One Identity Quick Connect Sync Engine 5.5.0

Administrator Guide

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

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

One Identity LLC.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

One Identity 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 http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

⊗ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

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

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

One Identity Quick Connect Sync Engine Administrator Guide
Updated - October 2017
Version - 5.5.0

Contents

1

One Identity Quick Connect Overview

About One Identity Quick Connect

Within the same organization identity information can be stored in many different data systems, such as directories, databases, or formatted dump files. To manage identity information and synchronize it between these data systems, administrators sometimes have to spend a considerable amount of time and effort. On top of that, performing the data synchronization tasks manually is error-prone and can lead to the duplication of information and incompatibility of data formats.

With Quick Connect, you can completely automate the process of identity data synchronization between the data systems used in your enterprise environment.

Quick Connect increases the data management efficiency by allowing you to automate the provision, deprovision, and update operations between the data systems you use. For example, when an employee joins or leaves the organization, the related information in the data systems managed by Quick Connect is automatically updated, thereby reducing your administrative workload and getting the new users up and running faster.

The use of scripting capabilities provides a flexible way to automate day-to-day administration tasks and integrate the administration of managed data systems with other business processes. By automating regular synchronization tasks, Quick Connect allows administrators to concentrate on strategic issues, such as planning the directory, increasing enterprise security, and supporting business-critical applications.

Quick Connect includes a core module called *One Identity Quick Connect Sync Engine* and a number of connectors that enable One Identity Quick Connect Sync Engine to access external data systems to read and synchronize the identity information they contain.

In order to synchronize identity data between external data systems, you must connect One Identity Quick Connect Sync Engine to these data systems through connectors. A connector enables One Identity Quick Connect Sync Engine to access specific data system to read and synchronize data in that system according to your settings.

Out of the box, One Identity Quick Connect Sync Engine includes a number of built-in connectors. These connectors allow you to access the following data systems:

- ActiveRoles Server
- Quest One Identity Manager
- One Identity Manager

The built-in connectors do not require any license file.

To connect One Identity Quick Connect Sync Engine to other data systems, you need to obtain and install special Quick Connect packages (also known as *bundles*), each including connectors for particular data systems.

To learn more about available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

Features and benefits

One Identity Quick Connect Sync Engine offers the following major features:

- Bidirectional synchronization
- Delta processing mode
- Synchronization of group membership
- Windows PowerShell scripting
- Attribute synchronization rules
- Rule-based generation of distinguished names
- Scheduling capabilities
- Extensibility

Bidirectional synchronization

Bidirectional synchronization allows you to synchronize all changes occurred to identity information between your data systems. Using this type of synchronization, you can proactively prevent potential identity information conflicts between different data sources.

> IMPORTANT: The bidirectional synchronization is not supported for some data systems. For more information, see the Quick Start Guide supplied with the Quick Connect package you use. For more information about available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

Delta processing mode

Delta processing mode allows you to more quickly synchronize identities by processing only the data that has changed in the source and target connected systems since their last synchronization.

Both the full mode and the delta mode provide you with the flexibility of choosing the appropriate method for your synchronization tasks.

> IMPORTANT: The delta processing mode is not supported for some data systems. For more information, see the Quick Start Guide supplied with the Quick Connect package you use. For more information about available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

Synchronization of group membership

One Identity Quick Connect Sync Engine allows you to ensure that group membership information is in sync in all connected data systems. For example, when provisioning a group object from an Active Directory domain to an AD LDS (ADAM) instance, you can configure rules to synchronize the Member attribute from the Active Directory domain to the AD LDS (ADAM) instance.

Windows PowerShell scripting

The Management Shell component of One Identity Quick Connect Sync Engine is an automation and scripting shell that provides a command-line management interface for synchronizing data between connected systems via the Quick Connect Service.

The Management Shell is implemented as a Windows PowerShell snap-in extending the standard Windows PowerShell functionality. The cmdlets provided by the Management Shell conform to the Windows PowerShell standards and are fully compatible with the default command-line tools that come with Windows PowerShell.

The Management Shell lets administrators perform attribute or password synchronization operations by using Windows PowerShell scripts. For example, you can compose and run a Windows PowerShell script that assigns values to the target object attributes using the values of the source object attributes. For more information, see Appendices.

Attribute synchronization rules

With One Identity Quick Connect Sync Engine, you can create and configure synchronization rules to generate values of target object attributes. These rules support the following types of synchronization:

- **Direct synchronization**. Assigns the value of a source object attribute to the target object attribute you specify.
- **Script-based synchronization**. Allows you to use a Windows PowerShell script to generate the target object attribute value.
- **Rule-based synchronization**. Allows you to create and use rules to generate the target object attribute value you want.

Rule-based generation of distinguished names

One Identity Quick Connect Sync Engine lets you create flexible rules for generating the distinguished names (DNs) of objects being provisioned. These rules allow you to ensure that objects created during provisioning operations are named in full compliance with the naming conventions existing in your organization.

Scheduling capabilities

You can schedule the execution of data synchronization operations and automatically perform them on a regular basis to satisfy your company’s policy and save time and effort.

Extensibility

To access external data systems One Identity Quick Connect Sync Engine employs special *connectors*. A connector enables One Identity Quick Connect Sync Engine to read and synchronize the identity data contained in a particular data system. Out of the box, One Identity Quick Connect Sync Engine includes built-in connectors that allow you to connect to the following data systems:

- ActiveRoles Server
- Quest One Identity Manager
- One Identity Manager

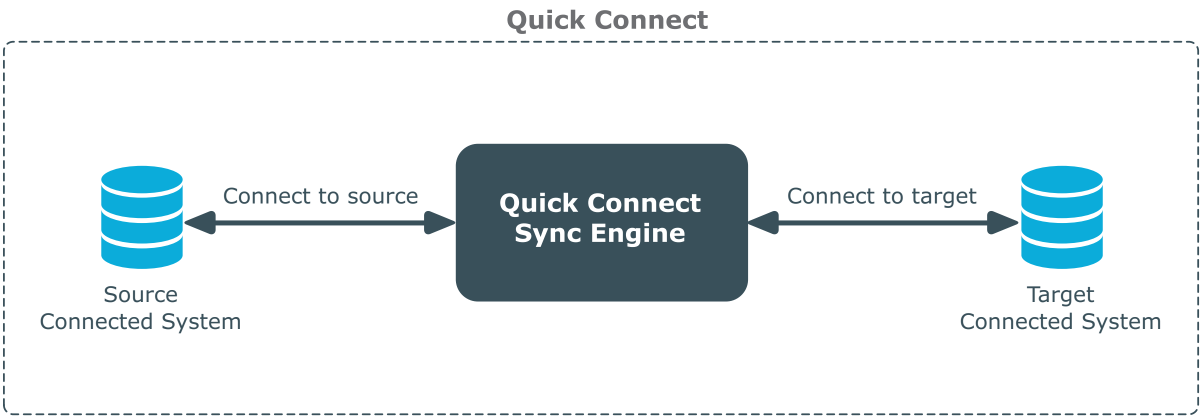
To connect One Identity Quick Connect Sync Engine to other supported data systems, you need to obtain and install one or more special Quick Connect packages (also known as *bundles*) providing connectors for accessing these data systems. For more information on available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

In case no ready-made connector is available for your data system, you can develop and implement your own custom connector. One Identity Quick Connect Sync Engine provides a Software Development Kit (SDK) containing documentation and samples for developing and implementing custom connectors.

Technical overview

Quick Connect environment comprises One Identity Quick Connect Sync Engine, Capture Agents, connected data systems, connectors, connections, and synchronization workflows.

The following illustration shows how Quick Connect synchronizes data between connected data systems.

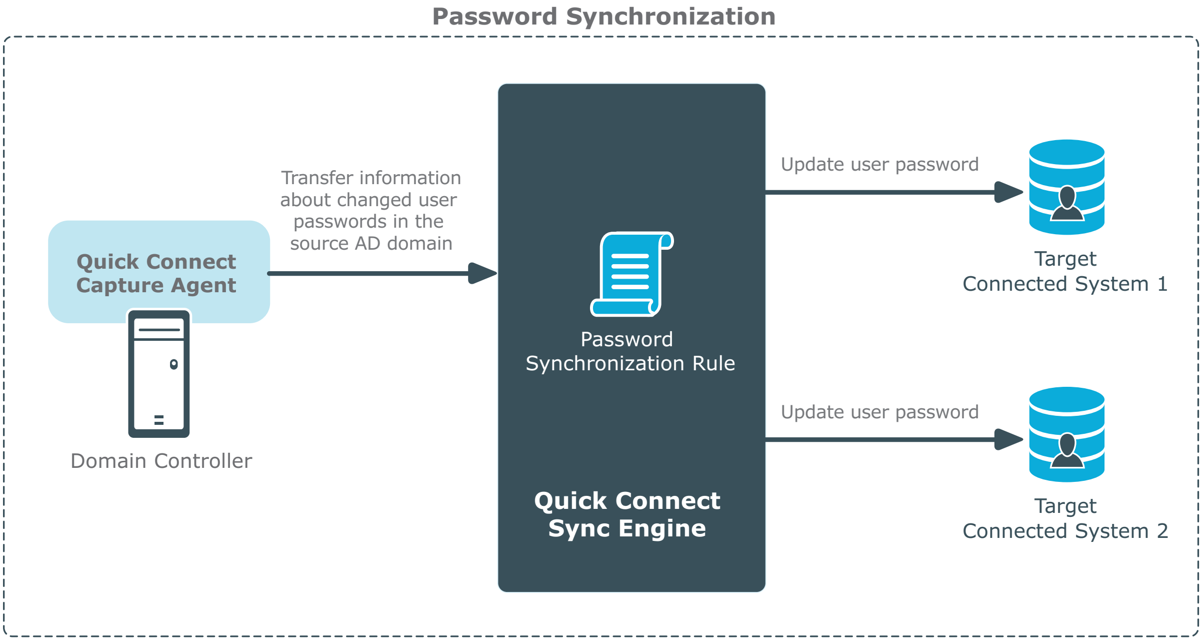


One Identity Quick Connect Sync Engine

One Identity Quick Connect Sync Engine, a core module of One Identity Quick Connect, includes the Quick Connect Service that performs data synchronization operations and the Quick Connect Administration Console that provides a graphical user interface for managing connections to data systems and data synchronization operations.

Capture Agent

Quick Connect Capture Agent allows you to synchronize user passwords between Active Directory domains managed by One Identity Quick Connect Sync Engine and other connected data systems. The following diagram shows how the Password Synchronization feature of One Identity Quick Connect Sync Engine works:


Password Synchronization
Quick Connect Capture Agent
Domain Controller
Transfer information about changed user passwords in the source AD domain
Password Synchronization Rule
Quick Connect Sync Engine
Update user password
Target Connected System 1
Update user password
Target Connected System 2

Quick Connect Capture Agent tracks changes to user passwords in the source Active Directory domain and provides that information to One Identity Quick Connect Sync Engine, which in turn synchronizes the changes with target connected data systems by using the password synchronization rules you specified. To synchronize passwords, you need to install Capture Agent on each domain controller in the Active Directory domain you want to use as a source for the password synchronization operations.

Connectors and connected data systems

One Identity Quick Connect Sync Engine lets you synchronize identity information between a wide variety of external data systems. To synchronize identities, you must connect One Identity Quick Connect Sync Engine to your data systems through special connectors. A connector enables One Identity Quick Connect Sync Engine to access a specific data system and read and synchronize identity data in that system.

Out of the box, One Identity Quick Connect Sync Engine supports the following data systems:

- ActiveRoles Server
- Quest One Identity Manager
- One Identity Manager

You can connect One Identity Quick Connect Sync Engine to other supported data systems only after installing Quick Connect packages providing connectors for those systems. For more information on available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

In addition to ready-made connectors, you can develop and implement your own custom connectors for specific data systems. For more information, refer to Dell One Identity Quick Connect Software Development Kit (SDK).

Synchronization workflows and steps

A *synchronization workflow* is a set of *synchronization steps* (or *synchronization operations*) that define how to synchronize objects between two connected data systems. A synchronization workflow can comprise one or more synchronization steps. You can use the Quick Connect Administration Console, a component of One Identity Quick Connect Sync Engine, to configure as many synchronization workflows as needed.

You can configure a *synchronization step* to perform one of the following operations:

- **Provision**. Creates objects in the target connected data systems based on the changes made to specific objects in the source connected system. When creating a new object, Quick Connect assigns initial values to the object attributes based on the attribute population rules you have configured.
- **Update**. Changes the attributes of objects in the target connected data systems based on the changes made to specific objects in the source connected system. To define the objects that will participate in the update operation you can use *object mapping rules*. For more information, see Mapping objects.
- **Deprovision**. Modifies or removes objects in the target connected data systems after their counterparts have been disconnected from the source connected system. One Identity Quick Connect Sync Engine can be configured to remove objects permanently or change them to a specific state.

Deploying One Identity Quick Connect Sync Engine

Licensing

The following Quick Connect components do not require a license:

- One Identity Quick Connect Sync Engine and built-in connectors (Quest ActiveRoles Server Connector and Quest One Identity Manager Connector).
- Capture Agent
- Management Shell

To use additional Quick Connect packages that provide connectors to external data systems, you may need to obtain and install a license file. For more information on available Quick Connect packages, please visit www.quest.com/activeroles-server/quickconnect-connectedsystems.aspx.

Installation steps

This section provides instructions on how to perform a clean installation of One Identity Quick Connect Sync Engine. If you want to upgrade One Identity Quick Connect Sync Engine, see Upgrading from an earlier version.

