Sys-Manage CopyRight2

Password Synchronization & Migration Add-On

Administrator Guide

Password Hash and Kerberos Key Migration
for Active Directory, Domain Member and Workgroup Systems

Copyright © 2012–2026 by Sys-Manage. All rights reserved.

Copyright © 2012 by Sys-Manage. All rights reserved.

This publication is protected by Copyright and written permission should be obtained from the publisher prior any prohibited reproduction, storage in retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise.

Sys-Manage Informatica SL
Phone: +1 (408) 345-5199
Phone: +1 (360) 227-5673
Phone: +44 (0) 8455273028
Phone: +49-(0)69-99999-3099
Phone: +34-810 10 15 34
Mail: Support@Sys-Manage.com
Web: http://www.Sys-Manage.com
YouTube: www.YouTube.com/SysManage
Facebook: www.facebook.com/pages/Sys-Manage/153504204665791
Bluesky: https://bsky.app/profile/sys-manage.bsky.social
Mastodon: https://techhub.social/@SysManage
Reddit: https://www.reddit.com/r/CopyRight2/

Use of trademarks: Microsoft, Windows, Windows NT, XP, Windows Vista, Windows 7, Windows 8, Windows 10, Windows 11 and the Windows logo are ® trademarks of Microsoft Corporation in the United States, other countries, or both. All other company, product, or service names may be trademarks of others and are the property of their respective owners.

Abstract

The CopyRight2 Password Migration Add-On extends user and computer migration capabilities by enabling the migration and synchronization of password-related authentication data across standalone systems and Active Directory domains. It supports password migration for Active Directory domain user accounts as well as local user accounts on domain member and workgroup systems.

Depending on the migration scenario and target security configuration, the add-on supports the migration of NT password hashes as well as real-time password-change synchronization for security-hardened environments, ensuring that the target domain generates the required Kerberos key material (including AES) as part of password updates. This allows users to authenticate seamlessly in the target environment without requiring password resets or forced password changes.

The add-on integrates with existing CopyRight2 migration workflows and supports both one-time password migrations and continuous synchronization scenarios, including one-way and two-way domain configurations, while accommodating environments with enhanced security controls.

Requirements

CopyRight2 has the following hardware requirements:

- At least 4GB of RAM
- At least 1 CPU with 2 cores (or hyper-threading)
- At least 256MB of available disk space

CopyRight2 supports the following versions of Windows:

- Microsoft Windows® 2000
- Microsoft Windows® 2003 / Windows® 2003 R2
- Microsoft Windows® 2008 / Windows® 2008 R2
- Microsoft Windows® 2012 / Windows® 2012 R2
- Microsoft Windows® 2016
- Microsoft Windows® 2019
- Microsoft Windows® 2022
- Microsoft Windows® 2025
- Microsoft Windows® XP
- Microsoft Windows® Vista
- Microsoft Windows® 7
- Microsoft Windows® 8.0 / 8.1
- Microsoft Windows® 10
- Microsoft Windows® 11
- Windows® Cluster Services

CopyRight2 supports the following Network Attached Storage Solutions:

- Synology® / Synology® Directory Server
- Many others...

For a successful operation the following Windows security privileges are required at a minimum, which are granted to members of the Administrators group by default:

- Migration of Active Directory User Account Password Hashes (NT-Hash)
    - Member of “Enterprise Admins”, “Domain Admins” or “Local Administrators” group

- Migration of Active Directory User Account Kerberos Authentication Keys
    - Either member of “Enterprise Admins”, “Domain Admins”, “Local Administrators” or alternatively delegated administrative permissions in target directory allowing to set passwords.

It is recommended that you specify computers using their computer names and that DNS or NetBIOS name resolution will provide addresses for those names. Specifying IP addresses can potentially create problems. In case of problems with name resolution, you can always create a LMHOSTS file to map computer names to network addresses (See chapter Troubleshooting / Name Resolution Problems if Specifying Servers by IP Address). This problem affects network drives connected to hosts using IP addresses as well. The most reliable solution is to create a LMHOSTS file.

Installing the Password Synchronization Add-on

The components of the Password Synchronization Add-On are installed by running PwdSyncAddon.msi.

On the Select Add-On Components page of the installer, select the components you want to install (for example, enable the Password Filter option to install the password filter component).

The same installer is used for both the traditional NT-Hash migration method and the advanced password filter method, which enables the migration of user passwords including Kerberos AES keys (for example, when RC4 is disabled in the target environment), real-time password synchronization, and password quality checks.

In this chapter, you will find information on whether you need to use the password filter method and where and how to install each component.

When do I need the Password Filter?

The Password Filter is an optional component that extends the default password migration and synchronization capabilities. It is installed by enabling the Password Filter option on the Select Add-On Components page of the installer.

You must use the Password Filter if any of the following applies:

- During domain migrations, Kerberos authentication must continue to work using modern encryption types (AES) after migration

  Reason: AES keys are domain/realm-specific and must be generated when the password is set/changed.

- Password changes must be synchronized continuously between environments

  Reason: Continuous synchronization requires capturing each password change event and applying it to the target environment.

- The password quality feature should be used to prevent weak or disallowed passwords

  Reason: Password quality checks must be enforced at the moment a new password is set.

The following challenges can be addressed either by installing the Password Filter or by applying alternative workarounds:

- NT password hash migration is blocked by security software

  Alternative workarounds: configure AV/EDR allowlisting/exclusions, or temporarily disable the blocking protection component during the migration.

- LSA is running as a protected process (PPL / LSA protection)

  Alternative workarounds: disable LSA protection / PPL (evade if possible, last resort)

- You plan to disable Kerberos RC4 as part of the migration (soft rollout option)

  To avoid enforcing “RC4-disabled” immediately, you can introduce it gradually: either enforce a one-time password change at first logon for migrated users, or wait until users have changed their passwords naturally (based on your maximum password age) and disable RC4 afterwards.

Validate if RC4 Kerberos Encryption Type is Already Disabled

You can run the PowerShell command below on computers and domain controllers in your target domain to query the configured Kerberos encryption types:

```
(Get-ItemProperty
"HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters" -Name
SupportedEncryptionTypes -ErrorAction SilentlyContinue).SupportedEncryptionTypes
```

PowerShell Command to Query SupportedEncryptionTypes

The table below shows some possible configuration values:

Value	Description
0 / undefined	Default setting, currently RC4+AES128+AES256 but in the future AES128+AES256 only!
24	RC4 disabled, AES128 + AES256 enabled.
28	RC4 + AES128 + AES256 enabled.

Example SupportedEncryptionTypes Values

Where do I need to install the Add-on?

NT-Hash Migrations

If you plan to migrate NT hashes only, you must install the add-on on the system where you run the CopyRight2 GUI. Unless this system is also a source or target of a user migration that includes passwords, you do not need to enable the Password Filter option during installation on this system.

Installing the add-on enables the Password option on the User and Group Migration job’s Settings page and installs the components that CopyRight2 deploys to the source and target servers to retrieve and/or set NT password hashes. You can also install the Password Filter (configured for NT-hash migration) directly on the job’s source and target servers. This can be useful if AV/EDR software blocks the remote installation of the required password migration components.

In addition, installing the Password Filter on the source and target servers can speed up job execution because the components do not need to be installed each time the job is launched.

Password Synchronization

If you plan to use the Password Filter for Password Synchronization, you do not need to install the add-on on the system where you run the CopyRight2 GUI.

To ensure that password changes are continuously synchronized, the add-on and the Password Filter must be installed on:

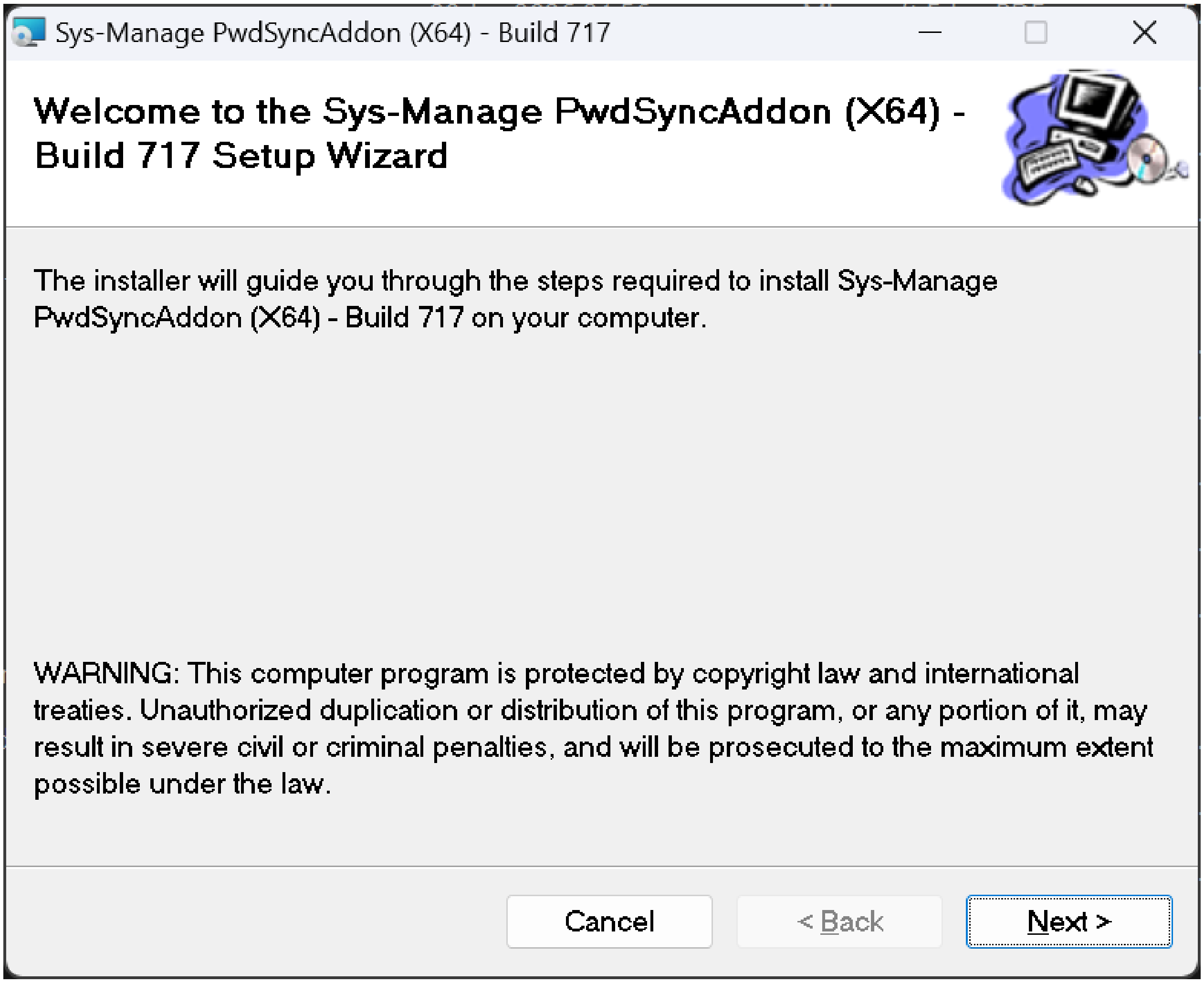
- All writable domain controllers of the source domain (if the source is a domain)
- At least one (preferably two for redundancy) writable domain controllers of the target domain (if the target is a domain)
- The source system (if the source is a workgroup-mode system or a domain member)
- The target system (if the target is a workgroup-mode system or a domain member)

Note: The software must be installed on all writable domain controllers, because password changes can occur on any of them. Read-only domain controllers (RODCs) relay password changes to writable DCs and therefore do not require the filter to be installed.

