Self-Service Password Reset 1.1.x

Contents

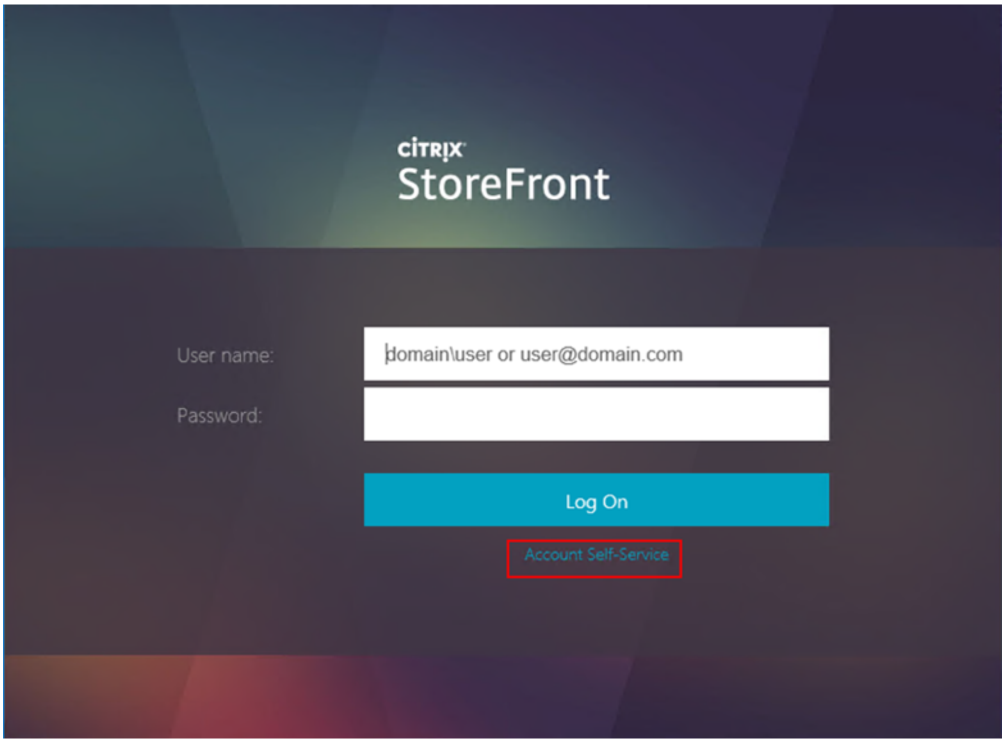
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Self-Service Password Reset 1.1.x

July 12, 2023

Self-Service Password Reset enables end users to have greater control over their user accounts. Once Self-Service Password Reset is configured, if end users have problems logging on to their systems, they can unlock their accounts or reset their passwords to something new by correctly answering several security questions.

> **Tip:**
>
> The **Account Self-Service** link can be seen on the logon page of StoreFront for users to do password unlock and reset.



Resetting user passwords is an inherently security sensitive process. We recommend that you refer to the Secure configuration article to ensure that your deployment is correctly configured.

What's new

August 24, 2018

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

What's new in version 1.1.20

You can configure IP addresses that are allowed to connect to the Self-Service Password Reset service. If you do not enter any IP address, all IP addresses are whitelisted, that is, allowed to connect.

What's new in version 1.1.10

This release addresses some issues that help to improve overall performance and stability.

What's new in version 1.1

This version includes the following key enhancements:

- Support for blacklist configuration - IT administrators can add users and groups to a blacklist. Users and groups in the blacklist cannot use any of the Self-Service Password Reset features.
- Support for simplified Chinese - Besides English, French, Japanese, and Spanish, simplified Chinese is now available for defining security questions.

Self-Service Password Reset contains three components:

- Self-Service Password Reset configuration console
- Self-Service Password Reset Service
- Security question enrollment in StoreFront

Self-Service Password Reset configuration console

- **Service configuration.** Configures the Self-Service Password Reset service, including the central store address, data proxy account, and Self-Service Password Reset account.
  - Central store address: Network share location for storing Self-Service Password Reset data.
  - Data Proxy Account: Communicates with the central store. The account requires read and write access to the central store.
  - Self-Service Password Reset account: Used to unlock the account and reset the password.
- **User configuration.** Configures which user/group/OU can use the Self-Service Password Reset feature, and specifies the license server address and default service address.
  - Name user configuration: Defines the target user groups of the Self-Service Password Service, which can include users/groups/OUs from Active Directory.

  - License server address: You can use Self-Service Password Reset with only Citrix Virtual Apps or Citrix Virtual Desktops Platinum edition. Minimum License Server version must be 11.13.1 or higher.
  - Select or deselect the **Unlock** and **Reset** features.
  - Default service address: Specify the URL of Self-Service Password Reset service.

- **Identity verification.** Configures the questionnaire used for enrollment and to unlock or reset the password.

  - Add a question or group to the question store from which questionnaires are generated.
  - Select a question list from the question store that will be used for enrollment.
  - Export/import security questions or groups.

Self-Service Password Reset Service

The Self-Service Password Reset Service runs on a Web server and allows users to reset their Windows passwords and unlock their Windows accounts. The end users'requests are sent to this service through StoreFront.

Security question enrollment in StoreFront Use StoreFront to allow users to enroll their answers to the security questions. When they are enrolled, they can reset domain passwords and unlock domain accounts. For more information, see the Self-Service Password Reset security questions section in Configure the authentication service.

Fixed issues

July 5, 2018

Version 1.1.20

This release does not have any fixed issues.

Version 1.1.10

The following issues have been resolved in this version.

- After you disable TLS 1.0 on the **Self-Service Password Reset** server, this error message might appear when you add the server URL to the wizard:

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

"Cannot access your server address."[#LC7741]

- When you enable the password reset feature and apply any customized password filters on the domain controller, the password reset feature might not work. This error message appears:

  "The supplied password is invalid."[#LC7570]

Known issues

August 24, 2018

Version 1.1.20

The following known issues exist in this version.

- Attempts to add a user group in the user configuration wizard can fail and a message shows that the user group is in a blacklist. The message is incorrect. The attempt failed because you have already added this group.

[#665520]

- You cannot add users and user groups that you just removed from the configuration wizard until you complete the removal process and close the wizard. Otherwise, an incorrect error message appears, stating that the users or groups are in a blacklist. As a workaround, complete the removal process and close the wizard, then reopen the wizard to add the users or groups back.

[#665352]

- If you upgrade Self-Service Password Reset to Version 1.1 while the Version 1.0 console is open, no corresponding and the Version 1.0 open console cannot be used.

[#664390]

- Attempts to upgrade or uninstall on Windows Server 2012 with only .Net Framework 4.5 installed, and attempts to upgrade or uninstall on Windows Server 2016 with only .Net Framework 4.6 installed can fail. The attempts fail because in-place upgrade or uninstalling on Windows Server 2012 and on Windows Server 2016 has a dependency on .Net Framework 3.5. As a workaround, install .Net Framework 3.5 before the upgrade and before you uninstall.

[DNA-22761]

Version 1.1.10

The following known issues exist in this version.

- Attempts to add a user group in the user configuration wizard can fail and a message shows that the user group is in a blacklist. The message is incorrect. The attempt failed because you have already added this group.

[#665520]

- You cannot add users and user groups that you just removed from the configuration wizard until you complete the removal process and close the wizard. Otherwise, an incorrect error message appears, stating that the users or groups are in a blacklist. As a workaround, complete the removal process and close the wizard, then reopen the wizard to add the users or groups back.

[#665352]

- If you upgrade Self-Service Password Reset to Version 1.1 while the Version 1.0 console is open, no corresponding and the Version 1.0 open console cannot be used.

[#664390]

- Attempts to upgrade or uninstall on Windows Server 2012 with only .Net Framework 4.5 installed, and attempts to upgrade or uninstall on Windows Server 2016 with only .Net Framework 4.6 installed can fail. The attempts fail because in-place upgrade or uninstalling on Windows Server 2012 and on Windows Server 2016 has a dependency on .Net Framework 3.5. As a workaround, install .Net Framework 3.5 before the upgrade and before you uninstall.

[DNA-22761]

Version 1.1

The following known issues exist in this version.

- Attempts to add a user group in the user configuration wizard can fail and a message shows that the user group is in a blacklist. The message is incorrect. The attempt failed because you have already added this group.

[#665520]

- You cannot add users and user groups that you just removed from the configuration wizard until you complete the removal process and close the wizard. Otherwise, an incorrect error message appears, stating that the users or groups are in a blacklist. As a workaround, complete the removal process and close the wizard, then reopen the wizard to add the users or groups back.

[#665352]

- If you upgrade Self-Service Password Reset to Version 1.1 while the Version 1.0 console is open, no corresponding and the Version 1.0 open console cannot be used.

[#664390]

- Attempts to upgrade or uninstall on Windows Server 2012 with only .Net Framework 4.5 installed, and attempts to upgrade or uninstall on Windows Server 2016 with only .Net Framework 4.6 installed can fail. The attempts fail because in-place upgrade or uninstalling on Windows Server 2012 and on Windows Server 2016 has a dependency on .Net Framework 3.5. As a workaround, install .Net Framework 3.5 before the upgrade and before you uninstall.

[DNA-22761]

Version 1.0

The following known issues exist in this version.

- After opening the Self-Service Password Reset console, you might not be able to pin it to the taskbar.

[#646300]

Workaround: Pin the console to the taskbar from the **Start** menu shortcut.

- Because of a known in issue in Windows 2016, you cannot search for the Self-Service Password Reset console in Windows 2016.

[#648939]

Workaround: Use the **Start** menu to locate Self-Service Password Reset.

- If the minimum password age in the password policy in the default domain policy is the default (one day), and your users try to reset their passwords but reset fails (for example, they do not meet the complexity requirement), and they close the Password Reset wizard, they cannot reset the password again for 24 hours.

[#653221]

- When using Citrix Workspace app for Mac, the task button for enrollment appears the first time the user logs on to StoreFront. After logging off StoreFront and then on again, the task button does not appear.

[#657263]

Workaround:
1. Click the User name in the upper-right corner in the StoreFront store.
2. Click the **Refresh Apps** button in the drop-down menu.
3. Close Citrix Workspace app for Mac, reopen it and the task button appears.

- When migrating security questions from Single Sign-on Identity Verification to Self-Service Password Reset, the questions might not display in the Self-Service Password Reset console, even after clicking **Refresh**.

[#657277]

Workaround: Close the console and then reopen it.

- Security questions in the questionnaire that contain the special character **&** do not display during enrollment in StoreFront.

[#654913]

Workaround: Do not include **&** in security questions.

- Attempts to upgrade or uninstall on Windows Server 2012 with only .Net Framework 4.5 installed, and attempts to upgrade or uninstall on Windows Server 2016 with only .Net Framework 4.6 installed can fail. The attempts fail because in-place upgrade or uninstalling on Windows Server 2012 and on Windows Server 2016 has a dependency on .Net Framework 3.5. As a workaround, install .Net Framework 3.5 before the upgrade and before you uninstall.

[DNA-22761]

System requirements

August 24, 2018

> **Important**
>
> Citrix does not support installation of any Self-Service Password Reset component on a domain controller. Deploy the Self-Service Password Reset components on dedicated servers.

This article describes the hardware and software requirements for your Self-Service Password Reset environment. This article assumes that each computer meets the minimum hardware requirements for the installed operating system.

Software

Computers in your Self-Service Password Reset environment might require the following supporting system software.

- **Windows 2016 and Windows 2012 R2** - Required by Self-Service Password Reset Server.
- **Microsoft Windows Installer 2.0 or later** - Required by all.
- **Microsoft .NET Framework** - Required by Self-Service Password Reset Server.
  - 4.6.x (Windows 2016)
  - 4.5.2 (Windows 2012 R2)
- **Internet Information Services (IIS)** - Required by Self-Service Password Reset Server.
  - IIS 10.0 (Windows 2016)
  - IIS 8.5 (Windows 2012 R2)
- **VC++ 2008 SP1 runtime** - Required by the Self-Service Password Reset Server.
  For a first-time installation, you must download vcredist_x86.exe from https://www.microsoft.com/en-us/download/details.aspx?id=26368, and install it on the Self-Service Password Reset Server.

Self-Service Password Reset Server

- Self-Service Password Reset Component - Central store
- Supported Environment - SMB File Share
- Hardware Requirement - 30 KB disk space per user

ASP.NET 3.5/4.X requirements

The ASP.NET component for your version of .NET framework on your Windows Server computer.

Security and account requirements

Before you install the Self-Service Password Reset Service, ensure that the appropriate accounts and components are available to support the service. Also, because the service uses secure HTTP (HTTPS), it requires a server authentication certificate for Transport Layer Security (TLS) communication with StoreFront.

Server Authentication Requirement:

Before you install the service, obtain a server authentication certificate for TLS communication from a Certificate Authority (CA) or your internal Public Key Infrastructure (PKI), if available.

Accounts Required for Service Modules:

Note: Ensure that both accounts will not expire.

The Self-Service Password Reset Service requires these account types to read and write data as it operates in your environment:

- Data proxy account
- Self-service account

When different modules require the same type of account, you can use the same account for multiple modules. Or you can specify different customized accounts for each module.

- **Data proxy account**

Requires read and write access to the central store. For more information, see the **Create a central store** section in Install and configure.

- **Self-service account**

Requires sufficient privileges to unlock and reset the password of the relevant users in User Configuration. For more information, Secure configuration.

StoreFront

- StoreFront 3.7
- StoreFront 3.8 or later

Citrix Workspace app

Supported:

- Citrix Workspace app for Web
- Citrix Workspace app for Windows
- Citrix Workspace app for Linux
- Citrix Workspace app for Mac (Requires StoreFront 3.8)

Not supported:

- Citrix Workspace app for Chrome
- Mobile devices (not even with Citrix Workspace app for Web)

External use with Citrix Gateway

Unsupported

Install and configure

June 15, 2020

Installation checklist

Before you start the installation, complete this list:

☒	Step
	Choose the computers in your environment where you will install the software and prepare them for installation. See System requirements. Install the TLS certificate and the accounts required for the service. See **Security and account requirements** in System requirements. Install or upgrade the License Server to a minimum of version 11.13.1.2. Download the License Server from https://www.citrix.com/downloads/licensing.html. For more information, see License server documentation.

Installation and configuration order

Citrix recommends that you install Self-Service Password Reset in this order:

1. Create a central store. See Create a central store.
2. Install Self-Service Password Reset. To install the service and run the Service Configuration wizard, your logon account must be a domain user and belong to the local administrator group on the server. For more information, see Install and configure Self-Service Password Reset.
3. Configure Self-Service Password Reset using the console. See Install and configure Self-Service Password Reset.
4. Configure Self-Service Password Reset on StoreFront. See Configure StoreFront.
5. Ensure that your Self-Service Password Reset configuration is securely configured. See Secure configuration.

Create a central store

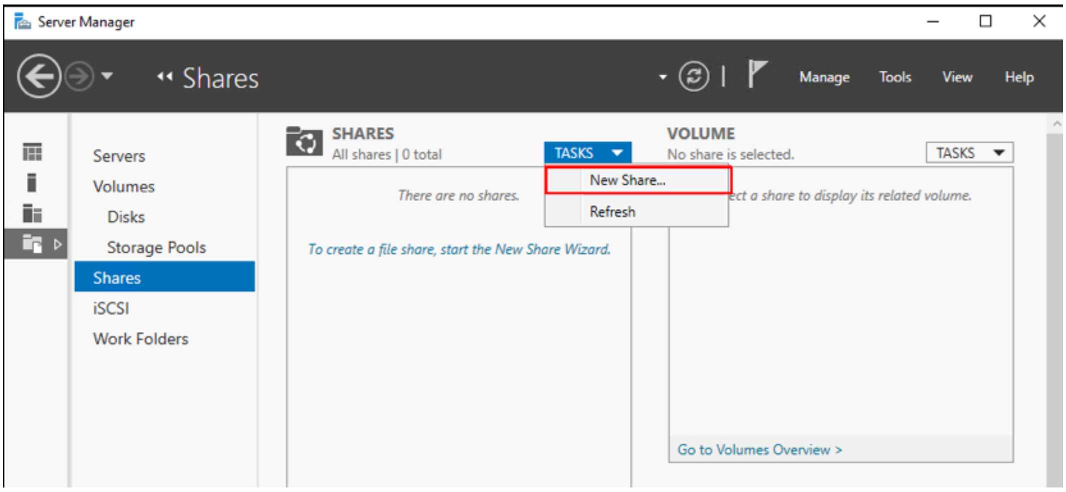
For security reasons, we recommend that you create the central store directly on the machine running the Self-Password Reset service. For deployments where more than one Self-Password Reset server is required, you can host the central store on a remote network share if the Self-Service Password Reset server and the server hosting the share both support SMB encryption.

