Quest

On Demand Migration Active Directory

User 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.

On Demand Migration Active Directory User Guide
Updated - April 2025
Version - 20.12.17

Contents

Introduction

On Demand Migration for Active Directory enables you to migrate and consolidate AD and Entra ID environments. This SaaS solution can integrate and migrate users, groups, and devices between Active Directory, Entra ID, and hybrid directory environments.

This is one of three SaaS solutions Quest offers for device migration. Please reference the user guide for the solution you have purchased:

- On Demand Migration Active Directory User Guide: Directory Sync, coexistence, domain rewrite, domain move, AD migration, device migrations
- On Demand Migration Active Directory Express User Guide: Device migrations that do not require coexistence
- On Demand Migration Entra ID for Devices User Guide: Device migrations from on-prem and hybrid AD to Entra ID that do not include an AD migration

Directory Sync Requirements

Directory Sync is built with Microsoft Azure. Our Software-as-a-Service (SaaS) platform is designed to handle a variety of directory synchronization scenarios to meet your coexistence and collaboration needs.

Directory Sync can manage simple AD to AD, Cloud to Cloud, and more complex scenarios including combinations of local and cloud mixed environments.

What is required to get Directory Sync set up?

You will need 2 items to get started with setting up Directory Sync.

1. The authorized account(s) that allow changes to your local and/or cloud directories
2. At least one (1) local on-premises server to host the local agent (if applicable)

The following information provides details around the specific component requirements.

Agents

Directory Sync is a 100% SaaS platform but to commit changes to on-premises directories (if applicable) such as Active Directory, a local agent must be installed and configured.

You will need at least one Directory Sync Agent installed per forest (environment). You may have up to five agents per forest. Adding more agents can offer limited fault-tolerance and can improve synchronization throughput, especially for near real-time password synchronization.

Note: The Directory Sync Agent should not be installed on a non-domain joined server.

Important Tip: If you are only connecting to Microsoft Entra ID, local agents are not required.

Hardware

This local agent must meet the following minimum requirements:

- At least one (1) Windows Server 2016, 2019, 2022, or 2025
- Additional Windows servers may be deployed. Limit to 5.
- CPU: 4 Cores

- Memory: 4GB Free
- Disk: 40GB Free Disk Space excluding Operating System.

Note: The local agent must be configured on the Member Server for Modern Password Copy.

Important Tip: Do not install any local agents on AD domain controllers in a production environment.

Software

This local agent must meet the following minimum requirements:

- Windows Server 2016, 2019, 2022, or 2025
- .NET 4.7.2 (will automatically be installed unless already present)
- TLS 1.2 or higher

Domain and Forest Functional Levels

- All AD Functional Levels supported by Microsoft for a Microsoft Windows Server operating system listed below are supported for migration from/to Domain controllers running on that same Operating System. For example, Windows Server 2016 functional levels are supported on Windows Server 2022, Windows Server 2019, and Windows Server 2016. For full details see Microsoft's documentation of Active Directory Domain Services Functional Levels in Windows Server on Microsoft Learn.
    - NOTE: Windows Server 2003 functional levels are supported only on Windows Server 2016. That is, Microsoft does not support Windows Server 2003 functional levels on Windows Server 2019 or Windows Server 2022.
- The following Windows Server versions are supported:
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
    - Windows Server 2025

Network

- Connecting to the Directory Sync web interface uses TCP port 443 (HTTPS).
- Agent connections are initiated by the agent and require port 443 access to Directory Sync SaaS application.
- Agent connections to the DCs use ports 88, 135, 137-139, 389 (UDP), 445, 1027, 3268 and 49152-65535.
- Port 636, 3269 is required for LDAPs. Please refer to Enable Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) - Windows Server | Microsoft Learn for LDAPs requirement
- Copying SIDHistory is an operation initiated by the agent and performed by the domain controllers.
    - Source/Target Domain Controller FQDNs must be resolvable by each other.
    - Open TCP ports 88, 135, 137-139, 389 (UDP), 445, 1027, 3268 and 49152-65535.

Accounts

Local Active Directory Account

- The agent installer will prompt for a domain account with permission to read and write on-premises Active Directory.
- An agent intended to sync all domains in a forest, must have access rights to all domains and objects used in workflows.

Microsoft Entra ID Application Account

- When creating a new Cloud Environment, an account with the Global Administrator Role is required to grant permissions and establish a connection.
- This account also needs the Global Administrator Role enabled during the first Read workflow so that it can create and configure Microsoft Entra ID PowerShell Accounts required for Directory Sync tasks.

Microsoft Entra ID PowerShell Accounts

- An OAuth token will be used by the application to create two (2) PowerShell accounts which are used to read and update objects in the cloud.
- The accounts will have Exchange Administrator, User Administrator and Teams Administrator roles assigned in order to read and update objects in the cloud.

- The accounts being used do not require any Microsoft 365 licenses.
- The accounts must be excluded from MFA requirements.
- An OAuth token will also be used by the used by the application to create a mail-enabled security group which will contain the two PowerShell accounts.

Password Synchronization

The following conditions must be met for Password Sync:

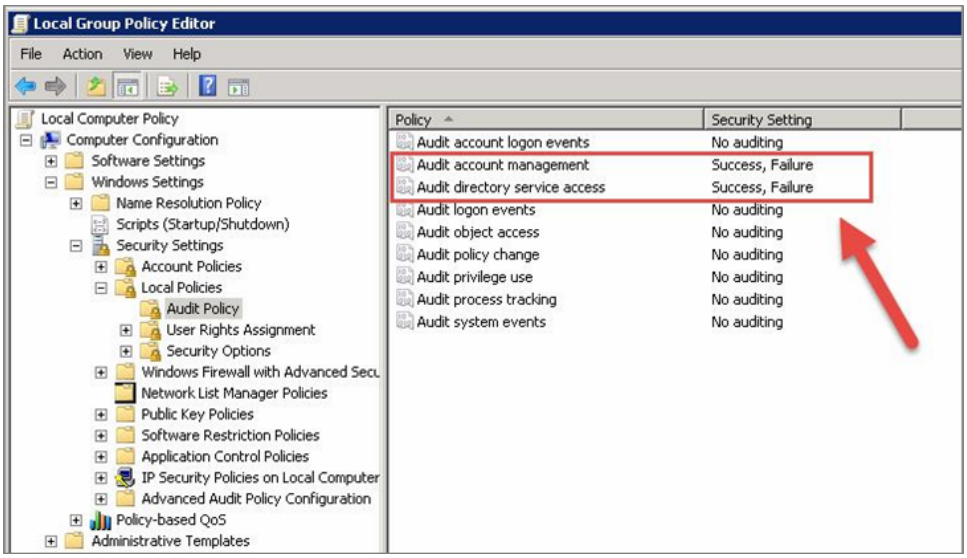
- ADMIN$ must be accessible on the domain controller from the Directory Sync agent server.
- The Password Sync functionality requires that either a domain admin role or built-in admin role be granted to the service account.
- Third-party anti-virus or threat prevention programs may block the execution of password tasks. These programs may need to be uninstalled from both the Domain Controller and the Directory Sync Agent Server or otherwise carefully whitelisted to allow proper operation.
- 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.

SID History

- A trust between that source and target domain is not required to populate SID History on target objects, but is required to make use of the SID History when attempting to access source side resources. Typically, a trust is created by establishing a Forest level trust, but can also be done as a domain trust.
- The target account must have administrator permissions in the source domain. To enable this, the target account of the Directory Sync agent should be added to the source PDC's built-in administrator group.

- Auditing of the source and target domain must be enabled. This can be enabled as a global policy for all domain controllers or as a local policy on the specific source and target DCs involved. To enable auditing as a local policy, go to gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy and enable the “Audit account management” and “Audit directory service access” settings.



- ‘Account Management’ and ‘DS Access’ Advance Audit policies of the source and target domain should be configured if Advance Auditing are configured in the environments. These settings can be enabled as a global policy for all domain controllers or as a local policy on the specific source and target DCs involved.

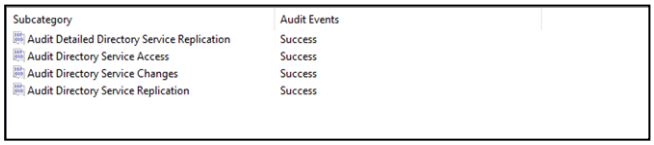
    - To enable advance audit policy for Account Management, go to gpedit.msc > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Account Management enable **Success** and **Failure** audit for the below policies.

        - Audit Application Group Management
        - Audit Computer Account Management
        - Audit Distribution Group Management
        - Audit Other Account Management Events
        - Audit Security Group Management
        - Audit User Account Management

Subcategory	Audit Events
Audit Application Group Management	Success and Failure
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure
Audit User Account Management	Success and Failure

    - To enable advance audit policy for DS Access, go to gpedit.msc > Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > DS Access and enable Success audit for the below policies.

        - Audit Directory Service Access
        - Audit Directory Service Changes
        - Audit Directory Service Replication
        - Audit Detailed Directory Service Replication

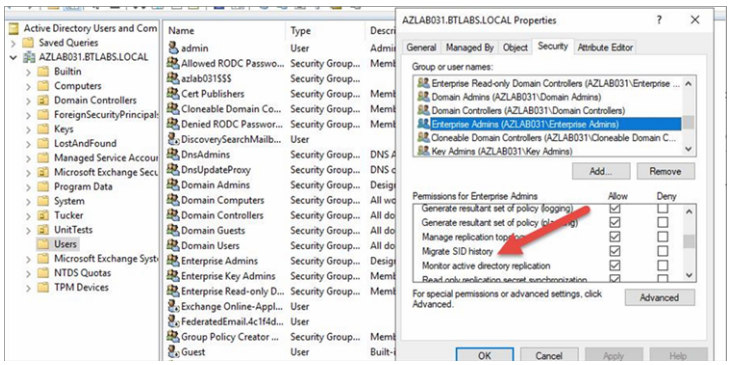


Subcategory	Audit Events
Audit Detailed Directory Service Replication	Success
Audit Directory Service Access	Success
Audit Directory Service Changes	Success
Audit Directory Service Replication	Success

- An empty Domain Local security group must be created in each source domain and named {SourceNetBIOSDomain}$$$.
- The HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\TcpipClientSupport registry key must be set to 1 on the source domain primary domain controller. You must restart the source domain primary domain controller after the registry configuration.

- MigratesIDHistory 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:

    1. Right-click on your target domain in Active Directory Users and Computers.
    2. Select the Security tab and add or update the desired group or user and enable the “Migrate SID History” permission.



Important Tip: For further guidance from Microsoft about Using **DsAddSidHistory**, click here.

Workflow Alerts

- To create a workflow alert, simply have a valid SMTP address ready.

Setup

Workflows

What is a Workflow?

A workflow is a configurable series of steps that provides an easy automation framework to connect and manage Directory object synchronization. Activities such as creating, updating and deleting objects along with property/attribute synchronization and transformation. In addition, workflows may also include a PowerShell script to be executed based on the workflow rules. Providing greater flexibility and extensibility to the workflow automation.

Where do I manage Workflows?

To manage workflows, simply open the left navigation menu and click **Workflows**, located under **Setup**, see *figure 1*.

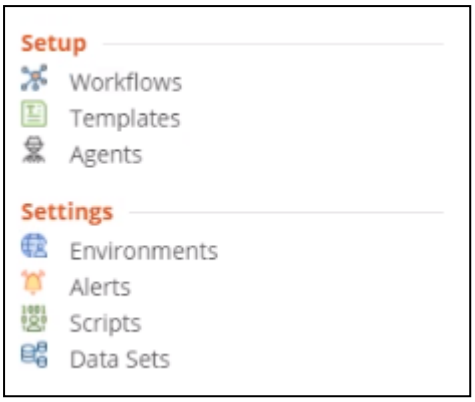


Figure 1: Directory Sync Setup and Settings Menu

What should be entered as the Workflow Name?

You can name your workflow anything you'd like but remember that you may be referencing the same environment in multiple workflows. We suggest a name that generally describes the flow of objects. Then use the description field for the distinguishing characteristics. After this step, the wizard will guide you through all the necessary components that will make up your workflow.

What should be selected for Workflow Type?

The workflow type choice determines which default set of workflow steps that the wizard will guide you through. No matter what choice you make here, you can always customize your workflow steps at any time, so if you aren't sure, start with a one-way sync. Once you have learned what settings work best for a particular project, you may want to enter those settings in an XML file and import it here so that you can easily recreate the steps for similar workflows. You can download the sample file and then customize to your needs, then import it.

What are the steps to create a Workflow?

When you create a new workflow, the wizard will ask you to choose a type of workflow. It will then prepopulate a workflow for you with the appropriate steps. You can modify this, or, start from scratch. We will start from scratch, to examine the possible steps that you will need for any workflow.

1. First is Read From. Here is where you will choose the environments that have the objects that you would like to use for matching and mapping, and ultimately for possible migration to a target environment. If you plan a many to one migration, you would choose several sources here. You have to have at least one environment to read from in any workflow. One Read From step can include several sources, so you don’t need a separate read from step for each one.

2. Match objects is next. Here is where you choose the environments to compare, AND, the criteria that Directory Sync will use to decide if an object in one environment is the same object as found in another environment, which we call a match. If you don't read from an environment, you cant choose it here.

   It is very important that the matching attribute selected is a unique value for that attribute in source. Selecting an attribute that is not unique could result in multiple source objects matched to a single target object. If UserprincipalName is selected as a matching attribute for both Source and Target, only the prefix data will be used for matching, however the mail attribute will require an entire string match including the prefix and domain suffix.

   Important: Objects created by Directory Sync will not be matched until they are **read and matched by running the Read and Match workflow task**.

3. The Stage Data step is required next. Stage Data is where you customize your workflow action. You will be asked to choose a template. A template contains specifc preferences that you can reuse, such as password options, and attribute mappings. You will choose your source and target environment pairs here. And again, you will only be able to choose those environments that you have read from. You will be able to choose your source OUs and even set up some OU filters if you want to narrow your scope.
4. And finally, you need to include at least one Write To environment. After data has been matched, mapped and filtered, what is your target, where do you want to place the new objects, and/or sync objects that were considered a match?

How is a Workflow scheduled?

You can run your workflow manually or choose to run at specific time intervals. Or choose a time of day. The minimum time interval is 15 minutes. No matter what you choose as part of the wizard, you can always trigger a manual run of a workflow from the welcome screen. You can access the welcome screen at any time by clicking the Directory Sync logo at the top left.

The set interval can be changed on the Discover tab of the Local Environment settings.

Can objects be deleted?

A Delete Objects step is also available. If an object is removed from scope and/or deleted from the Source, any matching object on the Target will be deleted. To configure this step, you must enter Source/Target endpoint pairs and a threshold (the max number of objects to delete per pair).

Can a PowerShell script be run?

An optional additional step would be the run PowerShell script step, in which you can choose a PowerShell script that will run each time the workflow is run.

Additional Information

Alerts
Workflow Test Mode
Evaluate Changed Objects Only
Product Licensing

Workflow Test Mode

What does the Workflow Test Mode do?

You can use Workflow Test Mode to view the normal processing and logs without making changes to the target environment.

How is the Workflow Test Mode enabled?

Workflow Test Mode can be enabled on the General tab of Settings. When the Test Mode option is checked, the workflow will execute the workflow while preventing the Write To jobs from executing and writing anything to the target environment.

What does the Skip Script option do?

When the Skip Scripts option is checked, all script tasks in the workflow will be skipped. If you choose to disable this option, object changes may occur based on the actions within the script.

How do you see the history of the Workflow run in Test Mode?

After running the workflow in Test Mode, You can view the History of the workflow and download the logs. The log will display the skipped Write To job as being skipped and the Script task as being skipped (if Skip Scripts is enabled).

Additional Information

Workflows
Alerts
Evaluate Changed Objects Only

Workflow: Evaluate Changed Objects Only

What does the "Only evaluate objects which have changed since last read" option do?

You can set a workflow to only evaluate objects which have changed on the General tab. When the "Only evaluate objects which have changed since last read" option is selected, only objects that have changed since the last read will be evaluated. When the option is not selected, all objects are evaluated.

Additional Information

Workflows
Alerts
Workflow Test Mode

Templates

What is a template?

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.

Where do I manage templates?

To manage templates, simply open the left navigation menu and click **Templates**, located under **Setup**, see *figure 1*.

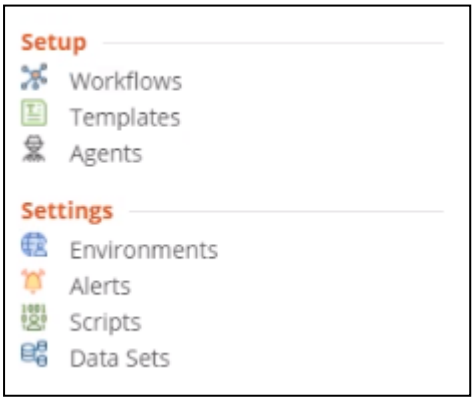


Figure 1: Directory Sync Setup and Settings Menu

How do I configure the template to update target objects if they are already mailbox enabled?

You can configure Directory Sync to update mailbox enabled target objects via Templates under Objects and General tab. See Template Options for more information. You should also review the mapping configuration to ensure mail attributes mappings are configured correctly per your project's need to avoid unwanted mail disruption.

What do mappings do?

A mapping entry defines a relationship between an attribute in the source, and an attribute in the target. It tells Directory Sync where to place the value from a source attribute, and how to modify it if necessary.

Normally this is a one-to-one relationship, for example the value found in the employeeID attribute in the source environment will be written to the employeeID attribute in the target.

Note: By default, msExchMailboxGUID and msExchArchiveGUID are not included in the default mapping template, customer may add them to the template if they wish to sync these attributes.

How do you change a mapping?

You can modify this mapping by double-clicking on it.

For example, suppose that this project was an acquisition, where the target environment company acquired the source. And in the source company, they use the employee ID field as a unique identifier, but in the target company they user employee number instead of employee ID. The first thing to do would be to remove the employee ID attribute entry as we don’t want that source value to be written as is.

Then, we would modify the employee number mapping, so that source will be the employeeID, and it would be written to employee number.

You can hold down your control key and select one or more mappings to remove if you don't want them. More options can be found under the advanced button.

When importing the mappings file, can the column order be changed?

If you choose to export and edit the mappings file and then import the file, the columns must remain in the same order or no mappings will be imported.

Additional Information

Template Options

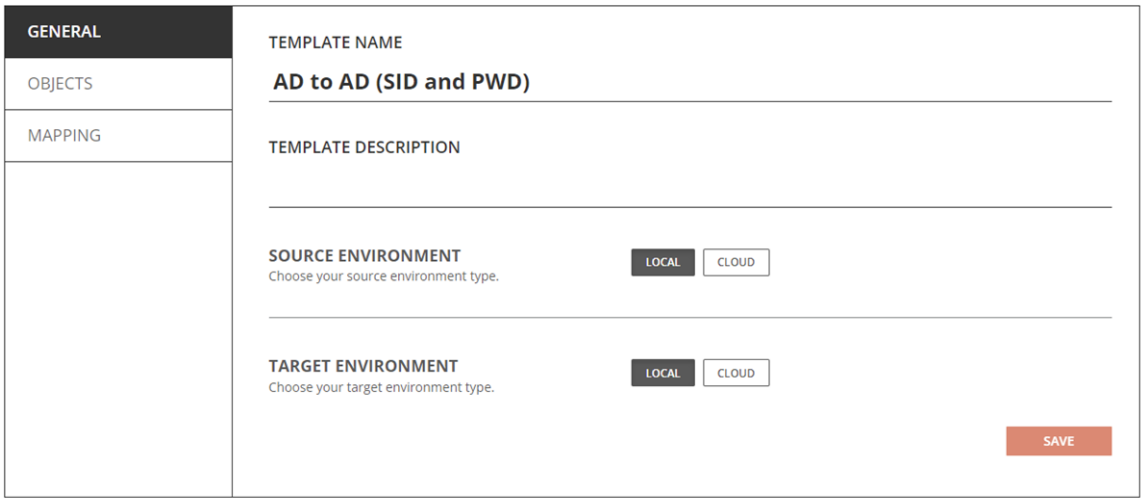
Advanced Mapping

Reset Mappings

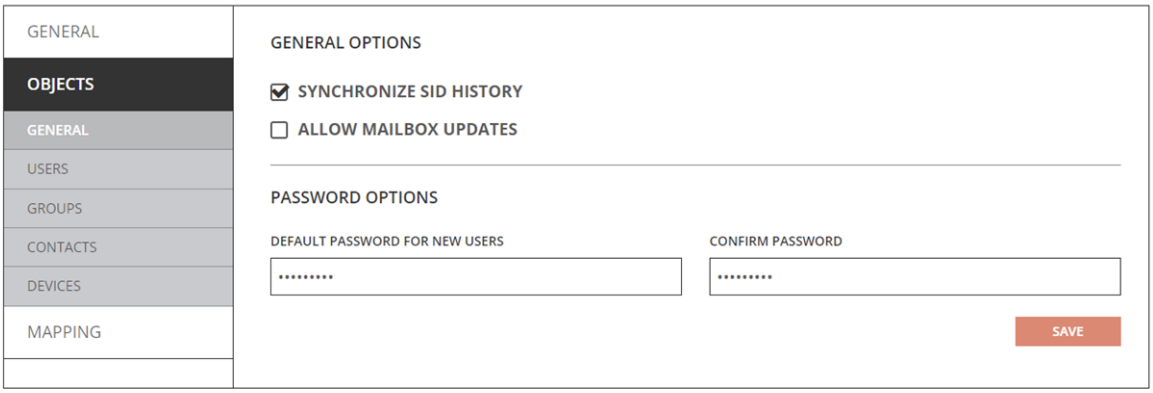
Local Environment Template Options

General Option

AD to AD (SID and PWD)



Objects General Tab – Local Environment



- Synchronize SID History – Directory Sync will migrate SID-History when this option is enabled.

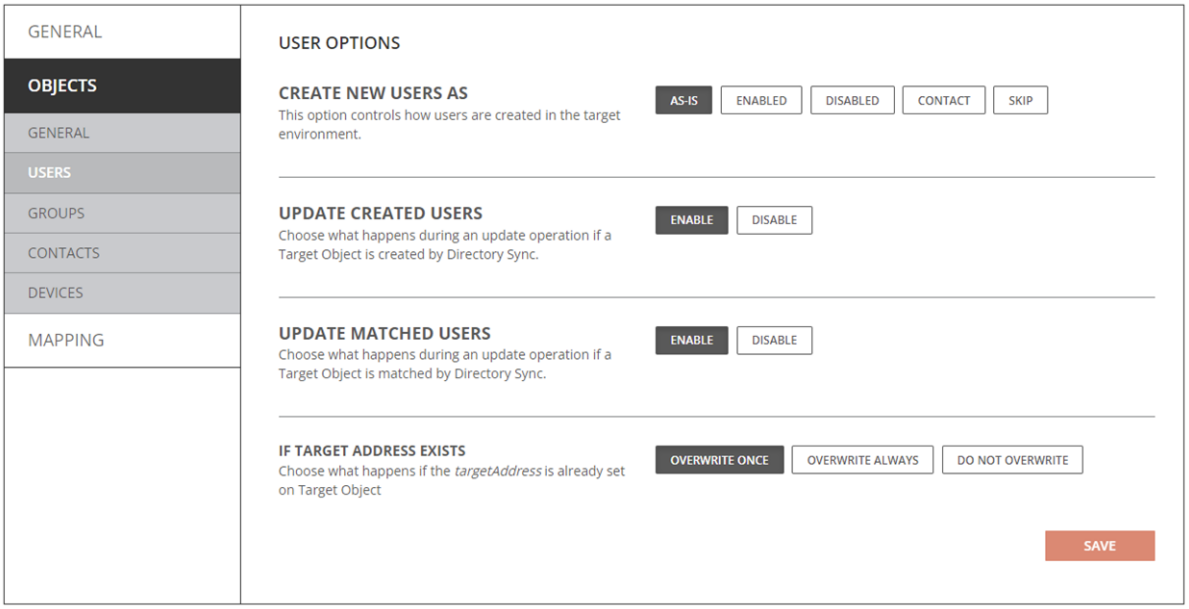
  Important Tip: Refer to the SID History Synchronization Quick Start Guide for additional information on how to migrate SID-History.

- Allow Mailbox Update - You can configure Directory Sync to update mailbox-enabled target objects via Templates under the Objects and General tab. You should also review the mapping configuration to ensure mail attributes mappings are configured correctly per your project's need to avoid unwanted mail disruption.

- Default Password for New Users – Define the default password for new users.

Important Tip: The default password defined should meet the password complexity policy for your target environment.

Objects Users Option – Local Environment

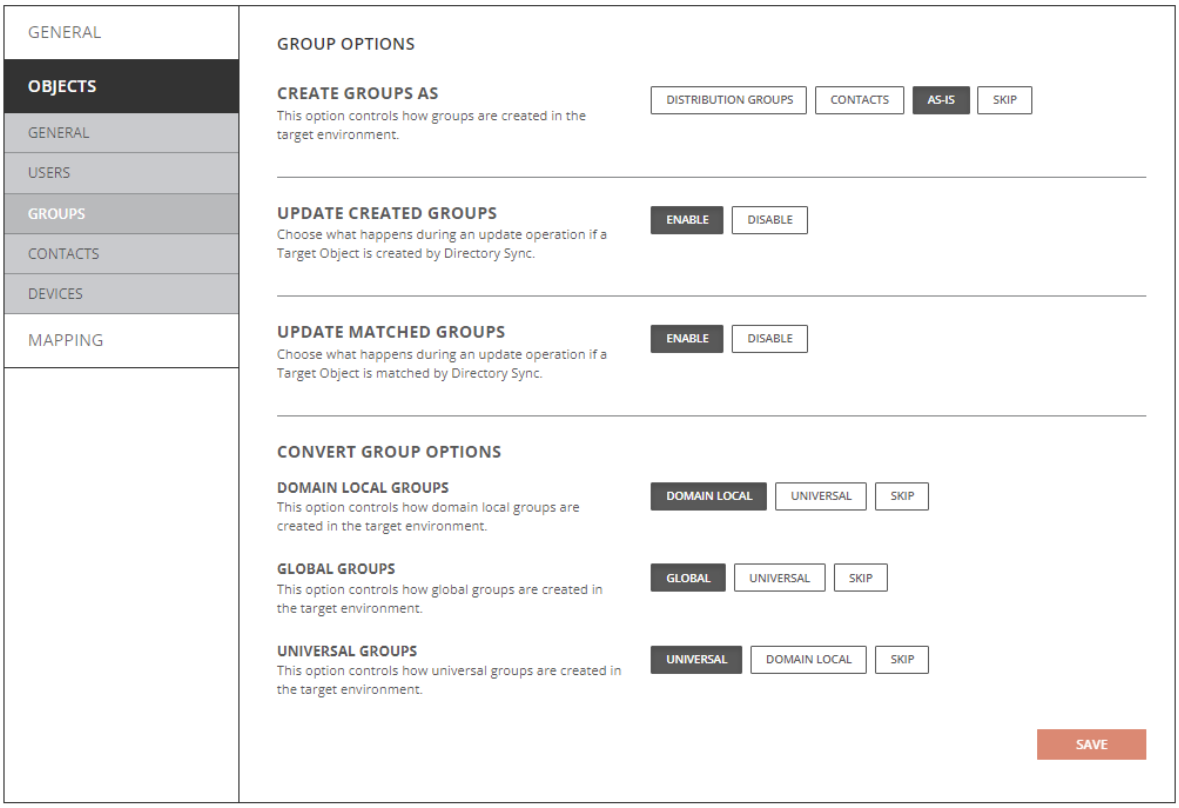


- Create New Users As
    - As-Is: Objects will be created just as they currently exist in the source. If the account was disabled in Active Directory in the source, it will be disabled in Active Directory when created in the target. If the account was enabled in Active Directory in the source, it will be created as enabled in Active Directory in the target.
    - Enabled: Objects will be created as enabled in the target Active Directory.
    - Disabled: Objects will be created as disabled in the target Active Directory.
    - Contact: Objects will be created as contact in the target Active Directory.
    - Skip: Objects will not be created in the target Active Directory.

Important Tip: Source User's UserAccountControl(UAC) setting can be synchronized to target as-is via attribute mapping in the template.

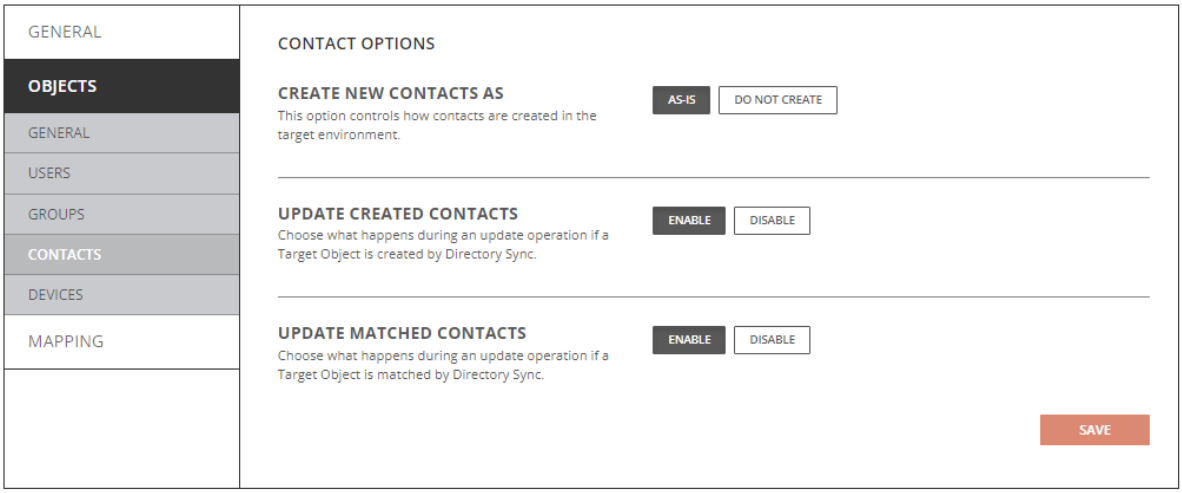
- Update Created Users
    - Enabled: Object changes will be synchronized to the target during delta sync after the users were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the users were created by Directory Sync.
- Update Matched Users
    - Enabled: Object changes will be synchronized to the target during delta sync after the users were matched by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the users were matched by Directory Sync.
- If Target Address Exists
    - Overwrite Once: TargetAddress attribute will only synchronized once during the initial sync.
    - Overwrite Always: TargetAddress attribute will always synchronized during initial and delta sync.
    - Do Not Overwrite: TargetAddress attribute will not be synchronized.

Objects Groups Option – Local Environment



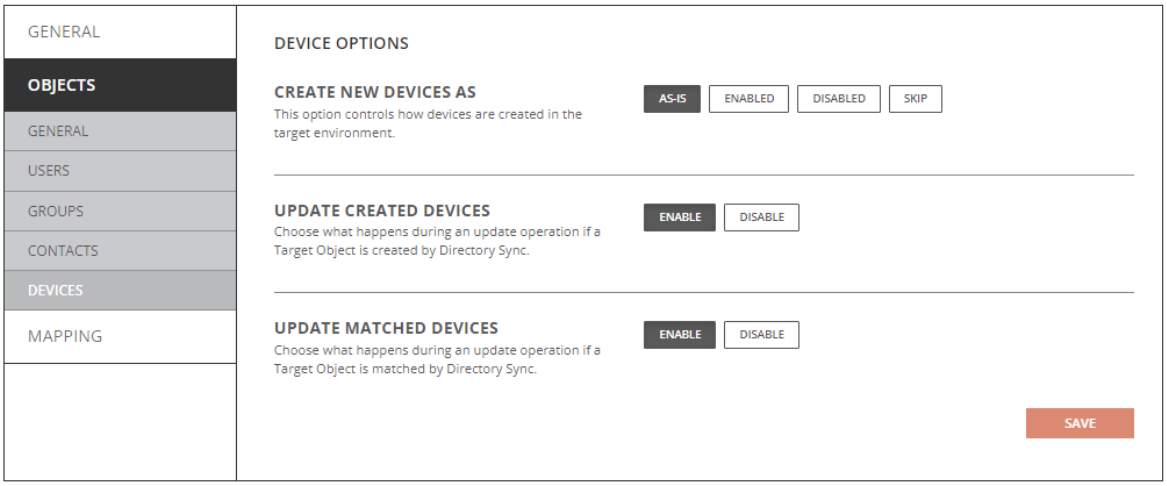
- Create Groups As
    - Distribution Groups: Objects will be created just as Distribution Group in the target Active Directory.
    - Contacts: Objects will be created just as Contacts in the target Active Directory.
    - As-Is: Objects will be created just as they currently exist in the source.
- Update Created Groups:
    - Enabled: Object changes will be synchronized to the target during delta sync after the groups were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the groups were created by Directory Sync.
- Update Matched Groups
    - Enabled: Object changes will be synchronized to the target during delta sync after the groups were matched by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the groups were matched by Directory Sync.
- Convert Group Options
    - Domain Local Groups
        - Domain Local: Source Domain Local Groups will be created as Domain Local Groups in the target.
        - Universal: Source Domain Local Groups will be created as Universal Groups in the target.
        - Skip: Source Domain Local Groups will not be created.
    - Global Groups
        - Global: Source Global Groups will be created as Global Groups in the target.
        - Universal: Source Global Groups will be created as Universal Groups in the target.
        - Skip: Source Global Groups will not be created.
    - Global Groups
        - Global: Source Global Groups will be created as Global Groups in the target.
        - Universal: Source Global Groups will be created as Universal Groups in the target.
        - Skip: Source Global Groups will not be created.
    - Universal Groups
        - Universal: Source Universal Groups will be created as Universal Groups in the target.
        - Domain Local: Source Universal Groups will be created as Domain Local Groups in the target.
        - Skip: Source Universal Groups will not be created.

Objects Contacts Option – Local Environment



- Create New Contacts As
  - As-Is: Source contacts will be created just as they currently exist in the source.
  - Do Not Create: Source contacts will not be created in the target.
- Update Created Contacts:
  - Enabled: Object changes will be synchronized to the target during delta sync after the contacts were created by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the contacts were created by Directory Sync.
- Update Matched Contacts:
  - Enabled: Object changes will be synchronized to the target during delta sync after the contacts were created by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the contacts were created by Directory Sync.

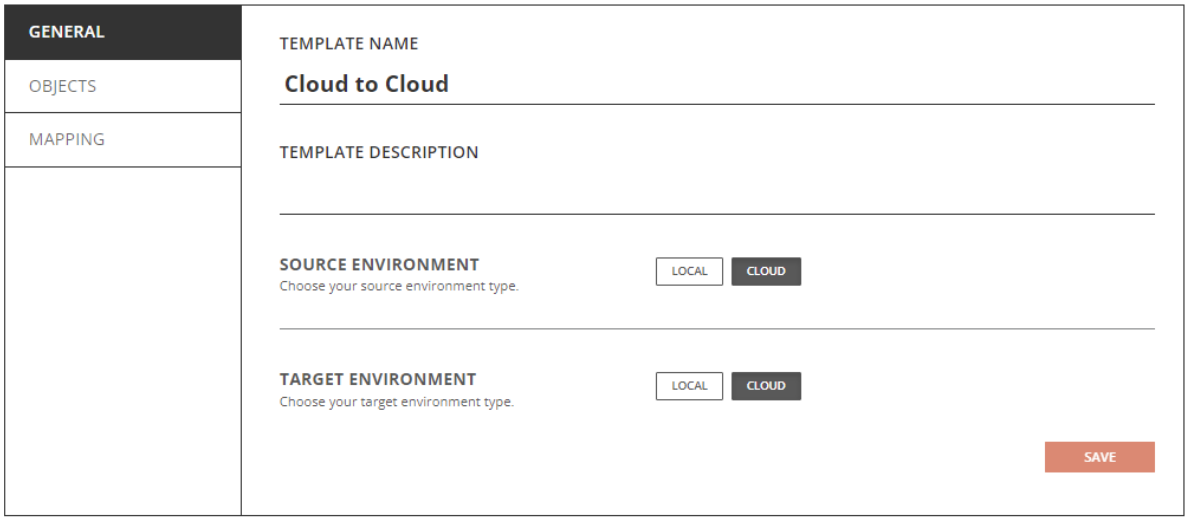
Objects Devices Option – Local Environment



- Create New Devices As
    - As-Is: Source devices will be created just as they currently exist in the source.
    - Enabled: Source devices will be created as enabled in the source.
    - Disabled: Source devices will be created as disabled in the source.
    - Do Not Create: Source devices will not be created in the target.
- Update Created Devices:
    - Enabled: Object changes will be synchronized to the target during delta sync after the devices were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the devices were created by Directory Sync.
- Update Matched Devices:
    - Enabled: Object changes will be synchronized to the target during delta sync after the devices were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the devices were created by Directory Sync.

Cloud Environment Template Options

General Option

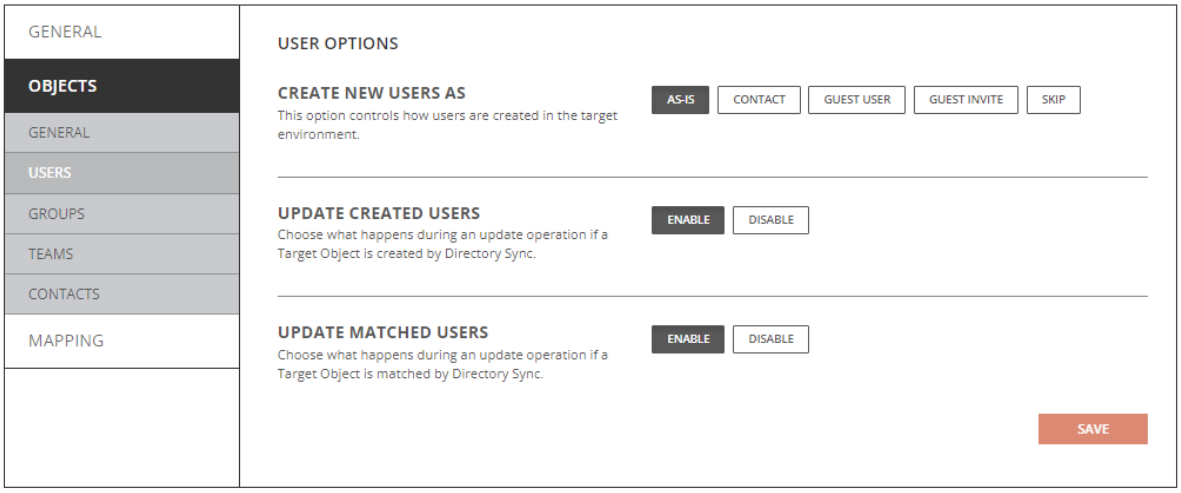


Objects General Tab – Cloud Environment

- Allow Mailbox Update - You can configure Directory Sync to update mailbox enabled target objects via Templates under Objects and General tab. You should also review the mapping configuration to ensure mail attributes mappings are configured correctly per your project's need to avoid unwanted mail disruption.
- Default Password for New Users – Define the default password for new users.

  Important Tip: The default password defined should meet the password complexity policy for your target environment.

Objects Users Tab – Cloud Environment

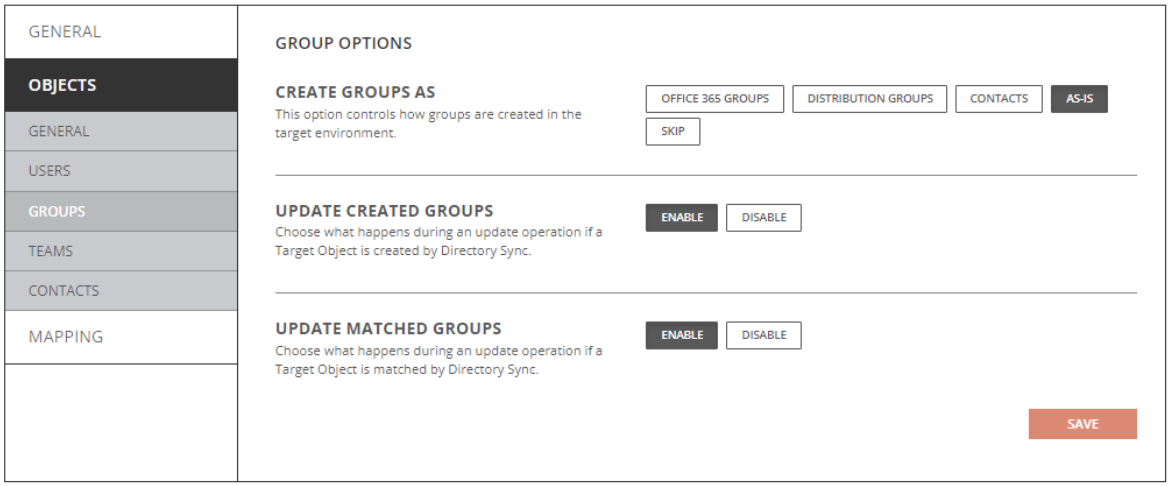


- Create New Users As
    - As-Is: Objects will be created just as they currently exist in the source.
    - Contact: Objects will be created as contact.
    - Guest User: Objects will be created as a guest user.
    - Guest Invite: Objects will be created as a guest user with invite.
    - Skip: Objects will not be created in the target.

Important Tip: For additional information related to Guest Objects synchronization, please refer to the Guest User How-To Guide in the help section.

- Update Created Users
    - Enabled: Object changes will be synchronized to the target during delta sync after the users were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the users were created by Directory Sync.
- Update Matched Users
    - Enabled: Object changes will be synchronized to the target during delta sync after the users were matched by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after the users were matched by Directory Sync.

Objects Groups Tab – Cloud Environment

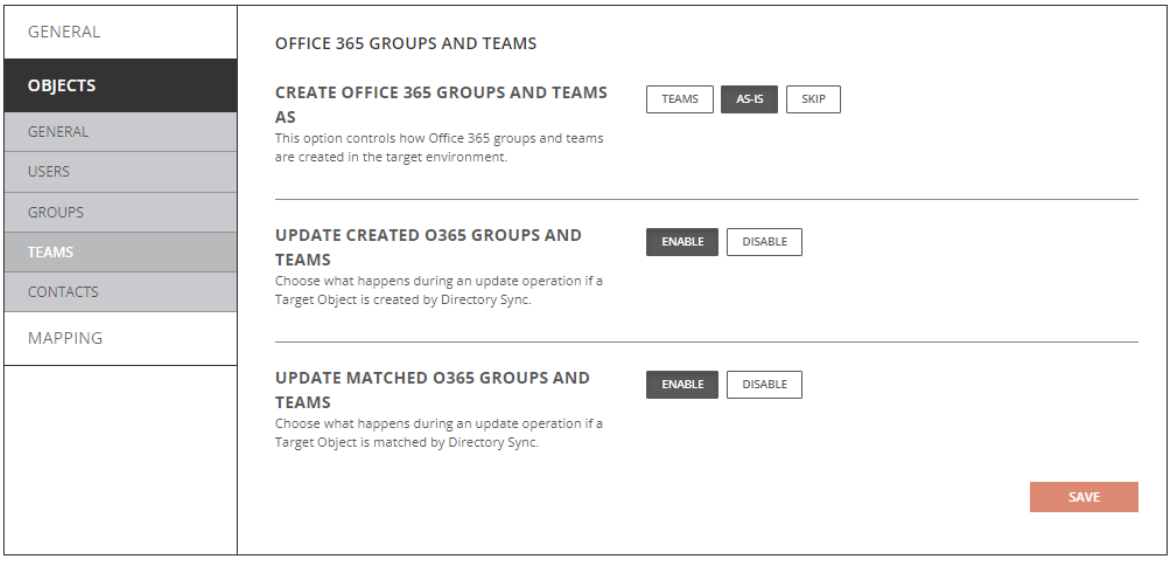


- Create New Users As
  - Office 365 Groups: Objects will be created as Office 365 Groups(Unified Groups) in the target.
  - Distribution Groups: Objects will be created as Distribution Groups.
  - Contacts: Objects will be created as contacts.
  - As-Is: Objects will be created just as they currently exist in the source.
  - Skip: Objects will not be created in the target.

Important Tip: If the source group is a security group, it will be created as security group when As-Is option selected.