Installing the desired components

You can begin the installation of components by launching the PwdSyncAddon.Msi file, usually the 64-bit version unless 32-bit systems are involved.

After launching the MSI installer you will be greeted by the welcome page of the installation wizard.



Sys-Manage PwdSyncAddon (X64) - Build 717

Welcome to the Sys-Manage PwdSyncAddon (X64) - Build 717 Setup Wizard

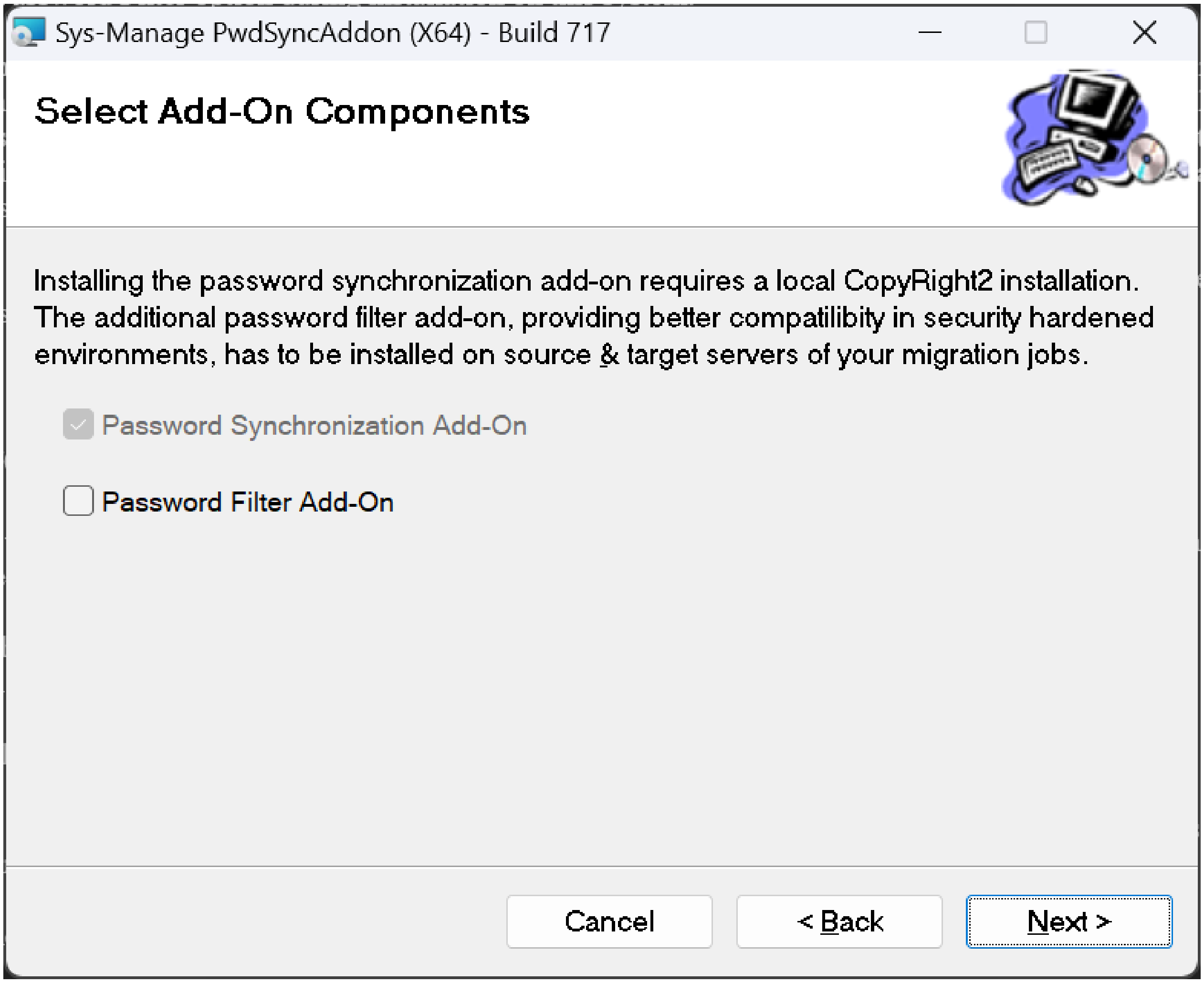
The installer will guide you through the steps required to install Sys-Manage PwdSyncAddon (X64) - Build 717 on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Click on the Next button to begin the installation process.

In the following component selection page, select the components you want to install on the local system.

If you run the installer on a system where CopyRight2 is installed, the NT-Hash migration components are selected automatically. Otherwise, the first option is not selected. Optionally, enable the Password Filter component. Installing the password filter requires a reboot so that the LSA process can load the filter.



Sys-Manage PwdSyncAddon (X64) - Build 717

Select Add-On Components

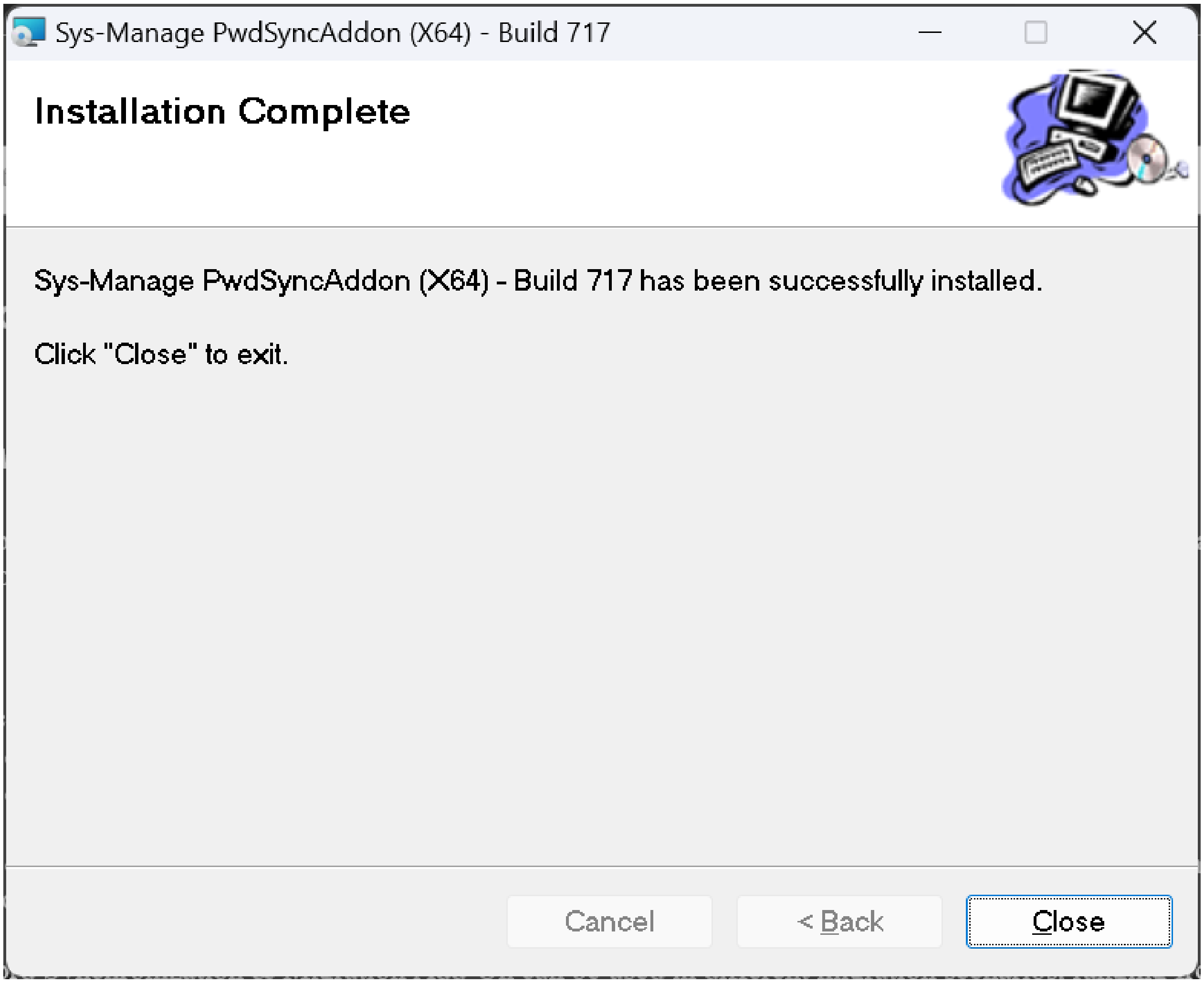
Installing the password synchronization add-on requires a local CopyRight2 installation. The additional password filter add-on, providing better compatilibity in security hardened environments, has to be installed on source & target servers of your migration jobs.

☑ Password Synchronization Add-On

□ Password Filter Add-On

Once you have selected the desired components, click Next to start the installation. If you run the installer from an account with UAC enabled, you may be prompted to confirm the elevation request.

After the installation has completed, click Close to exit the wizard. If a reboot is required, you will be prompted accordingly.



Sys-Manage PwdSyncAddon (X64) - Build 717 has been successfully installed.

Click "Close" to exit.

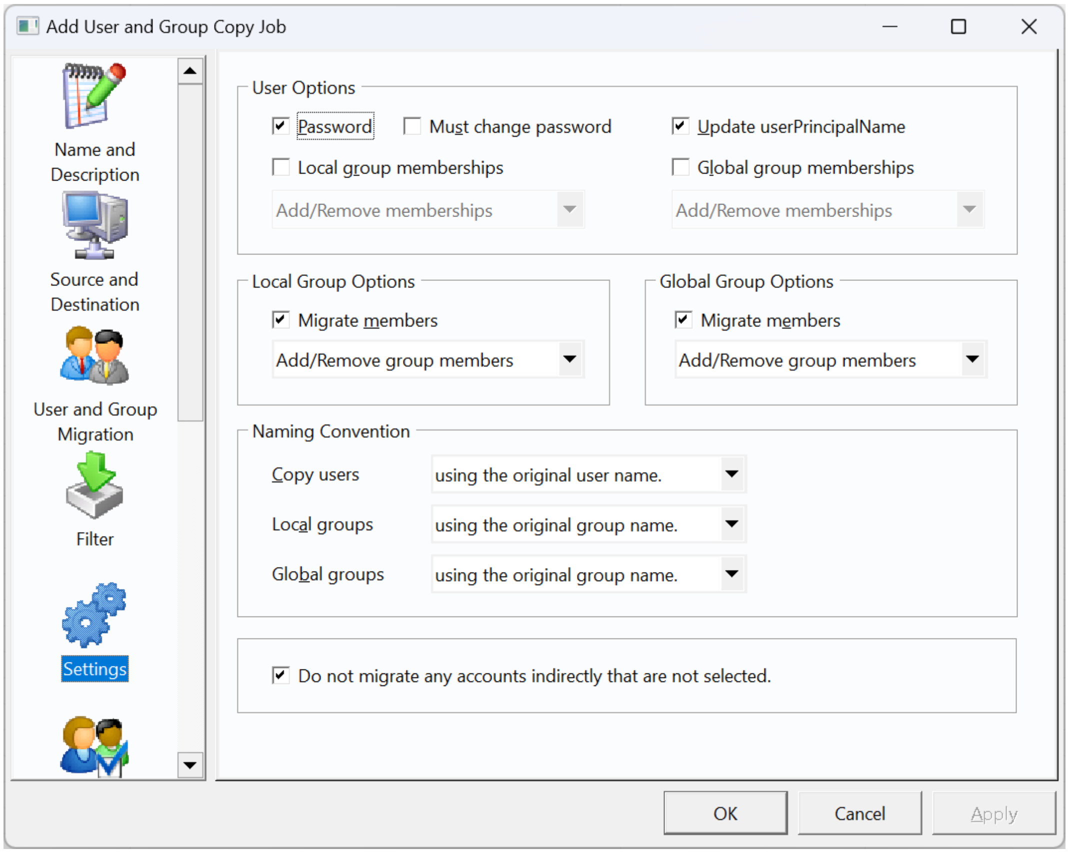
NT-Hash Migration

This chapter explains how to configure and run migration jobs with NT-hash migration enabled.

