Quest

SID History Synchronization

Quick Start Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

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.

SID History Synchronization – Quick Start Guide
Updated – April 2021

Contents

Introduction

The goal of this guide is to provide a step-by-step walk through of how-to setup SID History (sIDHistory) Synchronization for objects between your On-Premises Active Directory environments.

This guide will focus on sIDHistory synchronization between two on-premises Active Directory environments without a Trust enabled between two Directories. To set up Directory Sync for sIDHistory migration, 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 migration sIDHistory between two Active Directory environments.

Requirements

In order to facilitate the sIDHistory migration, the following is a list of minimum requirements to get set up using Directory Sync with your On-Premises Active Directory. Directory Sync supports sIDHistory migration for environments that have an Active Directory trust configured as well as environments without a trust configured.

Preparing the Source and Target Domains

To prepare each source and target domain for sIDHistory Synchronization, the following configuration steps must be completed:

1. In the source domain, create a local group called SourceDomain$$$, where SourceDomain is the NetBIOS name of your source domain. For example, if your domain's NetBIOS name is ADM, you must create a domain local group named ADM$$$.

   Notes: sIDHistory synchronization will fail if members are added to this local group.

2. Enable TCP/IP client support on the source domain PDC emulator:

a On the domain controller in the source domain that holds the PDC emulator operations master (also known as flexible single master operations or FSMO) role, click Start, and then click Run.

b In Open, type regedit, and then click OK.

c In Registry Editor, navigate to the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

d Modify the registry entry TcpipClientSupport, of data type REG_DWORD, by setting the value to 1.

e Close Registry Editor, and then restart the computer.

3 Enable auditing in the target domain:

a Log on as an administrator to any domain controller in the target domain.

b Click Start, point to All Programs, point to Administrative Tools, and then click Group Policy Management.

c Navigate to the following node: Forest | Domains | Domain Name | Domain Controllers | Default Domain Controllers Policy

d Right-click Default Domain Controllers Policy and click Edit.

e In Group Policy Management Editor, in the console tree, navigate to the following node: Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies | Audit Policy

f In the details pane, right-click Audit account management, and then click Properties.

g Click Define these policy settings, and then click Success and Failure.

h Click Apply, and then click OK.

i In the details pane, right-click Audit directory service access and then click Properties.

j Click Define these policy settings and then click Success.

k Click Apply, and then click OK.

l If the changes need to be immediately reflected on the domain controller, open an elevated command prompt and type “gpupdate /force”

m Repeat the above steps in the source domain.

4 Enable Advanced Auditing in the target domain when you have advanced audit policy enabled:

a Log on as an administrator to any domain controller in the target domain.

b Click Start, point to All Programs, point to Administrative Tools, and then click Group Policy Management.

c Navigate to the following node: Forest | Domains | Domain Name | Domain Controllers | Default Domain Controllers Policy

d Right-click Default Domain Controllers Policy and click Edit.

e In Group Policy Management Editor, in the console tree, navigate to the following node: Computer Configuration | Policies | Windows Settings | Security Settings | Advanced Audit Policy Configuration | Audit Policies | Account Management

f In the details pane, right-click Audit Application Group Management, and then click Properties.

g Click Configure the following audit events, and then click Success and Failure.

h Click Apply, and then click OK.

i Repeat the above for the following policies under Account Management

j Audit Computer Account Management

k Audit Distribution Group Management

l Audit Other Account Management Events

m Audit Security Group Management

n Audit User Account Management

o In Group Policy Management Editor, in the console tree, navigate to the following node: Computer Configuration | Policies | Windows Settings | Security Settings | Advanced Audit Policy Configuration | Audit Policies | DS Access

p In the details pane, right-click Audit Detailed Directory Service Replication and then click Properties.

q Click Configure the following audit events, and then click Success.

r Click Apply, and then click OK.

s Repeat the above for the following policies under Account Management

t Audit Directory Service Access

u Audit Directory Service Changes

v Audit Directory Service Replication

w If the changes need to be immediately reflected on the domain controller, open an elevated command prompt and type “gpupdate /force”

x Repeat the above steps in the source domain.

Notes: It may also be necessary to reboot the domain controller to have auditing take effect.

Even with group policy applied on the default domain controller for the domain audit, the server audit setting on the primary domain controller (PDC) may not be enabled. Please confirm this setting is enabled for the local security policy on the PDC server. If not enabled, use the local security policy to enable this setting.

Account Permissions

1 Migrate sIDHistory permissions are required on the target domain. This is typically enabled for Domain Admins and Enterprise Admins, but can be enabled for a specific group or user by following the below steps:

a Right-click on your target domain in Active Directory Users and Computers.

b Select the Security tab and add or update the desired group or user and enable the “Migrate sIDHistory” permission.