This feature is available only on Windows Server 2012 R2 or Windows Server 2016.

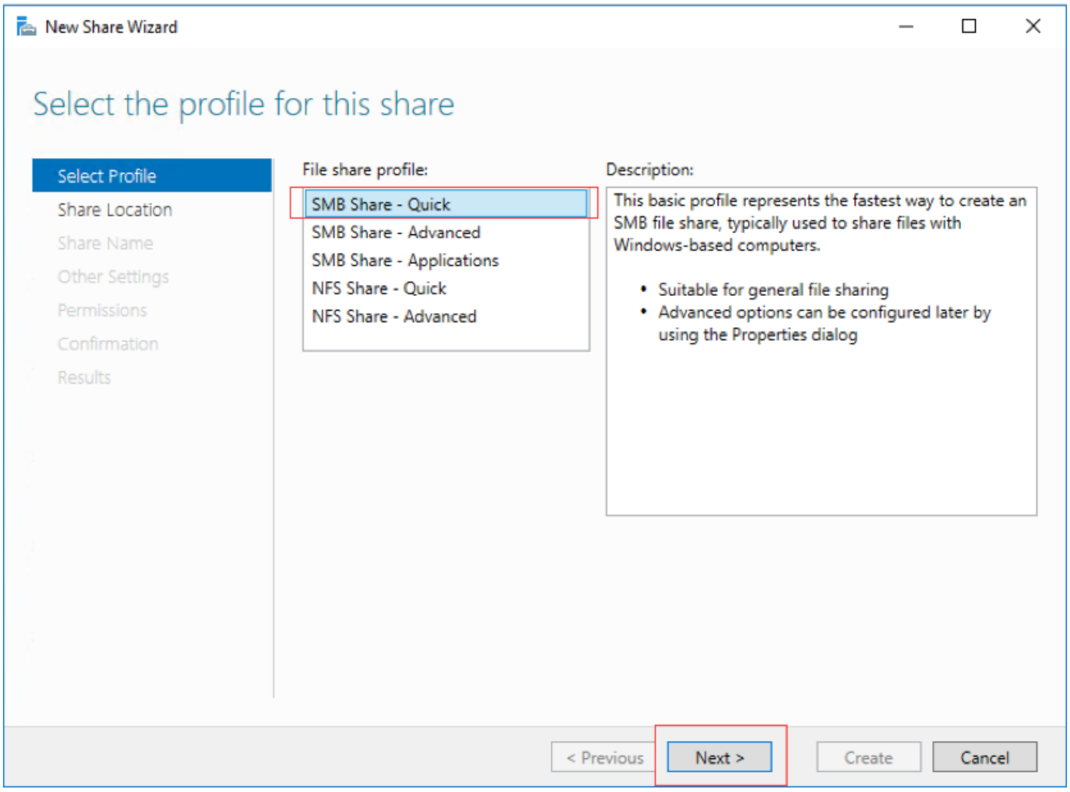
Create Data Proxy Account Create a normal domain user to be used as the Data Proxy Account. Don' t set a user from Domain Administrator/Local Administrator group as the Data Proxy Account.

Create a central store for Windows Server 2012 R2 or Windows Server 2016 When using Windows Server 2012 R2 or Windows Server 2016 for both the Self-Service Password Reset server and the central store, you can use a remote network share if configured as described in this section. Ensure that the **Encrypt data access** is selected and apply the guidance given in the Secure configuration.

1. To start the **New Share** wizard, open Server Manager. From the **File and Storage Services** details page, select **Shares** in the left pane, and click **Tasks > New Share**.



2. Choose **Select Profile** in the left pane, select **SMB Share - Quick**, and click **Next**.



Select the profile for this share

File share profile:

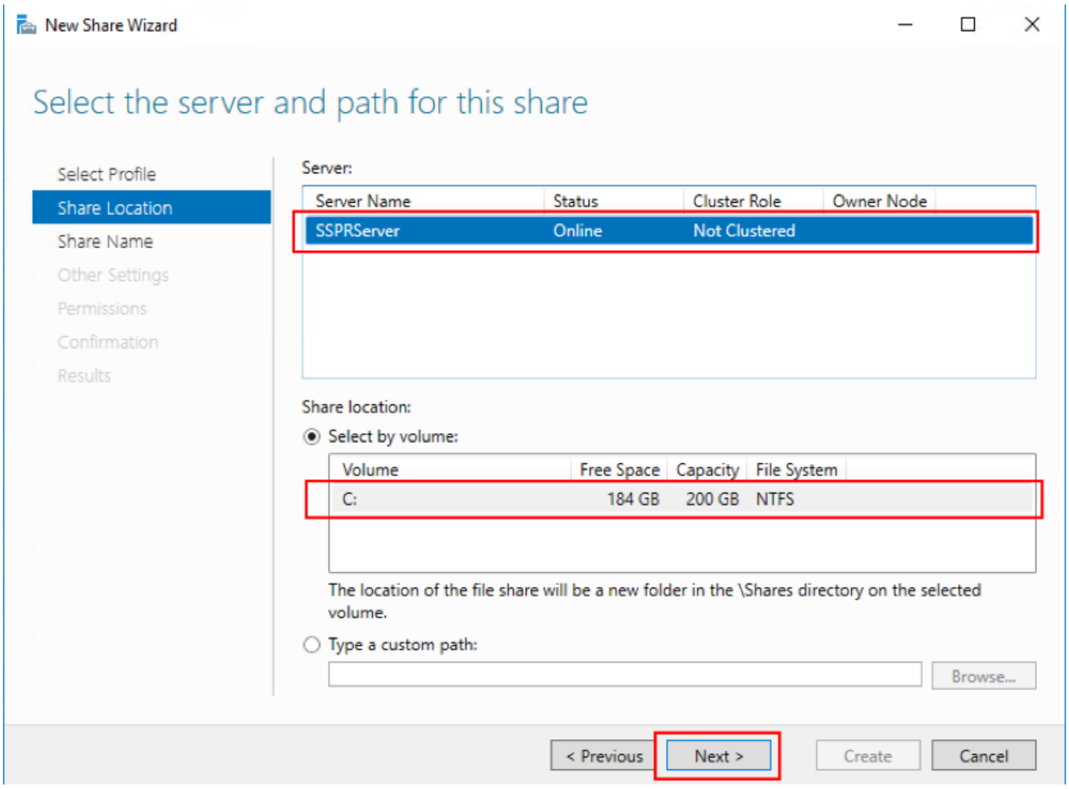
- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

Description:

This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

3. Choose **Share Location** in the left pane. From the list, select the server on which to create the new share and the volume on which to create the new shared folder, and then click **Next**.



Select the server and path for this share

Server:

Server Name	Status	Cluster Role	Owner Node
SSPRServer	Online	Not Clustered	

Share location:

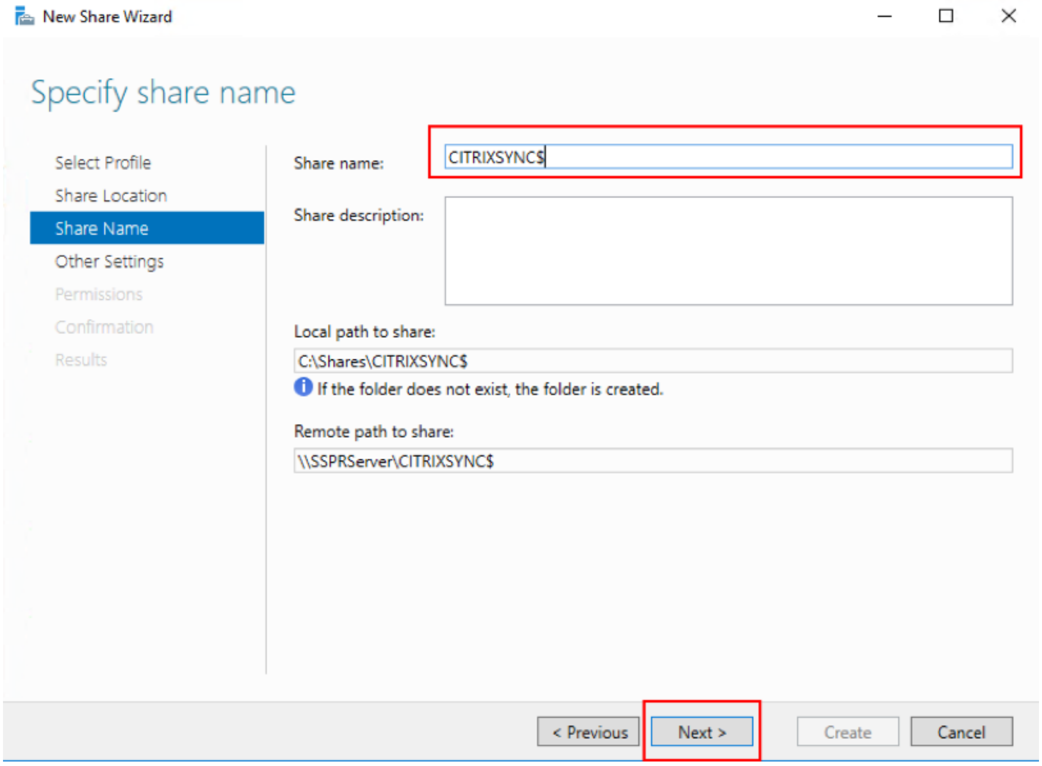
● Select by volume:

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

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

○ Type a custom path:

4. Choose **Share Name** in the left pane, type the name of your new Share name, for example **CITRIXSYNC$**, and click **Next**.



Specify share name

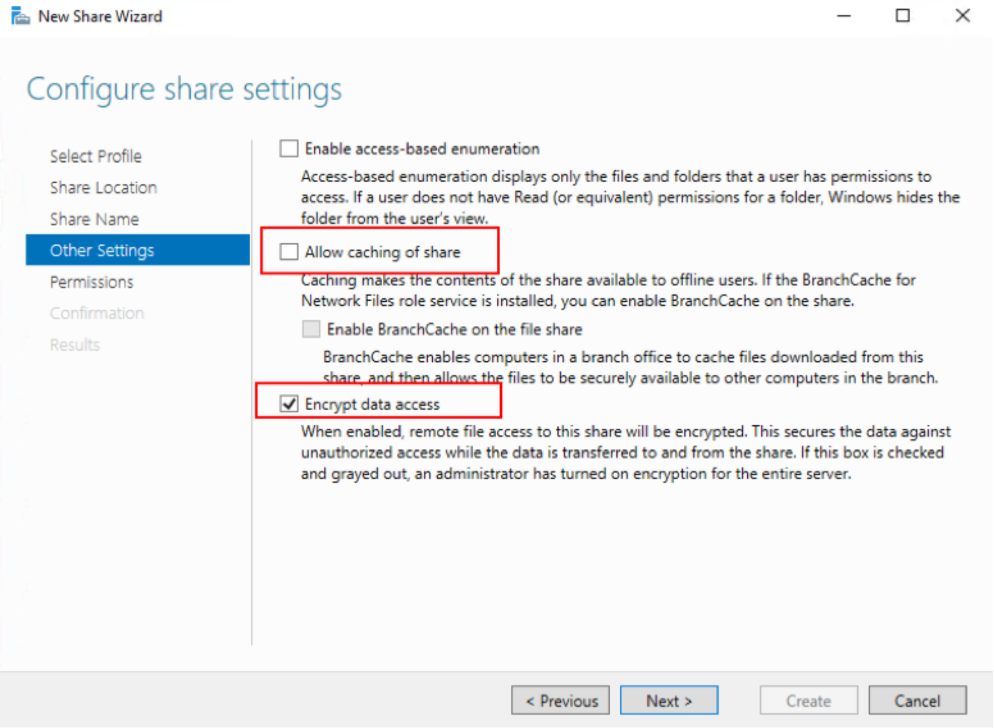
Share name: CITRIXSYNC$

Share description:

Local path to share:
C:\Shares\CITRIXSYNC$
If the folder does not exist, the folder is created.

Remote path to share:
\\SSPRServer\CITRIXSYNC$

5. Choose **Other Settings** in the left pane, select **Encrypt data**, deselect **Allow caching of share**, and click **Next**.



Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

□ Allow caching of share

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.

□ Enable BranchCache on the file share

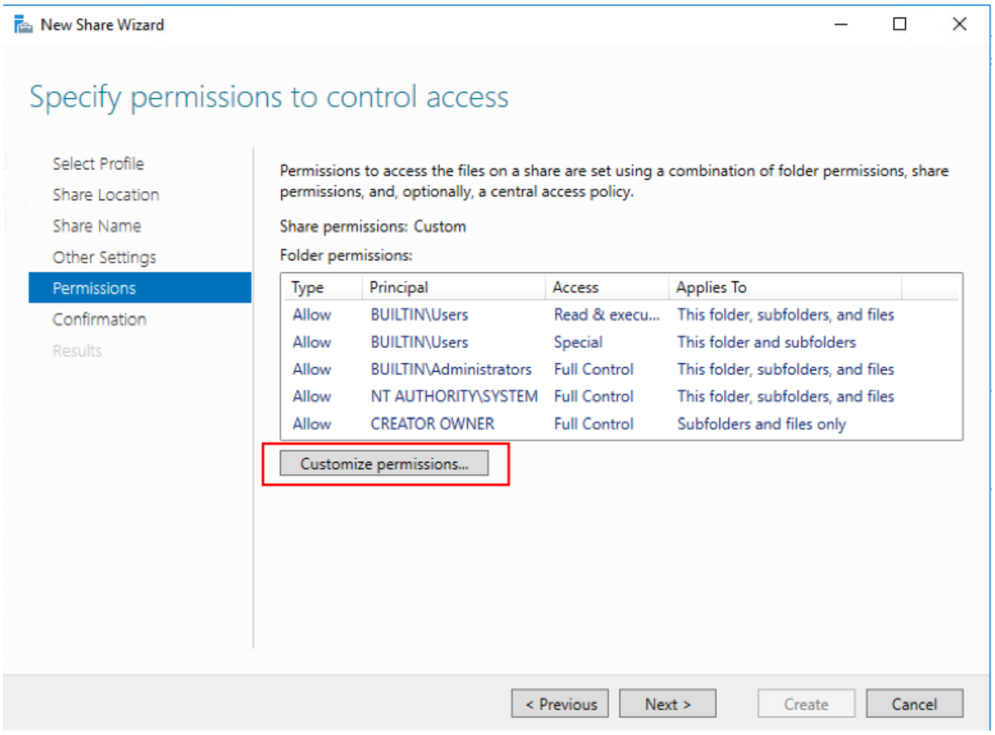
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☑ Encrypt data access

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.

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

6. To customize the **Share** permissions, choose **Permissions** in the left pane, and then select **Customize permissions > Share**.



