

Specops Password Sync 6.1

Product Documentation

Specops Software

Specops Software is an international software company offering IT management solutions based on the idea of improving and extending the functionality of Microsoft Active Directory and Group Policy to perform complex management tasks.

Our Windows integrated approach to IT management adds significant value to the business of thousands of customers all over the world by helping them achieve an extraordinary high degree of efficiency in their IT-environments.

The award winning Specops product line is consistently recognized as some of the most essential third party add-ons to Microsoft environments.

Contact information

Please contact us at one of our offices if you have any questions:

International HQ

Specops Software
Torsgatan 8
111 23 Stockholm
Sweden

Support: +46 8 465 012 50
Phone: +46 8 465 012 34
Fax: +46 8 465 012 35

North America

Specops Software Inc.
532 Front Street West
Toronto, Ontario, ON M5V 1B8
Canada

Support: +1-877-SPECOPS (773-2677)
Phone: +1-877-SPECOPS (773-2677)
Fax: +1-866-747-5327

United Kingdom

Specops Software Ltd.
4 Orchard Way
Stoke Gabriel, Totnes, Devon
TQ9 6PZ
United Kingdom

Phone: +44 845 017 7475

United States

Specops Software USA Inc.
600 Chestnut St. – Suite 772
Philadelphia
PA 19106
United States

Support: +1-877-SPECOPS (773-2677)
Phone: +1-877-SPECOPS (773-2677)
Fax: +1-866-747-5327

Copyright and Trademarks

Specops Password Sync™ is a trademark owned by Specops Software. All other trademarks used and mentioned in this document belong to their respective owners.

Disclaimer

The content of this document is provided “as is”. While Specops Software makes every effort to ensure the reliability and accuracy of our documentation there is no guarantee that the information in this document is applicable in all customer environments.



Contents

Overview	4
Usage scenarios	4
Implementation planning	5
System requirements.....	5
Licensing options	6
Architectural overview	6
Installation.....	9
The Setup Assistant.....	9
Post installation configuration.....	12
Using the Setup Wizard to create a basic configuration	13
Configuration and operation.....	16
The Specops Password Sync Admin Tool.....	16
Sync Scopes	16
Sync Servers	19
Sync Points	21
Policies.....	26
Settings.....	26
Specops Password Sync and Group Policy	27
Creating and editing Specops Password Sync policies.....	28
Sync Provider configuration reference	30
System Security.....	37
Registry Settings.....	43
Troubleshooting.....	45
Installation troubleshooting.....	45
Component troubleshooting	45
Configuration troubleshooting.....	46
Event logging.....	47
Debug logging.....	54
Support.....	55



Overview

Many IT systems within modern organizations still authenticate their users in their own user database rather than using Active Directory or another directory service.

This makes it hard for the users to remember all their passwords and reduces overall system security when the users try to find ways to improve their situation.

Specops Password Sync solves these issues by offering the ability to propagate password changes in Windows to other systems.

In combination with good password policies, like the ones you can create with Specops Password Policy, this enforces the use of strong passwords across all systems and forces the users to change their other passwords just as often as they change the Windows password.

In essence, Specops Password Sync enforces the same password security that you enjoy in Windows to all of your other business systems as well.

Usage scenarios

These are some of the most common scenarios where Specops Password Sync™ delivers value to current business problems.

Increased password security in all business systems

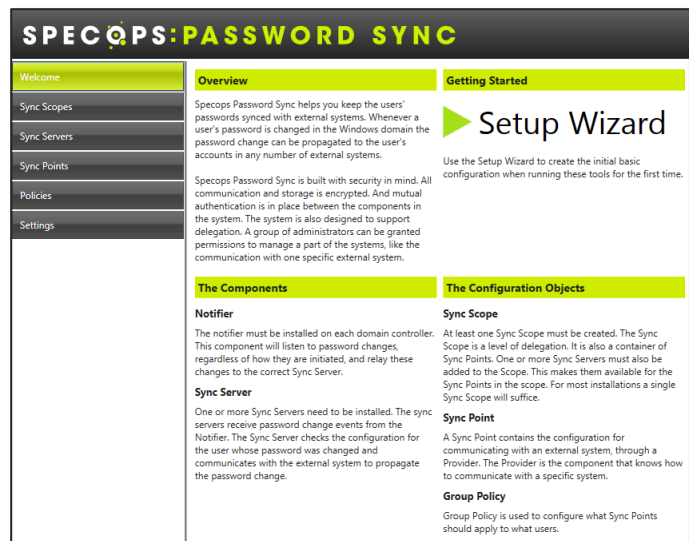
Many business systems, especially cloud services, do not require the same strict password security that you can achieve with products like Specops Password Policy. By enforcing the same set of password rules across all business systems you can reduce the likelihood of a password being cracked and ensure that all business systems follow your security policy.

Increased user productivity

Users who cannot access their business systems because they have forgotten their password are not productive until they have received a new password. Specops Password Sync minimizes the risk of users forgetting their password, as they only need to remember their Windows password.

Reduced support workload

By minimizing the risk of users forgetting the password the helpdesk personnel can spend less time resolving trivial issues to keep users productive and more time on developing the IT-infrastructure.



Specops Password Sync automatically synchronizes password changes in Active Directory to other systems.



Implementation planning

Implementing Specops Password Sync™ is very easy and straightforward. Before proceeding with the actual installation it is beneficial to spend a few moments considering the implications of how you wish to use the product in your environment.

System requirements

In order to use Specops Password Sync your organization must meet the following system requirements:

Password Sync Component	Supported OS configurations
Password Change Notifier	Windows Server 2003 SP4 or Windows Server 2003 R2 All editions of Windows Server 2008 / Server 2008 R2 All editions of Windows Server 2012 Writable domain controller
Sync Server	Windows Server 2003 SP4 or Windows Server 2003 R2 All editions of Windows Server 2008 / Server 2008 R2 All editions of Windows Server 2012 .Net Framework 4.0 installed.
Administration Tools	Any server OS supported by the Sync Server component. Windows XP SP3, Windows Vista, Windows 7 or Windows 8 client OS. OS must be a domain member. MMC 3.0 installed. .Net Framework 4.0 installed.

Specops Software always recommends running our software on the latest version of Windows.

Hardware requirements

There are no specific hardware requirements for Specops Password Sync. If your hardware is capable of running the supported operating systems, it is also capable of running Specops Password Sync.



Licensing options

There are four different licensing options for Specops Password Sync:

License type	Explanation
Trial	Unrestricted license usable for an unlimited amount of users until a fixed expiration date. The license is only valid for trial purposes.
Affected	The affected license has no expiration date but is limited to the number of user licenses that have been purchased. When the number of used licenses is counted the system counts the actual number of non-disabled user objects that are affected by GPOs containing Specops Password Sync settings.
All	The all license has no expiration date but is limited to the number of licenses that have been purchased. When the number of used licenses is counted the system counts the total number of non-disabled user objects under the configured scopes of management for Specops Password Sync in the domain.
Subscription	The license has no expiration date and no limit on the number of users the product can be used with. At the end of each month the system reports the number of used licenses and the customer is invoiced a subscription fee for that many users. The counting mechanism is the same as used in the Affected licensing mode.

Architectural overview

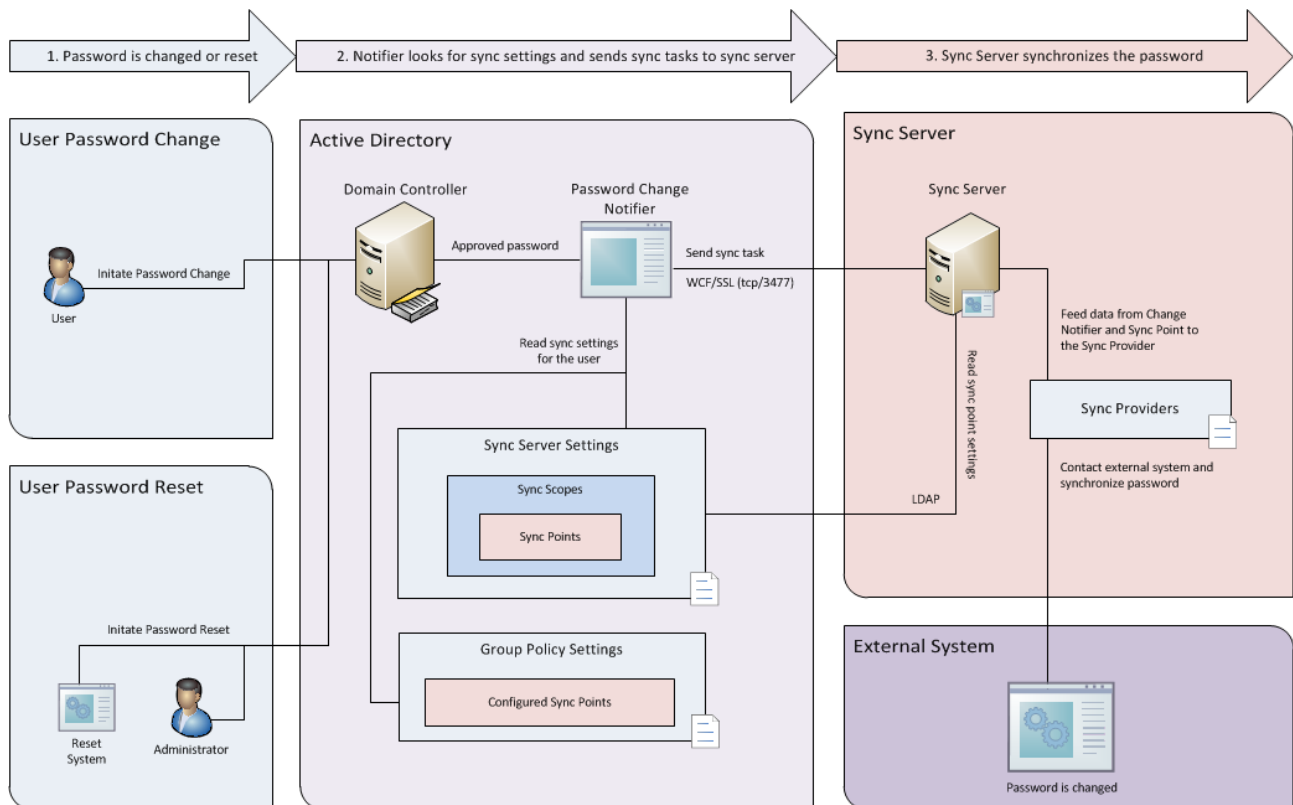
Specops Password Sync consists of these basic components:

Component	Purpose
Password Change Notifier	Reads all password changes performed by the domain controller where the component is installed and sends password synchronization jobs to the Sync Server component.
Sync Server	Receives password synchronization jobs and performs them in accordance with the settings configured in the system.
Administration Tools	Configures system settings like Sync Scopes, Sync Servers and Sync Points. Also used to create Group Policy settings for end users targeting them for password synchronization through specific Sync Points.

Depending on the requirements of your organization there are a few architectural issues to consider before installing the product in your environment.



Schematic overview



This schematic overview shows the flow of information through the various components involved in completing a password synchronization operation with Specops Password Sync.

Availability and the number of necessary servers

In a minimal installation it is possible to install all the system components on the same machine, which would then have to be a domain controller. However, as it is not best practice to install any unnecessary components on a domain controller the general recommendation is to use a separate server for the Sync Server and Administration Tools components.

In High Availability environments it is recommended to install several Sync Servers components and configure all Sync Providers to use both primary and secondary Sync Servers. The Password Change Notifier components must be installed on all domain controllers and are thus automatically always available as long as there still are accessible domain controllers.

A typical Specops Password Sync installation consists of one internal server running both the Sync Server and Administration Tools components and all domain controllers running the Password Change Notifier component.

