GAL Sync Set Up

Quick Start Guide

Contents

Introduction

The goal of this guide is to provide a step-by-step walk through of how-to set up 2-way Global Address List Synchronization between your Microsoft 365 Tenants, regardless of the tenant configuration, hybrid or cloud only.

Directory Sync supports Microsoft directories both on-premises and in the cloud. When setting up Global Address List (GAL) Synchronization there can be many different needs depending on where your Exchange Mailboxes reside and the project scope. These factors will determine the synchronization method for GAL sync. Below are two of the most common setups:

Cloud to Cloud

In most Microsoft O365 tenant setups, user mailboxes are exclusively hosted on Exchange Online, even when the user identities originate from On-Premises. In those cases, there is little need to set up local directory sync unless driven by other coexistence or migration needs, such as SID history or Password Sync. Cloud to Cloud is also the recommended configuration if you use Microsoft Azure Active Directory to manage your user identities.

Local to Local

When you have a Microsoft O365 Hybrid tenant setup and have requirements to leverage On-Premises Active Directory to manage the user identities or have the need for SID History migration and Password Sync, then it is recommended to configure your GAL Synchronization with Local to Local setup.

To set up Directory Sync for GAL sync, 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 set up GAL Sync for Microsoft 365 Hybrid Tenants.

Requirements

The following are a list of minimum requirements to get set up using Directory Sync with your Microsoft Azure Active Directory. If you are only deploying Directory Sync between Cloud only directories, then skip the next section of requirements.

● One (1) Global Administrator Account for each Microsoft 365 Tenant.

The following are a list of minimum requirements to get set up using Directory Sync with your Microsoft On-Premises Active Directory. If you are deploying Directory Sync between local directories for a hybrid deployment of Microsoft 365 then these additional items 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.

● One (1) Windows Server to install and host the Directory Sync Agent.

For more detailed information about agent installation and set-up requirements visit the On Demand Migration Active Directory User Guide.

The next section will provide a step-by-step guide on how to set up GAL Sync for Microsoft 365 Hybrid Tenants.

Setup

This section provides a step-by-step guide on how to set up GAL Sync for Microsoft 365 Hybrid Tenants.

Setup Environments

To begin at least two (2) hybrid tenants must be configured in Directory Sync. Each hybrid tenant will consist a cloud environment and a local Active Directory environment. At the end of this section there will be two (2) hybrid tenants with four (4) local and cloud 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 hybrid environments.

To create a cloud environment, an Office 365 Global Administrator is required during set up for each tenant. During the initial set up, Directory Sync will create a new unlicensed user account within each tenant. This account is used to orchestrate some of the PowerShell automation related to directory synchronization services. This account will be created with the Exchange, User and Team Administrator Roles to facilitate its designated jobs.

The Global Administrator account used to set up the environments, is required for directory synchronization services, as it is used to facilitate Graph API related automation activities. The account role can be safely lowered to User, Team and Exchange Administrator once the previously mentioned PowerShell account is created.

To create a local AD environment for the hybrid tenant, 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.

● One (1) Windows Server to install and host the Directory Sync Agent.

How to create a cloud environment

Follow these steps to setup the cloud environment endpoints.

1 Navigate to Environments

2 Click the New button

3 Click Cloud as the environment type, Click Next

4 Name the environment, Click Next

5   The Global Administrator credentials should be in-hand and ready

6   Click the Connect button

7   Login to Microsoft 365

8   Accept the requested Application Permissions

9   Select any discovery group(s) that will be used to determine which objects are part of the environment (See Pro Tip 1)

10   Do not place a check in the "INCLUDE OBJECTS SYNCHRONIZED WITH A LOCAL ACTIVE DIRECTORY VIA AZURE ACTIVE DIRECTORY CONNECT" option as this is a cloud environment with hybrid objects that originate in an On-Premises Active Directory. For hybrid objects, we will be utilizing Local to Local setup to perform the GAL Sync.