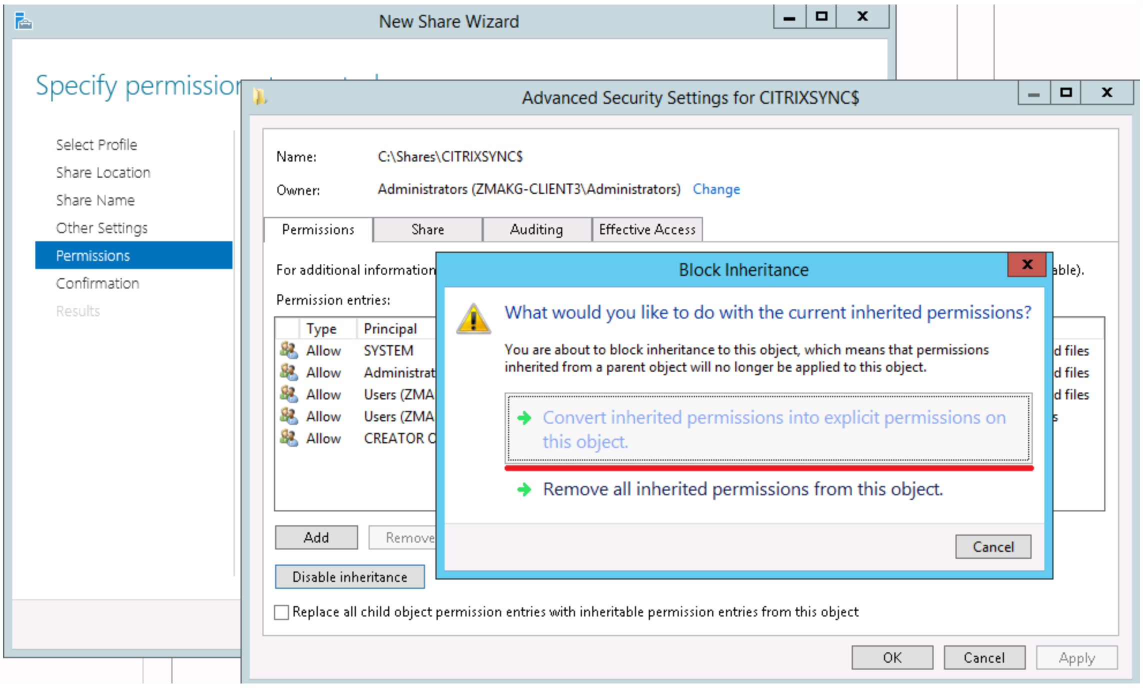
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Custom

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only

7. To customize the NTFS permissions, click **Disable inheritance**, and select **Convert inherited permissions into explicit permissions on this object**.



Name: C:\Shares\CITRIXSYNC$

Owner: Administrators (ZMAKG-CLIENT3\Administrators) Change

For additional information ... able).

Permission entries:

Type	Principal	
Allow	SYSTEM	d files
Allow	Administrat	d files
Allow	Users (ZMA	d files
Allow	Users (ZMA	s
Allow	CREATOR C	

What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

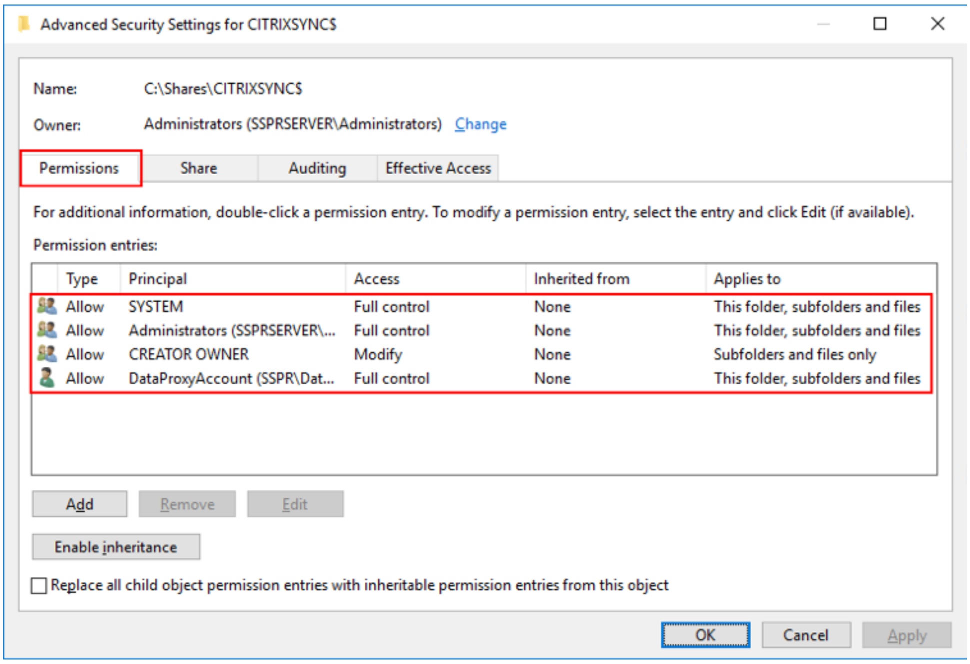
→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

□ Replace all child object permission entries with inheritable permission entries from this object

8. Click the **Permissions** tab, remove all users except **CREATOR OWNER**,**Local Administrators**,

and **SYSTEM**, and add the Data Proxy Account that was created with the Full Control permission.



Advanced Security Settings for CITRIXSYNC$

Name: C:\Shares\CITRIXSYNC$

Owner: Administrators (SSPRSERVER\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

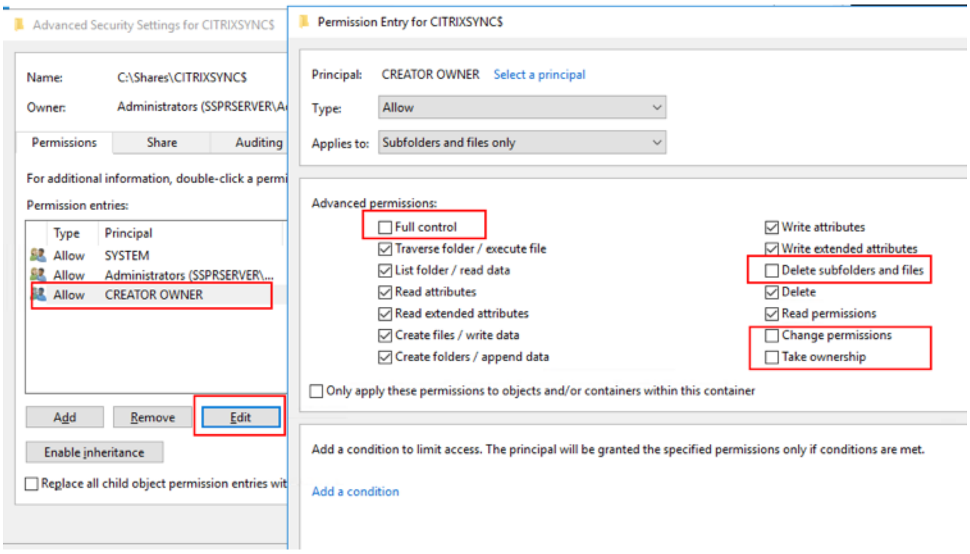
Permission entries:

Type	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\Dat...	Full control	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

9. Choose **CREATOR OWNER** and click **Edit** to uncheck the following permissions:

   - Full Control
   - Delete subfolders and files
   - Change permissions
   - Take ownership



Advanced Security Settings for CITRIXSYNC$

Name: C:\Shares\CITRIXSYNC$

Owner: Administrators (SSPRSERVER\A

For additional information, double-click a permi

Permission entries:

Type	Principal
Allow	SYSTEM
Allow	Administrators (SSPRSERVER\...
Allow	CREATOR OWNER

□ Replace all child object permission entries wit

Permission Entry for CITRIXSYNC$

Principal: CREATOR OWNER Select a principal

Type: Allow

Applies to: Subfolders and files only

Advanced permissions:

□ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
□ Delete subfolders and files
☑ Delete
☑ Read permissions
□ Change permissions
□ Take ownership

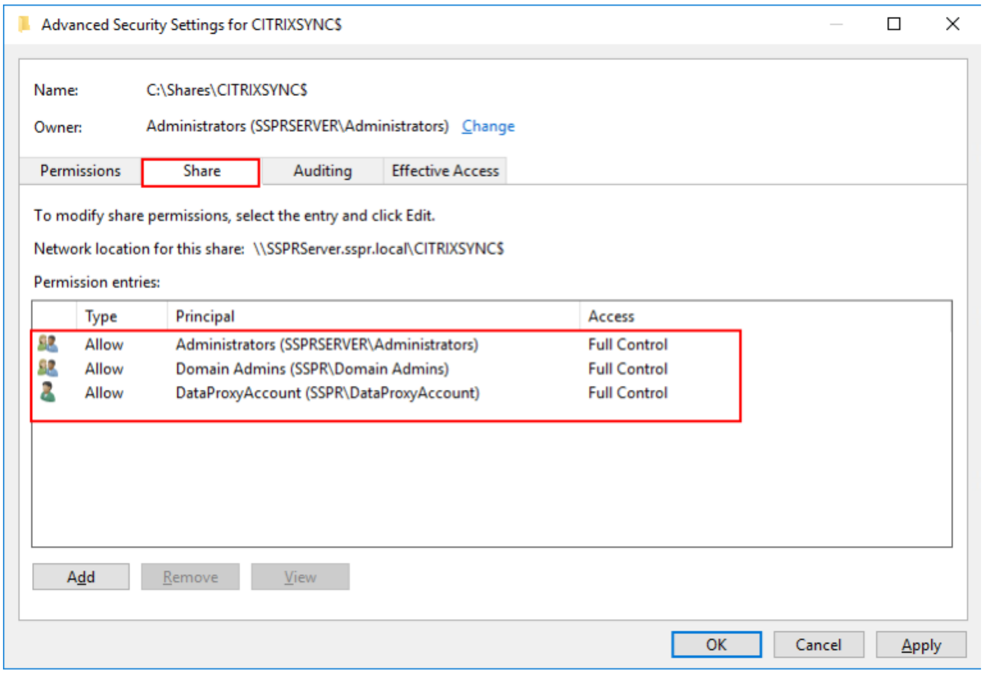
□ Only apply these permissions to objects and/or containers within this container

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

10. Choose the **Share** tab, remove **Everyone**, and add the Data Proxy Account, Local Administrators and Domain Admins with the Full Control permission.

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



Name: C:\Shares\CITRIXSYNC$

Owner: Administrators (SSPRSERVER\Administrators) Change

To modify share permissions, select the entry and click Edit.

Network location for this share: \\SSPRServer.sspr.local\CITRIXSYNC$

Permission entries:

Type	Principal	Access
Allow	Administrators (SSPRSERVER\Administrators)	Full Control
Allow	Domain Admins (SSPR\Domain Admins)	Full Control
Allow	DataProxyAccount (SSPR\DataProxyAccount)	Full Control

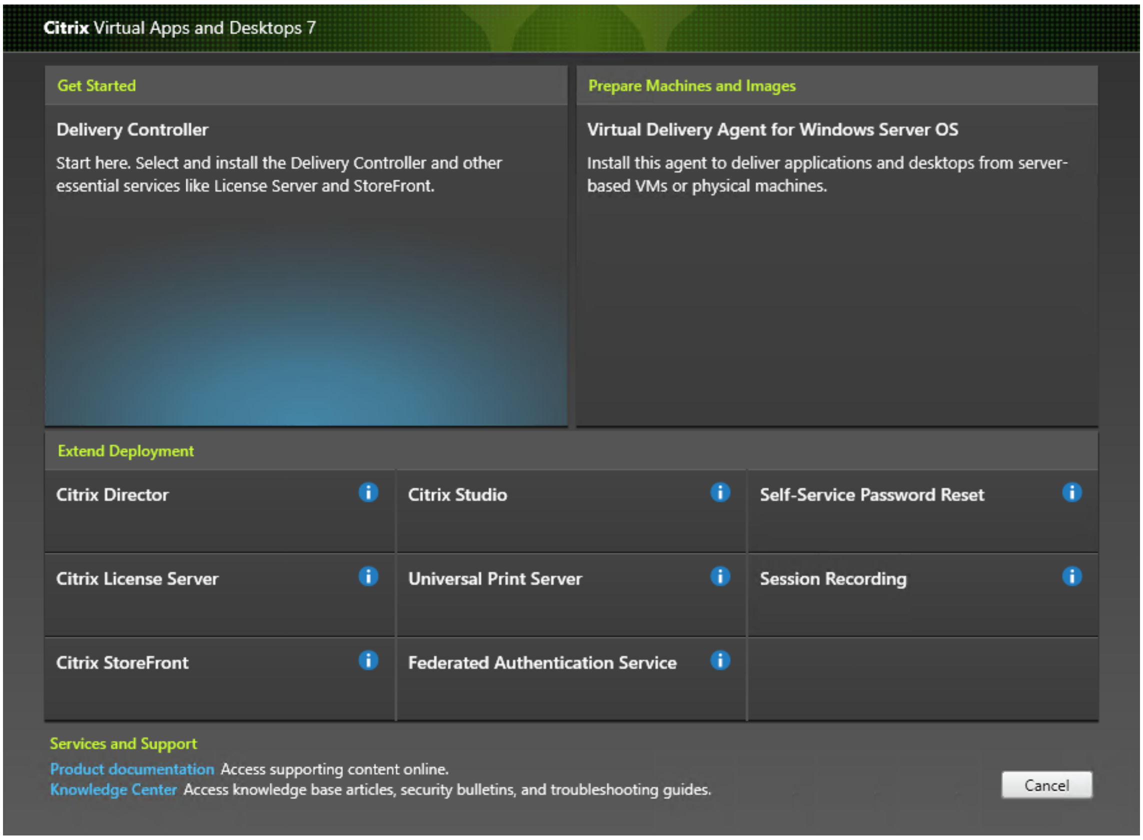
11. Choose **Confirmation** in the left pane of the New Share wizard, review the currently selected settings for sharing, and click **Create** to begin the process of creating the new folder, and then **Close**.
12. Create two subfolders under the **CITRIXSYNC$** share folder: **CentralStoreRoot** and **People**.

Important: Ensure that the Data Proxy Account has **Full Control** for these two subfolders.

You must configure EncryptData, RejectUnencryptedAccess, and RequireSecuritySignature for the Self-Service Password Reset central store. For more configuration information, see the following Microsoft articles:
https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbserverconfiguration
https://docs.microsoft.com/en-us/powershell/module/smbshare/set-smbshare

Install and configure Self-Service Password Reset

1. Install Self-Service Password Reset by using the Citrix Virtual Apps and Desktops installer.



Citrix Virtual Apps and Desktops 7

Get Started

Delivery Controller

Start here. Select and install the Delivery Controller and other essential services like License Server and StoreFront.

Prepare Machines and Images

Virtual Delivery Agent for Windows Server OS

Install this agent to deliver applications and desktops from server-based VMs or physical machines.