2 Source credential must have administrator access to the source PDC emulator. This is typically enabled for Domain Admins and Enterprise Admins, but can be enabled for a specific group or user by following the below steps:

a Navigator to Built-in organization unit in Active Directory Users and Computers.

b Locate the administrators group and ensure the source service account is a member of the group.

Setup

This section provides a step-by-step guide on how to set up sIDHistory 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 sIDHistory 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.
        i. Domain Name
        ii. Global Catalog Server
        iii. Username
        iv. Password
    d. Enter the Directory Sync Registration URL and Agent Registration Key information and click next.
    e. In the sIDHistory Migration section, provide the source Active Directory domain name, and user credential information. The source credential must have administrator permission in the source domain. If the source environment is a forest and contain multiple domains, ‘Use this account for all domains’ checkbox can be used to only a single source credential for all source domains in the forest.

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

8. Once 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

Setup Templates

Before we can build our workflow, 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 sIDHistory synchronization. Additional templates may be created based on your project requirements.

- Local to Local sIDHistory 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 sIDHistory 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 = AS-IS
13. Set UPDATE CREATED GROUPS = ENABLE
14. Set UPDATE MATCHED GROUPS = ENABLE
15. Set Convert Group Options with default settings:
    a. DOMAIN LOCAL GROUPS = DOMAIN LOCAL
    b. GLOBAL GROUPS = GLOBAL
    c. UNIVERSAL GROUPS = UNIVERSAL
16. Click Next
17. Set CREATE NEW CONTACTS AS = AS-IS
18. Set UPDATE CREATED CONTACTS = ENABLE

19. Set UPDATE MATCHED CONTACTS = ENABLE
20. Click Next
21. Set CREATE NEW DEVICES AS = SKIP
22. Set UPDATE CREATED CONTACTS = DISABLE
23. Set UPDATE MATCHED CONTACTS = DISABLE
24. Click Next
25. Enter a default password, Click Next
26. Check SYNCHRONIZE SID HISTORY checkbox, Click Next
27. Under mappings, we can leave the settings as default or update them based on your project requirements.
28. Click Next
29. Click Finish

Setup Workflows

Follow these steps to create two (2) new workflow 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 sIDHistory Synchronization, it is most important that existing objects are correctly matched before attempting to create new objects with the source object's sIDHistory.
10. Click the Select button to configure the Match Objects criteria for your source Cloud environment and target Cloud environment

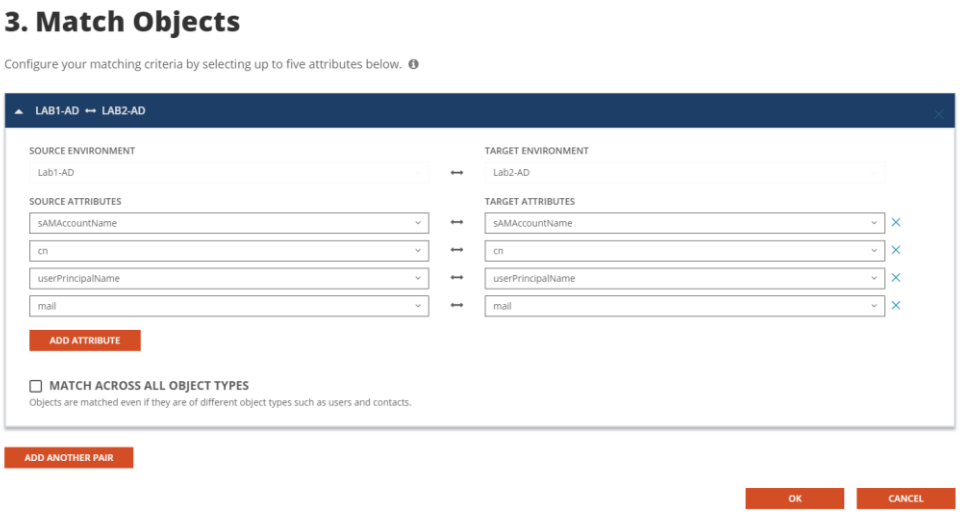

Figure 1: Example Match Objects Criteria

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 sIDHistory 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