If enabled, each target user of the migration job, will receive the NT-Hash the corresponding source user had. Additionally, it will enable the target user object, if the source user object was enabled. By default, AD user provisioning tools (e.g., ADUC / net user) assume passwords are required. An account typically cannot be enabled for interactive use until a password is set, unless the account is explicitly configured with ‘Password not required’ (UF_PASSWD_NOTREQD) and the domain password policy permits a blank password.

Job Configuration

If you want to migrate Windows NT hashes, you must install the Password Synchronization Add-On on the system where you run CopyRight2. This enables the otherwise grayed-out “Password” and “Must change password” options on the Settings page of User and Group Migration jobs.



User Options

☑ Password ☐ Must change password ☑ Update userPrincipalName

☐ Local group memberships ☐ Global group memberships

Add/Remove memberships | Add/Remove memberships

Local Group Options

☑ Migrate members

Add/Remove group members

Global Group Options

☑ Migrate members

Add/Remove group members

Naming Convention

Copy users: using the original user name.

Local groups: using the original group name.

Global groups: using the original group name.

☑ Do not migrate any accounts indirectly that are not selected.

Optionally, you can also install the Password Filter on the source and/or target system if NT hash migration is blocked by security software or if LSA is running as a protected process.

During a migration, the job checks whether the password filter component is installed on the source and/or target server. If it is not found, CopyRight2 deploys a service to retrieve and/or set password hashes. If the filter is present, the service deployment is not required and the job typically runs faster because the overhead of installing and starting the service is avoided.

Launching the Job

Execute the job either interactively in the GUI or as a scheduled background job. If the execution reports errors, review the log file.

In the log file, you will see that near the end of the job CopyRight2 first reads the password hashes from the source system and then stores them on the target system.

If security restrictions prevent the password operation, the log will report corresponding errors indicating whether the issue is caused by security software (AV/EDR) or by a hardened/protected LSA configuration.

Limitations of this method

If you migrate between two Active Directory domains and the target environment has Kerberos RC4-disabled as a valid encryption type (etype), migrating the NT hash alone is not sufficient. Target users will not be able to obtain Kerberos tickets to access resources.

In addition, users will not be able to change their password after the migration, because they cannot perform the initial authentication required to do so.

Password Synchronization (Password Filter)

This chapter explains the advanced features provided by the password filter, such as enabling AES-ready migrations in security-hardened environments, performing real-time password synchronization (one-way or two-way), and applying a password quality filter to block known weak or disallowed passwords.

Topologies and Roles

Password synchronization can be deployed in one-way or two-way mode:

- One-way synchronization: Password changes are replicated from the source environment to the target environment only.

- Two-way synchronization: Password changes are replicated in both directions between environments.

To support segmented networks and reduce cross-domain connectivity requirements (and firewall configurations), the solution uses two roles:

- Edge server: Receives password change events from local domain controllers and forwards them to the remote environment. It also terminates the X.509-based trust for cross-environment communication.

- Proxy server: Relays password change events between local domain controllers and an edge server, allowing domain controllers to communicate only with nearby proxy systems.

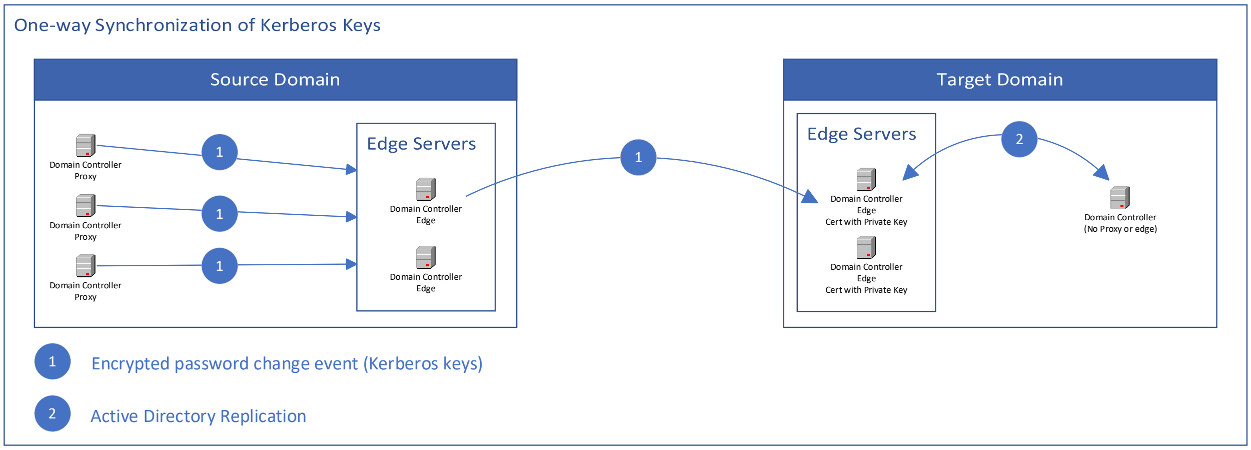
The add-on supports the following deployment topologies:

- Hub-and-spoke (star) topology: Multiple proxy domain controllers forward password change events to a central edge server. This is the most common layout and minimizes the number of systems that require cross-environment connectivity.

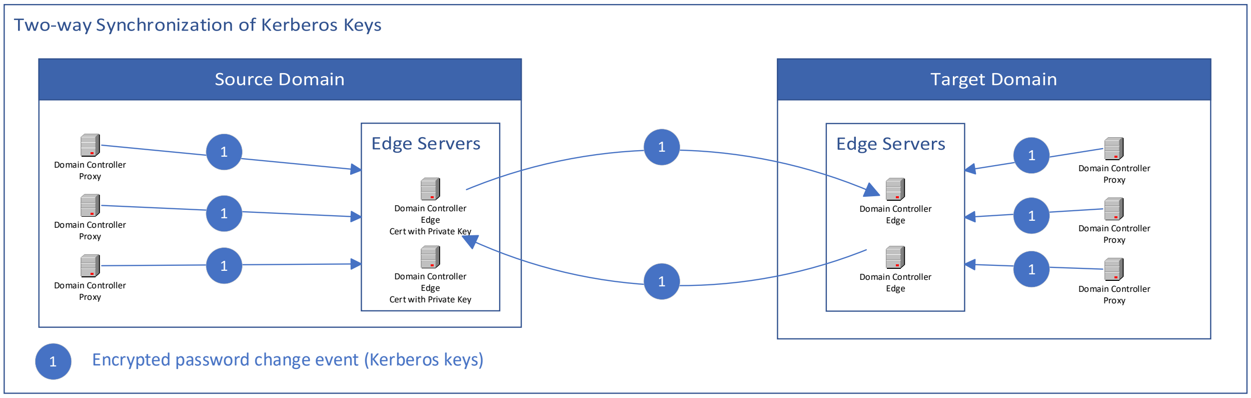
- For larger environments: Tiered hub-and-spoke topology: Proxies can be arranged in multiple tiers, where a proxy forwards to another proxy (or an aggregation proxy), which then forwards to the edge server. This is useful for large environments, branch offices, or networks with strict routing constraints.

In all cases, only the systems designated as edge servers need to be configured for cross-environment connectivity and certificate trust.

The diagram below, illustrates the flow of password change events from the originating domain controller to the target domain in case of a one-way synchronization:


One-way Synchronization of Kerberos Keys
Source Domain
Domain Controller Proxy
Domain Controller Proxy
Domain Controller Proxy
1
1
1
Edge Servers
Domain Controller Edge
Domain Controller Edge
1
Target Domain
Edge Servers
Domain Controller Edge Cert with Private Key
Domain Controller Edge Cert with Private Key
2
Domain Controller (No Proxy or edge)
1 Encrypted password change event (Kerberos keys)
2 Active Directory Replication

The diagram below shows the data flow in case of a two-way synchronization:



Password Policy and Complexity Considerations

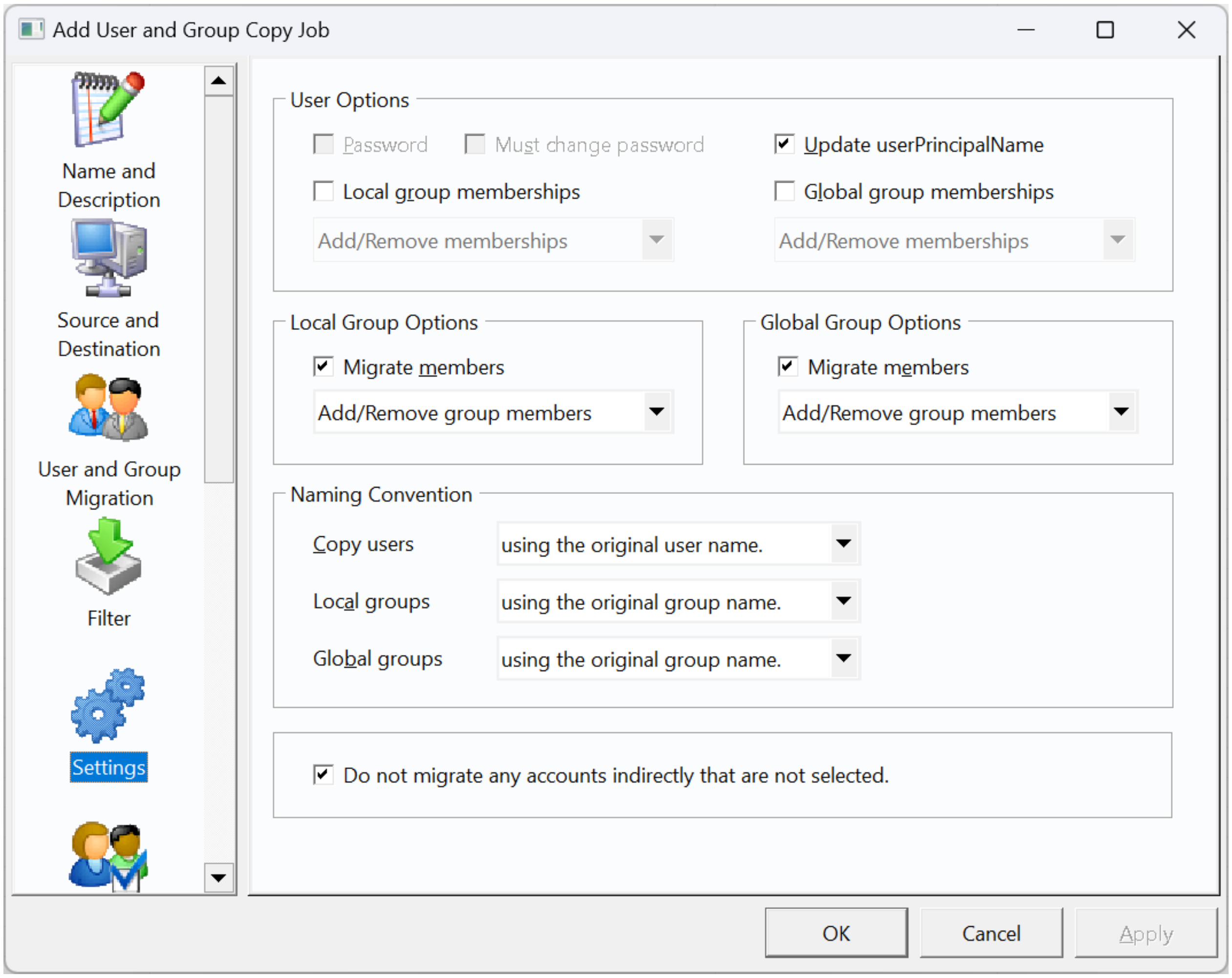
When using Password Filter–based password synchronization, the password change is applied to the target system using the cleartext password captured at the time of the change.