Extend Deployment

Citrix Director

Citrix Studio

Self-Service Password Reset

Citrix License Server

Universal Print Server

Session Recording

Citrix StoreFront

Federated Authentication Service

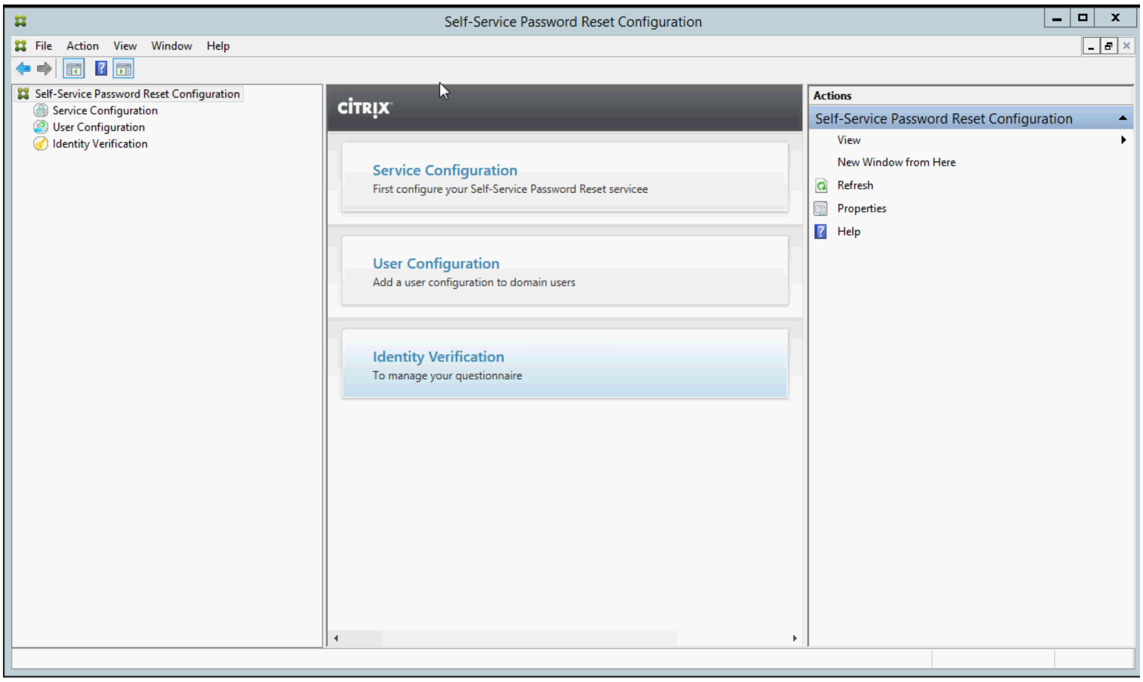
Services and Support

Product documentation Access supporting content online.

Knowledge Center Access knowledge base articles, security bulletins, and troubleshooting guides.

2. After installing Self-Service Password Reset, click **Start > All Programs > Citrix > Citrix Self-Service Password Reset Configuration** to configure the Citrix Self-Service Password Reset service.

3. When the console opens, follow these three basic procedures to configure the service.



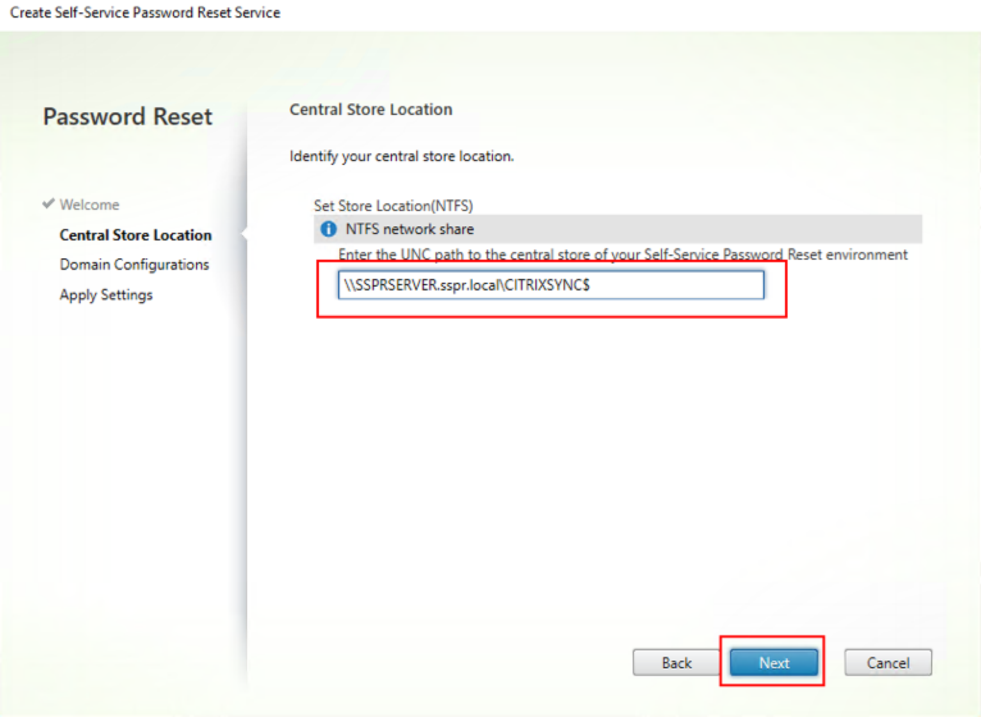
Service Configuration
First configure your Self-Service Password Reset servicee

User Configuration
Add a user configuration to domain users

Identity Verification
To manage your questionnaire

Service Configuration Before configuring the service, ensure you have created the central store, Data Proxy Account, and Self-Service account.

1. Select **Service Configuration** in the middle pane, and then click **New Service Configuration** in the right pane.
2. On the **Central Store Location** screen, specify the central store location, and click **Next**.



Create Self-Service Password Reset Service

Central Store Location

Identify your central store location.

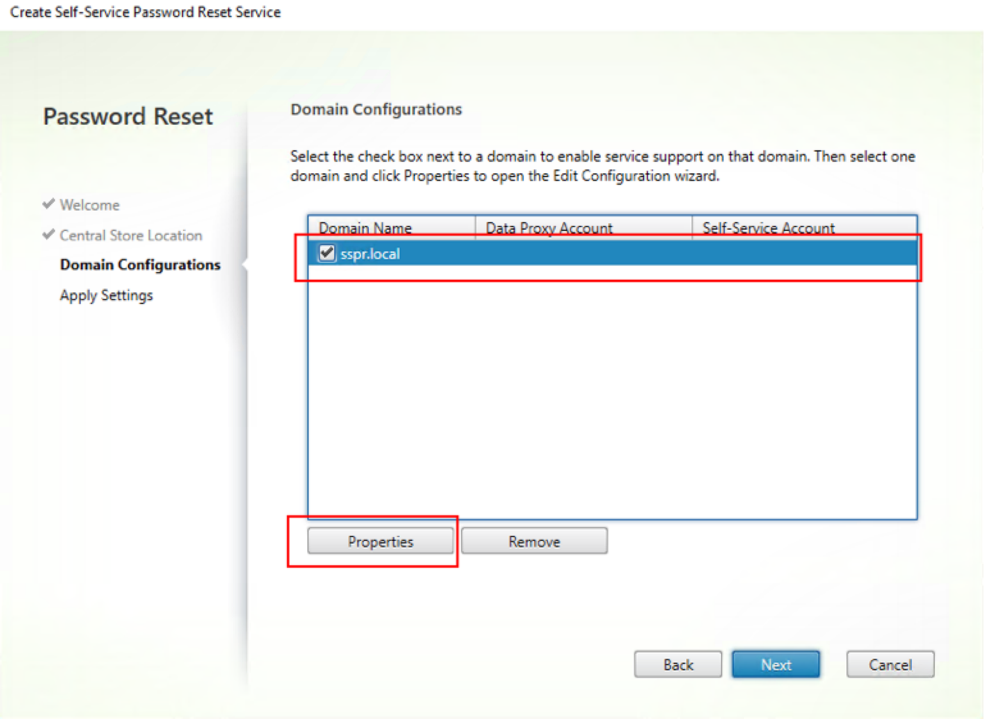
Set Store Location(NTFS)

NTFS network share

Enter the UNC path to the central store of your Self-Service Password Reset environment

\\SSPRSERVER.sspr.local\CITRIXSYNC$

3. On the **Domain Configurations** screen, select a domain where you want to enable the Self-Service Password Reset service, and click **Properties**.



Create Self-Service Password Reset Service

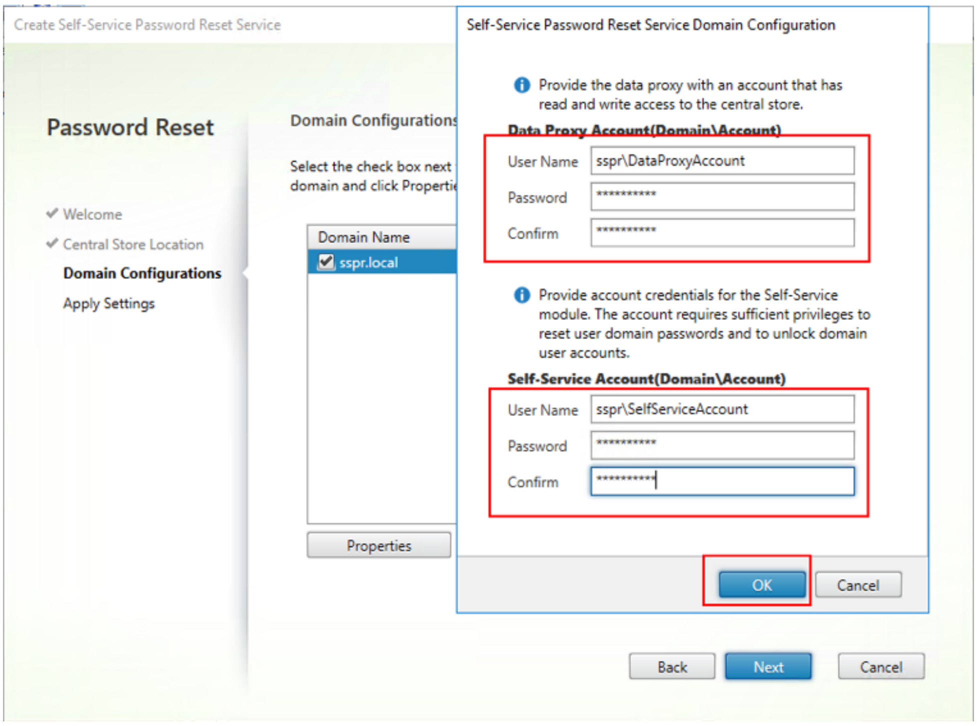
Domain Configurations

Select the check box next to a domain to enable service support on that domain. Then select one domain and click Properties to open the Edit Configuration wizard.

Domain Name	Data Proxy Account	Self-Service Account
☑ sspr.local		

4. Specify the **Data Proxy Account** user name and password and the **Self-Service Account** user name and password, and click **OK**.

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



Self-Service Password Reset Service Domain Configuration

Provide the data proxy with an account that has read and write access to the central store.

Data Proxy Account(Domain\Account)

User Name: sspr\DataProxyAccount

Password: **********

Confirm: **********

Provide account credentials for the Self-Service module. The account requires sufficient privileges to reset user domain passwords and to unlock domain user accounts.

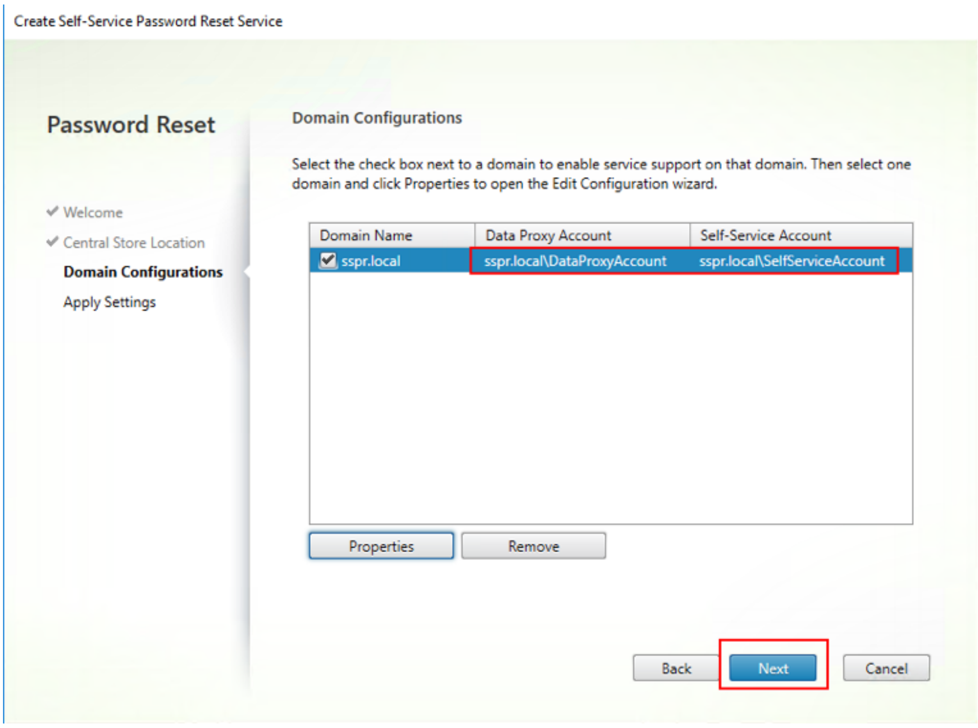
Self-Service Account(Domain\Account)

User Name: sspr\SelfServiceAccount

Password: **********

Confirm: **********

5. Click **Next** to apply all the settings.



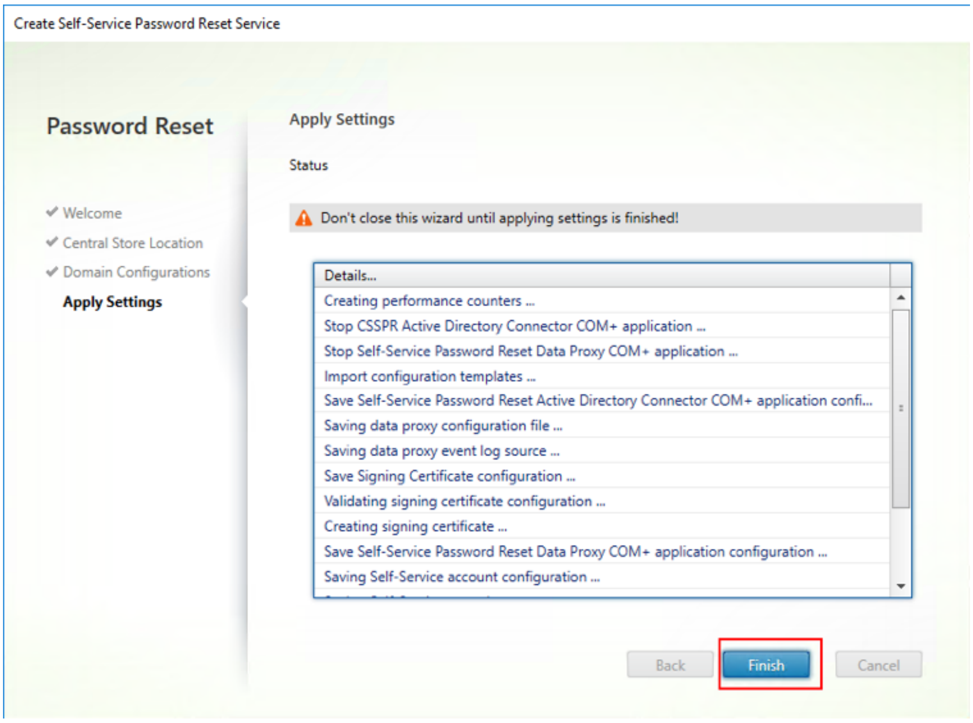
Domain Configurations

Select the check box next to a domain to enable service support on that domain. Then select one domain and click Properties to open the Edit Configuration wizard.

Domain Name	Data Proxy Account	Self-Service Account
☑ sspr.local	sspr.local\DataProxyAccount	sspr.local\SelfServiceAccount

6. Click **Finish** to complete the configuration.

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



Apply Settings

Status

Don't close this wizard until applying settings is finished!

Details...

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 ...