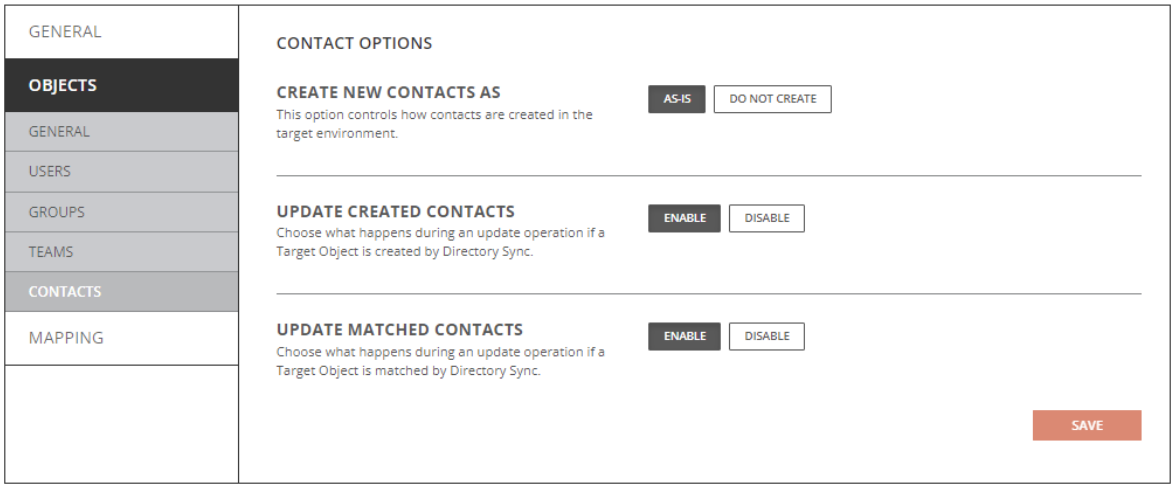
- Update Created Groups
  - Enabled: Object changes will be synchronized to the target during delta sync after the groups were created by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the groups were created by Directory Sync.
- Update Matched Groups
  - Enabled: Object changes will be synchronized to the target during delta sync after the groups were matched by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the groups were matched by Directory Sync.

Objects Teams Tab – Cloud Environment



- Create Office 365 Groups and Teams As
    - Teams: Objects will be created Teams in the target.
    - As-Is: Objects will be created just as they currently exist in the source.
    - Skip: Objects will not be created in the target.
- Update Created Office 365 Groups and Teams
    - Enabled: Object changes will be synchronized to the target during delta sync after they were created by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after they were created by Directory Sync.
- Update Matched Office 365 Groups and Teams
    - Enabled: Object changes will be synchronized to the target during delta sync after they were matched by Directory Sync.
    - Disabled: Object changes will not be synchronized to the target during delta sync after they were matched by Directory Sync.

Objects Contacts Tab – Cloud Environment



- Create New Contacts As
  - As-Is: Source contacts will be created just as they currently exist in the source.
  - Do Not Create: Source contacts will not be created in the target.
- Update Created Contacts:
  - Enabled: Object changes will be synchronized to the target during delta sync after the contacts were created by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the contacts were created by Directory Sync.
- Update Matched Contacts:
  - Enabled: Object changes will be synchronized to the target during delta sync after the contacts were created by Directory Sync.
  - Disabled: Object changes will not be synchronized to the target during delta sync after the contacts were created by Directory Sync.

Advanced Mapping

How is the advanced mapping info accessed?

Click on a mapping and choose the Advanced button. You can then customize the mapping behavior.

What are the components of an Advanced Mapping?

There are several components in an advanced mapping. Please review the advanced mappings guide before making any changes to an existing mapping.

- The first component is the value. This is single value, or, it could be a formula that will be used to determine the final written value. This can be a combination of functions, text and/or operations to construct the final value.

  There are some default values that already exist. If you do not have experience with advanced mappings, we suggest that you do not change the default values.
- The condition is a formula that must result in a True statement in order for the attribute to be mapped. It is a qualifier that acts like an on-off switch. If the condition sections is empty, as in this example the switch is On by default.
- The target attribute is the userprincipal name. The value that will be written, will be calculated by is called a Function. In this case, it is the replacedomain function. This function will take the userprincipal name from the source, and will replace the domain portion with the target domain that is selected in the StageData step of your workflow, referred to as profile, in this function. Please note that some functions are specific to the workflow type, such as local to local.

Additional Information

Reset Mappings

Reset Mappings

How do you reset the mappings?

You can undo all of any changes that you have made by clicking the advanced button resetting to the default mappings. This is going to set all mappings back to the factory default. Any mappings that you have manually added and any advanced customization that you have made to a particular mapping will be lost. With that in mind, before you choose reset mapping, it would be a best practice to choose export all, to save your customizations to a file. This file contains all current mappings.

Additional Information

Templates

Advanced Mapping

Agents

What is the Directory Sync agent?

The Directory Sync agent is the key component that communicates between a local Active Directory environment and the Directory Sync service.

Where do you install the agent?

The agent must be installed in every forest that you plan to include as a Directory Sync environment. We suggest that you create a virtual machine exclusively for this purpose. Review the Directory Sync Requirements for the minimal hardware and software requirements.

How do I download and install the agent?

First, choose the environment that the agent will be associated with.

You will be able to download the latest version of the agent from the Directory Sync agent screen. Copy the URL and the access key that will be needed during the install of the agent. The downloadable executable is the same for all projects, it is the Registration URL and Registration Key that makes the agent unique when it is installed.

To install of the agent enter credentials that have read or read\write access to the domain, depending on the direction of synchronization.

Copy and paste the information from the Directory Sync agent screen.

No further action is needed on the workstation. A look at services confirms that the Directory Sync agent is running.

A list of agents appears on summary screen, including status information as well as the registration URL and access keys should you need them again in the future.

Please Note: If using the agent Auto-Upgrade feature and deployment software that uses MSI ProductCode based detection, the Auto-upgrade feature should be disabled after initial deployment or the detection method should verify via a folder path.

Where do I manage agents?

To manage agents, simply open the left navigation menu and click **Agents**, located under **Setup**, see *figure 1*.

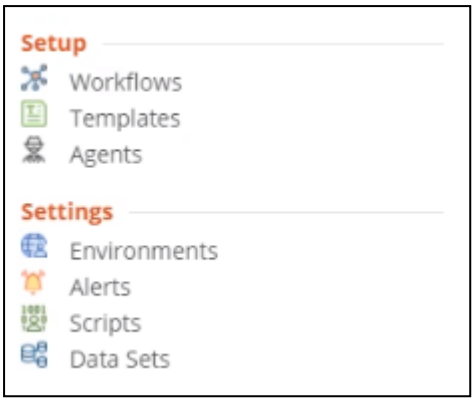


Figure 1: Directory Sync Setup and Settings Menu

How do I manage the agents?

On the Agents page, you can check the current status of your current agents or add new ones. Select an agent for additional options. You have the option to copy the Registration URL or the Registration Key if you need to reinstall the agent for any reason. The History button will give you details on the run history. When the agent is updated, any agent using the old version will offer you the upgrade option so that you can update your current agent installation.

How many agents can be installed on a computer?

You may configure up to five separate agents on a single computer. When running the agent installer, you have the option of registering a new agent on the computer or if there are existing agents on the computer, you may select an existing agent to configure or remove it.

Do I need to configure a Local Directory Sync agent if my tenant is a hybrid with local Active Directory attached?

A Local Directory Sync agent is only required when working with Hybrid MailUsers (a mailuser object synced with a local active directory object). A Directory Sync agent is used to configure the mail-forwarding rule on the local AD object when working with Hybrid MailUsers. A Directory Sync agent is not required when working with Mailbox and Cloud Only Objects as mail-forwarding rules are configured via EXO PowerShell.

How do I uninstall an agent?

If you need to uninstall an agent from any machine, in order to reinstall on the same machine, you must first delete the registry folder located at HKEY_LOCAL_MACHINE> SOFTWARE> Quest > Agent and then uninstall.

Afterwards, simply create a new agent (with a new access key) under Agents managements from the left navigation menu before re-installing on the same machine.

Guest Users in Directory Sync

What is a Guest User?

A guest user is an Microsoft Entra ID Business-to-Business account which is utilized to provide seamless collaboration between the Microsoft Cloud organizations.

For more context and details check out Microsoft's document on the topic, What is guest user access in Microsoft Entra ID B2B?

Can I create, update and delete Guest user objects with Directory Sync?

Yes, Directory Sync provides create, update and delete capabilities to keep your multiple identities, objects and properties in sync for short-term and long-term integration needs.

There are two (2) new additional options to create users in a target cloud directory, highlighted below. The image shows the Template wizard where you may manage how users are created.

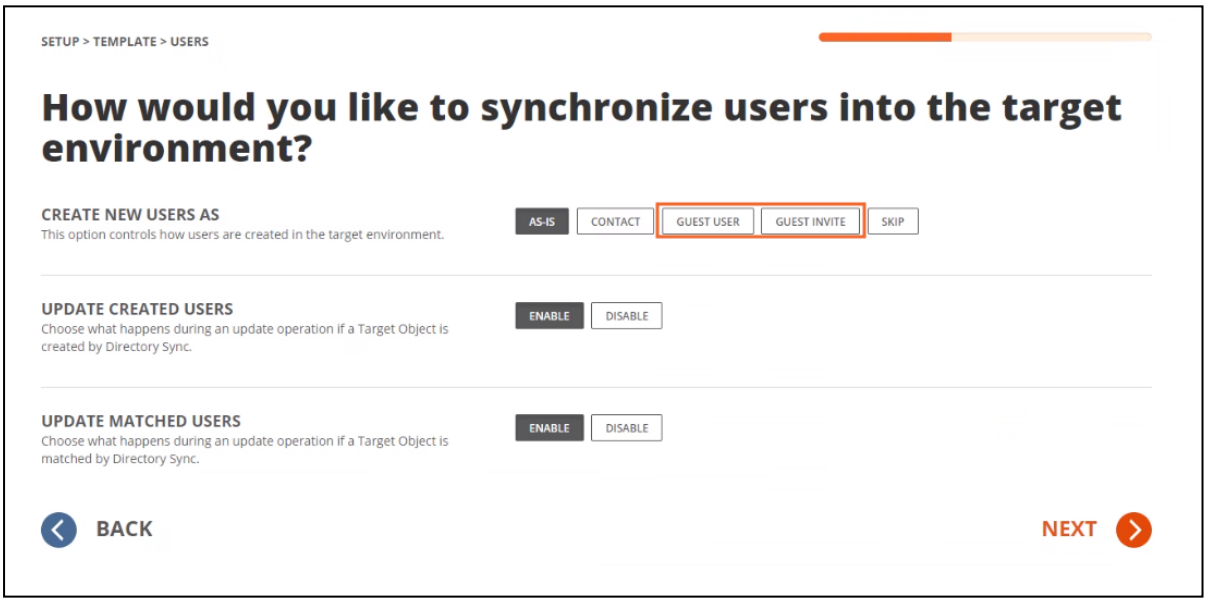


Figure 1: Example Template Wizard - Create New Users – Guest Options

What does the Guest User option do?

The **Guest User** option (see figure 1) will create a user object with the type of Guest within the destination directory configured in the workflow. This user's password will be set and managed within the target directory management controls. This user's UPN, Display Name and email address will be constructed based on the template mapping controls configured within the workflow.

What does the Guest Invite option do?

The **Guest Invite** option (see figure 1) will create a user object with the type of Guest within the destination directory configured in the workflow and immediately send an invitation to the source email user account. This user's UPN will be constructed automatically by Microsoft to meet their requirements for B2B functionality. This user's password will not be set and will continue to be managed from the source directory management tools and administrators. All other attributes set during creation will be determined by the template mapping controls configured within the workflow.

Can I send an invitation later if I didn't send one during creation?

Yes, Microsoft provides numerous methods for managing invitations. For more details, see the Microsoft Entra ID B2B documentation.

Can I match to an existing Guest user and update it?

Yes, Directory Sync can match and update existing Guest user types in Active Directory and Microsoft Entra ID.

What is the recommend matching attribute for Guest Users?

To match a source user object to a target Guest user object can sometimes be challenging because depending on the type of target Guest user object, there may not be a readily available attribute or property that can be used for an exact match to ensure an accurate match.

How to identify unique attributes for Matching to Guest Users

Before synchronization, you must first decide how to derive the matching attribute pairs between the source user object and target guest object. In other words, what parameters in your environment are unique to your external collaborators? Determine a parameter that distinguishes these external collaborators from members of your own organization.

A common approach to resolve this is to:

- Designate an unused attribute (for example, extensionAttribute1) to use as the source attribute that will match to a unique identifier attribute, such as email, in the target.
- Next construct the value for that attribute from other source properties, to create a unique identifier that will be found in the target. For example, use the email address of the source user to construct the extensionAttribute1 value as *Source Local Part @ Target Domain*.

Can I create a local user, so it is ready to be synchronized up to Microsoft Entra ID as a Guest?

Yes, Directory Sync supports the creation of local user objects for this purpose. Simply configure the template mappings to set the attribute value of the predetermined attributed which will be used by Microsoft Entra Connect to set the *UserType* = *Guest* in the cloud object. If you are using a different method within Microsoft Entra Connect, adjust your mapping rules to fit your needs.

You can use Microsoft Entra Connect to sync the accounts to the cloud as Microsoft Entra B2B users (that is, users with *UserType* = *Guest*). This enables your users to access cloud resources using the same credentials as their local accounts, without giving them more access than they require.

For more information about How to grant local users access to cloud apps read this Microsoft article on the topic.

For details on How to enable synchronization of UserType for Microsoft Entra Connect then please read this Microsoft document.

Additional Information

How To Use Guest Users in Directory Sync

What is guest user access in Microsoft Entra ID B2B?

Microsoft Entra ID B2B best practices

Microsoft Entra ID B2B documentation

Properties of an Microsoft Entra ID B2B collaboration user

Quickstart: Add guest users to your directory in the Azure portal

Add guests to the global address list

Product Licensing

The product licensing is based on the number of **unique source accounts** processed by a Directory Sync Workflow. The licenses are consumed when the Directory Sync Workflow creates or updates the target objects.

The following object types do not consume any license:

- Distribution Group
- Security Group
- Mail Enabled Security Group
- Teams
- M365 Group mailboxes
- Contacts
- Computer accounts
- Guest

Licensing for bi-directional, one to many and many to one scenario.

Since product licensing is based on unique source accounts, there will only be one license consumed per account in a bi-directional sync or in a one-to-many scenario. Additional licenses are consumed in a many-to-one scenario.

Refer to the below examples for details.

One to One Environment Pair with bi-directional sync

- User1@Contoso.com matched to User1@fabrikam.com
- User1@fabrikam.com matched to User1@Contoso.com

Only consumes one license because it is a bi-directional sync for source account User1@Contoso.com

One to Many Environment Pair

- User1@Contoso.com matched to User1@fabrikam.com
- User1@Contoso.com matched to User1@foo.dom

Only consumes one license, because even though the target users are from two different environments, the syncs are for the same source account User1@Contoso.com

Many to One Environment Pair

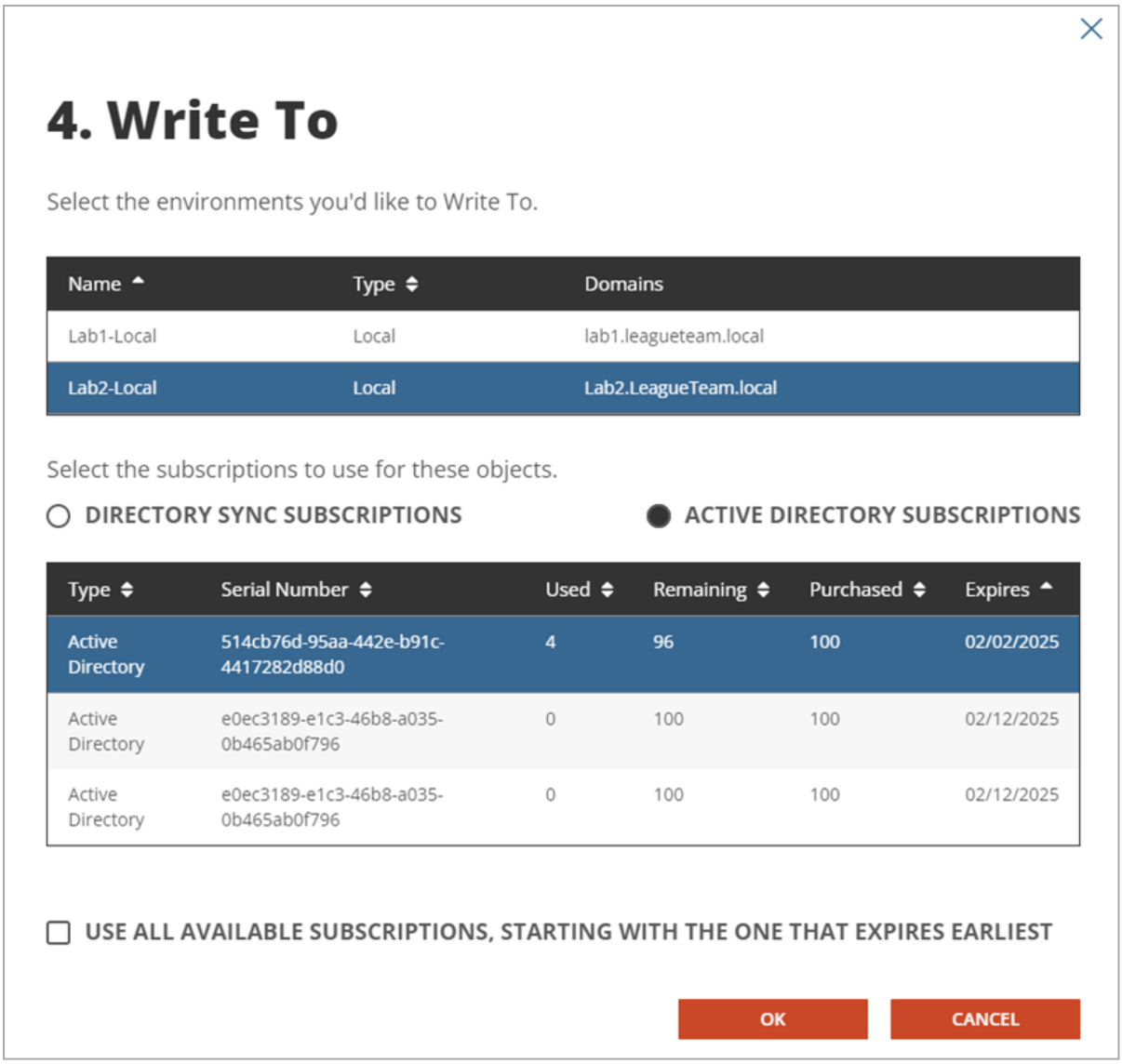
- User1@fabrikam.com matched to User1@Contoso.com
- User1@foo.dom matched to User1@Contoso.com

Consumes two licenses because User1@fabrikam.com and User1@foo.dom are two unique source accounts.

Licensing related to the Write To workflow task

Including at least one Write To environment is required. After data has been matched, mapped, and filtered, you must determine your target and where to place the new objects and/or sync objects that were matched.

The Write To workflow task is also where you need to configure the license consumption. From The Write To task screen, select the license subscription to use. You may select one or more licenses from the same subscription. The license that expires earliest will be consumed.



AI Features

Note: By default, AI features are enabled in your organization. To opt-out, please read this **article**.

On Demand Migration for Active Directory uses Artificial Intelligence to generate summary reports from logging data produced during directory synchronization operations.

- All data stays within your On Demand Region and reports are only available to view in the On Demand organization where they were generated.
- AI generated reports are cached for a period and then subsequently removed on the same schedule as the logs used to generate the report.

- Data is consumed by AI only when you request a report be generated.
- Data is used only to generate the summary report and will never be used for AI training.
- AI does not have access to privileged accounts or application consents and is not provided with the rights to perform any migration activities. All user-initiated AI activities are recorded for auditing purposes via the Activity Trail module in On Demand.

Workflow Run History AI Reports

Workflow run history reports generated by AI are available in Directory Sync.

To generate a Workflow run history AI report:

1. Select a Workflow from the Workflows list and click the **History** button.
2. Select the **Generate AI Report** link next to a run in the run history list.
3. Once generation is complete, click on **View AI Report** link.

The generated report contains a Migration Summary and an Issue Summary. Knowledge Base Articles may be suggested to assist in correcting issues. AI reports are available to view for 30 days.

Settings

Environments

What is an Environment?

If a workflow is a series of action steps, an environment is the receiver of those actions. On the Select Environments screen you will choose two or more environments that the workflow will take actions against. You need at least two so that you have at least one source and one target, but you can choose several in a more complex migration scenario. For example, you may choose to read from two different environments as sources, to be written to a single target environment.

Where do I manage Environments?

To manage environments, simply open the left navigation menu and click **Environments**, located under **Settings**, see *figure 1*.

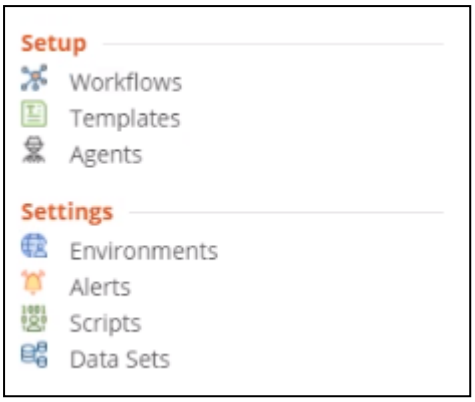


Figure 1: Directory Sync Setup and Settings Menu

How are Local Environments added?

To add a local environment:

1. On the *Environments* page, Click the **New** button. The *Select your Environment type* page appears.
2. Select Local and click **Next**.
3. Enter a name for your environment and click **Next**.
4. Enter a name for your agent and click **Next**.
5. Enter values in the following fields:
    - **Target Domain Controller IP Address** – The IP address of the target Domain Controller.
    - **Target Domain Controller Ping Interval** - The number of seconds the script will sleep between pings to the defined target domain controller. The default value is 300 seconds.
    - **Timeout Before Job Failure** – The number of minutes to wait after Credential Cache job is downloaded by the agent before marking the job a failure due to timeout. The default value is 180 minutes.
    - **Timeout for User Credential Prompt** – The number of minutes to prompt the user with a dialog box to enter their target domain credentials for caching. The default value is 5 minutes
6. Click **Save Profile**. The Credential Cache Profile is added to the list.

How do you export a list of Users, Groups, Contacts, and Devices in an environment?

Select an environment in the Environments table and then click **Details**. On the Details page, click the **Export** button to download a CSV file of the Users, Groups, Contacts, and Devices.

How do you unmatch Users, Groups, Contacts, and Devices so they will not be synchronized?

Select an environment in the Environments table and then click **Details**. On the Details page, select an object in the table and click the **Unmatch** button. The Match Status for the object will change to "Unmatched" and the object will not be synchronized.

The Unmatch action is not supported for objects belonging to the Tenant-to-Tenant project and registered devices.

How do you view logs for local environments?

Select a local environment in the Environments table and then click **Password Logs** or **Discovery Logs** to export a CSV with password or discovery information.

How do you discover local environments?

Select a local environment in the Environments table and then click **Discover** to begin the discovery process for the environment.

How do you filter out users and groups in cloud environments you do not want to synchronize?

Select a cloud environment in the Environments table and then click **Settings**. Then select the **Object Filter** tab to view the filter options. Uncheck the object types you wish to exclude. Options to exclude unlicensed and disabled accounts are also available. Click **Attribute Filters** to build filters that allow you to be more specific as to which object(s) to sync. Select the **Filter Groups** tab to enable Group filters.

How do you set the object filter to synchronize Microsoft Entra ID Joined devices in cloud environments?

If you subscribe to the Microsoft Entra ID Joined Device add on feature, you can enable the Microsoft Entra ID Joined device object filter option in Settings. To enable the Microsoft Entra ID Joined device option, select a cloud environment in the Environments table and then click **Settings**. Then select the **Object Filter** tab to view the filter

options. Check the **Microsoft Entra ID Joined** devices option. Click **Attribute Filters** to build filters that allow you to be more specific as to which device(s) to sync.

The below table displays filterable properties and the object types that can be filtered by them. ✓ = The property can be used to filter this object type.

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
AcceptMessagesOnlyFrom		✓	✓	✓	
AcceptMessagesOnlyFromDLMembers		✓	✓	✓	
AcceptMessagesOnlyFromSendersOrMembers		✓	✓	✓	
AccessType				✓	
AccountDisabled	✓				
AddressListMembership		✓	✓	✓	
AdministrativeUnits	✓	✓	✓	✓	
Alias		✓	✓	✓	
AllowAddGuests				✓	
AllowUMCallsFromNonUsers	✓				
AlwaysSubscribeMembersToCalendarEvents				✓	
ArbitrationMailbox		✓	✓		
ArchiveRelease	✓				
AssistantName	✓				
AuditLogAgeLimit				✓	
AuthenticationPolicy	✓				
AutoSubscribeNewMembers				✓	

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
BypassModerationFromSendersOrMembers		✓	✓	✓	
BypassNestedModerationEnabled			✓		
CalendarMemberReadOnly				✓	
CalendarUrl				✓	
CertificateSubject	✓				
City	✓				
Classification				✓	
Company	✓				
ConnectorsEnabled				✓	
ConsumerNetID	✓				
CountryOrRegion	✓				
CustomAttribute1		✓	✓	✓	✓
CustomAttribute10		✓	✓	✓	✓
CustomAttribute11		✓	✓	✓	✓
CustomAttribute12		✓	✓	✓	✓
CustomAttribute13		✓	✓	✓	✓
CustomAttribute14		✓	✓	✓	✓
CustomAttribute15		✓	✓	✓	✓
CustomAttribute2		✓	✓	✓	✓

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
CustomAttribute3		✓	✓	✓	✓
CustomAttribute4		✓	✓	✓	✓
CustomAttribute5		✓	✓	✓	✓
CustomAttribute6		✓	✓	✓	✓
CustomAttribute7		✓	✓	✓	✓
CustomAttribute8		✓	✓	✓	✓
CustomAttribute9		✓	✓	✓	✓
Database				✓	
DataEncryptionPolicy				✓	
Department	✓				
DirectReports	✓				
DisplayName	✓	✓	✓	✓	✓
DistinguishedName	✓	✓	✓	✓	
EmailAddressPolicyEnabled		✓	✓	✓	
ExchangeGuid				✓	
ExchangeVersion	✓	✓	✓	✓	
ExpansionServer			✓	✓	
ExtensionCustomAttribute1		✓	✓	✓	
ExtensionCustomAttribute2		✓	✓	✓	

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
ExtensionCustomAttribute3		✓	✓	✓	
ExtensionCustomAttribute4		✓	✓	✓	
ExtensionCustomAttribute5		✓	✓	✓	
Extensions		✓			
ExternalDirectoryObjectId	✓	✓	✓	✓	
ExternalEmailAddress		✓			
Fax	✓				
FileNotificationsSettings				✓	
FirstName	✓				
GeoCoordinates	✓				
GrantSendOnBehalfTo		✓	✓	✓	
GroupExternalMemberCount				✓	
GroupMemberCount				✓	
GroupPersonification				✓	
GroupSKU				✓	
GroupType			✓	✓	
Guid	✓	✓	✓	✓	
HasPicture		✓			
HasSpokenName		✓			

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
HiddenFromAddressListsEnabled		✓	✓	✓	
HiddenFromExchangeClientsEnabled				✓	
HiddenGroupMembershipEnabled			✓	✓	
HomePhone	✓				
Id	✓	✓	✓	✓	
Identity	✓	✓	✓	✓	
InboxUrl				✓	
Initials	✓				
InPlaceHolds				✓	
InPlaceHoldsRaw	✓			✓	
IsExternalResourcesPublished				✓	
IsLinked	✓				
IsMailboxConfigured				✓	
IsMembershipDynamic				✓	
IsSecurityPrincipal	✓				
IsSoftDeletedByDisable	✓				
IsSoftDeletedByRemove	✓				
IsValid	✓	✓	✓	✓	
Language				✓	

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
LastExchangeChangedTime		✓	✓	✓	
LastName	✓				
LegacyExchangeDN	✓	✓	✓	✓	
LinkedMasterAccount	✓				
MacAttachmentFormat		✓			
MailboxLocations	✓				
MailboxProvisioningConstraint	✓			✓	
MailboxProvisioningPreferences	✓				
MailboxRegion	✓			✓	
MailboxRegionLastUpdateTime	✓				
MailboxRelease	✓				
MailTip		✓	✓	✓	
MailTipTranslations		✓	✓	✓	
ManagedBy			✓	✓	
ManagedByDetails				✓	
Manager	✓				
MaxReceiveSize		✓	✓	✓	
MaxRecipientPerMessage		✓			
MaxSendSize		✓	✓	✓	

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
MemberDepartRestriction			✓		
MemberJoinRestriction			✓		
MessageBodyFormat		✓			
MessageFormat		✓			
MicrosoftOnlineServicesID	✓				
MigrationToUnifiedGroupInProgress			✓	✓	
MobilePhone	✓				
ModeratedBy		✓	✓	✓	
ModerationEnabled		✓	✓	✓	
Name	✓	✓	✓	✓	
NetID	✓				
Notes	✓			✓	
ObjectCategory	✓	✓	✓	✓	
ObjectClass	✓	✓	✓	✓	
ObjectState	✓	✓	✓	✓	
Office	✓				
OrganizationalUnit	✓	✓	✓	✓	
OrganizationId	✓	✓	✓	✓	
OriginatingServer	✓	✓	✓	✓	

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
OtherFax	✓				
OtherHomePhone	✓				
OtherTelephone	✓				
Pager	✓				
PeopleUrl				✓	
Phone	✓				
PhoneticDisplayName	✓				
PhotoUrl				✓	
PoliciesExcluded		✓	✓	✓	
PoliciesIncluded		✓	✓	✓	
PostalCode	✓				
PostOfficeBox	✓				
PreviousRecipientTypeDetails	✓				
RecipientType	✓	✓	✓	✓	
RecipientTypeDetails	✓	✓	✓	✓	
RejectMessagesFrom		✓	✓	✓	
RejectMessagesFromDLMembers		✓	✓	✓	
RejectMessagesFromSendersOrMembers		✓	✓	✓	
RemotePowerShellEnabled	✓				

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
ReportToManagerEnabled			✓	✓	
ReportToOriginatorEnabled			✓	✓	
RequireSenderAuthenticationEnabled		✓	✓	✓	
ResetPasswordOnNextLogon	✓				
RunspaceId	✓	✓	✓	✓	
SamAccountName	✓		✓		
SendModerationNotifications		✓	✓	✓	
SendOofMessageToOriginatorEnabled			✓	✓	
SeniorityIndex	✓				
ServerName				✓	
SharePointDocumentsUrl				✓	
SharePointNotebookUrl				✓	
SharePointSiteUrl				✓	
Sid	✓				
SidHistory	✓				
SiloName	✓				
SimpleDisplayName	✓	✓	✓		
SKUAssigned	✓				
StateOrProvince	✓				

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
StreetAddress	✓				
StsRefreshTokensValidFrom	✓				
SubscriptionEnabled				✓	
TelephoneAssistant	✓				
Title	✓				
UMCallingLineIds	✓				
UMDialPlan	✓				
UMDtmfMap	✓	✓	✓		
UpgradeDetails	✓				
UpgradeMessage	✓				
UpgradeRequest	✓				
UpgradeStage	✓				
UpgradeStageTimeStamp	✓				
UpgradeStatus	✓				
UseMapiRichTextFormat		✓			
UsePreferMessageFormat		✓			
UserAccountControl	✓				
UserCertificate		✓			
UserPrincipalName	✓				

Property Name	Users	Contacts	Distribution And Mail Enabled Security Groups	Unified Groups And Teams	Devices
UserSMimeCertificate		✓			
VoiceMailSettings	✓				
WebPage	✓				
WelcomeMessageEnabled				✓	
WhenChanged	✓	✓	✓	✓	
WhenChangedUTC	✓	✓	✓	✓	
WhenCreated	✓	✓	✓	✓	
WhenCreatedUTC	✓	✓	✓	✓	
WhenSoftDeleted	✓			✓	
WindowsEmailAddress	✓	✓	✓		
WindowsLiveID	✓				
YammerEmailAddress				✓	
Description			✓	✓	
OperatingSystem					✓
OperatingSystemVersion					✓
ProfileType					✓
EmailAddresses		✓	✓	✓	

Additional Information

Password Sync

Password Sync

What is Password Sync?

The Password Sync feature is designed to synchronize passwords from environment to environment without being directly tied to workflows.

However, a workflow that reads all the users in scope for password sync must exist and there must be a workflow that matches the source to target objects. If there is no match, passwords will not be synchronized.

How many agents can be set to monitor password changes?

You may only have one agent set to detect password changes. Having a single agent for this task avoids conflicts caused by multiple agents updating passwords at the same time.

What does the Allow password changes option do?

When the “Allow password changes” option is selected, objects passwords will be updated if matched to any environment set to detect password changes.

How is it determined which users are in scope for password sync?

The environment filter determines which users are in scope for password change. if matched and in environment scope, they will be updated if a source changes.

Is two-way password sync possible?

Two-way password sync is possible by selecting to monitor password changes in the source and target environments.

Are passwords encrypted during password sync?

The password hash is stored encrypted in the database to determine if password changes must occur on the target. Passwords are never converted to plain text.

How often does the agent check for password changes?

The agent designated for password change monitoring checks for changes every 30 seconds.

Creating an alert for when agents go offline is recommended in case the password monitoring agent encounters an issue.

What access is needed?

The account that the agent has been configured with must have access to the admin$ share of the domain controllers.

Can password sync be applied to a subset of users?

A LDAP query can be entered in the LDAP Filter field to control the application of the Password Sync feature.

What is Password Propagation Service?

Password Propagation Service is a component of Directory Sync that allows password synchronization in environments without RC4 Encryption. Unlike the Legacy Password Monitor Service, which requires RC4 Encryption, Password Propagation Service simply copies the password from the source to the target. When a password changes in the source, the password filter installed on every domain controller in the source environment will capture the password and use the Password Propagation Service to set the password in the target using LDAPS security. Please refer to the On Demand Migration Password Propagation Service User Guide for installation/configuration.

What is Modern Password Monitor Service?

Modern Password Monitor Service adds support for Microsoft Advance LSA Protection by installing a Password Filter on the Domain Controller. Additional details about Modern Password Monitor Service can be found in the On Demand Migration Active Directory Modern Password Sync Setup Quick Start Guide.

Alerts

What is an Alert?

Alerts may be added to keep administrators informed of the success completion and/or failure of any workflow. Alerts are delivered as status emails to the designated recipients. For each workflow choose the previously created alerts or add a new alert. Easily add multiple recipients, by separating the addresses with a semicolon.

Where do I manage Alerts?

To manage workflow alerts, simply open the left navigation menu and click **Alerts**, located under **Settings**, see *figure 1*.

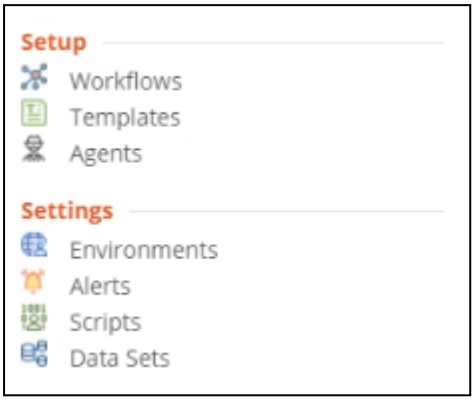


Figure 1: Directory Sync Setup and Settings Menu

How do you setup a new Alert?

Follow these steps to create a new workflow alert.

1. Navigate to Alerts.
2. Click *New*.
3. Enter a *Name*, click *Next*.
4. Enter recipients. To add multiple recipients, separate addresses with a semicolon (;).
5. Click *Next*.
6. Choose Language preference, click *Next*.
7. Choose which events trigger alerts.
8. Choose Workflow Failure at a minimum.
9. Do not choose Local Agent Offline for a Cloud only workflows and environments.
10. Click *Next*.
11. Click *Finish*.

How do you add an Alert to a workflow?

Follow these steps to add an alert to an existing workflow.

1. Navigate to Workflows.
2. Locate and select Write workflow created earlier.
3. Click the *Settings* button.

4. Click *Alerts*.
5. Click *Add*.
6. Select the *Alert* created in the previous steps.
7. Click *OK*.
8. Navigate to Workflows.
9. Repeat these steps for each workflow.

What workflow events can generate an alert?

You can select to have an email notification sent when the workflow finishes for the following events:

- Workflow Completion - A notification will be sent each time your workflow completes successfully.
- Workflow Failure - A notification will be sent each time your workflow completes successfully.
- Local Agent Offline - A notification will be sent each time local agents go offline.

How do I edit an Alert?

Alerts can be edited on the Alerts page by selecting an Alert in the table and clicking "Settings."

How do I enable or disable an Alert?

Active alerts can be disabled on the Alerts page by selecting the alert in the table and clicking "Disable." Disabled alerts can be activated on the Alerts page by selecting the alert in the table and clicking "Enable."

Additional Information

Workflows
Workflow Test Mode
Evaluate Changed Objects Only

Scripts

What is a script?

A script entry is used to securely store a PowerShell script file and can be run as part of workflow at any point in the process using the Script Task.

Where do I manage saved Scripts?

To manage saved scripts, simply open the left navigation menu and click **Scripts**, located under **Settings**, see *figure 1*.

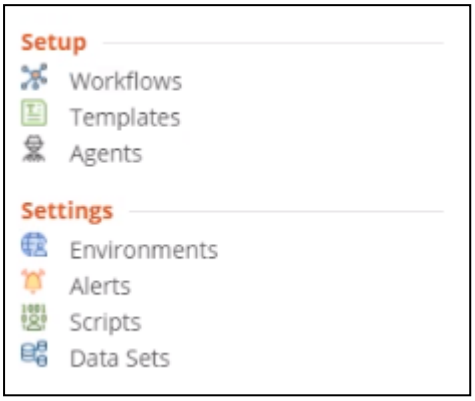


Figure 1: Directory Sync Setup and Settings Menu

How do you select a PowerShell script to run?

On the Run PowerShell Scripts screen, choose an existing script to run. Stop workflow on error will stop the workflow if an error is encountered, so placement of this step within the workflow sequence must be considered.

How do you add a new PowerShell script?

On the Scripts page, click the **New** button to add a new script to the collection. Name your script, and choose a local environment for it to apply to. Directory Sync does not validate your scripts, so be sure that you test them first in a non-production environment. Note that all scripts are run under the service account and an account with the required AD Rights must be configured to logon to the service.

Data Sets

What is a Data Set?

Data Sets can be used in conjunction with the “LookupValue” function to find source values and replace with target values.

What are Data Sets used for?

Data Sets are ideal for managing long lists of replacement strings commonly associated with Directory migration and consolidation projects.

For example, if a Data Set is named "Domains" and you want to replace "contoso.com" with "hr.contoso.com", set the Key Value to "contoso.com" and Return Value to "hr.contoso.com". Then in the appropriate attribute advanced mapping (e.g. UserPrincipalName) you could reference a formula like, LookupValue('Domains', s.UserPrincipalName, null)

This formula will find contoso.com from the UserPrincipalName attribute with hr.contoso.com.

Some other common uses cases might be:

- Update common attributes values like Department from the old format to the new format (e.g. HR to Human Resources)
- Reorganize OUs but applying data sets to determine the target OU
- Map complex environments with multiple source domains to different target domains
- Breakdown complex text strings into smaller pieces for use within another function

Where do I manage saved Data Sets?

To manage saved data sets, simply open the left navigation menu and click **Data Sets**, located under **Settings**, see *figure 1*.

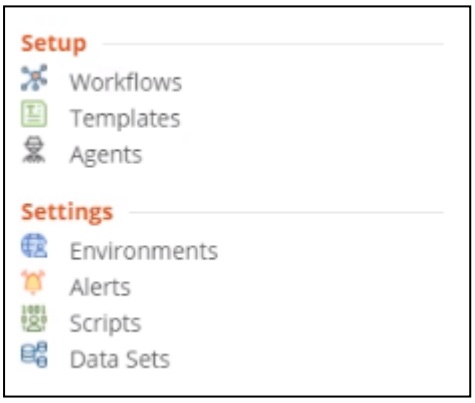


Figure 1: Directory Sync Setup and Settings Menu

How do I create a new Data Set?

To create a Data Set:

1. Select "Data Sets" under Settings in the left navigation menu.
2. Click “New”.
3. On the General tab, enter a name and description for the Data Set and click "Save".
4. Click the "Values" tab.
5. Click "New" to enter key values and return values or click "Import" to choose a file of key values and return values. If importing a data set, click "Download Example" to download an example CSV.

How do I import a Data Set?

On the Data Sets details screen, click the Import button to select a CSV with Key Value and Return Value columns.

Note: The imported CSV will replace any existing data in the data set.

Can you export a Data Set?

Select the data set(s) and click the Export button to generate a CSV file of existing data sets. You can then use the Import action to upload modifications to the list if desired.

How do I archive a Data Set?

Select the data set(s) and click the Archive button to archive the data set(s).

How-To

The following Quick Start Guides have been created to assist with common directory sync scenarios.

- 2-way GAL Sync
- AD Password Sync
- AD SID History Sync
- AD Users, Groups, and Contacts Sync
- Multi-Geo Tenant Users, Groups, Teams, and Unified Group Sync

How To Use Guest Users in Directory Sync

How do I prevent Guest Users from being sent an Invitation during creation?

To prevent an invitation being sent when a Guest user is created, modify the default mappings for the property named **SendInvitationMessage** to be **False** before creating your Guest users.

Follow these steps to complete this task:

1. From the landing page or the application menu, choose Directory Synchronization
2. Open the left navigation menu 

3. Select **Templates** under **Setup**

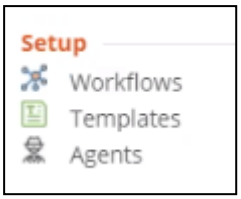


Figure 2: Navigate to Templates

4. Locate the template to be modified
5. Select the template then click **Settings**
6. Navigate to the **Mapping** tab
7. Search for the attribute **SendInvitationMessage**
8. Double click the resulting record to open for editing

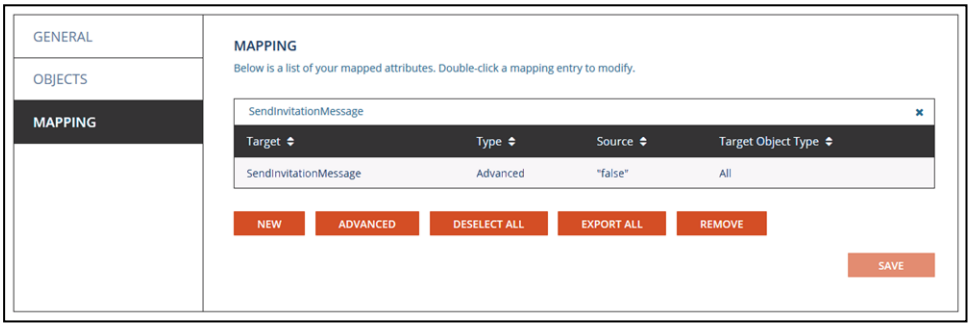


Figure 3: Example Search within Template Mapping Tab

9. Once open, click **Advanced**

10. Modify the default value of “True” to be “False”

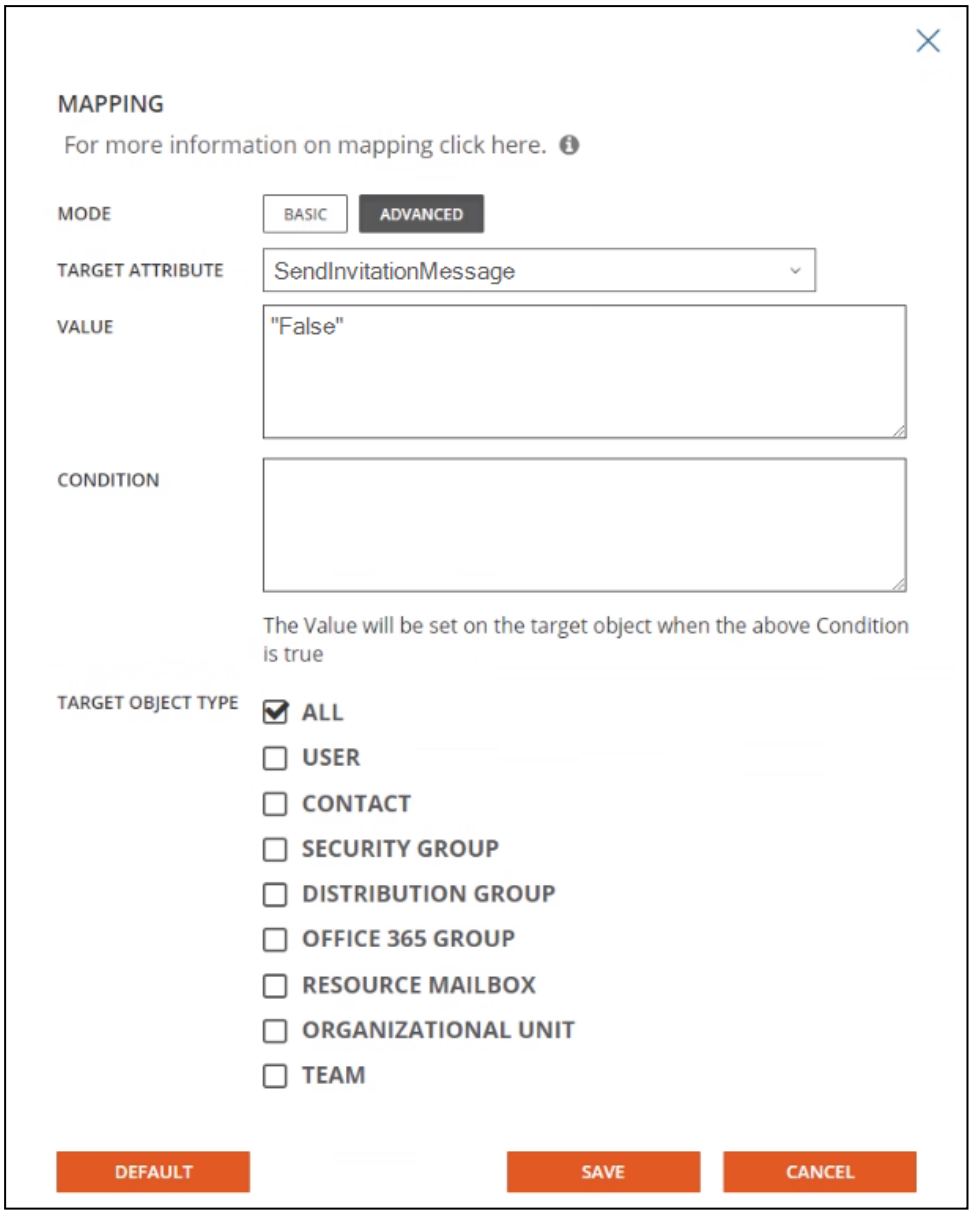


Figure 4: Example of Advanced Mapping used to prevent Guest Invitations from being sent

11. Click **Save**
12. Once saved you may navigate out of Templates to your next destination

How do I create local users, so they are ready to be synchronized up to Microsoft Entra ID as a Guest?

