher, dass folgende Einstellungen festgelegt sind: **Firewallstatus** auf **Ein**, **Eingehende Verbindungen** auf **Blocken** und **Ausgehende Verbindungen** auf **Zulassen**.



3. Wählen Sie die Registerkarten **Privates Profil** und **Öffentliches Profil** aus. Stellen Sie sicher, dass der **Firewallstatus** auf **Ein** gesetzt ist, und dass für **Eingehende Verbindungen** sowie **Ausgehende Verbindungen** die Option **Blockieren** eingestellt ist. Übernehmen Sie die Änderungen und speichern Sie sie.

4. Klicken Sie auf **Eingehende Regeln**, wählen Sie **Datei- und Druckerfreigabe (SMB eingehend)** und stellen Sie sicher, dass diese Regel **aktiviert** ist und **Verbindung zulassen** für **Aktion** festgelegt ist.



5. Wechseln Sie in den Eigenschaften für die **Datei- und Druckerfreigabe (SMB eingehend)** zur Registerkarte **Bereich**. Wählen Sie **Diese IP-Adressen** und fügen Sie alle IP-Adressen von Self-Service-Kennwortzurücksetzungsservern der Liste hinzu. Beispiel: Self-Service-Kennwortzurücksetzungsserver A (192.168.1.10) und Self-Service-Kennwortzurücksetzungsserver B (192.168.1.11).

6. Klicken Sie in **Eigenschaften von Datei- und Druckerfreigabe (SMB eingehend)** auf die Registerkarte **Erweitert**, aktivieren Sie **Domänenprofil**, **Privates Profil** und **Öffentliches Profil** und speichern Sie die Änderungen dieser Regel.

7. Wiederholen Sie diese Schritte unter **Eingehende Regeln** für **Dateiserver-Remoteverwaltung (SMB eingehend)** und **Datei- und Druckerfreigabe (NB-Sitzung eingehend)**.

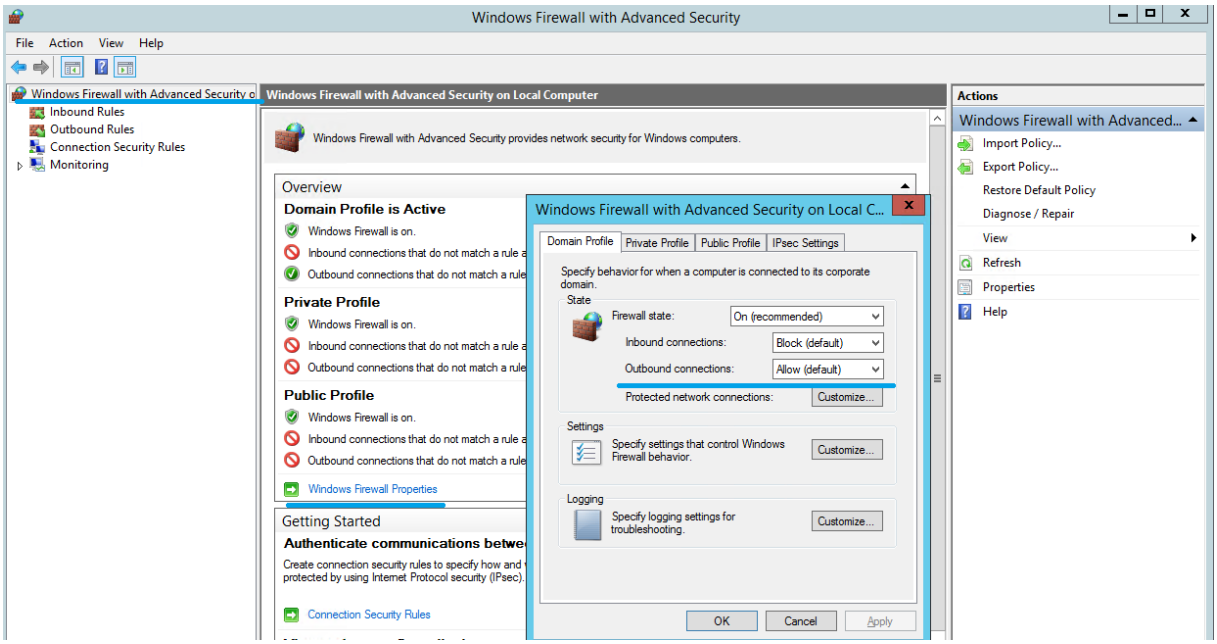
Konfigurieren der Firewall für den Self-Service-Kennwortzurücksetzungsserver

Nach dem Abschluss der Konfiguration können auf den Webdienst, der von den Self-Service-Kennwortzurücksetzungsservern bereitgestellt wird, nur die StoreFront-Server über HTTPS zugreifen. Außerdem könnrn die Self-Service-Kennwortzurücksetzungsserver auf den Dienst im Unternehmensnetzwerk zugreifen.