11   Click Next, then Finish

12   Repeat steps 2 – 11 for the next cloud environment

How to create a local environment for the hybrid tenant

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. 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   Under General Tab, select the Microsoft 365 tenant from the tenant drop down list under 'Which cloud environment should this environment associated with?" (See Pro Tip 18)

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

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

12   Click Save.

13   Repeat steps 2 – 12 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 templates will need to be created GAL objects. Additional templates may be created for group membership synchronization.

- Cloud to Cloud GAL Sync Source to Target
- Cloud to Cloud GAL Sync Target to Source
- Local to Local GAL Sync

How to create a Cloud to Cloud Source to Target 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 "Cloud to Cloud GAL Sync Source to Target", Click Next

5   Click Cloud as the source environment type, Click Next

6   Click Cloud as the target environment type, Click Next

7   Set CREATE NEW USERS AS = AS-IS (See Pro Tip 19)

8   Set UPDATE CREATED USERS= ENABLE

9   Set UPDATE MATCHED USERS= DISABLE

10   Click Next

11   Set CREATE GROUPS AS = SKIP

12   Set UPDATE CREATED GROUPS = DISABLE

13   Set UPDATE MATCHED GROUPS = ENABLE

14   Click Next

15   Set CREATE OFFICE365 GROUPS AND TEAMS AS = SKIP

16   Set UPDATE CREATED CONTACTS = DISABLE

17   Set UPDATE MATCHED CONTACTS = DISABLE

18   Click Next

19   Set CREATE NEW CONTACTS AS = DO NOT CREATE

20   Set UPDATE CREATED CONTACTS = DISABLE

21   Set UPDATE MATCHED CONTACTS = DISABLE

22   Click Next

23   Enter a default password, Click Next

24   Under mappings, we need to make several modifications to the default template in order to make the MEU to be compatible with Tenant to Tenant.

   o   Select mapping for 'EmailAddresses' and double click, enter the below expression under value field. (See Pro Tip 20)

   GetProxyAddresses(null, null, prefix(Result("WindowsEmailAddress"), "SMTP:"), prefix(LegacyExchangeDN, "x500:"))

   Select User as the Target Object Type

   o   Select mapping for 'CustomAttribute1 and double click, enter the below expression under value field. (See Pro Tip 21)

   "s.WindowsEmailAddress"

Select All as the Target Object Type

25 Leave rest of the mappings as default.

26 Click Next

27 Click Finish

How to create a Cloud to Cloud Target to Source 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 "Cloud to Cloud GAL Sync Target to Source", Click Next

5   Click Cloud as the source environment type, Click Next

6   Click Cloud as the target environment type, Click Next

7   Set CREATE NEW USERS AS = CONTACT (See Pro Tip 22)

8   Set UPDATE CREATED USERS= ENABLE

9   Set UPDATE MATCHED USERS= DISABLE

10 Click Next

11 Set CREATE GROUPS AS = SKIP

12 Set UPDATE CREATED GROUPS = DISABLE

13 Set UPDATE MATCHED GROUPS = ENABLE

14 Click Next

15 Set CREATE OFFICE365 GROUPS AND TEAMS AS = SKIP

16 Set UPDATE CREATED CONTACTS = DISABLE

17 Set UPDATE MATCHED CONTACTS = DISABLE

18 Click Next

19 Set CREATE NEW CONTACTS AS = DO NOT CREATE

20 Set UPDATE CREATED CONTACTS = DISABLE

21 Set UPDATE MATCHED CONTACTS = DISABLE

22 Click Next

23 Enter a default password, Click Next

24 Under mappings, we need to make several modifications to the default template in order to make the MailContact to be compatible with Tenant to Tenant.

   o   Select mapping for 'EmailAddresses' and double click, enter the below expression under value field. (See Pro Tip 20)

      GetProxyAddresses(null, null, prefix(Result("WindowsEmailAddress"), "SMTP:"), prefix(LegacyExchangeDN, "x500:"))

      Select Contact as the Target Object Type

   o   Select mapping for 'CustomAttribute1 and double click, enter the below expression under value field. (See Pro Tip 21)