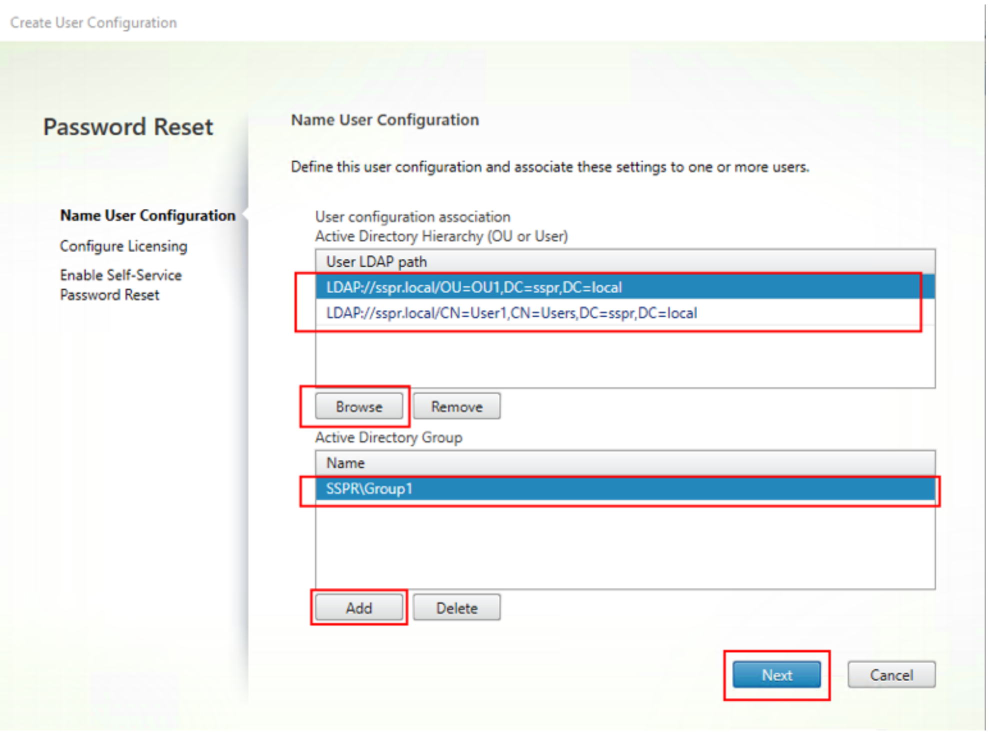
Creating signing certificate ...

Save Self-Service Password Reset Data Proxy COM+ application configuration ...

Saving Self-Service account configuration ...

User Configuration

1. In the left pane, select **User Configuration**, and then click **New User Configuration** in the right pane.
2. On the **Name User Configuration** screen, define the Self-Service Password Service target user groups, add users/groups/OUs from Active Directory, and click **Next**.



Create User Configuration

Password Reset

Name User Configuration

Configure Licensing

Enable Self-Service Password Reset

Name User Configuration

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

User configuration association

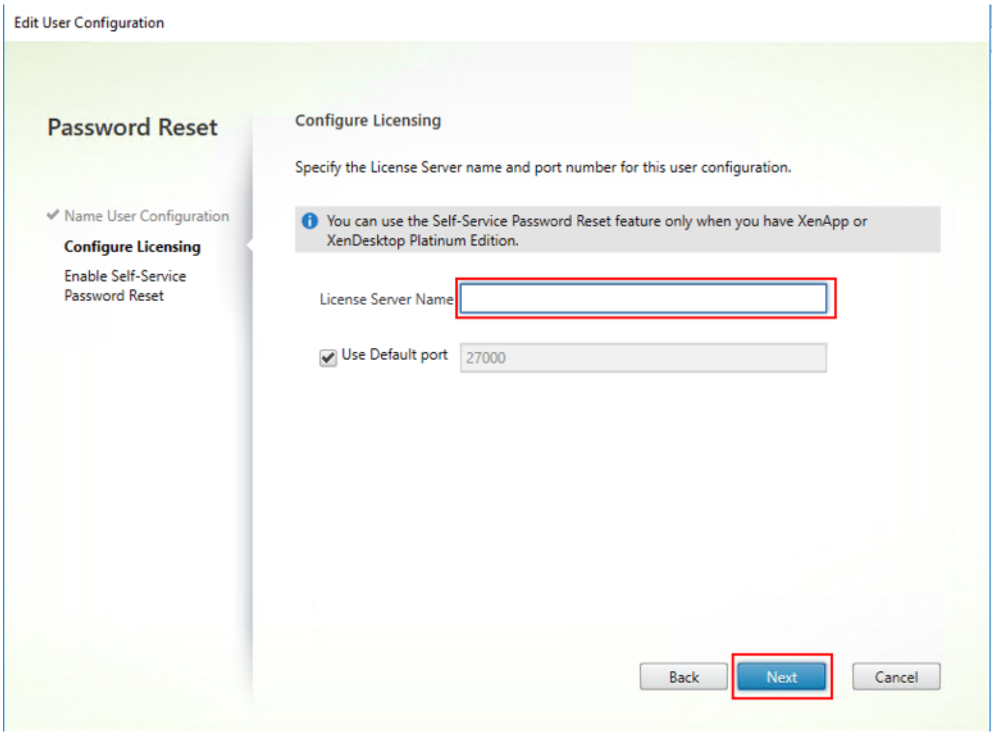
Active Directory Hierarchy (OU or User)

User LDAP path
LDAP://sspr.local/OU=OU1,DC=sspr,DC=local
LDAP://sspr.local/CN=User1,CN=Users,DC=sspr,DC=local

Active Directory Group

Name
SSPR\Group1

3. On the **Configure Licensing** screen, specify the License Server, and click **Next**.



Edit User Configuration

Password Reset

✓ Name User Configuration

Configure Licensing

Enable Self-Service Password Reset

Configure Licensing

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

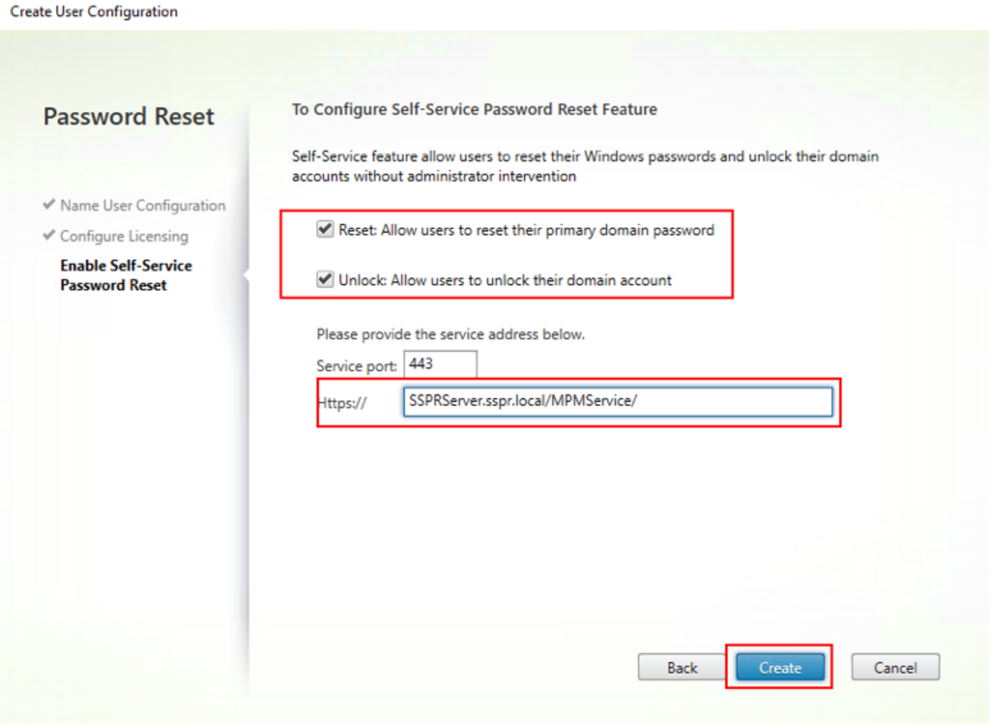
You can use the Self-Service Password Reset feature only when you have XenApp or XenDesktop Platinum Edition.

License Server Name

☑ Use Default port 27000

4. On the **Enable Self-Service Password Reset** screen, use the check boxes to specify whether users can reset their Windows passwords and unlock their domain accounts without administrative intervention, specify the service port and address, and then click **Create**.

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



Create User Configuration

Password Reset

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

To Configure Self-Service Password Reset Feature

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

☑ Reset: Allow users to reset their primary domain password

☑ Unlock: Allow users to unlock their domain account

Please provide the service address below.

Service port: 443

Https:// SSPRServer.sspr.local/MPMService/

For more information about managing user configurations, see Manage user configurations.

Identity Verification

1. In the left pane, select the **Identity Verification** node, and then click **Manage Questions** in the right pane.
2. On the **Question-Based Authentication** screen, select the default language, use the check box to enable or disable masking security question answers, and click **Next**.
3. On the **Security Questions** screen, click **Add Question**, type a question in the text box, click **OK**, and then click **Next**.
4. On the **Questionnaire** screen, click **Add**, and select a question. You can reorganize your questions and groups with the **Move Up** and **Move Down** buttons. When you are finished on this page, click **Create** and **OK**.

For more information about managing identity verification questions, see Manage Identity Verification questions.

Manage user configurations A user configuration enables you to control the behavior and appearance of the interface when users log on to Storefront. Creating a new configuration is the final step you take before distributing Self-Service Password Reset to users in your environment. You can edit existing user configurations at any time.

A user configuration is a unique collection of settings that you apply to users associated with an Active

Directory hierarchy (Organizational Unit [OU] or an individual user) or an Active Directory group.

A user configuration consists of the following:

- Users associated with an Active Directory domain hierarchy (OU or individual user) or Active Directory group

Important: Distribution groups and Domain Local groups in Active Directory mixed mode are not supported.

- License Server
- Self-service features (account unlock and password reset)

Before you create your user configurations, ensure that you already created or defined the following:

- Central store
- Service configuration

To create a user configuration:

1. Click **Start** > **All Programs** > **Citrix** > **Citrix Self-Service Password Reset Configuration**.
2. In the left pane, select the **User Configurations** node.
3. From the **Actions** menu, click **Add new user configuration**.

To add users, OU, or Group:

The **Name User Configuration** page of the **User Configuration** wizard allows you to associate the user configuration to the users.

User configuration association:

You have two choices: associate users according to Active Directory hierarchy (OU or individual user) or Active Directory Group. If necessary, you can associate the user configuration with a different hierarchy or group later, by clicking **Edit user configuration** in the **Actions** menu.

Associating user configurations to groups is supported only in Active Directory domains that use Active Directory authentication.

Select the OU, or Users, or Group on the **Name User Configuration** page (from Add New User Configuration or Edit User Configuration wizard).

Note: We recommend that you not include any privileged accounts (for example, Local Administrators or Domain Administrators) in the group of users for whom the Self-Service Password Reset account can reset passwords. Use a new dedicated group.

To configure licensing:

The **Configure Licensing** page of the **User Configuration** wizard allows you to configure the License Server used by the Self-service Password Reset service.

Note: You can use the Unlock and Reset features only if you have Citrix Virtual Apps or Citrix Virtual Desktops Platinum Edition.

Enter the License Server name and port number on the **Configure Licensing** page (from Add New User Configuration or Edit User Configuration wizard).

To enable Unlock or Reset features:

Self-Service Password Reset allows users to reset their Windows password and unlock their domain accounts without administrator intervention. From the **Enable Self-Service Password Reset** page, you can select which feature to enable.

Select which feature you want to users to use: **Unlock** or **Reset** on the **Enable Self-Service Password Reset** page (from Add New User Configuration or Edit User Configuration wizard).

To configure a blacklist:

IT administrators can add users and groups to the blacklist. Users and groups in the blacklist cannot use any of the Self-Service Password Reset features - including enrollment, account unlock, and password reset. Also, a user in the blacklist cannot see the **TASK** button on Citrix Workspace app after logging on.

To configure the blacklist:

1. Click **Start > All Programs > Citrix > Citrix Self-Service Password Reset Configuration**.
2. In the left pane, select **User Configuration**, and then click **Blacklist Configuration** in the right pane.
3. Use the **Add** and **Remove** buttons to add and remove users or groups to and from the blacklist.

Manage Identity Verification questions The Identity Verification of the Citrix Self-Service Password Reset Configuration Console provides you with a central location for managing all security questions associated with identity verification, Self-Service Password Reset, and account unlock. You can customize your own security questions to the list of default questions and create question groups.

- If you edit the existing default questions after users register their answers, consider the meaning of the edited questions. Editing a question does not force a user re-enrollment. But if you change the meaning of a question, users who answered that question originally might not be able to provide the correct answer.
- Adding, deleting, and replacing security questions after users are enrolled means that all users who were previously enrolled using an older set of questions cannot authenticate and reset their password until they reenroll. Users must answer the new set of questions when they open the Tasks in Citrix Workspace app.
- Individual security questions can belong to multiple security question groups. When you create your security question groups, all questions you create are available for use with any security question group.

Use these steps to access the settings referenced in the following procedures:

1. Click **Start** > **All Programs** > **Citrix** > **Citrix Self-Service Password Reset Configuration**.
2. In the left pane, select the **Identity Verification** node.
3. From the **Actions** menu, click **Manage Questions**.

To set the default language:

In most instances, users see security questions displayed in the language associated with their current user profile. If the language is not available, Self-Service Password Reset displays the questions in the default language that you specify.

1. Click **Start** > **All Programs** > **Citrix** > **Citrix Self-Service Password Reset Configuratio**n.
2. In the left pane, select the **Identity Verification** node.
3. From the **Actions** menu, click **Manage Questions**.
4. From the **Default Language** drop-down list on the **Question-Based Authentication** page, select the default language.

To enable security answer masking:

Security answer masking provides an added level of security for your users when they register their security question answers or provide their answers during identity verification. When this feature is enabled, the users'answers are hidden. During the answer registration process, these users are asked to type their answers twice to avoid typing and spelling errors. Users type their answers only once during identity validation because they are prompted to retry if there is an error.

Select **Mask answers for security questions** on the **Question-Based Authentication** page.

To create new security questions:

You can create many different questions and designate a language for each question. You can also provide multiple translations of a single question. The Enrollment in Citrix Workspace app presents the user with the questionnaire in the language that corresponds to the language settings of the user's profile. If the language is not available, Self-Service Password Reset displays the questions in the default language.

Note: When you specify a language for a security question, the question appears to users whose operating system settings are configured for that designated language. If the selected operating system settings do not match any of the questions available, users are shown your selected default language.

1. From the **Language** drop-down list on the **Security Questions** page, select a language and click **Add Question**. The Security Question dialog box appears.
2. Create the new question on the **Security Question** dialog box.

Important: Use the **Edit** button to include the translated text of existing questions. If you select **Add Question**, you are creating a new question that is not associated with the original.

To add or edit text for existing questions:

Adding, deleting, and replacing security questions after users are enrolled means that all users who were previously enrolled using an older set of questions cannot authenticate and reset their password until they reenroll. Users must answer the new set of questions when they open the Tasks in Citrix Workspace app. Editing a question does not force a user re-enrollment.

Important: If you are editing an existing question, be careful not to change the meaning of a question. This might cause a mismatch in user answers during reauthentication. That is, a user might provide a different answer that might not match the stored answer.

1. Select a language from the **Language** drop-down box on the **Security Questions** page.
2. Select the question and click **Edit**.
3. Edit the question in the **Security Question** dialog box.

To create a security question group:

You can create some security questions that your users answer to confirm their identities. Each question you add to the questionnaire must be answered by your users. However, you can also group these questions together in a security question group.

For example, putting your questions in a group enables you to add a group of six questions to your questionnaire, and allows your users to choose from that group of questions, answering, for example, three of the six. This gives your users flexibility in selecting questions and providing answers to be used for identity verification.

1. Click **Add Group** on the **Security Questions** page.
2. In the **Security Question Group** dialog box, name the group, select the questions, and set the number of questions the user must answer.

To edit a security question group:

Select the security group you want to edit and click **Edit** on the **Security Questions** page. The Security Question Group dialog box appears, with a list of security questions available to be part of the group. The questions currently in the group are indicated by a check mark. Here you can edit the name of the group, add questions to the group, and select the number of questions from this group that a user must answer.

To add or remove the existing questionnaire:

Add or remove security questions and question groups from the questionnaire. Move the questions up and down in the order to be presented to the user. If the questionnaire has changed, notify the user to do re-enrollment task after logging on Storefront.

1. Click **Add** on the **Questionnaire** page to add question or group to questionnaire.
2. Click **Remove** to remove a question from the questionnaire.

3. Click **Move Up** or **Move Down** to manage the questions presented to user.

To import or export the security questions:

You can import or export the data of security questions and groups.