1. Öffnen Sie den Server-Manager und wählen Sie im Menü **Extras** auf der oberen Navigationsleiste die Option **Windows-Firewall mit erweiterter Sicherheit**.

2. Wählen Sie im mittleren Bereich von **Windows-Firewall mit erweiterter Sicherheit** die Option **Windows-Firewalleigenschaften**. Es gibt drei Firewallprofile: Domänenprofil, Privates Profil und

Öffentliches Profil. Wählen Sie die Registerkarte **Domänenprofil**. Stellen Sie sicher, dass folgende Einstellungen festgelegt sind: **Firewallstatus** auf **Ein**, **Eingehende Verbindungen** auf **Blocken** und **Ausgehende Verbindungen** auf **Zulassen**.

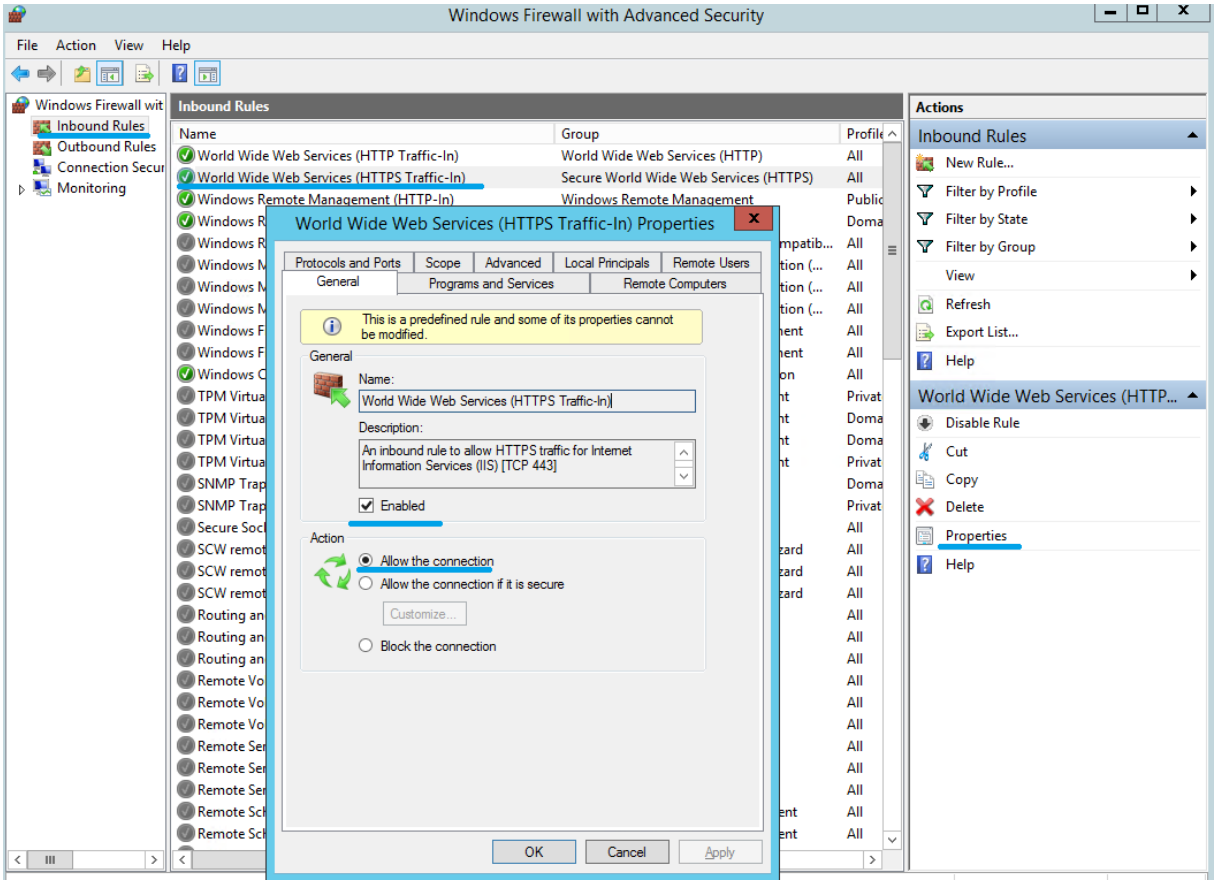


3. Wählen Sie die Registerkarten **Privates Profil** und **Öffentliches Profil**, und stellen Sie sicher, dass der **Firewallstatus** auf **Ein** gesetzt ist. Für **Eingehende Verbindungen** sowie **Ausgehende Verbindungen** muss die Option **Blockieren** eingestellt sein. Übernehmen Sie die Änderungen und speichern Sie sie.

