Quest

Password Sync Set Up

Quick Start Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Password Sync Set Up – Quick Start Guide
Updated – October 2024

Contents

Introduction

The goal of this guide is to provide a step-by-step walk through of how-to setup Real Time Password Synchronization for user objects between your On-Premises Active Directory environments. Directory Sync will monitor source Active Directory password changes in real time and synchronize the changes to matched or newly created user objects in the target Active Directory.

To set up Directory Sync for Real Time Password Synchronization, source user objects must be matched to existing or newly created user objects in the target environment. To accomplish this, four (4) configurations must be completed prior to the first synchronization.

1. Set up Environments
2. Set up Local Agents
3. Set up Templates
4. Set up Workflows

The next section will provide the list of requirements needed to successfully Synchronization Password between two Active Directory environments.

Requirements

In order to facilitate the Real Time Password Synchronization, the following is a list of minimum requirements to get set up using Directory Sync with your On-Premises Active Directory.

Preparing the Source and Target Domains

- ADMIN$ must be accessible on the domain controller from the Directory Sync agent server.
- Any third-party anti-virus program that prevents access the LSASS process may need to be updated with a whitelist entry for the Password Sync executable.
- The RC4 encryption (Rivest Cipher 4 or RC4-HMAC) is an element of Microsoft Kerberos authentication that Quest migration products require to sync Active Directory passwords between Source and Target environments. Disabling the use of the RC4 protocol enabled makes password syncing between environments impossible.

  Beginning on November 8, 2022 Microsoft recommended an out of band (OOB) patch be employed to set AES as the default encryption type. The enabling and disabling use of the RC4 encryption protocol has potential impact beyond the function of password syncing of Quest migration tooling and should be considered carefully.

Account Permissions

- One (1) Local Administrator Account for each Microsoft Forest and/or Domain that has permissions to create, update or delete depending on the scope of your Directory Sync workflows.
- The Password Sync functionality requires that either a domain admin role or built-in admin role be granted to the service account.

The next section will provide a step-by-step guide on how to set up Password Synchronization for Active Directory environments.

Setup

This section provides a step-by-step guide on how to set up Password Synchronization for Microsoft Active Directory Environments.

Setup Environments

To begin at least two (2) Active Directory environments must be configured in Directory Sync. At the end of this section there will be two (2) Active Directory environments fully configured.

An environment is an end-point connection that can control the scope of objects read. This guide will walk through how to create the source and target active directory environments.

To create a local AD environment, the following are required

- One (1) Local Administrator Account for each Microsoft Forest and/or Domain that has permissions to create, update or delete depending on the scope of your Directory Sync workflows. This Administrator Account should also meet the Password Synchronization requirement as stated in Account Permissions section above.
- One (1) Windows Server to install and host the Directory Sync Agent.

Follow these steps to setup the cloud environment endpoints.

1. Navigate to Environments
2. Click the New button
3. Click Local as the environment type, Click Next
4. Name the environment, Click Next
5. Name the local agent, Click Next
6. Note the agent registration URL and registration Key for later use, click Finish.
7. Install the agent in the Windows Server that is joined to the local AD domain.
    a. Launch the Directory Sync Agent installation in the target workstation or server
    b. Accept the license agreement and click on next.
    c. Enter the target active directory environment information by providing the following and click next.
    d. Domain Name

e Global Catalog Server

f Username

g Password

h Enter the Directory Sync Registration URL and Agent Registration Key information and click next.

i In the sIDHistory Migration section, you may skip this step if sIDHistory Migration is not part of your project scope.

Note, Refer to On Demand Migration Active Directory User Guide for detailed information about agent installation and set-up requirements.

8 Once the agent is installed and the environment is discovered, click on the Setting button to access the local AD environment setting page.

9 Click on the Organization Unit tab and define the OU filter based on your project scope.

10 Click on the Filters tab and define any LDAP filter based on your project scope.

11 Click Save.

12 Repeat steps 2 – 11 for the next local environment

Prepare source environment for Password Monitoring

Once both local environments are configured, the next step will be to prepare the environment for Real Time Password Synchronization. Password Monitoring must be configured in your source environment.