To install One Identity Quick Connect Sync Engine, complete these steps:

- Step 1: Install One Identity Quick Connect Sync Engine
- Step 2: Configure One Identity Quick Connect Sync Engine

Step 1: Install One Identity Quick Connect Sync Engine

To install One Identity Quick Connect Sync Engine

1. Make sure the system on which you wish to install One Identity Quick Connect Sync Engine meets the system requirements provided in the *One Identity Quick Connect Sync Engine Release Notes*.
2. Run one of the following files supplied with the One Identity Quick Connect Sync Engine installation package:
   a. In a 32-bit edition of Windows, run the file **QuickConnectSyncEngine_x86.msi**
   b. In a 64-bit edition of Windows, run the file **QuickConnectSyncEngine_x64.msi**
3. Step through the wizard that starts.
4. On the **Custom Setup** page, select the features you want to install, and then click **Next**.

   The following features are available:

   - **One Identity Quick Connect Sync Engine** (required). Installs Quick Connect Administration Console, Quick Connect Service, and built-in connectors. The Administration Console is a graphical user interface providing access to the Quick Connect functionality. The Quick Connect Service manages data flows between connected data systems. Connectors enable One Identity Quick Connect Sync Engine to access specific data systems to read and synchronize identity data.
   - **Configuration Import Wizard** (required). Installs a tool that allows you to import One Identity Quick Connect Sync Engine configuration settings from an earlier version of One Identity Quick Connect Sync Engine to the version you are installing.
   - **SDK** (optional). Installs documentation and samples that provide information about developing custom connectors for external data systems.
   - Administrative Templates (optional). Installs Group Policy administrative templates for deploying Capture Agent and configuring password synchronization parameters. For more information, see "Step 4 (Optional): Configure Capture Agent" on page 23.
5. On the **Specify Quick Connect Service Account** page, enter the name and password of the user account under which you want the Quick Connect Service to run, and then click **Next**.
6. Click **Install** and follow the instructions to complete the installation.

Step 2: Configure One Identity Quick Connect Sync Engine

To configure One Identity Quick Connect Sync Engine you installed in Step 1: Install One Identity Quick Connect Sync Engine, you can use one of the following methods:

- Specify new SQL Server databases for storing the One Identity Quick Connect Sync Engine data.
  With this method, you can select to store the configuration settings and synchronization data either in a single new SQL Server database or in two separate databases.
- Share existing configuration settings between two or more instances of One Identity Quick Connect Sync Engine.
- Use the configuration settings held in the SQL Server databases that have left after the removal of a One Identity Quick Connect Sync Engine instance.

To configure One Identity Quick Connect Sync Engine

1. Start the Quick Connect Administration Console.
2. Follow the steps in the wizard that starts automatically to configure One Identity Quick Connect Sync Engine.

   To create new SQL Server databases for storing data, on the step titled **Select a configuration method**, select the **Create a new configuration** option.

   If you want to store the configuration settings and synchronization data in a single SQL Server database, on the step titled **Specify where to store data**, clear the **Store sync data in a separate database** check box, and then specify the database name.

   If you want to store the configuration settings and synchronization data in two separate databases, select that check box, and then specify the database in which you want to store the synchronization data.

Upgrading from an earlier version

To upgrade One Identity Quick Connect Sync Engine to version 5.5.0, you can use the following upgrade methods:

In-place upgrade. This method is recommended if you do not use One Identity Quick Connect Sync Engine to synchronize passwords between data systems.

As compared to the side-by-side upgrade method, the in-place method involves less steps and does not require additional hardware: you install One Identity Quick Connect Sync Engine 5.5.0 on the same computer where an earlier version of One Identity Quick Connect Sync Engine is installed. Then, you import the configuration settings from the earlier One Identity Quick Connect Sync Engine version to version 5.5.0.

The in-place method automatically transfers connected system access passwords to the new installation of One Identity Quick Connect Sync Engine, therefore you do not have to retype the access passwords in the Quick Connect Administration Console.

Regardless of the upgrade method you choose, the upgrade operation will transfer the One Identity Quick Connect Sync Engine configuration settings from a earlier version to version 5.5.0. These configuration settings include connections to external data systems, synchronization scope, synchronization workflows, password synchronization settings, and mapping pairs and rules.

In-place upgrade

To perform an in-place upgrade, complete the following steps:

- Step 1: Install One Identity Quick Connect Sync Engine 5.5.0
- Step 2: Create new SQL Server databases
- Step 3: Import configuration settings
- Step 4: Upgrade Capture Agent on each DC

Step 1: Install One Identity Quick Connect Sync Engine 5.5.0

For instructions on how to install One Identity Quick Connect Sync Engine, see Step 1: Install One Identity Quick Connect Sync Engine.

Step 2: Create new SQL Server databases

In this step, you create new SQL Server databases in which One Identity Quick Connect Sync Engine 5.5.0 will save its data. You can select to store the configuration settings and synchronization data either in a single new SQL Server database or in two separate databases.

To create new SQL Server databases

1. Start the Quick Connect Administration Console.
2. In the wizard that starts automatically, on the step titled **Select a configuration method**, select the **Create a new configuration** option.
3. Follow the steps in the wizard to configure One Identity Quick Connect Sync Engine.

   If you want to store the configuration settings and synchronization data in a single SQL Server database, on the step titled **Specify where to store data**, clear the **Store sync data in a separate database** check box.

If you want to store the configuration settings and synchronization data in two separate databases, select that check box, and then specify the database in which you want to store the synchronization data.

Step 3: Import configuration settings

In this step, you use a tool supplied with One Identity Quick Connect Sync Engine 5.5.0 to import configuration settings from the SQL Server databases used by the earlier version of One Identity Quick Connect Sync Engine from which you upgrade. The configuration settings will be imported to the SQL Server databases you created in Step 2: Create new SQL Server databases.

To import configuration settings

1. On the computer on which you installed One Identity Quick Connect Sync Engine 5.5.0, start the Quick Connect Administration Console.
2. In the upper right corner of the Quick Connect Administration Console, click **Options | Import Configuration**.
3. Select the One Identity Quick Connect Sync Engine version whose configuration settings you want to import.

   Optionally, you can select the **Import sync history** check box to import the sync history along with the configuration settings.
4. Follow the steps in the wizard to complete the import operation.

   If the synchronization data you want to import is stored separately from the configuration settings, on the **Specify source SQL Server databases** step, select the **Import sync data from the specified database** check box, and then specify the database in the text box below.

Step 4: Upgrade Capture Agent on each DC

If you are using One Identity Quick Connect Sync Engine to synchronize passwords between an Active Directory domain and other connected data systems, upgrade Capture Agent installed on each domain controller in the source Active Directory domain.

To upgrade Capture Agent

1. On the domain controller, run one of the following files supplied with the One Identity Quick Connect Sync Engine 5.5.0 installation package:
   - In a 32-bit edition of Windows, run the file **QuickConnectCaptureAgent_x86.msi**.
   - In a 64-bit edition of Windows, run the file **QuickConnectCaptureAgent_x64.msi**.
2. Step through the wizard to complete the agent upgrade.

Silent installation

You can perform a silent installation of the following components:

- One Identity Quick Connect Sync Engine
- Capture Agent

Before performing a silent installation, check the *One Identity Quick Connect Sync Engine Release Notes* to make sure that your system meets the requirements for the components you want to install.

In this section:

- Silent installation of One Identity Quick Connect Sync Engine
- Silent installation of Capture Agent

Silent installation of One Identity Quick Connect Sync Engine

To perform a silent installation

- On a 32-bit system, enter the following syntax at a command prompt:

  ```
  msiexec /i "<Path to QuickConnectSyncEngine_x86.msi>" /qb
  INSTALLDIR="<Path to installation folder>" QCSVCUSERNAME="<Domain\UserName>"
  QCSVCPASSWORD="<Password>"
  ```

- On a 64-bit system, enter the following syntax at a command prompt:

  ```
  msiexec /i "<Path to QuickConnectSyncEngine_x64.msi>" /qb
  INSTALLDIR="<Path to installation folder>" QCSVCUSERNAME="<Domain\UserName>"
  QCSVCPASSWORD="<Password>"
  ```

In the above syntax:

Table 1: Arguments

Argument	Description
INSTALLDIR	Specifies the installation folder for the One Identity Quick Connect Sync Engine. When this argument is omitted, the following default installation folder is used: %ProgramFiles%\One Identity\Quick Connect
QCSVCUSERNAME	Specifies the user name of the account under which you want the Quick Connect Service to run. When this argument is omitted, the current user account is used.

Argument	Description
QCSVCPASSWORD	Specifies the password of the account you supplied in the QCSVCUSERNAME argument.

Silent installation of Capture Agent

To perform a silent installation

- On a 32-bit system, enter the following syntax at a command prompt:

  ```
  msiexec /i "<Path to QuickConnectCaptureAgent_x86.msi>" /qb
  INSTALLDIR="<Path to installation folder>" REBOOT="<Value>"
  ```

- On a 64-bit system, enter the following syntax at a command prompt:

  ```
  msiexec /i "<Path to QuickConnectCaptureAgent_x64.msi>" /qb
  INSTALLDIR="<Path to installation folder>" REBOOT="<Value>"
  ```

In the above syntax:

Table 2: Arguments

Argument	Description
INSTALLDIR	Specifies the installation folder for the Capture Agent. When this argument is omitted, the following default installation folder is used: %ProgramFiles%\One Identity\Quick Connect Capture Agent
REBOOT	Allows you to suppress a system restart in a situation where a restart is required for the Capture Agent installation to complete. To suppress the restart, use the following syntax: REBOOT="ReallySupress"

Communication ports

The following table lists the default communication ports used by One Identity Quick Connect Sync Engine:

Table 3: Default communication ports

Port	Protocol	Type of traffic	Direction of traffic
53	TCP/UDP	DNS	Inbound, outbound
88	TCP/UDP	Kerberos	Inbound, outbound
135	TCP	RPC endpoint mapper Port 135 is a dynamically allocated TCP port for RPC communication with Active Directory domain controllers. For more information about ports used for RPC communication, see the following Microsoft Support Knowledge Base articles at support.microsoft.com: Restricting Active Directory replication traffic and client RPC traffic to a specific port (article ID: 224196) How to configure RPC dynamic port allocation to work with firewalls (article ID: 154596) How to configure RPC to use certain ports and how to help secure those ports by using IPsec (article ID: 908472) The default dynamic port range for TCP/IP has changed in Windows Vista and in Windows Server 2008 (article ID: 929851)	Inbound, outbound
139	TCP	SMB/CIFS	Inbound, outbound
445	TCP	SMB/CIFS	Inbound, outbound
389	TCP/UDP	LDAP	Outbound
3268	TCP	LDAP	Outbound
636	TCP	SSL This port is only required if One Identity Quick Connect Sync Engine is configured to use SSL to connect to an Active Directory domain.	Outbound
3269	TCP	SSL	Outbound

Port	Protocol	Type of traffic	Direction of traffic
		This port is only required if One Identity Quick Connect Sync Engine is configured to use SSL to connect to an Active Directory domain.	
808	TCP	LDAP Quick Connect Capture Agent (only if One Identity Quick Connect Sync Engine is configured to synchronize user passwords from an Active Directory domain to other connected data systems.) Traffic between One Identity Quick Connect Sync Engine and Quick Connect Service	Inbound, outbound
7148	TCP	Quick Connect Capture Agent (only if One Identity Quick Connect Sync Engine is configured to synchronize user passwords from an Active Directory domain to other connected data systems)	Inbound, outbound

3

Getting started

Quick Connect Administration Console

The Quick Connect Administration Console is a graphical user interface that provides access to the One Identity Quick Connect Sync Engine functionality. You can use the Administration Console to connect One Identity Quick Connect Sync Engine to external data systems, manage existing connections, and perform data synchronization operations between the connected data systems. The Administration Console is installed as part of One Identity Quick Connect Sync Engine.

To start the Quick Connect Administration Console

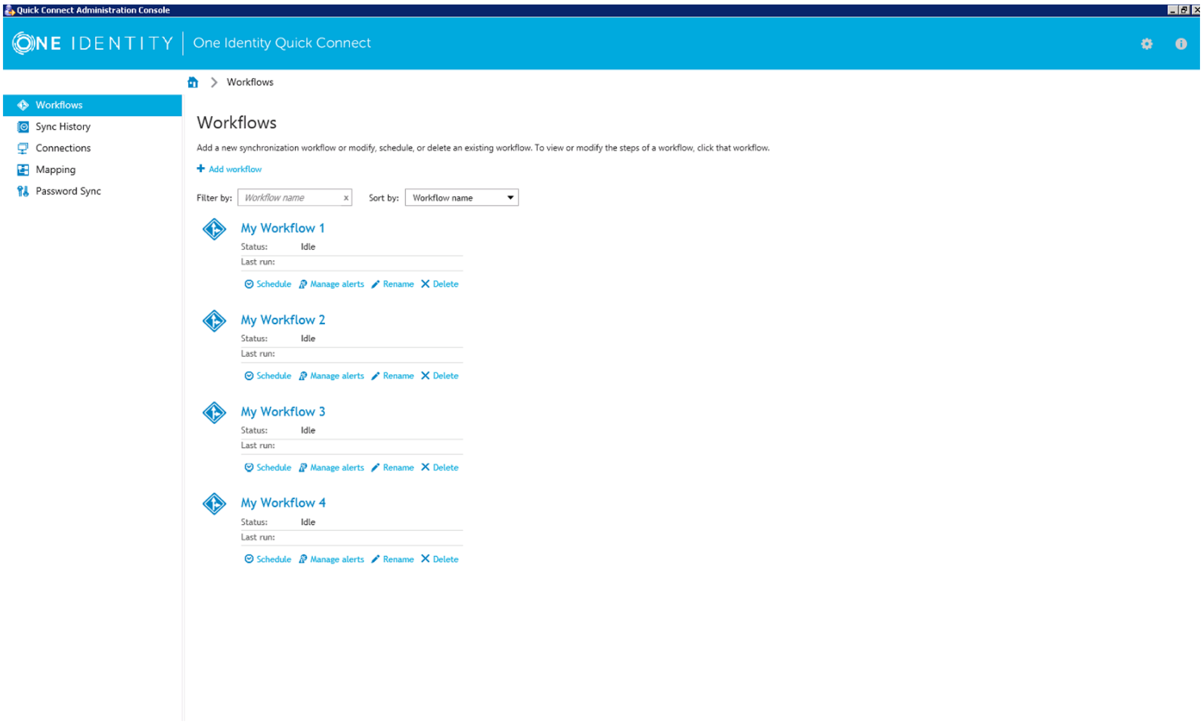
- Complete the steps related to your version of Windows:

Table 4: Steps to start Quick Connect Administration Console

Windows Server 2003 or Windows Server 2008	Windows Server 2012
1. Click **Start**. 2. Point to **All Programs | One Identity| Quick Connect**. 3. Click **Quick Connect Administration Console**.	• On the **Start** screen, click the **Quick Connect Administration Console** tile.