Sync Scopes

Sync Scopes are used to create a basic administration unit for password synchronization. The scope is tied to a level in your Active Directory structure and enables the use of Specops Password Sync on the user objects beneath the selected level.



Most organizations only need a single Sync Scope to cover all users. However, in larger environments where user administration takes place from more than one place it might be useful to create several Sync Scopes and delegate administration over them to different groups of administrators.

Sync Scopes can also be used to enable the product for use in different branches of the Active Directory structure, even if the same group of administrators is responsible for managing the users in each branch.

You should plan for as many Sync Scopes as is necessary to cover all the user objects you wish to use the system with.

Sync Servers

The Sync Server is the component that performs the actual synchronization to the connected systems. Depending on the amount of users in your environment and the frequency with which they change their passwords you may require more than a single Sync Server.

There are also network related considerations when deciding the appropriate number of Sync Servers. For instance, synchronization to certain systems might not be allowed from all network locations. In these cases it might be best to configure a separate Sync Server to handle this specific synchronization workload.

In a global organization with unreliable site connections it might also be wise to set up additional Sync Servers to ensure that the domain controllers can access them to submit synchronization jobs.

Sync Points

The Sync Points control the settings that are used when a password is synchronized with another system.

You will require at least one Sync Point per system you wish to synchronize passwords with. It is also possible to configure several Sync Points to synchronize with the same external system if your organization requires different synchronization settings to be used for different types of users.

The Sync Point also specify which Sync Server(s) to use for the synchronization, making it possible to create separate Sync Points with different server settings for different parts of your organization.

Sync Providers

Each Sync Point requires a Sync Provider to be able to connect to the external system. The Sync Provider contains the logic necessary to perform the password change operation in the external system and must be configured with the information required by the remote system to complete the

Specops Password Sync is shipped with a number of providers for the most common systems, but the development framework for creating Sync Providers is open and it is quite possible to develop your own Sync Providers for the systems used by your organization.

The API reference for creating new Specops Password Sync Providers is available in a separate document.



Installation

The “Installation” document area takes the reader through the process of installing the product.

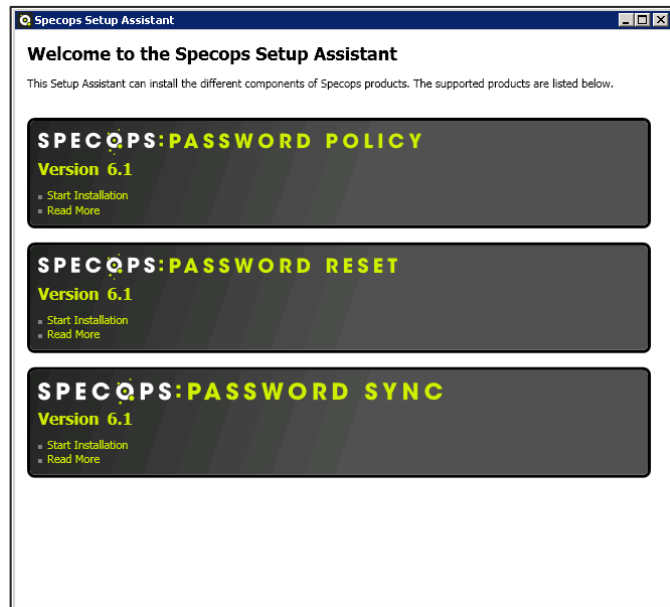
The Setup Assistant

The Specops Setup Assistant (SA) is designed as a step by step installation guide to help you install the various product components.

The SA also contains automation logic to verify that all prerequisite components have been installed and that the account running the SA has the appropriate permissions to complete the installation.

Every section of the SA is divided in individual steps which should be completed during the installation.

The Setup Assistant for Specops Password Sync also contains the other products in the Specops Password family – Specops Password Policy and Specops Password Reset. If you only intend to install Specops Password Sync the installation steps of the other two products can be safely ignored.



The Setup Assistant contains installations for all the Specops Password products.

Specops Password Sync installation

The installation procedure for Specops Password Sync consists of three simple steps.

Section 1 – Password Change Notifier

The Specops Password Sync Change Notifier component is triggered by any password change and must be installed on all domain controllers in your Active Directory.

While this installation step can be performed on your domain controllers through the Setup Assistant it is recommended that you deploy the Password Change Notifier through Group Policy Software Installation (GPSI), as this will ensure that any new domain controllers also get the Notifier installed automatically.

Manual installation

Simply start the Setup Assistant on each of your domain controllers and complete the Password Change Notifier installation step. You can also extract and run the Password Change Notifier msi-package on your domain controllers.



Deploying the Password Change Notifier through GPSI

Use the following procedure to create a GPSI deployment of the Password Change Notifier:

1. Copy the MSI-packages for the Password Change Notifier to a file share in your network infrastructure. Specops always recommends using DFS shares for this purpose.

The installation packages can be found where you extracted the setup files.
(The default location is “C:\temp\SpecopsPassword_Setup\[VersionNumber]\”).

2. Create a new GPO in your domain and link it to the Domain Controllers OU.
3. Expand the Computer Configuration\Policies\Software Settings node and select the “Software installation” node.
4. Add the SpecopsPasswordChangeNotification-x86.msi package.
 - a. Select the “Advanced” deployment method.
 - b. Make sure the “Assigned” deployment option is selected.
 - c. Go to the Deployment tab, click the “Advanced” button at the bottom of the screen and deselect the “Make this 32-bit X86 application available to Win64 machines.” option. This prevents 64-bit DCs from installing the 32-bit version of the notifier.
 - d. Save the changes and close the package.
5. Add the SpecopsPasswordChangeNotification-x64.msi package.
 - a. Select the “Assigned” deployment method.
 - b. Save the package with no further changes.
6. Close the GPO.

All domain controllers will now install the correct x86/x64 packages on their next restart.

Note

The correct x86/x64-bit version of the msi-package can also be installed manually on all domain controllers.

New domain controllers also need to have the notifier installed manually when using this method.

Warning!

*The domain controllers **must** be restarted before they can load the Password Change Notifier.*

This might require double restarts if the notifier is installed through the Group Policy Software Installation feature.

Section 2 – Sync Server installation

The Sync Server component is responsible for performing the actual synchronization of the new password to all connected systems which the user account has been configured to synchronize to through the Specops Password Sync Group Policy settings.

The Sync Server component requires .Net Framework 4.0 to be installed on the server.

Select Certificate

The certificate selected in this step verifies the identity of the Sync Server to the Password Change Notifier component. All communication between the Password Change Notifier component and the Sync Server is also SSL encrypted using the same certificate.



While it is possible to create and use a self-signed certificate in this step it is important to remember that all domain controllers who are going to communicate with the Sync Server are required to trust the selected certificate.

For this reason it is recommended to use a certificate generated by the Active Directory Certificate Services rather than a self-signed certificate in production environments. In smaller environments it is also possible to import the selected certificate on all domain controllers. This can be easily achieved through Group Policy.

Specops Password Sync Server Installation

When the certificate has been selected the installation is started by pressing the “Install” button. The Setup Assistant will automatically use the correct msi-package for the local system and install the appropriate version of the Sync Server component.

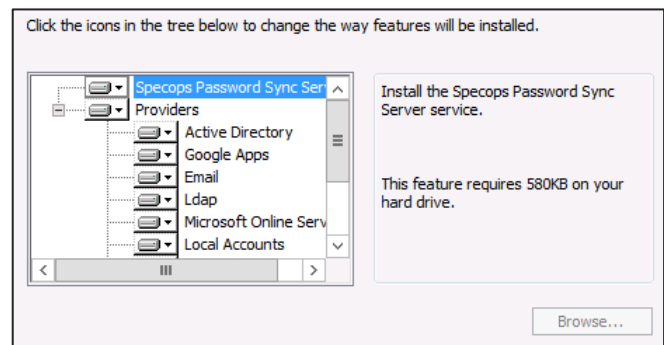
When the service is started during the installation it will add a service connection point beneath the computer object of the server in Active Directory and populate it with information about how to connect to the Sync Server.

Selecting Sync Providers

During the installation of the Sync Server you will be given the chance to select which Sync Providers you want to install on the Sync Server.

The default setting is to install all the providers that are shipped with the product, but if you wish to minimize the amount of space required you can remove the providers you do not wish to use.

It is very easy to add or remove Sync Providers from the Sync Server at a later time.



It is possible to select which providers will be installed during the installation of the Sync Server.

Section 3 – Administration tools installation

The Administration tools installation will install the Specops Password Sync Administration tool and the GPMC snap-in needed to configure Specops Password Sync Policies.

The tools should be installed on any computer where you wish to administrate the product. For instance, it is necessary to have the admin tools installed in order to see the Specops Password Sync group policy settings.

The administration tool requires the .Net Framework 4.0 to be installed on the local machine.

Specops Password Sync Admin Tools installation

Clicking the “Install” button in this step will install the administration tools.



Post installation configuration

When the all the components have been installed and started it is time to start looking at the basic configuration of the system.

The best place to start is the Specops Password Sync Admin tool, where you can use the Getting Started Wizard to configure the necessary basic settings.

Post installation configuration task list

The following steps must be completed before the system is fully ready for use in your organization:

- Add your license key in the Specops Password Sync Admin tool.
- Verify that the Password Change Notifier component has been installed on all of your domain controllers, and that the domain controllers have been restarted after the installation.
- Verify that the certificate(s) used on your Sync Server(s) are trusted by the domain controllers.
- Create at least one Sync Scope in the Admin tool.
- Add at least one Sync Server to each Sync Scope.
- Create at least one Sync Point.
- Create and link at least one Group Policy Object with your desired Specops Password Sync settings in your Active Directory.
- Make the appropriate accounts members of the Specops Password Sync local security groups.

Adding members to the Specops Password Sync local security groups

Permissions to use the Specops Password Sync Admin Tool and the permission to send jobs to a Sync Server are controlled through Local Security Groups where these components have been installed.

Members of the local Administrators group are always allowed to access the administration tools and do not have to be added to the security groups separately.

The permissions are handled through the following groups:

Local Security Group	Description
Specops Password Change Notifiers	Members of this group are allowed to send password synchronization jobs to the Sync Server running on the local server. This group should always contain the “Domain Controllers” domain security group, as all domain controllers in your domain can be expected to send sync jobs.
Specops Password Sync Admins	Members of this group are allowed to administrate the system through the Specops Password Sync Admin tool. This group can be found on machines where the admin tool has been installed and can be used to grant or deny access to specific groups or users.



Using the Setup Wizard to create a basic configuration

The Setup Wizard is accessible from the Welcome page in the Specops Password Sync Admin Tool. Completing the steps in the Wizard allows you to quickly create and configure the basic settings needed to start synchronizing passwords.

Creating the first Sync Scope

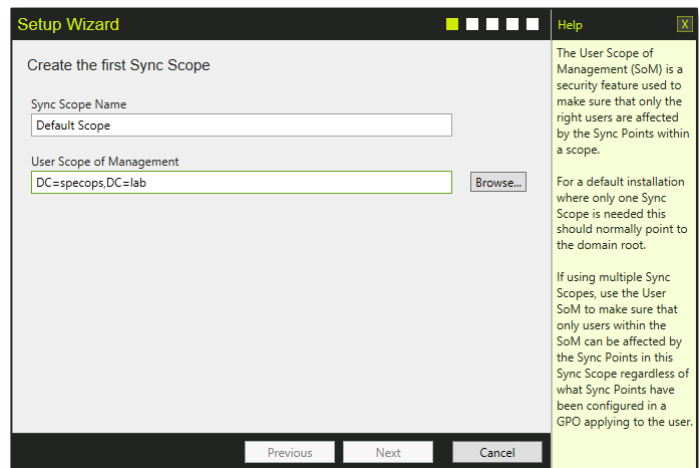
Sync scopes are used to assign a basic administrative level from which users can be configured to use the synchronization settings within the Sync Scope.

