



© 2020 Quest Software Inc.

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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.

# Table of Contents

<b>Table of Contents</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>4</b>
Goal .....	4
Requirements .....	4
Account Permissions.....	4
<b>Setup</b> .....	<b>4</b>
Setup Environments.....	5
Setup Templates.....	6
<i>How to create a Local to Local template .....</i>	<i>6</i>
Setup Workflows.....	7
<i>How to create a one-way sync workflow for Local to Local.....</i>	<i>7</i>
<b>Set up Test Objects</b> .....	<b>10</b>
<b>Validating the Workflow</b> .....	<b>11</b>
<b>Best Practices &amp; Tips</b> .....	<b>11</b>

# Introduction

Power365 Directory Sync supports users, groups and contact synchronization between environments. The following describes the supported environments and deployment models.

- **Local to Local** – Covered in this guide. Support synchronization between two local Active Directory environments.
- **Cloud to Cloud** – Support synchronization between two Microsoft 365 tenant environments.
- **Local to Cloud** – Support synchronization between an Active Directory and a Microsoft 365 tenant environment when source is Active Directory and target is Microsoft 365 tenant.
- **Cloud to Local** – Support synchronization between a Microsoft 365 tenant and an Active Directory environment when source is Microsoft 365 tenant and target is Active Directory.

## Goal

The goal of this guide is to provide a step-by-step walk through of how-to setup Users, Groups and Contacts Synchronization for between your On-Premises Active Directory environments.

To set up Power365 Directory Sync for Users, Groups and Contacts Synchronization, source objects must be either matched to existing objects or created as new 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 Users, Groups and Contacts between two Active Directory environments.

## Requirements

In order to facilitate synchronization of Users, Groups and Contacts, the following is a list of minimum requirements to get set up using Power365 Directory Sync with your On-Premises Active Directory.

## 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 next section will provide a step-by-step guide on how to set up Users, Groups and Contacts Synchronization for Active Directory environments.

# Setup

This section provides a step-by-step guide on how to set up Users, Groups and Contacts Synchronization for Microsoft Active Directory Environments.

## Setup Environments

To begin at least two (2) Active Directory environments must be configured in Power365 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.
- One (1) Windows Server to install and host the Power365 Directory Sync Agent.

Follow these steps to setup the cloud environment endpoints.

1. Login to [Power365](#)
  2. Navigate to [Environments](#)
  3. Click the [New](#) button
  4. Click *Local* as the environment type, Click *Next*
  5. *Name* the environment, Click *Next*
  6. *Name the* local agent, Click *Next*
  7. Note the agent registration URL and registration Key for later use, click *Finish*.
  8. Install the agent in the Windows Server that is joined to the local AD domain.
    - a. Launch the Power365 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 Power365 Directory Sync Registration URL and Agent Registration Key information and click next.
    - e. In the sIDHistory Migration section, you may skip this step if sIDHistory Migration is not part of your project scope.
- Note, Refer to [Power365 Online Help Center](#) for [detailed information about agent installation and set-up requirements](#).*
9. Once the agent is installed and the environment is discovered, click on the *Setting* button to access the local AD environment setting page.

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 3 – 12 for the next local environment

## 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 Synchronization for User, Group and Contact Objects. This guide also assume objects 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

- Local to Local Sync

### How to create a Local to Local template

1. Login to [Power365](#)
2. Navigate to [Templates](#)
3. Click the [New](#) button
4. *Name and Describe* the template
5. In our example, we will name our template “*Local to Local Sync*”, Click *Next*
6. Click *Local* as the source environment type, Click *Next*
7. Click *Local* as the target environment type, Click *Next*
8. Set *CREATE NEW USERS AS = AS-IS*
9. Set *UPDATE CREATED USERS= ENABLE*
10. Set *UPDATE MATCHED USERS= ENABLE*
11. Set *IF TARGET ADDRESS EXISTS* setting as *OVERWRITE ONCE*.
12. Click *Next*
13. Set *CREATE GROUPS AS = SKIP*
14. Set *UPDATE CREATED GROUPS = ENABLE*
15. Set *UPDATE MATCHED GROUPS = ENABLE*
16. Set Convert Group Options with default settings: (See *Pro Tip 17*)
  - a. *DOMAIN LOCAL GROUPS = DOMAIN LOCAL*
  - b. *GLOBAL GROUPS = GLOBAL*
  - c. *UNIVERSAL GROUPS = UNIVERSAL*