1. Click **Start** > **All Programs** > **Citrix** > **Citrix Self-Service Password Reset Configuration**.
2. In the left pane, select the **Identity Verification** node.
3. From the **Actions** menu, click one of the following:

   Import the security questions
   Specify the file location to import the data of security questions and groups.

   Export the security questions
   Specify the file location to export the data of security questions and groups.

Secure configuration

July 5, 2018

This article contains the procedures required to ensure that Self-Service Password Reset components are securely deployed and configured.

- Create a Domain user account to reset user password and unlock user account permission
- Configure the firewall settings

Create a Self-Service Account

If you are using the Password Reset or Account Unlock features of Self-Service Password Reset, specify a Self-Service account during Service Configuration that is used by the self-service module to execute Password Reset and Account Unlock. Ensure that the account has sufficient privilege, but we do not recommend using an account in the Domain Admins group for production deployments. The recommended account privileges are:

- Member of the domain
- Password reset and account unlock permission for the relevant domain users

In **Active Directory Users and Computers**, create the group or user account to have the rights to reset the user password and unlock user accounts.

1. In **Active Directory Users and Computers**, right-click the domain, and then click **Delegate Control** from the menu.

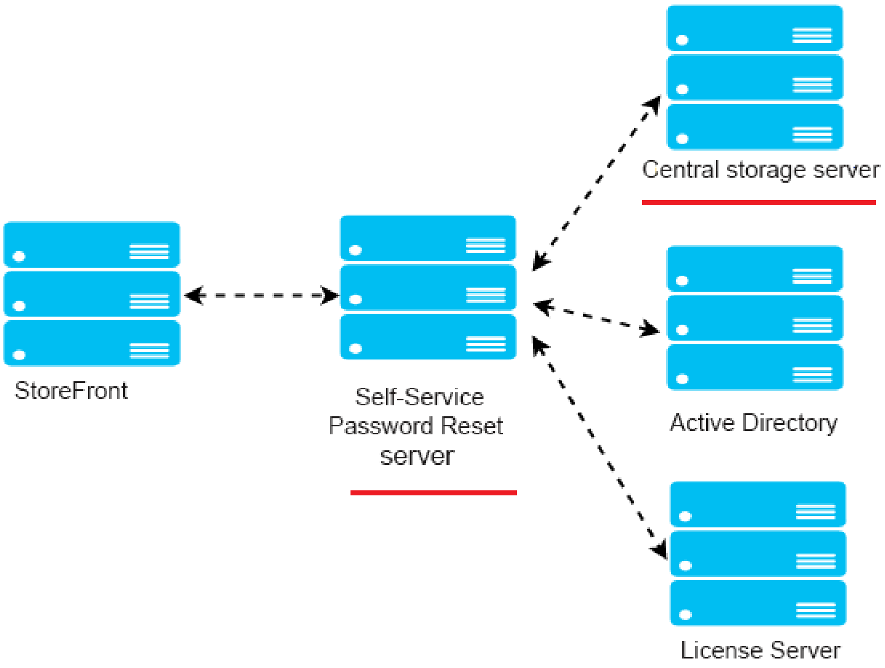
2. The **Delegation of Control** wizard displays. On the **Welcome** dialog box, click **Next**.
3. On the **Users and Groups** dialog box, click **Add**. Select the group in the list that you want to give the right to unlock accounts, and then click **OK**. On the **Users and Groups** dialog box, click **Next**.
4. On the **Tasks to Delegate** dialog box, click **Create a custom task to delegate**, and then click **Next**.
5. On the **Active Directory Object Type** dialog box, click Only the following objects in the folder > User objects, and then click **Next**.
6. On the **Permissions** dialog box, select the **General** and **Property-specific** check boxes. In the **Permissions** list, select the **Read lockoutTime** , **Write lockoutTime**, **Reset Password, Change Password, Read userAccountControl, Write userAccountControl, Read pwdLastSet, and Write pwdLastSet** check boxes, and then click **Next**.
7. On the **Completing the Delegation of Control** wizard dialog box, click **Finish**.

Configure the firewall settings

Because the Self-Service Password Reset server and the central storage server components manage user passwords, we strongly recommend that you deploy these components on a trusted network and that they are reachable only by specific trusted components. This section describes the steps to ensure that you correctly configure the Windows firewall for these servers. We also recommend that you configure existing network infrastructure to ensure that these servers are isolated from untrusted network traffic.

After you complete those configurations in the deployment, the Self-Service Password Reset central store servers can be accessed only from Self-Service Password Reset servers using Server Message Block (SMB). And the Self-Service Password Reset servers are accessed only from the StoreFront servers with HTTPS connections.

Remote file share deployment for Windows 2012 R2



Environment

- Deploy the Self-Service Password Reset components on dedicated servers. Do not deploy them on the same servers as the existing StoreFront or Delivery Controller components. Otherwise, the firewall configuration shown below might block the Storefront or controller traffic.
- There is no non-transparent HTTP/HTTPS proxy between StoreFront and Self-Service Password Reset server.

If any non-transparent proxy exists between StoreFront and the Self-Service Password Reset server, configure the Self-Service Password Reset server to be accessed only from the proxy server in the firewall rules.

- The configurations in these procedures are based on the windows default firewall rules.

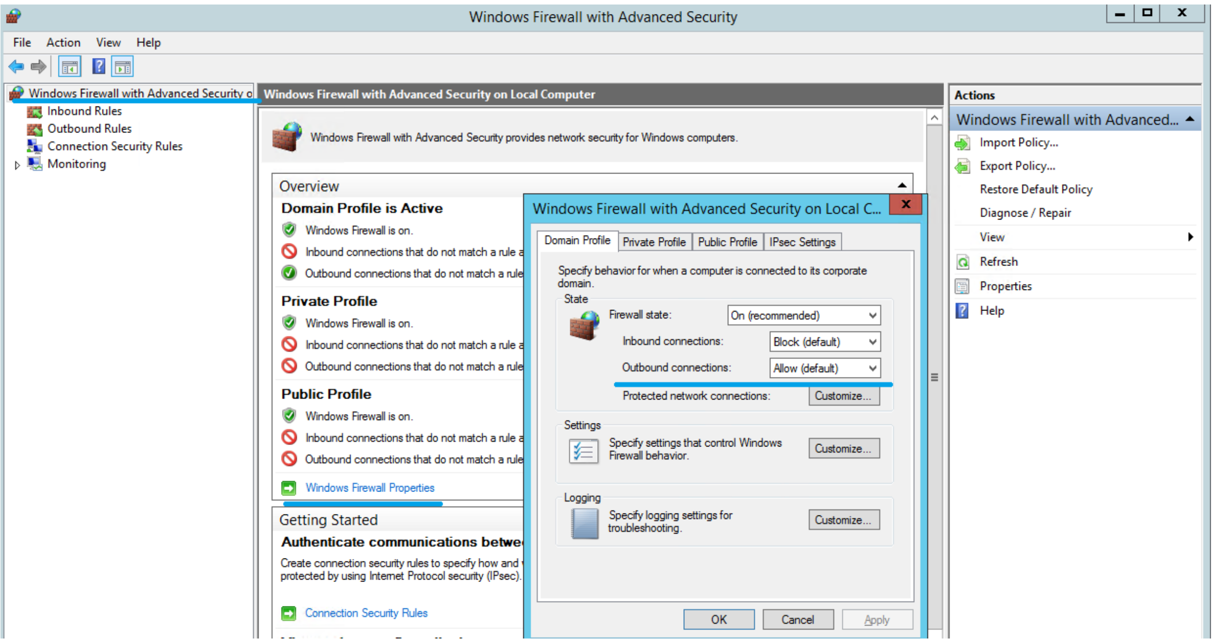
Configure the firewall for Self-Service Password Reset central store

After completing the configuration, the SMB service provided by the Self-Service Password Reset central store can be accessed only from the Self-Service Password Reset servers on the inbound. And the Self-Service Password Reset central store server can access service located on the corporate network only on the outbound.

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

1. Open the Server Manager, and from the **Tools** menu on the top navigation bar, select **Windows Firewall with Advanced Security**.

2. On **Windows Firewall with Advanced Security**, select **Windows Firewall Properties** in the middle pane. There are three firewall profiles - Domain, Private, and Public. Select the **Domain Profile** tab. Ensure that the **Firewall state** is set to **On**, the **Inbound connections** are set to **Block**, and the **Outbound connections** are set to **Allow**.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced Security o
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Overview
Getting Started
Windows Firewall Properties
Connection Security Rules
Actions
Windows Firewall with Advanced...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Windows Firewall with Advanced Security on Local C...
Domain Profile
Private Profile
Public Profile
IPsec Settings
State
Settings
Logging
Customize...
OK
Cancel
Apply

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile is Active

Windows Firewall is on.

Inbound connections that do not match a rule a

Outbound connections that do not match a rule

Private Profile

Windows Firewall is on.

Inbound connections that do not match a rule a

Outbound connections that do not match a rule

Public Profile

Windows Firewall is on.

Inbound connections that do not match a rule a

Outbound connections that do not match a rule

Authenticate communications betwe

Create connection security rules to specify how and protected by using Internet Protocol security (IPsec).

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

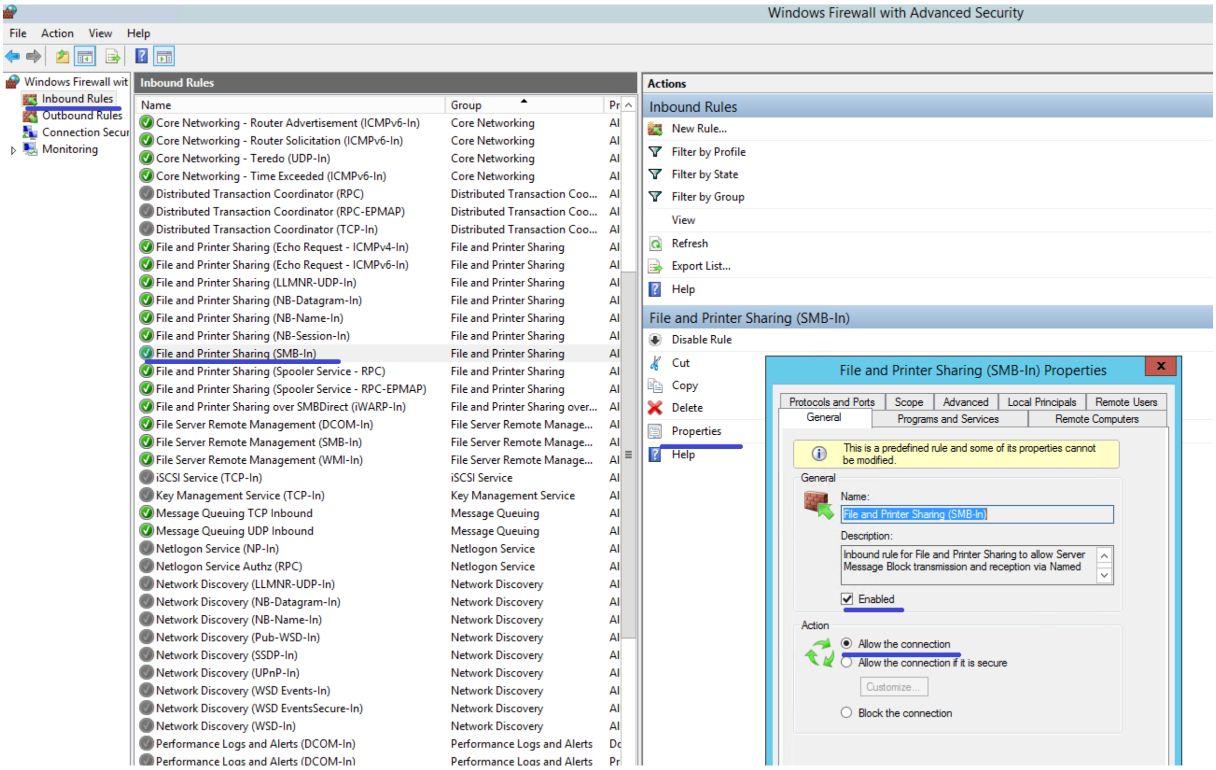
Protected network connections: Customize...

Specify settings that control Windows Firewall behavior.

Specify logging settings for troubleshooting.

3. Select the **Private Profile** and **Public Profile** tabs. Ensure that the **Firewall state** is set to **On**, and both the **Inbound connections** and **Outbound connections** are set to **Block**. Apply and save the changes.

4. From the **Inbound Rules**, choose **File and Printer Sharing (SMB-In)** and ensure that this rule is **Enabled** and the **Action** is set to **Allow the connection**.



Name	Group	Pr
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	Al
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	Al
Core Networking - Teredo (UDP-In)	Core Networking	Al
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	Al
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Al
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Al
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Al
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Al
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Al
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Al
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Al
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Al
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Al
File and Printer Sharing (SMB-In)	File and Printer Sharing	Al
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Al
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Al
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	Al
File Server Remote Management (DCOM-In)	File Server Remote Manage...	Al
File Server Remote Management (SMB-In)	File Server Remote Manage...	Al
File Server Remote Management (WMI-In)	File Server Remote Manage...	Al
iSCSI Service (TCP-In)	iSCSI Service	Al
Key Management Service (TCP-In)	Key Management Service	Al
Message Queuing TCP Inbound	Message Queuing	Al
Message Queuing UDP Inbound	Message Queuing	Al
Netlogon Service (NP-In)	Netlogon Service	Al
Netlogon Service Authz (RPC)	Netlogon Service	Al
Network Discovery (LLMNR-UDP-In)	Network Discovery	Al
Network Discovery (NB-Datagram-In)	Network Discovery	Al
Network Discovery (NB-Name-In)	Network Discovery	Al
Network Discovery (Pub-WSD-In)	Network Discovery	Al
Network Discovery (SSDP-In)	Network Discovery	Al
Network Discovery (UPnP-In)	Network Discovery	Al
Network Discovery (WSD Events-In)	Network Discovery	Al
Network Discovery (WSD EventsSecure-In)	Network Discovery	Al
Network Discovery (WSD-In)	Network Discovery	Al
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Dc
Performance Logs and Alerts (DCOM-In)	Performance Logs and Alerts	Pr

This is a predefined rule and some of its properties cannot be modified.

Name: File and Printer Sharing (SMB-In)

Description: Inbound rule for File and Printer Sharing to allow Server Message Block transmission and reception via Named

☑ Enabled

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

5. On **File and Printer Sharing (SMB-In) Properties**, change to the **Scope** tab. Choose **These IP addresses** and add all Self-Service Password Reset server IP addresses into the list. For example, Self-Service Password Reset server A (192.168.1.10) and Self-Service Password Reset server B (192.168.1.11).

6. On **File and Printer Sharing (SMB-In) Properties**, change to the **Advanced** tab, select the profiles **Domain**, **Private**, and **Public**, and save the changes of this rule.

7. Repeat this procedure on the **Inbound** rules for **File Server Remote Management (SMB-In)** and **File and Printer Sharing (NB-Session-In)**.