Administrative security can also be assigned to Sync Scopes to let different groups of administrators within the organization handle different Sync Scopes.

The name of the Sync Scope should be something descriptive for the purpose of the scope. However, if your organization only needs a single Sync Scope the name become less important and it might be easier to use the default name.

When using the Setup Wizard to create a Sync Scope the system defaults to assigning the domain root as the Scope of Management. This should be changed if you require a narrower selection of users which you would like to be able to use the system.

Please note that users will not start synchronizing their passwords simply because their accounts are located beneath the Scope of Management. Specific group policy settings are needed for each Sync Point before any synchronization will occur.



The Sync Scope is used to control which users that can be affected by the Sync Points within the scope.

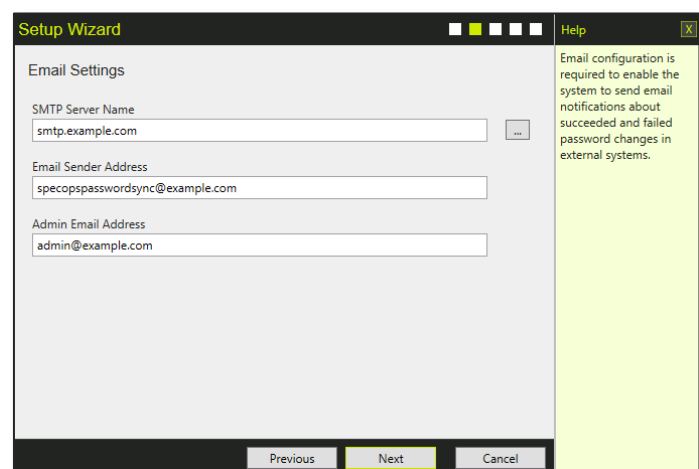
Configuring the system email settings

The email configuration assigns the default settings used by the system to send email.

Specify your smtp-server and the address from which the system should send email.

You should also specify an administrative email address where you wish to receive mail from the system regarding system events like license information.

The email settings are system wide, but it is possible to override them in each individual Sync Scope.



The email settings are system wide, but can be overridden by settings in each Sync Scope.

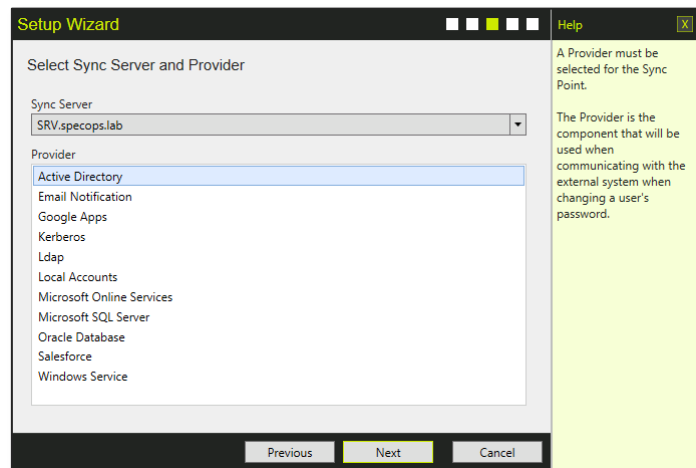


Creating a Sync Point with a Sync Server and a Sync Provider

The next page enables you to create your first Sync Point.

The Sync Server to use with the Sync Point is the first configurable item. In a completely new system there is normally just a single Sync Server to choose from.

Second, select the Sync Provider you wish to use with your new Sync Point. The provider specifies what sort of system you wish to synchronize passwords to, and will contain the necessary settings to do so.



Specify the Sync Server and Sync Provider you want to use with your new Sync Point.

Configuring the provider with synchronization settings

When you have selected your provider you need to configure it with the necessary settings to connect to the remote system and perform the password synchronization.

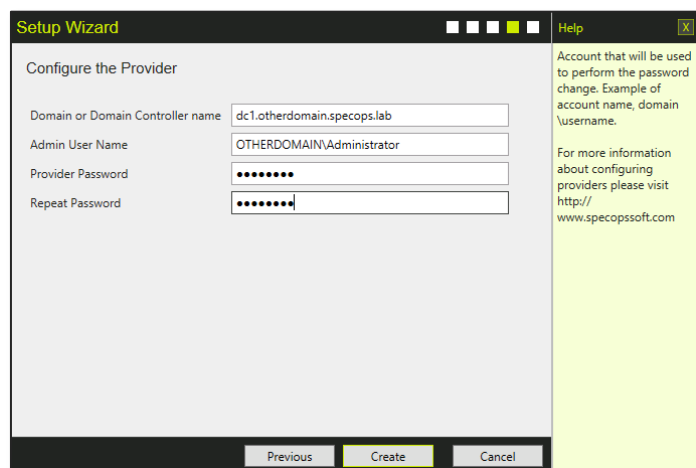
The configurable settings vary between each Sync Provider.

In the last page of the Setup Wizard, we selected to use the Active Directory provider to synchronize passwords to another Active Directory domain.

This provider only requires three pieces of information:

- The domain controller to connect to.
- An admin account in the remote domain.
- The password for the admin account.

With these settings properly configured we can finally move on to the last page of the wizard.



The Active Directory provider requires three basic pieces of information in order to be able to synchronize passwords.

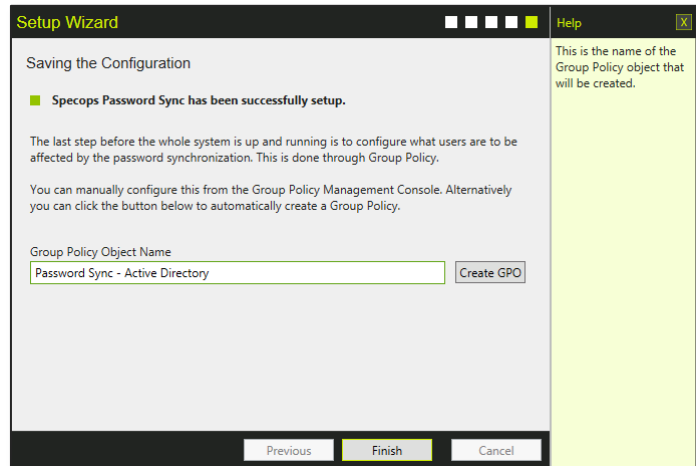


Creating a GPO with Specops Password Sync settings

Users will not get their passwords synchronized until they are affected by a Specops Password Sync GPO configured to use the newly created Sync Point.

The last page of the wizard allows you to automatically create this GPO in your domain, but it is also possible to create it manually from the Group Policy Management Console.

When automatically creating the GPO it will be linked to the same level in Active Directory as the Scope of Management level you selected for your Sync Scope in the first page of the Setup Wizard.



The "Create GPO" button can be used to automatically create a new GPO where the Sync Point is enabled.

Further configuration

The Sync Scope and Sync Point created through the Setup Wizard can be configured in further detail from the Specops Password Sync Admin Tool.

For instance, in most environments it is likely that the Sync Point should be configured to perform some sort of mapping between the account names in the local domain and the account names in the remote system.



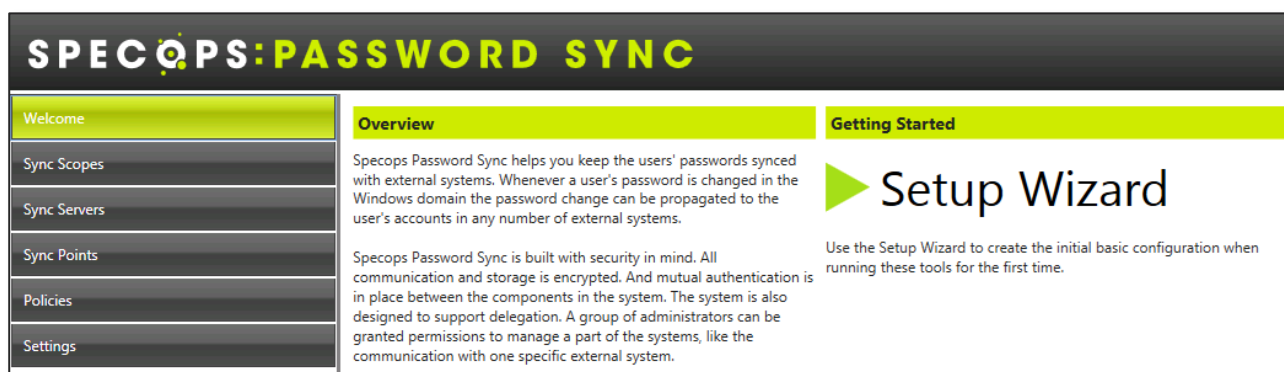
Configuration and operation

Specops Password Sync is easily configured from any computer in the domain where the Specops Password Sync Admin Tool is installed.

The Specops Password Sync Admin Tool

The Admin tool is used to administrate the basic components of the system.

When the tool is started for the first time in a new environment you will be asked to import your Specops Password Sync license. After completing this step, you will be able to proceed to configure the various settings controlled through the tool.



The Specops Password Sync Admin tool is used to administrate the components used by the system.

The Setup Wizard, which can be accessed from the Welcome page, can be used to quickly create a basic configuration with all the necessary components to start synchronizing passwords.

Sync Scopes

Sync Scopes are the main unit of administration in Specops Password Sync. Each Sync Scope is required to have at least one Scope of Management, which represents the level(s) in the Active Directory hierarchy the Sync Scope is valid for. The selected level(s) and all objects below are considered part of the Scope of Management.

Only user accounts located within the selected Scope of Management can use the Sync Points configured in the Sync Scope.

Sync Scopes can also be used to control administrative access in the product. By assigning specific security groups as “Delegated Security Groups” for the Sync Scope it is possible to restrict which users are able to edit the settings in the Sync Scope.

Users will not be able to select Sync Scopes to which they do not have administrative access in the Specops Password Sync Admin tool.

The Admin tool always works with a “Current Sync Scope” which can be selected by clicking the name of the desired Sync Scope and using the “Set Current” action on the Sync Scopes page in the Admin tool.



Creating and Editing Sync Scopes

New Sync Scopes can be easily created by using the “Add New” action from the Sync Scopes page in the Admin tool.

The minimum requirement to create a new Sync Scope is to enter a name for the scope and add at least one Scope of Management.

When creating Sync Scopes it is important to plan for the intended use of the scope.

Most organizations will be fine with a single Sync Scope covering the entire domain. However, if you need to delegate administrative access in one part of your Active Directory to a specific group of administrators it might be a good idea to create a separate Sync Scope for them and let them handle all of their settings within that scope.

Access to administrate the Sync Scope is controlled through the “Delegated Security Groups” settings, where security groups from your domain can be granted permissions to administrate the Sync Scope.

Built-in security groups, like “Domain Administrators” automatically have permissions to edit all Sync Scopes.

Multiple scopes of management

In some cases it might be necessary to assign multiple scopes of management to a single Sync Scope. This is typically useful when the Active Directory contains users on many different branches and you do not want the Sync Scope to affect all branches.

Email configuration

Each Sync Scope may have a separate email configuration from the global settings handled centrally by the system. Simply check the “Override Global Email Settings” checkbox and enter the appropriate email settings for the Sync Scope.

This functionality can be used to let different parts of your Active Directory use their closest email servers to handle communications.

The screenshot shows a configuration window for a Sync Scope. It has a title bar with 'Security Settings' and a 'Help' button. The 'Security Settings' section contains: 'Sync Scope Name' (Specops Lab), 'User Scope of Management' (OU=Lab,DC=specops,DC=lab), and 'Delegated Security Groups'. The 'Email Configuration' section contains: 'Override Global Email Settings' (unchecked), 'SMTP Server Name', 'Port Number' (25), 'Use Transport Layer Security (TLS)' (unchecked), 'Use custom SMTP credentials' (unchecked), 'SmtP User Name', 'SMTP Password', and 'Email address to send emails from'. A 'Help' panel on the right explains that the list contains security groups with delegated permissions and notes that inherited permissions are not displayed. At the bottom are 'OK' and 'Cancel' buttons.