The Quick Connect Administration Console looks similar to the following:

Figure 1: Quick Connect Administration Console



Add a new synchronization workflow or modify, schedule, or delete an existing workflow. To view or modify the steps of a workflow, click that workflow.

In the upper right corner of the console, you can click the following items:

Table 5: Menu items

Item	Description
The Gear icon	Provides the following commands: **Configure Sync Engine.** Starts a wizard that helps you change the configuration settings of the current One Identity Quick Connect Sync Engine instance. **Import Configuration.** Starts a wizard that helps you to import configuration settings from a configuration file created by another instance of One Identity Quick Connect Sync Engine**.** **Export Configuration.** Starts a wizard that helps you to save the configuration profile of the current One Identity Quick Connect Sync Engine instance to a file. You can use this file to apply the saved configuration to other instances of One Identity Quick Connect Sync Engine 5.5.0 deployed in your environment. **Mail Profiles**. Allows you to add, edit, or delete mail profiles for sending notification emails about workflow runs. For more information on how to use the email notification, see Using workflow alerts.

Item	Description
	Diagnostic Logging. Allows you to specify settings for writing Quick Connect diagnostic data to the Quick Connect log file or Windows Event Log. **Communication Port**. Allows you to change the communication port number used by the One Identity Quick Connect Sync Engine.
The Information icon	Displays a window where you can view a list of installed Quick Connect connectors and connector usage statistics (such as the average and maximum number of licensed objects in the connection scope for each installed connector).

In this section:

- Workflows tab
- Sync History tab
- Connections tab
- Mapping tab
- Password Sync tab
- Configuring diagnostic logging

For more information about the elements you can use on these tabs, see the next subsections.

Workflows tab

Allows you to manage data synchronization workflows for connected data systems. A workflow can include a number of synchronization steps, each performing a specific data synchronization operation (provision, deprovision, or update). For more information on synchronization workflows and their steps, see Synchronizing identity data.

You can also use this tab to manage email notification settings for each existing synchronization workflow. For more information, see Using workflow alerts.

On the **Workflows** tab, you can use the following elements (some of these elements become available only after you create at least one workflow with one or more synchronization steps):

- **Add workflow**. Creates a new synchronization workflow.
- **Filter by**. Allows you to filter existing workflows by the letters or text you type in the text box. The filter applies to the workflow names.
- **Sort by**. Allows you to sort existing workflows by workflow name, last run time, or the number of synchronization steps.

- **<Workflow Name>**. Represents a synchronization workflow. You can click the workflow name to view and add, delete, or modify synchronization steps in that workflow.
- **Schedule**. Allows you to create a schedule for running the synchronization workflow.
- **Manage alerts**. Allows you to add, delete, or edit alerts for the synchronization workflow. An alert allows you to automatically send notification emails about the completion of a workflow run to specified recipients.
- **Rename**. Allows you to rename the synchronization workflow.
- **Delete**. Deletes the workflow.

Sync History tab

Allows you to view and selectively clean up the synchronization history. This is the history of synchronization workflow runs and object mapping operations. For more information, see Synchronization history.

On the **Sync History** tab, you can use the following elements:

- **Clean up now**. Allows you to selectively clean up sync history entries by specifying the age of the entries that you want to clean up.
- **Schedule cleanup**. Allows you to schedule a recurring cleanup operation for the sync history.
- **Workflow History**. Allows you to view a list of completed workflow runs and the details of objects that participated in a particular workflow run.
- **Mapping History**. Allows you to view a list of completed map and unmap operations and the details of objects that participated in those operations.
- **Search**. Allows you to search the One Identity Quick Connect Sync Engine synchronization history for completed provision, deprovision, update, and sync passwords operations. You can search by a number of criteria, such as the target connected data system and object type on which the operation was performed and the time period during which the operation completed.

Connections tab

Allows you to manage connections between the One Identity Quick Connect Sync Engine and the external data systems you want to use for data synchronization operations.

For instructions on creating connections to external data systems supported out of the box, see External data systems supported out of the box. For instructions on creating connections to other types of external data systems, see the documentation supplied with the Quick Connect package that supports the data system.

On the **Connections** tab, you can use the following elements (some of these elements become available only after you create at least one connection):

- **Add connection**. Allows you to create a new connection to an external data system.
- **Filter by**. Allows you to filter existing connections by the letters or text you type in the text box. The filter applies to the connection names.
- **Sort by**. Allows you to sort existing connections by connection name, name of the connector used, or the frequency of usage in synchronization workflow steps.
- **<Connection Name>**. Represents a connection to external data system. You can click a connection name to view or modify the corresponding connection settings.
- **Connection settings**. Allows you to view or modify settings for the connection.
- **Synchronization scope**. Allows you to view or modify synchronization scope for the connection.
- **Delete connection**. Deletes the connection.

Mapping tab

Allows you to manage mapping pairs and mapping rules for existing connections. To view or modify mapping pairs or rules for a connection, click the name of that connection on the **Mapping** tab. For more information on mapping pairs and rules, see Mapping objects.

On the **Mapping** tab, you can use the following elements (some of these elements become available only after you create at least one connection to an external data system):

- **Filter by**. Allows you to filter existing connections by the letters or text you type in the text box. The filter only applies to the connection names.
- **Sort by**. Allows you to sort existing connections by connection name, name of the connector used, or the frequency of usage in the synchronization workflow steps.
- **<Connection Name>**. Displays the name of a connection. You can click a connection name to view or modify the mapping settings for the corresponding connection.

When you click a connection name on this tab, you can manage mapping pairs for the connection by using the following elements (some of these elements become available after you create at least one mapping pair for the connection):

- **Add mapping pair**. Allows you to specify the types of objects in two connected systems for which you want to create a mapping pair.
- **<ObjectType1> - <ObjectType2>**. Represents a mapping pair and displays the object types that belong to the same mapping pair. You can click a mapping pair to view and change the scope of conditions where the object types belonging to that mapping pair will be mapped. To define these conditions, you can create mapping rules.
- **Schedule**. Allows you to schedule a recurring map operation for the current pair of objects.
- **Map now**. Allows you to manually run the map operation on the current pair

of objects.

- **Delete**. Deletes the mapping pair on which you click this link.

When you click a mapping pair, you can manage mapping rules for the mapping pair by using the following elements (some of these elements become available only after you create at least one mapping rule for the mapping pair):

- **Map now**. Allows you to manually run the map operation on the mapping pair by using the conditions specified in the existing mapping rules.
- **Unmap**. Allows you to unmap the objects that were earlier mapped according to the settings specified for the mapping pair.
- **Schedule mapping**. Allows you to schedule a recurring map operation for the mapping pair.
- **Add mapping rule**. Allows you to create a rule that will define a condition for mapping objects that belong to the mapping pair.
- **Delete rule**. Deletes the mapping rule on which you click this link.
- **Move up**. Moves the current mapping rule one position up in the list.
- **Move down**. Moves the current mapping rule one position down in the list.

Mapping rules are applied in the order they are listed.

Password Sync tab

Allows you to manage password sync rules to automate password synchronization from a specified Active Directory domain to other connected data systems. For more information, see Automated password synchronization.

On the **Password Sync** tab, you can use the following elements (some of these elements become available only after you create at least one password sync rule):

- **Add password sync rule**. Allows you to create a rule for synchronizing passwords from an Active Directory domain to another connected system.
- **Password sync settings**. Allows you to specify how many times you want to retry the password synchronization operation in the event of a failure. Also allows you to type a Windows PowerShell script to generate passwords for the target connected system. For more information, see Appendix B: Using a PowerShell script to transform passwords.
- **Delete rule**. Deletes the password sync rule on which you click this link.

Configuring diagnostic logging

In the Quick Connect Administration Console, you can configure a number of settings to write the One Identity Quick Connect Sync Engine diagnostic data to a separate log file or to the Windows Event Log.

To configure diagnostic logging

1. In the upper right corner of the Quick Connect Administration Console, select **Settings | Diagnostic Logging**.
2. In the dialog box that opens, use the following options:

Table 6: Diagnostic logging options

Option	Description
Windows Event Log level	Drag the slider to select one of the following options to write One Identity Quick Connect Sync Engine data to the Windows Event Log: • **Error, Warning, and Information**. Records errors, warnings, and information events generated by One Identity Quick Connect Sync Engine to the Windows Event Log. • **Error and Warning**. Records error and warning events generated by One Identity Quick Connect Sync Engine to the Windows Event Log. • **Error**. Records error events generated by One Identity Quick Connect Sync Engine to the Windows Event Log. • **Off**. Disables writing One Identity Quick Connect Sync Engine data to the Windows Event Log.
Quick Connect Sync Engine log file	Drag the slider to select one of the following logging levels for the One Identity Quick Connect Sync Engine log file: • **All Possible Events**. Writes detailed diagnostic data to the One Identity Quick Connect Sync Engine log file. • **Important Events**. Writes only essential events to the One Identity Quick Connect Sync Engine log file. • **Off**. Disables writing data to the One Identity Quick Connect Sync Engine log file.

3. When you are finished, click **OK** to apply your settings.

Steps to synchronize identity data

On a very high level, you need to complete the following steps to synchronize identity data between two external data systems:

1. Connect the One Identity Quick Connect Sync Engine to the data systems between which you want to synchronize identity data.

   For more information, see Connections to external data systems.

2. Configure synchronization scope for the connected data systems.

   For more information, see Modifying synchronization scope for a connection.

3. Create a synchronization workflow.

   For more information, see Creating a synchronization workflow.

4. Create one or more steps in the synchronization workflow, and, if necessary, define synchronization rules for these steps.

   For more information, see Managing workflow steps.

5. Run the synchronization workflow you have created.

   For more information, see Running a synchronization workflow.

You can also use the One Identity Quick Connect Sync Engine to automatically synchronize passwords from a specified Active Directory domain to other connected data systems. For more information, see Automated password synchronization.

4

Connections to external data systems

External data systems supported out of the box

This section provides information on working with external data systems supported by One Identity Quick Connect Sync Engine out of the box. For instructions on working with other types of external data systems, see the documentation supplied with the Quick Connect packages that support those data systems.

This section covers:

- Working with ActiveRoles Server
- Working with Quest One Identity Manager
- Working with One Identity Manager
- Creating a connection
- Renaming a connection
- Deleting a connection
- Modifying synchronization scope for a connection

- Using connection handlers
- Specifying password synchronization settings for a connection

Working with ActiveRoles Server

To create a connection to ActiveRoles Server, you need to use One Identity Quick Connect Sync Engine in conjunction with a special connector called *Quest ActiveRoles Server Connector*.

The Quest ActiveRoles Server Connector supports the following One Identity Quick Connect Sync Engine features:

Table 7: Supported features

Feature	
Bidirectional synchronization Allows you to read and write data in the connected data system.	Yes
Delta processing mode Allows you to process only the data that has changed in the connected data system since the last synchronization operation, thereby reducing the overall synchronization operation time.	Yes
Password synchronization Allows you to synchronize user passwords from an Active Directory domain to the connected data system.	Yes

The Quest ActiveRoles Connector supports linked attributes in the Active Directory schema. Linked attributes allow you to associate one object with another object. Linked attributes exist in pairs:

- **Forward link attribute**. This is a linked attribute that exists on a source object (example: the **member** attribute on the Group object). Forward link attributes can be single-valued or multivalued.
- **Back link attribute**. This is a linked attribute that can be specified on a target object (example: the **memberOf** attribute on the User object). Back link attributes are multivalued and they must have a corresponding forward link attribute. Back link attributes are not stored in Active Directory. Rather, they are calculated based on the corresponding forward link attribute each time a query is issued.

In this section:

- Creating an ActiveRoles Server connection
- Modifying an ActiveRoles Server connection

See also:

- Renaming a connection
- Deleting a connection
- Modifying synchronization scope for a connection
- Specifying password synchronization settings for a connection

Creating an ActiveRoles Server connection

One Identity Quick Connect Sync Engine supports ActiveRoles Server out of the box, so you can create connection to ActiveRoles Server after you install One Identity Quick Connect Sync Engine on your computer.

To create a new connection

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Add connection**, and then use the following options:
    - **Connection name**. Type a descriptive name for the connection.
    - **Use the specified connector**. Select **Quest ActiveRoles Server Connector**.
3. Click **Next**.
4. On the **Specify connection settings** page, use the following options:
    - **Connect to**. Allows you to specify the ActiveRoles Server Administration Service to be used by the Short Product Name. You can use one of the following options:
        - **Administration Service on the specified computer**. Type the name of the computer running the Administration Service you want the Short Product Name to use.
        - **Any Administration Service of the same configuration**. Specify any Administration Service whose database holds the necessary configuration: type the DNS name of the computer running that Administration Service. If ActiveRoles Server replication is used to synchronize configuration data, this must be any Administration Service whose database server acts as the Publisher for the configuration database.
    - **Access ActiveRoles Administration Service using**. Allows you to specify an authentication option to access the ActiveRoles Administration Service. You can use one of the following options:
        - **Quick Connect service account**. Allows you to access the Administration Service in the security context of the user account under which the Quick Connect Service is running.