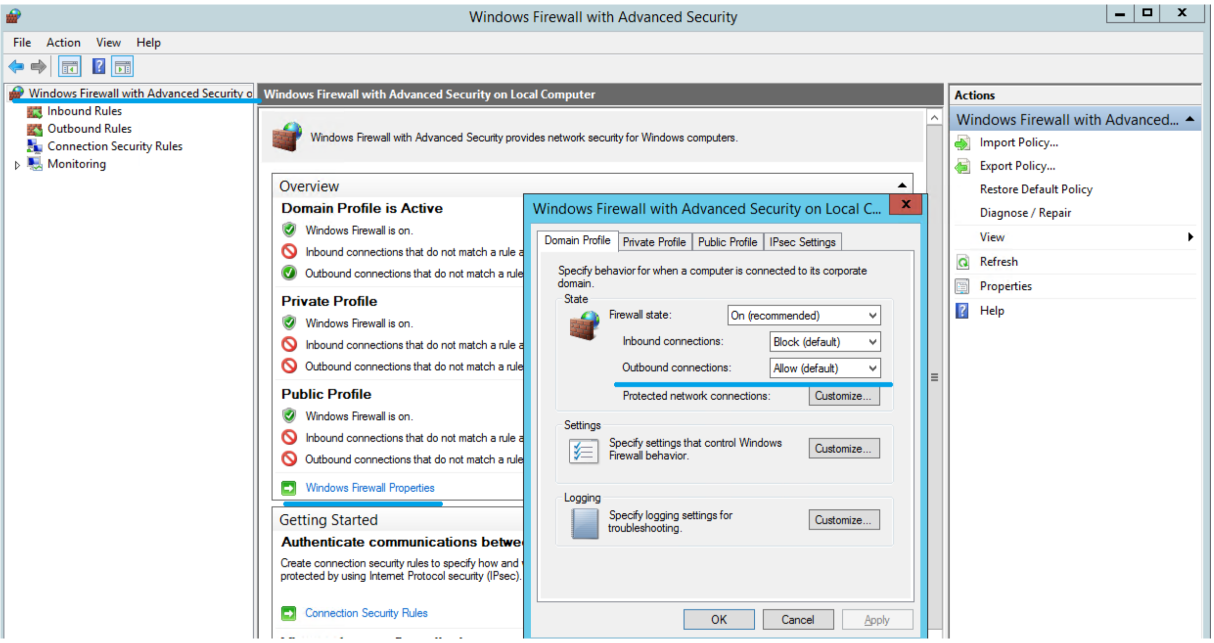
Configure the firewall for the Self-Service Password Reset server

After completing the configuration, the web service provided by the Self-Service Password Reset servers can be accessed only by the StoreFront servers using HTTPS. And the Self-Service Password Reset servers can access service located on the corporate network.

1. Open the Server Manager, and from the **Tools** menu on the top navigation bar, select **Windows Firewall with Advanced Security**.

2. On **Windows Firewall with Advanced Securit**y, select **Windows Firewall Properties** in the middle pane. There are three firewall profiles - Domain, Private, and Public. Select the **Domain Profile** tab. Ensure that the **Firewall state** is set to **On**, the **Inbound connections** are set to **Block**, and the **Outbound connections** are set to **Allow**.

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


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced Security o
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Overview
Getting Started
Windows Firewall Properties
Connection Security Rules
Actions
Windows Firewall with Advanced...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Windows Firewall with Advanced Security on Local C...
Domain Profile
Private Profile
Public Profile
IPsec Settings
State
Settings
Logging
Customize...
OK
Cancel
Apply

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile is Active
- Windows Firewall is on.
- Inbound connections that do not match a rule a
- Outbound connections that do not match a rule

Private Profile
- Windows Firewall is on.
- Inbound connections that do not match a rule a
- Outbound connections that do not match a rule

Public Profile
- Windows Firewall is on.
- Inbound connections that do not match a rule a
- Outbound connections that do not match a rule

Authenticate communications betwe

Create connection security rules to specify how and protected by using Internet Protocol security (IPsec).

Specify behavior for when a computer is connected to its corporate domain.

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Specify settings that control Windows Firewall behavior.

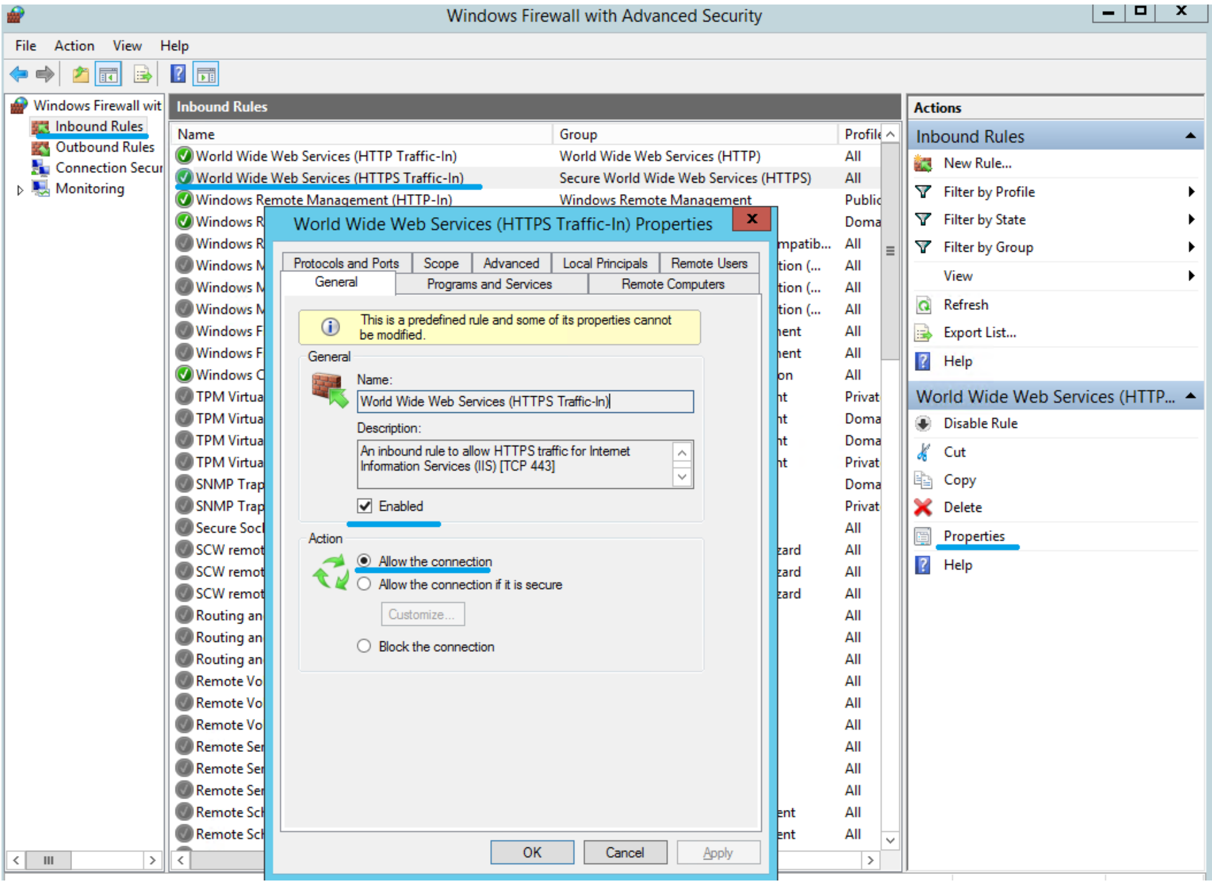
Specify logging settings for troubleshooting.

3. Select the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is set to **On**. And both the **Inbound connections** and **Outbound connections** are set to **Block**. Apply and save the changes.

4. From the **Inbound Rules**, choose **World Wide Web Services (HTTP Traffic-In)**. And ensure that this rule is **Enabled** and the **Action** is set to **Block the connection**.

5. On **World Wide Web Services (HTTP Traffic-In) Properties**, change to the **Advanced** tab. Select the profiles **Domain**, **Private**, and **Public**, and save the changes of this rule.

6. From the **Inbound Rules**, choose **World Wide Web Services (HTTPS Traffic-In)**. Ensure that this rule is **Enabled** and the **Action** is set to **Allow the connection**.



This is a predefined rule and some of its properties cannot be modified.

General

Name: World Wide Web Services (HTTPS Traffic-In)

Description: An inbound rule to allow HTTPS traffic for Internet Information Services (IIS) [TCP 443]

☑ Enabled

Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

7. On **World Wide Web Services (HTTPS Traffic-In) Properties**, change to the **Scope** tab. Choose **These IP addresses**, and add all StoreFront server IP addresses into the list. For example, StoreFront A (192.168.1.50) and StoreFront B (192.158.1.51).

8. On **World Wide Web Services (HTTPS Traffic-In) Properties**, change to the **Advanced** tab. Select the profiles **Domain**, Private, and **Public**, and save the changes of this rule.

Migrate data from the Single Sign-on central store

July 5, 2018

The Single Sign-on central store is a centralized repository used by Single Sign-on to store and manage user and administrative data. User data includes user credentials, security question answers, and other user-focused data. Administrative data includes password policies, application definitions, security questions, and other wider-ranging data.

You cannot migrate all data from the Single Sign-on central store to the Self-Service Password Reset central store. This table illustrates the data that can and cannot migrate.

Cannot migrate	Can migrate
Password policies - Not Supported	People folders containing enrollment Data
Application templates - Not Supported	Questionnaires used by customers
Application definitions - Not Supported	
User configurations - Created on the Self-Service Password Reset console	
Application groups - Not Supported	
Single Sign-on Service data - Created on the Self-Service Password Reset console	

> **Important**
>
> - Self-Service Password Reset does not support Active Directory as a central store, only network shares.
> - Self-Service Password Reset supports data only from Single Sign-on 4.8 or 5.0.

To migrate data from the Single Sign-on central store

Before migrating your data, familiarize yourself with Self-Service Password Reset installation and configuration. For more information, see Install and Configure.

1. Create a new central store.
2. Install the Self-Service Password Reset service and console.
3. In the console, specify the new central store location.
4. Create a new user configuration and include the users who have Self-Service Password Reset on Single Sign-on.
5. Copy the Single Sign-on enrollment data and security questions to the new central store.

Note: Ensure that the data proxy account has full control permission of all the copied files.

You need only two folders/files.

Examples

Copy all user's enrollment data:

\\SSO-SERVER\citrixsync$\People

to

\\SSPR-SVC\citrixsync$\People

Use this command:
Robocopy \\SSO-SERVER\citrixsync$\People\ \\SSPR-SVC\citrixsync$\People /e /xd QBA /Log+:copylog.txt /tee

Copy the security questions that are used by customers:

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

to

\\SSPRSVCcitrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\

Use this command:
Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\ \\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e /Log+:copylog.txt /tee

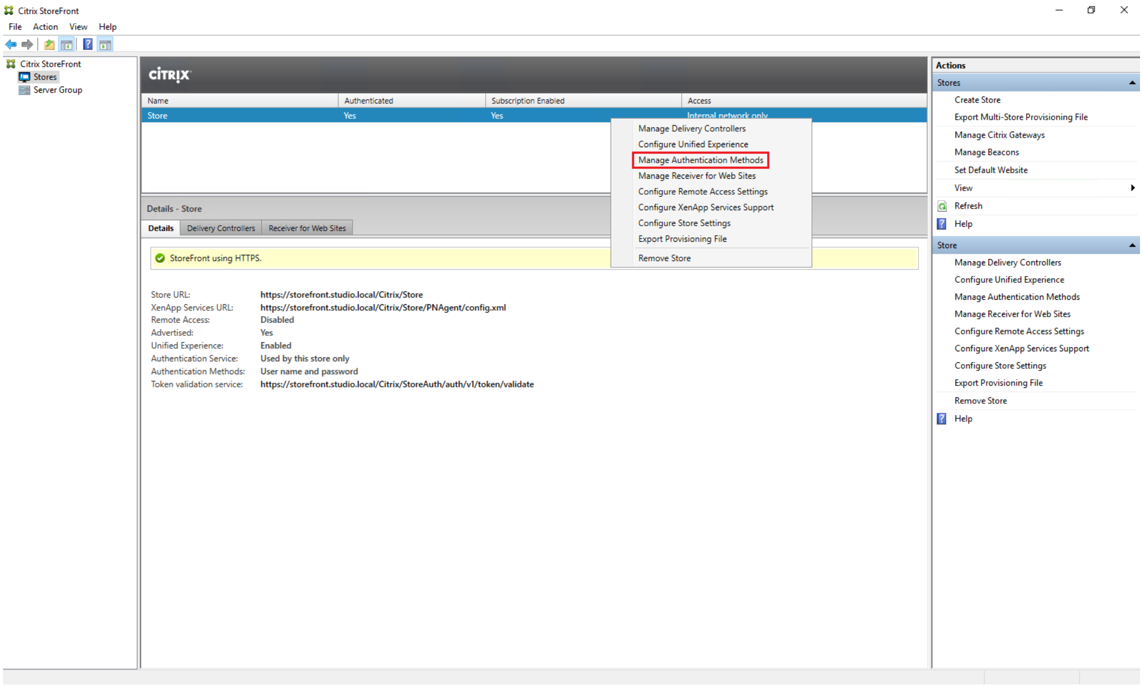
Now all users can unlock and reset using their Single Sign-on enrollment questions and answers.

Configure StoreFront to allow users to record answers to security questions

February 10, 2022

Configure StoreFront to allow users to enroll their answers to the security questions. When they're enrolled, they can reset domain passwords and unlock domain accounts. For more information, see the StoreFront documentation.

1. Configure StoreFront Internet Information Services (IIS) to HTTPS.
2. Create a deployment in StoreFront.
3. In the right pane of the StoreFront management console, right-click the store and choose **Manage Authentication Methods**.


Citrix StoreFront
File Action View Help
Citrix StoreFront
Stores
Server Group
CITRIX
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Methods
Manage Receiver for Web Sites
Configure Remote Access Settings
Configure XenApp Services Support
Configure Store Settings
Export Provisioning File
Remove Store
Actions
Stores
Create Store
Export Multi-Store Provisioning File
Manage Citrix Gateways
Manage Beacons
Set Default Website
View
Refresh
Help
Store
Manage Delivery Controllers
Configure Unified Experience
Manage Authentication Methods
Manage Receiver for Web Sites
Configure Remote Access Settings
Configure XenApp Services Support
Configure Store Settings
Export Provisioning File
Remove Store
Help

Name	Authenticated	Subscription Enabled	Access
Store	Yes	Yes	Internal network only

Details - Store

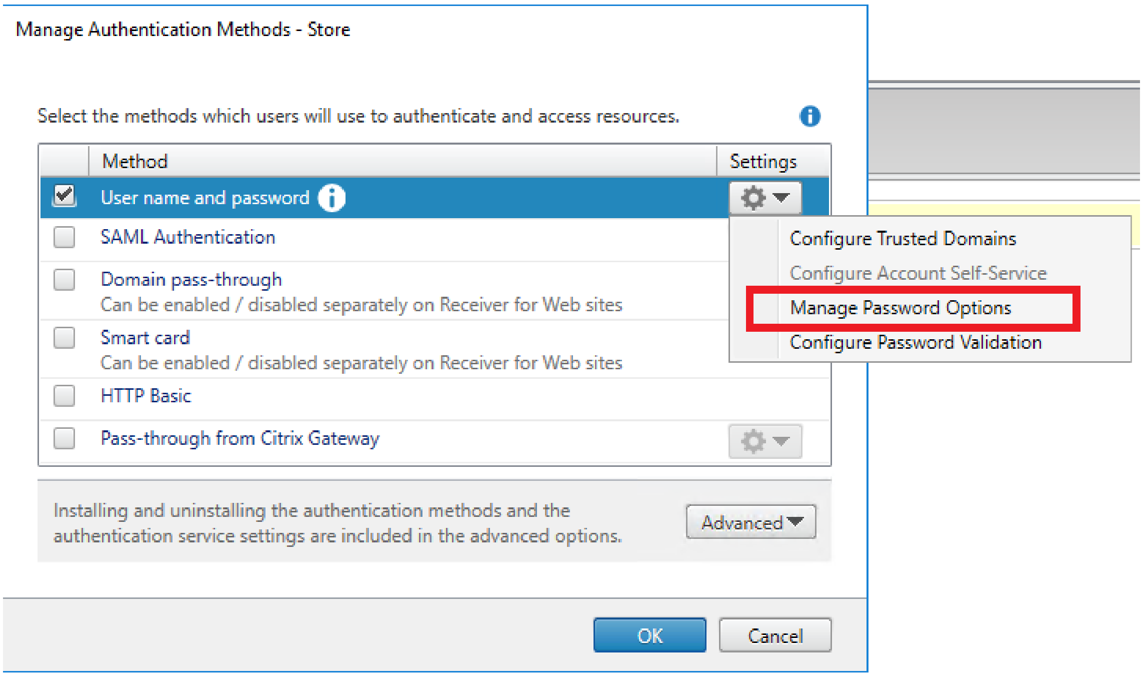
Details | Delivery Controllers | Receiver for Web Sites

StoreFront using HTTPS.