17. Click *Next*
18. Set *CREATE NEW CONTACTS AS = AS-IS*
19. Set *UPDATE CREATED CONTACTS = ENABLE*
20. Set *UPDATE MATCHED CONTACTS = ENABLE*
21. Click *Next*
22. Set *CREATE NEW DEVICES AS = SKIP*
23. Set *UPDATE CREATED CONTACTS = DISABLE*
24. Set *UPDATE MATCHED CONTACTS = DISABLE*
25. Click *Next*
26. Enter a default password, Click *Next*
27. Leave the *SYNCHRONIZE SID HISTORY* checkbox unchecked, Click *Next*
28. Under mappings, we can leave the settings as default or update them based on your project requirements. (See *Pro Tip 16*)
29. Click *Next*
30. 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. Login to [Power365](#)
2. Navigate to [Workflows](#)
3. Click the [New](#) button
4. *Name* and *Describe* the template, Click *Next*
5. Select the all two (2) local Active Directory environments created previously, Click *Next*
6. Select *ONE-WAY SYNC*, Click *Next*
7. The screen presented next will be a pre-configured set of workflow steps to facilitate the flow of object and attributes between your directories.
8. Start at the top of the steps, *1. Read From*. Click the *Select* button
9. Select all two (2) environments created previously the click *OK*
10. 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.
11. Click the *Select* button to configure the *Match Objects* criteria for your source Local environment and target Local environment

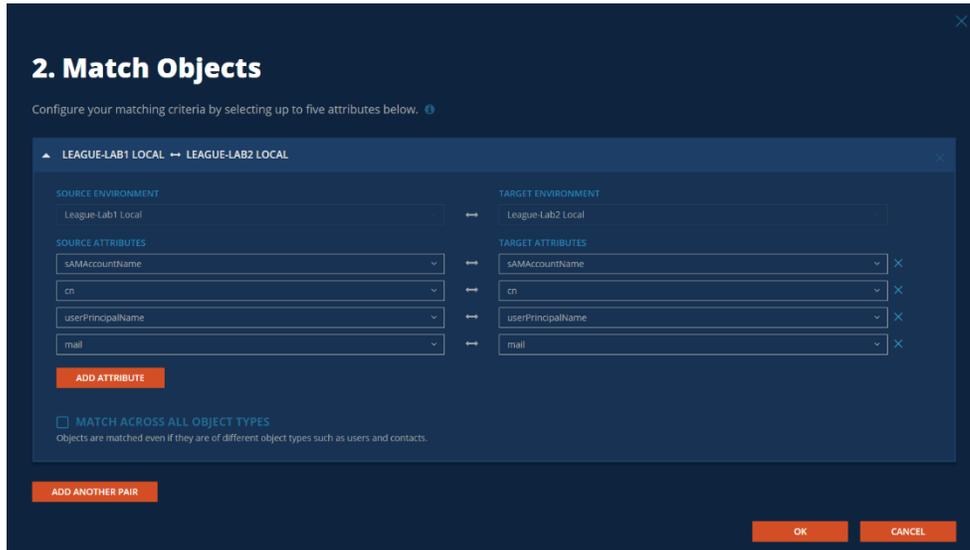


Figure 1: Example Match Objects Criteria

- 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. (See *Pro Tip 5 & 6*)
  - 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
12. 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 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*

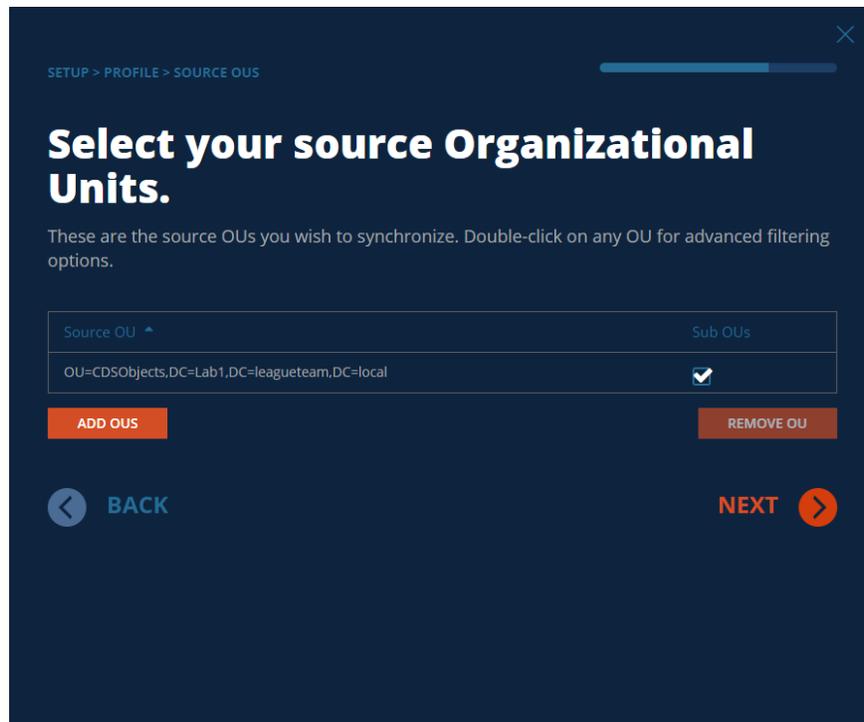


Figure 2: Example Source OU setup.