- **Windows account**. Allows you to access the Administration Service in the security context of the user account whose user name and password you specify below this option.
- **Test Connection**. Allows you to verify the specified connection settings.

5. Click **Finish** to create a connection to Quest ActiveRoles Server.

Modifying an ActiveRoles Server connection

To modify connection settings

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Connection settings** below the existing Quest ActiveRoles Server connection you want to modify.
3. Expand **Specify connection settings** and modify settings as necessary.
4. You can use the following options:
    - **Connect to**. Allows you to specify the ActiveRoles Server Administration Service to be used by the Short Product Name. You can use one of the following options:
    - **Administration Service on the specified computer**. Type the name of the computer running the Administration Service you want the Short Product Name to use.
    - **Any Administration Service of the same configuration**. Specify any Administration Service whose database holds the necessary configuration: type the DNS name of the computer running that Administration Service. If ActiveRoles Server replication is used to synchronize configuration data, this must be any Administration Service whose database server acts as the Publisher for the configuration database.
    - **Access ActiveRoles Administration Service using**. Allows you to specify an authentication option to access the ActiveRoles Administration Service. You can use one of the following options:
    - **Quick Connect service account**. Allows you to access the Administration Service in the security context of the user account under which the Quick Connect Service is running.
    - **Windows account**. Allows you to access the Administration Service in the security context of the user account whose user name and password you specify below this option.
    - **Test Connection**. Allows you to verify the specified connection settings.
5. Click **Save**.

Working with Quest One Identity Manager

To create a connection to Quest One Identity Manager, you need to use One Identity Quick Connect Sync Engine in conjunction with a special connector called *Quest One Identity Manager Connector*.

The Quest One Identity Manager Connector supports the following One Identity Quick Connect Sync Engine features:

Table 8: Supported features

Feature	
Bidirectional synchronization Allows you to read and write data in the connected data system.	Yes
Delta processing mode Allows you to process only the data that has changed in the connected data system since the last synchronization operation, thereby reducing the overall synchronization operation time.	Yes
Password synchronization Allows you to synchronize user passwords from Quest One Identity Manager domain to the connected data system.	Yes

In this section:

- Creating a Quest One Identity Manager connection
- Modifying a Quest One Identity Manager connection
- Quest One Identity Manager Connector configuration file

See also:

- Renaming a connection
- Deleting a connection
- Modifying synchronization scope for a connection
- Specifying password synchronization settings for a connection

Creating a Quest One Identity Manager connection

One Identity Quick Connect Sync Engine supports Quest One Identity Manager out of the box, so you can create a connection to Identity Manager right after you install One Identity Quick Connect Sync Engine.

To connect to Identity Manager, One Identity Quick Connect Sync Engine requires certain Dynamic Link Library (DLL) files supplied with Identity Manager. Before creating a connection to Identity Manager make sure that One Identity Quick Connect Sync Engine can access these DLL files as described in Step 1: Provide access to Identity Manager DLLs.

To create a new connection to Identity Manager, complete these steps:

- Step 1: Provide access to Identity Manager DLLs
- Step 2: Configure a connection to Quest One Identity Manager

Step 1: Provide access to Identity Manager DLLs

Make sure that One Identity Quick Connect Sync Engine can access the required Identity Manager DLLs. Depending on the Identity Manager version to which you want to connect, perform the corresponding steps in the next table.

Table 9: Providing access to Identity Manager DLLs

Identity Manager 6.0	Identity Manager 6.1
Install One Identity Quick Connect Sync Engine on the Identity Manager 6.0 computer.	Do one of the following: Install Quest One Identity Manager API on one of the following: - One Identity Quick Connect Sync Engine computer - Connector Access Service computer if you want to use the Quest One Identity Manager Connector remotely. For more information on using remote connectors, see Using remote connectors. Quest One Identity Manager API is published as Knowledgebase Solution SOL100525 at the following link: support.quest.com/SolutionDetail.aspx?id=SOL100525&pr=Quest%20One%20Identity%20Manager&st=Submitted On the Identity Manager 6.1 computer, install one of the following: - One Identity Quick Connect Sync Engine - Connector Access Service and the Quest One Identity Manager Connector

Identity Manager 6.0	Identity Manager 6.1
If Identity Manager is installed to a non-default installation folder, complete the additional steps below this table.	If Identity Manager is installed to a non-default installation folder, complete the additional steps below this table.

If Identity Manager is installed to a non-default installation folder, complete the following additional steps:

1. Use a text editor (such as Notepad) to open the **ConnectorConfig.xml** file located in *<One Identity Quick Connect Sync Engine installation folder>***\Q1IMConnector**

   This is the file where Quest One Identity Manager connector saves its configuration settings. For more information on these settings, see Quest One Identity Manager Connector configuration file.

2. Create a new `<PathToOneIdentityManagerDlls>` XML element in the file and then type the path to the Identity Manager installation folder in that element.

   Example:

   ```
   <PathToOneIdentityManagerDlls>C:\IdentityManagerInstallationFolder</PathToOneIde
   ntityManagerDlls>
   ```

3. Save the changes, and then close the .xml file.

   Do one of the following:

- If you installed One Identity Quick Connect Sync Engine on the Identity Manager computer, restart the Quick Connect Service on that computer.

- If you installed the Connector Access Service on the Identity Manager computer, restart the service.

Step 2: Configure a connection to Quest One Identity Manager

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Add connection**, and then use the following options:
   a. **Connection name**. Type a descriptive name for the connection.
   b. **Use the specified connector**. Select **Quest One Identity Manager Connector**.
3. Click **Next**.
4. On the **Specify connection settings** page, use the following options:
   - **Database type**. Use this list to select the type of the database in which Quest One Identity Manager stores its data. You can select one of the following database types:
   - **Oracle**. Select this item if Quest One Identity Manager stores its data in a database hosted on Oracle Database.
   - **SQL Server**. Select this item if Quest One Identity Manager stores its data in a database hosted on Microsoft SQL Server.
   - **Server**. If you have selected **SQL Server** in the **Database type** list, type the SQL Server instance that hosts the database where Quest One Identity Manager stores its data. Use the following format: *<ComputerName>/<SQLServerInstanceName>*

     If you have selected **Oracle** in the **Database type** list, type the DNS name or IP address of the Oracle Database computer that hosts the database where Quest One Identity Manager stores its data.
   - **Port**. Type the number of port on which you want to connect to the Oracle Database computer that hosts the database where Quest One Identity Manager stores its data.
   - **Database name**. Type the name of the database where Quest One Identity Manager stores its data.
   - **Connect using**. Use this area to specify the account with which you want to connect to the computer that hosts the Quest One Identity Manager database.

     If you have selected **SQL Server** in the **Database type** list, select one of the following authentication methods to access the SQL Server computer that hosts the Quest One Identity Manager database:
   - **Use Quick Connect Service accoun**t. Allows you to access the SQL Server within the security context of the account under which the Quick Connect Service is running.

- **Use SQL Server authentication**. Allows you to specify the user name and password of an account registered on the SQL Server.

  If you have selected **Oracle** in the **Database type** list, type the login and password of the account under which you want to access the Oracle Database computer that hosts the Quest One Identity Manager database.

- **Test Connection**. Allows you to verify the specified connection settings.

5. Click **Finish** to create a connection to Quest One Identity Manager.

Modifying a Quest One Identity Manager connection

To modify connection settings

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Connection settings** below the existing Quest One Identity Manager connection you want to modify.
3. Expand **Specify connection settings** and use the following options to modify the settings as necessary:
   - **Database type**. Use this list to select the type of the database in which Quest One Identity Manager stores its data. You can select one of the following database types:
   - **Oracle**. Select this item if Quest One Identity Manager stores its data in a database hosted on Oracle Database.
   - **SQL Server**. Select this item if Quest One Identity Manager stores its data in a database hosted on Microsoft SQL Server.
   - **Server**. If you have selected **SQL Server** in the **Database type** list, type the SQL Server instance that hosts the database where Quest One Identity Manager stores its data. Use the following format: *<ComputerName>/<SQLServerInstanceName>*

     If you have selected **Oracle** in the **Database type** list, type the DNS name or IP address of the Oracle Database computer that hosts the database where Quest One Identity Manager stores its data.
   - **Port**. Type the number of port on which you want to connect to the Oracle Database computer that hosts the database where Quest One Identity Manager stores its data.
   - **Database name**. Type the name of the database where Quest One Identity Manager stores its data.
   - **Connect using**. Use this area to specify the account with which you want to connect to the computer that hosts the Quest One Identity Manager database.

     If you have selected **SQL Server** in the **Database type** list, select one of the following authentication methods to access the SQL Server computer that hosts the Quest One Identity Manager database:

- **Use Quick Connect Service accoun**t. Allows you to access the SQL Server within the security context of the account under which the Quick Connect Service is running.
- **Use SQL Server authentication**. Allows you to specify the user name and password of an account registered on the SQL Server.

If you have selected **Oracle** in the **Database type** list, type the login and password of the account under which you want to access the Oracle Database computer that hosts the Quest One Identity Manager database.

- **Test Connection**. Allows you to verify the specified connection settings.

4. Click **Save**.

Quest One Identity Manager Connector configuration file

Quest One Identity Manager connector saves its configuration settings in the **ConnectorConfig.xml** file located in the folder *<One Identity Quick Connect Sync Engine installation folder>***\Q1IMConnector**. You can edit the XML elements in the file to configure the various parameters of the Quest One Identity Manager Connector. The table below describes the XML elements you can edit.

Table 10: XML elements

XML element	Description

<PathToOneIdentityManagerDlls>	Specifies the path to the Quest One Identity Manager .dll files required for One Identity Quick Connect Sync Engine to connect to the Identity Manager.
	Example:
	`<PathToOneIdentityManagerDlls>`
	`C:\IdentityManagerDLLs`
	`</PathToOneIdentityManagerDlls>`

<ExcludeDeletedObjects>	Specifies how One Identity Quick Connect Sync Engine will treat objects marked as deleted in Identity Manager. This element can take one of the following values: • **TRUE**. Specifies to ignore deleted objects during data synchronization operations. • **FALSE**. Specifies to process deleted objects during data synchronization operations.

XML element	Description

	Example:
	`<ExcludeDeletedObjects>`
	`TRUE`
	`</ExcludeDeletedObjects>`

<PasswordAttributes>	Specifies the default Identity Manager attribute to be used for storing passwords for objects of a particular type. Specifying an attribute for storing passwords in the One Identity Quick Connect Sync Engine GUI overrides the value set in this XML element.
	Example:
	`<PasswordAttributes>`
	`   <PasswordAttributeDefinitions>`
	`      <PasswordAttributeDefinition`
	`objectType="Person"`
	`attribute="CentralPassword" />`
	`   </PasswordAttributeDefinitions>`
	`</PasswordAttributes>`

<ReadFullSync>	Specifies a value of the FullSync variable for Read operations performed in Identity Manager.
<CreateFullSync>	Specifies a value of the FullSync variable for Create operations performed in Identity Manager.
<ModifyFullSync>	Specifies a value of the FullSync variable for Modify operations performed in Identity Manager.
<DeleteFullSync>	Specifies a value of the FullSync variable for Delete operations performed in Identity Manager.
<ObjRefFullSync>	Specifies a value of the FullSync variable for Modify Object Reference operations performed in Identity Manager.
<SyncStatusFullSync>	Specifies a value of the FullSync variable for Sync Status operations performed in Identity Manager.

For more information about the FullSync variable and the values it can take, see the Quest One Identity Manager documentation.

Working with One Identity Manager

To create a connection to One Identity Manager, you need to use One Identity Quick Connect Sync Engine in conjunction with a special connector called *One Identity Manager Connector*.

The One Identity Manager Connector supports the following One Identity Quick Connect Sync Engine features:

Table 11: Supported features

Feature	
Bidirectional synchronization Allows you to read and write data in the connected data system.	Yes
Delta processing mode Allows you to process only the data that has changed in the connected data system since the last synchronization operation, thereby reducing the overall synchronization operation time.	Yes
Password synchronization Allows you to synchronize user passwords from One Identity Manager domain to the connected data system.	No

In this section:

- Creating a One Identity Manager connection
- Modifying a One Identity Manager connection
- One Identity Manager Connector configuration file

See also:

- Renaming a connection
- Deleting a connection
- Modifying synchronization scope for a connection
- Specifying password synchronization settings for a connection

Creating a One Identity Manager connection

One Identity Quick Connect Sync Engine supports One Identity Manager out of the box, so you can create a connection to Identity Manager just after you install One Identity Quick Connect Sync Engine.

To create a new connection

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Add connection**, and then use the following options:
   a. **Connection name**. Type a descriptive name for the connection.
   b. **Use the specified connector**. Select **One Identity Manager Connector**.
3. Click **Next**.
4. On the **Specify connection settings** page, use the following options:
   - **Application Server URL**. Specify the address of the One Identity Manager application server to which you want to connect.
   - **Authentication module**. Identifies the One Identity Manager authentication module that is to be used to verify the connection’s user ID and password.
   - **User name**. Specify the user ID for this connection.
   - **Password**. Specify the password of the user ID for this connection.
   - **Test Connection**. Click to verify the specified connection settings.
5. Click **Next**.

   The One Identity Manager modules, target systems, and containers are displayed.
6. Select the required One Identity Manager modules.

   NOTE: The One Identity Manager target systems and One Identity Manager containers are applicable only for the Target System Base module (UNS..B tables).
7. Click **Finish** to create a connection to One Identity Manager.

Modifying a One Identity Manager connection

To modify connection settings

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Connection settings** below the existing One Identity Manager connection you want to modify.
3. Expand **Specify connection settings** and use the following options to modify the settings as necessary:
   - **Application Server URL**. View or change the address of the One Identity Manager application server for this connection.
   - **Authentication module**. Identifies the One Identity Manager authentication module that is used to verify the connection’s user ID and password.
   - **User name**. View or change the user ID for this connection.
   - **Password**. Specify the password of the user ID for this connection.
   - **Test Connection**. Click to verify the specified connection settings.