1 Navigate to Environments

2 Select the source environment where you would like Directory Sync to monitor password changes and click on SETTINGS

3 Click on the PASSWORDS tab

4 Select an agent to use for monitoring password changes from the Agent Drop down list.

5 Click Save, then Click Back.

Enable target environment for Password Changes

Allow Password Changes must be enabled in your target environment for Directory Sync to synchronize Passwords when they are changed in the source environment.

1 Navigate to Environments

2 Select the target environment where you would like Directory Sync to write password changes and click on SETTINGS

3 Click on the PASSWORDS tab

4 Check the checkbox for Allow Password Changes from Other Environments.

5 Click Save, then Click Back.

Setup Templates

Before we can build our workflows, it is best to set up your template(s). Templates contain common mappings and settings used to sync Users, Contacts, Devices, Groups, Office 365 Groups and Microsoft Teams. A template can then be applied to any workflow with a Stage Data step.

For the purpose of this guide, the following template will need to be configured to perform Password Synchronization for User Objects. This guide also assume users will be created in the target Active Directory if there is no match found. Additional templates may be created based on your project requirements.

- Local to Local Password Sync

How to create a Local to Local template

1. Navigate to Templates
2. Click the New button
3. Name and Describe the template
4. In our example, we will name our template “Local to Local Password Sync”, Click Next
5. Click Local as the source environment type, Click Next
6. Click Local as the target environment type, Click Next
7. Set CREATE NEW USERS AS = AS-IS
8. Set UPDATE CREATED USERS= ENABLE
9. Set UPDATE MATCHED USERS= ENABLE
10. Set IF TARGET ADDRESS EXISTS setting as OVERWRITE ONCE.
11. Click Next
12. Set CREATE GROUPS AS = SKIP
13. Set UPDATE CREATED GROUPS = DISABLE
14. Set UPDATE MATCHED GROUPS = DISABLE
15. Click Next
16. Set CREATE NEW CONTACTS AS = DO NOT CREATE
17. Set UPDATE CREATED CONTACTS = DISABLE
18. Set UPDATE MATCHED CONTACTS = DISABLE
19. Click Next
20. Set CREATE NEW DEVICES AS = SKIP
21. Set UPDATE CREATED CONTACTS = DISABLE
22. Set UPDATE MATCHED CONTACTS = DISABLE
23. Click Next
24. Enter a default password, Click Next
25. Leave the SYNCHRONIZE SID HISTORY checkbox unchecked, Click Next
26. Under mappings, we can leave the settings as default or update them based on your project requirements.
27. Click Next

28 Click Finish

Setup Workflows

Follow these steps to create two (2) new workflows for reading, matching, staging and writing data.

How to create a one-way sync workflow for Local to Local

1 Navigate to Workflows

2 Click the New button

3 Name and Describe the template, Click Next

4 Select the all two (2) local Active Directory environments created previously, Click Next

5 Select ONE-WAY SYNC, Click Next

6 The screen presented next will be a pre-configured set of workflow steps to facilitate the flow of object and attributes between your directories.

7 Start at the top of the steps, 1. Read From. Click the Select button

8 Select all two (2) environments created previously the click OK

9 Move to Match Objects

   a This is the step where you will decide on how to match existing objects across your local Active Directories

   b Matching is conducted by pairing sets of attributes to find corresponding objects

   c Your two (2) environments may already have some attributes that can be used to find similar objects between the different directories, or you may need to set some to ensure accurate matching

   d For the purpose of Password Synchronization, it is most important that existing objects are correctly matched to perform Password Synchronization.