Once you have decided on the local on-premises attribute to be used for this purpose, then it is simply a matter of setting that attribute mapping to set a value of “Guest” for the appropriate set of users.

The following provides a simple example template mapping using ExtensionAttribute1 as the designated local attribute to be set as “Guest” for Microsoft Entra Connect to sync them up to Microsoft Entra ID as B2B accounts.

1. From the landing page or the application menu, choose Directory Synchronization
2. Open the left navigation menu 
3. Select **Templates** under **Setup**

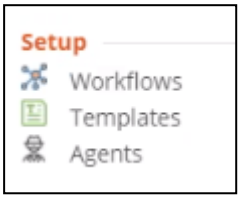


Figure 5: Navigate to Templates

4. Locate the template to be modified
5. Select the template then click **Settings**
6. Navigate to the **Mapping** tab
7. Search for the attribute **ExtensionAttribute1**
8. Double click the resulting record to open for editing
9. Once open, click **Advanced**
10. Modify the value to be “Guest”

11. Set the **Condition** to Action = *"create"* if you wish to only apply this rule to new users

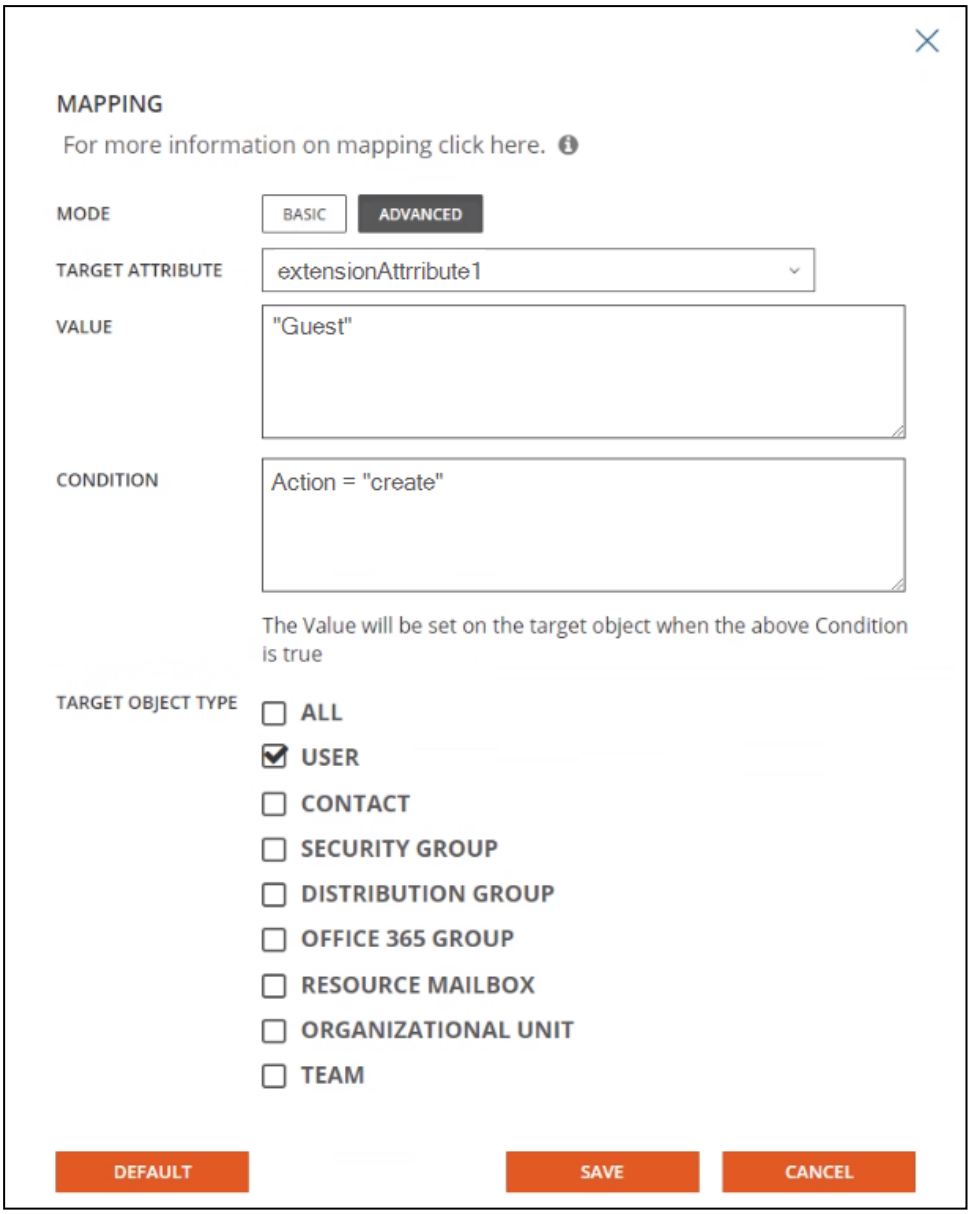


Figure 6: Example of Advanced Mapping used to create local users, so they are ready to be synchronized up to Microsoft Entra ID as a Guest

12. Select **User** as the **Target Object Type**
13. Click **Save**
14. Once saved you may navigate out of Templates to your next destination

When you run your workflow to create your local users with the above mappings and Microsoft Entra Connect is configured to sync as B2B users. This is only one example, there are different methods that be used to provide the same result depending on your environment needs.

Please note: If you choose this approach, you must ensure that the designated attribute is populated with the correct value (Guest or Member) for all existing user objects in on-premises Active Directory that are synchronized to Microsoft Entra ID before enabling synchronization of the “UserType” attribute.

For details on How to enable synchronization of UserType for Microsoft Entra Connect then please read this Microsoft document.

How do I ensure my Guest Users are visible in the Global Address Lists (GAL)?

By default, guests aren't visible in the Exchange Global Address List.

If you have already created your Guest Users manually or otherwise, you may run a few PowerShell commands to set the appropriate property. Here’s how to Add guests to the global address list.

If you are using Directory Sync to create and update your Guest Users, then use the steps listed below to make sure your guests are visible in the global address list.

To ensure the Guest user is visible in the GAL, modify the default mappings for the property named **HiddenFromAddressListsEnabled** to be False before creating or synchronizing your Guest users.

The default mapping for **HiddenFromAddressListsEnabled** is to synchronize the source user object visibility property to the same in the target. If this is not the desired behavior, then follow these steps to guarantee the user will be visible.

Follow these steps to complete the task:

1. From the landing page or the application menu, choose Directory Synchronization
2. Open the left navigation menu 
3. Select **Templates** under **Setup**

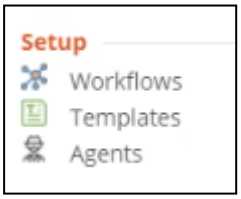


Figure 7: Navigate to Templates

4. Locate the template to be modified
5. Select the template then click **Settings**

6. Navigate to the **Mapping** tab

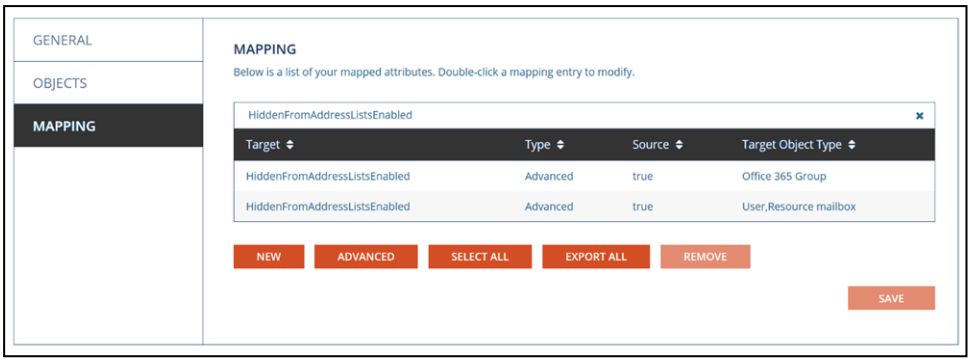


Figure 8: Example Search within Template Mapping Tab (click t enlarge)

7. Search for the attribute **HiddenFromAddressListsEnabled**
8. Locate the mapping where the **Target Object Type** is **User**
9. Double click the resulting record to open for editing
10. Once open, click **Advanced**

11. Modify the value to be “false”

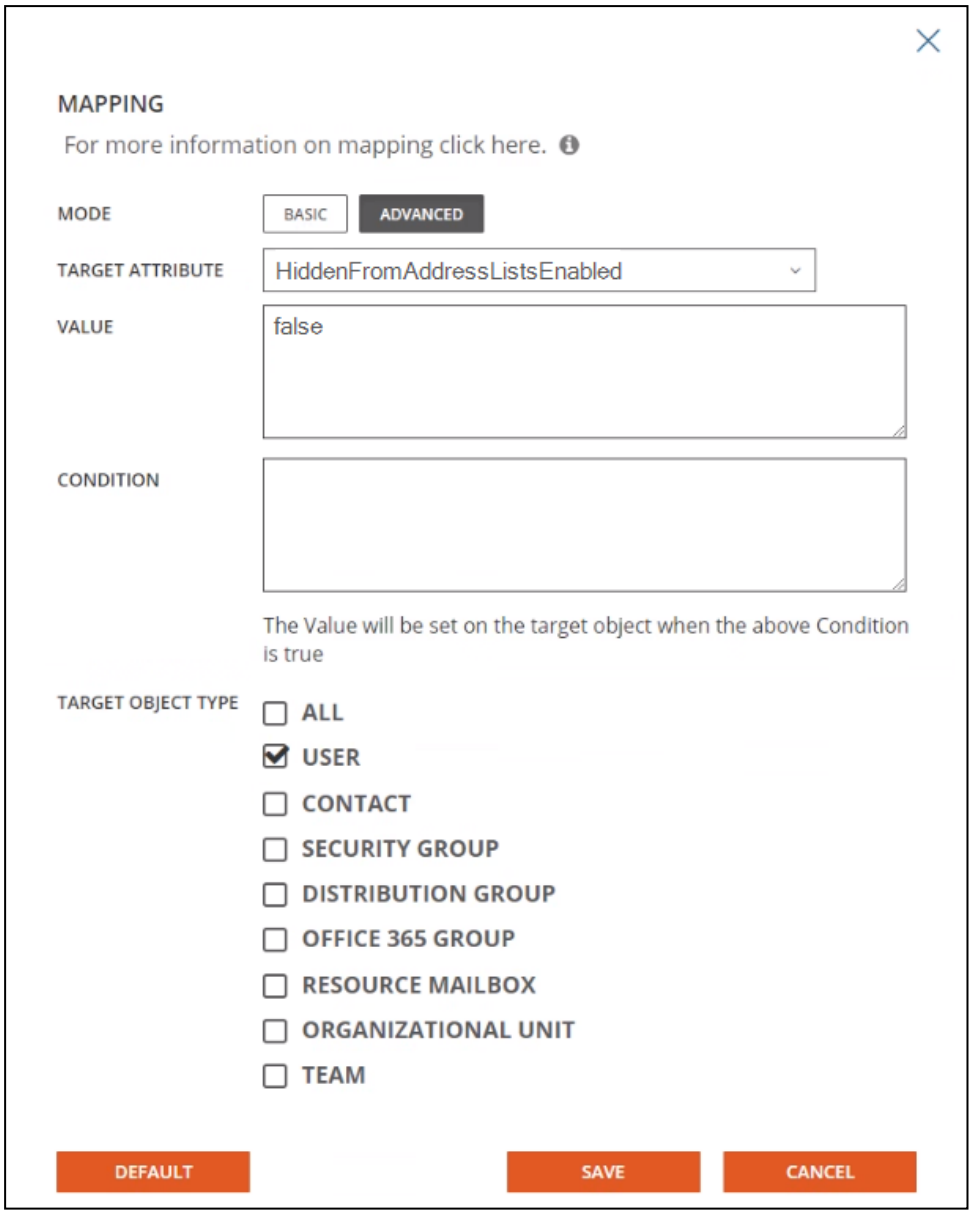


Figure 9: Example of Advanced Mapping used to ensure a Guest User is visible in the GAL

12. Optionally you may set a condition action ("create", "update", or "delete") whereby the object is only acted upon when the condition is satisfied
13. Click **Save**
14. Once saved you may navigate out of Templates to your next destination

Additional Information

Guest Users in Directory Sync

How-To

The following Quick Start Guides have been created to assist with common directory sync scenarios.

- 2-way GAL Sync
- AD Password Sync
- AD SID History Sync
- AD Users, Groups, and Contacts Sync
- Multi-Geo Tenant Users, Groups, Teams, and Unified Group Sync

Planning the Migration Project

A typical migration project using Active Directory can be broken up into six (6) phases.

- Phase 1: Install Directory Sync agents and create the Workflow
- Phase 2: Identify Devices and their related Users and Groups to migrate (Concurrent with Phase 3)
- Phase 3: Install Active Directory agents and Register Devices (Concurrent with Phase 2)
- Phase 4: ReACL Devices
- Phase 5: Cutover Devices
- Phase 6: Cleanup

  Note: The Cleanup process typically occurs several months after the completion of the project.

This user guide walks you through the steps required to complete each phase, which can also be used to migrate devices from AD environments to Entra environments. The Active Directory Entra-Join Quick Start Guide walks you through the process of configuring and performing migrations for AD to Entra migrations.

Best practices for each phase of the migration project are presented below:

Phase 1: Install Directory Sync agents and create the Workflow

- Directory Sync is used to synchronize objects and must be configured before using Active Directory.
- Only those Devices which are in scope of the synchronization Workflow and the filters on its Environments will be available in Active Directory.
- At a minimum the Read From and Match To steps of the synchronization Workflow must be present for Devices.

Phase 2: Identify Devices and their related Users and Groups to migrate (Concurrent with Phase 3)

- Before migrating Devices do some analysis and planning to see what Users and Groups may need to be migrated, what groups need to be consolidated, how duplicates will be handled, etc.

- More than one Workflow can be used to control the target destinations of Users and Groups.
- Identifying Devices, Users, and groups to migrate can be accomplished concurrently with installing Active Directory agents and Registering Devices in Phase 3.

Phase 3: Install Active Directory agents and Register Devices (Concurrent with Phase 2)

- The Active Directory agent should be installed on the Devices to be migrated or pushed out via third party tool.
- Sufficient time should be allowed to address any issues with Device registration with the server. Correcting registration issues can take more time than expected. A typical large company with a large number of Devices may need a couple of weeks of off and on work to resolve registration issues with all Devices.
- Resolving Device registration issues can be accomplished concurrently with identifying Users and groups to migrate in Phase 2.

Phase 4: ReACL Devices

- Run a ReACL (file level re-permissioning) job on as many Devices as possible early in the process.
- ReACL is a non-destructive process that can be repeated as often as necessary up until Cutover in Phase 5.
- Troubleshoot any Devices with ReACL jobs which did not complete successfully.
- Run a ReACL job again close to the actual Cutover date. This will allow you to complete most of the ReACL process early and provide time to resolve any issues with things such as anti-virus software and Group Policies.

Phase 5: Cutover Devices

- Using some test Devices, Users, and Groups, verify a successful Device Cutover.
- Create any custom Actions that may be required to run as part of the Cutover.
- Typically, a final ReACL job should be run the weekend before the scheduled Cutover to ensure any new Users and other changes are processed.
- Optionally, use the Auto-Pilot Cleanup option to prepare the AutoPilot-provisioned device for migation. This must be done before the cutover if the source Entra ID Joined device is Autopilot-provisioned and the Entra ID Join Profile has the Auto-Pilot Cleanup option selected.

- A workstation reboot is required after the target account is enabled, the source account is disabled, and the Cutover is complete. This is usually completed in the evening when fewer end-users are impacted. Any impacted end-users should be alerted that this reboot is necessary.

  Disabling SID Filter Quarantining on External Trusts

  To disable SID filter quarantining for the trusting domain, type a command using the following syntax at a command-prompt:

  ```
  Netdom trust TrustingDomainName /domain: TrustedDomainName
  /quarantine:No /usero: domainadministratorAcct /passwordo:
  domainadminpwd
  ```

  To re-enable SID filtering, set the `/quarantine:` command-line option to `Yes`.

  Allowing SID History to Traverse Forest Trusts

  The default SID filtering applied to forest trusts prevents user resource access requests from traversing the trusts with the credentials of the original domain. If you want to enable users to use the credentials that were migrated from their original domain, you can allow SID history to traverse forest trusts by using the Netdom command.

  To allow SID history credentials to traverse a trust relationship between two forests, type a command using the following syntax at a command-prompt:

  ```
  Netdom trust TrustingDomainName /domain: TrustedDomainName
  /enablesidhistory:Yes /usero: domainadministratorAcct /passwordo:
  domainadminpwd
  ```

  To re-enable the default SID filtering setting across forest trusts, set the `/enablesidhistory:` command-line option to `No`.

  For more information about configuring SID filtering refer to the Microsoft article available at https://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx.

Phase 6: Cleanup

- The Cleanup phase typically takes place about two months after all Device Cutovers are complete. During the Cleanup phase, all permissions should be removed from the source domain and then the Active Directory agent should be removed from the Devices.
- Before executing the Cleanup job to complete the Cleanup process it is recommended that you disable SID filtering/quarantine to verify that there are no issues with application access.
- Optionally, use the Set Intune Primary User action after the Device Cutover is completed.

Active Directory Requirements

Directory Sync

Environments

Prior to any migration of an Active Directory computer there are a few Directory Sync requirements to inventory your devices (computers). The first of which is your local on-premises environments or endpoints. To gain access to your devices from your on-premises Active Directory you must create and securely connect your Environments.

How do I add an Environment?

For complete details on how to add an environment, click here.

Workflows

The next required configuration for Directory Sync is to create a workflow that will inventory (read) your local on-premises Active Directory computers.

Directory Sync Agents

The final component required is to deploy at least one (1) Directory Sync agents that will be used to secure communicate and execute jobs against your Local Active Directory such a read or write.

How do I install a Directory Sync Agent?

For complete details on how to install an agent, click here.

Networking

Outbound Internet Access

By default, each computer being migrated will require outbound access to the public Internet to securely communicate with the Power365 services.

Important Tip: If your organization requires computers communicate externally using a web proxy see our web proxy configuration requirements.

Application Ports

Each computer being migrated will require the Active Directory device agent and this agent will communicate to the Power365 services, outbound over ports:

- 80
- 443
- 3030

Domain Controller Ports

Active Directory migrations also require a variety of Microsoft defined ports for communication between domain controllers. For a complete list of required ports, click here.

Important Tip: For complete port information, review the Service overview and network port requirements for Windows documentation from Microsoft Support.

Devices

The following is required for any Active Directory Computer(s) (devices) that will be migrated.

Device Agents

Each Active Directory Computer that will be migrated must have an agent installed on the workstation to orchestrate local jobs that must occur to prepare and execute the workstation's domain move.

Operating Systems

All computers or servers being migrated to the new domain must run one of the following operating systems:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019

- Windows Server 2022

Please Note: Entra ID Device Join is only supported for Windows 10 and 11.

PowerShell

- All client operating systems must have at least PowerShell 2.0 installed.

.NET Framework

- All Devices must have .NET Framework 4.7.2 or newer installed. This will appear as ".NET 4.7.2 Extended" in the add/remove programs list.
- If not present, an appropriate version of .NET Framework will be installed during agent installation if an internet connection is available.

Remote Devices

To successfully migrate a remote employee's remote device using the Offline Domain Join (ODJ) feature the Cache Credential action must be run to collect the user's target credentials, so later you may cutover the device, while it is disconnected from the network.

The following is required:

Cached Credentials Action

- One-way external trust must be configured from the source domain to the target domain when the Cache Credential activity is processed

For more information about AD Trusts, check out this MS Press article about configuring trusts.

Network

• Network connectivity to both the source and target environments (Active Directory Domain Controllers) when the Cache Credential activity is processed

Important Tip: Offline domain join files must be created prior to running the Offline Domain Join process. A full explanation of Microsoft's Djoin.exe utility and how to create these files can be found here.

How do I set up Offline Domain Join (ODJ)?

For complete details on how to set up ODJ, click here.

Web Proxy

Some organizations may require all computers communicating externally direct their traffic through a web proxy to centralize communications. Active Directory agents can be configured to use a web proxy for communication to the Power365 cloud services.

Proxy Server

- At least one (1) standard web proxy that supports http/TCP traffic.

Proxy Address

- The associated web proxy URL must be defined during configuration of the device agent.

Security

- If accessing the web proxy requires an additional username and password this will be required during configuration of the device agent.

Ports

All agents configured to use a web proxy will utilize the following outbound TCP ports:

- 80
- 443

Please Note: Agents configured to use a web proxy will not require UDP port 3030. For more information, see the Web Proxy Configuration under Architecture.

Important Tip: Additional bandwidth overhead may occur when a web proxy is utilized to centralize all traffic.

Repositories

The following four Device Actions, when used, will require a defined storage share accessible from the device being migrated:

1. Upload Logs
2. Device Download
3. Offline Domain Join
4. Microsoft Entra ID Cutover

How do I configure repositories?

For complete details on how to configure repositories, click here.

Additional Information

Directory Sync Requirements: Password Synchronization
Directory Sync Requirements: SID History

Setup

Environments

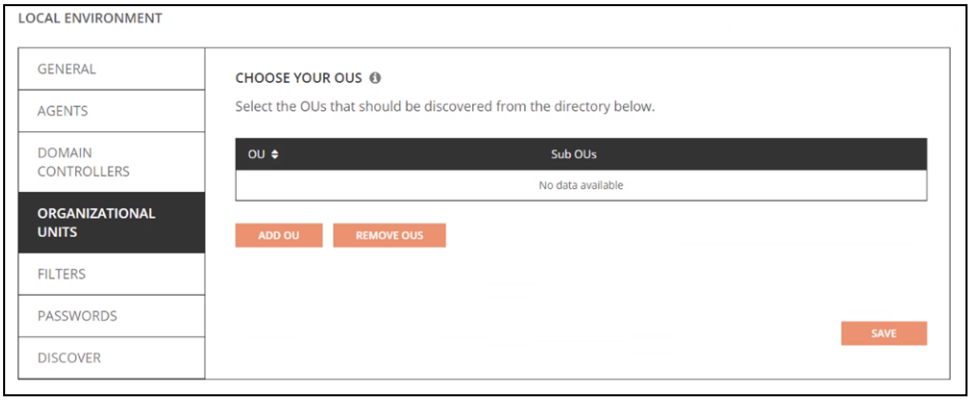
How do I set up environments?

To begin set up of Active Directory you must first configure an environment. Environments are managed in Directory Sync.

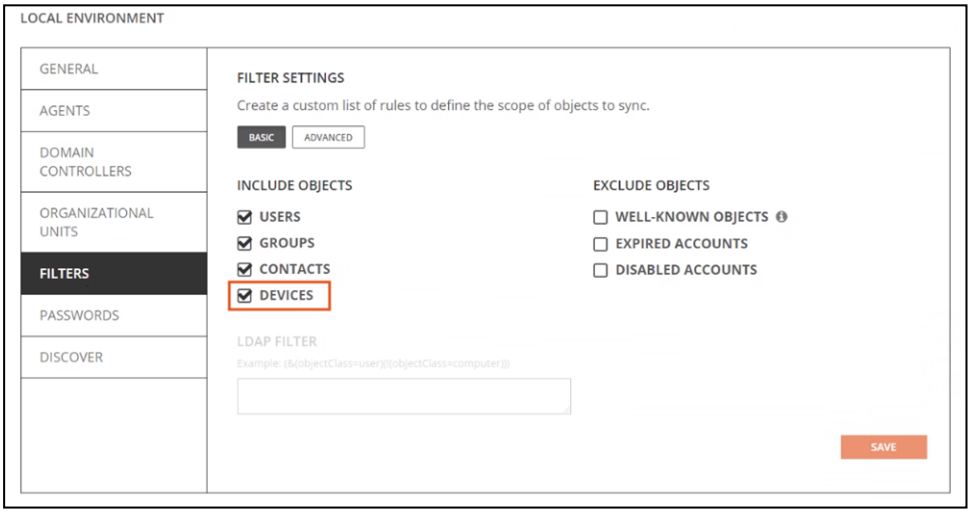
Please visit the Environments topic for more information.

Important Tip: There are two key settings which pertain to Device objects that you must enable when configuring Source and Target Environments for Device migrations.

1. *Define Scope:* Under the Environment Settings, Organizational Units section, be sure you have included the OUs which contain the Device (computer) Objects you want discovered for migration.



2. *Include Devices:* Under the Environment Settings, in the Filters section be sure to check the checkbox next to Devices under the Include Objects header.



Workflows

A workflow is a series of steps that ultimately lead to the migration of objects. Workflows are manged in Directory Sync. Please see the Workflows topic for more information.

For Directory Sync Workflows which will be used for Device migrations in Active Directory most of the settings will be similar to the settings for other kinds of migrations. There are two key settings which pertain to Device objects that you must enable when configuring for Device migrations: Workflow steps and Template Object settings.

For a Device migration to be successful the users and groups which have permissions to files on that machine must be in the Directory Sync database and have matching objects defined in the target. Otherwise, the Device ReACL process will not be able to correctly update the file access permissions on the device in preparation for moving to the new domain. It is not necessary to include User or Group objects in the same Workflow as Devices. Users and Groups will require Read In, Match, Stage Data, and Write Out Workflow steps. Device objects themselves at minimum require only the Reading and Matching steps.

A key part of Workflow settings which will apply to Device migrations are the Objects settings for the Template you use. In the Devices section of those Template Objects settings you can configure options to control how creation and updates of objects are handled.

Profiles

Migration Profiles

What is a Migration Profile?

A Migration Profile is a collection of common settings used to manage the domain join process during Device Cutover which can be defined once and then applied to multiple Devices. Migration Profiles are used for AD and Hybrid Microsoft Entra ID device migrations.

How are Migration Profiles created?

To create a Migration Profile:

1. On the *Migration* section of the *Profiles* page, click the **Add** button. The *Add Your Migration Profile* window appears.
2. Enter values for the following fields, then click **Next**:
    - *Profile Name* - A name to identify this profile (for example, "10 Second Reboot Delay").
    - *Domain Join Delay* - The delay time a Device agent processing a Cutover job applies before attempting to change the computer's domain to join the new domain.
    - *Reboot Delay* - The time for a Device agent processing a Cutover job to delay after joining the new domain before rebooting the computer.

      Note: If set to any value other than zero (0), the user will receive a pop-up notification informing them that the workstation will be rebooted when the Cutover is performed. If set to zero, no notification will appear.
3. Select desired Microsoft Entra ID Device Options, then click **Next**:
    - *Perform Microsoft Entra Hybrid Leave* – This will unjoin the Device from the source Microsoft Entra ID if it is currently hybrid Microsoft Entra ID joined.
4. Enter values for the following fields, then click **Next**:
    - *Empty Recycle Bin?* - How to handle the Recycle Bin during Cutover, either **Empty** or **Don't Empty**.

    Note: End users may get an error message that their Recycle Bin has been corrupted after migration if the Recycle Bin is not empty. See Troubleshooting for more information about this issue.

- *Specify Target OU* - The target OU where the Device will be created. If this field is left blank, they will default to the Computers container.
- *Join to Existing Computer Account* - Select **Yes** if you expect to join the Device to the existing target Computer during Cutover. Select **No** if you want the Device to be created in the target by the Cutover job.

5. Click **Save Profile**. The new migration profile is added to the list.

Network Profiles

What is a Network Profile?

A Network Profile is a collection of common network adapter settings that need to be updated during a Device's migration to the new domain which can be defined once and then applied to multiple Devices.

How are Network Profiles created?

To create a network Profile:

1. On the Network section of the *Profiles* page, click the **Add** button. The *Add Your Network Profile* window appears.
2. Enter values in the following fields, then click **Next**:
   - *Profile Name* - The name to identify this Network Profile
   - *Set DNS Servers For the Computer?* - Options include: **Don't Change This Setting**, **Use DHCP For DNS Server**, or **Manually Assign DNS Servers**.
   - *DNS Suffix For the Network Adapter* - The primary DNS suffix that will be set on the network adapter that is connected to the target domain.
3. Enter values in the following fields:
   - *Append DNS Suffixes to the Network Adapter* - Options include **Don't Change This Setting**, **Preserve Current DNS Suffixes From the Network Adapter**, or **Set the Following DNS Suffixes**.
   - *DNS Suffixes* (Enabled if **Set the Following DNS Suffixes** is selected above) - Enter each suffix and then press **Enter**.
   - .*Register the Network Adapter's Addresses in DNS* - Options include **Don't Change This Setting**, **No**, or **Yes**.
   - *Register the Network Adapter's Addresses in DNS* (Enabled if Yes is selected above) – select from **Don't Change This Setting**, **Include the Manual DNS Suffix**, or **Don't Include the Manual Suffix**.
   - Enter the WINS Servers: Primary WINS Server - The preferred WINS server and Secondary Wins Server - The alternate WINS server.
4. Click **Save Profile**. The new Network Profile is added to the list.

Device ReACL Profiles

What is a Device ReACL Profile?

A Device ReACL Profile is a collection of ReACL related settings which can be defined once and then applied to multiple Devices.

What is the default Device ReACL Profile used for?

The default Device ReACL Profile is used if a different profile is not defined and set on a Device. The default Device ReACL Profile can be edited.

How are Device ReACL Profiles created?

To create a Device ReACL profile:

1. On the *Device ReACL* section of the *Profiles* page, click the **Add** button. The *Add Your Device ReACL Profile* window appears.
2. In the **Profile Name** field, enter a name to identify this Device ReACL Profile.
3. Select a Logging Level, either **Informational** (default) or **Debugging**.

4. Select the desired components to process.

    - **Local Files/Folders:** Selected by default.
    - **Registry Permissions:** Selected by default.
    - **User Profiles:** Selected by default.
    - **Local Group Memberships:** Selected by default.
    - **Local Printer Permissions:** Selected by default.
    - **Network Share Permissions:** Selected by default.
    - **Printer Share Permissions:** Selected by default.
    - **Roaming Profiles:** Unselected by default.

      Note: If you select **Roaming Profiles**, users must be logged out of their roaming profiles during the ReACL process.
    - **Windows Services:** Selected by default. The **Windows Services** option will ensure that any source domain accounts that were given permission to a service will include the corresponding matched target domain account after a ReACL process.
    - **Windows Service Accounts:** Unselected by default. We recommend that the **Windows Service Accounts** box is left UNCHECKED. A change in the ACL of the service accounts of the target may have an impact on the applications currently running. Although the ReACL process can usually be rolled back in case of issues, there could be a temporary disruption in service until that can be resolved. Selecting the **Windows Service Accounts** box will switch the domain account that Windows services are running under to the corresponding matched target domain account after a completed ReACL process.
    - **User Rights Assignments:** Unselected by default.
    - **System ACLs:** Selected by default. The **System ACLs** option allows for the proper translation of accounts within the security audit logs.
    - **Preserve the "Archive" Bit:** Unselected by default. If the **Preserve the "Archive" Bit** box is left unchecked, the archive bit will be reset. If checked, the archive bit will not be reset.

5. Click **Next**.

6. Normally all files and folders are included in the ReACL process. If it is preferred to provide a specific list, enter the list in the **Only Process the Following and Their Subfolders** box. Separate each entry by pressing **Enter**. You may use just a file path starting with backslashes, or provide an exact drive letter. If a drive letter is provided, the ReACL is limited to that exact path.

   Note that if you choose to list folders here, these are the ONLY folders that will be included in the ReACL process. (The exception is if you selected the User Profiles component on the previous screen: those profiles would then always be included automatically in addition to your list specified here.)

7. In the **Exclude These Paths From Processing** box, enter folder paths that will not be included in the ReACL process. Wild card characters ('*' matches zero or more characters and '?' matches any single character) can be used when specifying excluded folders. Separate the paths by pressing **Enter**. By default, the following folders are excluded:

    - \Windows
    - \WINNT
    - \I386
    - \Windows\I386
    - \Program Files
    - \PROGRAM FILES (x86)
    - \MSOCACHE
    - \System Volume Information
    - \Recycler
    - \$RECYCLE.BIN
    - \CONFIG.MSI
    - \RECOVERY
    - \OEM
    - \Quarantine
    - \BOOT
    - \ProgramData\Microsoft\Windows Defender

8. In the **Exclude These Files From Processing** box, enter files that will not be included in the ReACL process. A leading '\' is not necessary. Wild card characters ('*' matches zero or more characters and '?' matches any single character) can be used when specifying excluded files. Separate the files by pressing **Enter**. The following wild card characters are permitted when specifying files:

    - * matches zero or more characters in a file name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent directories.

    Examples:

    - FileToSkip.dat – a single file in the root directory
    - \FolderToProcess\ExcludedFIle.sys – a single file in the FolderToProcess directory
    - \FolderToProcess***.dat – all .dat files anywhere under the FolderToProcess directory

9. In the **Exclude These Registry Keys From Processing** box, enter registry keys that will not be included in the ReACL process. A leading '\' is not necessary. Separate the keys by pressing **Enter**. The following wild card characters are permitted when specifying registry keys:

    - * matches zero or more characters in a key name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent keys.

    Examples:

    - HKEY_LOCAL_MACHINE\SOFTWARE\XYZ – a single key
    - HKEY_LOCAL_MACHINE\SOFTWARE\XY* – all keys starting with "XY" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE\SOFTWARE\?YZ – all 3-character keys ending with "YZ" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE**\XYZ – all keys named "XYZ" anywhere under HKEY_LOCAL_MACHINE
    - **\XYZ – all keys named "XYZ" in any registry hive

10. In the **Exclude These Security Identifiers From Processing** box, enter SIDS that will not be included in the ReACL process. Separate the SIDs by pressing **Enter**.

11. Click **Next**.

12. The **Reparse Point Processing Rules** page appears. Reparse Points like Symbolic Links, Mount Points, and OneDrive folders will be processed by ReACL. Additional Reparse Tags can be added to the rules list in the Advanced view to change how ReACL will process those items. Click the **Show Advanced** button to edit the rules list.

    When Show Advanced is clicked the rules list is displayed. Additional Reparse Points can added to the list in the "ReparseTag:Action" format. Skip, Recurse, Update, and Full are the available actions. Separate rules by pressing **Enter**.

m. Click **Next**.

n. Select an option from the **Elevated Permissions Failure Action** drop-down list to choose the action that should be taken if the ReACL process encounters permissions elevation errors.

In order to successfully adjust permissions, Active Directory must create a process with a security token that has been assigned additional permissions. The token is said to have elevated rights/permissions. If this process fails, it is likely that the ReACL will be largely unsuccessful in updating the operating system for use by target user accounts.

- The default is **Terminate processing with fatal error**, this means the ReACL job for a Device is stopped if a permissions elevation error occurs. This is a time-saving option. The ReACL Status will be **Failed** in the *Devices + Servers* table. A Device cannot be Cutover if the ReACL Status is **Failed**. This is the recommended setting.
- If you choose **Log informational entry**, an info entry will be logged if a permissions elevation error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *Devices + Servers* table. This choice allows experienced migration architects to analyze the logs and choose to proceed with Cutover based on their analysis of the results. We suggest choosing “Log warning entry” rather than “Log informational entry” as that will make the entries easier to locate in the log.
- If you choose **Log warning entry**, a warning entry will be logged if a permissions elevation error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *Devices + Servers* table. This choice allows experienced migration architects to analyze the logs and choose to proceed with Cutover based on their analysis of the results.
- If you choose **Log error entry**, an error entry will be logged if a permissions elevation error occurs. The ReACL job will continue, but the ReACL Status will be **Failed** in the *Devices + Servers* table. This selection may take significantly more time than "Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.

15. Select an option from the **Profile Failure Action** drop-down list to choose the action that should be taken when an invalid or duplicate profile exists in the target.

    - The default is **Terminate processing with fatal error**, this means the ReACL process for a Device is stopped if an invalid or duplicate profile error occurs. This is a time-saving option. The ReACL Status will be **Failed** in the *Devices + Servers* table. A Device cannot be Cutover if the ReACL Status is Failed. This is the recommended setting.
    - If you choose **Log informational entry**, an info entry will be logged if an invalid or duplicate profile error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *Devices + Servers* table. This choice allows experienced migration architects to analyze the logs and choose to proceed with Cutover based on their analysis of the results. We suggest choosing “Log warning entry” rather than “Log informational entry” as that will make the entries easier to locate in the log.
    - If you choose **Log warning entry**, a warning entry will be logged if an invalid or duplicate profile error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *Devices + Servers* table. This choice allows experienced migration architects to analyze the logs and choose to Cutover based on their analysis of the results.
    - If you choose **Log error entry**, an error entry will be logged if an invalid or duplicate profile error occurs. The ReACL job will continue and then complete as **Failed** and the ReACL Status on the *Devices + Servers* table will be **Failed**. This selection may take significantly more time than "Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.

p. Select an option from the **Preserve Rollback Metadata in ACLs** drop-down list.

Active Directory can leave behind metadata during the ReACL process to allow seamless rollback of the process if needed. This setting controls the creation of this metadata which is later removed during the Cleanup process.

- The default is **Always - Keep source security principles** and does not affect performance. We recommend this setting. This is the only setting where the changes performed by the ReACL process can be rolled back, or undone, in all scenarios.
- If you choose **Only If Ambiguous - Keep source security principles when necessary**, metadata will only be included when the rollback settings would be ambiguous. “Only If Ambiguous” results in the inclusion of less metadata, preserving usage for times when it may be impossible to determine the original file or folder permissions. For example, when users have accounts in multiple domains that will be consolidated into a single domain.

  Note that **Only If Ambiguous** guarantees that a ReACL can be rolled back to the original state only when the file system permissions remained unchanged. Modification of ACLs on the file system could create a state where a rollback cannot complete with 100% success. To ensure the ability to perform a ReACL Rollback in all scenarios, **Always** should be selected.
- If you are an experienced migration architect, you may choose **Never - Replace source security principles** to never include metadata.

  Note: If **Never** is selected, a complete ReACL Rollback may not be possible.

q. Select **Yes** under **Run Processing in Simulation Mode** to simulate the results of the ReACL process without actually making any changes to the ACLs. Visit the logs/reports to determine if there are any potential issues and correct them before changing this setting to **No** and running an actual ReACL process. Alternatively, you might use this setting to create a separate Device ReACL Profile specifically for testing purposes.

r. Click **Save Profile**. The new Device ReACL Profile is added to the list.

File Share ReACL Profiles

What is a File Share ReACL Profile?

A File Share ReACL Profile is a collection of ReACL related settings for File Shares which can be defined once and then applied to multiple File Shares.

What is the purpose of the default File Share ReACL Profile?

The default File Share ReACL Profile is used if a different profile is not defined and set on the File Share. The default File Share ReACL Profile can be edited.

How are File Share ReACL Profiles created?

To add a File Share ReACL profile:

1. On the *File Share ReACL* section of the *Profiles* page, click the **Add** button. The *Add Your File Share ReACL Profile* window appears.
2. In the **Profile Name** field, enter a name to identify this File Share ReACL Profile.
3. Select a Logging Level, either **Informational** (default) or **Debugging**.
4. Enter the network errors that will trigger a retry in the **Retry If the Following Error Codes Are Encountered** box. By default, errors 53 and 64 will trigger a retry.
5. Enter the number of retries to attempt on a network error in the **Retry Count** field. The default retry count is 10 times.
6. Enter the number of seconds to wait between retries on a network error in the **Retry Interval** field. The default interval is 1 second.
7. Click **Next**.
8. Select the components to process.

   By default the **System ACLs** and **Roaming Profiles** will be processed. If the **Preserve the "Archive" Bit** box is left unchecked, the archive bit will be reset. If checked, the archive bit will not be reset.

9. In the **Exclude These Paths From Processing** box, enter folder paths that will not be included in the ReACL process. Wild card characters ('*' matches zero or more characters and '?' matches any single character) can be used when specifying excluded folders. Separate the paths by pressing **Enter**. By default, the following folders are excluded:

    - \Windows
    - \WINNT
    - \I386
    - \Windows\I386
    - \Program Files
    - \PROGRAM FILES (x86)
    - \MSOCACHE
    - \System Volume Information
    - \Recycler
    - \$RECYCLE.BIN
    - \CONFIG.MSI
    - \RECOVERY
    - \OEM
    - \Quarantine
    - \BOOT
    - \ProgramData\Microsoft\Windows Defender

10. In the **Exclude These Files From Processing** box, enter files that will not be included in the ReACL process. A leading '\' is not necessary. Wild card characters ('*' matches zero or more characters and '?' matches any single character) can be used when specifying excluded files. Separate the files by pressing **Enter**. The following wild card characters are permitted when specifying files:

    - * matches zero or more characters in a file name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent directories.

    Examples:

    - FileToSkip.dat – a single file in the root directory
    - \FolderToProcess\ExcludedFIle.sys – a single file in the FolderToProcess directory
    - \FolderToProcess***.dat – all .dat files anywhere under the FolderToProcess directory

11. In the **Exclude These Registry Keys From Processing** box, enter registry keys that will not be included in the ReACL process. A leading '\' is not necessary. Separate the keys by pressing **Enter**. The following wild card characters are permitted when specifying registry keys:

    - * matches zero or more characters in a key name, but not the '\' path delimiter.
    - ? matches any single character.
    - ** matches zero or more parent keys.

    Examples:

    - HKEY_LOCAL_MACHINE\SOFTWARE\XYZ – a single key
    - HKEY_LOCAL_MACHINE\SOFTWARE\XY* – all keys starting with "XY" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE\SOFTWARE\?YZ – all 3-character keys ending with "YZ" in HKEY_LOCAL_MACHINE\SOFTWARE
    - HKEY_LOCAL_MACHINE**\XYZ – all keys named "XYZ" anywhere under HKEY_LOCAL_MACHINE
    - **\XYZ – all keys named "XYZ" in any registry hive

12. In the **Exclude These Security Identifiers From Processing** box, enter SIDs that will not be included in the ReACL process. Separate the SIDs by pressing **Enter**.
13. Click **Next**.
14. The **Reparse Point Processing Rules** page appears. Reparse Points like Symbolic Links, Mount Points, and OneDrive folders will be processed by ReACL. Additional Reparse Tags can be added to the rules list in the Advanced view to change how ReACL will process those items. Click the **Show Advanced** button to edit the rules list.

    When Show Advanced is clicked the rules list is displayed. Additional Reparse Points can added to the list in the "ReparseTag:Action" format. Skip, Recurse, Update, and Full are the available actions. Separate rules by pressing **Enter**.
15. Click **Next**.

16. Select an option from the **Elevated Permissions Failure Action** drop-down list to choose the action that should be taken if the ReACL process encounters permissions elevation errors.

    In order to successfully adjust permissions, Active Directory must create a process with a security token that has been assigned additional permissions. The token is said to have elevated rights/permissions. If this process fails, it is likely that the ReACL will be largely unsuccessful in updating the operating system for use by target user accounts.