"s.WindowsEmailAddress"

Select All as the Target Object Type

25   Leave rest of the mappings as default.

26   Click Next

27   Click Finish

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 GAL 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 = CONTACT (See Pro Tip 23)

8   Set UPDATE CREATED USERS= ENABLE

9   Set UPDATE MATCHED USERS= DISABLE

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 SYNCHRONIZE SID HISTORY unchecked, Click Next

26   Under mappings, we need to make several modifications to the default template in order to make the MailContact to be compatible with Tenant to Tenant.

   o   Select mapping for 'ExtensionAttribute1 and double click, enter the below expression under value field. (See Pro Tip 19)

   "s.mail"

   Select Contact as the Target Object Type

- o Select mapping for 'DistinguishName and double click, enter the below expression under value field. (See Pro Tip 24)

  GetDn(NewGuid())

- o Select mapping for 'targetAddress' and double click, enter the below expression under value field. (See Pro Tip 25)

  prefix(S.mail, "SMTP:")

- o Select mapping for 'msExchRecipientDisplayType' and double click, enter the below expression under value field. (See Pro Tip 26)

  "6"

- o Select mapping for 'msExchRecipientTypeDetails' and double click, enter the below expression under value field. (See Pro Tip 26)

  "64"

27 Leave rest of the mappings as default or update them based on your project needs.

28 Click Next

29 Click Finish

Setup Workflow

Follow these steps to create one (1) new workflow for reading, matching, staging and writing data.

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

1 Navigate to Workflows

2 Click the New button

3 Name and Describe the template, Click Next

4 Select the all four (4) environments (Cloud and Local environments per each hybrid tenant) 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. (Note, additional steps will be added as part of this guide to facilitate bi-directional synchronization.)

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

8 Select all four (4) 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 hybrid tenant directories

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

  c Your four (4) 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 GAL Sync, it is most important that email addresses do not conflict before attempting to create new objects in either environment

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 cloud environment from the drop-down menu

    b   Select your target cloud environment from the drop-down menu

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

    d   Choose the WindowsEmailAddress 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.   UserPrincipalName – UPN was added to ensure uniqueness of the local part of the address string. If creating new mail-enabled users in a destination directory it will be important to define any UPN conflicts that may exist

          ii.   ExternalEmailAddress – This attribute was added to ensure no existing MEUs or Mail Contacts have existing objects with the same external or target address

          iii.   WindowsEmailAddress to CustomAttribute1 – This matching pair is needed to create matching records for new objects created by Directory Sync.

    h   Ensure Match Across all object types is checked in this case.

    i   Check this box to ensure the workflow is evaluating conflicts regardless of the object type because in two-way GAL sync there may be instances where this condition is true, and we want to ensure you have identified these matches before deciding to create new objects or keep the matches

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

11 Drag a Match Objects workflow task from the left panel to the right under the Match Object task mentioned above. Click the Select button to configure the Match Objects criteria for your target Cloud environment and source Cloud environment

Figure 2: Example Match Objects Criteria

    a   Select your target cloud environment from the drop-down menu on the left as target will now become the source in a bi-directional setup.

b   Select your source cloud environment from the drop-down menu on the right as source will now become the target in a bi-directional setup.

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

d   Choose the WindowsEmailAddress 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.   UserPrincipalName – UPN was added to ensure uniqueness of the local part of the address string. If creating new mail-enabled users in a destination directory it will be important to define any UPN conflicts that may exist

    ii.   ExternalEmailAddress – This attribute was added to ensure no existing MEUs or Mail Contacts have existing objects with the same external or target address

    iii.   WindowsEmailAddress to CustomAttribute1 – This matching pair is needed to create matching records for new objects created by Directory Sync.

h   Ensure Match Across all object types is checked in this case.

i   Check this box to ensure the workflow is evaluating conflicts regardless of the object type because in two-way GAL sync there may be instances where this condition is true, and we want to ensure you have identified these matches before deciding to create new objects or keep the matches