Sync Scopes can be customized in many ways to fit the needs of your organization.



Sync Scope configuration reference

Setting	Description
Sync Scope Name	<p>The name of the Sync Scope.</p> <p>This is the name that will be displayed in the admin tools and the name of the actual object that is created in Active Directory representing the Sync Scope.</p> <p>The Sync Scope Name must be unique.</p>
User Scope of Management	<p>An Active Directory hierarchy level for which the Sync Scope will be used.</p> <p>Only user objects located beneath a User Scope of Management can have their passwords synchronized through Sync Points in this Sync Scope.</p>
Delegated Security Groups	<p>This list contains security groups that have been granted delegated permissions to configure Sync Points within this scope. Members of these groups can add, remove and edit the Sync Points.</p> <p>Note that permissions that are inherited in Active Directory are not displayed here. For example members of the Domain Admins group will not be listed since they do not need to be explicitly granted the delegated permissions.</p>
Override Global Email Settings	<p>Check this box to use custom SMTP settings for this Sync Scope.</p> <p>If the box is left unchecked the global SMTP configuration from the Settings page will be used for this scope.</p>
Smtp server name	<p>Enter the name of a mail server computer that can be used to handle the SMTP requests from the system.</p>
Port number	<p>The port to connect to on the SMTP server.</p> <p>This can be left blank to use the standard smtp-port (25).</p>
Use custom SMTP credentials	<p>Check this box to use custom SMTP credentials for the configured SMTP server</p>
Smtp user name	<p>User name for the custom SMTP credentials</p>
Smtp password	<p>Password for the custom SMTP credentials</p>
Email address to send emails from	<p>Enter an email address here. This will be the sender for all the emails that the system may send through this Sync Scope.</p>



Sync Servers

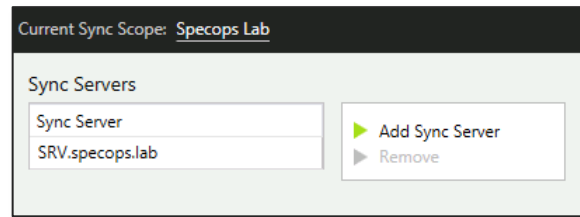
The Sync Servers page shows the Sync Servers that are configured to for use with the current Sync Scope.

It is recommended to configure at least two Sync Servers for each Sync Scope, to ensure that all Sync Points are able to use both a primary and secondary Sync Server for the synchronization jobs.

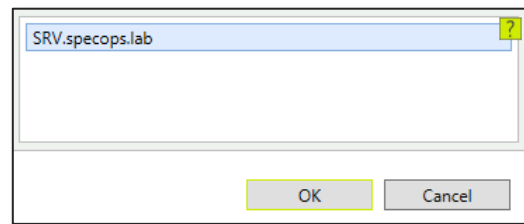
Servers can be added to the Scope by using the “Add Sync Server” action, while the “Remove” action removes a selected server from the Scope.

When adding servers to the scope you will be presented with a list of all currently available Sync Servers in your Active Directory. Simply select the servers you wish to add and press the “ok” button to add them to your Sync Scope.

A single Sync Server can be part of several different Sync Scopes.



Sync Server overview for the “Specops Lab” Sync Scope.



Select the Sync Servers you wish to add from the list to add them to your Scope.

Sync Server requirements

The system requires at least one Sync Server to be installed, but it is strongly recommended to install at least two in order to secure the system availability.

When the Password Notifier Service picks up a sync job it will always attempt to contact the primary server configured on the Sync Point first.

If the primary Sync Server is not responding when a sync job is attempted the secondary server will be contacted. If the secondary server is also unavailable the sync job will remain in the sync queue where it will be reprocessed until the Notifier Service reports that it was able to successfully transmit the job to one of the Sync Servers.

If possible, maintenance on Sync Servers should not be performed simultaneously.

If a Sync Server is taken out of service permanently it should first be removed from the Sync Points and Sync Scopes where it is used to make sure that no part of the system will not try to access it.

Warning!

A Sync job is created by the Password Notifier every time a password is changed on the domain controller where the notifier is running. The jobs typically require less than 1KB of storage space in the job queue and will normally be transferred to a Sync Server as soon as they have been created.

However, as there is no maximum limit on the total size of the job queues, leaving both Sync Servers in a Sync Point in an offline state for extended periods could potentially require a lot of disk space on the system partition of your domain controllers. If this is a serious concern you may want to consider changing the queue location to another partition. The queue path is controlled through the registry.



Specialized Sync Servers

When installing the Sync Server component the administrator is given the option to choose which Sync Providers to install. This makes it possible to create Sync Servers with specialized synchronization jobs. For instance, if a remote system only accepts incoming traffic from specific IP-addresses you can configure and use a Sync Server specifically for that system.

This is a common scenario in high security network environments with firewalls protecting each network segment.

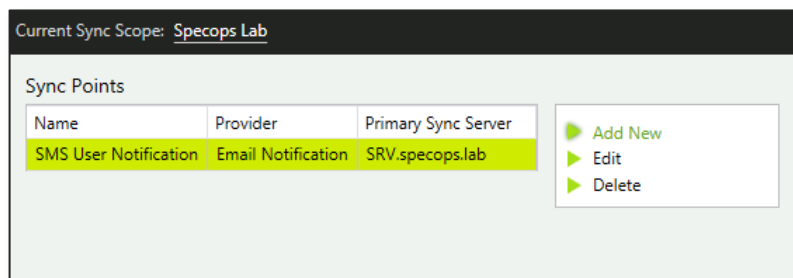


Sync Points

Sync Points contain all the necessary settings to perform a password synchronization job to another system.

Every created Sync Point exists as part of a Sync Scope and can only be used to synchronize passwords to users that are part of the Sync Scope.

Sync Points can be added, edited or deleted from the Sync Point page in the Specops Password Sync Admin tool.



The Sync Point page shows the currently configured Sync Points in the current Sync Scope.

Adding and editing Sync Points

Sync Points require a few basic pieces of information in order to perform their tasks.

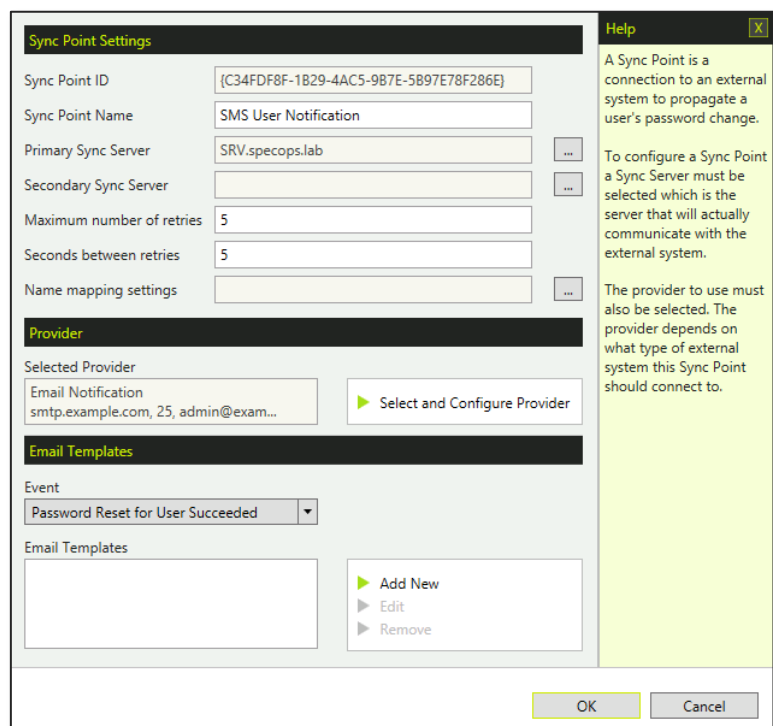
When creating a new Sync Point you need to specify the name of the Sync Point, which Sync Server(s) it is going to use and how it should behave if the synchronization job fails.

You also have to select and configure a Sync Provider from the list of available providers on the Sync Server you have selected to use.

If the remote system does not use the same format as your Active Directory for the user account names you should also configure Name mapping settings for the Sync Point.

At the bottom of the Sync Point configuration you can also find the Email Templates section, which is used to set up informational emails that can be sent to the users to inform them if the synchronization operation succeeded or failed.

Once the configuration has been completed the Sync Point will be ready for use with the users within the Sync Scope as soon as you have enabled the Sync Point in a GPO affecting them.



The Sync Point edit page displays the current configuration of the Sync Point.



Primary and Secondary Sync Servers

The primary and secondary Sync Server selection allows you to decide which servers the Sync Point should use for the synchronization. It is only necessary to specify a primary server, but it is strongly recommended that you specify a secondary server as well for redundancy purposes.

By alternating which server is primary and which server is secondary between different Sync Points it is also possible to achieve a rudimentary load balancing function in the system.

Retries

When a Sync Server receives a new job it will immediately attempt to contact the remote system according to the settings in the sync provider. If this is unsuccessful the server moves the job to a retry queue from which the job will be attempted again at a later point.

The retry settings on the Sync Point control how many retry attempts the Sync Server should make, and the amount of time to wait between each attempt.

Unless you are aware of any specific conditions in your environment that might make connectivity to your remote system unstable it is normally recommended to use short intervals for these settings.

The main reason for this is that the users will learn to expect instant password synchronization and might try to access the remote system before their password has been synchronized if they are not quickly informed that the synchronization operation has failed.

Provider

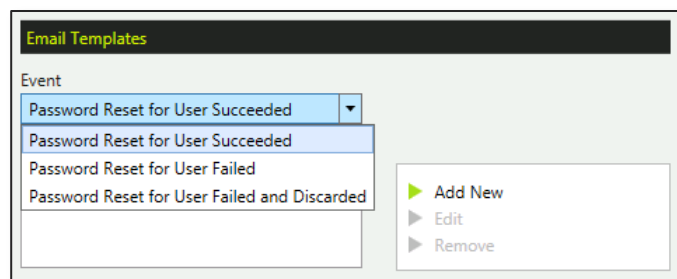
The Sync Provider contains the necessary configuration to contact the remote system and perform whatever actions the provider is designed for. Typically this means resetting a password, but since any type of logic can be put in a provider it can also be something else, like the Email Notification provider, which is used to send customized email when user passwords are changed. A full reference to the Sync Providers included out of the box with Specops Password Sync is available in the *Sync Provider configuration* section of this documentation.

Email Templates

The email templates in a Sync Point can be used to configure emails to be sent on certain system events.

This functionality can be used to inform the users that their password in the remote system the Sync Point connects to have been changed, or that the operation didn't succeed so they know that their old password will still apply.

Any number of templates can be configured for each Sync Point, even several templates for the same event.



The email template selection list allows several templates for the same event to be created.