    - The default is **Terminate processing with fatal error**, this means the ReACL job for a File Share is stopped if a permissions elevation error occurs. This is a time-saving option. The ReACL Status will be **Failed** in the *File Shares + Network Storage* table. This is the recommended setting.
    - If you choose **Log informational entry**, an info entry will be logged if a permissions elevation error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *File Shares + Network Storage* table. This choice allows experienced migration architects to analyze the logs and choose to proceed with Cutover based on their analysis of the results. We suggest choosing “Log warning entry” rather than “Log informational entry” as that will make the entries easier to locate in the log.
    - If you choose **Log warning entry**, a warning entry will be logged if a permissions elevation error occurs. If no other errors are encountered the ReACL job will complete as successful and the ReACL Status will be **Completed** in the *File Shares + Network Storage* table. This choice allows experienced migration architects to analyze the logs and choose to proceed with Cutover based on their analysis of the results.
    - If you choose **Log error entry**, an error entry will be logged if a permissions elevation error occurs. The ReACL job will continue, but the ReACL Status will be **Failed** in the *File Shares + Network Storage* table. This selection may take significantly more time than "Terminate processing with fatal error" because the entire process will attempt to finish before reporting as **Failed**.

17. Select an option from the **Preserve Rollback Metadata in ACLs** drop-down list.

    Active Directory can leave behind metadata during the ReACL process to allow seamless rollback of the process if needed. This setting controls the creation of this metadata which is later removed during the Cleanup process.

    - The default is **Always - Keep source security principles** which does not affect performance. We recommend this setting. This is the only setting where the changes performed by the ReACL process can be rolled back, or undone, in all scenarios.
    - If you choose **Only If Ambiguous - Keep source security principles when necessary**, metadata will only be included when the rollback settings would be ambiguous. **Only If Ambiguous** results in the inclusion of less metadata, preserving usage for times when it may be impossible to determine the original file or folder permissions. For example, when users have accounts in multiple domains that will be consolidated into a single domain.

      Note that **Only If Ambiguous** guarantees a ReACL can be rolled back to the original state only when the file system permissions remained unchanged. Modification of ACLs on the file system could create a state where a rollback cannot complete with 100% success. To ensure the ability to perform a ReACL Rollback in all scenarios, Always should be selected.
    - If you are an experienced migration architect, you may choose **Never - Replace source security principles** to never include metadata.

      Note: If **Never** is selected, a complete rollback may not be possible.

18. Select **Yes** under **Run Processing in Simulation Mode)** to simulate the results of the ReACL process without actually making any changes to the ACLs. Visit the logs/reports to determine if there are any potential issues and correct them before changing this setting to No and running an actual ReACL process. Alternatively, you might use this setting to create a separate File Share ReACL Profile specifically for testing purposes.
19. Click **Save Profile**. The new File Share ReACL Profile is added to the list.

Microsoft Entra ID Join Profiles

What is an Microsoft Entra ID Join Profile?

A Microsoft Entra ID Join Profile is a collection of settings used to manage the Azure join process during Device Cutover which can be defined once and then applied to multiple Devices. Microsoft Entra ID Join Profiles are used for AD to Azure device migrations.

How are Microsoft Entra ID Join Profiles created?

To add an Microsoft Entra ID Join Profile:

1. On the *Microsoft Entra ID Join* section of the *Profiles* page, Click the **Add** button. The *Add Your Microsoft Entra ID Join Profile* window appears.
2. Enter a **Profile Name** to identify this Microsoft Entra ID Join Profile.
3. Enter a value in the following field:

    - **Bulk Enrollment Package File Name** - The name of the Azure bulk enrollment package in packagename.ppkg format, which has been created by the client administrator using the Windows Configuration Designer and copied to the network share defined in the Azure Bulk Enrollment Repository

4. Select an option from the following drop-down list:

    - **Target Environment** – The cloud-only Azure environment associated with the Azure bulk enrollment package used in this Profile

5. Select a **Device Name Option**:

    - If you choose **Device Name Defined Per Provisioning Package**, the device will be migrated to Azure using the dynamic naming convention configured in the Azure bulk enrollment package used in this Profile
    - If you choose **Keep Original Device Name**, the dynamic name assigned by the Azure bulk enrollment package will be overwritten and replaced with the original device name when migrating to Azure

6. Select the **Enroll Into Intune Management** option to enroll the device for Intune management with the first logged on user after cutover as the PrimaryUser.
7. Select the **Intune Cleanup** option to clear existing Intune provisioning information from the device as part of the cutover.
8. Select the **Auto-Pilot Cleanup** option to clear existing Auto-Pilot provisioning information from the device as part of the cutover.
9. Select the **Active Directory Joined or Hybrid Microsoft Entra ID Joined** option if you wish to include Active Directory Joined or Hybrid Microsoft Entra ID Joined devices.
10. Enter values in the following fields under Source Domain Credentials:

    - **FQDN of Domain** - The domain FQDN of the source in source.domain.com format.
    - **Username** - The username to access the source domain in domain\username or UPN (username@domain.com) format.
    - **Password** - The password credential to access the source domain.

11. Under *Preflight Check Validation*, select the **Skip Source Local Active Directory Validation** option to not validate the source local Active Directory.
12. To add a new user to the local admin group, select the **Create Local Admin** option and enter a Username and Password for the new user.
13. Click **Save Profile**. The Microsoft Entra ID Join Profile is added to the list.

Credential Profiles

What is a Credential Profile?

A Credential Profile is a set of source and target domain credentials used for Cutover which can be defined once and then applied to multiple Devices.

How are Credential Profiles created?

The specified credentials must be able to join and disjoin a computer from the specified domain as well as disable a computer in the specified domain. A trust between the source and target domain is not required.

To add a Credential Profile:

1. On the Credentials section of the *Profiles* page, Click the **Add** button. The *Add Your Credentials Profile* window appears.
2. Enter a **Credential Name** to identify this Credentials Profile.
3. Enter values in the following fields under Source Domain Credentials:
    - **FQDN of Domain** - The domain FQDN of the source in source.domain.dom format.
    - **Username** - The username to access the source domain in domain\username or UPN (username@domain.dom) format.
    - **Password** - The password credential to access the source domain.
4. Enter values in the following fields under Target Domain Credentials
    - **FQDN of Domain** - The domain FQDN of the target in target.domain.dom format.
    - **Username** - The username to access the target domain in domain\username or UPN (username@domain.dom) format.
    - **Password** - The password credential to access the target domain.
5. Click **Save Profile**. The Credential Profile is added to the list.

Credential Cache Profiles

What is a Credential Cache Profile?

A Credential Cache Profile is a collection of settings related to the target domain controller used for caching a user's target credentials prior to completing an Offline Domain Join cutover which can be defined once and then applied to multiple Devices.

How are Credential Cache Profiles created?

To add a Credential Cache Profile:

1. On the *Credential Cache* section of the *Profiles* page, Click the **Add** button. The *Add Your Credential Cache Profile* window appears.
2. Enter a **Credential Cache Name** to identify this Credential Cache Profile.
3. Enter values in the following fields:
    - **Target Domain Controller IP Address** – The IP address of the target Domain Controller.
    - **Target Domain Controller Ping Interval** - The number of seconds the script will sleep between pings to the defined target domain controller. The default value is 300 seconds.
    - **Timeout Before Job Failure** – The number of minutes to wait after Credential Cache job is downloaded by the agent before marking the job a failure due to timeout. The default value is 180 minutes.
    - **Timeout for User Credential Prompt** – The number of minutes to prompt the user with a dialog box to enter their target domain credentials for caching. The default value is 5 minutes
4. Click **Save Profile**. The Credential Cache Profile is added to the list.

Configurations

Actions

What are Actions and Tasks?

Actions are a sequence of Tasks to complete a process.

The Actions screen will allow you to create a new Custom Actions that can be performed against Accounts, Computers or File Shares. Existing or new tasks can be added to a the desired Custom Action and then ordered as necessary to complete the custom process.

It is important to note that System actions and tasks can only be viewed or copied, they are not editable.

How is an Action created or copied?

To add or copy an action: Below the table, click **New** or select an existing Custom Action and click **Copy**. Check **Show System** to view and select any existing Systemactions.

- **Action Name** (Required): Enter a name for the Custom Action. The Action Name must be unique.
- **Action Display Name:** Enter the name that appears in the Actions menu.
- **Description:** Enter a description for the action.

- **Action Target:** Select one of the options from the drop-down list.
    - *Computer:* The Action will appear in the Actions menu on the Computers screen.
    - *File Share:* The Action will appear in the Actions menu on the File share screen.
- **Action Type:** Select one of the options from the drop-down list. The Action Type determines what validations are applicable to the job, and which status columns are updated when the job runs. For example, a Custom Action with the ReACL type, will have the same validations as the System ReACL action.
    - *Other* (default): An action not related to any System action. No predefined validations are applicable. By default, new Actions are assigned as type Other.
    - *Discovery:* Gathers properties from the computer.
    - *Cutover:* Moves a computer from the source domain to the new target domain.
    - *ReACL:* Updates computer domain user profiles for use by the matching target user after cutover.
    - *ReACL Share:* Updates the File Share's domain user profiles for use by the matching target user after cutover.
    - *ReACL Rollback:* Rolls back all changes made by the ReACLShare process.
    - *ReACL Rollback Share*: Rolls back all changes made by the ReACL process.
    - *Cleanup:* Removes the Source SIDs after the Cutover process completes.
    - *Cleanup Share:* Removes the Source SIDs after the Cutover process completes.
    - *Explicit Rollback:* Rejoins a computer back to the source domain.
    - *Upload Logs:* Uploads log files from the Active Directory Pro Agent to the Active Directory Pro Server using Microsoft BITS.

How is a Task created or copied?

To add or copy a task: Below the Tasks table, click **New** or select an existing task and click **Copy**. Check **Show System** to view and select an existing Systemtask.

- **Task Name** (Required): Enter a name for the task. The Task Name cannot begin with "BT-" which is used to identify system tasks.
- **Description:** Enter a description for the menu action.

- **Task Type** (Required): Select one of the options from the drop-down list.
    - *PowerShell Script:* Allows you to define a PowerShell script for the process on the Command and Rollback screens. Global Variables can be added and used in the script.
    - *Command Line:* Allows you to define a Command Line command for the process on the Command and Rollback screen. Global Variables can be added and used in the command line.
    - *Download File:* Downloads a file to the predefined Downloads folder.
- **Automatic Rollback:**
    - *Auto-Rollback On Error:* if checked, automatic rollback on error is added to the task.
- **Include Variables For:**
    - *Manage Credentials:* if checked, the PowerShell script or Command Line command includes the $CutoverCredentials_ XXXXX parameters.
    - *Network Profile Settings*: if checked, the PowerShell script or Command Line command includes the $NetworkProfile_ XXXXX parameters.
    - *Migration Profile Settings:* if checked, the PowerShell script or Command Line command includes the $MigrationOption_ XXXXX parameters.
    - *Global Variables:* if checked, the PowerShell script or Command Line command includes the Global Variables.
- **Script:** Enter a PowerShell script or Command Line command. If creating a PowerShell script, click **Load Script Framework** to populate the entry box with the basic framework of a script. Enter or edit the Command Line command or PowerShell script. Text is required. The return value of the script or command will determine success or failure.
- **Rollback:** Enter a PowerShell script or Command Line command to run in case of failure/Rollback. Ideally this would undo the effects of the above script. If creating a PowerShell script, click **Load Script Framework** to populate the entry box with the basic framework of a script. Enter or edit the Command Line command or PowerShell script. Text is required. The return value of the script of command will determine success or failure.
- **Task Timeout:** For PowerShell script or Command Line command, enter the number of seconds the process will be attempted before timing out.
- **Retry Count:** For the PowerShell script or Command Line command, enter the number of times the process will be retried.
- **Update Interval:** For PowerShell script or Command Line command, enter the number of seconds between process runs.

- **File Download:** Enter the following options if adding or copying a Download File task. When a new download job is created for a managed workstation, the specified file that is stored in the configured Custom Downloads Repository will be downloaded to c:\Program Files (x86)\Binary Tree\P365ActiveDirectoryAgent\Downloads\ on the workstation's local disk.
    - *File Name* (required): The file name. Based on the File Location for Download Jobs used during installation The File Name cannot contain invalid filepath characters and cannot use the following reserved file names: map.usr, map.gg, and ReACL-config.json.
    - *File Path:* The target Location of the download job. The Target Location cannot contain invalid filepath characters and cannot use the following reserved file names: map.usr, map.gg, ReACL-config.json. A Target Location is required if the File Name contains environment variables.

The local download folder on an Active Directory managed machine will be secured with permissions only for the BUILTIN\Administrators group.

Note: If rights other than BUILTIN\Administrators are required then the administrator will need to make a change on the local downloads folder (c:\Program Files (x86)\Binary Tree\P365ActiveDirectoryAgent\Downloads\) on the Agent machine.

How is a Task added to an Action?

To add a Task to an Action: Select a Task in the Tasks table, select an Action in the Select Action drop-down menu and click the **Add To** button.

Under a given Action the Tasks are listed in the order in which they will be executed. Drag and drop tasks to reorder them. Tasks can be viewed, copied, or removed by selecting the tasks and clicking the appropriate button.

How do you activate an Action?

Only Actions marked as Active will appear in the Actions menus. Select an Action in the table and click the **Disable** or **Enable** button to change the active status of the Action. Inactive actions can be displayed in the table by clicking the **Show Disabled** button. You may want to create a new action, enable it, and then disable the corresponding System action.

Additional Information

Custom Action Example

Downloads

How are Mapping Files downloaded?

Use the Downloads page to generate the User Mapping File (Map.usr) and Group Mapping File (Map.gg). These files are automatically created during the ReACL process so the only time they need to be created manually is when

re-permissioning SQL databases.

To create the mapping files:

1. Click the **Download** button.
2. Select the source and target environment and click **Submit**.
3. Use the browser options to open or save the mappings.zip file containing the User Mapping File (Map.usr) and Group Mapping File (Map.gg).

   Note: Each time the Create Mapping Files process is run, the Map.usr and Map.gg files are overwritten.

Note, Use the Downloads page to generate the mapping files for the Active Directory Processing Wizard and Quest Secure Copy, and the Exchange Processing Wizard. Additional detail for Active Directory and Exchange Processing Wizard Mapping Files can be found at Migration Manager for AD 8.15 - Resource Processing Guide (quest.com)

To enable GCC/GCCH Device Migration, please contact Quest Support for additional configuration described in the following article: Update GCC/GCCH tenant object's RID value for ReACL. This configuration is required for successfully switching the user profile during cutover.

How are device agents downloaded?

To download a device agent:

1. Select an available agent version from the drop-down menu.
2. Click the **Download** button.
3. Use the browser options to save the agent installer package.

What are the Device Agent Service URL and Auth key used for?

The Device Agent Service URL and Auth Key as defined on the Downloads section of the Configurations page are provided to the Device Agents at install and allow them to connect to the correct customer's Power365 project. They are unique to the agents in a given client and all agents of the same client should use the same values. If installing the agent from the command line without UI the arguments for providing the Service URL and Auth Key are their names in all uppercase i.e. SERVICEURL and AUTHKEY respectively.

How are device agents automatically upgraded?

To automatically upgrade the device agents:

1. Click the **Enable** button at the bottom of the Device Agent section.

Installing the Active Directory Agent

Each Active Directory Computer (device) that will be migrated must have an agent installed on the workstation to orchestrate local jobs that must occur to prepare and execute the workstation's domain move.

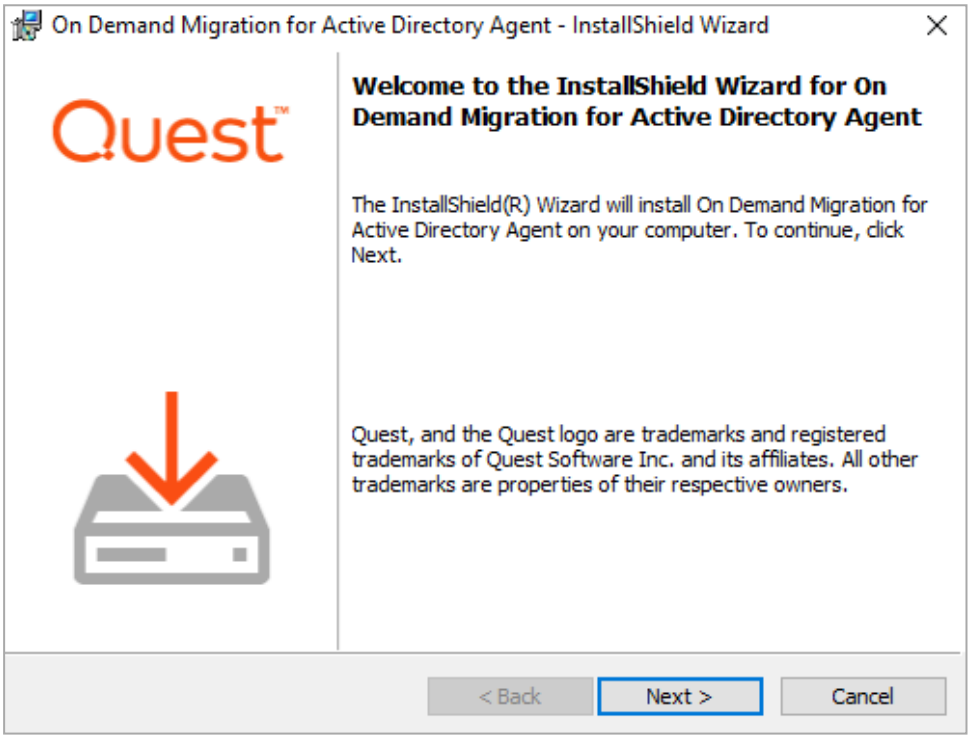
Refer to the Requirements for to verify all devices meet the requirements for agent installation.

The agent is available as an MSI package from the Downloads section of the Configurations page. You will also need the values of the Service URL and Auth Key found on that page.

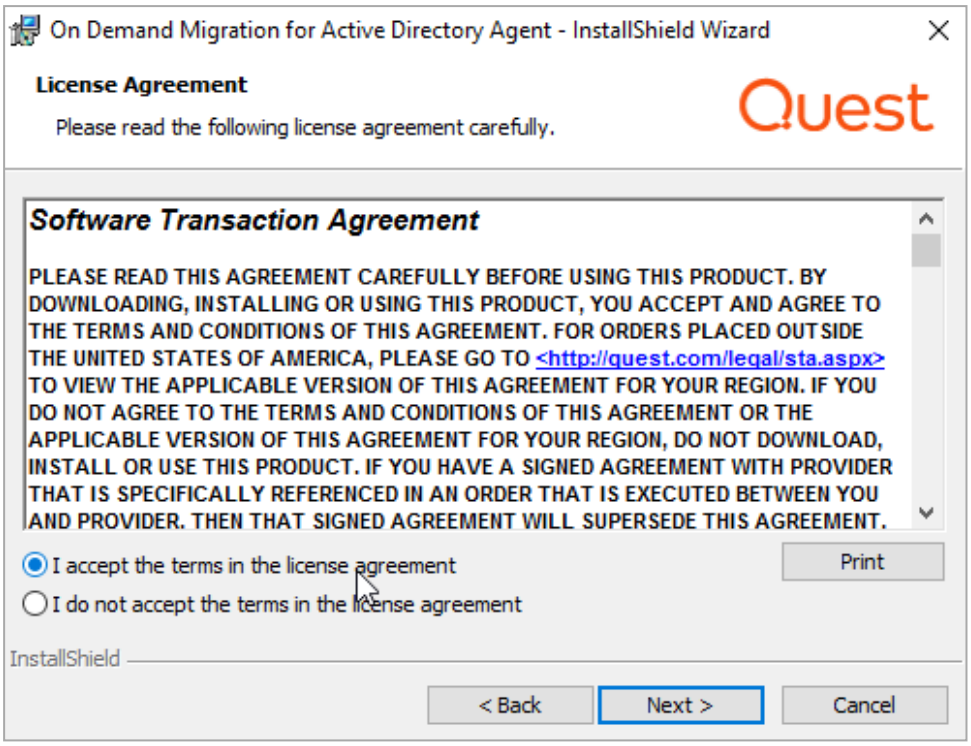
You can install the agent by running the MSI manually on the device, with a PowerShell command, or in bulk by using a GPO or other third-party delivery method.

How do you manually install the Active Directory Agent?

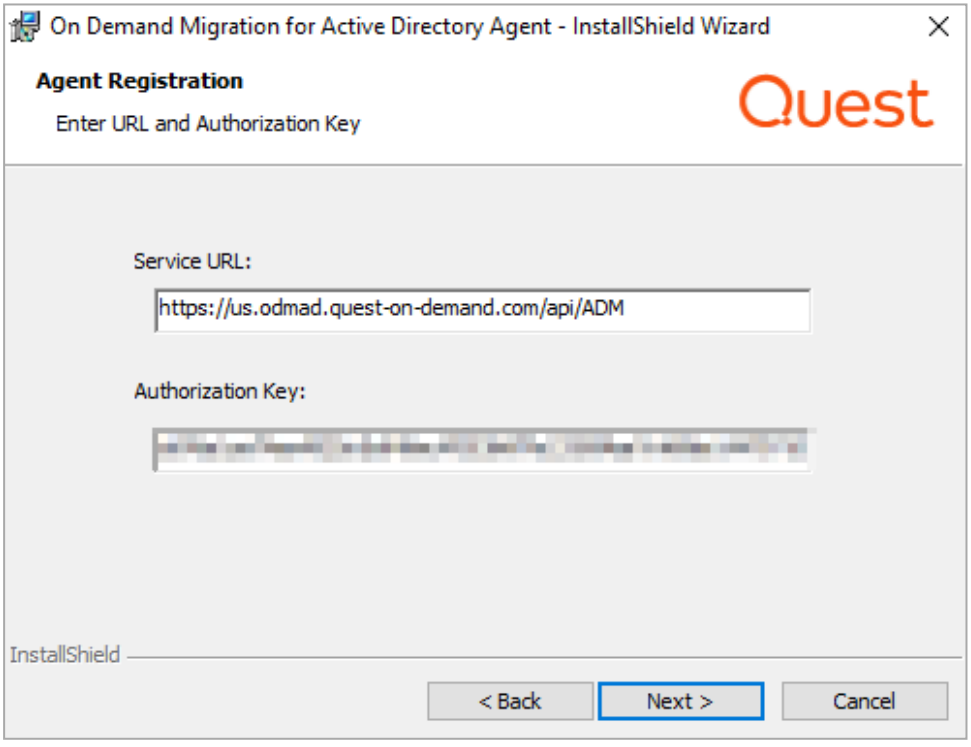
1. Download the Active Directory MSI file from the Downloads page.
2. Copy the Active Directory MSI file to each computer.
3. Double-click the file to open the installer.
4. On the Welcome screen, click **Next**.



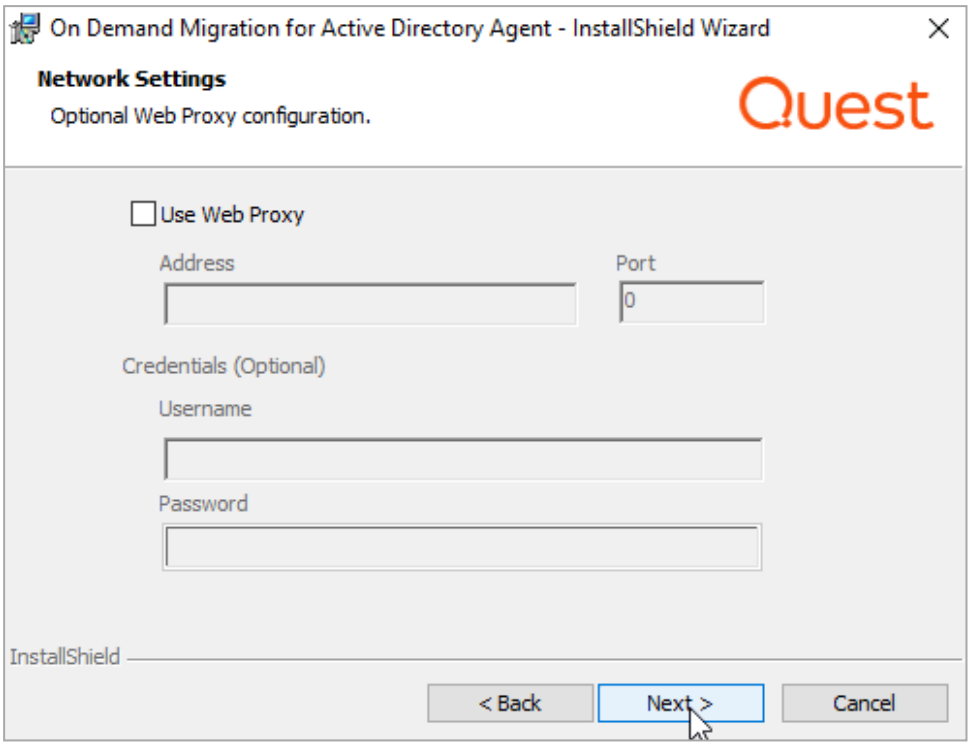
5. On the **License Agreement** screen, accept the agreement and click **Next**.



6. On the **Agent Registration** screen, enter the **Service URL** and **Authorization Key**, found on the Downloads page, and then click **Next**.



7. On the **Network Settings** screen, if using a Web Proxy, check **Use Web Proxy** and enter the Web Proxy settings. Click **Next**.



8. On the **Ready to Install the Program** screen, click **Install**.
9. When the install completes, click **Finish**.

Note: Once the agent is installed and the service is running it will connect to the server within four hours. This delay is randomized and uniformly distributed to avoid overloading the server when large numbers of agents come online at the same time.

How do you install the Active Directory Agent using a PowerShell Command?

1. Download the Active Directory MSI file from the Downloads page. The Service URL and Auth Key values also found on the Downloads page are required.
2. Create and run the PowerShell command with the required SERVICEURL (Service URL) and AUTHKEY (Auth Key) values.

   Example:

```
msiexec.exe /I 'C:\workspace\AD.Agent-20.3.1.1401.msi'
SERVICEURL=https://us.odmad.quest-on-demand.com/api/ADM
AUTHKEY
=#########################################################################
```

3. Walk through the install wizard, filling out the needed information and click Finish when completed. The settings for using a customer web proxy for communications are optional.

As needed the installer can also be invoked in quiet mode with the /QN switch (requires running PowerShell as admin).

Additionally, it is possible to configure the agent to use a Web Proxy using the below command line arguments:

- **WEBPROXYENABLE** – Is a Web Proxy used? Values: Yes=1, No=0
- **WEBPROXYURL** – The Web Proxy Address
- **WEBPROXYPORT** – The Web Proxy Port
- **WEBPROXYUSER** – The optional Web Proxy Credentials Username
- **WEBPROXYPASS** – The optional Web Proxy Credentials Password

How do you install the Active Directory Agent using a GPO (Group Policy Object)?

1. To install the agent using a GPO you must convert the MSI package and the parameters into an MST file. One method to do this is using Microsoft Orca. Install Orca (available in Windows SDK Components for Windows Installer Developers). Orca will be used to create the necessary MST file.
2. Download the Active Directory Agent MSI file from the Downloads page.
3. Right-click on the MSI file and select **Edit with Orca**.
4. Once you have Orca opened, click on the **Transform** menu and select **New Transform**.
5. Next, navigate to the **Property** table and add the following:
    - Add a Row with property of **SERVICEURL** and the Service URL value found on the Downloads page.
    - Add a Row with property of **AUTHKEY** and the Auth Key value found on the Downloads page.
    -
        - Optionally, the following properties and values can also be added to configure the agent to use a Web Proxy:
            - **WEBPROXYENABLE** – Is a Web Proxy used? Values: Yes=1, No=0
            - **WEBPROXYURL** – The Web Proxy Address
            - **WEBPROXYPORT** – The Web Proxy Port
            - **WEBPROXYUSER** – The optional Web Proxy Credentials Username
            - **WEBPROXYPASS** – The optional Web Proxy Credentials Password
6. Click the **Transform** menu and select **Generate Transform** to complete the MST file creation. This MST file will be used in a later step.

7. Right-click on the Active Directory Agent MSI, point to **Share with**, and click on **specific people**.
8. Add a security group. The "authenticated users" group already includes all computers and is a good group to use. The group you add must have the shared Read permission and NTFS permission.
9. Click **Share**.
10. Click **Done**.
11. From the **Start** menu, point to **Administrative Tools** and click on **Group Policy Management**.
12. Right-click on the domain or OU you will be migrating and click on **Create a GPO in this domain, and link it here**.
13. In the New GPO dialog box, enter a **Name** for the GPO and click **OK**.
14. Click on the new GPO and click **OK**.
15. Right-click on the GPO and select **Edit**.
16. Open **Computer Configuration** > **Policies** > **Software Settings** and right-click on **Software Installation** and then point to **New** and click on **Package**.
17. In the **File Name** field, enter the UNC path to the MSI file and click **Open**.
18. Select the Active Directory Agent MSI file and click **Open**.
19. In the **Deploy Software** window, select the **Advanced** deployment method and click **OK**.
20. Under the **Modifications** tab, add the MST file you created earlier and click **OK**.

Please Note: The computer must be rebooted for the applied group policy to complete the agent installation.

How do you verify the GPO?

1. Log on to a workstation within the scope of the GPO using administrator credentials.
2. From a command prompt on the workstation, run **gpresult -r**
3. The Computer Settings section will display the applied group policy.

Please Note:A newly applied group policy will not immediately be displayed. The Computer Settings section displays the applied group policy, but the agent installation is not completed until the computer is rebooted.

Please Note: If using the agent Auto-Upgrade feature and deployment software that uses MSI ProductCode based detection, the Auto-upgrade feature should be disabled after initial deployment or the detection method should verify via a folder path.

Repositories

What are the Repositories?

Repositories are storage locations (network shares) which you configure on your network used for four specific job types: Agent Logs, Custom Downloads, Offline Domain Join, and Microsoft Entra Device Join. These job types access or create files in the defined locations. If you are not using these job types you do not need to configure Repositories.

How do I manage Repositories?

Repositories are managed from the Repositories section of the Configurations page. There you can view and copy the currently defined share path for each job type. You can update and save the configuration. Make sure that the defined network share path is routable from the devices being migrated.

What can I do with a Repository?

Repositories are used to locate files for four job types:

- Agent Logs – Agent logs are maintained on individual workstations. To centralize them so that review does not require logging into each machine, the Upload Logs Action can be applied to the Devices of interest. This will create a copy of the Device's logs in the defined network share.
- Custom Downloads – Custom Actions with a Download File Task can be used to download a specified file from the defined network share to the workstation. A common use of this job type is distributing a new VPN client to workstations after Cutover.

  A Custom Download Repository should not be used with the Offline Domain Join Action type when configuring custom actions.
- Offline Domain Join – The Offline Domain Join Action and the associated Cache Credentials Action rely on access to ODJ files which have been generated by a client administrator prior to applying the Actions according to Microsoft instructions as described elsewhere in this guide.

  An Offline Domain Join Repository should be used with the Offline Domain Join Action type when configuring custom actions.
- Microsoft Entra Bulk Enrollment – The Microsoft Entra ID Cutover Action relies on access to an Azure bulk enrollment package which has been created by a client administrator using the Windows Configuration Designer as described in the Active Directory Entra-Join Quick Start Guide.

Variables

What are Variables?

Variables, also known as Global Variables, can be defined and be used across multiple scripts when defining Custom Actions. For example, a global variable to add the current date can be added to multiple scripts. Global

variables will appear when selecting a starter script when creating a Custom Action if the "Global Variables" option is selected.

How is a Variable created?

To add a Global Variable:

1. Open the left navigation menu.
2. Click **Configuration**.
3. Click **Variables**.
4. Click the **Add** button.
5. c. Enter values in the following fields:
    - **Variable Name** (Required): Enter a name for the global variable. The name must contain alphanumeric characters and underscores only.
    - **Variable Value** (Required): The value of the global variable. Check the **Encrypted** box to encrypt the value in the database and hide the variable value in the interface.
6. Click the **Save** button.

Migration Waves

What is a Migration Wave?

A Migration Wave in Active Directory is a named logical grouping of Devices. This can be a useful tool for organizing, tracking, and staging your migrations.

How do I manage Migration Waves?

There are two ways to manage Migration Waves in Active Directory. First, you can add Devices to a Wave by applying the ‘Set to Migration Wave’ Action to Devices from the Ready Devices table. The other way to manager Migration Waves is from the Migration Waves page which is accessible through ‘Waves’ in the left navigation menu. On that page you can create new Waves, Edit Wave names, Remove empty waves, and view how many Devices are in a Wave.

What can I do with a Migration Wave?

Migrations Waves in Active Directory can be used to filter the Ready Devices table to view Device status and apply Actions.

How do I create a New Migration Wave?

1. Login to Active Directory.
2. Select "Waves" in the left navigation menu.
3. A new page will open listing your current migration waves.
4. Click the Add icon.
5. Name the Migration Wave, remember use a logical name representing the migration event.
6. Click “Save.”
7. Now that the Migration Wave is created, Devices can be added to the Wave by applying the ‘Set to Migration Wave’ Action to Devices from the Ready Devices table.

How do I remove a Migration Wave?

1. Login to Active Directory.
2. Select "Waves" in the left navigation menu.
3. A new page will open listing your current migration waves.
4. Select one or more wave in the table.
5. Click the Remove icon.
6. Click "Yes" to confirm the removal.

How do I edit the name of a Migration Wave?

1. Login to Active Directory.
2. Select "Waves" in the left navigation menu.
3. A new page will open listing your current migration waves.
4. Select a wave in the table.
5. Click the Edit icon.
6. Edit the name of the Migration Wave.
7. Click “Save.”

How do I filter Devices by Migration Wave?

1. Login to Active Directory.
2. Select "Devices + Servers" in the left navigation menu.
3. On the Ready Devices tab, click the Filter icon.

4. Select one or more wave under the Waves filter category.

Migrate and Navigate

Devices + Servers

What is the Devices + Servers page used for?

The Servers + Devices screen allows the administrator to register devices and servers, set the ReACL profile, upload migration logs, and manage the device Discovery, ReACL, Cutover, and Cleanup processes.

Select the gear icon  above the "Ready Devices" list to select the columns to display for the current session.

What is the difference between a "Ready Device" and a "Not Ready Device?"

"Ready Devices" are devices that have the necessary agent installed, are communicating, and are ready for actions to be scheduled. "Not Ready Devices" are devices which that have not yet had an agent installed and communicating.

Note: Initial agent registration is uniformly distributed over a four hour interval from agent start time.

What actions can be performed on Devices and Servers?

The following actions can be performed on devices by selecting the devices in the list, selecting an action from the drop-down list, and then clicking the **Apply Action** button.

- **Discovery**

  The Discovery process gathers properties (OS versions, network properties, and so on) from the device to allow additional future functionality. The first discovery process begins for a device when the device becomes registered with Power365 which will automatically occur after the Device Agent has been installed, as long as the environment is properly configured.

  To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Discovery Status will be displayed as Queued in the Devices table and the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date.

- **Set Target Environment**

  The Set Target Environment action provides the ability to specify the target environment for the selected devices. The ReACL, Cache Credential, Offline Domain Join, Cutover, Cleanup, Rollback, and ReACL Rollback actions cannot be started for the selected devices if the target environment is not set.

  To set to the target environment, select a target environment for the selected devices from the list and click **Save**. The target environment can be cleared by selecting **None** from the list.

- **ReACL**

  The ReACL process updates the Device's domain user security ACL with the matching target user ObjectSID. User Profiles will only be processed during Device Cutover which will be triggered automatically when running the Cutover Actions.

  Note: During device cutover, ReACL also process the device's domain user profiles for use by the matching target user after cutover.

  Note: It is recommended to remove or disable anti-virus software immediately prior to the ReACL process and only after a recent clean scan has been completed.

  Before ReACL can occur, the target Users and Groups which have permissions set on the Device must be migrated to the target.

  To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the ReACL Status will be displayed as Queued in the Devices table and the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date.

  Note: Two checks are performed at the start of the ReACL process. The first check is for invalid Source Profiles, which will be logged as a WARNING and those profiles will be skipped. The second check is for invalid Target Profiles, where a user may have created a profile with the target account before their machine is ReACL'd and cutover. By default, this is logged as a FATAL ERROR and will halt the ReACL process. However, it can be changed to a WARNING with the –t switch passed by editing the command in SQL.

  The ReACL Agent will automatically create two files on the device being ReACL'd, map.usr and map.gg. These files are used to find the source permissions and add the appropriate target permissions during the ReACL process. System groups, such as Domain\Domain Admins and Domain\Domain Users are included in the map.gg file for updating the group permissions during the ReACL process. If the Active Directory environment is non-English, the values in the sAMAccountName column of the BT_SystemGroup table in the SQL database will need to be changed after Directory Sync is installed to have the appropriate non-English values.

  If the Mapped Network Drive is being mapped via GPO or using an integrated credential such as the current Windows logon session, ReACL will create a warning entry in the log "…WARNING: The UserName value for drive U was empty and could not be mapped to the target user." This warning does not mean that the mapped drive cannot be accessed after Cutover.

  Note: The user profile ReACL process is decoupled from actions against files and folders.

  ReACL will update all files and folders entries found on the machine except for the user profile folders, ntuser.dat, and usrclass.dat even if the user profiles option is selected in the ReACL profile.

  Remaining ReACL activities against user profiles and registry are processed by a separate ReACL task when a cutover operation is performed.

- **Cache Credential**

  The Cache Credentials process assigns a Cache Credentials job to workstation(s). See the Credential Cache and Offline Domain Join topic for more information.

- **Offline Domain Join**

  The Offline Domain Join process is similar to the Cutover process for machines that are directly connected to the network. See the Credential Cache and Offline Domain Join topic for more information.

  Warning: Do not perform the Cutover process on Offline Domain Join workstations. The Offline Domain Join process takes the place of Cutover for workstations connecting via VPN.

- **Cutover**

  The Cutover process moves a Device from the source domain to the new target domain.

  Check **Ignore ReACL Status** to cutover the device regardless of the ReACL status (otherwise the cutover process will not proceed if there is an error with ReACL process).

  Check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the Cutover Status will be displayed as Queued in the devices table and the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date. The Cutover process will begin as soon as possible if not using this option.

  Note: Devices should not be ReACL'd once they have been cutover to the Target. This is not a best practice and is not supported as this can cause problems with the registry and user profiles.

  Note: Certificates are not migrated with Device Cutover.

- **Microsoft Entra ID Cutover**

  The Microsoft Entra ID Cutover process moves a Device from the source domain to an Azure target environment.

  Check **Ignore ReACL Status** to cutover the device regardless of the ReACL status (otherwise the cutover process will not proceed if there is an error with ReACL process).

  Check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the Cutover Status will be displayed as Queued in the devices table and the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date. The Cutover process will begin as soon as possible if not using this option.

  Note: Devices should not be ReACL'd once they have been cutover to the target. This is not a best practice and is not supported as this can cause problems with the registry and user profiles.

  Note: If the Entra ID Join profile has the **Auto-Pilot Cleanup** option selected, the Autopilot remove status must be completed before the Microsoft Entra ID Cutover action can be used.

- **AutoPilot Cleanup**

  The AutoPilot Cleanup action clears existing Auto-Pilot provisioning information from the device. This must be done before the cutover if the source Entra ID Joined device is Autopilot-provisioned and the Entra ID Join Profile has the Auto-Pilot Cleanup option selected.

  Note: Due to the time needed to remove the Auto-Pilot provisioning information in Entra ID, AutoPilot Cleanup should be done several days or 1-2 weeks before device migration.

- **Set Intune Primary User**

  The Set Intune Primary User action is used after the Device Cutover is completed to set the primary user.

- **Cleanup**

  The Cleanup process removes the Source SIDs after the Cutover process completes.

  Note: Cleanup should be done when the migration project is completed. Before running the Cleanup process if a trust is in place, the trust can be broken to test if any application permissions are broken.

  In the Job Options window, click **Apply** to begin the Cleanup process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Cleanup Status will be displayed as Queued in the Devices table and the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date.

- **Upload Logs**

  Log files from the Active Directory Agent can be uploaded to the Active Directory Web Server using Microsoft BITS. To enable this functionality, the installer enables BITS Server Extensions for IIS and create a virtual directory called **DeviceLogs** where all uploaded files will be stored.

  In the Job Options window, click **Apply** to begin the Upload Logs process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Do Not Start Before column in the Device Jobs table will be populated with the selected date.

  The logs will be stored in the configured Agent Logs Repository

  The device logs will be zipped, and the file names will be in the following format with a unique file name: SMART-WIN7X86-1_201573111235.zip

- **Rollback**

  The Rollback process moves a Device back to the original source domain and restores any modified network settings. The Device must have attempted Cutover for this explicit Rollback process to work.

  In the Job Options window, click **Apply** to begin the Rollback process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date.

  Note: Rollback is not supported for Entra ID Device Cutover.

- **ReACL Rollback**

  The ReACL Rollback process rolls back all changes made by the ReACL process. ReACL Rollback can be performed on Devices that have completed the ReACL process.

  In the Job Options window, click **Apply** to begin the ReACL Rollback process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the "Do Not Start Before" column in the Device Jobs table will be populated with the selected date.

- **Status Resets**

  Use the Status Resets action to reset the statuses of the selected devices.

- **Set Device ReACL Profile**

  Use the Set Device ReACL Profile action to assign a Device ReACL profile to the selected devices.

- **Set Migration Wave**

  Use the Set Migration Wave action to set a migration wave to the selected devices.

- **View Jobs**

  Use the View Jobs action to view the device jobs of the selected devices.

  Note: Jobs can be canceled when the Status or Rollback Status is either Queued, Scheduled, Started, or In Progress.

- **View Profiles**

  Use the View Profiles action to view the profiles of the selected devices.

- **View Properties**

  After the Discovery process has been completed for a Device, you can view the properties of that Device.

  Click the **Export All** button to export the content of the window in Excel, text, CSV, or HTML format.

- **Custom Actions**

  If any Custom Actions have been created for Devices, they will appear in the Actions menu.

  In the Job Options window, check **Do not start before** and enter a date if you do not want the job to begin immediately. Select the **Admin Agent** and the **Agent Admin Credentials** to use from the drop-down lists. The Cutover options will also appear if the selected Admin Agent action includes the Cutover action.

File Shares + Network Storage

What is the File Shares + Network Storage page used for?

The File Shares + Network Storage screen allows you to ReACL File Share and Network Storage devices via a network share.

How is a File Share or Network Storage device added?

To add a File Share or a Network Storage device:

1. Select the **Add** icon. The File Share window appears.
2. Enter values in the following fields:
    - UNC Path - the UNC path that will be the starting location for ReACL on the File Share computer
    - Device - The name of the Computer used to access the File Share computer. This computer must be local (same network, region, and so on) to the File Share device. This is a sAMAccountName, not an FQDN.
    - Username - The username to access the File Share device. UserPrincipalName values (user@domain.dom) or domain\username format are supported.
    - Password - the Password to credential access the File Share computer
3. Click **OK**. The File Share device is added to the list.

What actions can be performed on File Shares and Network Storage devices?

The following actions can be performed on File Shares and Network Storage devices by selecting the devices in the list, selecting an action from the drop-down list, and then clicking the **Apply Action** button.

- **ReACL**

  The ReACL process updates the File Share's domain user profiles for use by the matching target user after cutover.

  In the Job Options window, click **Apply** to begin the ReACL process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the ReACL Status will be displayed as Queued in the File Share table and the "Do Not Start Before" column in the File Share Computer Jobs table will be populated with the selected date.

- **Cleanup**

  The Cleanup process removes the Source SIDs after the Cutover process completes.

  In the Job Options window, click **Apply** to begin the Cleanup process as soon as possible. To select when the process will begin check **Do not start before** and then enter or select a date and time. If using the **Do not start before** option, the Cleanup Status will be displayed as Queued in the File Share table and the "Do Not Start Before" column in the File Share Computer Jobs table will be populated with the selected date.

- **ReACL Rollback**

  The ReACL Rollback process rolls back all changes made by the ReACL process. ReACL Rollback can be performed on File Share computers that have completed the ReACL process.

  In Job Options window, click **Apply** to begin the ReACL Rollback process as soon as possible. Check **Do not start before** and then enter or select a date and time when the process will begin. If using the **Do not start before** option, the Do Not Start Before column in the File Share Computer Jobs table will be populated with the selected date.

- **Set Share ReACL Profile**

  Use the Set Share ReACL Profile action to assign a File Share ReACL profile to the selected devices.

- **View Jobs**

  Use the View Jobs action to view the device jobs of the selected devices.

- **Custom Actions**

  If any Custom Actions have been created for File Share, they will appear in the Actions menu.

How-To

Offline Domain Join (ODJ)

Normally, right after a Device is Cutover to a new domain VPN users can't log in to their workstation because Windows must be able to contact the target domain to authenticate against a domain controller for that very first login. Typically, a remote user not on the VPN would need to log in to their machine first and then establish a VPN connection.