4. Wählen Sie unter **Eingehende Verbindungen** die Option **WWW-Dienste (Eingehender HTTP-Datenverkehr)**. Stellen Sie sicher, dass diese Regel **Aktiviert** und für **Aktion** die Option **Verbindung blockieren** eingestellt ist.

5. Klicken Sie in **Eigenschaften von WWW-Dienste (Eingehender HTTP-Datenverkehr)** auf die Registerkarte **Erweitert**. Wählen Sie die Profile **Domäne**, **Privat** und **Öffentlich** und speichern Sie die Änderungen dieser Regel.

6. Wählen Sie unter **Eingehende Verbindungen** die Option **WWW-Dienste (Eingehender HTTPS-Datenverkehr)**. Stellen Sie sicher, dass diese Regel **Aktiviert** und für **Aktion** die Option **Verbindung zulassen** eingestellt ist.



7. Klicken Sie in **Eigenschaften von WWW-Dienste (Eingehender HTTPS-Datenverkehr)** auf die Registerkarte **Bereich**. Wählen Sie **Diese IP-Adresse** und fügen Sie der Liste alle IP-Adressen für StoreFront-Server hinzu. Beispiel: StoreFront A (192.168.1.50) und StoreFront B (192.158.1.51).

8. Klicken Sie in **Eigenschaften von WWW-Dienste (Eingehender HTTPS-Datenverkehr)** auf die Registerkarte **Erweitert**. Wählen Sie die Profile **Domäne**, "Privat" und **Öffentlich** und speichern Sie die Änderungen dieser Regel.

Migrieren von Daten aus dem zentralen Speicher für Single Sign-On

October 29, 2018

Der zentrale Speicher für Single Sign-On ist ein zentrales Repository, das von Single Sign-On zum Speichern und Verwalten von Benutzerdaten und administrativen Daten verwendet wird. Benutzerdaten sind zum Beispiel die Anmeldeinformationen der Benutzer, Antworten auf Sicherheitsfragen und andere auf Benutzer bezogene Daten. Administrative Daten sind zum Beispiel Kennwortrichtlinien, Anwendungsdefinitionen, Sicherheitsfragen und andere allgemeine Daten.

Sie können nicht alle Daten aus dem zentralen Speicher für Single Sign-On in den zentralen Speicher

von Self-Service-Kennwortzurücksetzung migrieren. Diese Tabelle zeigt, welche Daten migriert werden können und welche nicht.

Migration nicht möglich	Migration möglich
Kennwortrichtlinien - nicht unterstützt	Persönliche Ordner mit Registrierungsdaten
Anwendungsvorlagen - nicht unterstützt	Von Kunden verwendete Fragebögen
Anwendungsdefinitionen - nicht unterstützt	
Benutzerkonfigurationen - erstellt auf der Konsole von Self-Service-Kennwortzurücksetzung	
Anwendungsgruppen - nicht unterstützt	
Single Sign-On-Dienstdaten - erstellt auf der Konsole von Self-Service-Kennwortzurücksetzung	

> **Wichtig**
>
> - Self-Service-Kennwortzurücksetzung unterstützt nur Netzwerkfreigaben als zentralen Speicher und nicht Active Directory.
> - Self-Service-Kennwortzurücksetzung unterstützt nur Daten aus Single Sign-On 4.8 oder 5.0.

Migrieren von Daten aus dem zentralen Speicher für Single Sign-On

Bevor Sie Daten migrieren, machen Sie sich mit der Installation und Konfiguration von Self-Service-Kennwortzurücksetzung vertraut. Weitere Informationen finden Sie unter “Installation und Konfiguration”.

1. Erstellen Sie einen neuen zentralen Speicher.
2. Installieren Sie den Self-Service-Kennwortzurücksetzungsdienst und die Konsole.
3. Geben Sie in der Konsole den neuen Speicherort des zentralen Speichers an.
4. Erstellen Sie eine neue Benutzerkonfiguration und schließen Sie die Benutzer ein, die Self-Service-Kennwortzurücksetzung für Single Sign-On haben.
5. Kopieren Sie die Single Sign-On-Registrierungsdaten und -Sicherheitsfragen in den neuen zentralen Speicher.