As a result, the password policy of the target system or target domain is fully enforced, including complexity, length, and password history requirements.

If the source environment allows passwords that do not meet the target policy, such password changes cannot be applied and synchronization will fail for the affected accounts until a compliant password is set.

Job Configuration

The password filter uses a separate configuration module and is not configured from within the CopyRight2 GUI. If you use the filter to migrate user passwords, the Password and Must change password options in CopyRight2 may remain grayed out and should not be enabled, because password migration and synchronization are performed by the filter as a separate process.



User Options

☐ Password ☐ Must change password ☑ Update userPrincipalName

☐ Local group memberships ☐ Global group memberships

Add/Remove memberships | Add/Remove memberships

Local Group Options

☑ Migrate members

Add/Remove group members

Global Group Options

☑ Migrate members

Add/Remove group members

Naming Convention

Copy users: using the original user name.

Local groups: using the original group name.

Global groups: using the original group name.

☑ Do not migrate any accounts indirectly that are not selected.

In this scenario, the User and Group Migration job is used only to migrate the remaining account data, such as user properties, group memberships, Active Directory attributes, and the target OU/location where the user objects should be created. It also updates the target user's account activation status: users initially created by the filter are created disabled, and CopyRight2 will enable the target account if the corresponding source account is enabled.

If the user account migration should be executed before the password filter creates the target user object, the resulting target user object will be disabled and get enabled by the password filter once a password change is replicated.

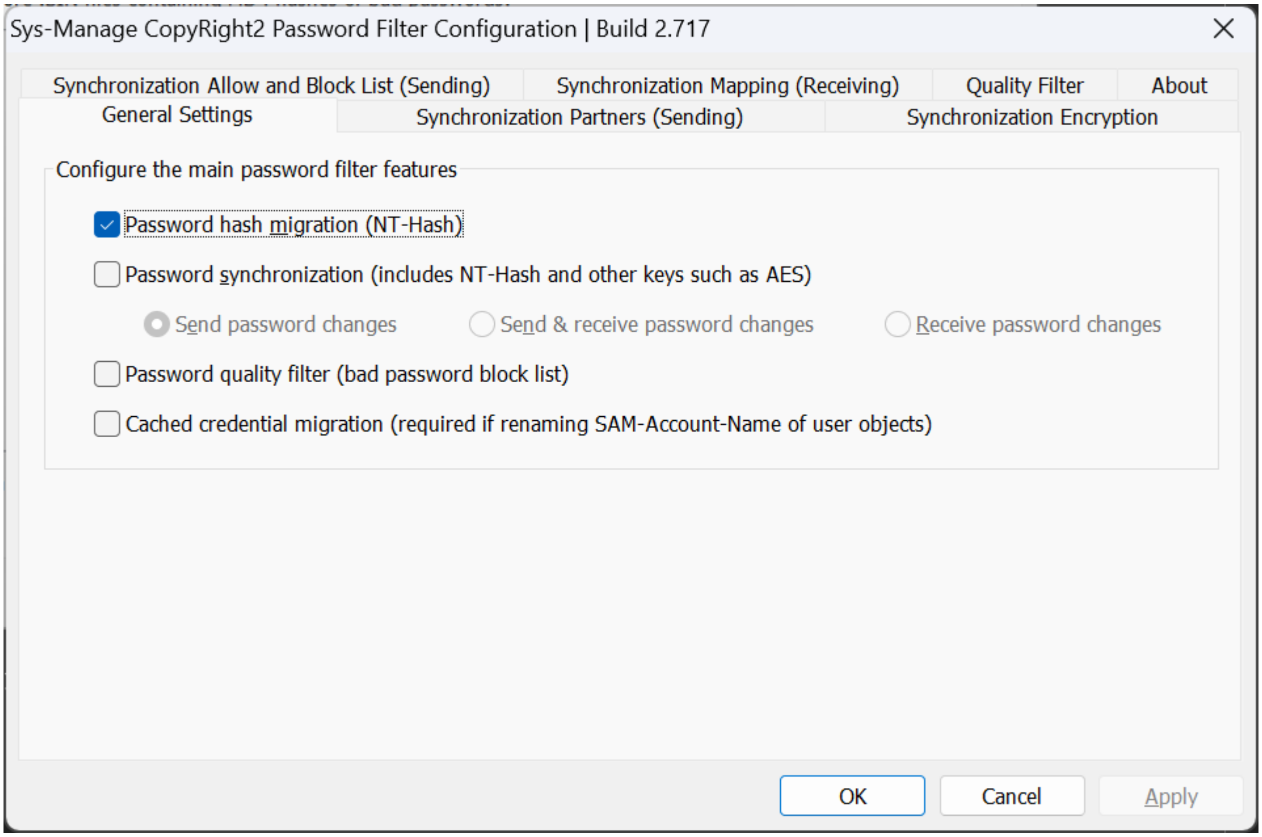
Password Filter Configuration

Configuration

After installing the password migration filter, you will find a shortcut on the desktop labelled “Password Filter Configuration” that will launch a configuration tool.

General Settings

In the “General Settings” page you can turn on and off specific password migration filter features. By default, it has the NT-Hash migration option selected. To use the advanced password synchronization option, please enable the second option along with the corresponding direction (send, receive or send & receive in case of a two-way replication).


Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717
Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About
General Settings
Synchronization Partners (Sending)
Synchronization Encryption
OK
Cancel
Apply

Configure the main password filter features

☑ Password hash migration (NT-Hash)

□ Password synchronization (includes NT-Hash and other keys such as AES)

● Send password changes ○ Send & receive password changes ○ Receive password changes

□ Password quality filter (bad password block list)

□ Cached credential migration (required if renaming SAM-Account-Name of user objects)

Additionally, you can enable the password quality filter or the cached credential migration feature.

If the password quality filter is enabled, it loads predefined lists of bad password hashes to block. You can create these lists from plain-text passwords by using PwdFilterCli.exe with the /compile parameter. Copy the resulting .BIN files to C:\ProgramData\Sys-Manage\CopyRight\PwdFilter\Config and then assign them on the Quality Filter page.

If cached credential migration is enabled, it allows migrating cached credentials stored on workstations during Computer & Profile Migrations in the one scenario where it is required: when users' sAMAccountName values are renamed (based on a mapping file) and cached logons must keep working (for example for VPN or Wi-Fi authentication). Cached credentials are salted with the user's sAMAccountName, so they would stop working after a rename if not updated. This does not require the clear-text password, because cached credentials are derived from the NT hash (a "hashed hash"). If enabled, the client requests updated cached-credential material from the target domain controller for the affected users whose profiles are being migrated.

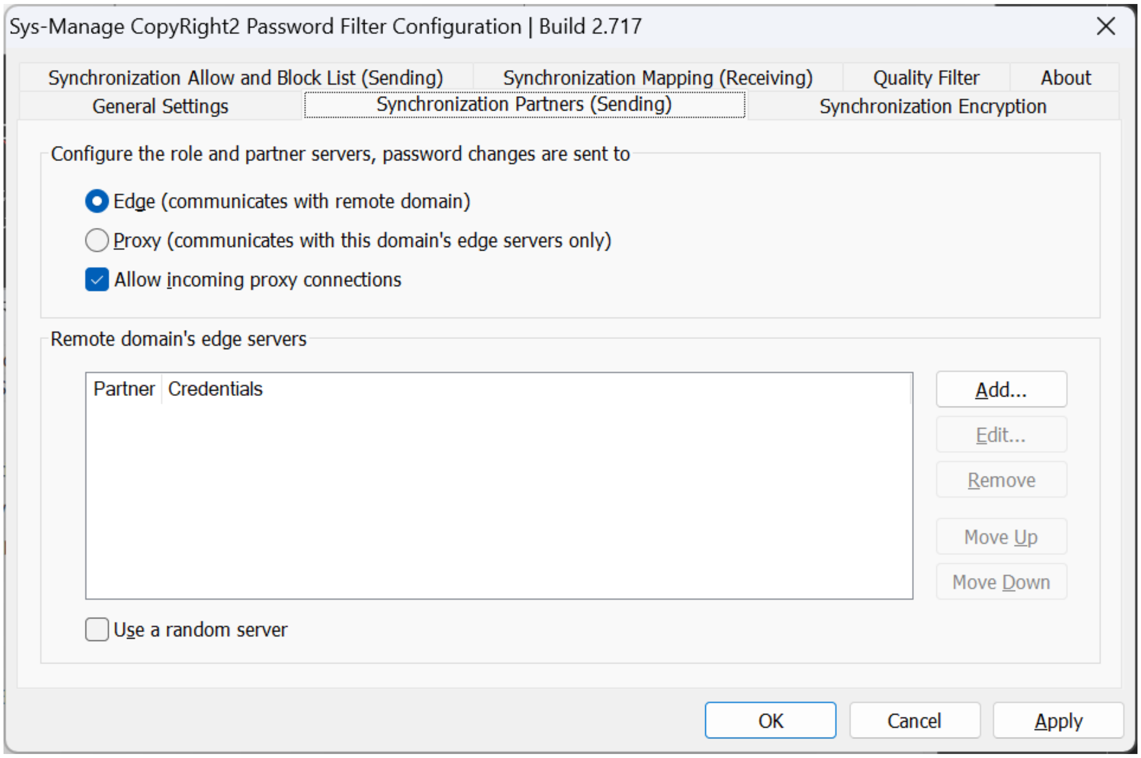
Synchronization Partners

On the Synchronization Partners page, you configure whether the system acts as an edge server or a proxy server, and you specify the list of servers that it should forward password change events to.

If the system is configured as an edge server, the list contains the remote servers acting as edge servers in the remote domain.

If the system is configured as a proxy server, the list contains the edge servers in the local domain.