4. Click **Next**.

   The One Identity Manager modules, target systems, and containers are displayed.

5. Select the required One Identity Manager modules.

   > NOTE: The One Identity Manager target systems and One Identity Manager containers are applicable only for the Target System Base module (UNS..B tables).

6. Click **Finish** to create a connection to One Identity Manager.

One Identity Manager Connector configuration file

One Identity Manager connector saves its configuration settings in the file **ConnectorConfig.xml** located in the folder *<One Identity Quick Connect Sync Engine installation folder>***\D1IMConnector**. You can edit the XML elements in the file to configure the various parameters of the One Identity Manager Connector. The table below describes the XML elements you can edit.

Table 12: XML elements

XML element	Description

<ExcludeDeletedObjects>	Specifies how One Identity Quick Connect Sync Engine will treat objects marked as deleted in Identity Manager. This element can take one of the following values:
	• **TRUE**. Specifies to ignore deleted objects during data synchronization operations.
	• **FALSE**. Specifies to process deleted objects during data synchronization operations.
	Example:
	`<ExcludeDeletedObjects>`
	`TRUE`
	`</ExcludeDeletedObjects>`

<PasswordAttributes>	Specifies the default Identity Manager attribute to be used for storing passwords for objects of a particular type. Specifying an attribute for storing passwords in the One Identity Quick Connect Sync Engine GUI overrides the value set in this XML element.
	Example:
	`<PasswordAttributes>`
	`   <PasswordAttributeDefinitions>`

XML element	Description

	`<PasswordAttributeDefinition objectType="Person" attribute="CentralPassword" />`
	`</PasswordAttributeDefinitions>`
	`</PasswordAttributes>`

<ReadFullSync>	Specifies a value of the FullSync variable for Read operations performed in Identity Manager.
<CreateFullSync>	Specifies a value of the FullSync variable for Create operations performed in Identity Manager.
<ModifyFullSync>	Specifies a value of the FullSync variable for Modify operations performed in Identity Manager.
<DeleteFullSync>	Specifies a value of the FullSync variable for Delete operations performed in Identity Manager.
<ObjRefFullSync>	Specifies a value of the FullSync variable for Modify Object Reference operations performed in Identity Manager.
<SyncStatusFullSync>	Specifies a value of the FullSync variable for Sync Status operations performed in Identity Manager.

For more information about the FullSync variable and the values it can take, see the Quest One Identity Manager documentation.

Using remote connectors

You can install and use Quick Connect connector packages not only on the One Identity Quick Connect Sync Engine computer (locally), but also on remote computers that do not host the One Identity Quick Connect Sync Engine. Connectors installed on remote computers are called *remote connectors*. A remote connector provides the same functionality as a locally installed connector.

One Identity Quick Connect Sync Engine communicates with a remote connector via a single port. For this reason, using a remote connector makes it easier for you to configure a connection to an external data system in a situation where it is separated from the One Identity Quick Connect Sync Engine computer by a firewall.

Consider a scenario where you want to synchronize data between two Active Directory domains that are separated by a firewall. In this scenario, you can install the One Identity Quick Connect Sync Engine in one domain, and then deploy the Active Directory Connector on a domain controller in the other domain. Then, ensure the firewall allows traffic on the port used for communications between the One Identity Quick Connect Sync Engine and the remotely installed Active Directory Connector.

In this section:

- Steps to deploy a remote connector
- Creating a connection using a remote connector

Steps to deploy a remote connector

The key component that enables One Identity Quick Connect Sync Engine to access remote connectors and communicate with them is called the *Connector Access Service*. Each computer on which you want to install and use remote connectors must be running the Connector Access Service. The Connector Access Service is supplied with the One Identity Quick Connect Sync Engine as a standalone component.

To deploy a remote connector, complete these steps:

- Step 1: Install Connector Access Service
- Step 2: Install connector

Step 1: Install Connector Access Service

To install the Connector Access Service

1. Ensure the remote computer meets the system requirements for installing the Connector Access Service.

   For details, see the *One Identity Quick Connect Sync Engine Release Notes*.

2. On the remote computer, run one of the following files supplied with the One Identity Quick Connect Sync Engine:

   - If the remote computer is running a 32-bit edition of Windows, run the **QuickConnectConnectorAccessService_x86.msi** file.
   - If the remote computer is running a 64-bit edition of Windows, run the **QuickConnectConnectorAccessService_x64.msi** file.

3. Follow the steps in the setup wizard to complete the Connector Access Service installation.

Step 2: Install connector

In order you could use a connector remotely, you need to install it on:

- The remote computer on which you have deployed the Connector Access Service.
- The computer on which you plan to use the Quick Connect Administration Console to create connections.

For instructions on installing a connector, see the documentation supplied with the Quick Connect connector pack that includes the connector.

Creating a connection using a remote connector

Before creating a new connection, make sure you deploy the connector as described in Steps to deploy a remote connector.

To create a connection using a remote connector

1. Start the Quick Connect Administration Console.
2. On the **Connections** tab, click **Add connection**.
3. In the **Connection name** text box, type a descriptive name for the connection.
4. From the **Use the specified connector list**, select the connector you want to use.
5. Click to expand the **Remote connector access** element, and then use the following options:
    - **Use remote connector**. Select this check box to use the connector installed on a remote computer.
    - **Connector host**. Type the Fully Qualified Domain Name (FQDN) of the computer on which the remote connector is installed.
    - **Port**. Type the port number on which you want the One Identity Quick Connect Sync Engine to access the remote connector. By default, this is port 8080.
        - **Connect using**. Specify an account under which to access the remote connector. The account must be a local administrator on the computer where the remote connector is installed. Select one of the following:
            - **Quick Connect Service account**. Allows you to access the remote connector using the account under which the Quick Connect Service is running on the One Identity Quick Connect Sync Engine computer.
            - **Windows account**. Allows you to type the user name and password of the account with which you want to access the remote connector.
    - **Verify Settings**. Click this button to verify that One Identity Quick Connect Sync Engine can access the remote connector using the settings you have specified.
6. Step through the wizard to complete the connection creation.

For more information on other options available in the wizard, see the documentation for the connector you use.

Creating a connection

To create a connection

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Add connection**.
3. On the wizard page that opens, use the following options:
   - **Connection name**. Type a descriptive name for the connection being created.
   - **Use the specified connector**. From this list, select the connector you want to use.
   - **Remote connector access**. Expand this element to specify settings to access the connector installed on a remote computer. For more information, see Using remote connectors.
4. Follow the steps in the wizard to create a connection.

For information on the options you can use in the subsequent steps of the wizard, see the documentation for the Quick Connect package that includes the connector you have selected.

Renaming a connection

To rename a connection

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click the name of the existing connection you want to rename.
3. On the **General** tab, edit the connection name in the **Connection name** box.
4. Click **Save**.

Deleting a connection

To delete a connection

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Locate the connection you want to delete, and then click **Delete connection** for that connection.
3. When prompted, confirm that you want to delete the connection.

Modifying synchronization scope for a connection

For each connected data system, you can modify the scope of objects participating in the data synchronization operations.

To modify the synchronization scope

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Locate the connection for which you want to modify the synchronization scope, and then click
   Synchronization scope.
3. Use the following options to modify the synchronization scope:
   - **Include objects from selected containers only**. Select the check boxes next to the containers that hold the objects you want to participate in data synchronization operations. Note that this option may be unavailable for some types of connected data systems, such as Microsoft SQL Server or Oracle Database.
   - **Objects must meet these conditions**. Set up a list of conditions that objects must meet in order to participate in data synchronization operations.
4. When you are finished, click **Save**.

Using connection handlers

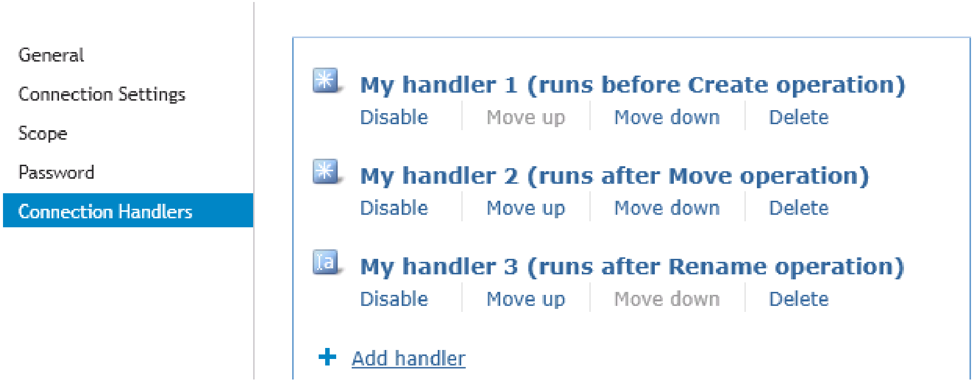
Connection handlers allow you to automatically perform specific actions on connected data systems before, after, or instead of specific data synchronization operations (such as create, modify, move, rename, delete, or password synchronization operation). When creating a connection handler, you can specify the action you want to perform and set the conditions for triggering the action.

Out of the box, One Identity Quick Connect Sync Engine includes only one predefined handler type that can execute your custom PowerShell script and thus perform the action you want.

> IMPORTANT: If the predefined connection handler is configured to run your PowerShell script instead of a data synchronization operation, the script must return a system entry object.

You can also develop and implement your own handler types. For more information, see the Software Development Kit (SDK) supplied with this One Identity Quick Connect Sync Engine version.

To create, modify, or delete handlers for a connection, you can use the **Connection Handlers** tab in the connection settings:



This tab provides the following elements:

- **Add handler**. Starts a wizard that helps you add a new connection handler. By default, the wizard creates a new handler that allows you to run your PowerShell script.
- **Disable**. Disables the connection handler.
- **Enable**. Enables the connection handler.
- **Move up**. Moves the connection handler one position up in the list.
- **Move down**. Moves the connection handler one position down in the list.
- **Delete**. Deletes the connection handler.

To create a connection handler

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click the name of the connection for which you want to create a handler, and then click the **Connection Handlers** tab.
3. Click **Add handler**, and then follow the steps in the wizard to create your handler.

To modify a connection handler

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click the name of the connection for which you want to modify a handler, and then click the **Connection Handlers** tab.
3. Click the name of the handler you want to modify, and then modify the handler settings as necessary. When you are finished, click **OK**.

   You can also do the following:

   - **Change the order in which handlers are activated**. One Identity Quick Connect Sync Engine activates handlers in the order in which they appear in the list. To move a handler in the list, use the **Move up** and **Move down** links below the handler.
   - **Disable or enable handlers**. You can enable or disable existing handlers. To do so, use the **Enable** or **Disable** link below the handler.
4. When you are finished, click **Save**.

To delete a connection handler

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click the name of the connection for which you want to delete a handler, and then click the **Connection Handlers** tab.
3. Click **Delete** below the handler you want to delete.

Specifying password synchronization settings for a connection

For each connected data system that supports password synchronization, you can set password synchronization settings. These settings allow you to enable or disable password synchronization and manage passwords in the data system by using Quest Password Manager.

Optionally, you can use the password synchronization settings to type a custom Windows PowerShell script you want to run each time the password synchronization completes for the connected data system.

To specify password synchronization settings

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click the name of the connection for which you want to modify password synchronization settings.
3. Open the **Password** tab, and use the following options to modify the password synchronization settings as necessary:
    - **Synchronize and manage passwords**. Allows you to enable or disable password synchronization for this connection. Selecting this check box also allows you to manage passwords in the connected data system by using Quest Password Manager. For more information about this product, please visit www.quest.com/password-manager.
    - **Synchronize passwords for objects of this type**. Allows you to specify an object type that will participate in password synchronization. Click **Select** next to this text box, and then specify the object type you want. This option is only available for certain types of connected systems, such as LDAP directory service.
        - **Password synchronization method**. Allows you to select a password synchronization method. This option is only available for certain types of connected systems, such as LDAP directory service. You can select one of the following methods:

    - **Write password to this attribute**. Displays the object attribute in which the object password will be stored. To specify a different attribute, click **Select** next to the text box in this option.
    - **Use LDAP extended operation**. Allows you to automate the synchronization of user passwords in the connected data system regardless of the form of the authentication identity or the password storage mechanism used (for example, in the case of non-directory storage of passwords).
  - **Configure Query**. Allows you to use an SQL query to specify the data you want to participate in the password synchronization. Click **Configure**, and then type your SQL query. This option is only available for certain types of connected systems, such as SQL Server or Oracle Database. For a sample SQL query, see the documentation supplied with the Quick Connect connector pack you are using.