10 Click the Select button to configure the Match Objects criteria for your source Local environment and target Local environment

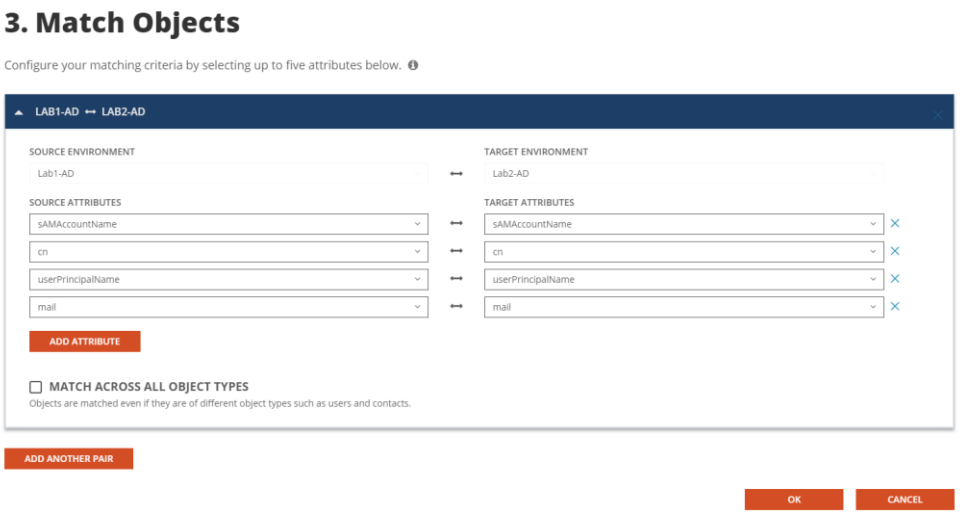

Figure 1: Example Match Objects Criteria

a. Select your source local environment from the drop-down menu

b. Select your target local environment from the drop-down menu

c. Choose your first attribute pairings, we will use WindowsEmailAddress for our first match criteria

d. Choose the sAMAccountName attribute for the source and target fields

e. To add more attribute pairs, click the Add Attribute button

f. Additional pairings are evaluated as “OR” conditions. After the first match is found, the additional pairings are not assessed.

g. In our case we are adding three (3) additional attribute pairings to our criteria

   i. cn – This attribute was added to ensure we can match existing objects based on CN.

   ii. UserPrincipalName – UPN was added to ensure uniqueness of the local part of the address string.

   iii. Mail – This attribute was added to ensure we can match existing objects based on Mail.

   Note: Matching attributes should be reviewed and adjusted based on actual project scope; there isn’t a set matching rule that will fit all scenarios.

h. Ensure Match Across all object types is not checked in this case.

i. There is no need in this guide to Add Another Pair, click OK to close this configuration

11. Drag a Stage Data workflow task from the left panel to the right under the Stage Data task mentioned above. Click the Select button to configure the fourth STAGE DATA workflow task for your target local to source local synchronization rule.

a. Select the “Local to Local Password Sync” template, Click Next

b. Select the source local environment as your source, Click Next

c. Select the target local environment as your target, Click Next

d. Select the default target domain name, Click Next

e. Select the source Organizational Units that will be in scope of the project by click on the ADD OUS button.

f. In the new OU pop-up window, select the OU that will be in-scope, check the INCLUDE ALL SUB OUS checkbox, click OK to close the pop-up.

g. Configure any Stage Data filter you like by double click on the OU in the OUs list, it is highly recommended to setup filter to limit the scope to perform a test on the first sync as part of the validation. Click Next

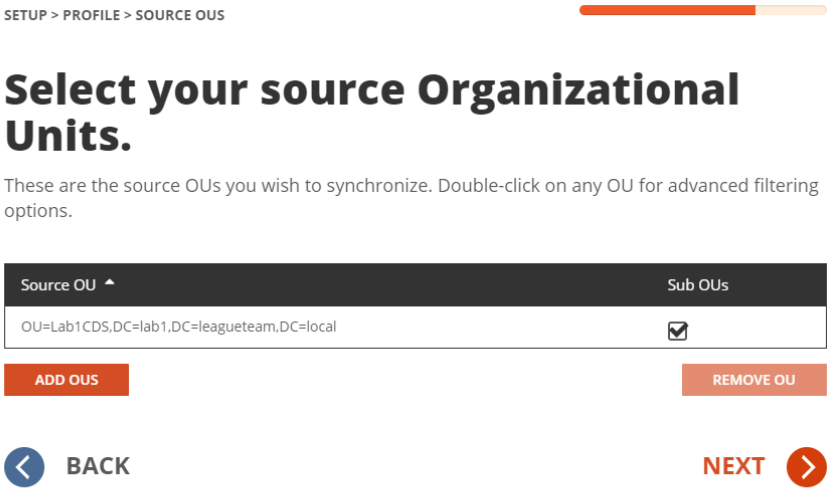

Figure 2: Example Source OU setup.

h Select the default OU for newly created objects for Users, Groups, Contacts, and Devices.