The Allow incoming proxy connections option controls whether an edge server exposes the RPC interface that domain controllers in the same domain can call to relay password change events to the edge server.



Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717

Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About
General Settings
Synchronization Partners (Sending)
Synchronization Encryption

Configure the role and partner servers, password changes are sent to

● Edge (communicates with remote domain)

○ Proxy (communicates with this domain's edge servers only)

☑ Allow incoming proxy connections

Remote domain's edge servers

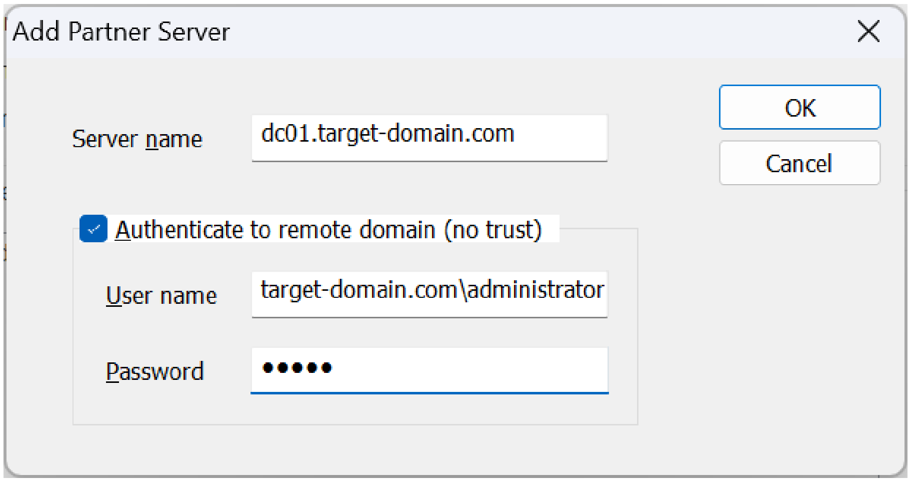
Partner	Credentials

Add...
Edit...
Remove
Move Up
Move Down

☐ Use a random server

If there are no domain controllers configured as proxies in the source domain, this option can and should be turned off.

To add a partner, click Add… and enter the computer name, preferably as an FQDN.



Add Partner Server

Server name: dc01.target-domain.com

☑ Authenticate to remote domain (no trust)

User name: target-domain.com\administrator

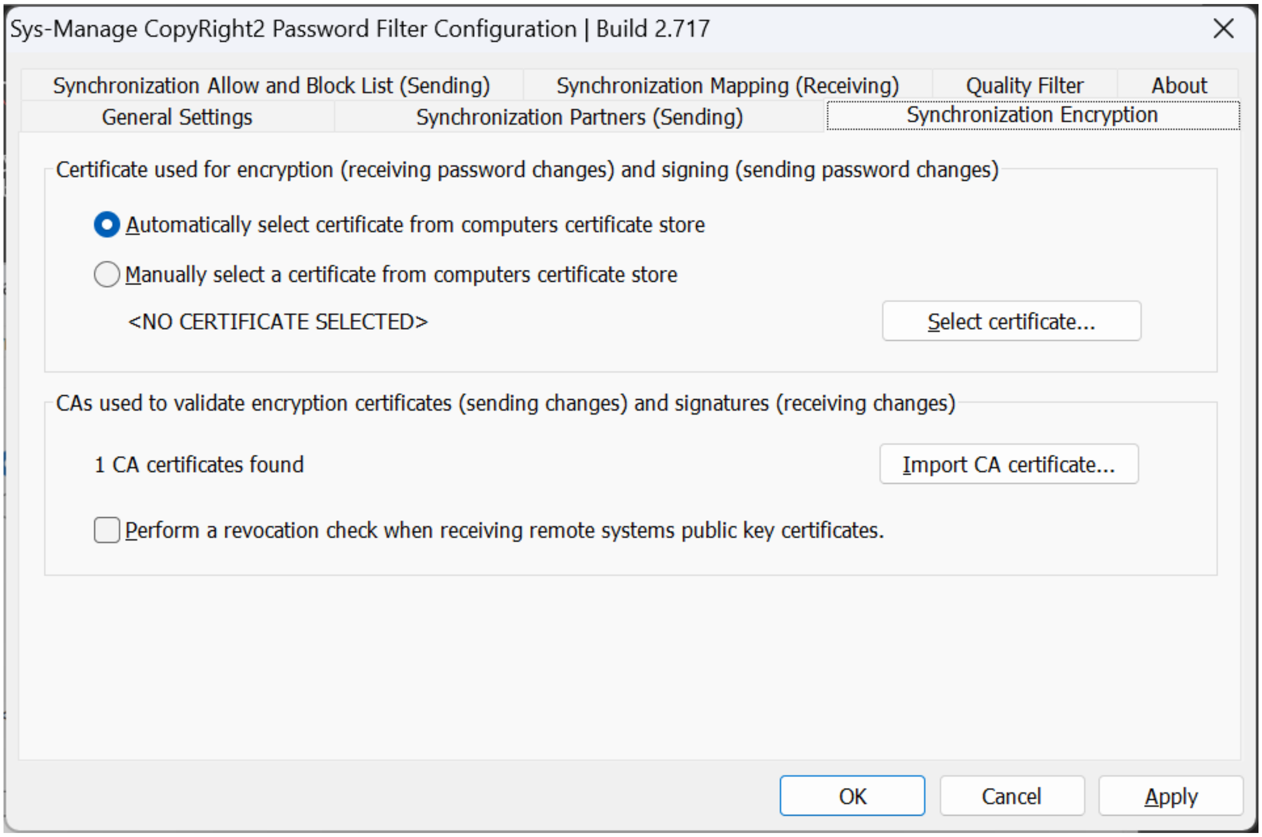
Password: •••••

In case the system is an edge server, communicating with the receiving domain’s edge server(s), you will additionally need to check “Authenticate to remote domain” and provide a security context that is used to update passwords for existing users and, optionally, to create new users. This can be an administrator account or a delegated account with the required permissions. Specify the user name either in the format DNS-DOMAIN-NAME\USER-NAME or as a user principal name (UPN) in the format USER-NAME@FQDN-DNS-DOMAIN-NAME.

If the system is configured as a proxy and communicates with the source domain’s edge server(s), you do not need to enable authentication or provide credentials, because this communication is authorized based on membership in the source domain’s Domain Controllers group, which the proxy DC is a member of.

Synchronization Encryption

On the Synchronization Encryption page, you configure X.509 certificate-based encryption. This page only needs to be configured on edge servers.


Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717
Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About
General Settings
Synchronization Partners (Sending)
Synchronization Encryption
Select certificate...
Import CA certificate...
OK
Cancel
Apply

Certificate used for encryption (receiving password changes) and signing (sending password changes)

● Automatically select certificate from computers certificate store

○ Manually select a certificate from computers certificate store

<NO CERTIFICATE SELECTED>

CAs used to validate encryption certificates (sending changes) and signatures (receiving changes)

1 CA certificates found

□ Perform a revocation check when receiving remote systems public key certificates.

The first setting controls which certificate is used for synchronization traffic. If the system sends password change events, it selects the certificate used to sign outgoing events so the receiver can validate the request. If the system receives password change events, it selects the certificate whose public key is used by the sender to encrypt events for this system.

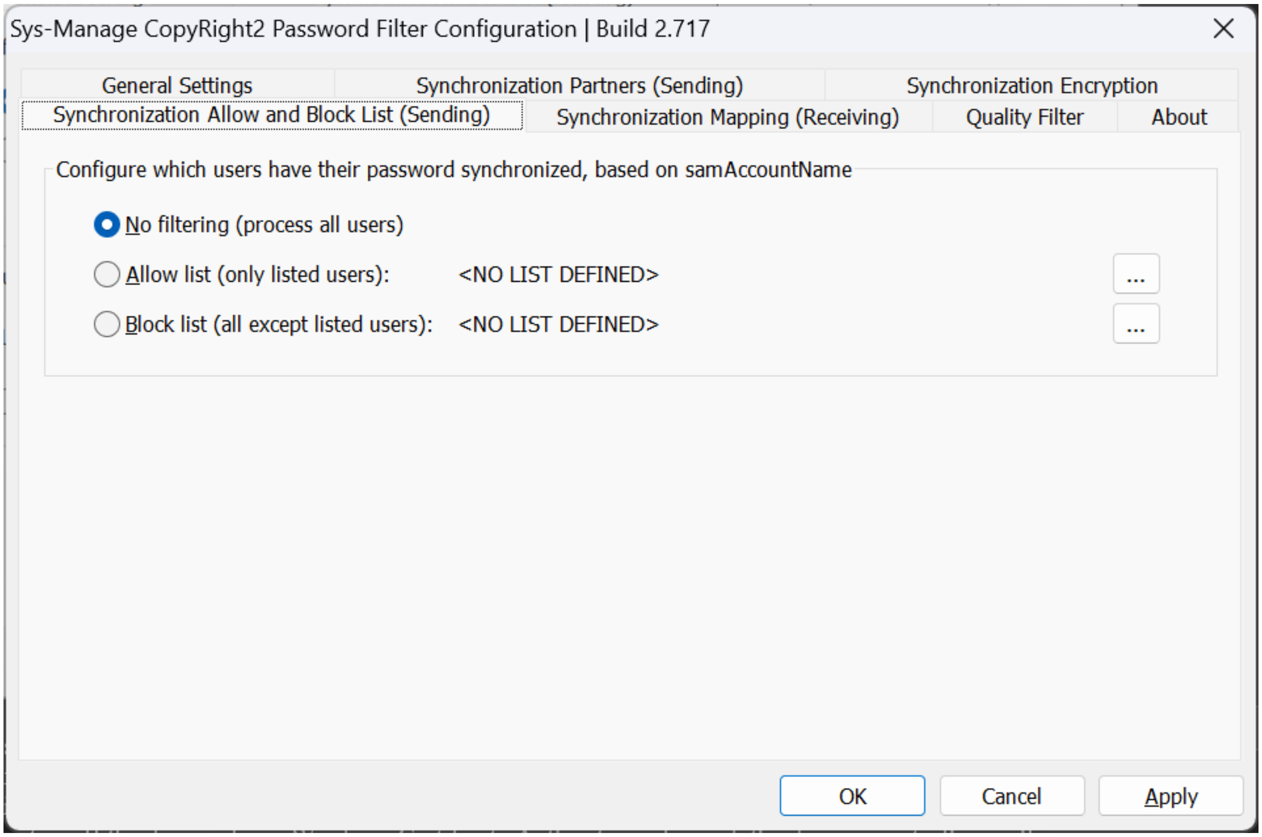
By default, the add-on attempts to automatically find a suitable certificate with an available private key in the computer certificate store. If the domain has a Windows Certificate Authority, domain controllers typically receive a suitable certificate automatically (for example via GPO auto-enrollment). If no CA is available, a self-signed certificate can be used instead.

The second setting controls which certificate authorities are trusted when validating the certificate presented by the remote edge server. Add the CA that issued the remote certificates here, or, if self-signed certificates are used, add the actual X.509 certificate(s) of the remote server(s). This allows the system to validate certificates received from the remote peer.

Optionally, you can enable certificate revocation checking when validating incoming certificates. This requires the network infrastructure to provide access to the revocation information (CRL/OCSP) of the issuing authority.