The available events are described in the table below:

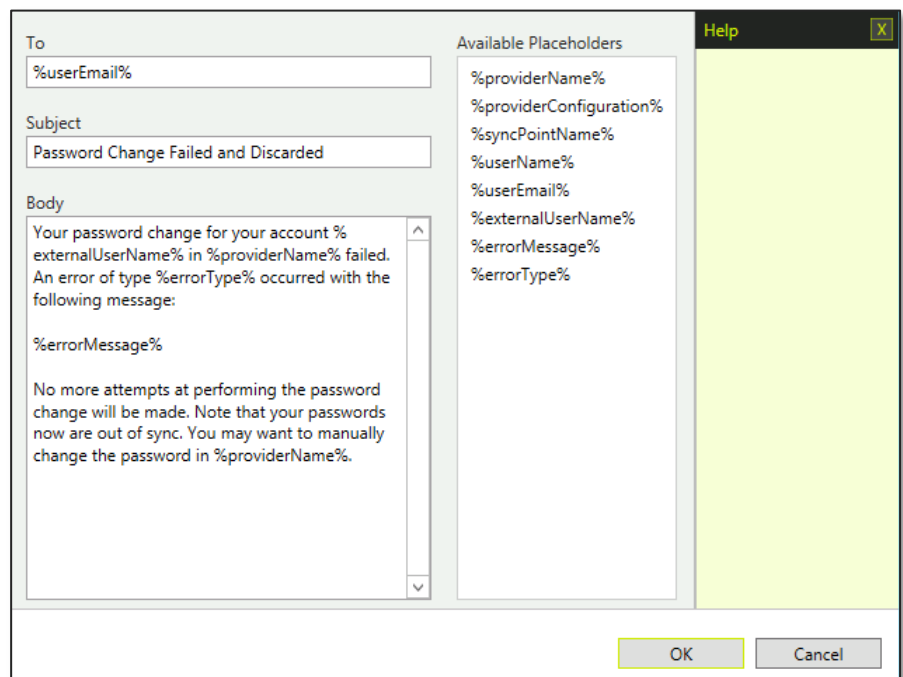
Event Name	Description
Password Reset for User Succeeded	This event occurs when the password has been successfully changed in the external system.
Password Reset for User Failed	This event occurs whenever a password change in the remote system fails. If the remote system is offline this event will happen once for each retry configured on the Sync Point, which might cause many emails to be sent for the same synchronization job if this template is used.
Password Reset for User Failed and Discarded	This event occurs when the password change in the external system has failed the maximum number of times according to the retry settings in the Sync Point. After the last failure the password change job will be discarded by the Sync Server. It is recommended to inform the user if this event occurs.

When creating a new email message you select the event you want the message to be triggered on, which opens the message editor.

New email templates use the default text for the selected event, but it is very easy to customize the text to the needs of your organization.

The available placeholders for the event can be found in a list on the right-hand side of the screen. These placeholders can be used to insert information from the system in the email.

For instance, the placeholder %UserEmail% represents the email address of the user who tried to change their password.



Email templates can be configured to meet the needs of your organization through the message editor.



This table describes the full list of placeholders:

Placeholder	Description
%providerName%	The name of the provider used by the Sync Point.
%providerConfiguration%	A list with all the configuration properties for the provider.
%syncPointName%	The name of the Sync Point
%userName%	The windows user account name of the user whose password is being changed.
%userEmail%	The email address of the user whose password is being changed. This is loaded from the user account in Active Directory.
%externalUserName%	If name mapping is used this contains the translated user name that is used in the external system. If no name mapping is in place this will be the same as the %userName% placeholder.
%errorMessage%	Information about the error that occurred
%errorType%	The type of error that occurred.

Account name mapping

Name mapping can be used in the Sync Point to translate account name from your Active Directory to the user name format in the remote system.

Name mapping must be used in all Sync Points where there is a difference between the Active Directory account name and the remote system account name.

Specops Password Sync offers two methods to perform name mapping, transformation and user attribute mapping.

Variable	Description
1-<2>	U = Convert to upper case, may be left blank L = Convert to lower case, may be left blank 1 = Start character index, required 2 = End character index, may be left blank

Use custom attribute

Use transformation pattern [1-2][4-]

Test for User

OK Cancel

Help

If transforming a user name, enter the pattern here according to the legend above.

If, for example, a user name is BobJohnson the pattern x[U1-4] would result in xBOBJ

If a custom attribute has been selected, the value from that attribute is the one that will be transformed.

The Name Mapping configuration for a Sync Point.



Transformation

If the remote system uses account names which are somewhat similar to your Active Directory account names it might be possible to simply transform the AD user names into your remote system user names.

The transformation pattern consists of a string of expressions that instruct the transformation algorithm what it should do with the incoming data from Active Directory.

If a custom attribute has been configured instead of the AD user name the transformation algorithm will transform the attribute data instead of the user name.

All transformation expressions have to be enclosed in brackets.

The available transformation variables are:

Variable function	Description	Example
U Convert to upper case	Converts characters to upper case. This variable is not required in pattern.	[U1-] Converts "Specops" to "SPECOPS".
L Convert to lower case	Converts characters to lower case. This variable is not required in a pattern.	[L1-] Converts "Specops" to "specops".
1- Start character index	The index position of the character to start the current operation from. If there is no end character the whole string will be transformed.	[4-] Converts "Specops" to "cops".
2 End character index	The index position of the character where the current operation should end. This variable is not required in a pattern.	[1-4] Converts "Specops" to "Spec"

It is also possible to use multiple transformation expressions in the same pattern to create complex transformations. For example, the pattern "[1-4][U5-5][6-]" would transform "Specops" to "SpecOps".

Attribute mapping

By specifying a custom attribute to be used the Sync Server can retrieve data from any attribute on the user object of the user in the sync job and use that.

For example, many cloud services use the email address of the user as the login name. In these cases it is sufficient to specify the

Warning!

Attributes on user objects used to provide account names in remote systems should not be writable by the users as this poses a serious security risk.

More information can be found in the security section of this document.

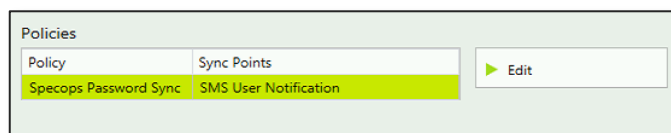


“mail” attribute to be used without any further transformation.

It is also possible to populate unused user attributes with their account names in remote systems and use the attribute mapping against them in the appropriate Sync Points.

Policies

The Policies section in the Specops Password Sync admin tool lists all Group Policy Objects with Specops Password Sync settings in your domain. Selecting a GPO and clicking the Edit action will open up the Group Policy Editor and allow you to change the settings in the policy.



Policy	Sync Points
Specops Password Sync	SMS User Notification

The policies list in the Specops Password Sync Admin Tool.

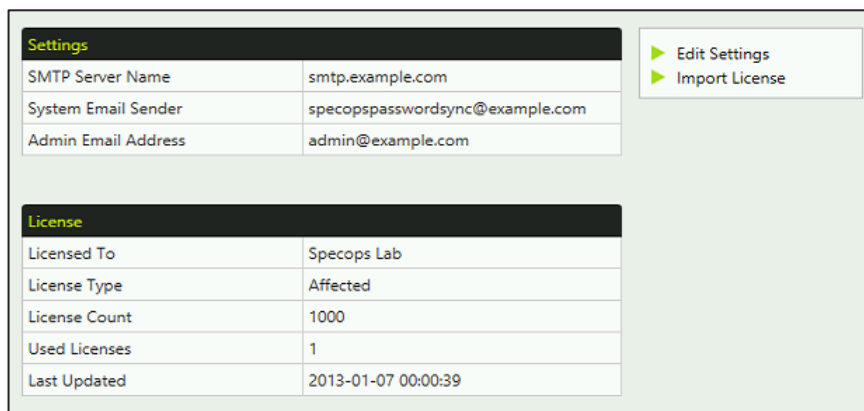
More information about editing the policy settings can be found in the *Specops Password Sync and Group Policy* section of this documentation.

Settings

The Settings section displays the system wide configuration settings used by Specops Password Sync.

The email settings can be edited by using the “Edit Settings” action and the product license can be updated by using the “Import License” action.

The License information also displays a timestamp from the daily license count performed by the product.



Settings	
SMTP Server Name	smtp.example.com
System Email Sender	specopspasswordsync@example.com
Admin Email Address	admin@example.com

License	
Licensed To	Specops Lab
License Type	Affected
License Count	1000
Used Licenses	1
Last Updated	2013-01-07 00:00:39

The Settings page displays the current email configuration and license data.



Specops Password Sync and Group Policy

Specops Password Sync extends the functionality of Group Policy to make it possible to assign Specops Password Sync configuration settings to your users through any Group Policy Object.

Assigning these settings through Group Policy makes it extremely simple to control which users should be affected and also makes it possible to use different settings for different groups of users.

What user accounts will be affected?

All user accounts that are located in locations where your GPOs are linked will be affected by the settings in the respective GPOs. If more than one GPO with Specops Password Sync settings is affecting the user account the normal GPO processing order will apply.

GPO processing order

In order to determine which settings are applied to a user or computer all Group Policy Objects that apply to the object is processed in a pre-determined sequence. If settings from different policies are in conflict, the GPO that was processed last will overwrite the previous settings.

Group Policies are processed in the following order:

1. Local Group Policy objects. Specops Password Sync settings cannot be created on this level.
2. Site linked Group Policy Objects. These are domain GPOs that are linked on the site level. Specops Password Sync settings can be created on this level.
3. Domain linked Group Policy Objects. These are domain GPOs that are linked on the domain level. Specops Password Sync settings can be created on this level.
4. OU linked Group Policy Objects. This is the most common way to link GPOs in the domain.

If more than one GPO is linked on the same level the link order of the GPOs determine in which order the GPOs will be processed. The link order can be controlled from the Group Policy Management Console.

Security filtering

Security filtering allows an administrator to control on a permission level which users and computers are allowed to read the contents of the GPO. If an object cannot read the GPO, it will not be able to process it, and thus it will not be affected by the GPO.

By controlling access this way it is easy to apply different policy settings to objects located on the same level in Active Directory.

Specops strongly recommends using security filtering to assign Specops Password Sync settings when the standard GPO processing order is not sufficient to apply the settings you prefer.

WMI filtering

WMI filtering can also be used to determine if a GPO should be processed or not when Group Policy settings are applied. However, since the Specops Password Sync settings are interpreted by the Password Change Notifier rather than the client computers it is NOT possible to use WMI filtering to control which users should receive which settings.



Creating and editing Specops Password Sync policies

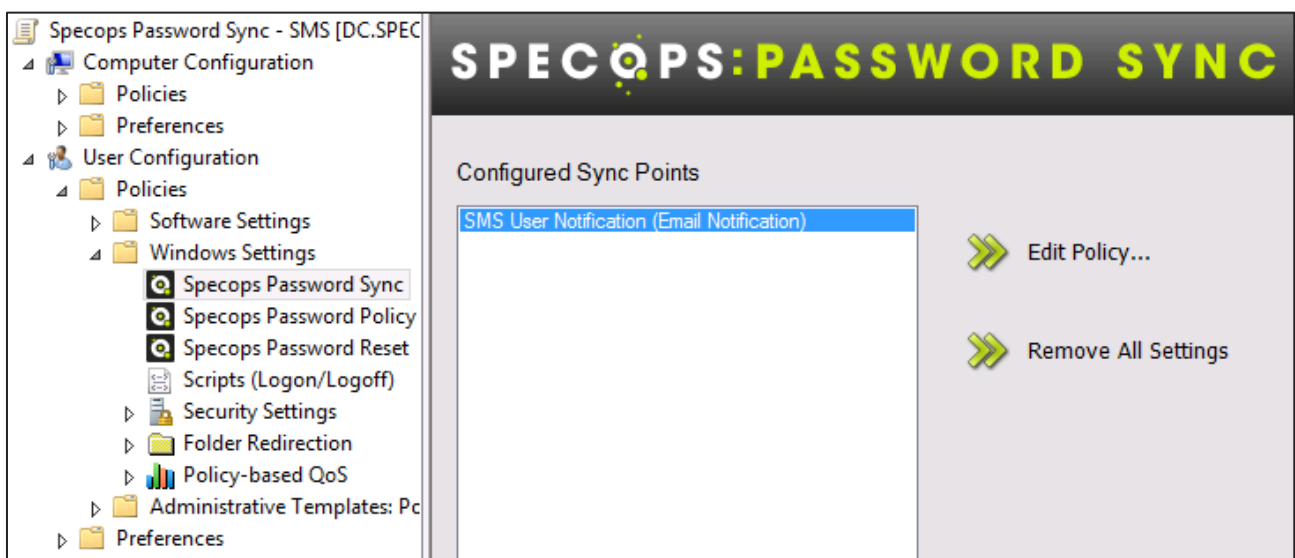
Password synchronization is enabled for the users by assigning them to use specific Sync Points in Group Policy.