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

12   Drag a Match Objects workflow task from the left panel to the right under the Match Object task mentioned above. Click the Select button to configure the Match Objects criteria for your source Local environment and target Local environment
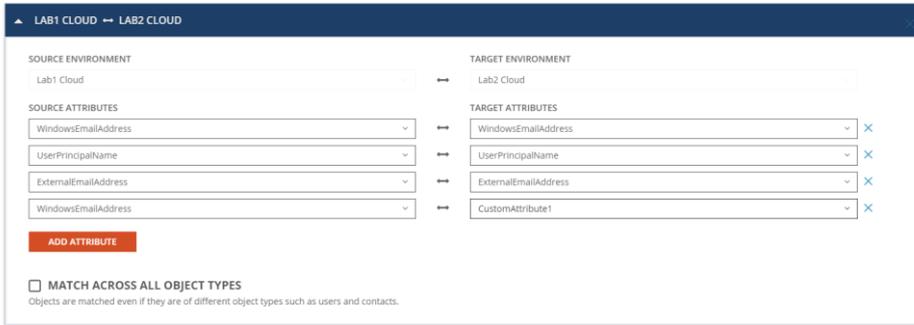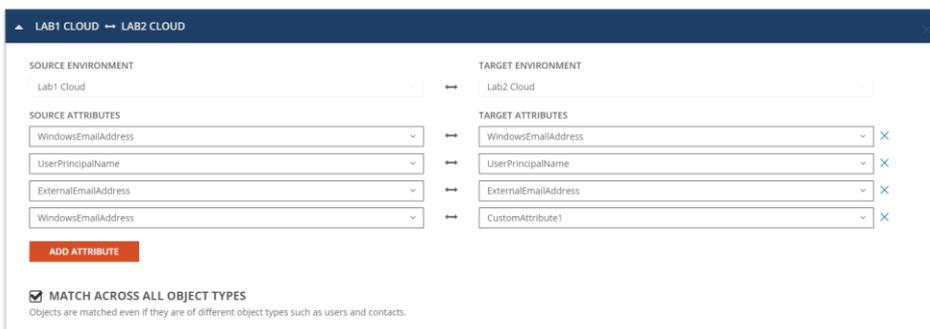

Figure 3: Example Match Objects Criteria

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

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

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

d   Choose the mail 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 two (2) additional attribute pairings to our criteria

    i.   Mail to targetAddress – This matching pair created to ensure the system can match onto existing mail contacts in the target with targetAddress pointed to the source mail attribute.

    ii.   Mail to extensionattribute1 – This matching pair is needed to create matching records for new objects created by Directory Sync.

h   Ensure Match Across all object types is checked in this case.

i   Check this box to ensure the workflow is evaluating conflicts regardless of the object type because in two-way GAL sync there may be instances where this condition is true, and we want to ensure you have identified these matches before deciding to create new objects or keep the matches

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

13 Drag a Match Objects workflow task from the left panel to the right under the Match Object task mentioned above. Click the Select button to configure the Match Objects criteria for your target Local environment and source Local environment

3. Match Objects

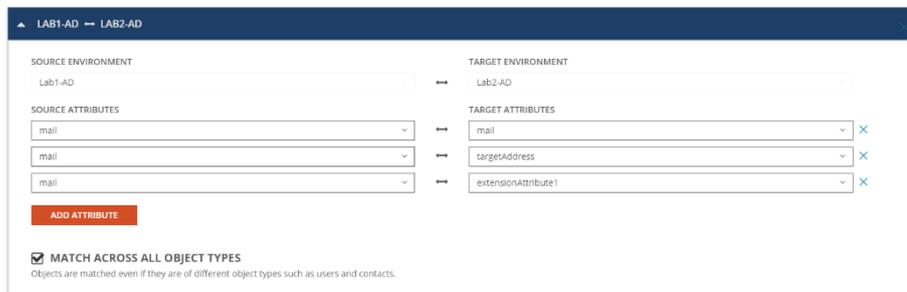Configure your matching criteria by selecting up to five attributes below. ⓘ
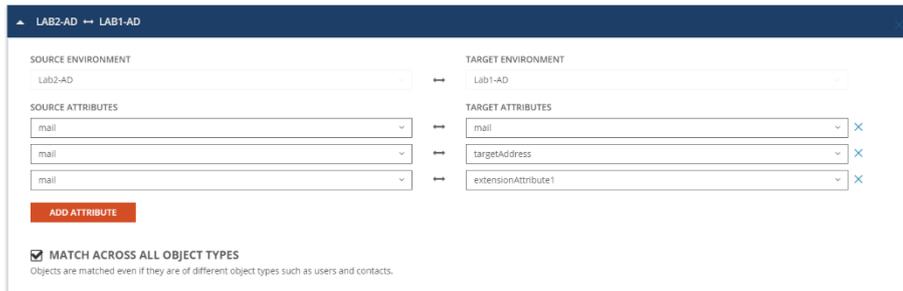
Figure 4: Example Match Objects Criteria