Synchronization Allow and Block List

In the Synchronization Allow and Block List, you can define lists of sAMAccountName values to control which user accounts' password changes are synchronized. If filtering is not enabled, any user's password change is synchronized according to the configuration.


Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717
General Settings
Synchronization Partners (Sending)
Synchronization Encryption
Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About
...
...
OK
Cancel
Apply

Configure which users have their password synchronized, based on samAccountName

● No filtering (process all users)

○ Allow list (only listed users): <NO LIST DEFINED>

○ Block list (all except listed users): <NO LIST DEFINED>

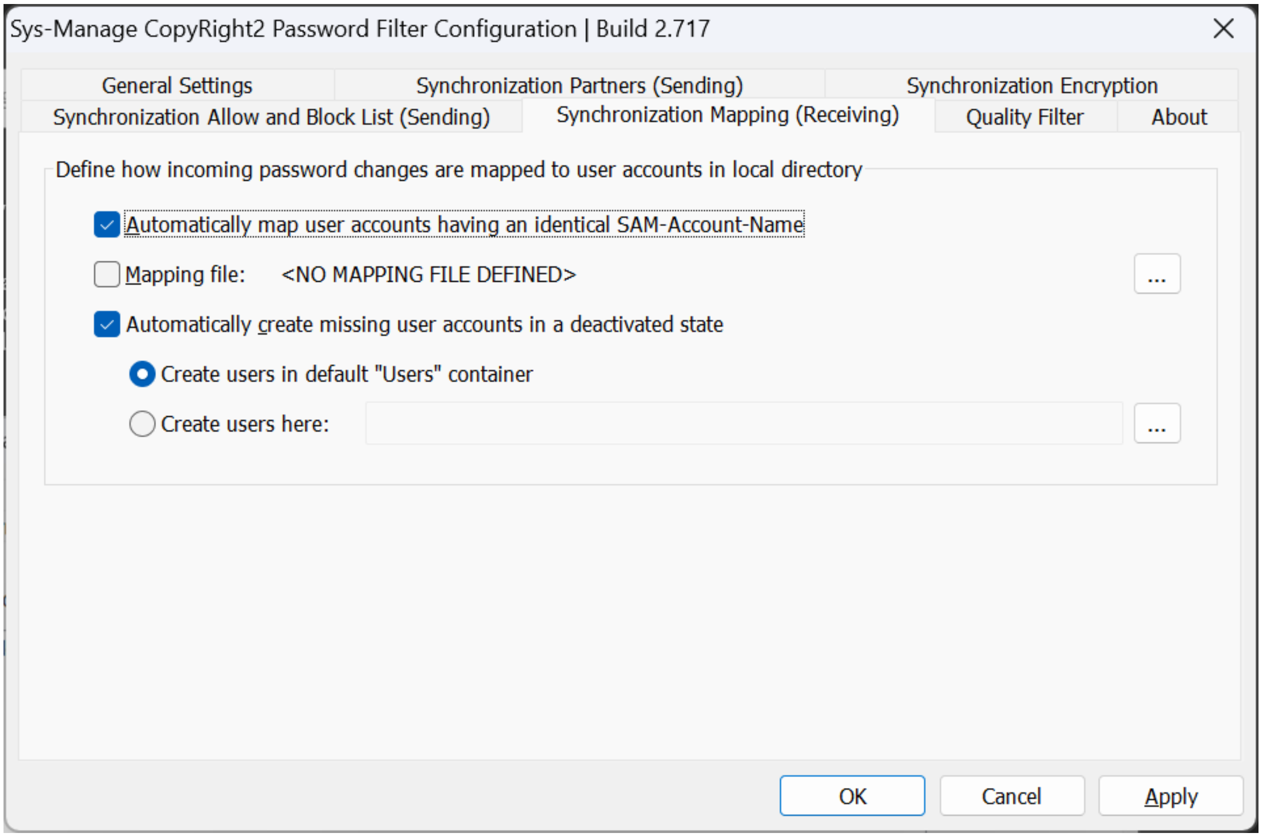
By default, no filtering is applied and the add-on attempts to replicate all password change events.

To assign a new list, copy the text file containing the users' sAMAccountName values (one per line) to "C:\ProgramData\Sys-Manage\PwdFilter\Config", and then select it by clicking the "…" button.

Note: Please ensure that a supplied user allow or block list is encoded either in ANSI or UNICODE (UTF-16LE) format.

Synchronization Mapping

On the Synchronization Mapping page, you define how the software maps password change events to the corresponding target user account.



Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717

General Settings
Synchronization Partners (Sending)
Synchronization Encryption
Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About

Define how incoming password changes are mapped to user accounts in local directory

☑ Automatically map user accounts having an identical SAM-Account-Name

□ Mapping file: <NO MAPPING FILE DEFINED>

☑ Automatically create missing user accounts in a deactivated state

● Create users in default "Users" container

○ Create users here:

By default, user accounts are mapped by identical sAMAccountName values.

Optionally, you can specify a mapping file that defines which sAMAccountName in the source domain corresponds to which sAMAccountName in the target domain. The format of mapping files is described in the CopyRight2 manual in the chapter “CREATING A MAPPING DEFINITION FILE TO REASSIGN PERMISSIONS”.

Note: Please ensure that a supplied mapping file is encoded either in ANSI or UNICODE (UTF-16LE) format.

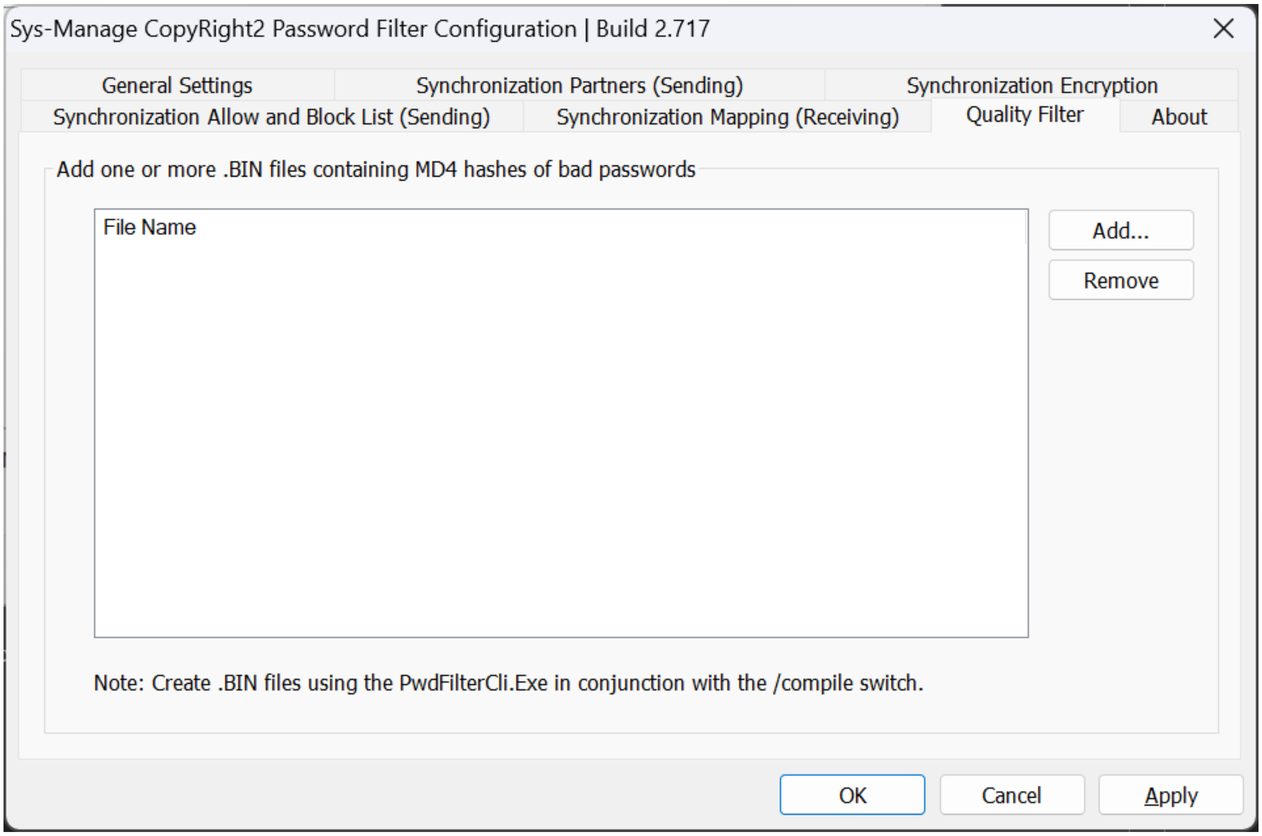
The “Automatically create missing user accounts” option controls whether the software should automatically create a user in the target domain when it receives a password change request for a user that does not yet exist. If enabled, the user is created in a disabled state before the password is set. This ensures the account cannot be used until the actual user migration is performed through a CopyRight2 User and Group Migration job.

If the “Automatically create missing user accounts” option is enabled, you can additionally configure the OU/container where the new user objects should be created.

Quality Filter

On the Quality Filter page, you can assign one or more binary files containing hashes of known bad passwords. These binary files can be generated from plain-text password lists.

If an attempt is made to set a user’s password to a password contained in one of these lists, the domain controller rejects the request (as a password policy violation).



Sys-Manage CopyRight2 Password Filter Configuration | Build 2.717

General Settings
Synchronization Partners (Sending)
Synchronization Encryption
Synchronization Allow and Block List (Sending)
Synchronization Mapping (Receiving)
Quality Filter
About

Add one or more .BIN files containing MD4 hashes of bad passwords

Note: Create .BIN files using the PwdFilterCli.Exe in conjunction with the /compile switch.

To add a BIN file, you can click on the “Add…” button. To remove a file from the list, you can use the “Remove” button. Please copy the BIN file to “C:\ProgramData\Sys-Manage\PwdFilter\Config”, and then select it by clicking the “Add…” button.

About

On the About page, you can view version information for the installed software.

You can also check the activation status and activate the software by clicking Activate this system… and entering an activation key.

For more information about activation, see the CopyRight2 manual chapter “LICENSING”.