Store URL:	https://storefront.studio.local/Citrix/Store
XenApp Services URL:	https://storefront.studio.local/Citrix/Store/PNAgent/config.xml
Remote Access:	Disabled
Advertised:	Yes
Unified Experience:	Enabled
Authentication Service:	Used by this store only
Authentication Methods:	User name and password
Token validation service:	https://storefront.studio.local/Citrix/StoreAuth/auth/v1/token/validate

4. Choose **Manage Password Options** under settings of **User name and password**.

> **Note:**
>
> Self-Service Password Reset (SSPR) supports only the **User name and password** authentication method of StoreFront. It doesn't support other methods such as domain pass-through.


Configure Trusted Domains
Configure Account Self-Service
Manage Password Options
Configure Password Validation
Advanced
OK
Cancel

Manage Authentication Methods - Store

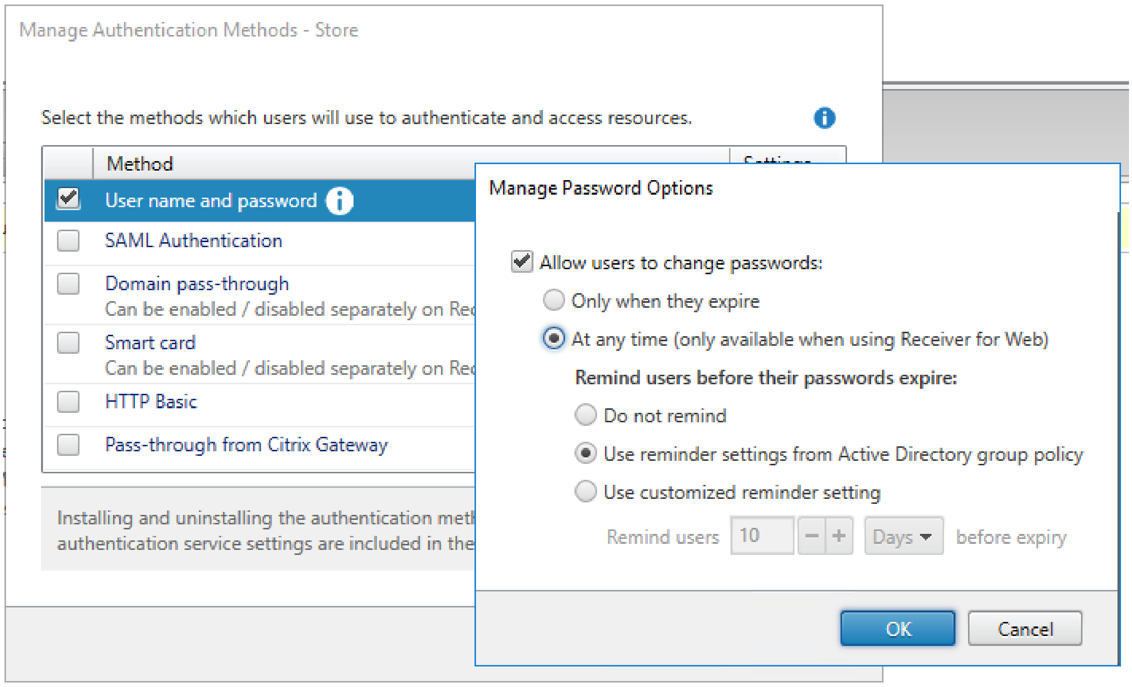
Select the methods which users will use to authenticate and access resources.

	Method	Settings
☑	User name and password	
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
□	Smart card Can be enabled / disabled separately on Receiver for Web sites	
□	HTTP Basic	
□	Pass-through from Citrix Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

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

5. Choose when you want users to change passwords and click **OK**.



Manage Authentication Methods - Store

Select the methods which users will use to authenticate and access resources.

	Method
☑	User name and password
□	SAML Authentication
□	Domain pass-through Can be enabled / disabled separately on Rec
□	Smart card Can be enabled / disabled separately on Rec
□	HTTP Basic
□	Pass-through from Citrix Gateway

Installing and uninstalling the authentication meth
authentication service settings are included in the

Manage Password Options

☑ Allow users to change passwords:

○ Only when they expire

● At any time (only available when using Receiver for Web)

Remind users before their passwords expire:

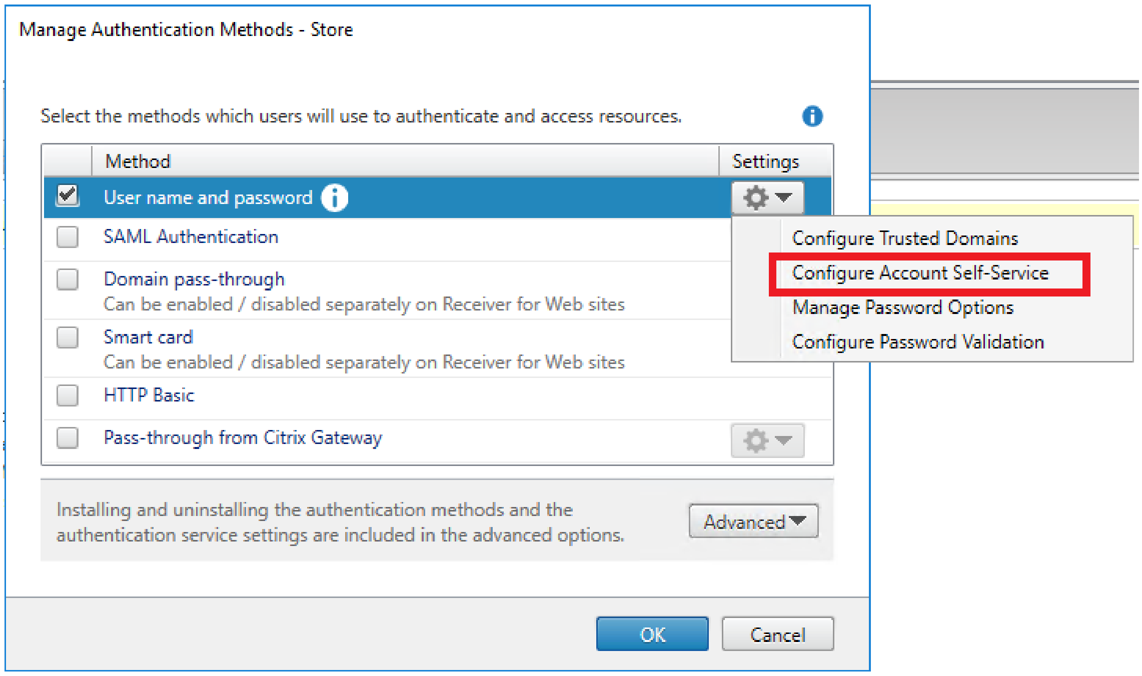
○ Do not remind

● Use reminder settings from Active Directory group policy

○ Use customized reminder setting

Remind users 10 Days before expiry

6. Choose **Configure Account Self-Service** under settings of **User name and password**.



Manage Authentication Methods - Store

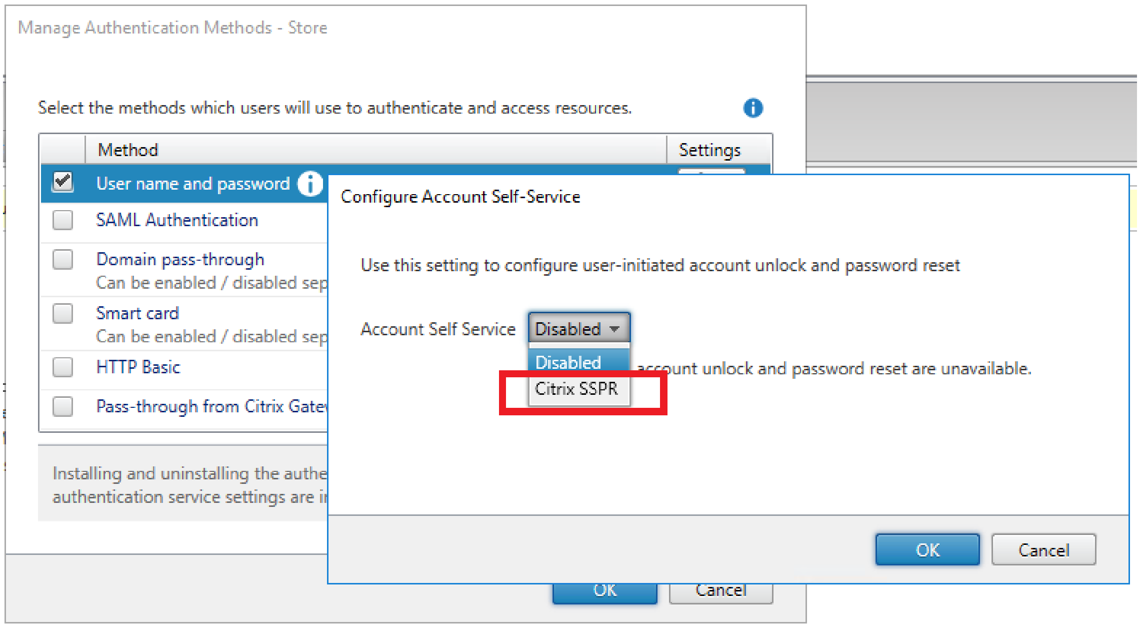
Select the methods which users will use to authenticate and access resources.

	Method	Settings
☑	User name and password	⚙
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
□	Smart card Can be enabled / disabled separately on Receiver for Web sites	
□	HTTP Basic	
□	Pass-through from Citrix Gateway	⚙

Configure Trusted Domains
Configure Account Self-Service
Manage Password Options
Configure Password Validation

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

7. Choose **Citrix SSPR** to enable **Account Self-Service**.



Manage Authentication Methods - Store

Select the methods which users will use to authenticate and access resources.

	Method	Settings
☑	User name and password	
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled sep	
□	Smart card Can be enabled / disabled sep	
□	HTTP Basic	
□	Pass-through from Citrix Gate	

Installing and uninstalling the authe
authentication service settings are i

OK Cancel

Configure Account Self-Service

Use this setting to configure user-initiated account unlock and password reset

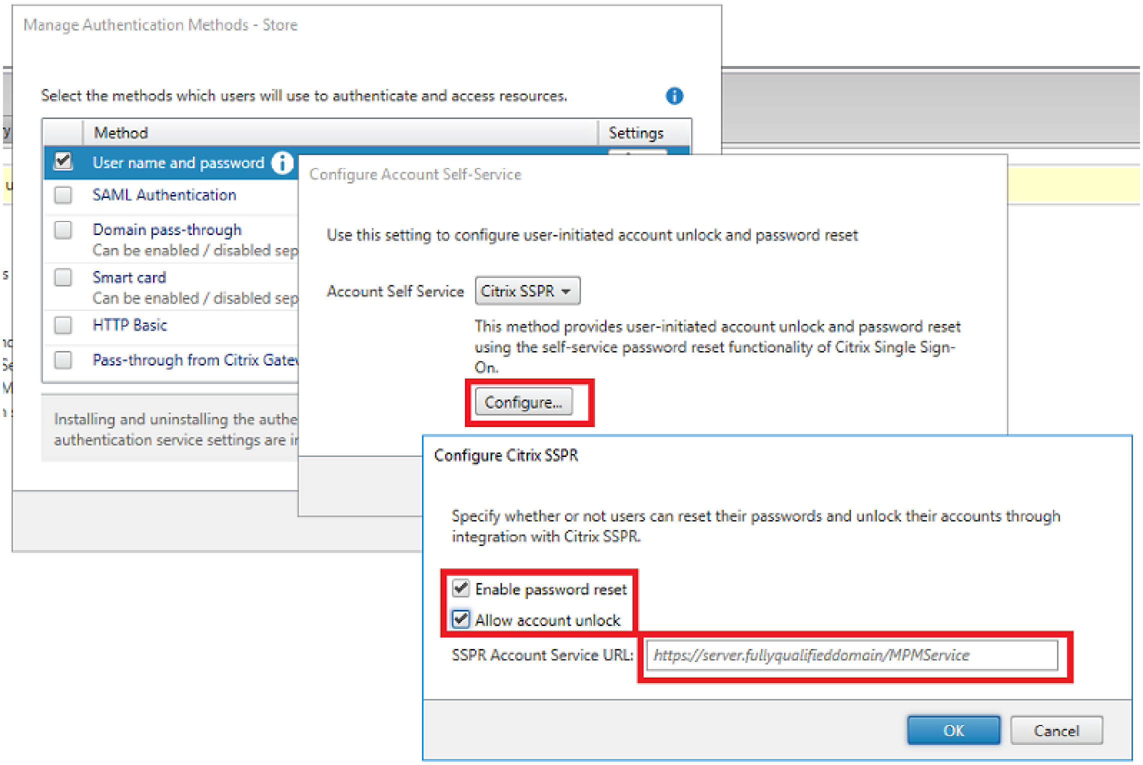
Account Self Service: Disabled ▾

Disabled
Citrix SSPR

account unlock and password reset are unavailable.

OK Cancel

8. Click **Configure**, choose **Enable password reset** and **Allow account unlock**, and configure the **SSPR Account Service URL** (https://< FQDN of the SSPR server>/MPMService).



Manage Authentication Methods - Store

Select the methods which users will use to authenticate and access resources.

	Method	Settings
☑	User name and password	
□	SAML Authentication	
□	Domain pass-through Can be enabled / disabled sep	
□	Smart card Can be enabled / disabled sep	
□	HTTP Basic	
□	Pass-through from Citrix Gate	

Installing and uninstalling the authe
authentication service settings are i

Configure Account Self-Service

Use this setting to configure user-initiated account unlock and password reset

Account Self Service: Citrix SSPR ▾

This method provides user-initiated account unlock and password reset using the self-service password reset functionality of Citrix Single Sign-On.

Configure...

Configure Citrix SSPR

Specify whether or not users can reset their passwords and unlock their accounts through integration with Citrix SSPR.

☑ Enable password reset
☑ Allow account unlock

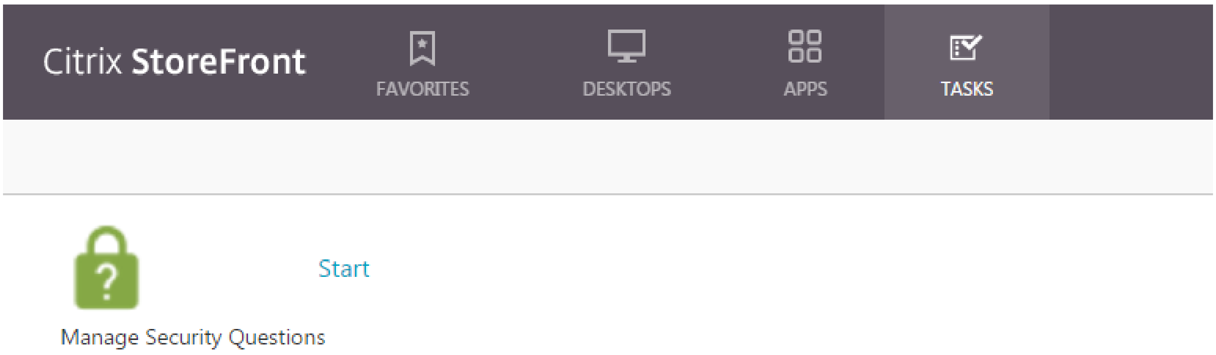
SSPR Account Service URL: https://server.fullyqualifieddomain/MPMService

OK Cancel

9. Click **OK** to apply all the settings.

> **Note:**
>
> Configure the site to use a unified experience.

The next time the user logs on to Citrix Workspace app or Citrix Workspace app for Web, security enrollment is available. The user can click
Start to specify answers to the security questions for future password resetting or account unlocking.



© 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).