This requires at least one GPO to be created with settings that assign a Sync Point to the users affected by the policy. Creating and editing Group Policy Objects is performed through the Group Policy Management Console (GPMC) in Windows. The computer needs to have the Specops Password Sync Admin tools installed in order to see the Specops Password Sync settings when editing GPOs.

Since Specops Password Sync is completely integrated with the Windows Group Policy functionality every aspect of administrating these settings work the same way as when working with other Group Policy settings.

The following steps take you through the process of creating a new GPO and adding some Specops Password Sync settings:

1. Open the Group Policy Management Console (GPMC)
2. Expand your domain node and locate the Group Policy Objects node beneath it.
3. Right-click the Group Policy Objects node and select “New”.
4. Select an appropriate name for your Group Policy Object and click OK. The new GPO will now be created.
5. Locate the new GPO beneath the Group Policy Objects node. Right-click it, and select “Edit...”.
6. The Group Policy Management Editor will now start and load the settings from your GPO. Expand the User Configuration -> Policies -> Windows Settings node.
7. Locate the Specops Password Sync node and click it to display the settings overview page.
8. Click the “Edit Policy...” button in order to open the policy settings and start configuring the policy.



The Specops Password Sync GPO extension shows the currently enabled Sync Points in the GPO.



Specops Password Sync GPO settings

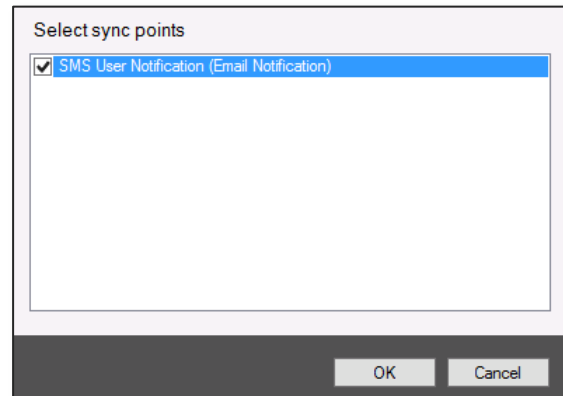
The GPO settings in a Specops Password Sync GPO are very simple. The only setting that is possible to create is which Sync Points the users affected by the GPO should use.

Enabling or disabling a Sync Point for use

Sync Points are enabled by selecting them from the list of available Sync Points.

Checked Sync Points will be used by the users affected by the GPO.

Sync Points can also be removed from a GPO by unchecking them in the list.



Select the Sync Points you want to enable in this GPO.

Note

The GPO editor lists all Sync Points configured for the domain regardless of which Sync Scope they were created in.

If your organization uses more than one Sync Scope it might be a good idea to implement a naming convention for Sync Points to ensure that the correct Sync Points are used in the GPOs as Specops Password Sync will not synchronize passwords for users outside of the Sync Scope the Sync Point is created in.



Sync Provider configuration reference

The Sync Providers are the bits of logic that perform the actual action against a remote system. Specops Password Sync ships with a number of included providers, but it is also possible to create your own using an open API.

The configuration specification for the included providers can be found below.

Active Directory provider

The Active Directory provider is used to synchronize passwords changes to another Active Directory domain.

The other Active Directory domain can be either trusted or untrusted.

Prerequisites

- Admin account in the remote domain.
- Open network communication between the Sync Server and the target domain controller. This typically means that the following two ports must be open:
 - tcp/389 (LDAP)
 - tcp/445 (SMB)

Parameters

Parameter	Description
Domain or Domain Controller Name	The FQDN of the remote Active Directory Domain or a Domain Controller in it.
Admin User Name	The name of the admin account used to reset passwords in the remote domain. Example: EXAMPLE\Administrator
Provider Password	The password of the admin account.

Email Notification provider

The email notification provider is used to trigger customized email to be sent when the password of a user is changed.

This can be used for a wide range of purposes, but perhaps the best example is to trigger an SMS to be sent to the mobile device of the user to remind them that they should also change their Active Sync password on the device to match the new Active Directory password.



Prerequisites

An email server must be available to send mail from the service account used on the Sync Server.

Parameters

Parameter	Description
SMTP Server Name	The FQDN of the SMTP server to use when sending email.
Port	The port number on the SMTP server. Default value: 25.
From	The email address the email should be sent from. Supports placeholders.
To	The email address the email should be sent to. Supports placeholders.
Subject	The subject of the email. Supports placeholders.
Body	The body text of the email. Supports placeholders.

Placeholders

The email fields in the Email Notification provider also support using placeholders to customize the email content. The placeholders can be used multiple times in the same field if necessary.

User attribute

Values from attributes on the user object of the user who triggered the password change can be retrieved through the %User.<attribute>% placeholder.

For instance, %User.mail% will be replaced with the mail attribute of the user, to retrieve an email address.

All attributes on the user object are accessible through this placeholder, but depending on their content the resulting data may be more or less useful for your intended purposes.

Password

Since Specops Password Sync also has access to the new password of the user the %Password% placeholder can be used to include the new password in the email sent by the provider.

Warning!

The %Password% placeholder poses a significant security risk to your organization.

You should only use this placeholder after verifying that the resulting action is compatible with the information security policy of your organization and/or other legal requirements in the countries the organization operates in.



Google Apps provider

The Google Apps provider is used to synchronize passwords with Google Apps.

Prerequisites

- Admin account in the Google Apps domain where passwords should be synchronized.
- Internet access on the Specops Password Sync Server.

Parameters

Parameter	Description
Google Apps Domain	The Google Apps domain name.
Administrator Account	The admin account name.
Provider Password	The password of the administrator account.

Kerberos provider

The Kerberos provider is used to synchronize passwords to Kerberos based systems.

Prerequisites

- Admin account with permissions to reset passwords in the Kerberos realm of the target users.
- Open network communication from the Specops Password Sync Server to the Kerberos server.

Parameters

Parameter	Description
Target Realm	The Kerberos realm where the target account exists.
KDC Address	The address of the Kerberos KDC to contact. This field is optional.
Admin Realm	The Kerberos realm where the administrator account exists.
Admin User Name	The user name of the admin account.
Provider Password	The password of the admin account.



LDAP Provider

The LDAP provider is used to synchronize passwords to remote LDAP systems.

Prerequisites

- Admin account in the remote system.
- Open network communication between the Sync Server and the remote server. This typically means that one the following two ports must be open:
 - tcp/389 (non-SSL-encrypted LDAP)
 - tcp/636 (SSL-encrypted LDAP)

Parameters

Parameter	Description
Server name	The name of the remote LDAP server.
Port number	The port number to use when contacting the remote LDAP server. Default port = 636.
Use SSL	Set to “true” if SSL is used and “false” if the communication should be non-encrypted. Default value = “true”
Attribute Name	The name of the user attribute in the LDAP system where the password is stored. Default value = “unicodePwd”
Convert to Unicode	Set to “true” if the password should be converted to Unicode before being stored in LDAP, or “false” if no conversion should occur. Default value = “true”
Admin User Name	User name of the admin account in the LDAP system. The user name should be in distinguished name format (CN=admin, DC=example, DC=com).
Provider Password	The password of the admin account.

Note

While it is possible to use the LDAP provider to synchronize passwords against remote Active Directories it is strongly recommended to use the Active Directory provider in these scenarios.

If you insist on using the LDAP provider against Active Directory the Admin User Name should be specified in the SAM Account Name format rather than the DN of the admin account.



Local Accounts provider

The Local Accounts provider is used to reset passwords for local user accounts on a specific computer.

Prerequisites

- Admin account for the target computer
- Open network communication from the Specops Password Sync Server to the target computer.

Parameters

Parameter	Description
Administrator Account	The user name of the admin account.
Computer Name	The name of the target computer.
Provider Password	The password of the admin account.

Microsoft Online Services provider

The Microsoft Online Services provider is used to synchronize passwords to Microsoft Online Services, such as Office 365.

Prerequisites

- The following Microsoft Online Services components must be installed on the Specops Password Sync Server:
 - [Microsoft Online Services Sign-in Assistant](#)
 - [Microsoft Online Services Module for Windows PowerShell](#)
- Internet access on the Specops Password Sync Server

Parameters

Parameter	Description
Administrator Account	The user name of the admin account.
Provider Password	The password of the admin account.



Microsoft SQL Server provider

The Microsoft SQL Server provider is used to synchronize passwords to MS SQL server users.

Prerequisites

- SQL Server authenticated admin account (Windows authentication is **not** supported).
- SQL Server user accounts (accounts stored within custom databases are **not** supported).
- Open network communication between the Specops Password Sync Server and the target MS SQL Server.

Parameters

Parameter	Description
SQL Server	The name of the target MS SQL Server.
Admin User Name	The user name of the admin account.
Provider Password	The password of the admin account.

Oracle Database provider

The Oracle Database provider is used to synchronize passwords to Oracle database users.

Prerequisites

- The provider is designed for Oracle 11g, but may work on other versions as well.
- Oracle admin account.
- Oracle authenticated users (accounts stored within custom databases are **not** supported).
- [Oracle Data Provider for .NET 4](#) must be installed on the Specops Password Sync Server.

Parameters

Parameter	Description
Database Server	The name of the target Oracle Server.
Admin User Name	The user name of the admin account.
Provider Password	The password of the admin account.



Salesforce provider

The Salesforce provider is used to synchronize passwords to Salesforce.com organizations.

Prerequisites

- Admin account in the target Salesforce.com organization.
- Valid Salesforce security token for the admin account. Note that this token is changed every time the password of the admin account is changed.

Parameters

Parameter	Description
URL	The URL to the Salesforce.com API. Default value = <code>https://login.salesforce.com/services/Soap/c/23.0</code>
Admin User Name	The user name of the admin account.
Provider Password	The password of the admin account.

Windows Service provider

The Windows Service provider is used to update the password used in a Windows Service when the password of the domain service account is changed. The provider will find all services running as the domain account on the target server set the new password on them.

Prerequisites

- Admin account on the target server.
- Open network communication between the Specops Password Sync Server and the target server.

Parameters

Parameter	Description
Administrator Account	The user name of the admin account that will be used to change the password on the remote server.
Server Name	The name of the target server where the service is running.
Provider Password	The password of the admin account.



System Security

Specops Password Sync is designed with security as a primary objective. This chapter will give you an understanding of how Specops Password Sync works from a security perspective and how to best configure the system in different types of environments.

Security features and considerations are present in multiple areas of the systems. The following sections are divided into subsections for the different SPS system components.

Password Change Notifier

The Notifer filter will perform the following validations when a successful password change is detected:

Verify Protected Groups

Any user that has the adminCount user object property set to 1 in Active Directory will automatically be filtered out and never synchronized. This prevents the system from attempting to synchronize passwords of users that are members of groups like Domain Admins, Schema Admins etc.

An event will be written to the event log every time a password synchronization job for a protected user is detected.

The adminCount property and the administrative group membership that will set this property differ somewhat depending on the version of Active Directory in your organization, but they are all fully documented on the Microsoft website.

Verify the Scope of Management

Every Sync Scope is required to have at least one User Scope of Management configured. If a Group Policy that affects a user is linked outside of the scope, this will result in the password not being synchronized and an event log entry written on the domain controller.

This security feature prevents admins that only have privileges in certain parts of an Active Directory from linking a GPO and trying to synchronize the passwords of the users they manage to systems where they do not have permissions.

Verify the configured Sync Servers

The configured Sync Servers in each Sync Point are verified that they are actually valid servers configured by a Sync Scope admin, e.g. domain admins.