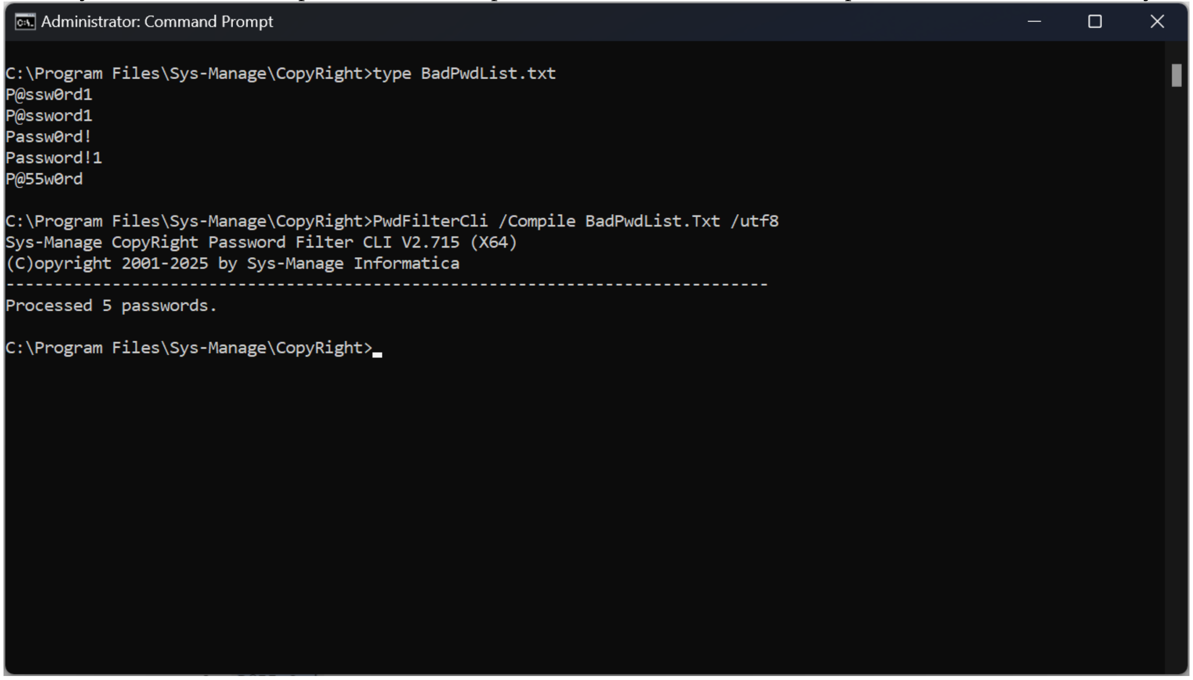
Compiling Passwords into Binary Hash Files

To compile an existing list of passwords into a binary file that can be added to the password quality filter, you can use the PwdFilterCli.Exe executable and its “/Compile” parameter.

It has the following syntax: /Compile {Input-File} [/ANSI | /UNICODE | /UTF8]

Parameter	Description
{Input-File}	Text file containing passwords, one per line, cr/lf delimited
/ANSI	The input file in encoded in ANSI character encoding.
/UNICODE	The input file in encoded in UNICODE (UTF16-LE) character encoding.
/UTF8	The input file is encoded in UTF8 character encoding.

Below you can see an example of how to compile a UTF-8 encoded list of bad passwords into a .BIN binary file:



```
C:\Program Files\Sys-Manage\CopyRight>type BadPwdList.txt
P@ssw0rd1
P@ssword1
Passw0rd!
Password!1
P@55w0rd

C:\Program Files\Sys-Manage\CopyRight>PwdFilterCli /Compile BadPwdList.Txt /utf8
Sys-Manage CopyRight Password Filter CLI V2.715 (X64)
(C)opyright 2001-2025 by Sys-Manage Informatica
-------------------------------------------------------------------------------
Processed 5 passwords.

C:\Program Files\Sys-Manage\CopyRight>
```

After conversion, the BIN file can be added in the Quality Filter page of the password filter configuration tool.

Reference / Technical Background

Supported Password Hashes and Keys

The Password Synchronization & Migration Add-On synchronizes password updates into the target domain so that the correct Kerberos key material for advanced encryption types (including AES) is generated.

The supported password hashes and authentication keys are listed below.

NT Password Hash (MD4)

The NT password hash is derived from the user’s clear-text password using the MD4 algorithm.

It is used for:

- NTLM authentication
- Kerberos authentication using legacy encryption types

Migration of the NT password hash allows users to authenticate in the target environment using their existing passwords without requiring an immediate password change.

NT password hash migration is supported for:

- Active Directory domain user accounts
- Local user accounts on domain member systems
- Local user accounts on workgroup mode systems

Kerberos Authentication Keys (Advanced Encryption Types)

Active Directory supports Kerberos authentication using multiple encryption types (etypes).

Modern environments typically rely on advanced encryption types that do not depend on the NT password hash.

The Password Synchronization & Migration Add-On supports password synchronization into the target domain so that the correct target-domain Kerberos key material for advanced encryption types (including AES) is generated:

- Kerberos AES-128
- Kerberos AES-256

Kerberos authentication keys are stored as separate key material from the NT hash (different derived keys/fields), even though all are ultimately derived from the same password.

Password synchronization for AES-ready / RC4-disabled environments is supported for:

- Active Directory domain user accounts

Kerberos authentication keys do not apply to local user accounts on domain member systems or workgroup mode systems.

Windows automatically selects the best available Kerberos encryption type. If no AES keys are present (for example because only the NT hash was migrated), Windows falls back to RC4 if RC4 is permitted in the target environment.

Based on this behavior, you can introduce RC4-less Kerberos authentication gradually in one of two ways:

Wait until all migrated users have changed their password at least once in the target domain (so AES keys are generated) and then disable RC4.

Force migrated users to change their password once at first logon with the target user account, ensuring AES keys are generated immediately. This requires RC4 to remain enabled until users can authenticate and complete the password change.

Relationship Between Password Hashes and Kerberos Authentication Keys

The NT password hash and Kerberos authentication keys are independent credentials.

- Migrating the NT password hash does not automatically create Kerberos authentication keys for advanced encryption types

- Kerberos authentication keys for advanced encryption types are generated when a password is set or changed. In cross-domain migrations, this can be achieved by replicating password changes into the target domain so that the correct target-domain key material (including AES) is generated

- The availability of Kerberos authentication depends on the presence of suitable encryption keys for the configured encryption policy

The selected migration scenario determines which password hashes or authentication keys are migrated and how authentication is performed in the target environment.

Password Migration Mechanisms

Depending on the environment, different mechanisms are used.

For NT password hash migration, the required components can be deployed automatically to remote systems during job execution or installed permanently on source and/or target as a Windows password filter. The permanent installation method is recommended when code injection into LSASS is restricted by third-party security solutions or to improve the migration performance (no deployment required if filter is already running).

When migrating passwords into environments that require advanced Kerberos encryption types (AES), a different method is used. In this case, the password filter component is installed permanently on all writable Windows domain controllers of the source domain and on the designated edge domain controller(s) in the target domain and additional configuration is applied using the CopyRight2 Password Filter Configuration tool.

Scenario	**Add-On Required (where main program is installed)**	**Password Filter required**
NT-Hash Migration	✓	✗ (Optional)
NT-Hash Migration with EDR/Security Solution blocking Code Injection	✓	✓ (Source and/or Target)
Password Synchronization (Password Filter) AES-ready / RC4-disabled environments	✗ (Optional)	✓ (All writable source DCs and at least one (preferably two) target edge DCs)

When the Password Filter feature is installed and enabled using the Password Filter Configuration Tool, the required components are installed automatically.

Installing the Password Filter places the required binaries on the system. The filter is loaded by LSASS when it is registered/enabled and the system is restarted (as with standard Windows password filters).

If the system is not configured to capture local password changes, the Password Filter is still loaded by LSASS but operates in a disabled mode: it ignores local password-change notifications and does not queue them for processing.

In that case, the Password Filter Service remains active and receives password-change events from the source side and applies them according to the configured partners.

Password Hashes, Kerberos and Encryption Types

Windows authentication relies on different password-related credentials depending on the authentication protocol and the configured security policy. Understanding how these credentials are used is essential when selecting the appropriate password migration scenario.

This chapter describes how NT password hashes and Kerberos authentication keys are used by Windows and Active Directory and why different migration approaches are required in modern, security-hardened environments.

NT Password Hash Usage

The NT password hash is derived from the user's clear-text password using the MD4 algorithm.

It is used for:

- NTLM authentication
- Kerberos authentication when legacy encryption types are enabled

Historically, Kerberos authentication in Active Directory relied on encryption types that are directly based on the NT password hash. This allowed Kerberos authentication to function without requiring additional password-related key material.

As a result, migrating the NT password hash alone was sufficient in many legacy and mixed-mode environments.

Kerberos Authentication and Advanced Encryption Types

Modern Active Directory environments support Kerberos authentication using advanced encryption types (etypes) that are not based on the NT password hash.

These encryption types provide stronger cryptographic protection and are increasingly required in security-hardened environments.

Kerberos authentication using advanced encryption types requires dedicated Kerberos authentication keys that are stored separately from the NT password hash.

If suitable Kerberos authentication keys are not available for the configured encryption policy, Kerberos authentication fails, even if the NT password hash is present.

Kerberos Key Derivation and the Role of the Salt

Kerberos authentication keys for advanced encryption types are derived from the user's password in combination with additional parameters, including a Kerberos-specific salt.

In Active Directory environments, the salt is derived from the account's Kerberos identity information, such as:

- The Kerberos realm (typically the AD DNS domain name in uppercase, e.g., CORP.EXAMPLE.COM)
- The account's Kerberos principal identity in that realm (for example the username portion of the principal)

Note: The effective salt is based on the account's Kerberos identity in that domain (for example realm + principal), which is why AES key material from the source domain does not remain valid after a cross-domain migration unless the password is updated in the target domain.

When a user account is migrated to a different domain, the Kerberos realm changes and previously derived Kerberos authentication keys are no longer valid for the target domain.

For this reason, Kerberos authentication keys must either be generated in the target domain by setting/changing the password, or the password change must be replicated into the target domain so the correct target-domain key material (including AES) is generated.

This behavior is inherent to Kerberos key derivation and applies in particular to AES-based Kerberos keys in Active Directory, which are realm-specific due to the salt.

Legacy Encryption Types and RC4 Deprecation

Legacy Kerberos encryption types rely on the NT password hash and have historically been enabled by default in Active Directory environments.

Due to known cryptographic weaknesses, these legacy encryption types are increasingly disabled in modern environments.

When legacy encryption types are disabled:

- Kerberos authentication requires advanced encryption types
- The NT password hash alone is insufficient
- Accounts without suitable Kerberos authentication keys cannot authenticate using Kerberos

This makes NT-hash–only password migration unsuitable in environments where legacy encryption types are disabled.

Password Migration Scenarios

The Password Synchronization & Migration Add-On supports multiple password migration approaches. The right approach depends mainly on:

- Account type (local accounts vs. Active Directory users)
- Target security policy (whether Kerberos RC4 / legacy etypes are still allowed during the migration)
- Operational goal (one-time migration vs. continuous synchronization)

This chapter helps you select the appropriate scenario and shows which components must be deployed where.

Quick Selection Guide

Use the following decision points:

Are you migrating local user accounts?
→ Use Scenario A: NT Password Hash Migration for Local User Accounts

Are you migrating Active Directory users and RC4 is still allowed during migration?
→ Use Scenario B: NT Password Hash Migration for Active Directory Domain Users

Optionally use Scenario C if you want faster AES key readiness.

Do you need Kerberos AES keys immediately, or is RC4-disabled (or will be disabled early)?
→ Use the Password Filter–based synchronization method (covered in Password Synchronization (Password Filter) and Scenario D later in this chapter).

Component Deployment by Scenario

The matrix below shows, which scenario requires which components to be installed and where:

Scenario	CopyRight2 Add-On on system where job is being run	Password Filter on Source	Password Filter on Target	Notes
A) Local accounts – NT hash migration	✓	Optional (only if needed)	Optional (only if needed)	Kerberos not applicable
B) AD users – NT hash migration (RC4 allowed)	✓	Optional (only if needed)	Optional (only if needed)	AES keys appear only after password change
C) AD users – NT hash + forced password change (RC4 allowed)	✓	Optional (only if needed)	Optional (only if needed)	Requires RC4 until users complete first logon/password change
D) Password Synchronization (Password Filter),	Optional	all source DCs	target edge DCs	Requires filter configuration; supports one-

AES only / RC4 off				way/two-way and proxy/edge roles

Note: If a third-party security solution blocks the default method (e.g., restrictions around LSASS/code injection), you can install the Password Filter on the source and/or target system to perform password operations locally.