a   Select your target local environment from the drop-down menu on the left as target will now become the source in a bi-directional setup.

b   Select your source local environment from the drop-down menu on the right as source will now become the target in a bi-directional setup.

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

d   Choose the mail 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 two (2) additional attribute pairings to our criteria

    i.   Mail to targetAddress – This matching pair created to ensure the system can match onto existing mail contacts in the target with targetAddress pointed to the source mail attribute.

    ii. Mail to extensionattribute1 – This matching pair is needed to create matching records for new objects created by Directory Sync.

h   Ensure Match Across all object types is checked in this case.

i   Check this box to ensure the workflow is evaluating conflicts regardless of the object type because in two-way GAL sync there may be instances where this condition is true, and we want to ensure you have identified these matches before deciding to create new objects or keep the matches

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

14 Click the Select button to configure the first STAGE DATA workflow task for your Source Cloud to Target Cloud synchronization rule.

a   Select the "Cloud to Cloud GAL Sync Source to Target" template, Click Next

b   Select the source cloud environment as your source, Click Next

c   Select the target cloud environment as your target, Click Next

d   Select the default target domain name, Click Next

e   Configure any Stage Data filter you like, 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 (See Pro Tip 8)

      f   Click Finish

15   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 second STAGE DATA workflow task for your target Cloud to source Cloud synchronization rule.

      a   Select the "Cloud to Cloud GAL Sync Source to Target" template, Click Next

      b   Select the source cloud environment, Click Next

      c   Select the target cloud environment, Click Next

      d   Select the default target domain name, Click Next

      e   Configure any Stage Data filter you like, 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 (See Pro Tip 8)

      f   Click Finish

16   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 third STAGE DATA workflow task for your source local to target local synchronization rule.

      a   Select the "Local to Local GAL Sync" template, Click Next

      b   Select the source local environment, Click Next

      c   Select the target local environment, 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 (See Pro Tip 8)

Select your source Organizational Units.

These are the source OUs you wish to synchronize. Double-click on any OU for advanced filtering options.

Source OU ▲	Sub OUs
OU=Lab1GAL,OU=Lab1Objects,DC=lab1,DC=leagueteam,DC=local	☑

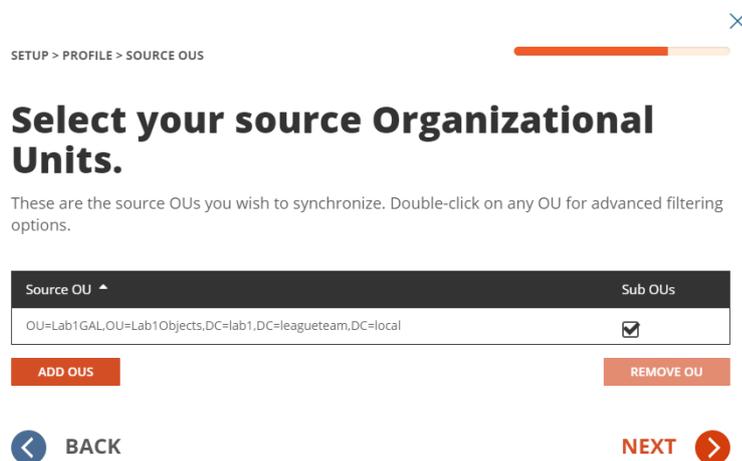ADD OUS   REMOVE OU

◀ BACK   NEXT ▶

Figure 5: 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.