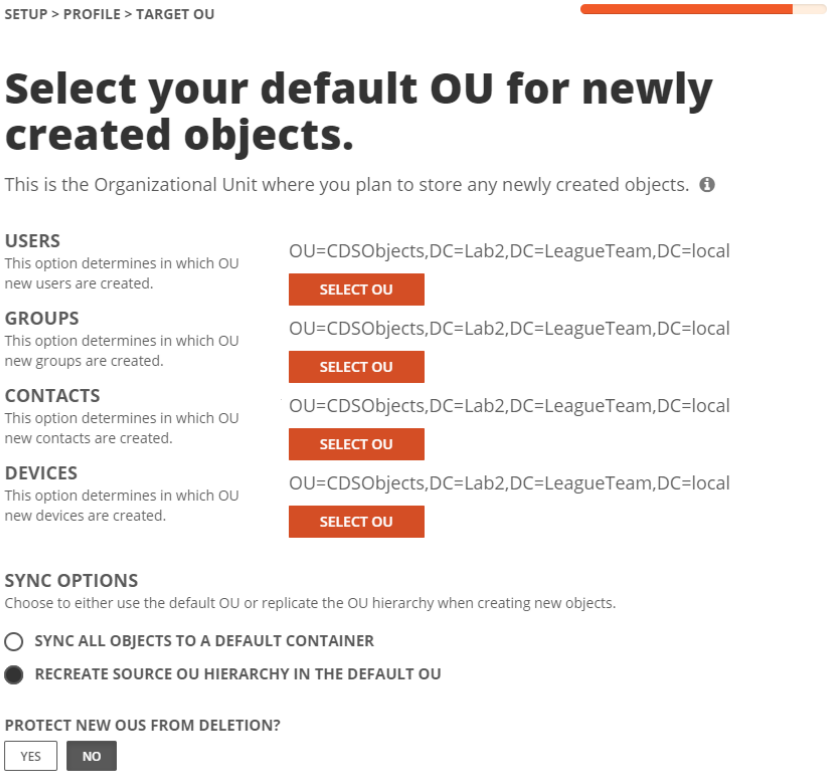

Figure 3: Example Target OU setup.

i Click Finish

12 Click the Select button to configure the WRITE TO workflow task. Ensure the target environment is selected, Click OK

13 Click Next

14. Configure the workflow sync interval, select Manual for now and we can setup a sync schedule once the test sync has completed. Click Next
15. Setup any workflow alert you may wish to configure, for now, Click SKIP
16. Click Finish

Set up Test Objects

Follow these steps to create test objects in the source environment to validate the Password Sync workflow.

1. Setup 2 Users in the source local environment and ensure it is part of the OU filter setup for the Local Environment.
    a. DisplayName: Lab1PWD1
    b. DisplayName: Lab1PWD2

       Description: Matched User
2. Setup a User in the target local environment it is part of the OU filter setup for the Local Environment.
    a. DisplayName: Lab1PWD2
3. Setup a workstation in the target Active Directory environment for Password validation test.

Validating the Workflow

Follow the below steps to perform Real Time Password Sync workflow and validation.