4. When you are finished, click **Save**.

Synchronizing identity data

Getting started with identity data synchronization

To synchronize identity data between connected data systems, you can use *synchronization workflows* and *synchronization steps*. A *synchronization workflow* is a set of data synchronization operations called *synchronization steps.* A workflow can include one or more steps. Each synchronization step defines a synchronization operation to be run between the source and target connected data systems. To manage workflows and their steps, you can use the **Workflows tab in the Quick Connect Administration Console.**

You can configure a synchronization step to perform one of the following operations:

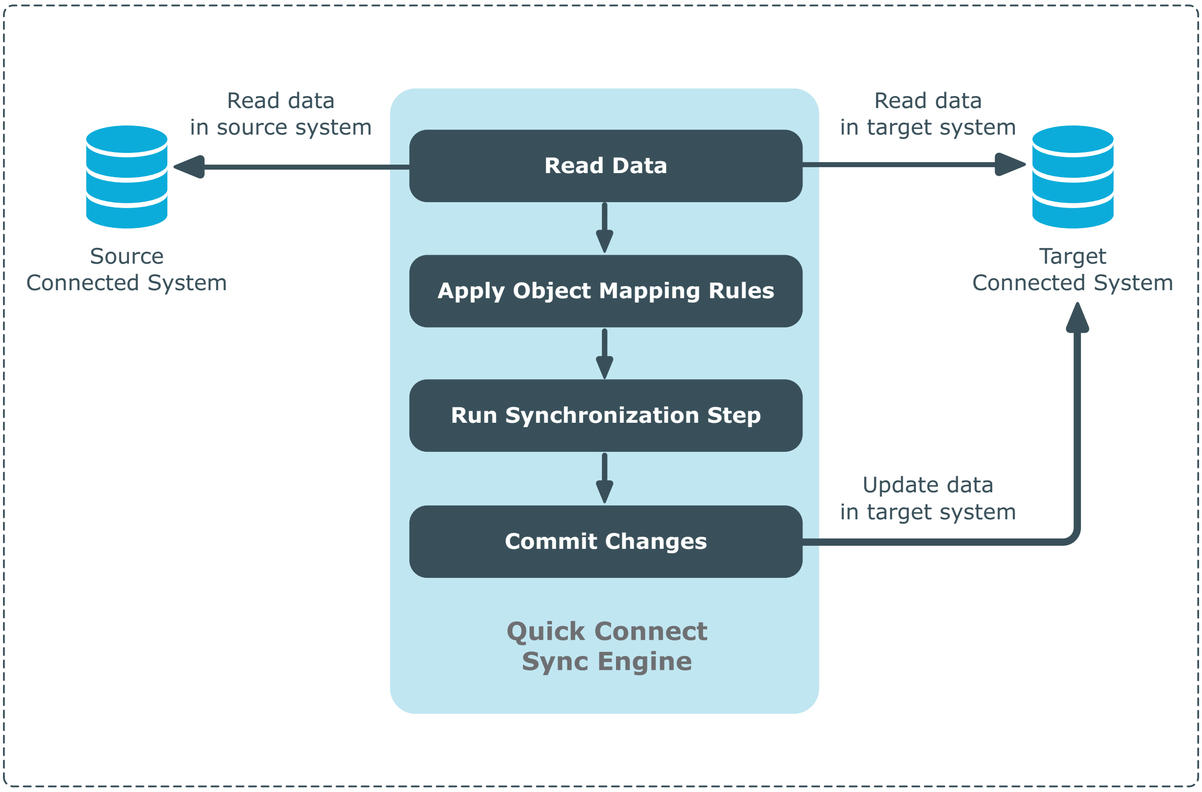
- **Provision**. Creates objects in the target data system based on the changes made to specific objects in the source data system. When creating a new object in the target data system, One Identity Quick Connect Sync Engine generates initial values for the object attributes using the attribute population rules you have configured.
- **Update**. Modifies object attributes in the target data system based on the changes made to specific objects in the source data system. To specify the objects that will participate in the update operation you can use object mapping rules. For more information, see Mapping objects.
- **Deprovision**. Modifies or removes objects in the target data system after their counterparts have been disconnected from the source data system. One Identity Quick Connect Sync Engine can be configured to remove target objects permanently or change them to a specific state. To specify the objects that will participate in the deprovision operation you can use object mapping rules. For more information, see Mapping objects.

When configuring a synchronization step you can specify the following:

- Containers to which you want to provision or move objects.
- Settings to generate names for objects being created or modified.
- Settings to synchronize group memberships.
- Settings to synchronize attribute values.

To synchronize identity data between two data systems, you need to create a synchronization workflow, populate the workflow with synchronization steps, and then run the workflow manually or schedule the workflow run. The following figure illustrates how One Identity Quick Connect Sync Engine synchronizes identity data in connected data systems:

Identity Data Synchronization



Read data in source system
Read data in target system
Source Connected System
Read Data
Target Connected System
Apply Object Mapping Rules
Run Synchronization Step
Update data in target system
Commit Changes
Quick Connect Sync Engine

Running a workflow causes One Identity Quick Connect Sync Engine to read data in the source and target data systems according to the settings in the workflow steps and prepare a list of changes to be made in the target system. Then, you can commit these changes to the target data system.

Running a workflow manually allows you to review a list of changes before committing them to the target data system. A scheduled workflow run always commits changes to the target data system automatically.

You can configure as many synchronization workflows as needed, each performing its own set of synchronization steps.

In this chapter:

- Managing synchronization workflows
- Managing workflow steps

Managing synchronization workflows

In this section:

- Creating a synchronization workflow
- Running a synchronization workflow
- Renaming a synchronization workflow
- Deleting a synchronization workflow

Creating a synchronization workflow

To create a synchronization workflow

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click **Add workflow**.
3. Use the **Synchronization workflow name** text box to type a name for the workflow being created.
4. Click **OK**.

   The new workflow appears on the **Workflows** tab.

   After you have created a workflow, you need to populate it with one or more synchronization steps. For more information, see Managing workflow steps.

Running a synchronization workflow

After you have created a synchronization workflow and populated it with one or more steps, you can run the workflow. Before running a workflow, you can select the workflow steps you want to run. A workflow can be run manually or automatically on a recurring schedule.

In this section:

- Running a workflow manually
- Running a workflow on a recurring schedule
- Disabling a workflow run schedule

Running a workflow manually

This method allows you to select specific steps in a workflow and run them. You can also specify how you want to commit the changes to the target data system: automatically or manually. With the manual method you can review a list of changes before committing them to decide whether or not you want these changes in the target system.

To run a workflow manually

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow you want to run.
3. Click **Run now**.
4. Select the check boxes next to the workflow steps you want to run.
5. If you want to automatically commit the changes made by the workflow run, select the **Automatically commit changes** check box. If you want to review the changes before committing them, leave this check box cleared.
6. Click one of the following to run the workflow:
    - **Full Run**. With this option, One Identity Quick Connect Sync Engine retrieves the data required to run the synchronization workflow from the connected data systems.
    - **Quick Run**. With this option, One Identity Quick Connect Sync Engine first tries to run the synchronization workflow by using the data that is available in the local cache. If the local cache is missing or cannot be used to run the workflow, then One Identity Quick Connect Sync Engine retrieves the required data from the connected data systems.

Running a workflow on a recurring schedule

This method allows you to create a recurring schedule to automatically run specific steps in a synchronization workflow.

When scheduling a workflow, you can choose the workflow steps to run, specify how frequently you want to run the steps, and set the date and time when you want the run schedule to come into effect. If you have two or more One Identity Quick Connect Sync Engine instances installed in your environment, you can also select a Quick Connect Service to be used for running the workflow.

A scheduled workflow automatically commits changes to the target data system.

To run a workflow on a recurring schedule

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click **Schedule** below the name of the workflow you want to run on a recurring schedule.

3. In the dialog box that opens, select the **Schedule the task to run** check box, and then specify a schedule.
4. If there are several One Identity Quick Connect Sync Engine instances deployed in your environment, under **Run the task on**, select the computer that hosts the Quick Connect Service you want to use for running the workflow.
5. Expand **Workflow Steps**, and then select the check boxes next to the workflow steps you want to run on the schedule.
6. Click **OK** to activate the schedule.

Disabling a workflow run schedule

To disable a workflow run schedule

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click **Schedule** below the workflow for which you want to disable the run schedule.
3. In the dialog box that opens, clear the **Schedule the task to run** check box.
4. Click **OK** to disable the schedule.

Renaming a synchronization workflow

To rename a synchronization workflow

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click **Rename** below the workflow.
3. Use the **Synchronization workflow name** text box to type a new workflow name.
4. Click **OK** to apply the change.

Deleting a synchronization workflow

To delete a synchronization workflow

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click **Delete** below the workflow.
3. When prompted, confirm that you want to delete the workflow.

Managing workflow steps

In this section:

Creating a provisioning step

To create a provisioning step

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to create a provisioning step.

   If necessary, create a new workflow. For more information, see Creating a synchronization workflow.
3. Click **Add synchronization step**.
4. Select **Provision**, and then click **Next**.
5. Specify the provision source by using these options:
   - **Source connected system**. Allows you to choose a source data system for the provision operation. Click **Specify** to select a data system connected earlier or add and select a new data system.
   - **Source object type**. Allows you to specify the object type you want to use as a source for the provision operation. Click **Select** to specify an object type.
   - **Provisioning Criteria**. Allows you to narrow the scope of source data system objects that participate in the provisioning step. Expand **Provisioning Criteria** to specify the containers that hold the source objects you want to participate in the step. You can also specify additional conditions to include objects into the scope.
6. Click **Next**.
7. Specify the provision target by using these options:
   - **Target connected system**. Allows you to choose a target data system for the provision operation. Click **Specify** to select a data system connected earlier or

add and select a new data system.

- **Target object type**. Allows you to specify the target data system object type to which you want to provision objects from the source data system. Click **Select** to specify an object type.
    - **Target container**. Allows you to specify the target data system container in which you want to create objects. Click the down arrow on the button, and then select one of the following:
        - **Browse**. Click to locate and select a single target container.
        - **PowerShell Script**. Click to compose a PowerShell script that calculates the target container name.
        - **Rule**. Click to configure a set of rules for selecting target containers.
        - **Use Mapping**. Click to define a target container based on the mapping of the source object.
        - **Clear**. Click to use an empty value.
- **Rules to generate unique object name**. Allows you to set up a list of rules to generate a unique name for each object being provisioned. For more information, see Generating object names by using rules.

8. Click **Next**.
9. Specify rules to provision objects into the target data system. You can use the following options:
    - **Initial Attribute Population Rules**. Expand this element to specify how you want to populate the attributes of provisioned objects. For more information, see Modifying attribute values by using rules.
    - **Initial Password**. Expand this element to specify an initial password for each provisioned object.
    - **User Account Options**. Expand this element to specify settings for the user accounts to be created.
10. Click **Finish** to create the provisioning step.

You can modify the settings of an existing synchronization step. For more information, see Modifying a step.

Creating an updating step

To create an updating step

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to create an updating step.

    If necessary, create a new workflow. For more information, see Creating a synchronization workflow.

3. Click **Add synchronization step**.
4. Select **Update**, and then click **Next**.
5. Specify the update operation source by using these options:
   - **Source connected system**. Allows you to choose a source data system for the update operation. Click **Specify** to select a data system connected earlier or add and select a new data system.
   - **Source object type**. Allows you to specify the data system object type you want to use as a source for the update operation. Click **Select** to specify an object type.
   - **Updating Criteria**. Allows you to narrow the scope of source data system objects that will participate in the updating step. Expand **Updating Criteria** to specify the containers that hold the source objects you want to participate in the step. You can also specify additional criteria for selecting source objects.
6. Click **Next**.
7. Specify an update target by using these options:
   - **Target connected system**. Allows you to choose a target connected system for the update operation. Click **Specify** to select a data system connected earlier or add and select a new data system.
   - **Target object type**. Allows you to specify what type of objects you want to update in the target data system. Click **Select** to specify an object type.
8. Click **Next**.
9. Specify rules to update objects in the target data system. You can use the following options:
   - **Rules to Modify Object Attributes**. Allows you to set up a list of rules to modify specific attributes of objects in the target data system. For more information, see Modifying attribute values by using rules.
     - **Rules to Move Objects**. Allows you to specify the location to which you want to move objects. Click the down arrow on the button, and then select one of the following:
       - **Browse**. Click to locate and select a single target container.
       - **PowerShell Script**. Click to compose a PowerShell script that calculates the target container name.
       - **Rule**. Click to configure a set of rules for selecting target containers.
       - **Use Mapping**. Click to define a target container based on the mapping of the source object.
       - **Clear**. Click to use an empty value.
   - **Rules to Rename Objects**. Allows you to set up a list of rules to rename objects in the result of the update operation. For more information, see Generating object names by using rules.
10. Click **Finish** to create the updating step.

You can modify the settings of an existing synchronization step. For more information, see Modifying a step.

Creating a deprovisioning step

To create a deprovisioning step

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to create a deprovisioning step.

   If necessary, create a new workflow. For more information, see Creating a synchronization workflow.
3. Click **Add synchronization step**.
4. Select **Deprovision** and then click **Next**.
5. Specify a deprovisioning source and criteria by using the following options:
   - **Source connected system**. Allows you to choose a source data system for the deprovision operation. Click **Specify** to select a data system connected earlier or add and select a new data system.
   - **Source object type**. Allows you to specify the data system object type you want to use as a source for the deprovision operation. Click **Select** to specify an object type.
   - **Deprovision target objects if**. Allows you to specify criteria for deprovisioning objects in the target data system.
6. Click **Next**.
7. Specify a deprovisioning target by using the following options:
   - **Target connected system**. Allows you to choose a target data system for the deprovision operation. Click **Specify** to select a data system connected earlier or add and select a new data system.
   - **Target object type**. Allows you to specify what type of objects you want to deprovision in the target data system. Click **Select** to specify an object type.
8. Click **Next**.
9. Select a method to deprovision objects in the target data system. You can select **Delete target objects** to delete target objects or **Modify target objects** to modify target objects using the rules configured in the following options:
   - **Rules to Modify Object Attributes**. Expand this option to set up a list of rules to modify object attributes in the target data system. For more information, see Modifying attribute values by using rules.
     - **Rules to Move Objects**. Expand this option to specify the location to which you want to move objects. Click the down arrow on the button, and then select one of the following:

        - **Browse**. Click to locate and select a single target container.
        - **PowerShell Script**. Click to compose a PowerShell script that calculates the target container name.
        - **Rule**. Click to configure a set of rules for selecting target containers.
        - **Use Mapping**. Click to define a target container based on the mapping of the source object.
        - **Clear**. Click to use an empty value.
    - **Rules to Rename Objects**. Expand this option to set up a list of rules to rename objects.

10. Click **Finish** to create the deprovisioning step.

    You can modify the settings of an existing synchronization step. For more information, see Modifying a step.