Select your default OU for newly created objects.

This is the Organizational Unit where you plan to store any newly created objects. ⓘ

USERS
This option determines in which OU new users are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...

SELECT OU

GROUPS
This option determines in which OU new groups are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...

SELECT OU

CONTACTS
This option determines in which OU new contacts are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...

SELECT OU

DEVICES
This option determines in which OU new devices are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...

SELECT OU

SYNC OPTIONS
Choose to either use the default OU or replicate the OU hierarchy when creating new objects.

● SYNC ALL OBJECTS TO A DEFAULT CONTAINER
○ RECREATE SOURCE OU HIERARCHY IN THE DEFAULT OU

PROTECT NEW OUS FROM DELETION?

YES | NO

Figure 6: Example Target OU setup.

    i   Click Finish

17 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 GAL Sync" template, Click Next

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

    c   Select the source 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

Select your source Organizational Units.

These are the source OUs you wish to synchronize. Double-click on any OU for advanced filtering options.

Source OU ▲	Sub OUs
OU=Lab1GAL,OU=Lab1Objects,DC=lab1,DC=leagueteam,DC=local	☑

ADD OUS   **REMOVE OU**

◀ BACK   **NEXT ▶**

Figure 7: 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.

Select your default OU for newly created objects.

This is the Organizational Unit where you plan to store any newly created objects. ⓘ

USERS
This option determines in which OU new users are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...
SELECT OU

GROUPS
This option determines in which OU new groups are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...
SELECT OU

CONTACTS
This option determines in which OU new contacts are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...
SELECT OU

DEVICES
This option determines in which OU new devices are created.

OU=Contacts,OU=FromLab1,OU=Lab2Objects,DC=Lab2,DC=L...
SELECT OU

SYNC OPTIONS
Choose to either use the default OU or replicate the OU hierarchy when creating new objects.

● SYNC ALL OBJECTS TO A DEFAULT CONTAINER
○ RECREATE SOURCE OU HIERARCHY IN THE DEFAULT OU
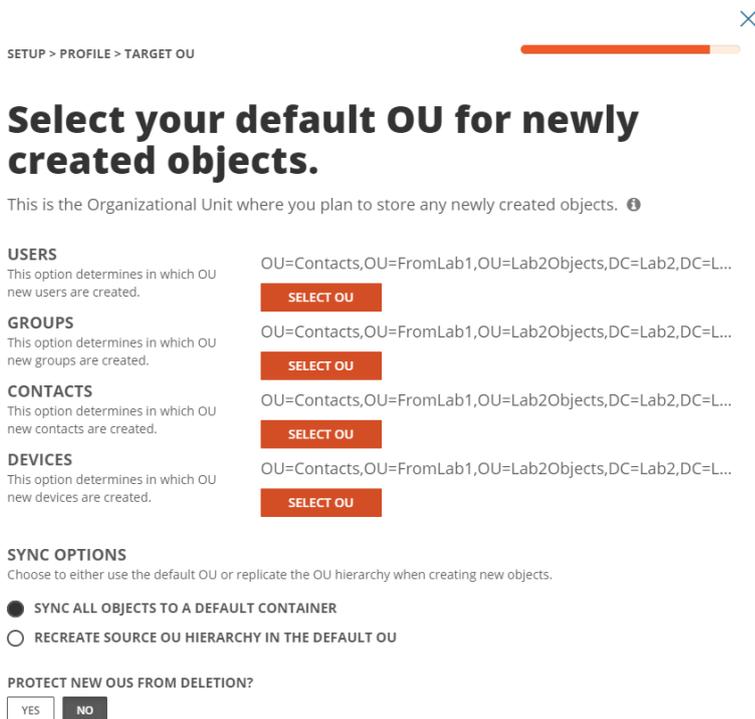
PROTECT NEW OUS FROM DELETION?
YES   **NO**