1. Select the workflow configured and click on RUN.
2. Allow the workflow execution to complete.
3. Validate Lab1PWD1 from source local Active Directory will be created in target.
4. Validate Lab1PWD2 from source local Active Directory will match to the existing Lab1PWD2 user in target. Source user's description value will be added to the target user.
5. Select the workflow configured and click on Run again. This is needed to read the newly created object into system, this will allow Directory Sync can update Password for the user object.
6. Make Password changes to both Lab1PWD1 and Lab1PWD2 users.
7. Wait for about 1-2 minutes, navigate to the Environment page and select the source environment. Click on PASSWORD LOGS button and export the logs with default setting.
8. Once the log is downloaded, open the log file and confirm Directory Sync has read the Password changes from source environment. Below are the sample loggings:

5109,171,League-Lab1 Local,"Read: Detected password change for object CN=Lab1PWD1,OU=CDSUsers,OU=CDSObjects,DC=Lab1,DC=leagueteam,DC=local",,5/23/2020 1:53:52 AM

CN=Lab1PWD2,OU=CDSUsers,OU=CDSObjects,DC=Lab1,DC=leagueteam,DC=local",,5/23/2020 1:53:55 AM

9 Select the target environment and click on PASSWORD LOGS button and export the log with default setting.

10 One the log is downloaded, open the log file and confirm Directory Sync has written the Password changes to target environment. Below are the sample loggings:

5111,175,League-Lab2 Local,"Write: Using global catalog server from configured DCs list: Lab2-DC.Lab2.LeagueTeam.local, Domain=lab2.leagueteam.local",,5/23/2020 1:53:59 AM

5112,175,League-Lab2 Local,Write: Connecting to Domain Controller using port: 389,,5/23/2020 1:53:59 AM

5113,175,League-Lab2 Local,Write: Applying changeset e6180232-2ac7-4f7f-b7df-16217c78e3c5,,5/23/2020 1:53:59 AM

5114,175,League-Lab2 Local,Write: Finished applying changeset e6180232-2ac7-4f7f-b7df-16217c78e3c5,,5/23/2020 1:54:01 AM

5113,175,League-Lab2 Local,Write: Applying changeset f6180232-2ac7-4f7f-b7df-16217cd3421,,5/23/2020 1:53:59 AM

5114,175,League-Lab2 Local,Write: Finished applying changeset f6180232-2ac7-4f7f-b7df-16217cd3421,,5/23/2020 1:54:01 AM

11 Use the target workstation and log into the machine with target Lab1PWD1 user using the most recent password from the source environment. Verify the target user can be logged in and target environment.

12 Use the target workstation and log into the machine with target Lab1PWD2 user using the most recent password from the source environment. Verify the target user can be logged in and target environment.

Common Troubleshooting Guide

This list contains the common errors that may occur during Password Synchronization and troubleshooting steps we can use to address these errors.

Question: Do I need to run my workflow to have my password changes synced?

Answer: Although Password Syncs does not require user to run the workflow if the source and target users are correctly matched by Directory Sync, it is necessary to run the workflow at least once to allow existing target users to be matched with the source users based on the matching rules you have defined. For users created by Directory Sync, running the workflow again will be required to have the new target user matched to the source user. Once users are correctly matched, Directory Sync will monitor the password changes and synced to the target without the need of running the workflow.

Question: Why does Directory Sync generate password read log in the target Active Directory when I have Password Sync enabled from Source to Target?

Answer: Directory Sync needs to read the target user password hash into system so it can compare with the source user password hash to determine if it was changed and synced.

Question: I see BTPass folder being created under ADMIN$, however I do not see BTPassSvc.exe executable in the folder, why?

Answer: The password utility executable may have been flagged as a Malware by the anti-virus software as it was trying to inject the service onto LSASS process. To remediate this behavior, BTPass utility folder and all of its content must be added to the Anti-Virus whitelist policy.

Question: I am getting 'Error connecting to remote share (WNetAddConnection2 error code: 5)' from my DirSync Agent when Password Sync is enabled, how can I resolve this error?

Answer: This error typically happens when Directory Sync agent service account do not have the proper access to ADMIN$ share on the domain controller. As part of the Password Sync process, 'BTPass Utility' must be copied to the domain controller's ADMIN$ share folder using the service account credential, please ensure the service account is a member of the administrator group to access the share.

Question: Can I setup a workflow that only perform password sync for existing users and not sync any other attributes?

Answer: Yes, you may setup a workflow template and only includes 'unicodePwd' attribute in the template. Alternately, you can setup a workflow that only perform Read and Match operation, once a matching record is created for the source and target user, Directory Sync will sync across passwords when changes are detected for the source users.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.