Hinweis: Stellen Sie sicher, dass das Datenproxykonto Vollzugriff auf alle kopierten Dateien hat.

Sie benötigen nur zwei Ordner bzw. Dateien.

Beispiele

Kopieren der Registrierungsdaten aller Benutzer:

\\SSO-SERVER\citrixsync$\People

nach

\\SSPR-SVC\citrixsync$\People

Verwenden Sie den folgenden Befehl:
Robocopy \\SSO-SERVER\citrixsync$\People\ \\SSPR-SVC\citrixsync$\People /e /xd QBA /Log+:copylog.txt /tee

Kopieren der von Kunden verwendeten Sicherheitsfragen:

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

nach

\\SSPRSVCcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\

Verwenden Sie den folgenden Befehl:
Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ \\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee

Jetzt können alle Benutzer mit Single Sign-On-Sicherheitsfragen und -Antworten ihre Konten entsperren und Kennwörter zurücksetzen.

Konfigurieren von StoreFront, um Benutzern das Aufzeichnen von Antworten auf Sicherheitsfragen zu ermöglichen

October 29, 2018

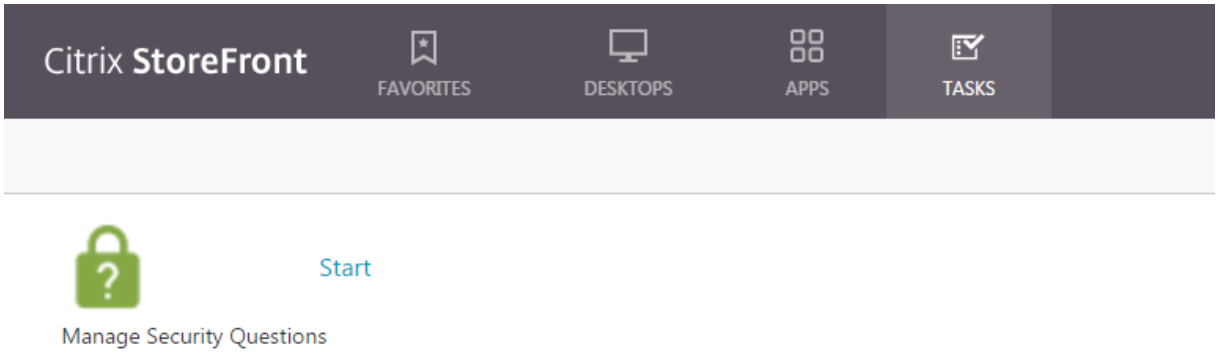
Konfigurieren Sie StoreFront, sodass Benutzer die Antworten auf Sicherheitsfragen registrieren können. Wenn sie sich registriert haben, können sie Domänenkennwörter zurücksetzen und die Sperrung von Domänenkonten aufheben. Weitere Informationen finden Sie in der StoreFront-Dokumentation.

1. Konfigurieren Sie für StoreFront die Internetinformationsdienste (IIS) für HTTPS.
2. Erstellen Sie eine neue Bereitstellung in StoreFront.
3. Klicken Sie im rechten Bereich der StoreFront-Verwaltungskonsole auf **Authentifizierungsmethoden verwalten > Benutzername und Kennwort**. Wählen Sie in der Dropdownliste **Kennwortoptionen verwalten**.
4. Wählen Sie, wann Benutzer ihre Kennwörter ändern können, und klicken Sie auf **OK**.

5. Wählen Sie im Dropdownmenü **Benutzername und Kennwort** die Option **Konto-Self-Service konfigurieren**, wählen Sie dann **Citrix SSPR** und klicken Sie auf **Konfigurieren**.
6. Geben Sie an, ob Benutzer mit Self-Service-Kennwortzurücksetzung ihre Kennwörter zurücksetzen und die Sperrung ihrer Konten aufheben können, fügen Sie die Kontodienst-URL für den Kennwortdienst hinzu und klicken Sie auf **OK**.

Hinweis: Sie müssen die Site so konfigurieren, dass die einheitliche Benutzeroberfläche verwendet wird.

Das nächste Mal, wenn ein Benutzer sich an Citrix Workspace-App oder Citrix Workspace-App für Web anmeldet, ist die Registrierung für Sicherheitszwecke verfügbar. Nachdem der Benutzer auf **Start** geklickt hat, werden Fragen angezeigt, die er beantworten muss.



Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States