Active Directory answers this problem by building on Microsoft's Offline Domain Join (ODJ) process to allow a workstation to join a domain without contacting a Domain Controller. This solution is achieved by first creating an ODJ file for each workstation and then taking advantage of Windows' ability to cache credentials. If users have logged in to the target domain previously, Windows can log them in again even if they can no longer reach a domain controller by using cached credentials.

Active Directory's ODJ process has users pre-login to the new domain before the computer needs to be Cutover so the target credentials can be cached and used for the first post-Cutover login without the need to contact a domain controller first. Then when the administrator is ready to Cutover workstations using the ODJ Action, Active Directory allows the workstation to join the new domain without having the user connect to the corporate VPN and manually join their workstation to the new domain.

The computers that the ODJ process is being run on must have network connectivity to BOTH the source and target environments at the same time sometime pre-cutover in order to have the Cache Credentials function work properly.

Additionally, computers will be unable to save the cached credentials unless the source environment trusts the target environment. The AD Offline Domain Join Credential Cache Quick Start Guide provides guidance on configuring an AD trust to enable Offline Domain Join functionality.

1. CREATING ODJ FILES FOR EACH WORKSTATION

The first step in the ODJ process is for an administrator to use Microsoft's DJOIN utility to create a provisioning file. Only the provisioning part of the DJOIN process is needed. Complete information on DJOIN can be found here.

The Provision, Domain, Machine, and Savefile parameters are required at a minimum. There is the option to control where the target machine will be created using the MachineOU parameter as in the sample shown here.

DJOIN.EXE /Provision /Domain BTADLAB.com /Machine Sales220 /Savefile "\\server\odj-share\Sales220.txt" /MACHINEOU OU=SalesComputers,OU=Sales,DC=BTADLAB,DC=COM

The file must be saved in the ODJ folder in the Repositories path that was configured in the UI.

Generating these files can be completed for all in scope workstations early in the migration process.

WARNING: Be sure to name each text file with the exact matching machine name.

2. CONFIGURING THE CREDENTIAL CACHE PROFILE

The next step is to configure the existing Default Credential Cache profile with the IP address of a Target domain controller, or to create a new profile for this setting.

From the Profiles page select Credential Cache Profiles. Click on **Add** to create a new profile, or **Edit** to modify an existing profile. If you choose to use the Default profile, you must edit it to include a Target DC IP address.

- The **Target Domain Controller Ping Interval** setting determines how long the script will sleep before pinging the DC again.
- The **Timeout Before Job Failure** setting determines the Credential Cache app timeout value that will be used for the job once downloaded to the agent managed machine.
- The **Timeout For User Credentia**l setting determines how long the user is presented with a dialog box to enter their target domain credentials.

3. CACHE CREDENTIALS JOBS

Now that a profile has been configured with a target DC IP address, we can assign a Cache Credentials job to each in scope workstation.

In the Devices list, select one or more Computers. Select **Cache Credentials** from the Actions dropdown menu and click the **Apply Action** button. The Credential Cache Options box appears.

Select a Credential Cache Profile.

A date and time for the Cache Credentials job can be chosen to run the job at a later time. This date/time combination represents the earliest time that this job could run.

If a date/time is not chosen, this job will run on the workstation the next time the agent checks for jobs.

The Devices list will reflect a status of "Queued". When the job is collected by the agent the status will change to "In Progress", and then finally it will transition to a status of "Completed" or "Failed".

On the workstation side, when the Cache Credentials Job is received, the user will be prompted to enter their target credentials. Below is an example of what the user will see when the Cache Credential job runs:

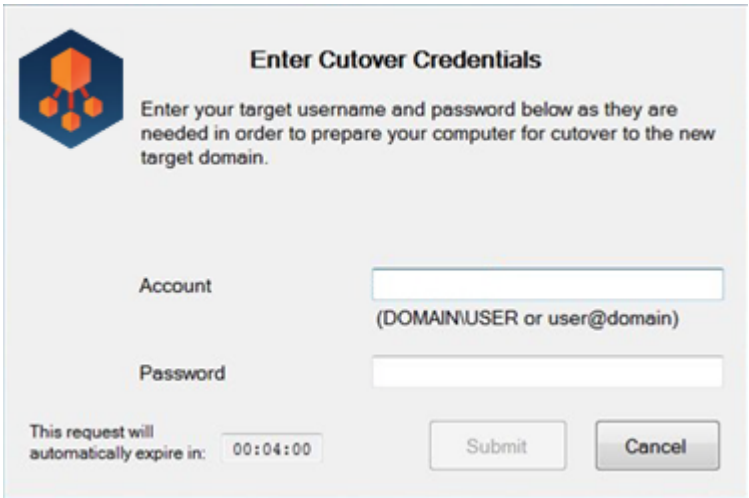


Figure 1: Enter Cutover Credentials

4. REACL

Following Cache Credentials the next recommended step is the ReACL process. The ReACL process can be run repeatedly as needed before ODJ, but it is suggested to be run at least once right after the Cache Credentials process is run.

In the Devices list, select one or more Computers. Select ReACL from the Actions dropdown menu and click the Apply Action button.

The Job Options box appears. A specific date/time combination can be chosen for when to run the job, or just click Apply Action to have this job received by the workstations during their next check for jobs.

5. OFFLINE DOMAIN JOIN JOB

The final step is the actual Offline Domain Join job itself. This is similar to the Cutover process used for machines that are directly connected to the network.

WARNING: Do not perform the Cutover process on Offline Domain Join workstations. The Offline Domain Join process takes the place of Cutover for workstations connecting via VPN.

In the Devices list, select one or more Computers. Select **Offline Domain Join** from the Actions dropdown menu and click the **Apply Action** button.

The Job Options box appears. A specific date/time combination can be chosen for when to run the job, or just click **Apply Action** to have this job received by the workstations during their next check for jobs.

WARNING: The Offline Domain Join (Job Scheduling Options dialog box) start date and time must be set AFTER the Cache Credentials job (Cache Credential Options dialog box) start date and time.

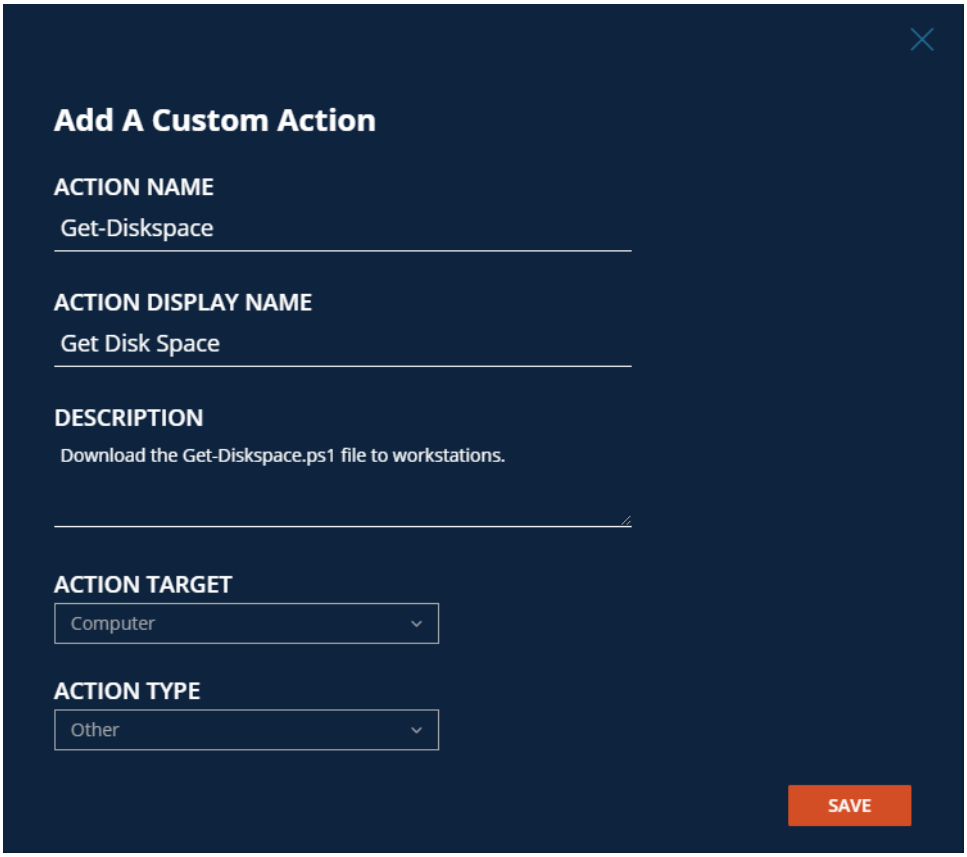
The Offline Domain Join process does not support rollback.

Custom Action Example

Scenario: The administrator wants to download the Get-DiskSpace.ps1 file on selected workstations.

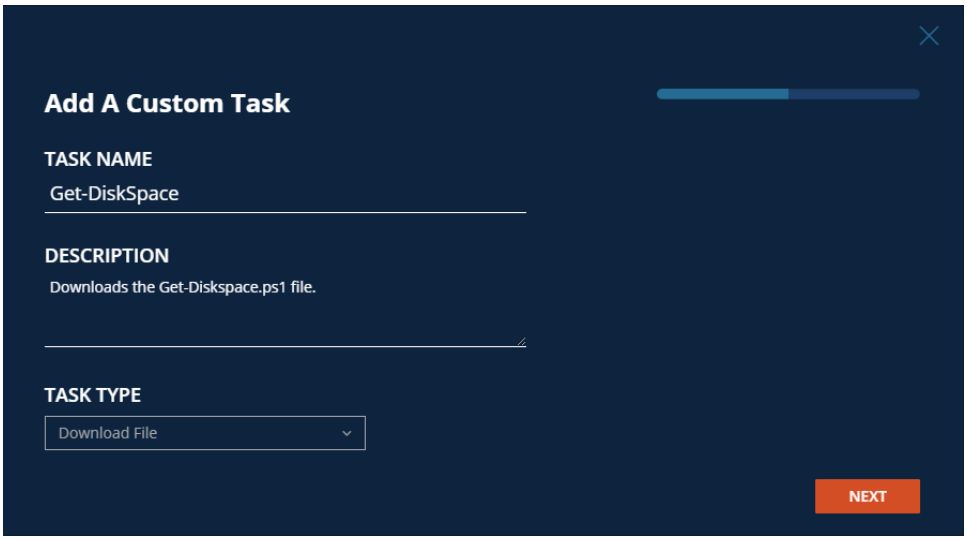
Steps:

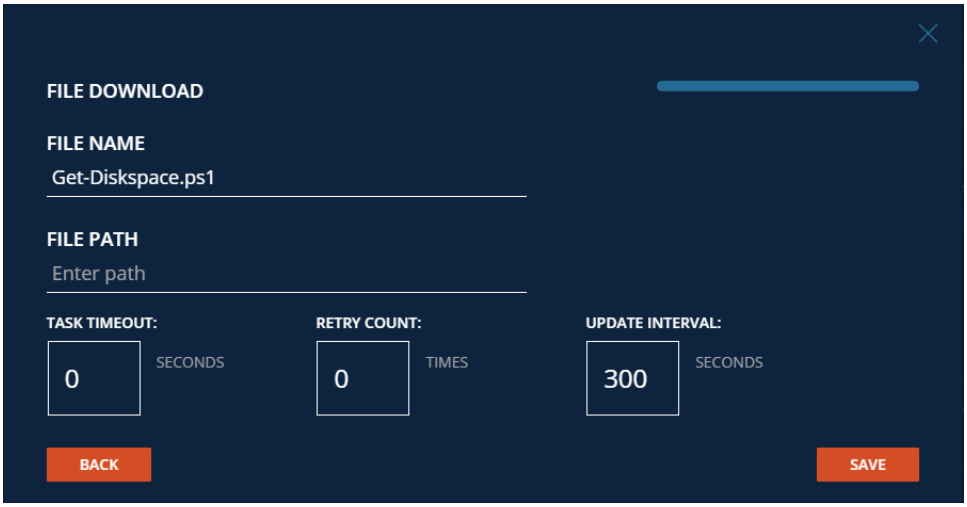
1. Copy the Get-DiskSpace.ps1 file into the file location of the configured Custom Downloads Repository.
2. On the Actions screen, click the **New** button under the Actions table.
3. Add a Custom Action named "Get-Diskspace". The Action Display Name is how the option will appear in the Actions menu. Select the "Computer" Action Target so the menu option will appear in the Actions menu on the Computer Actions screen.



4. Click the **New** button under the Tasks table.

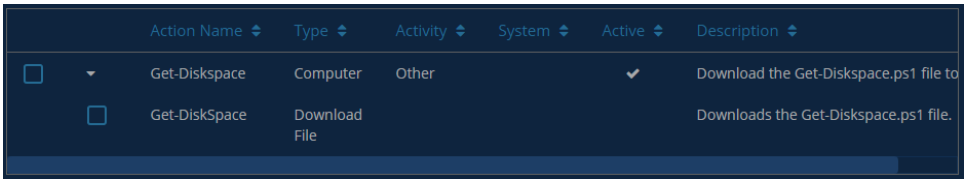
5. Select the "Download File" Task Type and enter the File Name. The full path to the file should not be entered.





6. Select the task, select "Get-Diskspace" from the Select Action drop-down menu and click the **Add To** button.

   Ensure the Action is active. The action can be expanded to view the associated Task.



7. On the Devices + Servers screen, select the devices and then select the new "Get Disk Space" option from the Actions menu. When the new download job is run successfully against a machine, the Get-DiskSpace.ps1 file will reside locally on disk at c:\Program Files (x86)\Binary Tree\P365ActiveDirectoryAgent\Downloads\.

FAQs

Active Directory FAQs

What ports does the agent use to connect?

The Active Directory Agent uses three outbound ports

- TCP 443/80
- UDP 3030

I've installed the agent and the device isn't ready, what do I do?

On startup the Active Directory agent will phone home sometime in the first four hours. This communication offset time is an agent specific random and evenly distributed offset so the initial communications of a large number of devices set up at once will be spaced out and not overload the servers. If your device has the agent installed but you haven't waited up to four hours yet, wait up to four hours and then re-check the Ready Devices list to see if your device shows up before proceeding to other network troubleshooting operations.

How do I adjust the agent polling interval?

In Active Directory, unlike in Active Directory Pro, the agent polling interval is not end user adjustable. The polling interval is every two minutes over UDP and every four hours over TCP. Should this amount of network traffic be an issue contact Support to investigate reducing the polling interval. Note that reducing the polling interval will cause queued migration actions to take longer to be picked up by the agents.

How many migration actions can I queue at once?

In Active Directory you can queue as many migration actions at once as you would like. There is a hard limit of 600 agents per each two minutes who will be notified by the job availability cache that they have a job waiting for them. Therefore the minimum amount of time which could be required for those queued migration actions to be picked up will be the number of queued migration actions divided by 600 and multiplied by two minutes.

Agent last contact time isn't updating every two minutes is something wrong?

In Active Directory the Agent last contact time is updated based on the TCP connection with the back end. This will occur if a job is retrieved or every 4 hours as a fall back. It is not expected that the agent last contact time will update

every two minutes even if the UDP requests to the job availability cache are functioning correctly.

The machine name was changed during the migration project, will it keep working?

Changing the machine name during a migration project may have unexpected implications. We recommend that you avoid doing so if possible. If not, you will need to delete the device from Power365 and reinstall the agent. Use the Status Resets action to reset the registration status of the device, then set the Directory Sync Workflow to reconcile on next run and run it. This will delete the old device from the database. Finally, reinstall the Active Directory Agent on that device and run the Workflow again to read it in.

How do I remove Devices from Active Directory?

To delete registered Devices from Active Directory, first use the Status Resets action to clear their registration status, then run the related Directory Sync Workflow with the setting 'Reconcile on next run' enabled. Any unregistered device records in scope of the Workflow will be removed from the database during a reconcile.

Can I migrate to and from GCC/GCCH tenants?

Active Directory supports GCC and GCCH as target environments, in addition to Commercial tenants. Only Commercial and GCC are supported as source environments. To enable GCC/GCCH Device Migration, please contact Quest Support for additional configuration described in the following article: Update GCC/GCCH tenant object's RID value for ReACL. This configuration is required for successfully switching the user profile during cutover.

Additional Info

Active Directory Architecture

The first step towards success on a project using Active Directory is to understand the product architecture and how this architecture will operate in your environment.

Active Directory consists of the following components:

- A directory synchronization engine
- A REST based web service
- A management interface
- A lightweight agent for workstations and member servers

The directory synchronization engine, the web service, and the management interface will all access the same SQL database. In most scenarios, these components will be installed on the same system. In larger or more complex network environments, the components can be distributed across multiple systems.

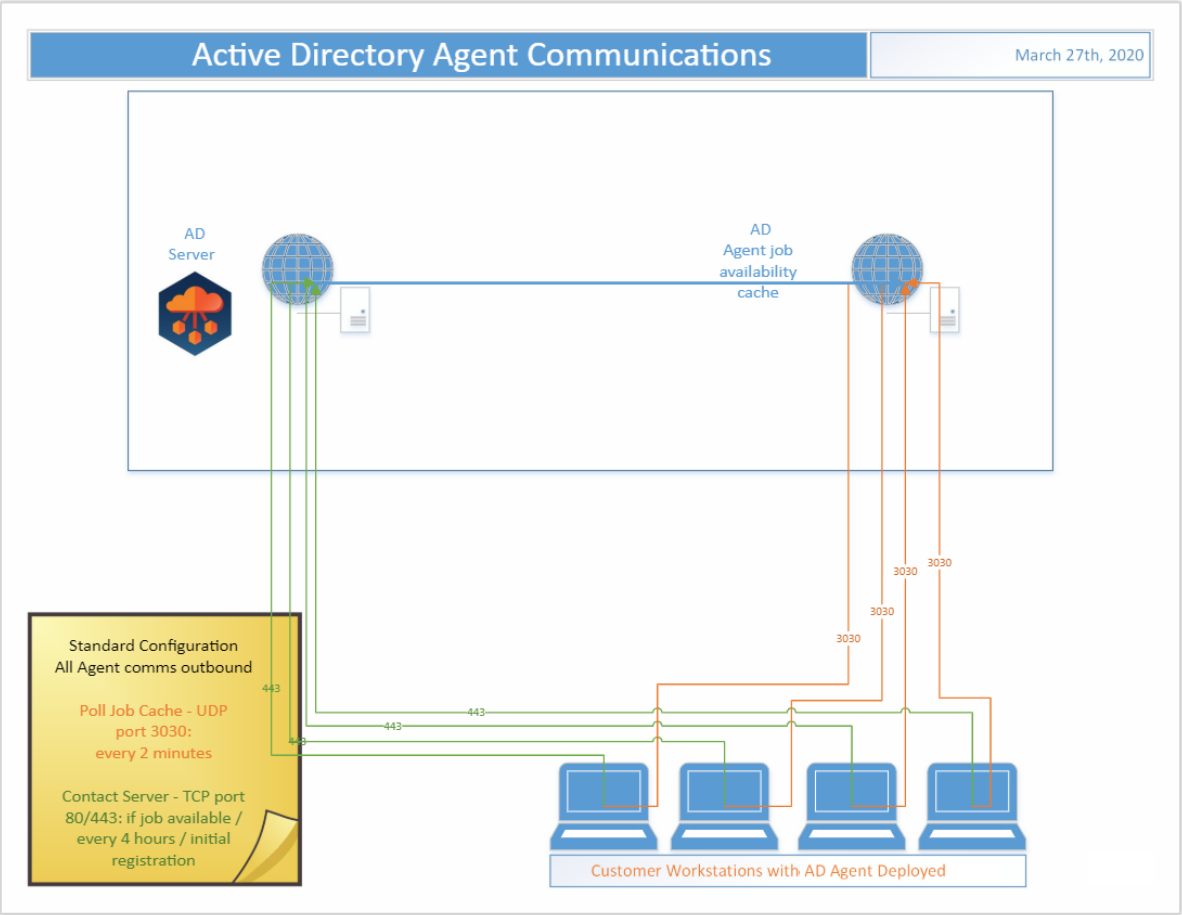
The directory synchronization engine is provided by Directory Sync. Directory Sync is included as part of Active Directory.

User workstations, member servers and computers are collectively referred to as Devices in Active Directory. Computers communicate with the Active Directory web service using the Active Directory Agent. The Active Directory Agent is a lightweight application that installs as a service on Windows computers.

To ensure that no firewall exceptions are required, the web service does not “call” the Devices to be migrated. Instead, the Active Directory Agents contact the web service at defined polling intervals, using standard HTTPS or HTTP requests to collect jobs. Jobs include key tasks such as system discovery, updating the operating system, file system, and user profile permissions, and migrating the computer to the new domain.

Standard Configuration

In the Standard Configuration for Active Directory the Agent is deployed to each Device to be migrated. Those Agents communicate outbound to the Active Directory webserver in Azure over ports 80/443 every 4 hours, when a job is available, or when initially registering. They also communicate outbound to the Active Directory Agent job availability cache in Azure over UDP on port 3030 every 2 minutes.



Web Proxy Configuration

In the Web Proxy Configuration for Active Directory the Agent is deployed to each Device to be migrated and use of a web proxy is enabled. Those Agents communicate outbound through the defined proxy port to the Active Directory webserver in Azure over port 443 every 4 hours, when a job is available, or when initially registering. They also communicate outbound through the defined proxy port to the Active Directory Agent job availability cache in Azure on port 80 every 2 minutes.

Troubleshooting

- **Problem:** What do you do when a user tries to use a network printer post ReACL process and/or Cutover and receives an access denied error?

  Solution: Synchronize the SID History for that User to resolve the problem.

- **Problem:** Observed Access Denied error when trying to ReACL a Windows NAS Shared Drive.

  Solution: To fix this:

  1. Add the user credential in the NAS Profile screen in the Active Directory Pro Console. This user should be installed on a workstation with Local Admin Rights
  2. After the Agent is installed on the workstation, change the Active Directory Pro Agent Service account from Local System to the user credential specified in step 1. This user should also be logged in on the workstation as well
  3. Turn off UAC on the workstation
  4. ReACL the Windows NAS Shared Drive

- **Problem:** A workstation that has been successfully cutover no longer responds to any additional jobs, such as Cleanup.

  Solution: If a workstation that has been successfully cutover now fails to respond to any additional jobs, such as Cleanup, check the Application event log. If you see a *"The remote name could not be resolved"* error, this most likely means that the SRV record for the Active Directory Pro Server can no longer be resolved due to a DNS lookup failure.

  If you cannot "Ping" the Migrator Pro for Active Directory server from any other machines in the target domain, then you will need to remedy this on a more global scale, such as creating a conditional forwarder on the target machines' current DNS server pointing to the appropriate location.

  If you are able to "Ping" the Migrator Pro for Active Directory server, then check the Network Profile that was used during the Cutover to verify that the DNS settings were correct in that profile.

Cutover Job Result Codes

Result Code	Error	Rollback Possible
1	Unidentified Error - PowerShell Command Error	No
2	Source Domain could not be contacted	No
4	Bad Source Credentials	No
8	Target Domain could not be contacted	No
16	Bad Target Credentials	No
32	Target DNS Server could not be contacted or could not resolve the target DNS domain	No
64	Change Obtain DNS by DHCP	
128	Set DNS Server IPs	
256	Set WINS Servers	
512	Register NIC with DNS	
1024	Clear DNS Suffix Search List / Set to use NIC	

Result Code	Error	Rollback Possible
2048	Set Alternate DNS Suffix List	
4096	Enable Dynamic DNS Registration	
8192	Set NIC Specific DNS Suffix	
16384	Domain Disjoin Failed	
32768	Domain Join Failed	
65536	Source domain name does not match the system's domain	No
131072	Computer Reboot failed	
262144	Target Domain Name could not be resolved via existing DNS, and new DNS Servers were not provided	No

Note: An odd numbered result code represents an error running the Cutover PowerShell script. The most common cause of an odd numbered result code during Cutover is that the computer either has no network card with a default gateway or more than one network card with a default gateway.

Note: Result codes are additive. There are likely multiple errors if the result code is not represented in the table.

Upload Logs Result Codes

This table includes result codes for BT-UploadLogs PowerShell jobs.

Result Code	Error	Rollback Possible
32	(zip folder) could not be created.	No
64	Failed to Zip log files on computer.	No
128	Upload failed to contact the server. Please verify the URL (url) is correct and BITS is enabled.	No

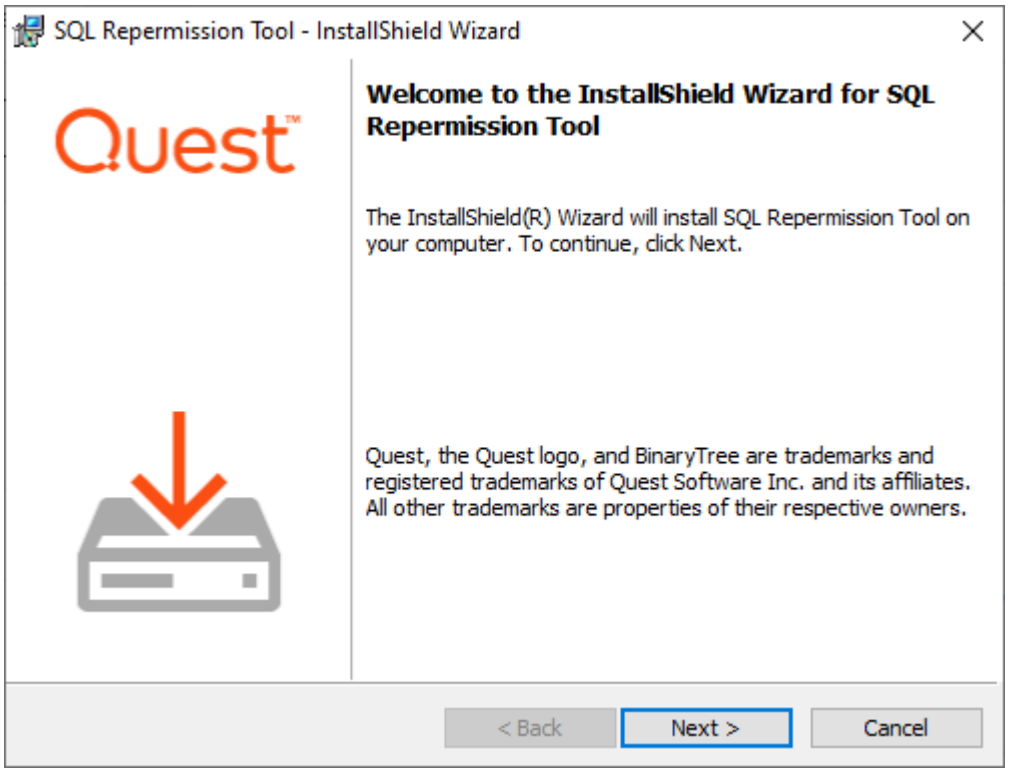
SQL Repermission Tool

Use the SQL Repermission Tool to update a SQL Server's Source AD Windows Authentication Group Login permissions and their associated database users for the Target domain to which the user and group objects have been migrated.

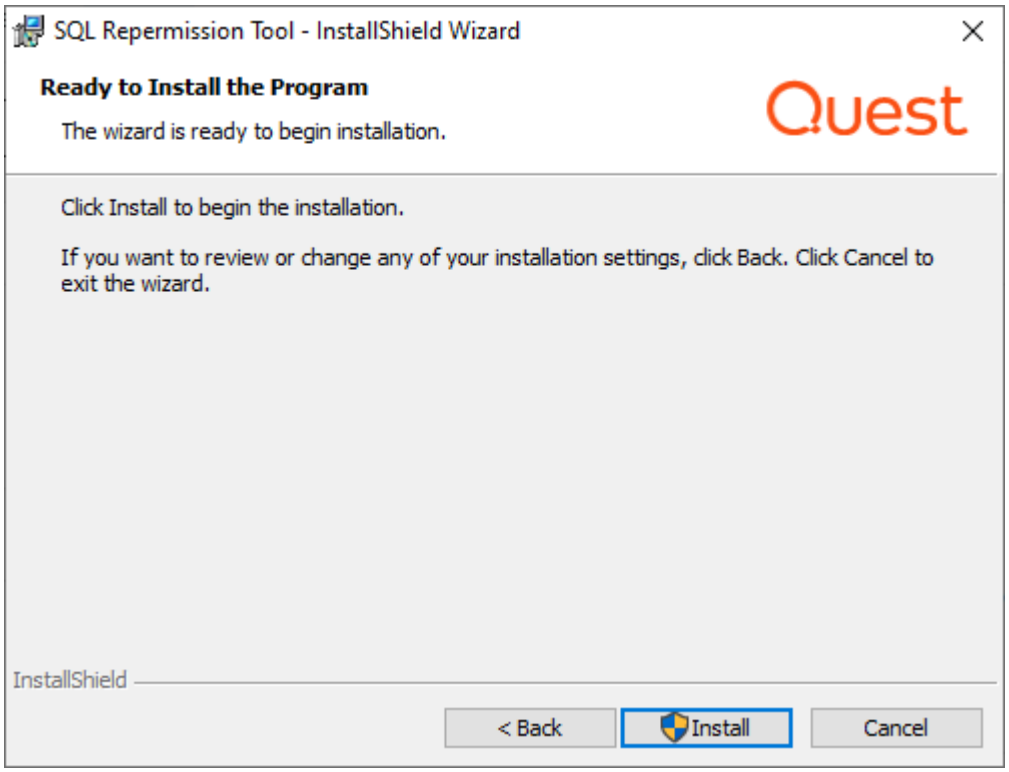
Prior to re-permissioning SQL servers, accounts must be migrated and Mapping Files created.

1. Download the **SQL Repermission.msi** file from the Downloads screen.
2. Run the installer on a machine that will have access to the SQL Server instance and databases to be re-permissioned.

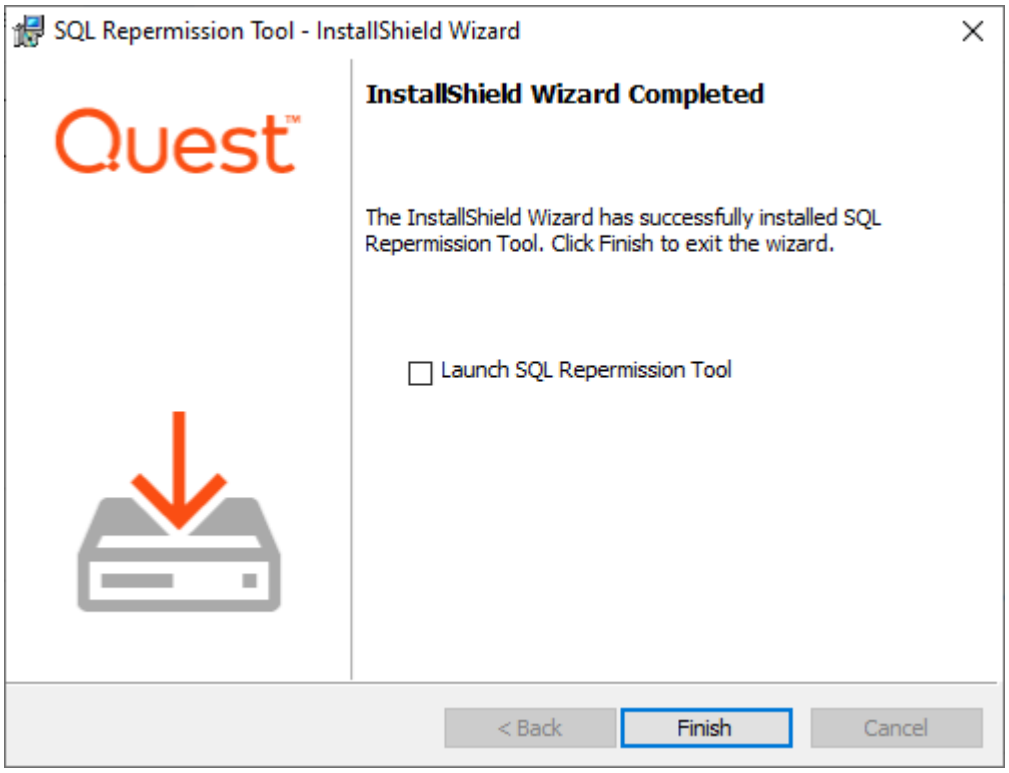
3. The Welcome screen appears. Click **Next** to continue.



4. The "Ready to Install the Program" screen appears. Click **Install** to begin the installation.

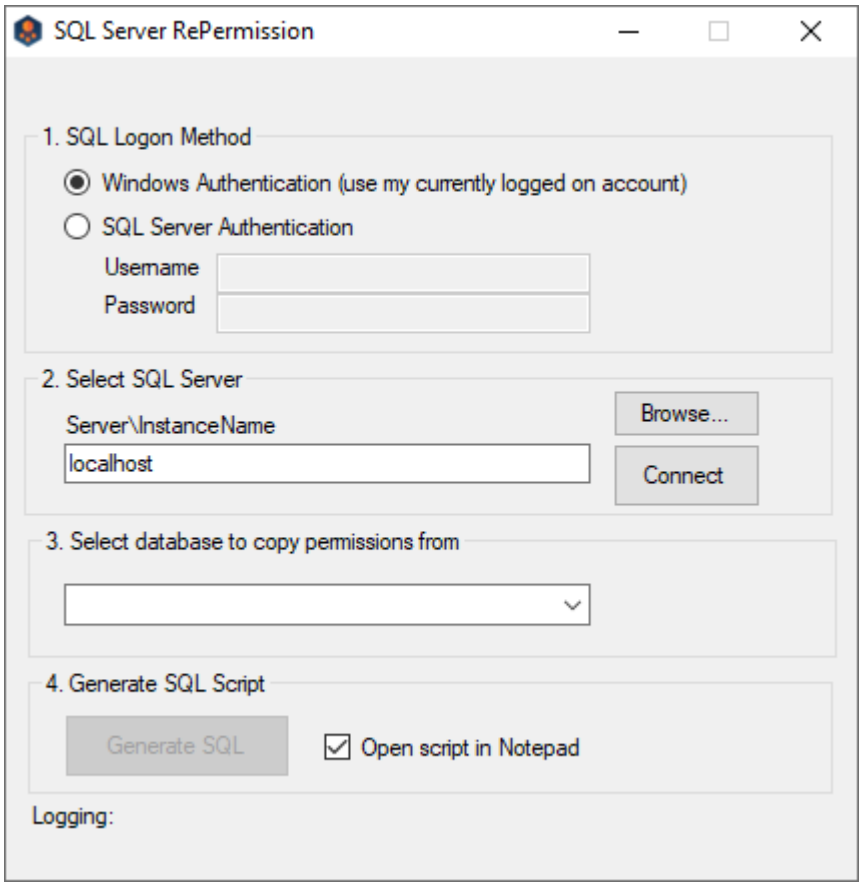


5. When the installation completes, the "InstallShield Wizard Completed" message appears. Click **Finish** to close the wizard.



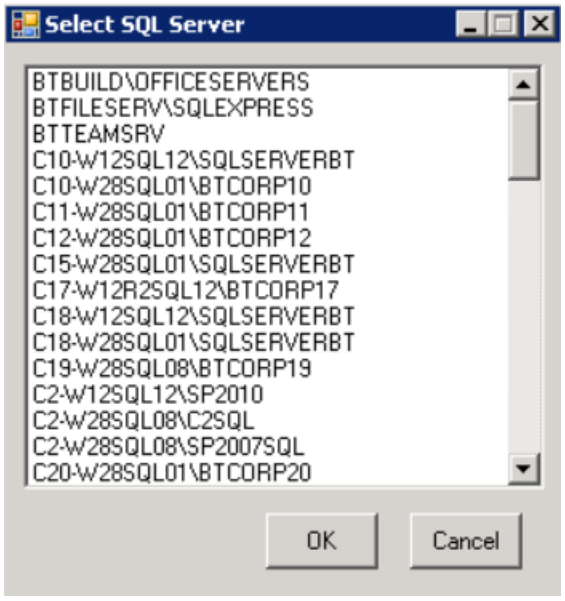
6. Copy the **map.usr** and **map.gg** files created to the SQL Repermission installation folder, default location is "C:\Program Files\Quest\SQL Repermission".

7. Launch the SQL Repermission tool from the Apps screen or the Start menu.

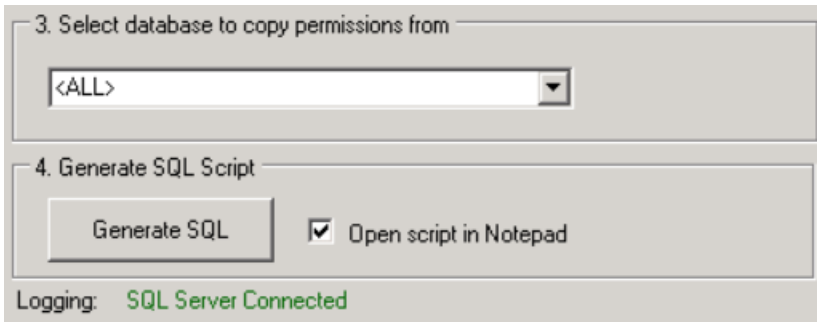


8. Select the **SQL Logon Method**. If SQL Server Authentication is selected, enter the Username and Password. If Windows Authentication will be used, you must be logged onto the machine with an account that has access to the SQL Server instance and databases to be re-permissioned.
9. Click on **Browse** to select the SQL Server instance to be re-permissioned.

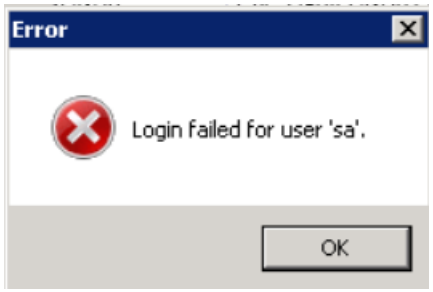
10. Select the SQL server instance from the list and click on **OK**.



11. Click on the **Connect** button. If connection is successful, the Logging message should read “SQL Server Connected” and there should be databases available to pick from in the drop-down list.



Note: If the login information is incorrect, the following error will be received. The credentials to connect to the SQL server instance should be corrected, and then the Connect should be retried.



12. Once successfully connected to the SQL Server instance, in the drop down select either **<ALL>** or a specific database that needs to be re-permissioned.

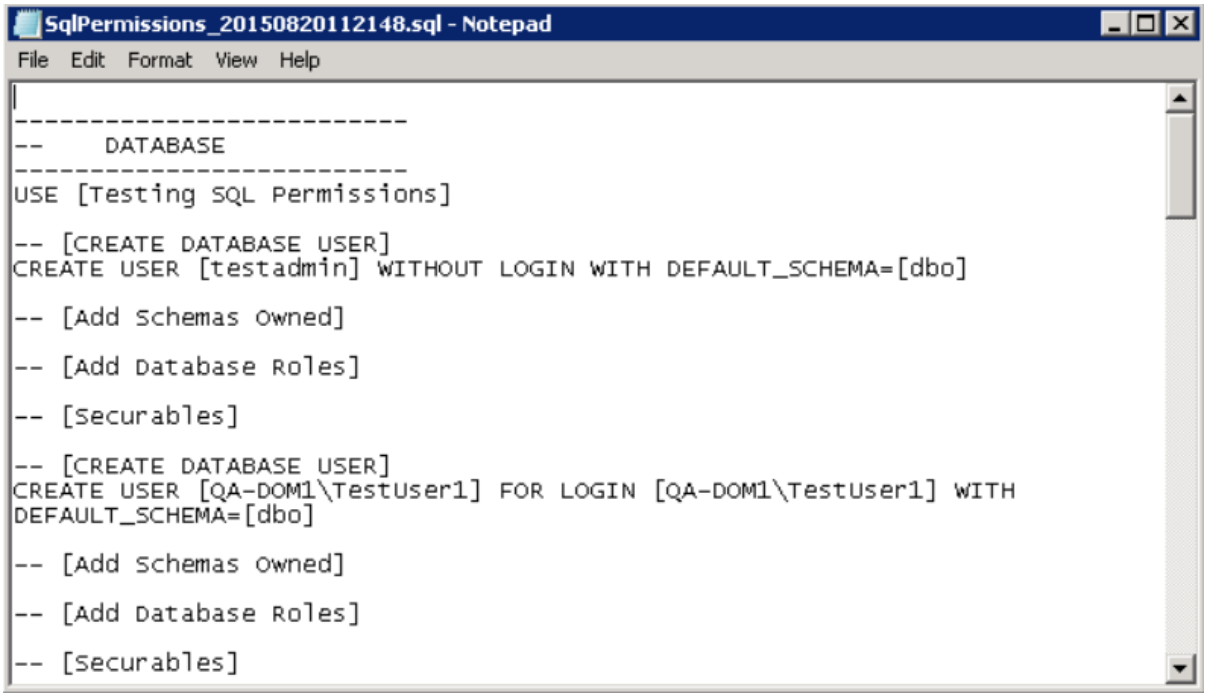
13. Click on the **Generate SQL** button. If the **Open script in Notepad** option is left checked, the results will be displayed when completed.

14. The Logging information will display the name of the SQL file created in the directory that the application is located.

Logging: C:\Program Files\Quest\SQL Repermission\SQLPermissions_20150820112148.sql

15. If the option to open the file in Notepad was not checked, navigate to where the file was saved and right-click and choose **Open with Notepad**.

16. The results of the process can be reviewed prior to actually executing it on the SQL Server instance.



17. When the SQL file has been reviewed, either open the file in SQL Server Management Studio or create a new Query in SQL Server Management Studio and copy/paste the contents of the file into the Query.

18. Execute the Query and the new target credentials will be created.

Domain Rewrite

What is Domain Rewrite?

For mergers and acquisitions, email rewriting allows a company to present a unified email address to the outside world before and after the user's mailbox has been migrated. Domain Rewrite is a key requirement for any organization utilizing more than one Microsoft 365 tenant to service their end-users.

Domain Rewrite substitutes the From, To, and Cc addresses in the outgoing and incoming emails with the addresses from the target or source tenant depending on the selected domain rewriting scenario. Emails are automatically redirected to the source or target mailbox, and you can specify the users processed by the service. For example, you can turn on the service for only Sales and Marketing team members.

Domain Rewrite will take all the necessary steps to create this coexistence space in the Exchange online environment, including creating and managing all the required connectors, mail flow rules, mail-enabled users, and groups in source and target environments.

Domain Rewrite supports the following scenarios:

- Replace senders' address with the target primary email address.
- Replace senders' address with the source primary email address.

Note: The address is only rewritten in the messages that go to the recipients outside your organization. Internal users receive the message with the original address.

This user guide covers the steps required to configure and enable Domain Rewrite. The Domain Rewrite Quick Start Guide summarizes these steps and addresses some frequently asked questions.

How do I enable domain rewrite service for users using Domain Rewrite?

If the **Rewrite With Target Address** mode is selected, their outbound email messages will be intercepted by Domain Rewrite. Domain Rewrite will rewrite the message header with the target tenant's SMTP Accepted Domain information. To the outside world, it looks as if the sender was already using a mailbox in the target tenant.

This scenario commonly applies to users from the Source tenant that need to communicate with external recipients from the name of the Target organization. It usually happens when the mail migration is not yet finished, but you want to use the consistent branding.

Rewrite With Target Address

To enable a user for Rewrite with Target Address, select the matched user, click **Email Rewrite** from the action menu, and then click **Apply Action**. Select **Rewrite With Target Address** mode, select either the **Prepare User(s) for Address Rewrite** or **Enable User(s) for Address Rewrite** option, and then click **Submit**.

The **Prepare User(s) for Address Rewrite** option sets forwarding but does not enable rewrite. If an account is mailbox-enabled or a cloud-only MEU, forwarding is set on the tenant object. If an account is a hybrid MEU,

forwarding is set on the AD object and the changes must replicate to the tenant via Entra Connect. This option is useful for confirming all permissions and access is working prior to enabling rewrite. Performing Prepare ahead of time reduces the steps and duration of enabling address rewrite later.

The **Enable User(s) for Address Rewrite** option sets forwarding, waits for Microsoft replication, and then begins the process to enable rewrite.

When the **Skip Mail Forwarding Configuration** option is checked, the rewrite enablement process begins without setting forwarding.

Note: To ensure that all incoming mail is automatically redirected to the Source mailbox, Domain Rewrite will enable SMTP Forwarding on Target Mailboxes and will update the External Address on Target Mail Users.

Rewrite With Source Address

If the **Rewrite With Source Address** mode is selected, any email sent from that user will appear as if they are still coming from the source mailbox's primary SMTP address. During a merger or acquisition project, this allows a company to hide the migration process from the outside world, until all users have been migrated and the Accepted Domains can be migrated themselves.

This scenario commonly applies to migrated users in the Target tenant that still need to communicate with external recipients from the name of the Source organization. It usually happens when you need to keep the original brand while merging all accounts in the Target Tenant.

To enable a user for Rewrite with Target Address, select the matched user, click **Email Rewrite** from the action menu, and then click **Apply Action**. Select the **Rewrite With Source Address** mode, select either the **Prepare User(s) for Address Rewrite** or **Enable User(s) for Address Rewrite** option, and then click **Submit**.