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

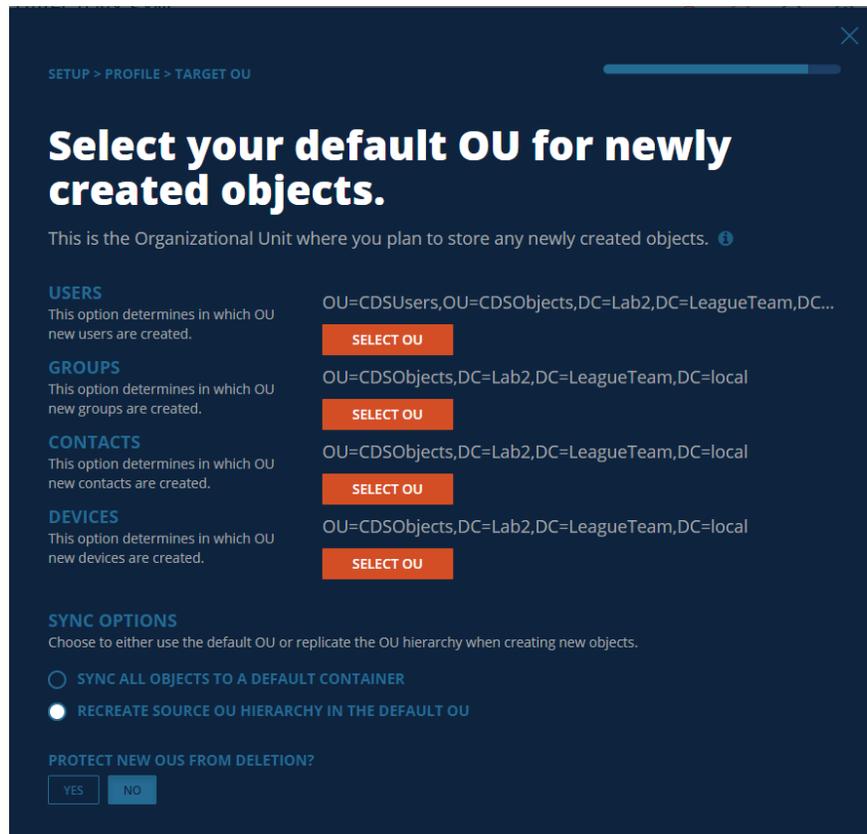


Figure 3: Example Target OU setup.

- i. Click *Finish*
13. Click the *Select* button to configure the *WRITE TO workflow task*. Ensure the target environment is selected, Click *OK*
14. Click *Next*
15. Configure the workflow sync interval, select *Manual* for now and we can setup a sync schedule once the test sync has completed. Click *Next*
16. Setup any workflow alert you may wish to configure, for now, Click *SKIP*
17. Click *Finish*

## Set up Test Objects

Follow these steps to create test objects in the source environment to validate the Users, Groups, Contacts Sync workflow.

1. Setup the user object in the source local environment and ensure it is part of the OU filter setup for the Local Environment.
  - a. User Object - DisplayName: Lab1User1
2. Setup the group object in the source local environment and ensure it is part of the OU filter setup for the Local Environment.

- a. Global Group Object - DisplayName: *Lab1Grp1*
  - b. Universal Group Object – DisplayName: *Lab1Grp2*
  - c. Domain Local Group Object - DisplayName: *Lab1Grp3*
3. Setup the contact object in the source local environment and ensure it is part of the OU filter setup for the Local Environment.
    - a. Contact Object - DisplayName: *Lab1Contact1*

## Validating the Workflow

Follow the below steps to perform Real Time Users, Groups, Contacts Sync workflow and validation.

1. Select the workflow configured and click on RUN.
2. Allow the workflow execution to complete.
3. Validate *Lab1User1* from source local Active Directory will be created in the correct target OU defined in the workflow.
4. Validate *Lab1Grp1* from source local Active Directory will be created as Global Group in the correct target OU defined in the workflow.
5. Validate *Lab1Grp2* from source local Active Directory will be created as Universal Group in the correct target OU defined in the workflow.
6. Validate *Lab1Grp3* from source local Active Directory will be created as Domain Local Group in the correct target OU defined in the workflow.
7. Validate *Lab1Contact1* from source local Active Directory will be created in the correct target OU defined in the workflow.

## 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 “UserPrincipalName” 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 the 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 in the cloud environment, we grant our BT 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 default template contains the most commonly used mapping configuration between two environments, depends on the project requirements and scopes, mapping template can be modified to suite your project specific requirements.
17. Target Group Scope can be configured using these settings if you wish to convert the group scope as new groups created in target Active Directory.