Modifying a step

To modify an existing step

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to modify a step.
3. Click the name of the step you want to modify.
4. Use the following tabs to modify the step as necessary:
    - General Options tab
    - Source tab
    - Target tab
    - Provisioning Rules tab
    - Deprovisioning Rules tab
    - Updating Rules Tab
    - Step Handlers tab

    For more information on these tabs, see the next subsections.
5. When you are finished, click **Save** to apply your changes.

General Options tab

On this tab you can rename the step, specify a method for processing data in the source and target connected systems, and specify conditions to stop data processing.

This tab has the following elements:

- **Step name**. Allows you to rename the step: type a new step name in this text box.
- **Specify how to process data in connected systems**. Allows you to select one of the following methods for processing data in the source and target data systems:
    - **Process all data**. If you select this method, each run of the step will process all data in the configured synchronization scope.
    - **Process delta from last run**. If you select this method, each run of the step will process only the data that has changed in the configured synchronization scope since the last run.
- **Stop data processing if**. Allows you to specify the conditions where you want to stop data processing in the source and target data systems.

Source tab

Allows you to view information about the source connected system and source object type specified for the synchronization step. You can also view or modify the criteria used to perform the provision, deprovision, or update operation in the step.

For all types of synchronization steps (provisioning, deprovisioning, and updating) this tab provides the following options:

- **Source connected system**. Displays the name of the source data system.
- **Source object type**. Displays the object type that is used as a source for the synchronization step.

For deprovisioning steps, this tab also provides the **Deprovision target objects if** option. It allows you to modify the criteria used for triggering the deprovision operation in the target data system.

For provisioning steps, this tab also provides the **Provisioning Criteria** option. It allows you to modify the scope of source data system objects that participate in the provisioning step. Expand **Provisioning Criteria** to modify the list of containers that hold the source objects you want to participate in the step. Also you can specify additional criteria for selecting source objects.

For updating steps, this tab also provides the **Updating Criteria** option. It allows you to modify the scope of source data system objects that participate in the updating step. Expand **Updating Criteria** to specify the containers that hold the source objects you want to participate in the step. You can also specify additional criteria for selecting source objects.

Target tab

Allows you to view information about the target connected system and target object type specified for the synchronization step. For provisioning steps, you can use this tab to view and modify the target container to which objects are provisioned and rules to generate unique names for provisioned objects.

For all types of synchronization steps (provisioning, deprovisioning, and updating) this tab provides the following elements:

- **Target connected system**. Displays the name of the data system that is currently used as a target for the synchronization step.
- **Target object type**. Displays the object type that is currently used as a target for the synchronization step.

For provisioning steps related to certain types of target data systems, this tab may also provide any of the following additional elements:

- **Target container**. Allows you to specify the target data system container to which you want to provision objects from the source data system. For more information, see Generating object names by using rules.
- **Rules to generate unique object name**. Allows you to set up a list of rules to generate a unique name for each object being provisioned. For more information, see Generating object names by using rules.

Provisioning Rules tab

Allows you to view or modify the rules used for provisioning objects. This tab has the following elements:

- **Initial Attribute Population Rules**. Expand this element to view or modify the rules for populating the attributes of objects being provisioned.
- **Initial Password**. Expand this element to view or modify how an initial password is generated for each object being provisioned.
- **User Account Options**. Expand this element to view or modify the settings used for creating user accounts in the result of the provision operation.

You can use this tab to import or export initial attribute population rules.

To export a population rule to a file

1. In the list of configured attribute population rules, select the rule you want to export.
2. Click **More**, and then click **Export**.
3. In the **Save As** dialog box, specify an XML file to store the rule.

To import a population rule from a file

1. Expand **Initial Attribute Population Rules**, click **More**, and then click **Import**.
2. Use the **Open** dialog box to open the XML file that stores the population rule to import.

Deprovisioning Rules tab

Allows you to select a method for deprovisioning objects. You can select **Delete target objects** to delete the target objects if the source objects meet the criteria specified earlier in the wizard or **Modify target objects** to modify the target objects using the rules configured in the options below:

- **Rules to Modify Object Attributes**. Expand this option to set up a list of rules to modify the attributes of target objects. For more information, see Modifying attribute values by using rules.
- **Rules to Move Objects**. Expand this option to specify the location to which you want to move objects. Click the down arrow on the button, and then select one of the following:
  - **Browse**. Click to locate and select a single target container.
  - **PowerShell Script**. Click to compose a PowerShell script that calculates the target container name.
  - **Rule**. Click to configure a set of rules for selecting target containers.
  - **Use Mapping**. Click to define a target container based on the mapping of the source object.
  - **Clear**. Click to use an empty value.
- **Rules to Rename Objects**. Expand this option to set up a list of rules to rename objects.

Updating Rules Tab

Allows you to view or modify the rules used for updating objects. This tab has the following elements:

- **Rules to Modify Object Attributes**. Allows you to view or change the list of rules used to modify the attributes of target objects. For more information, see Modifying attribute values by using rules.
- **Rules to Move Objects**. Allows you to specify the location to which you want to move objects. Click the down arrow on the button, and then select one of the following:
  - **Browse**. Click to locate and select a single target container.
  - **PowerShell Script**. Click to compose a PowerShell script that calculates the target container name.
  - **Rule**. Click to configure a set of rules for selecting target containers.
  - **Use Mapping**. Click to define a target container based on the mapping of the source object.
  - **Clear**. Click to use an empty value.

- **Rules to Rename Objects**. Allows you to view or change the list of rules used to rename target objects. For more information, see Generating object names by using rules.

Step Handlers tab

Allows you to create, modify, or delete handlers for the workflow step. For more information on step handlers, see Using workflow step handlers. This tab has the following elements:

- **Add handler**. Starts a wizard that helps you add a new handler for the workflow step. By default, the wizard creates a new handler that runs your PowerShell script.
- **Disable**. Disables the step handler.
- **Enable**. Enables the step handler.
- **Move up**. Moves the step handler one position up in the list.
- **Move down**. Moves the step handler one position down in the list.
- **Delete**. Deletes the step handler.

Deleting a step

To delete a workflow step

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to delete a step.
3. Click **Delete** below the step you want to delete.
4. When prompted, confirm that you want to delete the step.

Changing the order of steps in a workflow

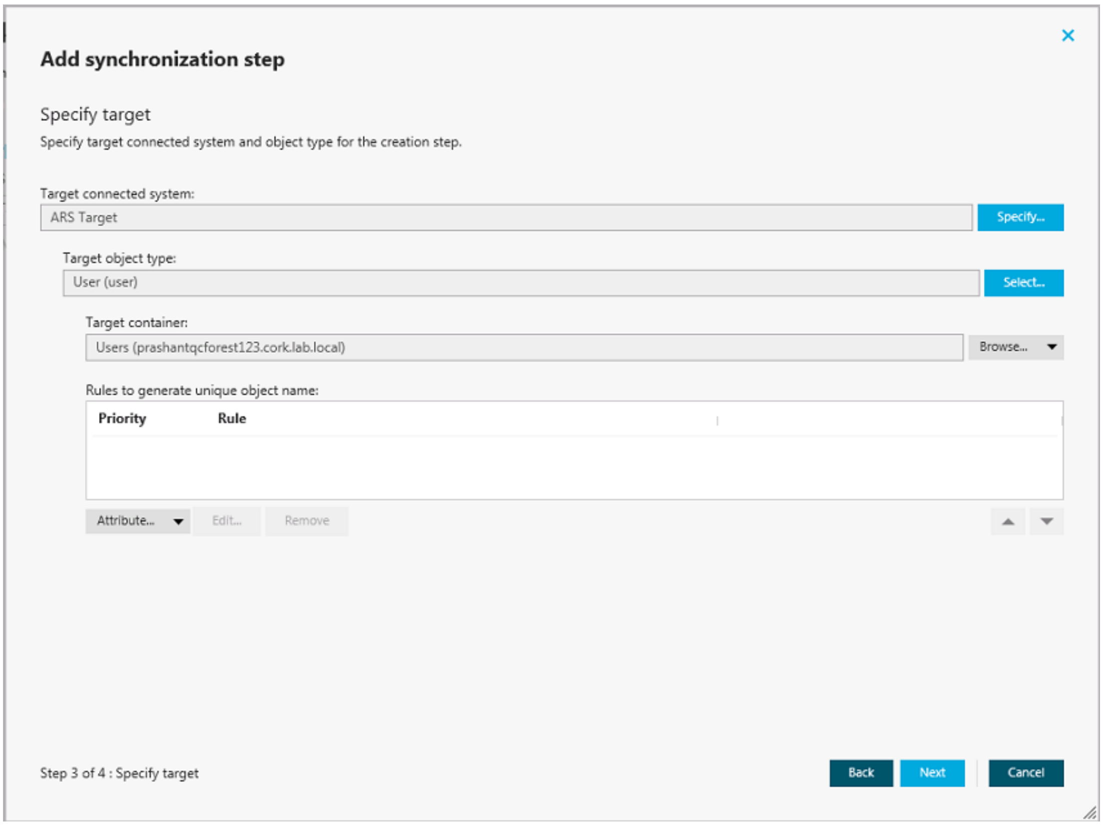
When you run a workflow, its steps are executed in the order they are displayed in the Quick Connect Administration Console. If necessary, you can change the order of steps in a workflow.

To change the order of steps in a workflow

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the workflow in which you want to change the order of steps.
3. Use the **Move up** and **Move down** links to arrange the steps as necessary.

Generating object names by using rules

When configuring a synchronization step, you can use the **Rules to generate unique object name** list to specify rules for creating or modifying object names in the target connected system. The **Rules to generate unique object name** list looks similar to the following:



Add synchronization step

Specify target

Specify target connected system and object type for the creation step.

Target connected system: ARS Target

Target object type: User (user)

Target container: Users (prashantqcforest123.cork.lab.local)

Rules to generate unique object name:

Priority	Rule

Step 3 of 4 : Specify target

To configure rules for generating object names

1. Click the down arrow on the leftmost button provided below the **Rules to generate unique object name** list.
2. Select a list item:
   - **Attribute**. Allows you to select the target object attribute whose value you want to use as the object name.
   - **Rule**. Allows you to configure a rule to generate target object names. For details, see Using value generation rules.
   - **PowerShell Script**. Allows you to type a PowerShell script to generate target object names.

When the **Rules to generate unique object name** list includes two or more entries, Quick Connect uses the uppermost rule in the list to generate the target object name. If the generated object name is not unique, Quick Connect uses the next rule in the list, and so on.

To copy and paste an existing rule

1. In the **Rules to generate unique object name** list, right-click a rule, and then select **Copy** from the shortcut menu.
2. In the rules list, right-click an entry, and then select **Paste** from the shortcut menu.

Modifying attribute values by using rules

In a workflow step you can configure a set of rules to automatically modify attribute values during the step run. By using these rules, you can select or generate an initial value, transform this value if necessary, and then assign the resulting value to the object attribute you want.

To create a rule to modify attribute values

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the appropriate workflow, then click the name of the workflow step.
3. Depending on the workflow step type, complete the corresponding actions:
   - **Provisioning step**. Click the **Provisioning Rules** tab, and then expand the **Initial Attribute Population Rules** element.
   - **Updating step**. Click the **Updating Rules** tab, and then expand the **Rules to Modify Object Attributes** element.
   - **Deprovisioning step**. Click the **Deprovisioning Rules** tab, and then expand the **Rules to Modify Object Attributes** element.
4. In the element you have expanded, click the down arrow on the leftmost button to select a rule type:
   - **Forward Sync Rule**. Allows you to create a rule that synchronizes attribute values from the source to the target data system. This type of rule is available in provisioning, updating, and deprovisioning steps. For more information, see Configuring a forward sync rule.
   - **Reverse Sync Rule**. Allows you to create a rule that synchronizes attribute values from the target to the source data system. This type of rule is available in provisioning, updating, and deprovisioning steps. For more information, see Configuring a reverse sync rule.
   - **Merge Sync Rule**. Allows you to create a rule that merges the values of specified attributes between the source and the target data systems. As a result, the attribute values in the source and the target become identical. This type of rule is only available in updating steps. For more information, see Configuring a merge sync rule.

Configuring a forward sync rule

A forward sync rule allows you to synchronize data from the source data system to the target data system. To create such a rule, follow the instructions in Modifying attribute values by using rules to select the **Forward Sync Rule** type. Then, configure your rule by using the options in the dialog box that opens.

Source item

This option allows you to obtain an initial value for the synchronization operation. You can then transform the obtained initial value before assigning it to the attribute you want.

To get started, click the down arrow on the button in this option, and then select an item from the drop-down list:

- **Attribute**. Allows you to select the attribute whose value you want to use.
- **Rule**. Allows you to obtain a value by using a value generation rule. For more information, see Using value generation rules.
- **PowerShell script**. Allows you to obtain a value by executing a Windows PowerShell script.
- **Text**. Allows you to type a text value.
- **Referenced object attribute**. Allows you select an attribute of a referenced object and use the value of the selected attribute.
- **Parent object attribute**. Allows you to select an attribute of a parent object and use the value of the selected attribute.
- **Empty**. Generates an empty value.

Once you have explicitly selected an attribute in this option, you can click the **Advanced** link to configure some advanced synchronization settings for the attribute.

For example, you can specify which characters to retrieve from the attribute value, how to modify the retrieved value (remove white-space characters or change the capitalization), or set how to process references in the attribute. The available settings depend on the attribute types selected in the **Source item** and **Target item** options.

Target item

This option allows you to select the target attribute whose value you want to modify.

To get started, click the down arrow on the button in this option, and then select an item from the drop-down list:

- **Attribute**. Allows you to select the object attribute whose value you want to modify.
- **Referenced object attribute**. Allows you to select the referenced object attribute whose value you want to modify.

- **Parent object attribute**. Allows you to modify attribute values of objects that are parents to the target object type selected in the workflow step settings.