This control prevents an administrator who is in charge of a specific Sync Point to change the Sync Server to a server that they control and thus intercept passwords being sent. Any tampering with this value will result in the password not being synchronized and an event written to the event log.



Notifier job queues

When all the security verifications have been successfully performed, a password change request file will be created for each Sync Point configured to be used for the user changing his or her password.

The password is encrypted with the Windows Data Protection (DPAPI) mechanism using the System credentials of the Domain Controller. This means that it is only the Domain Controller itself that can decrypt the password.

If the Password Change Notifier is unable to contact a Specops Password Sync server when a new job is created the job is kept in the queue. This ensures that password changes are not lost due to temporary network problems or Sync Server maintenance.

The default path to the job queues is:

```
%SystemRoot%\System32\SpecopsPasswordSync\Queues
```

It is only the Local System that has permissions to access this location.

Queue decryption and Sync Server communication

The Specops Password Change Notifier Service will pick up the job file from the queue and get the correct Sync Server from Active Directory.

The Notifier Service runs in the security context of the Domain Controller and is thus able to decrypt the password that should be synchronized.

The Notifier will first try to set up an encrypted SSL session with the primary Sync Server for the Sync Point. If this fails, the secondary Sync Server is contacted.

When the session is established, the identity of the remote Sync Server Service is verified using Kerberos Mutual Authentication to verify that the remote computer is the actual computer configured in Active Directory.

The password change request will then be passed to the Sync Server through the secure encrypted channel. As soon as a successful communication attempt is made the local encrypted password file is deleted from the queue.

In the event that both the primary and secondary Sync Servers are unavailable the Password Change Notifier Service will keep on trying to establish a connection until it is successful.

Note

The job queues are handled automatically by the system, but if a Sync Server is offline for an extended period of time the queue size could grow very large.

Ideally the queues should be empty at all times.



Sync Server

Notifier communication

The Sync Server maintains server side SSL connection on port 4377 (by default) that the Notifier connects to and sends the actual password change requests.

When a Sync Server is contacted by the Notifier the Sync Server verifies that the connecting computer is in fact the Domain Controller it claims to be through Kerberos Mutual authentication.

This behavior can be altered to allow only certain Domain Controllers or servers to send password sync requests by editing the membership of the local group “Specops Password Change Notifiers” on the Sync Server.

When the request is validated the password is encrypted with the System credentials DPAPI and this information is then saved in the local SQL CE database. The encrypted password can only be decrypted by the local system.

Sync Server security considerations

Membership to any local group on the Sync Server should be restricted in high security environments.

For example, an administrator on the Sync Server could replace the Sync Providers with their own custom providers or try to run processes in the context of Local System to attempt to decrypt changed passwords.

Note

Sync Servers should be treated with the same security considerations as you would apply to your domain controllers.

By ensuring that only Domain admins can administrate the Sync Servers you deny the ability of administrators with lesser security clearance to tamper with the Sync Server in order to retrieve user password data.



Sync Server TCP IP Ports

On the internal network the Sync Server uses two ports for communication.

Port number	Usage
tcp/4377	Password Sync Job communication between the Notifier Service and the Sync Server.
tcp/4378	Admin tool communication. Used when the admin tool communicates with the Sync Server, for example when updating a provider password.

This configuration is stored in the service configuration file called “PasswordSync.Server.exe.config” which can be found in the service installation directory.

The port numbers can be changed as required by editing the following sections of this file:

```
<service name="Specopssoft.PasswordSync.Server.HttpPasswordChangeListener"
behaviorConfiguration="SpsServiceBehavior">
<add baseAddress="https://SRV01.specops.demo:4377/SPS"/>
<service name="Specopssoft.PasswordSync.Server.SyncServerAdminHost"
behaviorConfiguration="DevelopmentSpsServiceBehavior">
<add baseAddress="net.tcp://SRV01.specops.demo:4378/SPS"/>
```

Restart the Sync Server service to apply the changes after the file has been saved.

The Windows firewall will automatically add 4377 and 4378 as Specops Password Sync exceptions during the installation.

If the ports and firewall settings are changed manually, the changes have to be performed again after an upgrade since the upgrade will reset the default values.

Providers

Since new providers can be added or removed in a plug-and-play manner there are security considerations regarding provider installation. The provider reference section documents the ports needed by each provider.

Sync Scope security delegation

When using the security delegation option on the Sync Scopes what actually happens is that the permissions on the Sync Scope container in Active Directory is updated at the path:

“CN=<SPS Scope Name>,CN=SyncScopes,CN=Password Sync,CN=Specops,CN=System” under the domain root.



Sync Point Name Mapping

Name Mapping must be implemented carefully to be secure. There are two main points to consider.

User attribute permissions

You should never store user account names in attributes where the end users have write permissions.

For example, if the users are allowed to edit the “Description” attribute on their own user objects and this value is used for Name Mapping, the user could change this value to another user name, change their own password and then use the new password to log in as the other user on the external system.

Use separate Sync Scopes for separate groups of administrators

Make sure to use separate Sync Scopes if there are different groups of administrators working in different parts of your Active Directory.

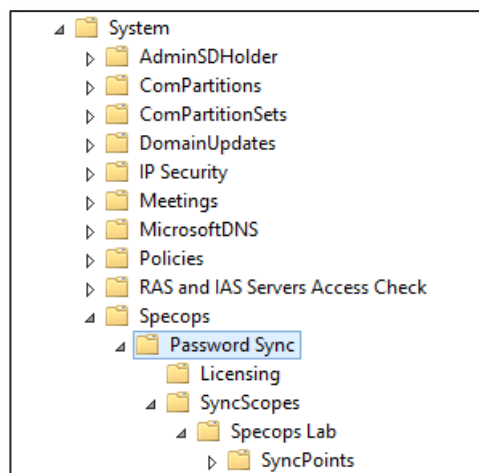
This restricts each group of administrators to working within their own scopes, and prevents attacks where one group of administrators could configure Group Policy objects to use Sync Points not intended for their group of users.

Active Directory integrated configuration storage

Specops Password Sync uses the Active Directory to store the configuration data used by the system. The settings for Specops Password Sync can be found in a container with the canonical name “<your_domain_fqdn>/System/Specops/Password Sync”.

Configuration data is stored in container and serviceConnectionPoint objects, both of which are part of the standard Active Directory schema.

By storing the information in Active Directory the system ensures reliable operation with little or no effect on the end users in case of any maintenance operations.



The Sync Scope, Sync Point and License information is stored in Active Directory.

Note

There is one important exception to the Active Directory integrated storage model.

The Administrator password configured for the Sync Provider used in a Sync Point is stored internally on the Sync Server used by the Sync Point.



Sync Server Database

Each Specops Password Sync Server maintains a local SQL Server Compact Edition database.

While most of the configuration in Specops Password Sync is stored in Active Directory, the primary function of the database is to keep the passwords configured in all the Sync Providers in a secure location.

The database is also used to temporarily store pending password changes. When a new password synchronization job is received from a Password Change Notifier it is immediately saved in a queue in the database. This database is then polled and the password changes are sent to the corresponding external system. When the password change is completed in the external system the password change is removed from the database queue.

Database location

The first time the Sync Server is started it will copy an empty database file from the service installation directory to the designated database path.

The default path differs depending on the version Windows the service is running on:

Windows version	Default database path
Windows Server 2003 Windows Server 2003 R2	C:\Documents and Settings\Default User\Local Settings\Application Data
Windows Server 2008 Windows Server 2008 R2 Windows Server 2012	C:\Windows\system32\config\systemprofile\AppData\Local

If the database location needs to be changed, the following procedure should be followed:

1. Stop the Specops Password Sync Server service.
2. Copy the existing database file to the new location.
3. Change the “DatabaseFilePath” registry setting to point to the new location.
4. Restart the Specops Password Sync Server service.

Refer to the registry settings section for more information on the “DatabaseFilePath” registry value.



Registry Settings

This section contains detailed information about the registry settings used by Specops Password Sync. During normal operation of the product it is not necessary to modify any of these settings, but it can be useful when the product is used in advanced usage scenarios.

Password Change Notifier registry settings

Registry key	Explanation
HKLM\Specopssoft\Specops Password Sync\ QueuesFolder	The full path to the folder where password synchronization jobs should be queued. Reboot of the DC is required after changing this key. Default value: %SystemRoot%\System32\SpecopsPasswordSync\Queues
HKLM\Specopssoft\Specops Password Sync\ChangeNotifierService NetworkOperationTimeout	Time in milliseconds between the DC and the Sync Server before operation to Sync Server times out. If there is high latency between DC and Sync Server, this can be increased. However, normally this value shouldn't be changed. Default value = 5000
HKLM\Specopssoft\Specops Password Sync\ChangeNotifierService IntervalBetweenRefreshConfigFromAD	Interval in milliseconds between looking for configuration changes in Active Directory. Default value = 60000
HKLM\Specopssoft\Specops Password Sync\ChangeNotifierService IntervalBetweenPollingSyncPointQueue	Interval in milliseconds between polling for new password changes in a Sync Point's queue folder. Default value = 2500
HKLM\Specopssoft\Specops Password Sync\ChangeNotifierService LicenseCheckStartTime	The time of day when license check should start. Default value = "00:00" (midnight).



Password Sync Server service registry settings

Registry key	Explanation
HKLM\Specopssoft\Specops Password Sync\Server ClearLogFile	Clear the log file when the service is started. 0 = Keep log file 1 = Clear log file Default value: 1
HKLM\Specopssoft\Specops Password Sync\Server DatabaseFilePath	The path to the Specops Password Sync Server database file. The default path is handled internally by the service. Default value: Empty
HKLM\Specopssoft\Specops Password Sync\Service LogFilePath	Interval in milliseconds between looking for configuration changes in Active Directory. Default value: C:\SPS.SyncServer.log
HKLM\Specopssoft\Specops Password Sync\Service MaxMbFileSize	Maximum size of a log file before a new log file is created. Note that only the two latest log files will be kept. Default value: 0x0000000a (10)
HKLM\Specopssoft\Specops Password Sync\Service QueuePollingIntervalSeconds	Number of seconds between polling the database for new password changes. Setting a low value increases the server load. Setting a high value increases the latency between the user password change and the synchronization to the external system. Default value: 0x00000005 (5)
HKLM\Specopssoft\Specops Password Sync\Service SyncPointCacheTTLSeconds	The number of seconds the Sync Server should cache Sync Point data. Changing this value controls how often the Sync Server has to read Sync Point data from Active Directory. Default value: 0x0000001e (30)



Troubleshooting

Configuring password synchronization to external systems can be tricky. With several different components involved to complete a synchronization job it can also be difficult to troubleshoot unexpected behavior by the product.

This section attempts to explain the best procedures to handle troubleshooting.

Installation troubleshooting

If you are struggling to get the system up and running after the initial configuration this is a good procedure to verify that all the basic parts are connected correctly:

1. Verify that the Password Change Notifier component has been installed on all Domain Controllers.
2. Look at the event log on the DCs to verify that the DC has been restarted and that the start events from the notifier filter and notifier service have been logged to the event log.
3. Also verify that the Domain Controllers have been restarted after the installation in order to make sure that the Notifier filter is running.
4. Verify that the Sync Server service is started on the Sync Server
5. Verify that the following configuration has been made:
 - a. Sync Scope created and target user located beneath the Sync Scope.
 - b. Sync Server added to the Sync Scope
 - c. Sync Point created and configured to use the Sync Server.
 - d. Specops Password Sync GPO created, configured to use the Sync Point, and linked to affect the target user.

With these basic steps complete the system should be able to process your password changes. If you still have problems, follow the component troubleshooting procedure to identify the problem source.

Component troubleshooting

If you still have problems after you have confirmed that the basic configuration of the system is correct you should follow the chain of actions that is supposed to take place when a password is changed to track down the problem source. This is best performed from a DC, and requires a test account which is configured to use a Sync Point.