Scenario A: NT Password Hash Migration for Local User Accounts

Goal:

- Migrate local account passwords so users can log on with their existing password immediately.

Applies to:

- Local user accounts on domain member systems
- Local user accounts on workgroup systems

What happens:

- The NT password hash is migrated to the target system.
- Users can authenticate on the target system using their existing password.
- No password reset or password change is required.

Notes:

- Kerberos (and therefore AES/RC4) does not apply to local user accounts.

Recommended when:

- You are migrating local accounts and want the simplest, least disruptive approach.

Scenario B: NT Password Hash Migration for Active Directory Domain Users (RC4 Allowed)

Goal:

- Migrate AD user passwords without forcing password changes, while allowing a transitional period where RC4 is still permitted.

Applies to:

- Active Directory domain user accounts
- Environments where legacy Kerberos encryption types (e.g., RC4) are still enabled during migration

What happens:

- The NT password hash is migrated to the target domain.
- Users can authenticate using their existing password.
- Kerberos may fall back to legacy encryption types as long as they remain permitted.
- AES keys are generated only after the user changes their password in the target domain.

Notes:

- This scenario is “fully completed” only after users have changed their password at least once in the target domain (naturally or via policy), because that is when domain-specific Kerberos keys are refreshed.
- Accounts with “Password never expires” may keep using legacy etypes indefinitely unless their password is changed.
- Do not disable RC4 until you have a strategy to ensure all required users have generated AES keys (see the soft-introduction options in the Technical Background section).

Recommended when:

- RC4 can remain enabled during the transition and you want minimal user disruption.

Scenario C: NT-Hash Migration with Forced Password Change at First Logon (RC4 Allowed)

Goal:

- Speed up AES readiness by ensuring users generate fresh Kerberos key material early.

Applies to:

- Active Directory domain user accounts
- Environments where RC4 is still permitted during the transition but will be disabled after users have generated AES keys (via a forced first-logon password change)
- One-time migration scenarios where users can perform an interactive logon to complete the forced password change

What happens:

- The NT password hash is migrated.
- Users can authenticate using their existing password.
- Users are required to change their password at first logon.
- The password change generates domain-specific Kerberos key material (including AES keys) immediately.

Notes:

- Enable “Must change password” in the Settings page of the User and Group Migration job.
- This approach requires RC4 to remain enabled until users can authenticate and complete the password change (otherwise first logon may fail if AES keys are not present yet).
- Not suitable for all accounts:
  - Service accounts
  - Restricted logon accounts
  - Accounts that cannot perform interactive logon
- Recommended if you want faster AES key availability but can tolerate a controlled first-logon password change.

Recommended when:

- You want a soft introduction of RC4-less Kerberos and need AES keys generated quickly for migrated users.

Scenario D: Password Synchronization with Filter in AES-ready / RC4-disabled environments

Goal:

- Support environments where Kerberos AES must work immediately (including RC4-disabled targets) and/or where passwords must be synchronized continuously.

Applies to:

- Active Directory domain user accounts
- One-way or two-way synchronization between environments

What happens:

- The Password Filter captures password changes on writable domain controllers and replicates them to the target domain.
- This ensures the correct target-domain Kerberos key material (including AES) is generated.

Notes:

- Install on all writable source domain controllers (password changes can occur on any writable DC).
- Configure at least one (preferably two) edge servers per domain for redundancy.
- Requires configuration using the Password Filter Configuration tool (partners, encryption trust, mapping, filtering, etc.).

Recommended when:

- RC4 is disabled (or must be disabled early) and Kerberos must work immediately with AES in the target domain.
- You need ongoing synchronization (one-way or two-way).
- You want password quality filtering at password-set time.

Network Ports and Firewall Considerations

NT-Hash Migration

For NT password hash migrations, CopyRight2 uses a centralized client/server communication model where the CopyRight2 server initiates all network connections.

Communication pattern:

- CopyRight2 Server → Source System
- CopyRight2 Server → Target System

Network requirements:

- **TCP 445 (SMB)** must be permitted:
    - from the CopyRight2 server to the source system
    - from the CopyRight2 server to the target system

This communication is used to retrieve NT password hashes from the source system and to apply them to the target system during migration jobs. The password hashes are processed in memory only and are not persisted to disk by CopyRight2.

Password Filter based Synchronization

Password synchronization traffic between proxy and edge systems uses RPC over named pipes, transported via SMB.

The following network connectivity is required:

- TCP 445 (SMB) between:
    - Proxy server(s) and edge server(s) within the same domain
    - Edge server(s) across domains in cross-domain scenarios

No additional RPC endpoint mapper or dynamic RPC ports are required for password synchronization.

Domain controllers do not require cross-domain network connectivity unless they are explicitly configured as proxy or edge servers.

All password change events are encrypted using X.509 certificates as described in the Synchronization Encryption section.

The password change payload is encrypted in the Password Filter when the event is captured and can be decrypted only by the target domain’s edge server that has access to the corresponding X.509 private key.

Troubleshooting

Below is a list of known problems and solutions.

Troubleshooting Password Synchronization (Password Filter)

When troubleshooting password synchronization issues, the Password Migration Filter exposes multiple diagnostic points that allow you to determine whether password changes are captured, queued, and successfully relayed to the target environment.

Windows Event Log

The Password Migration Filter writes informational and error events to the Windows System Event Log on the system where the filter is installed.

These events indicate whether password change notifications are received, processed, or rejected by the filter.

Password Filter Service Log

The Password Filter service (CrPwdFilterSvc.exe), located in “C:\Program Files\Sys-Manage\CopyRight”, writes a service log file named: CrPwdFilterSvc.log

This log provides detailed information about:

- Receipt and processing of password change events.
- Communication with synchronization partners
- Encryption, authentication, and transmission errors

Password Change Queue

Successfully captured password change events are written to an on-disk queue before being forwarded to the target system.

The queue is located at: “C:\ProgramData\Sys-Manage\CopyRight\PwdFilter\Queue”

Each entry represents a pending password synchronization request.

Failed Synchronization Attempts

If the Password Filter service is unable to relay a queued password change event to the target environment (for example due to network connectivity, authentication, or encryption errors), the request is moved automatically to the following subfolder: “C:\ProgramData\Sys-Manage\CopyRight\PwdFilter\Queue\Bad”

Entries in the Bad folder indicate password change events that were captured successfully but could not be delivered.

Recommended troubleshooting steps

- Review the System Event Log for Password Filter–related events.
- Inspect CrPwdFilterSvc.log for communication, encryption or other errors.
- Verify that new password change events appear in the Queue folder.
- If entries are moved to the Queue\Bad folder, verify:
    - Network connectivity and firewall rules
    - Synchronization partner configuration
    - Certificate trust and encryption settings

Known Issues

Error Message during Installation

A message box appears during installation reading “Error reading from file {path to a file}. Verify that the file exists and that you can access it”.

Solution: Please try to move the MSI installation file to a different location. This can occur because of the folder depth or because of security reasons. Please verify the MSI file’s security permissions.

Error 2012 or 2013 (Win32Err=5) Access Denied During NT-Hash Migration

In environments protected by third-party security solutions, password migration may fail with internal error 2012 or 2013, typically accompanied by Win32 error 5 (Access Denied).

In this case, install the CopyRight2 Password Migration Filter locally by running the add-on installer on the source and/or target system of the migration job, depending on where the error occurs. Installing the filter requires a system reboot.

The Password Migration Filter is supported on domain controllers, domain member systems, and workgroup-mode systems.

As an alternative, you may temporarily disable or remove the blocking security component during the password migration. This approach should be considered a last resort.

Error 3500 (Win32Err=87) During NT-Hash Migration

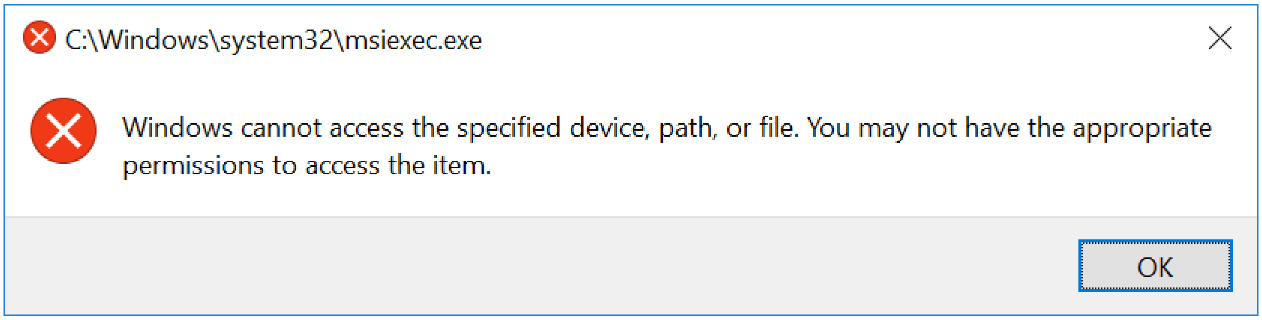
Please check if you are running some kind of Anti-Virus or Host Intrusion Prevention system on the target server. If yes, please have a look at the solutions log files. You may have to add an exception for CopyRight2’s CrPwdSvc.Exe file or alternatively install the Password Filter instead.

Product Uninstallation from Settings -> Apps & Features Fails if UAC is Disabled

To work around the issue, you can either logon with a different user account that has UAC enabled or alternatively use the classic control panel -> Programs and Features.

This issue is a known limitation in Windows that arises when User Account Control (UAC) is disabled. This can happen either if UAC is turned off system-wide or if you log in using the built-in Administrator account, which automatically disables UAC for its session. The root cause appears to be a dependency between Windows' new Settings app and UAC.

When attempting to uninstall, the following error message may appear:



C:\Windows\system32\msiexec.exe

Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.

To resolve this issue, you can either:

1) Log in with a different user account that has UAC enabled, or

2) Use the classic Control Panel -> Programs and Features to complete the uninstallation process.

Contacting Support

Please specify the following information when contacting support:

1. Your product and build number (visible in about dialog, shown if you click on the blue question mark within the main application window)
2. Your source server operating system version, service pack level and processor architecture (x86 or x64)
3. Your destination server operating system version, service pack level and processor architecture (x86 or x64)
4. The role of the source server. Is it a domain member or a domain controller or in workgroup mode?
5. The role of the destination server. Is it a domain member or a domain controller or in workgroup mode?
6. The log file if applicable. CopyRight2's log file is located in the program's installation folder having the same name as the copy job with a ".LOG" file extension.
7. The copy job definition file if applicable. The copy job definition file, containing the settings of the copy job, is located in the CopyRight2 installation folder having the same name as the copy job with a ".JOB" file extension.

Our support might ask you for additional required information after receiving your support request.

Contact Information

If you should have further questions regarding the product or its documentation, please feel free to contact us any time:

By eMail:

Support@Sys-Manage.Com

By phone / fax:

Phone: +1 (408) 345-5199
Phone: +1 (360) 227-5673
Phone: +44 (0) 8455273028
Phone: +49-(0)69-99999-3099
Phone: +34-810 10 15 34
Fax: ++49-69-99999-3083