The **Prepare User(s) for Address Rewrite** option sets forwarding but does not enable rewrite. If an account is mailbox-enabled or a cloud-only MEU, forwarding is set on the tenant object. If an account is a hybrid MEU, forwarding is set on the AD object and the changes must replicate to the tenant via Entra Connect. This option is useful for confirming all permissions and access is working prior to enabling rewrite. Performing Prepare ahead of time reduces the steps and duration of enabling address rewrite later.

The **Enable User(s) for Address Rewrite** option sets forwarding, waits for Microsoft replication, and then begins the process to enable rewrite.

When the **Skip Mail Forwarding Configuration** option is checked, the rewrite enablement process begins without setting forwarding.

Note: To ensure that all incoming mail is automatically redirected to the Target mailbox, Domain Rewrite will enable SMTP Forwarding on Source Mailboxes.

Does Domain Rewrite rewrite the address when a "Send-on-Behalf" delegate sends a message for an enabled Domain Rewrite user's mailbox?

Yes. Domain Rewrite supports rewriting the address of the mailbox owner and/or delegate. If Domain Rewrite is enabled for both, both addresses are rewritten. If Domain Rewrite is enabled for the mailbox owner, then only their address will be rewritten.

Domain Rewrite Requirements

Domain Rewrite (Email Rewrite)

To deploy Domain Rewrite between tenants the following will need to be ready prior to the configuration of the service.

Domain Rewrite Deployment Checklist:

The following checklist provides a quick reference to the items or decisions required to begin configuration of Domain Rewrite.

1. Procure one (1) SSL single domain certificate for each tenant environment using one (1) of the accepted domains.
2. The password associated with the SSL certificate will be required when uploading each certificate.
3. Choose which domains will particulate in Domain Rewrite.
4. Deploy DKIM DNS TXT records for each tenant environment during project set up.

SSL Certificates

To successfully configure the Email Rewrite Service, a valid SSL certificate must be procured for each source and target tenant. Each certificate must contain a single accepted domain, one (1) for each tenant. The selected certificate cannot contain subject alternative names (SAN). The common name (Subject Name) must match one (1) of the Exchange Online accepted domains configured within the tenant.

This certificate is utilized to secure the Exchange Online connectors over TLS that will be used to transfer message between the Email Rewrite service and each tenant. The new certificates will be uploaded to the project using a PFX formatted certificate. PFX files contain the public key file (SSL Certificate file) and the associated private key file (password).

The requirements for the certificate are as follows: (Names are for example purposes only.)

- Common Name: contoso.com
- Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider
- Bit length: 2048 or higher
- Must be valid for Server Authentication and Client Authentication.
- Must be signed by a trusted public root CA.
- Must contain a private key (password).
- Must not expire before the end of the project.
- Must have a Friendly Name defined.

Important Tip: The domain listed on the certificate cannot be moved as part of a Domain Cutover process. If you plan to move all accepted domains, you should plan to acquire a certificate for a newly created accepted

domain to use as a placeholder. This domain will not be moved or used; it will be used only as the subject for the TLS certificate.

DKIM (Email Signatures)

Domain Rewrite ensures email authenticity after rewrites by signing messages using a Domain Keys Identified Mail (DKIM) certificate. To properly sign emails, a DKIM certificate will automatically be generated and assigned to each participating domain(s) in the source and target tenants.

Each participating Accepted SMTP Domain from the source and target tenants will require a DKIM TXT record be created in your public DNS. During project configuration, Domain Rewrite will generate all the required parameters to easily and quickly publish your TXT records for each domain.

Each participating Accepted SMTP Domain from the source and target tenants will require to enable DKIM at the tenant level, additional information can be found at this Microsoft Link How to use DKIM for email in your custom domain - Office 365 | Microsoft Learn

DNS

To complete set up of Domain Rewrite the DKIM/Email Signatures DNS txt record must be published in the source and target public DNS. Once the records are published, Domain Rewrite will automatically verify the records. Once verified you will be able to complete the project's Domain Rewrite configurations.

The following is an example of the TXT record parameters required to publish the record. Your key will be unique to your project.

- Name: selector1._domainkey
- Type: TXT
- TTL: 10
- Value: v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmvFUb+TkozfdnA0dA3AHOwAUYdfNVlBkR72+gqp2GxwK8yYPRI/E1/zp5DDZ/i8epWTR/F9u4jDJxjLqYF9d8m7qhJFjXxzWH2TbMQC4VgUfRtq5WAJmPUrCBdxxvMoOAKQ+aYagtXpv9HlH7PAKXsUFbqGGZ0GQFSvM0GKC7hQIZZQAB

Please Note: Domain Rewrite supports existing Exchange Online DKIM certificates and does not interfere with the Domain Rewrite DKIM certificates. A unique selector will be provided if Exchange Online DKIM certificates are found.

SPF

When planning the deployment of Domain Rewrite Service we recommend the following regarding Sender Policy Framework (SPF) records:

- Update your existing SPF record to include the On Demand Migration Domain Rewrite list of acceptable domains. This will prevent any hard failures when routing mail through the Rewrite Relay Service.
    - Include one of the following domains with your SPF record from all source and target domains participating in Domain Rewrite based on the region where your On Demand Migration Domain Rewrite project is configured.

      Global Record which includes all region-specific records

        - spf.odmad.quest-on-demand.com

      On Demand region-specific records

      US

        - spf.us.odmad.quest-on-demand.com

      Canada

        - spf.ca.odmad.quest-on-demand.com

      EMEA

        - spf.eu.odmad.quest-on-demand.com

      United Kingdom

        - spf.uk.odmad.quest-on-demand.com

      Australia

        - spf.au.odmad.quest-on-demand.com

Important Tip: Do not plan on utilizing the default “tenant.onmicrosoft.com” domain when deploying On Demand Migration Domain Rewrite Services. This is due to concerns regarding the external recipient domain's having SPF hard fail enabled.

DMARC

If your organization utilizes Domain-based Message Authentication, Reporting and Conformance (DMARC) to prevent email spoofing, then Domain Rewrite is DMARC ready.

There are no additional requirements to support DMARC with Domain Rewrite, however it is highly recommended that the following related topics be reviewed prior to execution.

DKIM

What is DKIM?

DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails, a technique often used in phishing and email spam. DKIM allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. Wikipedia

Why is DKIM required for Domain Rewrite (ERS)?

A DKIM or commonly known as an Email Signature, is required for Email Rewrite Services (ERS) to ensure Domain Alignment and Authenticity. Without the proper email signature, DMARC would fail if quarantine or reject are enabled. For more information about DMARC and ERS, see this article.

When is DKIM required for Domain Rewrite (ERS)?

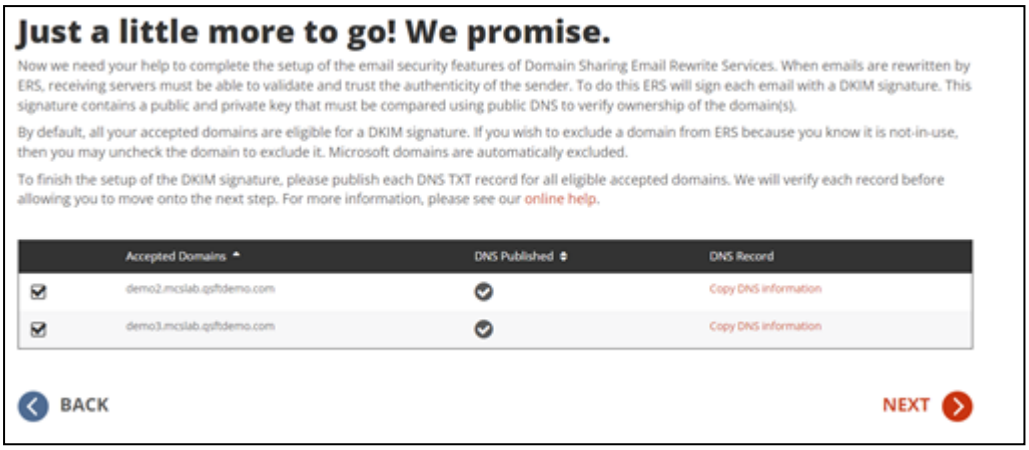
When emails are rewritten by ERS, receiving servers must be able to validate and trust the authenticity of the sender. To do this ERS will sign each email with a DKIM signature. This signature contains a public and private key that must be compared using public DNS to verify ownership of the domain(s).

By default, all your accepted domains are eligible for a DKIM signature. If you wish to exclude a domain from ERS because you know it is not-in-use, then you may uncheck the domain to exclude it. Microsoft domains are automatically excluded.

When do I choose my DKIM domains for ERS?

During project setup of the ERS components.

The project wizard will walk you through the configurations of ERS. During this process you will be asked to choose which domains will require email signatures. It is recommended any accepted domain being used by any mail-enabled object within your tenant environments be published. If the accepted domain is not in use by anyone, then it is not required. If in doubt, enable it.



How do I publish my DKIM DNS records?

It's simple if you have access to your public DNS. In most cases, even as IT administrators we may not have direct access to update public DNS. In those cases, you'll need to submit a change control to publish DNS TXT records for all the accepted domains. And each record must contain the public key provided in the *"Copy DNS Information"* action in the project wizard.

On Demand Migration will present a unique public key associated with the domains. That key is to be published as a DNS TXT record for the selected domain. Here is an example of such a record.

Example TXT Record:

Name: selector1._domainkey.contoso.com

Type: TXT

Value: v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUXA4GNADCBiQKBgQC0uekhrGKBUmlvPXcy2XxEBG
7Hn+64l505xl0vwk3cnHwWaVw1LTFcsFxUCf2tXpNE02ap5EhCCTjGGOyEJ/ZX1ScptyDP3
X/eJDn4jq5sQQruK3F9KdU9kLTmkALK+ySz+lpX40DLXWw2BauOEzpVD65XZUwiN5DJUc
37/RcozRwIDAQAB

The Project implementer will copy this information and provide it to the team that manages DNS for this domain. On Demand Migration will immediately begin monitoring DNS for this record. Once the DNS TXT record has been validated by On Demand Migration, the Project implementer may select the desired domains to complete the setup.

TLS/SSL

What is TLS?

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer, are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP. Wikipedia

Why is TLS required for Domain Rewrite (ERS)?

To ensure encrypted, secure mail routing, TLS is enforced for all connections.

To successfully implement the Domain Rewrite, a valid SSL certificate is required for all source and target tenants in scope for this service.

When the Email Rewrite Service is enabled for the first time, Connectors will be automatically created in Exchange Online to provide secure (TLS) email routing between the tenants and the Domain Rewrite relays.

When is TLS required for Domain Rewrite (ERS)?

It is always required. An SSL certificate is always required to ensure a secure connection between ERS and Exchange Online.

What is required to setup TLS for Domain Rewrite (ERS)?

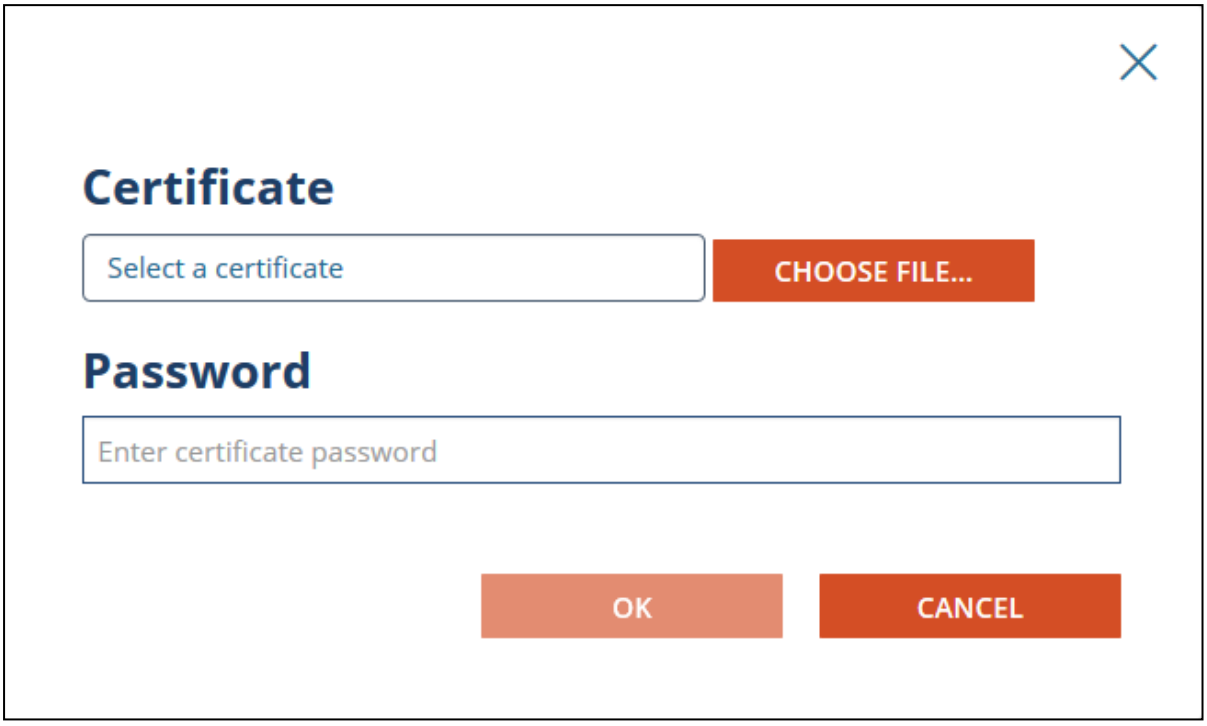
Each tenant configured within the Domain Rewrite project will require 1 SSL certificate in the PFX format. The SSL certificate can only be uploaded to Domain Rewrite in the required PFX file format. PFX files contain the public key file (SSL Certificate file) and the associated private key file (password).

The requirements for the certificate are as follows (names are for example only):

- Common Name: contoso.com
- Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider
- Bit length: 2048 or higher
- Must be valid for Server Authentication and Client Authentication.
- Must be signed by a trusted public root CA.
- Must contain a private key (password).
- Must not expire before the end of the project.
- Must have a Friendly Name defined.
- No Wildcards Certificates
- No SAN (Subject Alternate Name) Certificates
- PFX file format with Password
- Paired with Email Signatures (DKIM) Domain

How do I upload the PFX certificate?

During project setup, the wizard will ask you to upload your pfx file and enter in the password.



When the SSL certificates are successfully uploaded and activated in On Demand Migration, an email notification will be sent to the project administrators. And, as with most Project settings, you can always return to the Dashboard to upload new certificates or make changes.

Rules, Connectors, and Groups

I've finished project setup for Domain Rewrite, what's next?

After Domain Rewrite is configured in your project, each tenant will have a series of configurations automatically deployed through our orchestration engine. The following FAQs will help you get acquainted with the Domain Rewrite configuration components.

What is setup when I enable Domain Rewrite?

When Domain Rewrite is enabled, the following configuration items are created and managed. If Domain Rewrite is disabled, the same configurations will be removed.

1. Exchange Online Transport Rules to redirect mail flow for Domain Rewrite eligible users
2. Exchange Online Connectors to manage encrypted mail flow between Domain Rewrite and Exchange Online
3. Mail-Enabled Groups to managed user's eligibility for Domain Rewrite

All configurations can be reviewed for any tenant from the Exchange Online portal. You may also view all configurations using PowerShell.

How can I confirm everything was created?

You may verify the configurations from the Microsoft 365 admin portal or by using PowerShell.

To verify by portal, simply login to the Exchange Online Admin Portal. Then navigate to Mail Flow. Under Mail Flow you will find the rules and connectors. To view the groups, navigate to recipients then groups.

The simplest way is to use a PowerShell query to get a list of all rules, connectors and groups. Follow these easy steps to do just that.

1. Launch PowerShell.
2. Connect to your tenant, if you don't know how, here is a quick article from MS:
    a. How to connect to Exchange Online PowerShell
3. Once authenticated, run these example commands:

    Get-TransportRule BT- -ErrorAction SilentlyContinue | select @{Name='Identity'; Expression={'Rule: '+$_.Identity }}*

    Get-InboundConnector BT- -ErrorAction SilentlyContinue | select @{Name='Identity'; Expression={'Inbound: '+$_.Identity }}*

    Get-OutboundConnector BT- -ErrorAction SilentlyContinue |select @{Name='Identity'; Expression={'Outbound: '+$_.Identity }}*

    Get-DistributionGroup BT- -ErrorAction SilentlyContinue | select @{Name='Identity'; Expression={'Group: '+$_.Identity }}*
4. Repeat these steps for each tenant.

How are Transport Rules & Send Connectors used?

Exchange Online transport rules and send connectors are the way in which mail is routed from an Microsoft 365 tenant to On Demand Migration Domain Rewrite Service. Transport Rules examine a message to determine if it should be rewritten and the connectors route the message to On Demand Migration Domain Rewrite Service. This ensures that only messages that need to be rewritten are routed to Domain Rewrite and messages that do not are immediately sent to the recipients.

There are 3 categories of transport rules. The following section outlines each category and describes the naming convention used for the rules.

Sorting Rules

For outbound messages, a sorting rule examines each recipient on an SMTP message and adds an SMTP header to identify if the recipient is internal or external.

- `BT-IntegrationPro-Out-S-Internet` – rule for external recipients.
- `BT-IntegrationPro-Out-S-[Guid]-[#]` – rules for internal recipients in target tenant [Guid] where [#] indicates a block of SMTP domains. E.g. BT-IntegrationPro-Out-S-15d82781-e5e8-4691-a77f-0f5fb10b6482-1

From, To, CC Rules

For outbound messages, these rules determine if any of the From, To or CC addresses on an SMTP message include an internal or external recipient that should be rewritten and updates the SMTP header added above appropriately.

- `BT-IntegrationPro-Out-[From/ToCc]` – rules for external recipients.
- `BT-IntegrationPro-Out-[Guid]-[From/ToCc]` – rules for internal recipients in target tenant [Guid]. E.g. BT-IntegrationPro-Out-15d82781-e5e8-4691-a77f-0f5fb10b6482-From.

Inbound Rules

The outbound rules ensure that Microsoft 365 routes only the messages that need to be rewritten to On Demand Migration Domain Rewrite Service. The inbound rules have two functions.

- `BT-IntegrationPro-In` - rule for messages returning from On Demand Migration Domain Rewrite Service.

  After a message is rewritten it is returned to the original tenant for delivery to external recipients.

  This rule removes the header added by the outbound rules so that a message is only processed by On Demand Migration Domain Rewrite Service once.

- `BT-IntegrationPro-In-DKIM` - rule for messages returning from On Demand Migration Domain Rewrite Service.

  When an external recipient replies to an ERS user, the message is rewritten back to the original domain. After which, the message is redirected to the original tenant.

  This rule removes the secret key added to the header by the sending tenant to ensure the message was securely delivered before and after being rewritten.

How are Connectors used?

Domain Rewrite adds an inbound and outbound connector to all Microsoft 365 tenants defined on a project. The purpose of these connectors is to ensure mail flow from an Microsoft 365 tenant to Domain Rewrite is encrypted with the assigned TLS/SSL certificate. This outbound connector contains the FQDN of the Domain Rewrite ERS Relay used to receive mail for the tenant. Some versions of ERS include connectors for each Client/Project combination.

- `BT-IntegrationPro-In` – inbound connector
- `BT-IntegrationPro-Out` – outbound connector

How are groups used?

When an Email Address Rewrite mode is selected for a user, the user is added to either the ERS Day One group (Rewrite with Target Address) or the ERS Day Two group (Rewrite with Source Address).

The ERS day One and day Two groups are cloud-only Exchange Online distribution groups. ERS Day One is used to control which (not migrated) source users should be presented to external recipients using their target address. ERS Day Two is used to control which (migrated) target users should be presented to external recipients with their source address. Some versions of ERS include groups for each Client/Project combination.

Administration Groups

Domain Rewrite automatically adds the following two (2) groups in the source tenant(s) of a project. These groups are managed by the administrator(s) of the tenant.

- `BT-IntegrationPro-[DayOne/DayTwo]` – day one or day two mailbox users. E.g. BT-IntegrationPro-DayOne.

Internal Groups

Domain Rewrite automatically adds several groups in the source and target tenant(s) for internal use. These groups should not be changed or deleted by administrators and are managed by Domain Rewrite.

- **Source Tenants** – Domain Rewrite adds the following groups in the **source tenant(s)** of a project.
    - `BT-IntegrationPro-[DayOne/DayTwo]-[Guid]` – target addresses (contacts) of day one or day two users in target tenant [Guid]. E.g. BT-IntegrationPro-DayOne-15d82781-e5e8-4691-a77f-0f5fb10b6482
- **Target Tenants** – Domain Rewrite creates the following groups in the **target tenant (s)** of a proj
    - `BT-IntegrationPro-[DayOne/DayTwo]` – source addresses (contacts) of day one or day two users from all source tenants. E.g. BT-IntegrationPro-DayOne.
    - `BT-IntegrationPro-[DayOne/DayTwo]-[Guid]` – source addresses (contacts) of day one or day two users from source tenant [Guid]. E.g. BT-IntegrationPro-DayOne-15d82781-e5e8-4691-a77f-0f5fb10b6482.
    - `BT-IntegrationPro-NC-[Guid]` – source addresses (contacts) of users from source tenant [Guid] that have not been cutover. E.g. BT-IntegrationPro-NC-15d82781-e5e8-4691-a77f-0f5fb10b6482.

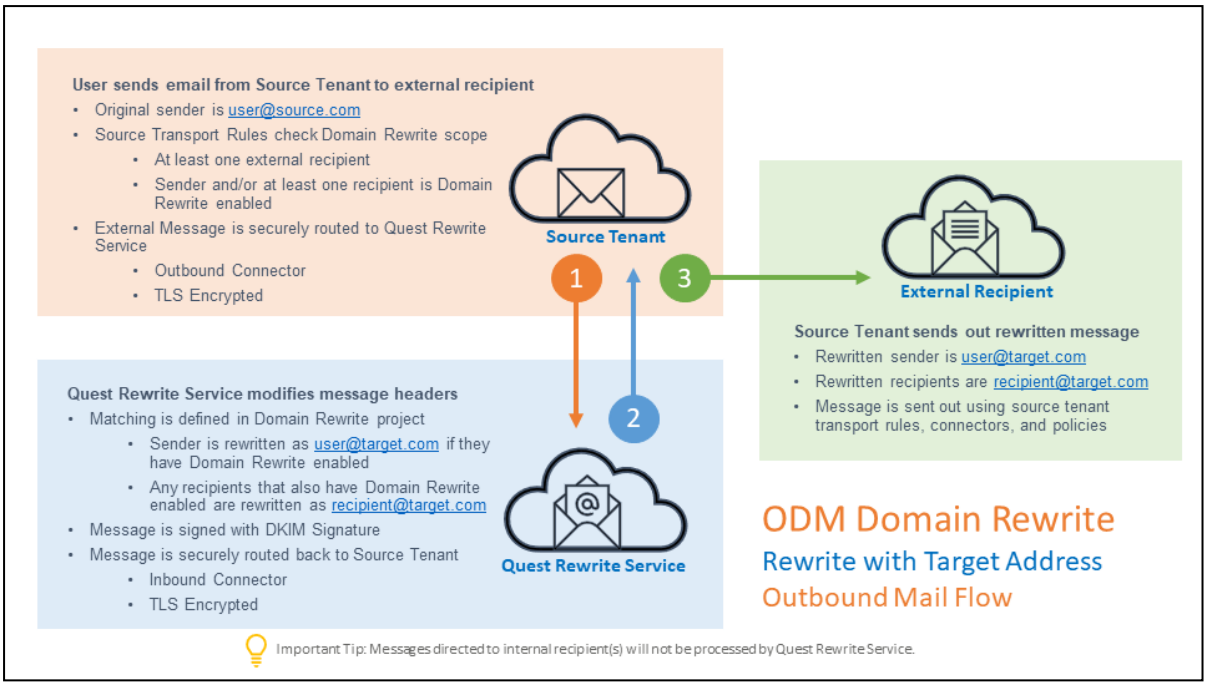
How does Mail Flow work with Domain Rewrite?

Important Tip: Microsoft 365 Advanced Threat Protection default settings may cause issues with Domain Rewrite for inbound messages. Please ensure that "Automatic forwarding" is set to "On" in the "Outbound spam filter policy" for your source or target tenant depending on the rewriting scenario you choose.

Rewrite with Target Address – Outbound Mail Flow

- When a user sends an email as user@source.com, the Transport Rules in the Source Tenant check whether the message is in scope for Domain Rewrite
    - At least one external recipient in “To” or “Cc”
    - Sender and/or at least one recipient in “To” or “Cc” is Domain Rewrite Enabled
- If the message is in scope for Domain Rewrite and there are multiple internal and external recipients, the message will be bifurcated and:
    - Copy of the message sent to external recipient will be securely redirected to the Quest Rewrite Service using the Outbound Connector in the Source Tenant.
    - Copy of the message sent to internal recipient is delivered by Exchange Online at the Source tenant with unchanged addresses.

    Important Tip: Messages directed to internal recipient(s) will not be processed by Quest Rewrite Service.
- When the Quest Rewrite Service receives the message from user@source.com, it processes it by rewriting @source.com to @target.com for every user that has Domain Rewrite enabled. The addresses in "From", "To", and "Cc" of the email message are rewritten for all external recipients.
- The Quest Rewrite Service signs the message and securely (via the certificate uploaded during project setup) redirects it back to the Source Tenant using the Inbound Connector.
- Exchange Online at the Source sends the message to external recipients as if it was sent by user@target.com, and all addresses of message recipients in "To" and "Cc" that have Domain Rewrite enabled appear as @target.com for external recipients

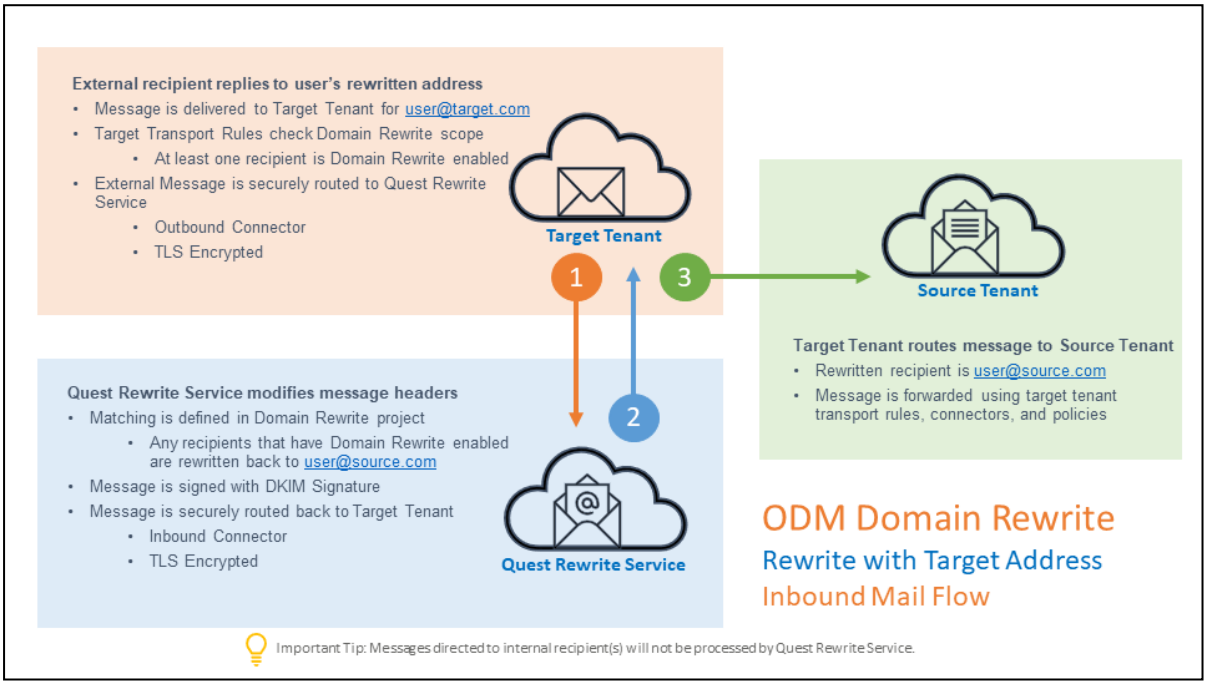


Rewrite with Target Address – Inbound Mail Flow

- External recipient is not aware about @source.com and replies (or create a new email) to user@target.com
- When the reply or a new mail arrives to the Target mail domain, the Transport Rules in the Target Tenant check whether any recipients in the “To” or “Cc” are in scope for Domain Rewrite
- If the message is in scope for Domain Rewrite, it is securely redirected to the Quest Rewrite Service using the Outbound Connector in the Target Tenant
- If the message is in scope for Domain Rewrite and there are multiple internal (recipients in the target tenant) and external recipients (recipients in the source tenant with Rewrite Service enabled), the message will be bifurcated and:
    - Copy of the message sent to external recipient (recipients in the source tenant with Rewrite Service enabled) will be securely redirected to the Quest Rewrite Service using the Outbound Connector in the Source Tenant.
    - Copy of the message sent to internal recipient is delivered by Exchange Online at the target tenant with unchanged addresses.

Important Tip: Messages directed to internal recipient(s) will not be processed by Quest Rewrite Service.

- When the Quest Rewrite Service receives the message addressed to user@target.com, it processes it by rewriting @target.com back to @source.com for every user that has Domain Rewrite enabled
- The Quest Rewrite Service signs the message and securely (via the certificate uploaded during project setup) redirects it back to the Target Tenant using the Inbound Connector
- Exchange Online at the Target forwards the message to the Source
- Source recipient gets the message as if it was addressed to user@source.com



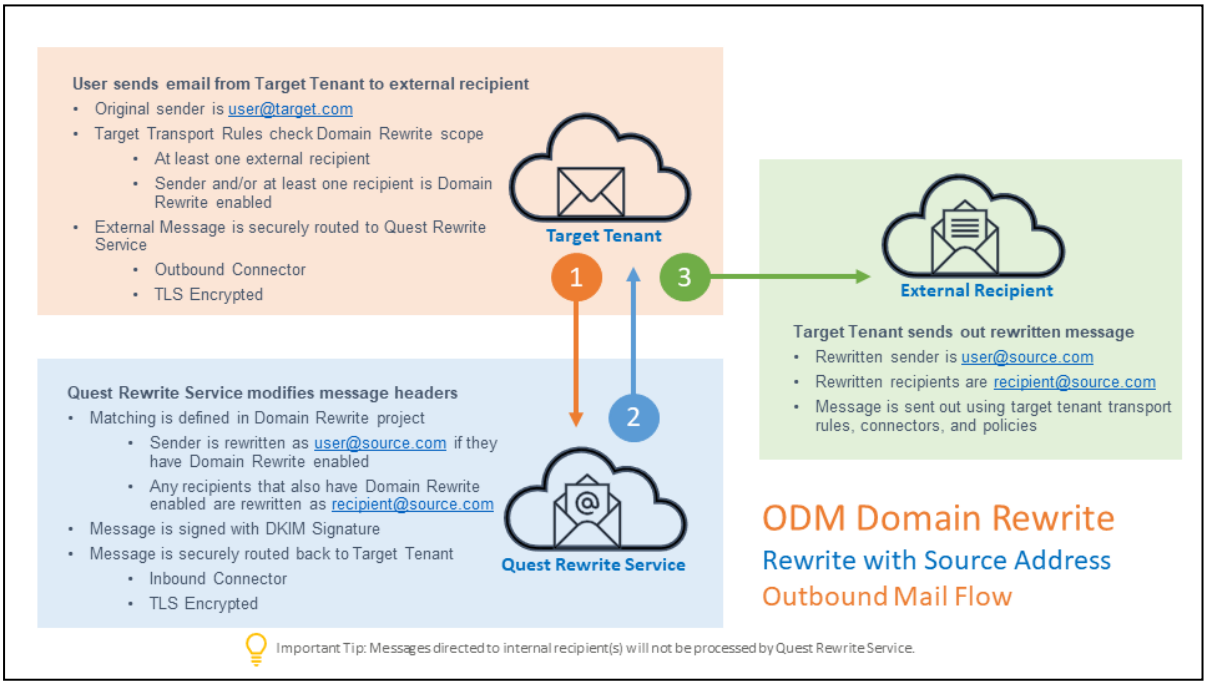
Rewrite with Source Address – Outbound Mail Flow

- When a user sends an email as user@target.com, the Transport Rules in the Target Tenant check whether the message is in scope for Domain Rewrite
- At least one external recipient in “To” or “Cc”
- Sender and/or at least one recipient in “To” or “Cc” is Domain Rewrite Enabled
- If the message is in scope for Domain Rewrite, it is securely redirected to the Quest Rewrite Service using the Outbound Connector in the Target Tenant

- If the message is in scope for Domain Rewrite and there are multiple internal (recipients in the target tenant) and external recipients, the message will be bifurcated and:
    - Copy of the message sent to external recipient will be securely redirected to the Quest Rewrite Service using the Outbound Connector in the Target Tenant.
    - Copy of the message sent to internal recipient is delivered by Exchange Online at the target tenant with unchanged addresses.

Important Tip: Messages directed to internal recipient(s) will not be processed by Quest Rewrite Service.

- When the Quest Rewrite Service receives the message from user@target.com, it processes it by rewriting @target.com to @source.com for every user that has Domain Rewrite enabled. The addresses in "From", "To", and "Cc" of the email message are rewritten for all external recipients
- The Quest Rewrite Service signs the message and securely (via the certificate uploaded during project setup) redirects it back to the Target Tenant using the Inbound Connector
- Exchange Online at the Target sends the message to external recipients as if it was sent by user@source.com, and all addresses of message recipients in "To" and "Cc" that have Domain Rewrite enabled appear as @source.com for external recipients

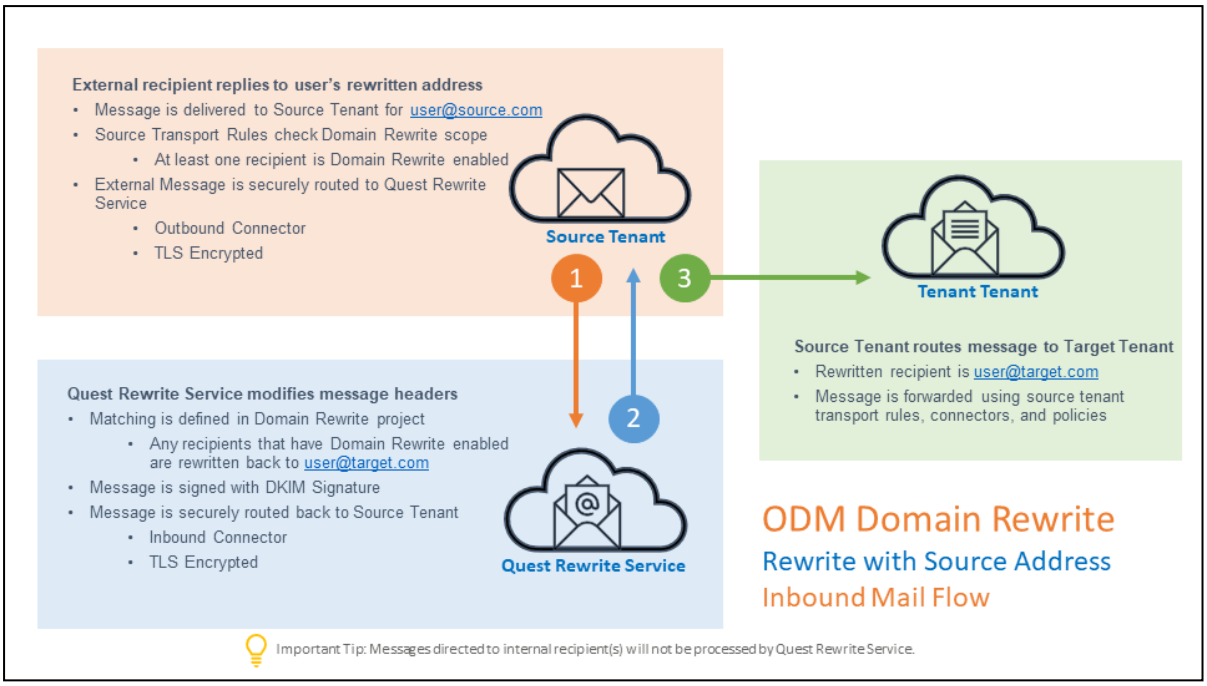


Rewrite with Source Address – Inbound Mail Flow

- External recipient is not aware about @target.com and replies (or create a new email) to user@source.com
- When the reply or a new mail arrives to the Source mail domain, the Transport Rules in the Source Tenant check whether any recipients in the “To” or “Cc” are in scope for Domain Rewrite
- If the message is in scope for Domain Rewrite, it is securely redirected to the Quest Rewrite Service using the Outbound Connector in the Source Tenant
- If the message is in scope for Domain Rewrite and there are multiple internal (recipients in the source tenant) and external recipients (recipients in the target tenant with Rewrite Service enabled), the message will be bifurcated and:
    - Copy of the message sent to external recipient (recipients in the target tenant with Rewrite Service enabled) will be securely redirected to the Quest Rewrite Service using the Outbound Connector in the Source Tenant.
    - Copy of the message sent to internal recipient is delivered by Exchange Online at the source tenant with unchanged addresses.

Important Tip: Messages directed to internal recipient(s) will not be processed by Quest Rewrite Service.

- When the Quest Rewrite Service receives the message addressed to user@source.com, it processes it by rewriting @source.com back to @target.com for every user that has Domain Rewrite enabled
- The Quest Rewrite Service signs the message and securely (via the certificate uploaded during project setup) redirects it back to the Source Tenant using the Inbound Connector
- Exchange Online at the Source forwards the message to the Target
- Target recipient gets the message as if it was addressed to user@target.com



When is it safe to remove Domain Rewrite ERS configurations?

You may disable Domain Rewrite when production services are no longer required. Upon disabling, the related configurations will automatically be removed.

DMARC

What is DMARC?

DMARC is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. Wikipedia

Is DMARC supported with Email Rewrite Services (ERS)?

Yes, DMARC is fully supported in all ERS mail flow scenarios. Either natively or through product supported methods.

ERS MAIL FLOW	DMARC
Mail Sent to External Recipients	Natively Supported
Mail Sent to Cross-Tenant Recipients	Natively Supported
Mail Received from External Recipients	Product Supported
Mail Received from Cross-Tenant Recipients	Natively Supported

Table 1: Supported DMARC Mail Flow Scenarios

What does product supported mean?

Product supported means that Domain Rewrite maintains domain authenticity, through internal methods to ensure the message received by the originating Microsoft 365 tenant was DMARC compliant before it is rewritten and redirected to the destination Microsoft 365 tenant.

In other words, Domain Rewrite ERS will verify and sign the rewritten email with a secret key so that when it is received by the destination Microsoft 365 tenant, transport rules may verify its authenticity then deliver to the intended user.

What does natively supported mean?

Natively supported means that DKIM domain alignment is achieved when an ERS rewritten email is sent or received. Therefore, DMARC will pass when received without interruption by the intended recipient domain.

What is required for DMARC to function with ERS?

DMARC is supported natively for all ERS users when sending mail outbound to an external domain recipient or across to a neighboring Microsoft 365 tenant. Simply choose the accepted domains in use during your project setup of the DKIM signatures. This will ensure the required domains are signed to achieve domain alignment and pass DMARC. The project wizard will guide you through the process.

Why are reply emails sent to the Junk folder?

When an ERS user receives a reply email from an external user, it is rewritten back to the original email address. This disrupts domain alignment and Exchange Online Protection by default will mark such emails as SPAM, delivering it to the end-user's junk email folder.

How do I prevent ERS reply emails from being marked as SPAM?

It's very easy to do. Simply setup a new action in one of the ERS transport rules. When ERS is deployed in each tenant environment, transport rules are created to manage to flow of mail for ERS users only.

This new action will allow ERS validated emails only to by-pass SPAM and deliver the message directly to the end-user's inbox.

How do I setup an action in my transport rule to prevent ERS reply mail going to Junk?

During this deployment, a rule named *"BT-IntegrationPro-In-DKIM"* is created and configured in each Microsoft 365 tenant in scope for Email Rewrite Services.

Follow these steps to setup a new action in the ERS Transport Rule using the Exchange Admin Center.

1. Login into Exchange Admin Center with your Exchange Online Administrator or higher role account.
2. Navigate to Mail Flow, Rules.
3. Locate the rule named, *BT-IntegrationPro-In-DKIM*.
4. Click *Edit*.
5. Click *Add Action*.
6. From the *Do the following…* field select, Modify the Message Properties.
7. Select *set the spam confidence level (SCL)*.
8. Select the *specify SCL to be Bypass spam filtering*.
9. Select *OK*.
10. Select *Save*.

PowerShell may also be used to modify the rule. Here is an example.

```
Set-TransportRule "BT-IntegrationPro-In-Dkim" -SetSCL –1
```

See the Set-TransportRule for more information.

May I set additional actions to the rule such as add a disclaimer or append the subject?

Yes, additional actions are supported on this rule. For example, it may be desired that a disclaimer be added to these ERS emails informing the recipient they are safe and were rewritten by our authorized service provider. Another common example is to prepend to the subject line that this is an ERS email. This provides additional awareness to the end-user users receiving and sending these types of email.

If additional actions are added to this rule, please validate the changes do not impact any functionality. And do not modify the rule order or add rules that reorder the ERS rules.

If this rule is deleted will it be recreated automatically?

Yes, Domain Rewrite health monitoring will recreate any rules that it created for ERS. If ERS is disabled in your project, all rules will automatically be removed from all tenant environments.

Will the rule be recreated with my additional actions?

No, any additional actions you may have added to the rule must be added again to the newly created rule.

How do I make a back-up of my rules with my custom actions?

You may easily use Exchange Online PowerShell to export your rules to a CSV file as a back-up. For example, here is a script that will export all rules created by Domain Rewrite during the ERS deployment.

```
Get-TransportRule BT-Integration* | export-csv C:\Users\%USERNAME%\Downloads\BT-Integration_TransportRules.csv
```

Domain Move

This user guide covers the steps required to configure and perform a Domain Move. The Domain Move Quick Start Guide summarizes these steps and addresses some frequently asked questions.

Platform Requirements

Supported Environment Deployments

Domain move between two Microsoft 365 tenants cloud-only or hybrid tenants is supported.

Exchange Hybrid Deployments

Domain Move currently provides limited support for Exchange hybrid deployments. Environments with an Exchange Server 2013 (or later) hybrid deployment are supported, but with the following limits on functionality:

- Mail flow configurations that use the on-premises Exchange environment or third-party messaging systems for inbound and outbound message delivery may require additional customization of transport rules and third-party configurations.

Application Service Account Requirements

To set up a Domain Move project the following must be provided by the owner of each of the associated Microsoft 365 tenants.

1. **Application Account:** One (1) dedicated and licensed application service account to grant permissions and automatically orchestrate various activities within the project. This account must have the Exchange Online plan assigned to facilitate automatic email communications to end-users and project administrators during cutover activities, otherwise all communications will appear to be sent from the PowerShell account.
2. **Roles:** The Global Administrator role is required for connecting environments for projects and workflows to grant permissions and to create a PowerShell account within each configured tenant.
3. **Licenses:** At least one (1) E1 or above license must be available to be assigned to the PowerShell account for Migration/Integration Projects.

What are the minimum administrator roles required to manage a project?

At a minimum, after project set up the following Microsoft 365 Role is required to automatically manage various aspects of your project.

1. Global Administrator Role

Important Tip: For the best application experience, it is always recommended to use the Global Administrator role. However, it is only required during the initial Project setup, reconnections to the tenant or during a Domain Cutover event, where more authority is required. All account and role management are strictly the responsibility of the tenant administrators.

Modern Authentication Requirements

Domain Move projects take advantage of Modern Authentication to help manage your projects. Modern Authentication is the default behavior for all Microsoft 365 tenants. Unless it was disabled, no action is required. However, we recommend the following configuration parameter is validated prior to deployment.

```
Get-OrganizationConfig | Format-Table Name,OAuth* -Auto
```

If Modern Authentication is disabled it must be enabled prior to any migration activities can proceed. To enable Modern Authentication for Exchange Online, run this command under the correct authority.