Figure 8: Example Target OU setup.

i   Click Finish

18   Click the Select button to configure the WRITE TO workflow task. Ensure all four (4) environments are selected, Click OK

19   Click Next

20   Configure the workflow sync interval, select Manual for now and we can setup a sync schedule once the test sync has completed. Click Next

21   Setup any workflow alert you may wish to configure, for now, Click SKIP

22   Click Finish

Set up Test Objects

Follow these steps to create one test objects in each environment to validate the GAL Sync workflow.

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

    a   DisplayName: Lab1RMBX1

    b   PrimarySMTPAddress: Lab1RMBX1@Lab1.Leagueteam.us

2   Setup a Remote Mailbox in the target local environment it is part of the OU filter setup for the Local Environment.

    a   DisplayName: Lab2RMBX1

    b   PrimarySMTPAddress: Lab2RMBX1@Lab2.Leagueteam.us

3   Setup a Mailbox in the source cloud environment.

    a   DisplayName: Lab1CLDMBX1

    b   PrimarySMTPAddress: Lab1CLDMBX1@Lab1.Leagueteam.us

4   Setup a Mailbox in the source cloud environment.

    a   DisplayName: Lab2CLDMBX1

    b   PrimarySMTPAddress: Lab2CLDMBX1@Lab2.Leagueteam.us

5   Capture the LegacyExchangeDN value for the above test objects for later use.

6   Add the test cloud objects as a member of the filter group for the Cloud Environment if filter group is configured when the environment was first configured.

Validating the Workflow

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

1   Select the workflow configured and click on RUN.

2   Allow the workflow execution to complete.

3   Validate Lab1RMBX1 from source local environment will be created in target local environment as Mail Contact. The target Mail Contact should have the following set:

    1.   Source Mailbox's PrimarySMTPAddress will be added as targetAddress

    2.   Source Mailbox's LegacyExchangeDN will be added as x500 address.

    3.   Source Mailbox's PrimarySMTPAddress will be added as PrimarySMTPAddress.

    4.   Target Contact's cn will be created as a random GUID to ensure there will be no name collisions.

4   Validate Lab1CLDMBX1 from source cloud environment will be created in target cloud environment as Mail Contact. The target Mail Contact should have the following set:

    1.   Source Mailbox's PrimarySMTPAddress will be added as external email address

    2.   Source Mailbox's LegacyExchangeDN will be added as x500 address.

5   Source Mailbox's PrimarySMTPAddress will be added as PrimarySMTPAddress. Validate Lab1CLDMBX1 from source cloud environment will be created in target cloud environment as Mail User. The Mail User should have the following set:

1. Source Mailbox's PrimarySMTPAddress will be added as external email address

2. Source Mailbox's LegacyExchangeDN will be added as x500 address.

3. Source Mailbox's PrimarySMTPAddress will be added as PrimarySMTPAddress.

6 Validate Lab2CLDMBX1 from source cloud environment will be created in target cloud environment as Mail Contact. The Mail Contact should have the following set:

1. Source Mailbox's PrimarySMTPAddress will be added as external email address

2. Source Mailbox's LegacyExchangeDN will be added as x500 address.

3. Source Mailbox's PrimarySMTPAddress will be added as PrimarySMTPAddress.

Best Practices & Tips

This list of best practices and tips has been assembled to further the understanding and assist with implementation questions that may arise during setup and testing.

1 Mappings have no impact on the matching attributes.

2 Mappings do not modify the Read Step; all object metadata is read.

3 If creating an object, such as Unified Groups in the destination the default mappings such as "GroupType" or "ObjectType" are not required because they will be auto generated by Exchange Online during creation.

4 If only synchronizing Group Membership, then all User attributes can be removed from the default mappings related to your group workflow and template.