Follow this procedure:

1. Log in on to the selected domain controller and open the Active Directory Users and Computers console.
2. Reset the password of the test account.
3. Monitor the Application event log on the domain controller. The event log should show entries from the Change Notifier Filter and Notifier service indicating that that password change was picked up.
4. Verify that the Sync Server service is running.
5. Monitor the Event log on the Sync Server. Events should be logged for the new sync job.
6. There are two common problems that can occur in the communication between the Change Notifier and the Sync Server:



- a. A firewall is blocking the communication. The Change Notifier on the domain controllers need to be able to connect to the Sync Server (default port tcp/4377) in order to deliver the sync jobs.
- b. The connection is refused because either the domain controller or the Sync Server does not trust the certificate of the remote partner. The most common cause for this is that the Sync Server is using a self-signed certificate which is not trusted by the domain controllers.

If the event logs have not shown any problems it is likely that the source is outside of the product. This can be verified by using the Filewriter provider to test the system.

File Writer provider

The File Writer provider is shipped with the setup package and can be used to test the Specops Password Sync component configuration. As with all other providers, this component should be installed on the Sync Server.

The File Writer will not communicate with any external system when it receives a password change request, instead it will just write the user name and a timestamp to a log file.

The File Writer installation package can be found in the directory where you extracted the Specops Password setup package (“C:\temp” by default).

The path to the package is

“\Products\SpecopsPasswordSync\SpecopsPasswordSyncTestProviders-xXX.msi”. Run the appropriate 32 or 64 bit version depending on your Sync Server OS.

The Specops Password Sync Server service must be restarted after the installation before the new provider is visible in the admin tool.

When the File Writer provider has been installed you can follow the procedure below to test it:

1. Create a new Sync Point and configure it to use the File Writer provider. Note that you must select the Sync Server where the File Writer is installed in order for this to work.
2. Follow the Component troubleshooting procedure to reset the password and monitor the appropriate event logs.
3. If everything works you should see a number of entries indicating that the File Writer provider successfully completed the synchronization.

Configuration troubleshooting

If all the components are installed and working properly the error is most likely related to the configuration of your Sync Point or Sync Policy. Try these simple steps:

1. Start troubleshooting by making sure that your target user is affected by the appropriate Sync Policy.
2. Look through the provider reference section of this documentation and make sure that there is nothing blocking communication between the Sync Server and the remote system.
3. Verify that the correct information has been entered in the provider configuration of the Sync Point.

As a final step, debug logging can be enabled on the Sync Server. The debug log will provide all details of what happens when the sync job is processed.



Event logging

The Specops Password Sync components log many of their operations to the application event log. This can be used to monitor the service for problems or for gathering information about the system usage.

Password Change Notifier filter events

Information events

ID	Error Level	Explanation
150	Information	Filter has been loaded.
151	Information	A password change will take place for the user indicated in the event log message. Even if this change arrives from multiple GPOs and/or involves multiple Sync Points, this message will only occur once per password change.
152	Information	User is member of a Windows protected group. For security reasons, Specops Password Sync does not attempt to synchronize the passwords of users who are members of protected groups. In order to avoid this message you should probably ensure that protected accounts are not affected by Specops Password Sync GPOs.

Warning events

ID	Error Level	Explanation
250	Warning	Failed to queue a password sync job. The event message contains more information.
251	Warning	The policy contains no Sync Points. This happens if a password change takes place for a user that is affected by a Specops Password Sync policy, but the policy doesn't have any enabled Sync Points. This is likely a configuration error and no password changes will be synced for this user.
252	Warning	Failed to get Sync Points from policy. The event message contains more information.
253	Warning	The XML data containing the policy is invalid. The event message contains more information.



ID	Error Level	Explanation
254	Warning	<p>User is not in scope.</p> <p>This happens if password change takes place for a user affected by a Specops Password Sync policy, but the user is outside the scope of management for that policy.</p> <p>This is a configuration error. Either this user should not be affected by this policy (change this from group policy management), or the scope of management for the Sync Scope should be updated to include this user.</p>
255	Warning	<p>The configuration for this Sync Point was invalid.</p> <p>The event message contains more information.</p>
256	Warning	<p>The Sync Server for this Sync Point is not authorized to be used within this Sync Scope.</p> <p>This is an unexpected configuration error. Open the Specops Password Sync Admin tools and update the valid Sync Servers for the scope and Sync Servers to use for the Sync Point.</p>

Error events

ID	Error Level	Explanation
350	Error	<p>Failed to initialize password filter.</p> <p>The event message contains more information.</p>
351	Error	<p>Crashed while initializing password filter.</p> <p>The event message contains more information.</p>
352	Error	<p>Exception during password sync.</p> <p>The event message contains more information.</p>
353	Error	<p>Exception during password change.</p> <p>The event message contains more information.</p>
354	Error	<p>Crashed during password sync.</p> <p>The event message contains more information.</p>



Change Notifier service events

Information events

ID	Error Level	Explanation
151	Information	Service start initiated from service control manager.
152	Information	Service start completed.
153	Information	Service stop initiated from service control manager.
154	Information	Service stop completed.
155	Information	Service has started to serve a Sync Point.
156	Information	Service detected an updated Sync Point configuration and started using it.
157	Information	An obsolete Sync Point queue folder was deleted. This happens during service startup, if a queue folder is detected for a Sync Point that no longer exists.
158	Information	License check started.
159	Information	License check completed.
160	Information	License is valid. The event message contains more information.



Warning events

ID	Error Level	Explanation
251	Warning	Notifier service failed to send password change notification to Sync Server. This will repeat until the notification has been sent successfully.
252	Warning	There is no Sync Server defined for this Sync Scope. Solve this by opening the Specops Password Sync admin tool and configure the Sync Server(s) within the Sync Scope.
253	Warning	License is about to expire or about to be exceeded. The event message contains the license information.

Error events

ID	Error Level	Explanation
350	Error	An exception occurred in the Notifier service. This is an unexpected error condition that should be reported to Specops Support.
351	Error	An unexpected error occurred while for a Sync Point. This is an unexpected error condition that should be reported to Specops Support.
352	Error	Service failed to start. The event message contains more information.
353	Error	Invalid Sync Point configuration. The event message contains more information.
354	Error	Failed to process a password change. No further processing will occur for this change. The event message contains more information.
355	Error	Service stopped serving a Sync Point due to an exception. The event message contains more information.
356	Error	The Password Change Notifier filter is not loaded and therefore password changes will not be synchronized. This happens if the server has not been restarted after installation. Please reboot the server.



ID	Error Level	Explanation
357	Error	<p>Sync Server URL does not match the DNS name.</p> <p>This means that the URL to the Sync Server in the server's SCP does not match its DNS name.</p> <p>This is a configuration error, and password changes for this Sync Point will not be synchronized.</p>
358	Error	<p>The Sync Server specified for this Sync Point is not allowed within this Sync Scope.</p> <p>Open the Specops Password Sync Admin tool and make sure that the specified Sync Server(s) are listed as Sync Servers for this Sync Scope.</p>
359	Error	<p>Failed to read Sync Point configuration.</p> <p>The event message contains more information.</p>
360	Error	<p>License check failed.</p> <p>The event message contains more information.</p>
361	Error	<p>License is invalid.</p> <p>It might be corrupt, missing, or in need of an update.</p> <p>The event message contains more information.</p>
362	Error	<p>Failed to send license e-mail.</p>
363	Error	<p>No valid license was found.</p>



Sync Server events

Information events

ID	Error Level	Explanation
150	Information	Specops Password Sync Server started.
151	Information	Specops Password Sync Server stopped.
152	Information	A password for a Sync Point was updated.
153	Information	The “Domain Controllers” group was added to the “Specops Password Change Notifiers” group.
154	Information	The “Domain Controllers” group was not added to the “Specops Password Change Notifiers” group because it is already added.
155	Information	A successful password change was made by a provider. The event message contains more information.
156	Information	A provider was loaded. The event message contains more information.

Warning events

ID	Error Level	Explanation
250	Warning	A valid provider was not found. The event message contains more information.
251	Warning	Could not send email to user. The event message contains more information.



Error events

ID	Error Level	Explanation
350	Error	Failed to start the Specops Password Sync Server.
351	Error	Failed to stop the Specops Password Sync Server.
353	Error	Password change event referring to an unknown Sync Point.
354	Error	Failed to change password for a user.
355	Error	Failed to change password for a user, no more attempts will be made.
356	Error	Failed to change password for a user because the configured Sync Point refers to an unsupported provider.
357	Error	No password was configured for the provider on the Sync Point.
358	Error	Failed to transform the user name.
359	Error	Could not find the “Domain Controllers” group to the “Specops Password Change Notifiers” group.
360	Error	Could not add the “Domain Controllers” group to the “Specops Password Change Notifiers” group.
362	Error	Failed to load provider.
363	Error	Failed to send email.
365	Error	Invalid SMTP configuration on Sync Scope.
366	Error	Could not consume reset data.
367	Error	Failed to load meta data for provider.
368	Error	Password change was rejected by the server.
369	Error	Failed to change password because the Sync Point has an invalid configuration for the provider.
370	Error	Unhandled exception occurred in the Specops Password Sync Server.



Debug logging

All components in a Specops product can be configured to log their internal activity to a verbose debug log. Since the debug logs allow you to follow exactly what the component is doing when an error occurs it is usually a very good first step to enable debug logging and reproduce the error when you need to analyze a problem.

Debug logging is enabled by changing the relevant registry key for the affected component. Specops Password Sync also supports three levels of debug logging:

Debug value	Log level
0	No debug logging.
1	Normal debug logging. Use this log level when starting troubleshooting.
2	Verbose debug logging. Use this log level for advanced troubleshooting.
3	Very verbose debug logging. Use this log level in extreme cases when full debug data is necessary to troubleshoot the system. This debug level is not supported by the Change Notifier component.

The following registry keys are used to enable or disable debug logging:

Registry Key	Explanation
HKLM\Specopsoft\Specops Password Sync\ChangeNotifier Debug	Controls debug logging for the Change Notifier filter. Log files (spsflt*.log) are stored under %SystemRoot%\Debug\ Default value = 0
HKLM\Specopsoft\Specops Password Sync\ChangeNotifierService Debug	Controls debug logging for the Change Notifier service. Log files (spsChangeNotifier*.log) are stored under %SystemRoot%\Debug\ Default value = 0
HKLM\Specopsoft\Specops Password Sync\Server Debug	Controls debug logging for the Sync Server service. The default log file path is "C:\SPS.SyncServer.log". Default value = 0

Note

The debug logs will look better if you use the Specops Log Viewer to read them. The Log Viewer is a free component delivered as part of the Specops Deploy setup package.

Visit www.specopsoft.com for more

Warning!

Do not leave the debug logging turned on unless you need it.

Verbose logging over an extended amount of time can create large log files, potentially filling up your system disk.



Support

If you are unable to resolve a product related issue by yourself you are always welcome to contact Specops Support for further assistance.

Online support channel

The best way to access our support services is to submit your case directly on our website at:

<http://www.specopsoft.com/support>

This ensures a quick response from our support team and enables you to get your case submitted directly into our support system.

Telephone support channel

If you have experienced a critical issue with the product you should contact Specops Support in your region directly through one of our support phone numbers:

International Support (located in Stockholm, Sweden)

Open from 09:00 to 17:00 CET

+46 8 465 012 50

North American Support (located in Toronto, Canada and Philadelphia, USA)

Open from 09:00 to 17:00 EST

+1-877-SPECOPS (773-2677)

Customer satisfaction

Happy customers are very important to us at Specops. If you would like to share your feelings about our products or service with us, please don't hesitate to contact us.

Call your sales representative, talk to our support staff or if all else fails, send email to infomaster@specopsoft.com.

We wish you a pleasant experience using Specops Password Sync.