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true
```

Here is some additional information about how to Enable modern authentication in Exchange Online.

PowerShell

The following accounts are required:

- *Account:* One Cloud-only account will automatically be created during project setup.
- *Microsoft 365 Administrator Roles:* Automatically assigned the Exchange and SharePoint Administrator roles.
- *Microsoft 365 License Requirements:* Automatically assigned one available license (E1 minimum) for destination tenants.
- The accounts must be excluded from MFA requirements.

Important Note: This account will automatically be assigned the Global Administrator role at the start of a Domain Cutover event, where more authority is required to complete the process.

Domain Move Requirements

Source and Target Domain Pairing

During configuration, you will be asked to choose your source and target domains for each tenant. This process is called domain pairing.

Source & Target User Matching Attributes

- You will need to select a pair of attributes that will match exact values from the source user object to the target user object to discover and match the appropriate user accounts.
    - The available matching attributes are as follows, choose at least 1 with a maximum of 3:
        - *userPrincipalName*
        - *mail*
        - *extensionAttribute1-15*

Note: The *userPrincipalName* and mail attributes are matched based on the local part of the address and the paired Domains (e.g. *Tom.Dean@contoso.onmicrosoft.com* would use *Tom.Dean@binarytree.onmicrosoft.com* as a match against the target account.)

Multiple AD Forest Support

If your organization has multiple Active Directory Forests are connected to your Microsoft 365 tenants, this is supported scenario for migration and integration. There are no additional requirements to support this deployment type.

Directory Synchronization

Domain Move projects provide automatic orchestration of directory objects to provide capabilities to create and update directory objects during critical points within the migration or coexistence life cycle. To facilitate these activities the following is required for set up.

Local Agents for hybrid AD deployments

For complete details about local Agents, visit Directory Sync Requirements.

Source & Target Organization Units for hybrid AD deployments

Domain Move does not create Organizational Units. When deploying a Domain Move project that involves at least one (1) hybrid environment you must choose or create designated Organizational Units within your local AD Forest to allow new User or Contact objects be created.

Hybrid Tenant Support

The Active Directory forest attached to the Microsoft 365 Tenant must have the Microsoft Exchange 2010 SP3 (or later) schema extensions applied.

What is required to set up Directory Synchronization for Integration projects?

For **hybrid or mixed environments**, where your local Active Directory (AD) is being synchronized to Microsoft Entra ID the following is required.

1. At least one (1) Windows server to host the local Agent.
2. During set up, install at least one (1) local Agent in each AD Forest. Up to 5 agents are supported. One (1) agent per server.
3. Account credentials for one (1) AD account with permissions to create and update objects within the designated Organizational Units (OU).
4. Account credentials for one (1) Global Administrator within your Microsoft 365 tenant.
5. Designated OUs in each environment to create new objects.

For additional details about local Agents, visit Directory Sync Requirements.

For **cloud only environments**, where there is no local Active Directory the following is required.

1. Account credentials for one (1) Global Administrator within your Microsoft 365 tenant.

For more information about account permissions, click here.

Local Agents for hybrid AD deployments

For complete details about local Agents, visit Directory Sync Requirements.

Source & Target Organization Units for hybrid AD deployments

When deploying a Premium Integration project that involves at least one (1) hybrid environment you must choose or create designated Organizational Units within your local AD Forest to allow new User or Contact objects be created.

Hybrid Tenant Support

The Active Directory forest attached to the Microsoft 365 Tenant must have the Microsoft Exchange 2010 SP3 (or later) schema extensions applied.

Domain Sharing (Email Relay Services)

To deploy Email Relay Services (ERS) between tenants the following will need to be ready prior to the configuration of the service.

During initial project set up you may choose to configure ERS now, if you are ready or later after the initial discovery is complete.

ERS Deployment Checklist:

The following checklist provides a quick reference to the items or decisions required to begin configuration of ERS.

1. Procure one (1) SSL single domain certificate for each tenant environment using one (1) of the accepted domains.
2. The password associated with the SSL certificate will be required when uploading each certificate.
3. Choose which domains will particulate in ERS.

Important Tip:When using advanced Email Relay Service, please ensure the MTA-STS policy includes the Email Relay Server's MX record to avoid email disruption.

SSL Certificates

To successfully configure the Email Relay Service, a valid SSL certificate must be procured for all source and target tenants. The certificate must contain a single accepted domain, one (1) for each tenant. The selected certificate cannot contain subject alternative names (SAN). The common name (Subject Name) must match one (1) of the Exchange Online accepted domains configured within the tenant.

This certificate is utilized to secure the Exchange Online connectors over TLS that will be used to transfer message between the Email Relay service and each tenant. The new certificates will be uploaded to the project using a PFX formatted certificate. PFX files contain the public key file (SSL Certificate file) and the associated private key file (password).

The requirements for the certificate are as follows: (Names are for example purposes only.)

- Common Name: contoso.com
- Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider
- Bit length: 2048 or higher
- Must be valid for Server Authentication and Client Authentication.
- Must be signed by a trusted public root CA.
- Must contain a private key (password).
- Must not expire before the end of the project.
- Must have a Friendly Name defined.

Important Tip: The domain listed on the certificate cannot be moved as part of a Domain Cutover process. If you plan to move all accepted domains, you should plan to acquire a certificate for a newly created accepted domain to use as a placeholder. This domain will not be moved or used; it will be used only as the subject for the TLS certificate.

Domain Cutover

There are no additional requirements to set up Domain Cutover services, however it is recommended that the following related topics be reviewed prior to execution.

Important Tip: The domain listed on the SSL certificate cannot be moved as part of a Domain Cutover process. If you plan to move all accepted domains, you should plan to acquire a certificate for a newly created accepted domain to use as a placeholder. This domain will not be moved or used; it will be used only as the subject for the TLS certificate.

Setup

Projects

What is a Domain Move Project?

A project in Domain Move allows you to configure and manage a subset of features, services and capabilities related to specific environments and/or user groups.

How do I create a new Project?

To create a new project, follow these steps:

1. Click New Project to open the start of a project.
2. If a project option is not available, this means you do not have the required licenses.
3. Follow the wizard which will guide you through the setup process until it is complete.

Environments

All Domain Move Projects require at least 2 Microsoft 365 environments be added to your Domain Move Project to establish at least one source and one target environment for integration activities. Additional environments can be added for more complex migration scenarios.

What is an Environment?

A “tenant” or “environment” is this context is referring to an Microsoft 365 Worldwide subscription.

What should I prepare before adding a tenant?

Before creating your project, it is recommended that an Application Service Account be created in each of your Microsoft 365 environments. This account will be used for the duration of the project or services requirement.

This account will be used to grant delegated permissions to Domain Move on-behalf of the signed-in user. The administrator consents to the permissions that the app requests and the app has delegated permission to act as the signed-in user when making calls to Microsoft Graph. Some higher-privileged permissions require administrator consent. Domain Move requires Global Administrator consent for 4 Graph permissions anytime a tenant is added or reconnected.

Follow these recommended steps to prepare your accounts for project setup:

1. Create a cloud only Domain Move Application Service Account in each environment.
2. The recommended name of the account would be “Domain Move App Services”.
3. Set the account password expiration date to correspond with the project end date or set to “do not expire”.
4. Assign Global Administrator Role to the account.
5. Assign an Microsoft 365 License to the user. The minimal subscription should include Exchange Online.
6. Login to the account for the first time in Microsoft 365 to verify access.
7. Make the account information available to the authorized administrator for each client environment.

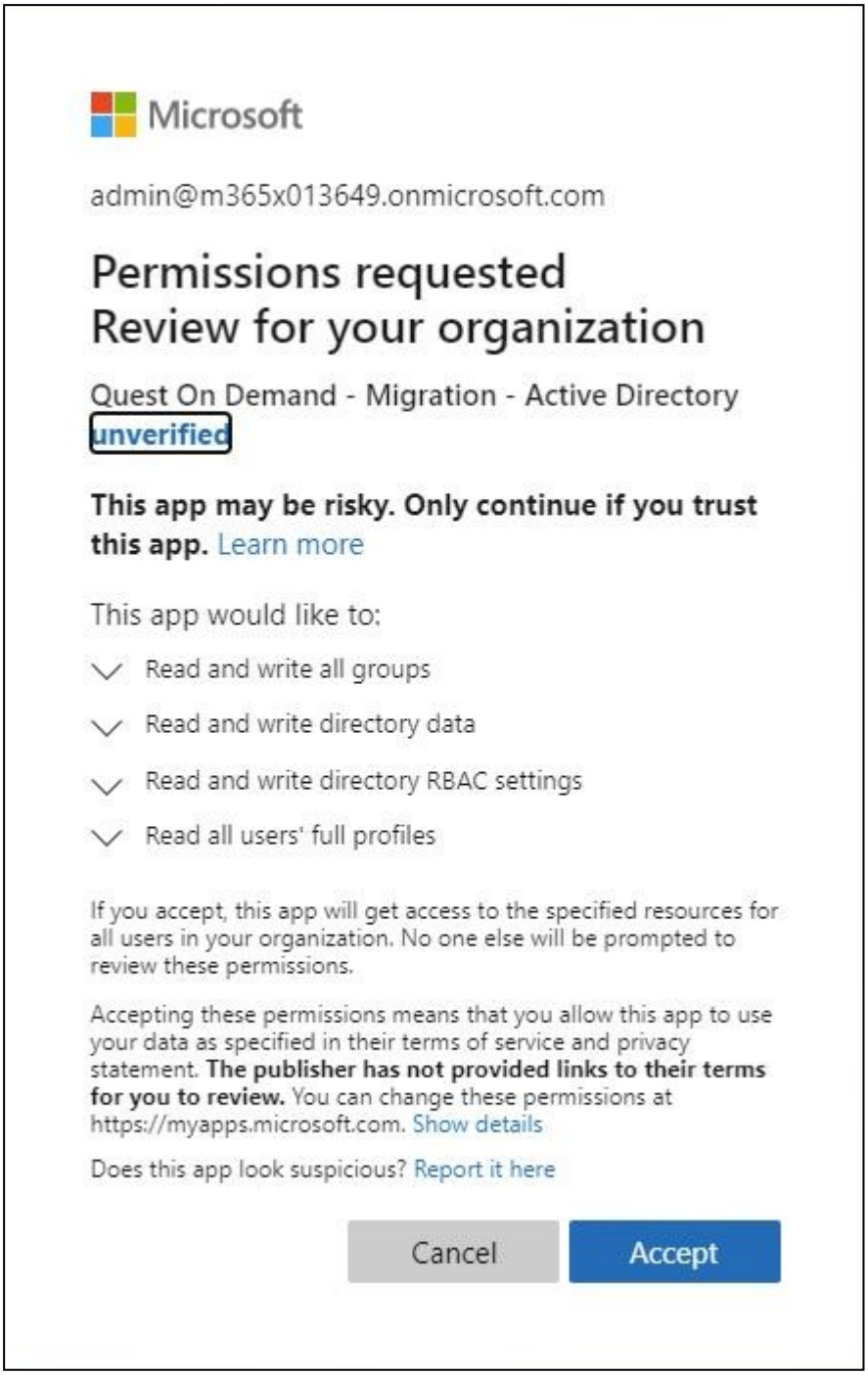
Please Note: It is acceptable to use an existing administrator account if that is preferred.

How do I add an environment to my project?

During the start of your project setup you will be asked to add your environments. Follow these steps to complete the process.

1. Click the New Project button or open your existing project.
2. Navigate through the setup wizard to the add an environment step.
3. Click the New button.
4. When you add a tenant, you will be prompted for your Microsoft account.
5. Enter the credentials of an administrative account for this Office365 tenant.

6. Read and accept the permission notice related to MS Graph permissions required to manage your projects. Note that two SharePoint Migration API permissions are included to allow OneDrive for Business Accelerated Velocity Mode migration to function.



(click to view larger)

7. You will then be returned to the Add Tenant screen. You will repeat this process for each tenant that is part of the project.

What happens when I add a Tenant to my Project for the first time?

When setting up your project for the first time, a Binary Tree PowerShell account will be created in each tenant added to the project and the Domain Move App will be installed. This account is used for PowerShell related tasks and to provide full access to the source and target mailboxes for migration purposes.

To complete this process, each tenant must have at least 1 available Microsoft 365 license, so it may be assigned to the account.

1. Domain Move will use your Application Service Account you created to connect to Microsoft 365. Credentials are never stored or transmitted between Domain Move and Microsoft 365.
2. Domain Move will add the Domain Move App to your Tenant. See figure 2 below.
3. Domain Move will create a cloud only account in your Microsoft 365 tenant for PowerShell.
4. Domain Move will license your new account with the available subscription that has the Exchange Online plan. A lower cost license will be used if available. For example, if you have both E3 and E1; E1 will be used if a license is available.
5. Domain Move by default will grant the Exchange and SharePoint Administrator Roles to this account.

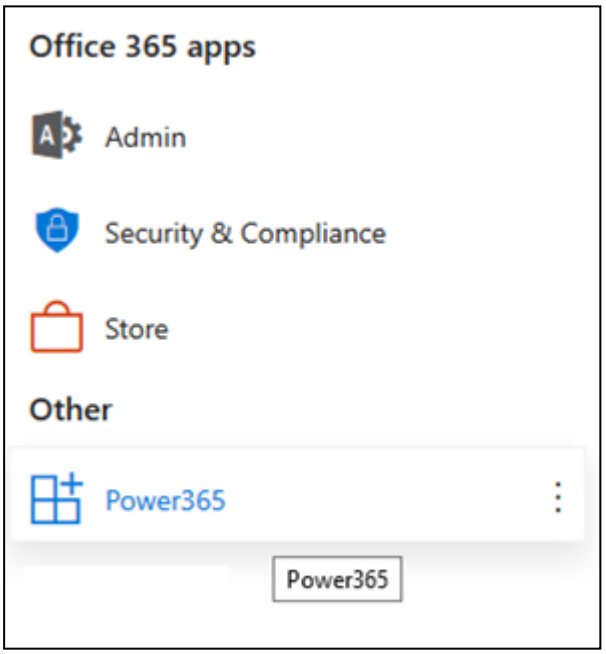


Figure 2: Example Domain Move App (click to view larger)

What permissions am I granting to Domain Move?

Here is the list of minimal Graph permissions required to operate a Domain Move project.

1. Read and write all users' full profile (User.ReadWrite.All)
2. Read and write all groups (Group.ReadWrite.All)
3. Read and write directory data (Directory.ReadWrite.All)

How are these permissions being used?

The following lists the basic need for each Graph permission.

1. Read and write all users' full profile (User.ReadWrite.All) - Used to read and move email addresses.
2. Read and write all groups (Group.ReadWrite.All) – Used to read and move email addresses.
3. Read and write directory data (Directory.ReadWrite.All) - Used to discover Azure directory and automate licensing.

Does Domain Move save my account password?

Domain Move will not ask you to save or transmit your administrator credentials in any cloud environment endpoint configuration.

What account roles are required to manage my project(s)?

For daily migration and integration operations and services, the minimum Microsoft 365 administrator roles required are:

1. Global Administrator

What account roles are required to add or reconnect a tenant to my project(s)?

Anytime a tenant is connected for the first time or reconnect later, the minimum Microsoft 365 administrator role required is:

1. Global Administrator

When should I reconnect my tenant?

There are a few reasons why you could be required to reconnect your Microsoft 365 tenant to your Domain Move project. The following lists the most common reasons this action is required.

1. *Office 365 OAuth Token has Expired* – After 90 days a standard OAuth token will expire. So, if your project is running longer than 3 months, please be sure to update your token by reconnecting your tenant to your project.
2. *Before a Domain Cutover Even*t – Before a domain cutover event, it is required that you raise your application account's role to Global Administrator to facilitate the domain move orchestration and automation.
3. *Application Account has Changed* – If the Application Account is deleted, recreated or changed it will be required that you reconnect your tenant to the project to continue services.

Pairing Environments, Domains, and Attributes

What is pairing?

Pairing in this context means to identify the source and target relationships in your project. There are three (3) pairing types in a project. Those are environment pairing, the accepted domain pairing and the object attribute pairing.

Why is pairing required?

Pairing environments, domains and objects are important because without designating the source and target locations, it will not be possible to migrate data, match objects, orchestrate mail flow or translate email addresses.

When do I setup my pairings?

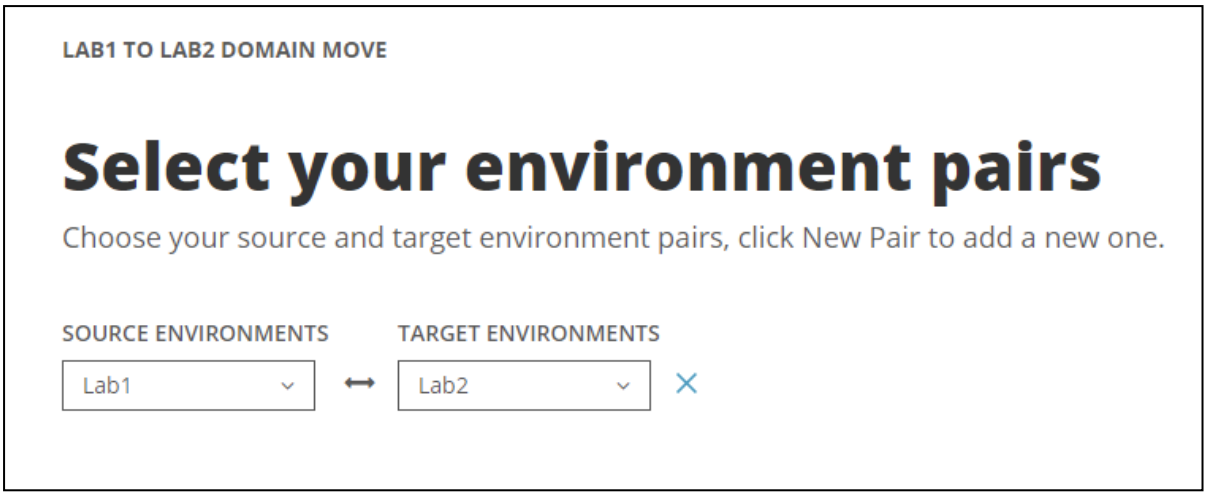
The project setup wizard will ask a few questions about the required pairings. And authorized administrators may update pairings when needed.

How do I setup environment pairings?

After adding your environments in the project setup wizard, it is time to set up your environment pairs. This is where you identify the source and target relationships in your project.

Domain Move will use this information as it guides you through configuring your project. You start with your environments, and then it's just a matter of "from" and "to." From what environment would you like to migrate accounts? And to where are they going?

With only two environments it might be just a simple one-to-one relationship. If you have multiple environments like in a divestiture, you may need to set up several environment pairings.



(click to view larger)

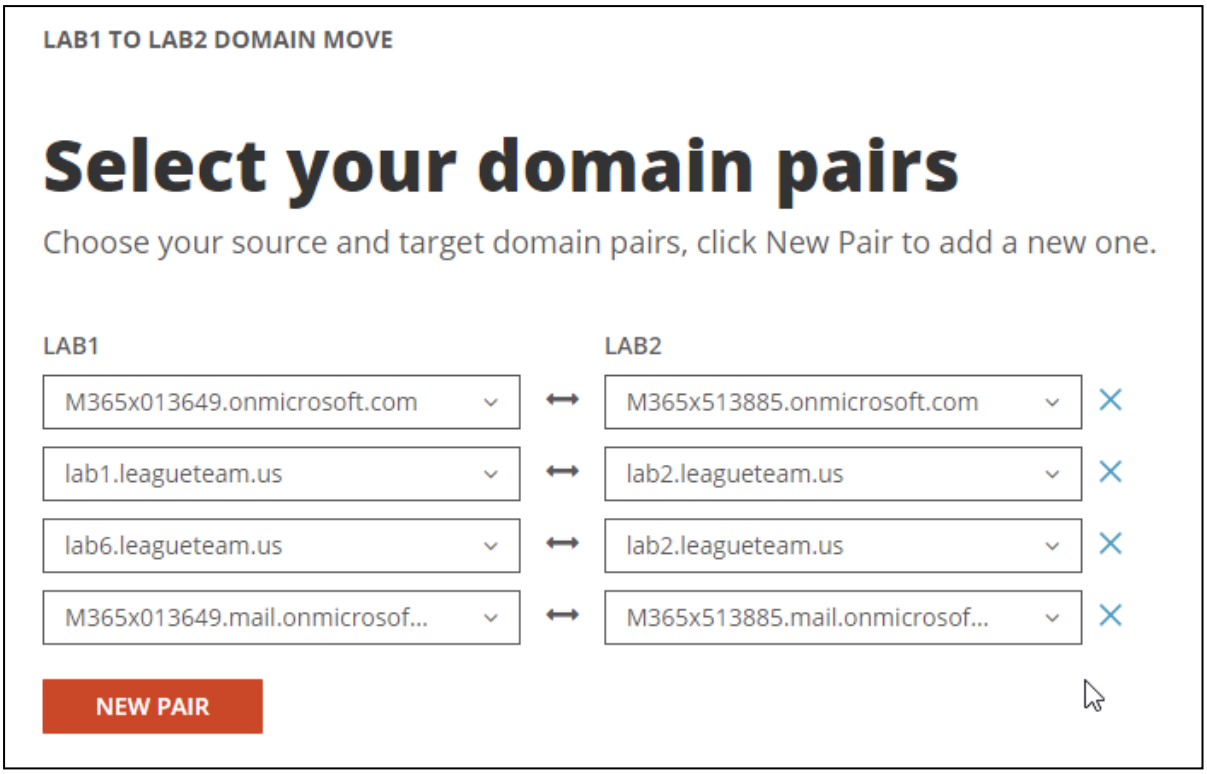
How do I setup domain pairings?

After setting up environment pairs, the next step is to pair the domains. Domain Pairing is setting up accepted domains from the source environment with accepted domains in the target.

When an account is setup in the target, the email address is automatically stamped with the paired domain in the target. The default domain might be a different domain altogether, so pairing makes sure you know what you will have in the target after migration.

Create one pairing at time. Choose an accepted domain from the source. And then a domain from the target. That's the basic pairing.

Create whatever combination of domain pairings meets your needs. You can do a simple one-to-one relationship, or pair several source domains to a single target domain.



(click to view larger)

How do I setup attribute pairings?

After setting up domain pairs, the next step is to pair the attributes for the purposes of matching objects between environments. Attribute Pairing is setting up value pairs from the source object and the target object.

Matching

What is matching?

Matching is a process in Domain Move that provides a method for objects between different directories to be paired together for migration and synchronization purposes.

Why is matching required?

Matching is required because it provides a mapping between source and target objects for the purposes of group membership synchronization and email address translation during migration.

What is matched?

All Users and Groups are matched between a source environment and a target.

When does matching occur?

Matching automatically occurs during the discovery process and can be run manually at any time by an authorized project administrator.

How does matching work?

Domain Move will attempt to match users and groups in the source environment with users and groups in the target environment.

During project setup, you may choose up to 3 attribute pairs that Domain Move will use to make this object pairing determination.

Matching is processed in the order listed. If there is no match on the first attribute, Domain Move moves down the list.

With the Integration project type, if no match is found, Domain Move may create the users and groups for you.

What are the projects requirements for matching?

To complete the project setup and match objects, you will be required to setup pairs for Environments, Domains and Attributes for Users and Groups.

Can I run a match myself?

Yes, there is an action available called Match. This action will match an unmatched user or group against the target environment without the need to run a full discovery in source and target.

How do I run the match action?

It's easy, navigate to the users or group you would like to match. Select the item then select the Match action from the action drop-down menu. Once selected, click the Apply Action button to begin. The status of the object will change to Matching. When successfully complete, the status will change to Matched.

Are there matching logs?

Yes, within the discovery logs, matched objects will be logged. However, the easier method is to export all discovered users and groups. The export of all discovered objects will provide a list of all matched and unmatched

objects. Navigate to the user or group management view then select all the objects. Afterwards, select the Export action from the action drop-down menu.

Agents

What is the Directory Sync agent?

The Directory Sync agent is the key component that communicates between a local Active Directory environment and the Directory Sync service.

Where do you install the agent?

The agent must be installed in every forest that you plan to include as a Directory Sync environment. We suggest that you create a virtual machine exclusively for this purpose. Review the Directory Sync Requirements for the minimal hardware and software requirements.

How do I download and install the agent?

First, choose the environment that the agent will be associated with.

You will be able to download the latest version of the agent from the Directory Sync agent screen. Copy the URL and the access key that will be needed during the install of the agent. The downloadable executable is the same for all projects, it is the Registration URL and Registration Key that makes the agent unique when it is installed.

To install of the agent enter credentials that have read or read\write access to the domain, depending on the direction of synchronization.

Copy and paste the information from the Directory Sync agent screen.

No further action is needed on the workstation. A look at services confirms that the Directory Sync agent is running.

A list of agents appears on summary screen, including status information as well as the registration URL and access keys should you need them again in the future.

Where do I manage agents?

To manage agents, simply open the left navigation menu and click **Directory Integration**, located under **Setup**, see *figure 1*.

Figure 1: Domain Move Setup and Settings Menu

How do I manage the agents?

On the Agents page, you can check the current status of your current agents or add new ones. Select an agent for additional options. You have the option to copy the Registration URL or the Registration Key if you need to reinstall the agent for any reason. The History button will give you details on the run history. When the agent is updated, any agent using the old version will offer you the upgrade option so that you can update your current agent installation.

How many agents can be installed on a computer?

You may configure up to five separate agents on a single computer. When running the agent installer, you have the option of registering a new agent on the computer or if there are existing agents on the computer, you may select an existing agent to configure or remove it.

How do I uninstall an agent?

If you need to uninstall an agent from any machine, in order to reinstall on the same machine, you must first delete the registry folder located at HKEY_LOCAL_MACHINE> SOFTWARE> Quest > Agent and then uninstall.

Afterwards, simply create a new agent (with a new access key) under Agents managements from the left navigation menu before re-installing on the same machine.

Discovery

What is discovery?

The discovery service is used to collect user and group identity and properties for the purposes of Domain Cutover preparation.

What is discovered?

When discovery is complete, it will have collected all user, group, and contact information within the configured Azure directory environments. It will use this data based on project configuration to find matching objects between environments for the purposes of synchronization.

When does discovery occur?

The Domain Move Directory Discovery Service runs by default every twenty-four (24) hours. This frequency may be changed as needed.

Should I change the default discovery frequency?

After the initial discovery has successfully completed, subsequent discovery jobs will be deltas, which are quicker. Monitor the time it takes to run a delta sync. If the total discovery time exceeds 24 hrs., adjust the frequency to fit the environment size. The more directory objects, the more time a discovery will take. Be sure the initial discovery completed successfully. Otherwise, each new discovery job will run a full discovery again.

When can I run discovery?

The Domain Move Directory Discovery Service may be run at any time by an authorized project administrator.

Can I run a full discovery?

Yes, a full discovery may be run after the initial discovery has completed when required. However, it is recommended that delta discovery be allowed to run to ensure new and modified object changes are processed quickly.

How do I run full discovery?

1. Click the drop-down menu located in the top left corner.

2. Click the *Discovery* link from menu.
3. Hover over the desired tenant environment.
4. Click *RUN DISCOVERY* to begin the process.

When should I run a full discovery?

Full discovery should only be run when previously skipped objects are now required for the project.

Can I suspend discovery?

Yes, the Domain Move Directory Discovery Service can be disabled at any time by an authorized project administrator. Click DISABLE for the desired environment while in the discovery management page.

How do I suspend discovery?

To manually disable all future discoveries, follow these steps.

1. Click the drop-down menu located in the top left corner.

2. Click the *Discovery* link from menu.
3. Hover over the desired environment.
4. Click *DISABLE* to stop all future the processes.

When should I disable discovery?

In most cases, discovery services should not be disabled during an active project. Inactive projects can either be archived if they are no longer required, which will end all related services, or the discovery service can be disabled until the project becomes active.

It is recommended that discovery services be disabled before a Domain Cutover event is started. For more information about Domain Cutovers, review this help article.

Is there a discovery log?

Yes, Domain Move provides authorized administrators access to the discovery and tenant logs. To download the logs, simply navigate to the DISCOVERY section from your project dashboard then click the LOGS link for the desired environment.

Domain Cutover

What is a Domain Cutover?

The Domain Move project type includes the “Domain Cutover” or move functionality. After a tenant mailbox and group migration, the next step during a domain consolidation or divestiture project will be to move your registered Microsoft 365 Domain (i.e. Exchange Online Accepted Domain) from one Microsoft Microsoft 365 tenant to another.

Moving a domain from one Microsoft 365 tenant to another is a tedious, multi-step, manually intensive procedure that must be carefully planned and executed at the proper time to ensure a seamless user transition. One of the biggest obstacles during this process is email sent to the domain in transit is not deliverable because it is held until the Domain move is complete. This can cause delays, lost messages and productivity.

The On Demand Migration Domain Cutover is the solution. This powerful feature guides the migration operator through the domain move process, and streamlines many of the steps. It works in conjunction with the Email Relay Service (ERS) to maintain deliverability throughout the move. Mail is never held but delivered on-time, ensuring your users never miss that business-critical message.

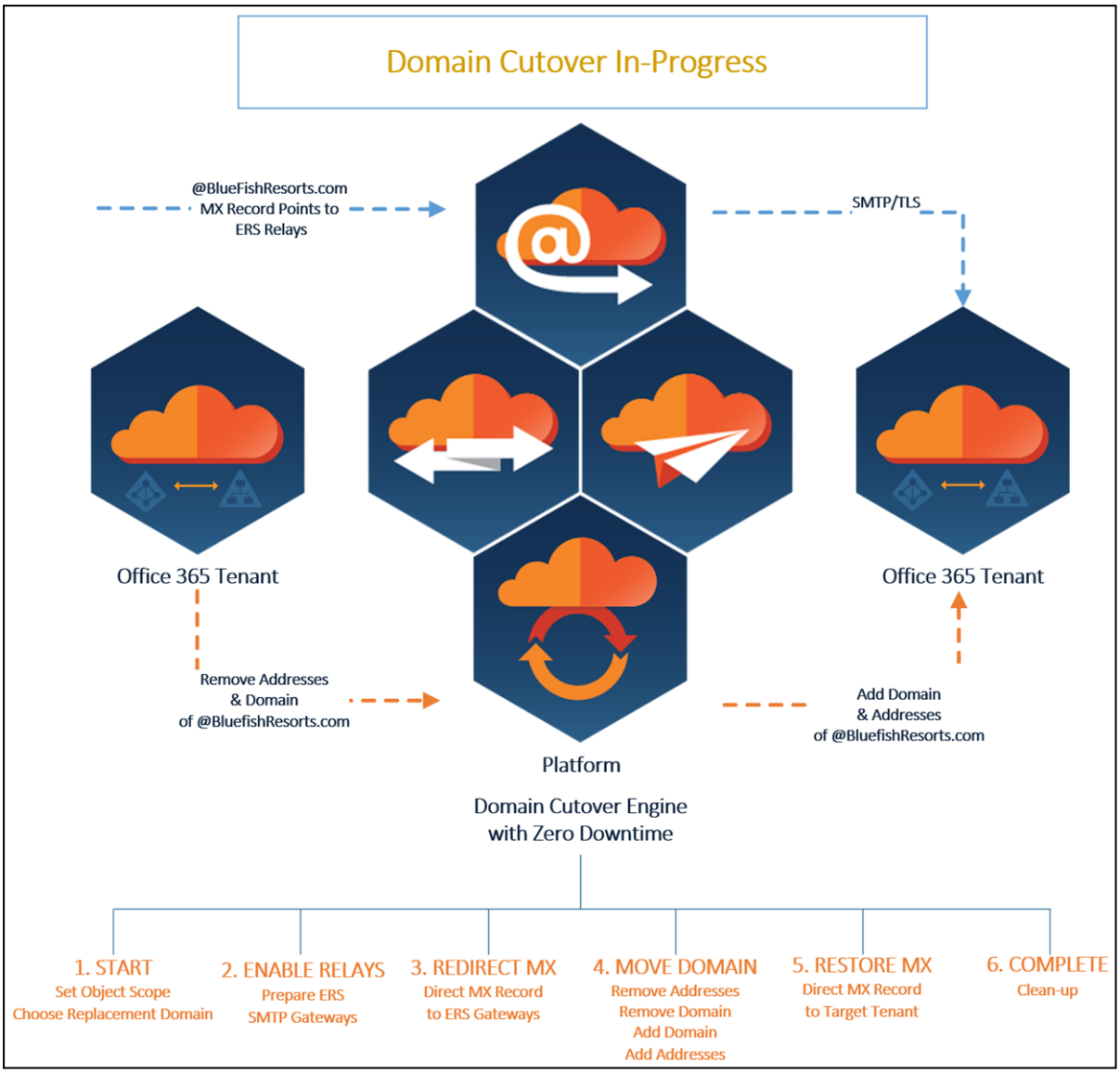


Figure 1: Domain Cutover In-Progress

How does Domain Cutover Work?

The Domain Cutover feature is designed to fulfill three major needs when moving an Accepted Domain from one tenant to another. Those are, moving user's addresses, moving the domain and most importantly, ensure continuity of mail routing during the domain transition.

The Domain Cutover wizard will follow these 6 primary stages. Read through each one before continuing. They provide important details to the process that will help with planning and preparation.

1. Start

During the start of this process Domain Move will validate groups and request some input before beginning.

a. Domain Move will warn that any Mailbox or Group not migrated cannot be migrated after the Domain Cutover begins. *Note the option to refresh changed Mailboxes and Groups and migrate them again after Domain Cutover is finished is available.*

b. Choose Replacement Source Domain – When removing a primary address from a source user, it must be replaced with a new domain. Choose the domain to replace the domain being moved. This may impact the user's UPN, Mail and Proxyaddresses attributes. *Note this will remove the source domain name configured for cutover from the source environment.*

c. Choose Target Address Assignment Scope of Users to be Updated – When moving Domains, select how the target address is assigned. This only impacts the target environment. User Logins (userPrincipalName) are not modified in the target user.

i. As Primary Email Address - Domain will be added as the primary email address and will replace the existing primary email address for matched objects.

ii. As Secondary Email Address Only - Domain will be added as a secondary email address for matched objects.

iii. Do Not Update – Domain will not be added for matched objects.

2. Enable Relay

During Step 2, if you have chosen to used the On Demand Migration Email Relay Service, the Email Relay Service (ERS) Relay servers will brought online to service the Domain being cutover to the target tenant. This step can take up to 60 minutes before the relays are activated. Don't worry, Domain Move will keep you up to date. Once this step is complete you will be able to move onto Step 3.

3. Redirect MX

During Step 3, the DNS administrator of the Domain being moved will execute an update to their public DNS MX record to direct traffic to the ERS Relay Servers. It can take up to 2 hours before an MX record change is propagated globally. Be sure to keep your TTL low during the transition.

After this step is complete, all inbound mail from the Internet for the domain being moved will be routed to the Domain Move ERS relays that were setup during step 2. Mail will be delivered to the target user's mailbox until step 5 is complete.

The Project Administrator may elect to skip redirection to the ERS relays but instead choose to queue mail using their own systems. This is also acceptable. Domain Move will continue with the remainder of the Domain Cutover process. Quest is not responsible for any mail flow if by-passing ERS is elected.

Important Note to Administrators: If you are using a 3rd party email provider or relay system to receive all Internet mail before directing traffic to the Domain Move, it is recommended that you contact Support with a list of IPs to have them whitelisted during the Domain Cutover process to avoid any mail delivery delays.

4. Move Domain

During Step 4, Domain Move will do most of the heavy lifting. This step is the most complicated, lengthy and error prone depending on the size and complexity of the environment. The following actions will take place during this step. User status will begin to update during this step. The Domain Move Project administrator will also receive notifications if the Domain Cutover fails during these activities and when it complete.

a. Read email addresses in source AD and tenant
b. Remove email alias addresses (*Proxyaddresses*) from the source AD and tenant
c. Replace Primary address from the source AD and tenant
d. Replace User Login (*userPrincipalName*) from the source AD and tenant
e. Remove domain from source tenant
f. Add domain to target tenant
g. Administrator must verify domain in target (This is a manual step executed by the Tenant Administrator within the Microsoft 365 Admin Portal or using the Powershell *Confirm-MsolDomain* cmdlet.)
h. Add email addresses in target (The target UPN is not modified)

5. Restore MX

During Step 5, the DNS administrator of the Domain being moved will execute an update to their public DNS MX record to direct traffic to the Exchange Online Protection (EOP) (e.g. *contoso-com.mail.protection.outlook.como*) or another relay service.

After this step is complete, all inbound mail from the Internet for the domain being moved will be routed to the new destination tenant. Domain Move ERS relays will no longer be used.

6. Complete

During this final step of the Domain Move Domain Cutover please allow up to 48 hours for the Cutover Domain wizard to deprovision the ERS engine and cleanup this domain move; this is to ensure that any outstanding mail items are delivered before the service is shut down. During this time, you may be prevented from making certain changes to this Domain Move project.

If all Domains have been cutover and ERS is no longer required it is recommended that it be disabled in the Domain Move Project. Once ERS is disabled, the associated Transport Rules, Groups and Connectors will be removed in the configured Microsoft 365 tenants. The same is true for the Calendar Sharing configured between the tenants using Domain Move. If this feature is disabled in the Domain Move Project, the associated Organization Relationships setup in each tenant will be removed automatically.

What to plan for using Domain Cutover

As each production environment has different operations, standards and policies, be sure to carefully plan your environment's domain cutover process. While this wizard will assist with specific portions of the domain cutover process, there may be additional reconfiguration necessary to support a successful domain cutover.

Updating the Source Environment

During the 4th step of the Domain Cutover process, the source objects (users, groups, contacts) both local and in the cloud, will have their proxyaddresses and UserPrincipalName (users only) updated to replace the Domain being cutover. Therefore, be sure to plan your local Mailbox migrations beforehand and Unified Groups (Office 365 Groups) and Microsoft Teams must be manually remediated to remove the proxy address or the group must be deleted before proceeding.

Updating the Target Environment

Once the domain has been moved to destination Microsoft 365 tenant during step 4, the wizard will re-assign their addresses (userPrincipalName is not updated, logins remain unchanged) to users and groups that have been matched by Domain Move. However, the wizard will not update the following objects in the target environment:

- Users not Prepared by Domain Move
- Distribution Groups not Migrated by Domain Move
- Mail-Enabled Public Folders
- Mail-Enabled Contacts

Please ensure that these object types are remediated with the proper address after the Domain Cutover is complete.

Other Considerations during a Domain Cutover

- Only one domain can be cutover at a time using Domain Move.
- Disable the scheduled Discovery jobs in all environments before starting the Domain Cutover.
- All Users and Groups in Domain Move must be migrated before Domain Cutover. If not, they cannot be migrated after the Domain Cutover is complete.
- Any user or group in the source that contains a proxyaddress of the Domain being Cutover will have their status updated in Domain Move. Their proxyaddresses will be removed in the source to remove the Domain later. These users will not be able to be migrated afterwards.
- Plan to move or remediate Office 365 Groups (Unified Groups) and Microsoft Teams before the Domain Cutover. Either remove the address associated with the Domain Cutover or delete the group or team.
- Plan to manually reassign primary or alias addresses to Mail contacts, Public Folders or unmatched users and groups in the Target environment.

- Plan to migrate local Exchange Mailboxes before the Domain Cutover.
- Plan to setup the local AD Domains before the Domain Cutover if UPN reassignment is required in the Target environment.
- Plan to move other configurations related to the domain being cutover such as Exchange Policies, Transport Rules, Connectors, EOP Rules, GPOs, etc.
- Remove all Skype for Business licenses from the users in the Source tenant using the Skype for Business Admin Portal. This will remove the Skype for Business SIP address connected to the domain.
- Update your SharePoint Online website address 24 hours before your Domain Cutover.
- You cannot remove a domain that has subdomains. You must first delete the subdomains before you can remove the parent domain.
- The Microsoft Online routing domain that's issued by Microsoft 365 (for example, contoso.onmicrosoft.com) cannot be moved or deleted.
- If using a 3rd party email relay system to receive all Internet mail before directing traffic to the Domain Move mail gateways, it is recommended that you contact Support with a list of IPs to have them whitelisted during the Domain Cutover process to avoid any mail delivery delays.

Domain Cutover Logging

- Domain Cutover Logs – At various stages of the Domain Cutover Wizard the Domain Cutover Logs download link will be presented. Click this link to open the current logs. These logs pertain to the activities being driven by the Domain Move engine.
- User Move Logs – During the Domain Cutover the User status will be updated. Double click a user to display their activity logs. Click on the Move log to review the history of the user's Domain Cutover process.
- Directory Sync Lite Logs – When the Domain Move engine has a job that needs to be executed on the local Active Directory, it gives this job to Directory Sync Lite. Launch the Directory Sync Lite Console then click the View Logs button to review the actions taken locally.

User Status Types during a Domain Cutover

- Moving – During Step 4 the user's status will update to the Move state.
- Moved – When Step 4 is complete for the user, their status will change to the Moved state.
- Move Error – During Step 4 if at any time a local user or group cannot be remediated, an error will be logged. Open the user Move log to determine why. Remediate the problem and rerun Step 4.

What account roles are required for Domain Cutover?

There are two accounts used during the domain cutover process. Each require the Global Administrator role to facilitate the process on your behalf.

- Application Service Account – Global Administrator Role
- Binary Tree PowerShell Account – Global Administrator Role

If I lowered my application account roles to the minimum, should I raise them before the domain cutover?

If you have your application account roles are set to the minimum requirements, then assign the Global Administrator role before beginning the domain cutover. Otherwise it will fail, and you will be required to restart the process.

Is my organization required to modify our MX records?

Domain Move does not require you utilize our Email Relay Services to route inbound mail to the target mailbox during the Domain Cutover event. The Project Administrator may elect to skip redirection to the ERS relays but instead choose to queue mail using their own systems. This is also acceptable. Domain Move will continue with the remainder of the Domain Cutover process. Quest is not responsible for any mail flow if by-passing ERS is elected. The Domain Cutover process will still provision the mail relays for your project, this can take as much as 60 minutes to complete. You will not be able to continue to the next step until this process is complete, please plan accordingly.

Are 3rd party email service providers such as Proofpoint or Mimecast supported during a Domain Cutover?

If you choose to have all inbound Internet mail for your domains to be directed to a 3rd party email relay prior to directing the traffic to the Domain Move Email Gateways as recommended, you may experience rate controls being applied, causing email delivery delays.

To avoid this situation, bypass your 3rd party provider during the domain cutover event or contact Support with a list of IPs and dates to have the system whitelisted.

Additional Information on Domain Migrations

- Common Errors when trying to remove a domain from Microsoft 365
- How to migrate mailboxes from one Microsoft 365 tenant to another
- Confirm-MsolDomain

Settings

Directory Integration

What is Directory Integration?

Directory Integration refers to the Directory Sync components that are automatically deployed and configured when you set up a Premium Integration project.

Where do I manage Directory Integration?

Directory Integration will display under **Settings** when a Domain Move project is created. To manage the Directory Sync components of your project, click **Directory Integration** from the left navigation menu, see figure 1.

Figure 1: Settings Menu for Domain Move Project

What can be managed from Directory Integration?

After project configuration, You may use the Directory Integration tab to check on the status of their workflows and local agents, download history logs and manage the Organizational Units (OU) for creating new objects during Prepare and Cutover activities.

How do I create a new agent?

From Directory Integration management, see *figure 2*, click the **New** button to begin creating a new agent for your existing environments.

Are agents automatically upgraded when a new version is available?

Yes, if the Auto Upgrade feature is checked (see *figure 2*), then agents will automatically be upgraded when new versions are available.

Certificates

What are certificates?

Certificates will display, under **Settings** within the Domain Move project. Certificates are used to ensure secure message transit with TLS.

Figure 1: Settings Menu for Domain Move Project

What is required to ensure mail delivery during Domain Move?

For full details about TLS certificate requirements see the SSL requirements.

Where can I verify the status of my certificates?

Existing certificates can be viewed by selecting **Certificates** from the left navigation menu, see *figure 1*. The Mail Relay Service page will open,*figure 2*.

Figure 2: Mail Relay Service

Where do I manage certificates?

Certificates are managed within your project. They are uploaded during project setup and can be removed or newly uploaded by editing your project. Follow these steps to add a new certificate or remove an existing certificate from your project setup.

1. Open the desired project.
2. From the project dashboard click **Setup**.
3. From the project summary, click **Security**.
4. The project certificate page will open.

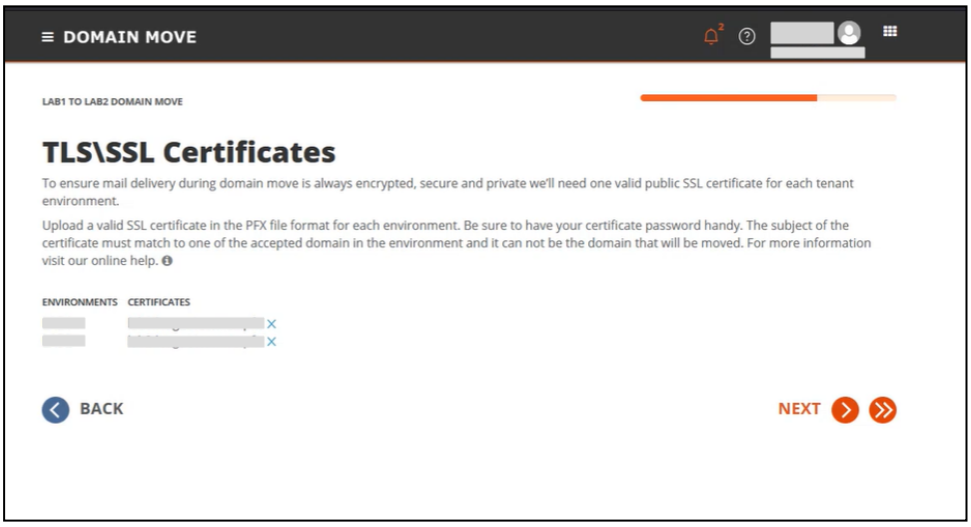


Figure 5: Project Wizard Certificate Management

5. If a certificate has expired and you need to upload a new version, then simply click the **X** to remove the existing certificate.
6. After removing the old certificate, click **Upload** to provide a valid certificate. Be sure it meets requirements. It must be in the PFX format with a valid password.
7. After uploading the new certificate, click **Next** to navigate to project summary.
8. Click **Next** again.
9. Now click **Skip Discovery** to return to the project dashboard.

Email Relay Service

What is the Email Relay Service?

One of the biggest obstacles during this process is that email sent to the domain in transit is not deliverable because it is held until the Domain move is complete. This can cause delays, rejected messages, and productivity. On Demand Migration for Active Directory addresses these concerns with its robust Email Relay Service which provides the administrator options on how email should be delivered. Migration Administrators can choose Either Basic Mode or Advanced Mode s based on their project requirements.

Microsoft has enabled “MTA-STS for Exchange Online” security feature in Exchange Online, and will refuse deliver messages to servers that don’t support TLS and have a trusted certificate. Customer will need to update their MTA-STS policy and add the Email Relay Server’s MX records to the policy. Below is a sample of the policy, additional detail for MTA-STS implementation in Exchange Online, please refer to Introducing MTA-STS for Exchange Online - Microsoft Tech Community link.

When Should Basic Mode be used?

Choose this mode if you would like to queue your emails using your existing delivery service during the domain move process. Mail flow for your domain will be resumed after the domain move has completed.

Basic Mode is easy to setup and requires no configuration changes to the tenant. Tenant administrators have the option to hold the email message delivery while the domain is being moved or to send the email messages to their own relay service provider for final delivery. In this mode, the directory synchronization component of On Demand Migration for Active Directory will facilitate the move for email addresses and domain names between tenants but it will not be responsible for the mail flow.

Basic Mode is the best choice when:

- Only a handful of objects associated with the tenant and the domain move process will be done within a couple hours.
- Continuous email delivery during domain move is not a requirement, and messages can be queued for delivery after domain move is completed.
- Custom Transport rules and connectors are not allowed in Exchange Online for either source or target tenant.

When should Advanced Mode be used?

Choose this mode if you would like to have mail delivered to your users in the target tenant during the domain move process. Transport rules and connectors will be configured in the tenants when this mode is selected.

Advanced Mode offers the full coexistence experience for end-users that are affected by the domain move. It will relay incoming email messages sent to the source user mailboxes to their matching target user mailboxes. The benefit of choosing Advanced Mode is there is no email disruption while the domain is being moved.

Advanced Mode is the best choice when:

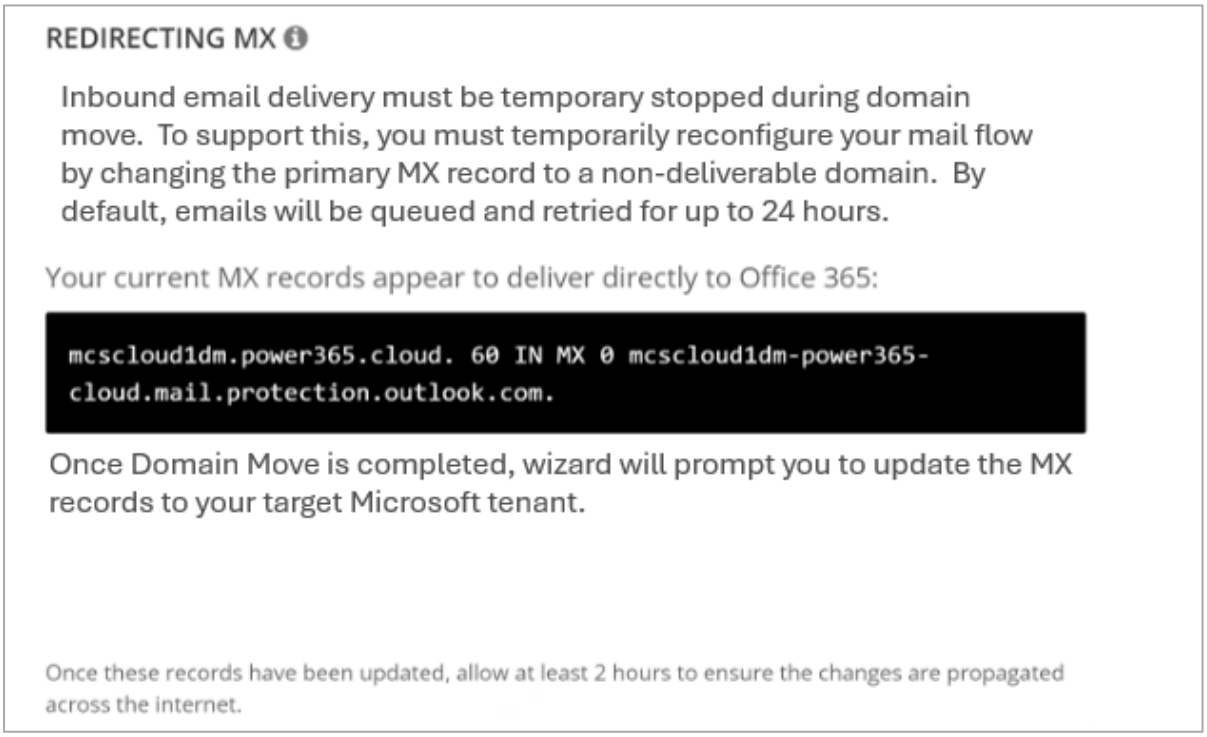
- A large number of objects are associated with the tenant and the domain move process is expected to take hours.
- Continuous email delivery during the domain move is a requirement. Mission critical systems and businesses are impacted when email delivery is suspended.
- Custom Transport rules and connectors are allowed in Exchange Online for either source or target tenant.

Domain Move Relay Service being discontinued after Dec 31, 2025.

The Domain Move Relay Feature which automatically redirects incoming email to target user mailboxes during domain transfer process will be discontinued after Dec 31, 2025. To facilitate this change, inbound email delivery can be temporarily interrupted to facilitate the domain migration between two M365 tenants. Typically, Internet mail servers will attempt to deliver new email for up to 24 hours. Email queuing can be achieved by changing the primary MX record from the M365 tenant to an unreachable domain.

However, note that using this method may result in some email returning as non-deliverable (NDR) if the primary MX record is not promptly restored to M365. Alternatively, a third-party email queuing service can be used to queue your email for extended periods (days or weeks). Once the migration is complete, queued messages will be delivered to the target M365 tenant.

During the migration of the domain, the system will prompt for redirecting the MX record, the admin may temporarily reconfigure the mail flow by changing the primary MX record to a non-deliverable domain. By default, email will be queued and retried for up to 24 hours.



Navigate

Dashboard

How do I navigate to the project dashboard?

The project dashboard includes overall project status statistics and summary sections covering project status, environments, and Domains ready for Cutover. Quick navigation icons are available at the top of the dashboard to go directly to project setup, settings, and refresh functions. Names and figures can be clicked on to view more detailed information for each item.

Does each project have its own dashboard?

Yes. Each project has its own dashboard. The project's name and number appears in the upper left of the dashboard. To change to another project’s dashboard, select "Projects" in the navigation menu.

How do I use the project dashboard?

A visual guide to the features of the project dashboard are presented in the images below. Click on a image to enlarge the image.

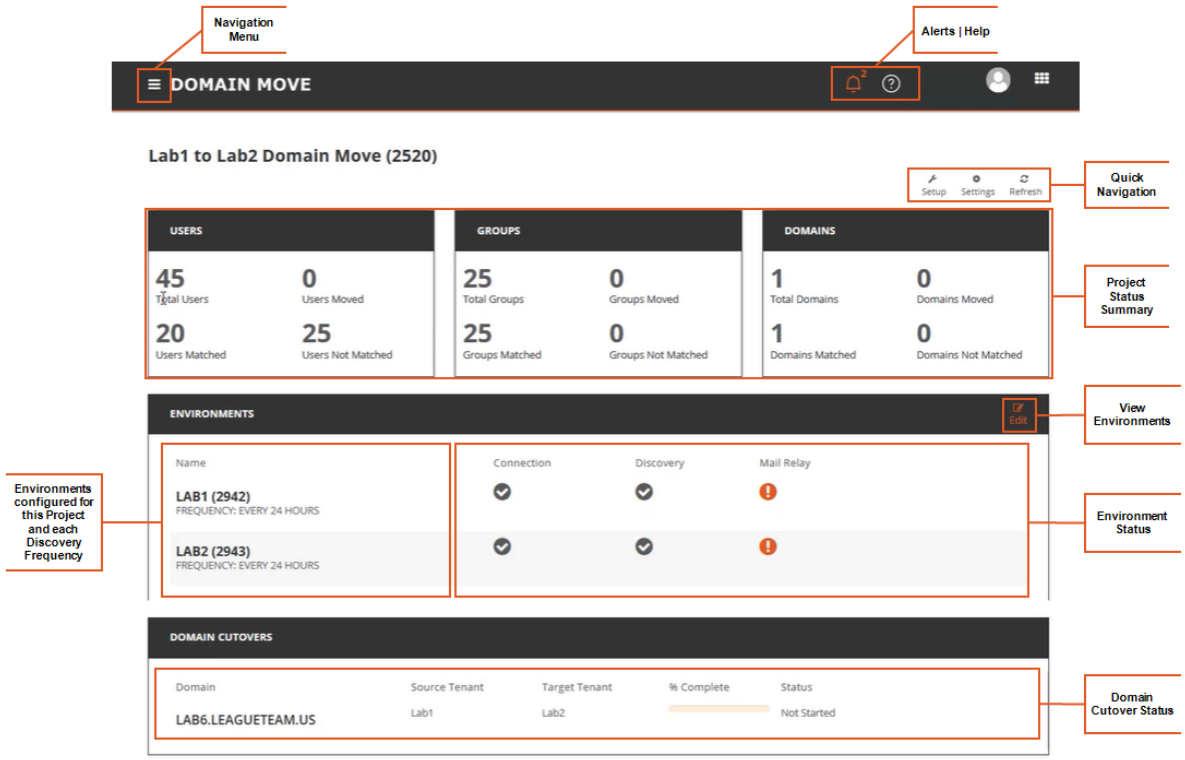


Figure 1: Example Dashboard

Menus

What menus are available?

Domain Move consists of two (2) menus. The left navigation menu which is sometimes referred to as the “Hamburger” menu and the right application menu, which is called, the “Waffle” menu.

The hamburger menu is used to navigate through the application’s different areas of management and configurations.

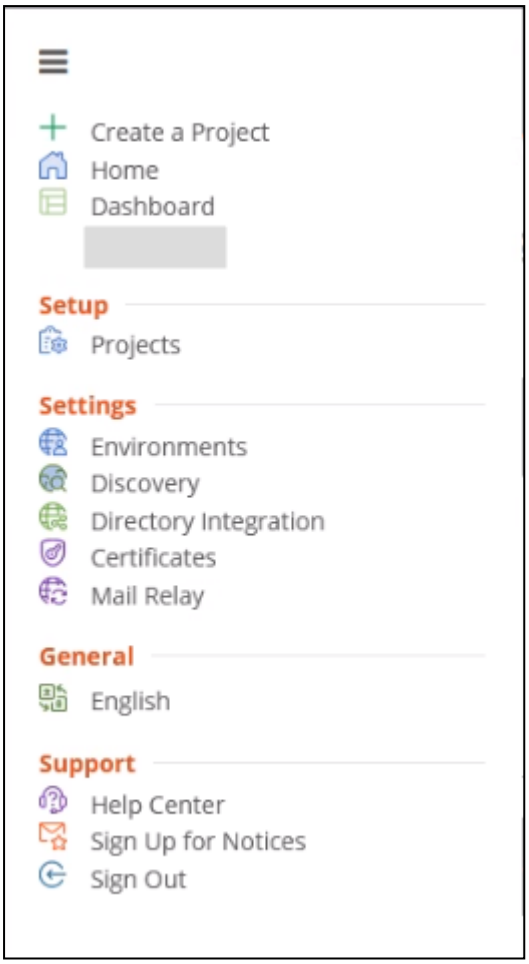


Figure 1: Example of Domain Move Menu

The waffle menu is your application menu where you can quickly navigate directly to an applications dashboard.

Figure 2: Example Applications Menu with all applications

Actions

What are actions?

Actions are activities that can started either manually by clicking the action button or some may be scheduled to start.

What actions are available?

Within Domain Move projects the following actions are available.

- **Match** – Match accounts against the target environment.
- **Export** – Export selected items to a file.

Where are actions?

Actions are located within each Users and Groups management table. From the Dashboard, just click **Total Users** to open the management view for either **Users + Mailboxes** or **Groups + Teams**.

Once you have selected the desired table, actions are located below the list of records. Simply select the desired records, the chosen action then Click, **Apply Action**.

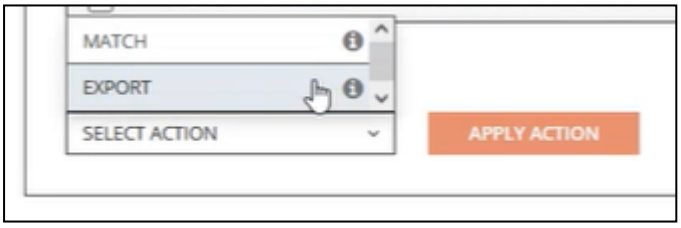


Figure 2: Example Action Menu

Users + Mailboxes

What is a user?

A user within Domain Move is any Microsoft 365 or Active Directory objects with an associated Mailbox. This includes users, rooms, equipment, shared and group mailboxes.

When are users displayed?

After you have discovered your users.

How do I view users and mailboxes?

You may navigate to your users and mailboxes from the Project Dashboard.

From the Dashboard, just click **Total Users** to open the user management view.

Can I filter the user view?

Yes, you can filter the list by many criteria including migration wave and synchronization status. The list will narrow as you add criteria.

When you have narrowed your search, you can select one or more users, and then perform any actions against them or choose **View Selected User** to narrow your view even more. You may narrow the list by entering a search term. Each column can be sorted via the directional arrows.

How do I view user and mailbox details?

Double-clicking on a user will bring up detailed information about the status of all processes in progress for that user.

Groups + Teams

How do I view groups and teams?

You may navigate to your groups and teams from the Project Dashboard.

From the Dashboard, just click **Total Groups** to open the group management view.

What is an Office 365 Group?

Microsoft Office 365 Groups are a shared workspace for email, conversations, files, and events where group members can collectively get stuff done.

Available through the Microsoft 365 suite of cloud services, Office 365 Groups allows users to create and manage ad hoc "groups" for collaboration. The group provides members access to a shared inbox (conversations), calendar and file repository.

For more information, check out these Microsoft articles on the topics.

- Collaborate with colleagues using Office 365 Groups
- Office 365 Groups

What is Microsoft Teams?

Microsoft Teams is a Group Chat feature of Microsoft 365 that brings everything together in a shared workspace where you can chat, meet, share files, and work with business apps.

Click here to learn more about Microsoft Teams.

Deleting Customer Data

To satisfy GDPR requirements, On Demand Migration Active Directory provides customers the ability to delete their data.

What pieces of data can be deleted?

On Demand Migration Active Directory provides the following ability:

- Delete Project and Environment data
- Monitor and off-board project and environment data when the On Demand Organization is deleted
- Monitor and off-board project and environment data when the On Demand Migration Active Directory License SKUs expire

How do you delete data?

Project data can be deleted by selection the"Delete" option next to each project on the Projects page. Environment data can be deleted by clicking the "Delete" button on the Environments page.

Does the data get removed immediately when choosing to delete?

Upon selecting the delete option and confirming the deletion of data, all project data including project configuration, tenant objects, object mappings and migration history will be marked as deleted, will no longer appear in the user interface, and will not be accessible. All migration jobs will stop processing including ones that are already running. After 30 days, the data is permanently removed from the database.

How is Email Address Rewrite Service disabled?

The Email Address Rewrite Service must be disabled in the Project Settings before a project can be deleted.

Appendix A: Using PowerShell

You can use the On Demand Migration PowerShell API to interact with objects in your On Demand Migration environment. The PowerShell cmdlets allow you to perform tasks, such as account discovery, mail migration, OneDrive migration, task and event management in a PowerShell scripting environment. The ODM API is available for install or download from the PowerShell Gallery.

Note: Usage of the PowerShell Gallery requires the PowerShellGet module to be installed on your computer. The module is normally installed with operating system, but may need an upgrade to the latest version. For more information, see How to Install PowerShellGet.

Gallery

On Demand User Role Requirements User must have the Migration Administrator role to access and run any of the On Demand Migration PowerShell commands. On Demand ships with this role. See the On Demand Global Settings Current User Guide for more information about setting up roles.

Deploying the ODM PowerShell API Module

The ODM PowerShell API module must be installed or download from the PowerShell Gallery.

Searching in PowerShell gallery