5 Matching by "UserPrincipleName" will only match on the local part value, not the domain part.

6 Matching by "WindowsEmailAddress" will match on the entire string, not just the local part.

7 For membership/ownership to sync, within the template option, "If Users are matched" must be set to "Update", not Skip. Skip will prevent membership from synchronizing.

8 During testing/piloting you may create a filter under Stage Data step to isolate a subset of test Groups to create and sync membership. This will provide a method to validate a few examples before proceeding onto creating all groups.

9 The Test Mode option in the workflow prevents the write data step from occurring in a workflow.

10 If the RecipientTypeDetails attribute mapping is missing, you will receive this error during the Stage Step. "No mapping found for RecipientTypeDetails."

11 If this Name attribute mapping is missing, you will receive this error during the Write Step. "Missing required attribute: Name".

12 The default mappings for Proxy Addresses (i.e. EmailAddresses) may prevent the creation of Unified Groups. The following error is received during the Write Step, "There should be at least one MOERA in Email Addresses.".

13 When we create a group, we grant our account Owner access. This can be removed once Sync services are no longer required.

14 The "ONLY EVALUATE OBJECTS WHICH HAVE CHANGED SINCE THE LAST READ" option only affects the Stage Step. Enable this option after the initial data has been read. Do not set that setting on read and write only workflows.

15 By default, the "ReplaceDomain" function is used by the "WindowEmailAddress" attribute to set your default email address to the Target Domain selected within the Stage Data step. This can be changed if required.

16 The Delete Objects Step in a workflow is required to delete target objects if that is in scope for your project. Here are details on this step:

1. Reconcile finds source object XYZ is no longer in scope and removes it from CDS, adds it to a list of "Reconciled objects" for that source.

2. Delete step looks in "Reconciled objects" for anything from the configured source. It finds object XYZ.

3. Delete step then looks for a match to object XYZ from the configured target. If found, the target object is deleted.

In summary, the Reconcile step captures anything removed from the source, the delete step looks for any matching objects on the target and deletes them.

17 A cloud environment filter is highly recommended, so we only must process in-scope objects to be read-in for the cloud environment. This will reduce the time needed to read in the objects by Directory Sync.

18 Both cloud and local environments will be added and associated automatically if we create the Tenant to Tenant project first.

19 Due to O365 limitation, there can be no more than one cloud only objects having the same ExternalAddress, therefore, we must create the GAL object as MEU in the target cloud tenant. Contact object will be created after mailbox provisioning.

20 The below custom mapping will copy the source object's WindowsEmailAddress value to target as PrimarySMTPAddress, and it will also copy the source object's LegacyExchangeDN to the target as an x500 address.

Select mapping for 'EmailAddresses' and double click, enter the below expression under value field:

GetProxyAddresses(null, null, prefix(Result("WindowsEmailAddress"), "SMTP:"), prefix(LegacyExchangeDN, "x500:"))

21 The below custom mapping will copy the source object's WindowsEmailAddress value to the target's customattribute1 for matching purposes after the object is created. Customattribute1 can be replaced by another attribute if it is already taken in the tenant.

Select mapping for 'CustomAttribute1 and double click, enter the below expression under value field:

"s.WindowsEmailAddress"

22 Target user objects will be created in the source as contact object because the limitation described in number 19 does not apply here. The source user object will not have the ExternalAddress set, hence there will be no duplication.

23 For Local to Local, the limitation described in number 19 no longer applies; therefore, we can create the GAL object as contact with ExternalAddress configured.

24 The below custom mapping will set the target contact's CN as a random GUID; this is needed to avoid possible name collision as CN is not a unique attribute in Active Directory.

Select mapping for 'DistinguishName and double click, enter the below expression under value field:

GetDn(NewGuid())

25 The below custom mapping will set the target contact's targetAddress field with the source object's mail attribute (which is also the PrimarySMTPAddress).

Select mapping for 'targetAddress' and double click, enter the below expression under value field:

prefix(S.mail, "SMTP:")

26 msExchRecipientTypeDetails and msExchRecipientDisplayType will need to be set per Microsoft requirement for Mail Contact. In this case, they should be set to "64" and "6".

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.