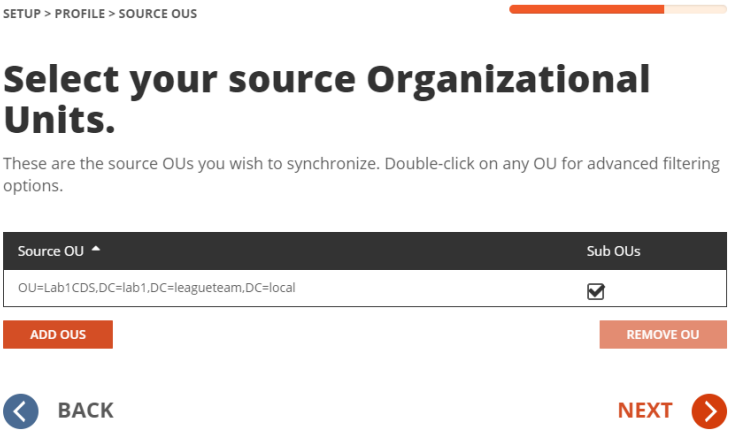

Figure 2: Example Source OU setup.

h Select the default OU for newly created objects for Users, Groups, Contacts, and Devices. In our case, we can select the same OU for all object types as we are only syncing user as contact.

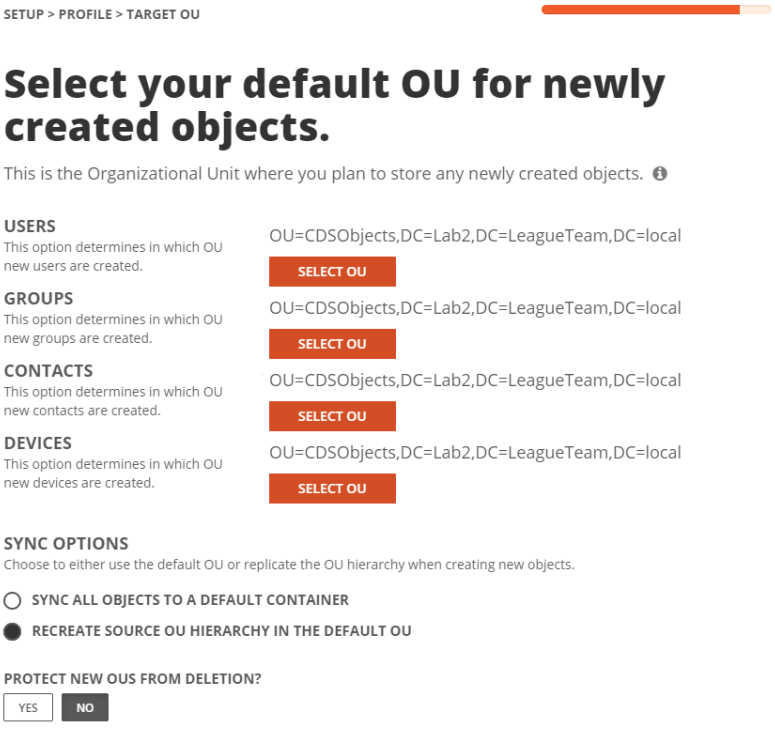

Figure 3: Example Target OU setup.

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 sIDHistory Sync workflow.

1 Setup a User in the source local environment and ensure it is part of the OU filter setup for the Local Environment.

   a DisplayName: Lab1SIDTest1

2 Setup a group in the source local environment it is part of the OU filter setup for the Local Environment.

   a DisplayName: Lab1SIDGrp1

3 Capture the objectSid value for the above test objects for later use.

Validating the Workflow

Follow the below steps to perform the sIDHistory Sync workflow and validation.

1 Select the workflow configured and click on RUN.

2 Allow the workflow execution to complete.

3 Validate Lab1SIDTest1 from source local Active Directory will be created in target. Source user's objectSid will be copied to the target user's sIDHistory attribute.

4 Validate Lab1SIDGrp1 from source local Active Directory will be created in target. Source group's objectSid will be copied to the target group's sIDHistory attribute.

Common Troubleshooting Guide

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

Question: I am getting "The handle is invalid (Error code = 6)." Error when my sIDHistory workflow runs, objects were created without sIDHistory information.

Answer: This error indicates an RPC problem where the migration tool cannot bind to an RPC endpoint on the source primary domain controller. Possible causes include:

- TcpipClientSupport on the source primary domain controller or primary domain controller emulator has not been turned on.
- The primary domain controller or primary domain controller emulator was not restarted after TcpipClientSupport was configured.
- DNS or NetBIOS name resolution is not working.

Question: I am getting " Could not verify auditing and TcpipClientSupport on domains. Will not be able to migrate Sid's. The specified local group does not exist." Error when my sIDHistory workflow runs.

Answer: This error typically indicates that a user or a global or universal group with the {SourceNetBIOSDom}$$$ name already exists. ADMT typically creates the local group of that name, but it cannot do so if a security principal already exists with the name.

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.