```
Find-Module OdmApi -Repository PSGallery
```

Installing the module from the PowerShell gallery

```
Install-Module OdmApi -Repository PSGallery
```

Downloading the module from the PowerShell gallery (without installing it)

```
Save-Module OdmApi -Repository PSGallery -Path "C:\temp"
```

Connecting to the ODM service

Before you can use the ODM PowerShell cmdlets to interact with your ODM environment, you must connect and authenticate your access to your ODM host. The credentials you use must be granted a role with sufficient privileges to work with the On Demand Migration services.

Connecting to the ODM service - Interactive mode

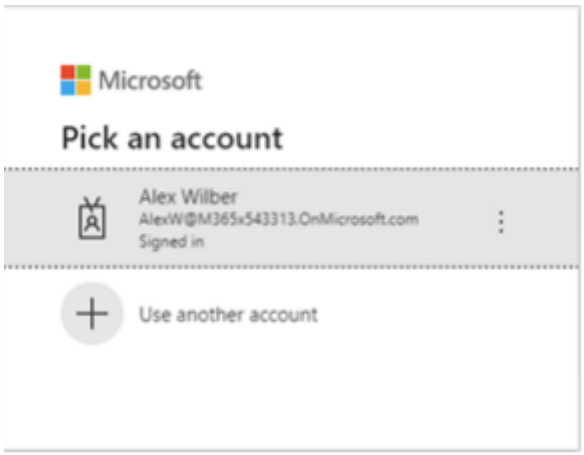
The Microsoft Account Authentication Workflow requires user interaction for the initial authentication with Microsoft. When Microsoft Account authentication is used all authentication is handled via Microsoft and the user's Microsoft Entra ID. This type of authentication supports MFA and is fully controlled by the user's Microsoft Entra ID Conditional Access Policies. Any password and lockout policies are also managed directly by the customer through their Microsoft Entra ID.

- Run the following command to connect to your ODM Service. The default region is US.

  Connect-OdmService

  To connect to a specific region like Europe, run the command Connect-OdmService -Region EU. The region value can be set in the OdmApi.psm1 file by editing this line: [string]$Region = 'us'. For example to set default region to Europe replace the line to [string]$Region = 'EU'.

- This command will redirect the user to the Microsoft Authentication workflow to authentication against the user's Azure Active Directory. In the authentication dialog, enter the credentials of the On Demand account (not the tenant account)



  If MFA is enforced, users will see an additional window

Connecting to the ODM service - Unattended (or Headless) mode

The Microsoft Account Authentication Workflow requires user interaction for the initial authentication with Microsoft. This type of authentication doe not supports MFA. It is used primary for work or school accounts. The Tenant ID is required.

Connect-OdmService -Username "admin@democorp.com" -Password "P@ssword!" -TenantId "81f2b32e-c198-44fd-99d4-109665c16f34"

If you only have On Demand Migration Active Directory or Directory Sync for your subscription,

Connect-OdmService -Username "admin@democorp.com" -Password "P@ssword!" -TenantId "81f2b32e-c198-44fd-99d4-109665c16f34"

Example: Selecting the organization and migration project

Get the organization id

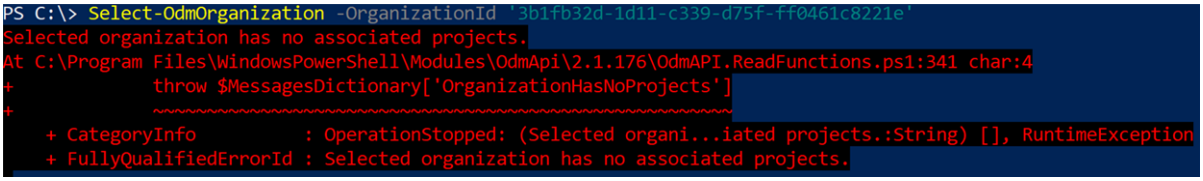
- Log in to Quest On Demand
- From the Choose an organization page, note the organization id.
- Click the logged in user name from the top right corner of the page.
- Click the Organization Name from the drop-down to open the Edit Organization page. Then make a note of the organization id.

Connect to the organization

In your PowerShell session console, enter the command:

Select-OdmOrganization -OrganizationId '6a079d6e-e98a-475b-acba-8b08e9caa430'

Note that if there are no On Demand Migration projects associated with the organization, a warning message like the following will appear. OdmAd cmdlets will still function despite this warning.



Retrieve a list of Directory Sync Workflows

In your PowerShell session console, enter the command:

Get-OdmAdWorkflow

```
PS C:\> Get-OdmAdWorkflow


WorkflowId          : 1409
ClientId            : 288
Name                : Workflow L1.46811-035
Description         :
ScheduleId          : 1747
Schedule            :
CreatedDate         : 1/1/0001 12:00:00 AM
UpdatedDate         : 2/19/2025 12:03:01 PM
NextExecutionDate   :
IsConfigured        : True
TestMode            : False
SkipScripts         : False
SyncScope           : SyncEverything
WorkflowSteps       :
WorkflowStepsCount  : 5
Environments        :
EnvironmentsCount   : 2
ActiveExecutionId   :
Status              : Idle
```

Retrieve a list of Directory Sync Environments

In your PowerShell session console, enter the command:

Get-OdmAdEnvironment

```
PS C:\> Get-OdmAdEnvironment


EndpointId                      : 647
ClientId                        : 288
Name                            : L1.Source
Discovery                       : Discovered
LastDiscovery                   : 2/19/2025 10:47:11 AM
LastReconcile                   : 2/11/2025 10:28:18 PM
UserAttributeName               : adminDescription
GroupAttributeName              : adminDescription
ContactAttributeName            : adminDescription
GlobalFilterId                  :
GlobalFilterEnabled             : False
GlobalFilter                    :
```

Start a Directory Sync Workflow

In your PowerShell session console, enter the command:

Start-OdmAdWorkflow -Identity <WorkflowId>

```
PS C:\Windows\system32> Start-OdmAdWorkflow -Identity 1409


WorkflowId          : 1409
ClientId            : 288
Name                : Workflow L1.46811-035
Description         :
ScheduleId          : 1747
Schedule            :
CreatedDate         : 1/1/0001 12:00:00 AM
UpdatedDate         : 2/19/2025 12:03:01 PM
NextExecutionDate   :
IsConfigured        : True
TestMode            : False
SkipScripts         : False
SyncScope           : SyncEverything
WorkflowSteps       :
WorkflowStepsCount  : 5
Environments        :
EnvironmentsCount   : 2
ActiveExecutionId   :
Status              : Pending
```

Retrieve logging for a Directory Sync Workflow's most recent run

In your PowerShell session console, enter the command:

Get-OdmAdWorkflowRun -Workflow <WorkflowId> -Limit 1 | Get-OdmAdWorkflowLog | ft timestamp, level, message

```
PS C:\Windows\system32> Get-OdmAdWorkflowRun -Workflow 1409 -Limit 1 | Get-OdmAdWorkflowLog | ft timestamp, level, messa
ge
WARNING: There are more results available than are currently displayed. To view them, increase the value for the Limit
parameter.

timestamp            level message
---------            ----- -------
2/19/2025 12:43:42 PM Info  Read: Done creating retrieval jobs.
2/19/2025 12:43:42 PM Info  Read: LastPushUsn updated to 549730.
2/19/2025 12:43:42 PM Info  Read: Reading deleted objects in CN=Deleted Objects,DC=btauto1,DC=com with LDAP query: (...
2/19/2025 12:43:42 PM Info  Read: Using global catalog server from configured DCs list: BTAuto1DCEX.btauto1.com, Dom...
2/19/2025 12:43:42 PM Info  Read: Reading objects in OU=QAAv2-OutOfScope,DC=btauto1,DC=com using LDAP query: (&(|(cn...
2/19/2025 12:43:42 PM Info  Read: Reading objects in OU=QAAv2-OutOfScope,DC=btauto1,DC=com
2/19/2025 12:43:42 PM Info  Read: Using global catalog server from configured DCs list: BTAuto1DCEX.btauto1.com, Dom...
2/19/2025 12:43:42 PM Info  Read: Reading objects in OU=QAAv2,DC=btauto1,DC=com using LDAP query: (&(|(cn=L1.*)(disp...
2/19/2025 12:43:42 PM Info  Read: Reading objects in OU=QAAv2,DC=btauto1,DC=com
2/19/2025 12:43:42 PM Info  Read: Using global catalog server from configured DCs list: BTAuto1DCEX.btauto1.com, Dom...
2/19/2025 12:43:42 PM Info  Read: Creating retrieval jobs.
2/19/2025 12:43:42 PM Info  Read: Verifying internal fields are set.
2/19/2025 12:43:42 PM Info  Read: Connecting to Domain Controller using port: 389
2/19/2025 12:43:42 PM Info  Read: Using global catalog server from configured DCs list: BTAuto1DCEX.btauto1.com, Dom...
```

Retrieve a list of Domain Rewrite / Domain Move tenants

In your PowerShell session console, enter the command:

Get-OdmAdExEnvironment

```
PS C:\> Get-OdmAdExEnvironment


TenantId                : 368
TenantName              : MCS Cloud 2
TenantGuid              : b5b4cbca-441a-4bc2-bfc7-39d530d58d1b
T2TPowerShellUsername   : BinaryTreePowerShellUser.6c03c0a4e4a542c69bee59a1b7347be8@qrdcloud2.onmicrosoft.com
IsConnected             : True
IsHybrid                : True
SkipUserDiscovery       : False
DiscoveryFrequencyHours : 24
DiscoveryStarted        : 2/19/2025 10:47:17 AM
DiscoveryFinished       : 2/19/2025 10:49:04 AM
DiscoveryDeltaTimestamp : 2/19/2025 10:47:16 AM
DiscoveryState          : Complete

TenantId                : 367
TenantName              : MCS Cloud 1
TenantGuid              : 51cbbf41-7b88-4913-a238-24632a9338d0
T2TPowerShellUsername   : BinaryTreePowerShellUser.416c5d09d8b54d0c881be2418e99b2a2@qrdcloud1.onmicrosoft.com
IsConnected             : True
IsHybrid                : True
SkipUserDiscovery       : False
DiscoveryFrequencyHours : 24
DiscoveryStarted        : 2/19/2025 10:47:16 AM
DiscoveryFinished       : 2/19/2025 10:49:13 AM
DiscoveryDeltaTimestamp : 2/19/2025 10:47:13 AM
DiscoveryState          : Complete
```

Getting Help

OdmApi module supports online help via Get-Help command. Any command syntax and examples of usage can be displayed by the Get-Help command.

Examples:

Get-Help Get-OdmAdEnvironment

```
PS C:\> Get-Help Get-OdmAdEnvironment

NAME
    Get-OdmAdEnvironment

SYNTAX
    Get-OdmAdEnvironment [-Identity] <Object> [-Detailed]  [<CommonParameters>]

    Get-OdmAdEnvironment [-Filter <string>] [-EndpointType {ActiveDirectory | Office365 | All}] [-Schedule <Object>]
    [-Limit <int>] [-Detailed]  [<CommonParameters>]
```

Active Directory Third Party Components

Component	License	Aknowledgment
Microsoft.Graph.Core 1.19.0	MIT N/A	© Microsoft Corporation. All rights reserved.
Mvc.JQuery.Datatables 1.3.44	MIT N/A	
Mvc.JQuery.Datatables.Core 1.3.44	MIT N/A	
ANTLR 3.4.1	BSD-style license N/A	Sam Harwell, Terence Parr
ARSoft.Tools.Net 2.2.6	Apache 2.0	
bluebird 3.5.3	MIT N/A	The MIT License (MIT) Copyright (c) 2013-2018 Petka Antonov Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions

Component	License	Aknowledgment
		of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Bootstrap 3.4.1	MIT N/A	Copyright (c) 2011-2016 Twitter, Inc.
BouncyCastle 1.8.1	MIT N/A	Copyright (c) 2000 - 2017 The Legion of the Bouncy Castle Inc
Castle.Core 4.4.0	Apache 2.0	Copyright (c) 2004-2019 Castle Project - http://www.castleproject.org/
clipboard.js 2.0.0	MIT N/A	
CommonServiceLocator 1.3.0	Microsoft Permissive License (Ms-PL) N/A	Microsoft Public License (MS-PL) This license governs use of the accompanying software
CookComputing.XmlRpcV2 3.0.0	MIT N/A	

Component	License	Aknowledgment

CsvHelper 2.16.3	Microsoft Public License (Ms-PL) 1.0 - October 12, 2006	// Copyright 2009-2016 Josh Close and Contributors
		// This file is a part of CsvHelper and is dual licensed under MS-PL and Apache 2.0.
		// See LICENSE.txt for details or visit http://www.opensource.org/licenses/ms-pl.html for MS-PL and http://opensource.org/licenses/Apache-2.0 for Apache 2.0.
		// http://csvhelper.com

DotNetZip 1.15.0	Microsoft Permissive License (Ms-PL) N/A	
EntityFramework 6.1.4	MS-.NET-Library License N/A	
EntityFramework.Extended 6.1.0.168	BSD 3-Clause License N/A	Copyright (c) 2014, LoreSoft
EntityFramework.Server 6.1.4	MS-.NET-Library License N/A	
FontAwesome.WPF 4.7.0.9	MIT N/A	Copyright (c) 2014-2016 charri
HtmlAgilityPack.dll 1.11	MIT N/A	
jquery 3.5.1	MIT N/A	
jquery.validate 1.13.0	MIT N/A	
jquery.validate 1.15.0	MIT N/A	
jquery.validate 1.8	MIT N/A	
jquery.validate.unobtrusive 3.2.3	MIT N/A	

Component	License	Aknowledgment
Json.NET 11.0.2.21924	MIT 1.0	The MIT License (MIT) Copyright (c) 2007 James Newton-King Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN

Component	License	Aknowledgment
		CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Kentor.OwinCookieSaver 1.1.1	MIT 1.0	
Knockout 3.5.0	MIT N/A	
knockout.validation 2.0.3	MIT N/A	
knockout-kendo 0.9.7	Apache 2.0	
knockout-sortable 0.14.0	MIT N/A	
Microsoft.Azure.ActiveDirectory.GraphClient 2.1	MS-.NET-Library License N/A	
Microsoft.Azure.KeyVault 2.3.2	MIT N/A	Copyright (c) Microsoft Corporation
Microsoft.Azure.KeyVault.Core 2.0.4	MIT N/A	Copyright (c) Microsoft Corporation
Microsoft.Azure.KeyVault.Cryptography 2.0.5	MIT N/A	
Microsoft.Azure.KeyVault.Extensions 2.0.5	MIT N/A	
Microsoft.Azure.KeyVault.WebKey 2.0.7	MIT N/A	Copyright (c) Microsoft Corporation
Microsoft.Azure.Management.ResourceManager 1.1.5-preview	MIT N/A	
Microsoft.Azure.Management.ResourceManager.Fluent 1.14	MIT N/A	

Component	License	Aknowledgment
Microsoft.Azure.WebJobs 2.0.0	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions 2.0.0	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
Microsoft.Data.Edm 5.8.4	OData .NET Libraries - ODataLib 2018	© Microsoft Corporation. All rights reserved.
Microsoft.Data.OData 5.8.4	OData .NET Libraries - ODataLib 2018	© Microsoft Corporation. All rights reserved.
Microsoft.Data.Services.Client 5.8.4	MIT 1.0	Copyright (c) 2018 Microsoft. All rights reserved.
Microsoft.DiaSymReader.Native.amd64 14.00	MICROSOFT .NET LIBRARY 1.0	
Microsoft.DiaSymReader.Native.x86 14.00	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Exchange.WebServices 15.00	MIT 1.0	
Microsoft.Exchange.WebServices.Auth 15.00	MIT 1.0	
Microsoft.Extensions.Logging 1.1.2	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Extensions.Logging.Abstract 1.1.2	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Graph 1.21.0	MIT N/A	Copyright (c) Microsoft. All rights reserved.
Microsoft.Identity.Client 4.41.0	MIT Template 2020	
Microsoft.IdentityModel 6.1.7600.16394	Microsoft Permissive License (Ms-PL) N/A	-

Component	License	Aknowledgment
Microsoft.IdentityModel.Clients.Active Directory 3.13.3	MIT N/A	
Microsoft.IdentityModel.Clients.Active Directory 3.19.5	MIT N/A	
Microsoft.IdentityModel.Clients.Active Directory 5.2.7	MIT N/A	
Microsoft.IdentityModel.Clients.Active Directory.Platform 3.13.3	MICROSOFT Public License 2012	
Microsoft.IdentityModel.Clients.Active Directory.Platform 3.19.5	MIT N/A	
Microsoft.IdentityModel.Protocol.Extensions 1.0	MIT N/A	
Microsoft.Office.Client.Policy 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.Office.Client.TranslationServices 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.Office.SharePoint.Tools 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.Online.SharePoint.Client.Tenant 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.Open.AzureAD16.Graph.Client 2.0.0	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin 3.0.40213.64	Microsoft.Owin 1	
Microsoft.Owin.Host.SystemWeb	MICROSOFT .NET	

Component	License	Aknowledgment
3.0.40213.64	LIBRARY 1.0	
Microsoft.Owin.Security 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin.Security.ActiveDirectory 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin.Security.Cookies 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin.Security.Jwt 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin.Security.OAuth 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.Owin.Security.OpenIdConnect 3.0.40213.64	MICROSOFT .NET LIBRARY 1.0	
Microsoft.PowerBI.Api 2.0.14	MIT N/A	© Microsoft Corporation. All rights reserved.
Microsoft.PowerBI.Api 2.11.0.19267	MIT N/A	
Microsoft.PowerBI.Core 1.1.11.17109	MIT N/A	
Microsoft.Practices.EnterpriseLibrary.Common 6.0.1304.0	Microsoft Public License (Ms-PL) http://www.opensource.org/licenses/MS-PL	
Microsoft.Practices.ServiceLocation 1.3.0.0	MICROSOFT Public License 2012	
Microsoft.Practices.Unity 4.0.1	Apache 2.0	
Microsoft.ProjectServer.Client 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	

Component	License	Aknowledgment
Microsoft.Protocols.TestTools.Messages.Runtime 1.0	MIT N/A	
Microsoft.Rest.ClientRuntime 2.1.0.0	MIT N/A	
Microsoft.Rest.ClientRuntime 2.3.10.0	MIT N/A	
Microsoft.Rest.ClientRuntime 2.3.21.0	MIT N/A	
Microsoft.Rest.ClientRuntime.Azure 3.1.0.0	MIT N/A	
Microsoft.Rest.ClientRuntime.Azure 3.3.12	MIT N/A	Copyright (c) Microsoft Corporation
Microsoft.Rest.ClientRuntime.Azure 3.3.15.0	MIT N/A	
Microsoft.Rest.ClientRuntime.Azure.Authentication 2.3.1.0	MIT N/A	
Microsoft.ServiceFabric.Actors 4.0.0.0	MICROSOFT .NET LIBRARY 1.0	
Microsoft.ServiceFabric.Data 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Data.Extensions 1.4.5.0	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Data.Interfaces 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Diagnostics 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.FabricTransport 7.0.457.9590	MS-.NET-Library License N/A	

Component	License	Aknowledgment
Microsoft.ServiceFabric.Internal 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Internal.Strings 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Preview 7.0.457.9590	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.ReliableCollection.Interop 1.0	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Services 4.0.0.0	MS-.NET-Library License N/A	
Microsoft.ServiceFabric.Services.Remoting 4.0.0.0	MS-.NET-Library License N/A	
Microsoft.SharePoint.Client 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.DocumentManagement 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.Publishing 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.Runtime 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.Runtime.Windows 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.Search 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	

Component	License	Aknowledgment
Microsoft.SharePoint.Client.Search.Applications 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.Taxonomy 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.UserProfiles 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.SharePoint.Client.WorkflowServices 16.1.20122.12000	MICROSOFT SHAREPOINT CLIENT COMPONENTS as of Jan'16, 2020	
Microsoft.Web.Infrastructure 1.0.0	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
Microsoft.Win32.Primitives 4.6.2	MS-.NET-Library License N/A	
Microsoft.WindowsAzure.Configuration Manager 3.2.3.0	MIT N/A	
Microsoft.WindowsAzure.Storage 8.7.0.0	MIT N/A	
Microsoft.WindowsAzure.Storage 9.3.2	Apache 2.0	
MimeKit 1.8.0	MIT N/A	
MimeTypesMap 1.0.8.0	MIT N/A	
Moment.js 2.29.1	MIT momentjs n/a	
Nancy 1.4	MIT N/A	Copyright (c) 2010 Andreas Håkansson, Steven Robbins and contributors

Component	License	Aknowledgment
Nancy.Hosting.Self 1.4.1	MIT N/A	
NCrontab 3.2.20120.652	Apache 2.0	
Newtonsoft.Json 10.0.2	MIT N/A	Copyright (c) 2007 James Newton-King
Newtonsoft.Json 11.0.1	MIT 1.0	Copyright (c) 2007 James Newton-King
Newtonsoft.Json 11.0.2	MIT N/A	Copyright (c) 2007 James Newton-King
Newtonsoft.Json 13.0.1	MIT Template 2020	MIT License _____ Permission is hereby granted, free of charge, to any person obtaining a copy of _____ (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice (including the next paragraph) shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL _____ BE

Component	License	Aknowledgment
		LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Ninject.dll 3.2.2	Apache 2.0	Copyright ? .NET Foundation and Contributors. All Rights Reserved
Ninject.Web.Common 3.2.3	Apache 2.0	
Ninject.Web.Mvc 3.2.1.0	Apache 2.0	
NLog 3.2.0.0	BSD 3-Clause License N/A	
NLog 4.4.4	BSD - Kowalski 2011	Copyright (c) 2004-2016 Jaroslaw Kowalski <jaak@jkowalski.net>, Kim Christensen, Julian Verdurmen Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disc

Component	License	Aknowledgment
NLog 4.6.8	BSD 3-Clause License N/A	
Owin 1.0.0	Apache 2.0	Copyright 2012 OWIN contributors
PAExec 1.0	PowerAdmin 1.0	https://www.poweradmin.com/paexec/paexec_eula.txt
PowerBI-JavaScript 2.6.5	MIT N/A	
Redemption Distributable 5.22	Redemption 2010	
respond.js 1.2	MIT N/A	Copyright (c) 2012 Scott Jehl

RestSharp 105.2.3	Apache 2.0	// Copyright 2010 John Sheehan
		//
		// Licensed under the Apache License, Version 2.0 (the "License");
		// you may not use this file except in compliance with the License.
		// You may obtain a copy of the License at
		//
		//
		http://www.apache.org/licenses/LICENSE-2.0
		//
		// Unless required by applicable law or agreed to in writing, software
		// distributed under the License is distributed on an "AS IS" BASIS,
		// WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or i

Swashbuckle 5.6.0	BSD 3-Clause License N/A	Copyright (c) 2016, Richard Morris
Swashbuckle.Core 5.6.0	BSD 3-Clause License N/A	Copyright (c) 2013, Richard

Component	License	Aknowledgment
		Morris. All rights reserved.
System.AppContext 4.6.23	MS-.NET-Library License N/A	
System.Buffers 4.4.0	MIT N/A	© Microsoft Corporation. All rights reserved.
System.Collections.Immutable 4.6.24	MIT N/A	
System.Console 4.6.2	MICROSOFT .NET LIBRARY 1.0	
System.Diagnostics.DiagnosticSource 4.6.0	MIT N/A	
System.Diagnostics.FileVersionInfo 4.6.24	MS-.NET-Library License N/A	
System.Diagnostics.Process 4.6.24	MS-.NET-Library License N/A	
System.Diagnostics.StackTrace 4.6.24	MS-.NET-Library License N/A	
System.Fabric 7.0.457.9590	MS-.NET-Library License N/A	
System.Fabric.Management.ServiceModel 7.0.457.9590	MS-.NET-Library License N/A	
System.Fabric.Strings 7.0.457.9590	MS-.NET-Library License N/A	
System.IdentityModel.Tokens.Jwt 4.0.2.206221351	Apache 2.0	Copyright (c) Microsoft Corporation. All rights reserved
System.IO.Compression 4.6.24	MS-.NET-Library License N/A	

Component	License	Aknowledgment
System.IO.FileSystem 4.6.24	MS-.NET-Library License N/A	
System.IO.FileSystem.DriveInfo 4.6.24	MS-.NET-Library License N/A	
System.IO.FileSystem.Primitives 4.6.24	MS-.NET-Library License N/A	
System.IO.Pipes 4.6.24	MS-.NET-Library License N/A	
System.Management.Automation.dll 10.0.10586.0	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Management.Automation.dll System.Management.Automation_ PowerShell_3.0	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Memory 4.6.2	MIT 1.0	
System.Net.Http.Extensions.dll 2.2.2	MS-.NET-Library License N/A	
System.Net.Http.Formatting 5.2.3	MS-.NET-Library License N/A	
System.Net.Http.Primitives 4.2.2	MS-.NET-Library License N/A	
System.Numerics.Vectors 4.6.25519.03	MIT Template 2020	Licensed under MIT License terms can be found at: https://dot.net/ Copyright .NET Foundation and Contributors --- Licensed under MIT License terms can be found at: https://github.com/dotnet/runtime Copyright .NET Foundation and Contributors

Component	License	Aknowledgment
System.Reflection.Metadata 4.6.24	MS-.NET-Library License N/A	
System.Runtime.CompilerServices.Unsafe 4.6.2	MS-.NET-Library License N/A	
System.Security.AccessControl 4.6.24	MIT 1.0	
System.Security.Claims 4.6.2	MS-.NET-Library License N/A	
System.Security.Cryptography.Algorithms 4.6	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Security.Cryptography.Encoding 4.6	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Security.Cryptography.Primitives 4.6	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Security.Cryptography.X509Certificates 4.6	MICROSOFT .NET LIBRARY 1.0	© Microsoft Corporation. All rights reserved.
System.Security.Principal.Windows 4.6.2	MIT 1.0	
System.Spatial 5.8.40	MIT N/A	© Microsoft Corporation. All rights reserved.
System.Text.Encoding.CodePages 4.6.25519.03	MIT 1.0	
System.Threading.Tasks.Dataflow 4.5.24.0	MIT N/A	
System.Threading.Thread 4.6.24705.01	MICROSOFT .NET LIBRARY 1.0	
System.ValueTuple 4.6.24705.01	MIT 1.0	

Component	License	Aknowledgment
System.Web.Helpers 3.0.3	MS-.NET-Library License N/A	
System.Web.Http 5.2.30128.0	MICROSOFT .NET LIBRARY 1.0	
System.Web.Http.Owin 5.2.30128.0	MICROSOFT .NET LIBRARY 1.0	
System.Web.Http.WebHost 5.2.30128.0	MICROSOFT .NET LIBRARY 1.0	
System.Web.Mvc 5.2.30128.0	MICROSOFT .NET LIBRARY 1.0	
System.Web.Optimization 1.1.4	MS-.NET-Library License N/A	
System.Web.Razor.dll 3.0.30128.0	Apache 2.0	
System.Web.WebPages 3.0.3	MS-.NET-Library License N/A	
System.Web.WebPages.Deployment 3.0.3	MS-.NET-Library License N/A	
System.Web.WebPages.Razor 3.0.3	MS-.NET-Library License N/A	
System.Xml.ReaderWriter 4.6.2	MS-.NET-Library License N/A	
System.Xml.XmlDocument 4.6.2	MS-.NET-Library License N/A	
System.Xml.XPath 4.6.3	MS-.NET-Library License N/A	
System.Xml.XPath.XDocument 4.6.2	MS-.NET-Library License 1.0	

Component	License	Aknowledgment
WebActivatorEx 2.2.0	Apache 2.0	Copyright © Microsoft 2010
WebGrease 1.6.x	Apache 2.0	Copyright 2012 Microsoft
WindowsAzure.ServiceBus 4.1.11	MICROSOFT SOFTWARE LICENSE TERMS Windows Azure Libraries	Copyright © Microsoft Corporation. All rights reserved.

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