Once you have selected an attribute, you can click the **Advanced** link to configure some advanced synchronization settings for the attribute.

For example, you can select how to handle the existing attribute value (overwrite or append data to the value) or set how to process references in the attribute. The available settings depend on the attribute types selected in the **Source item** and **Target item** options.

Configuring a reverse sync rule

A reverse sync rule allows you to synchronize data from the target to the source data system.

To create such a rule, follow the instructions in Modifying attribute values by using rules to select the **Reverse Sync Rule** type. Then, configure your rule by using the options in the dialog box that opens.

Source item

This option allows you to select the source attribute whose value you want to modify.

To get started, click the down arrow on the button in this option, and then select an item from the drop-down list:

- **Attribute**. Allows you to select the object attribute whose value you want to modify.
- **Referenced object attribute**. Allows you to select the referenced object whose attribute value you want to modify.
- **Parent object attribute**. Allows you to modify attribute values of objects that are parents to the source object type selected in the workflow step settings.

Once you have selected an attribute, you can click the **Advanced** link to configure some advanced synchronization settings for the attribute.

For example, you can select how to handle the existing attribute value (overwrite or append data to the value) or set how to process references in the attribute. The available settings depend on the attribute types selected in the **Source item** and **Target item** options.

Target item

This option allows you to obtain an initial value for the synchronization operation. You can then transform the obtained initial value before assigning it to the attribute you want.

To get started, click the down arrow on the button in this option, and then select an item from the drop-down list:

- **Attribute**. Allows you to select the attribute whose value you want to use.
- **Rule**. Allows you to obtain an initial value by using a value generation rule. For more information, see Using value generation rules.
- **PowerShell script**. Allows you to obtain an initial value by executing a Windows PowerShell script.
- **Text**. Allows you to type an initial value.
- **Referenced object attribute**. Allows you select an attribute of a referenced object and use its value.
- **Parent object attribute**. Allows you to select an attribute of a parent object and use the value of the selected attribute.
- **Empty**. Generates an empty initial value.

Once you have explicitly selected an attribute in this option, you can click the **Advanced** link to configure some advanced synchronization settings for the attribute.

For example, you can specify which characters to retrieve from the attribute value, how to modify the retrieved value (remove white-space characters or change the capitalization), or set how to process references in the attribute. The available settings depend on the attribute types selected in the **Source item** and **Target item** options.

Configuring a merge sync rule

A merge sync rule allows you to merge attribute values between the source and the target data system. As a result these values become identical.

To create such a rule, follow the instructions in Modifying attribute values by using rules to select the **Merge Sync Rule** type. Then, configure your rule by using the options in the dialog box that opens:

- **Source item**. Allows you to specify an attribute in the source data system. Click the **Attribute** button to select an attribute.
- **Target item**. Allows you to specify the attribute in the target data system. Click the **Attribute** button to select an attribute.
- **Merge Settings**. Allows you to select a method to merge the values of two multivalued attributes. This link is only available if both the source and the target attributes you have selected are multivalued.

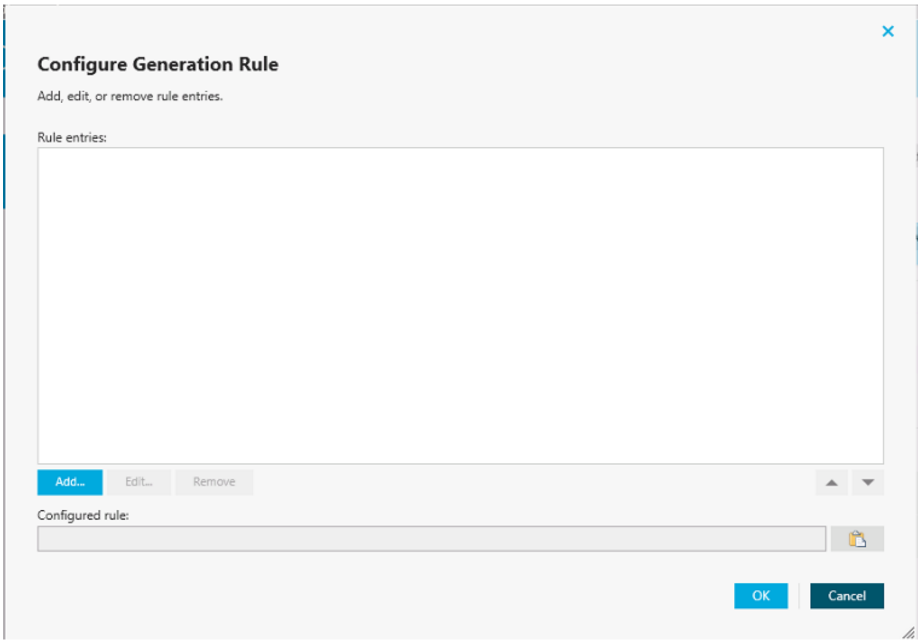
When running a workflow step that has a merge sync rule configured for the first time, One Identity Quick Connect Sync Engine synchronizes attribute values from the source to the target. In each subsequent run of the workflow step, the synchronization direction depends on which attribute value (source or target) is more recent, as follows:

Table 13: Synchronization direction

More recent value	Synchronization direction
Source	Source => Target
Target	Source <= Target
Source and target are equally recent	Source => Target

Using value generation rules

To configure a list of rules for selecting an attribute value or generating a value, you can use the **Configure Generation Rule** dialog box that looks similar to the following:



Configure Generation Rule

Add, edit, or remove rule entries.

Rule entries:

Configured rule:

To add a new rule entry

1. Click **Add**.
2. Configure the rule entry as appropriate. For more information, see Configuring a rule entry.

To remove an existing rule entry

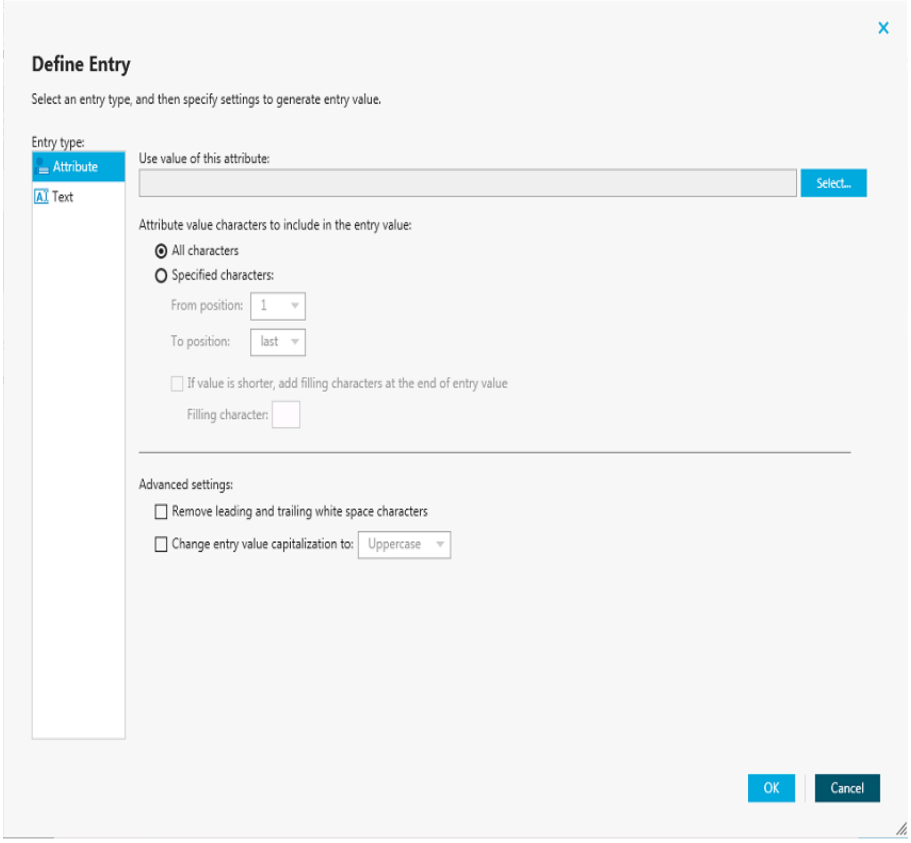
- From the **Rule entries** list, select the entry you want to remove, and then click **Remove**.

To edit an existing rule entry

1. From the **Rule entries** list, select the entry you want to modify, and then click **Edit**.
2. Configure the rule entry as appropriate. For more information, see Configuring a rule entry.

Configuring a rule entry

This section provides instructions on how to configure a rule entry in the **Define Entry** dialog box that looks similar to the following:



Define Entry

Select an entry type, and then specify settings to generate entry value.

Entry type:
- Attribute
- Text

Use value of this attribute:

Attribute value characters to include in the entry value:

● All characters

○ Specified characters:

From position: 1

To position: last

□ If value is shorter, add filling characters at the end of entry value

Filling character:

Advanced settings:

□ Remove leading and trailing white space characters

□ Change entry value capitalization to: Uppercase

To configure a text entry

1. Under **Entry type**, select **Text**.
2. In the **Text value** box, type the value.
3. Click **OK**.

To configure an attribute-based entry

1. Under **Entry type**, select **Attribute**.
2. Click **Select** to select the attribute whose value you want to use, and then click **OK**.

3. If you want the entry to include the entire value of the attribute, select the **All characters** option. Otherwise, click the **Specified characters** option, and then specify the characters to include in the entry.
4. Optionally, click the **If value is shorter, add filling characters at the end of entry value** option to specify a character to add to the entry.
5. Optionally, specify **Advanced settings**.
6. When finished, click **OK**.

Using workflow step handlers

Workflow step handlers allow you to automatically perform custom actions either before running a workflow step or after the workflow step run results have been committed (written) to the data system. Out of the box, One Identity Quick Connect Sync Engine includes a single predefined handler type that can automatically execute your custom PowerShell script and thus perform the desired action.

You can also develop and implement your own handler types. For more information, see the Software Development Kit (SDK) supplied with this One Identity Quick Connect Sync Engine version.

To create, modify, or delete handlers for a workflow step, you can use the Step Handlers tab in the workflow step properties.

To create a workflow step handler

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the appropriate workflow.
3. Click the name of the workflow step for which you want to create a handler, and then click the **Step Handlers** tab.
4. Click **Add handler**, and then follow the steps in the wizard to create your handler.

To modify a workflow step handler

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the appropriate workflow.
3. Click the name of the workflow step whose handler you want to modify, and then click the **Step Handlers** tab.
4. Click the name of the handler you want to modify.
5. Modify the handler settings as necessary. When you are finished, click **OK**.

   You can also do the following:

   - **Change the order in which handlers are activated**. One Identity Quick Connect Sync Engine activates handlers in the order in which they appear in the list. To move a handler in the list, use the **Move up** and **Move down** links below the handler.

- **Disable or enable the handler**. You can enable or disable existing handlers. To do so, use the **Enable** or **Disable** link below the handler.

6. When you are finished, click **Save**.

To delete a workflow step handler

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the name of the appropriate workflow.
3. Click the name of the workflow step whose handler you want to delete, and then click the **Step Handlers** tab.
4. Click **Delete** below the handler you want to delete.

Example: Synchronizing group memberships

This example illustrates how to configure a provisioning step to synchronize group memberships from an Active Directory domain to an AD LDS (ADAM) instance. The example demonstrates how to create rules in the step to synchronize the value of the **member** attribute in the Active Directory domain to the **member** attribute in AD LDS (ADAM).

To synchronize the member attribute

1. Follow the steps described in the Creating a provisioning step section until you reach the wizard page titled **Specify provisioning rules**.
2. In the **Initial Attribute Population Rules** element, click the down arrow on the leftmost button below the list to select **Forward Sync Rule**.
3. In the dialog box that opens, add the following pair of attributes:
   a. Source item: **member** attribute (Active Directory)
   b. Target item: **member** attribute (AD LDS)

   For more information about the options in this dialog box, see Configuring a forward sync rule.
4. When you are finished, click **OK**.
5. Follow the steps in the wizard to complete the creation of the provisioning step.

Example: Synchronizing multivalued attributes

This example illustrates how to configure a provisioning step to synchronize multivalued attributes from an Active Directory domain to an AD LDS (ADAM) instance. The example demonstrates how to create rules in the step to synchronize the value of the

otherTelephone attribute in the Active Directory domain to the **otherTelephone** attribute in AD LDS (ADAM).

To synchronize the otherTelephone attribute

1. Follow the steps provided in the Creating a provisioning step section until you reach the wizard page titled **Specify provisioning rules**.
2. In the **Initial Attribute Population Rules** element, click the down arrow on the leftmost button below the list to select **Forward Sync Rule**.
3. In the dialog box that opens, add the following pair of attributes:
   - Source item: **otherTelephone** attribute (Active Directory)
   - Target item: **otherTelephone** attribute (AD LDS)

   For more information about the options in this dialog box, see Configuring a forward sync rule.
4. When you are finished, click **OK**.

Follow the steps in the wizard to complete the creation of the provisioning step.

Using workflow alerts

The One Identity Quick Connect Sync Engine provides an email notification service that allows you to inform recipients about the completion of a workflow run.

For each synchronization workflow that includes at least one synchronization step, you can configure multiple alerts. Then, when a workflow run completes, the recipients signed up for the alert receive an email message informing them about the completion of the workflow run. For example, you can use workflow alerts to inform recipients when a workflow run completes with errors.

To manage alerts for a workflow, go to the **Workflows** tab in the Quick Connect Administration Console, and then click the **Manage alerts** link below the workflow.

To manage outgoing mail profiles for sending workflow alerts, in the Quick Connect Administration Console, click the **Settings** menu in the upper right corner, and then click the **Mail Profiles**.

In this section:

- Creating or editing a workflow alert
- Deleting a workflow alert
- Managing outgoing mail profiles

Creating or editing a workflow alert

To create or edit an alert

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the **Manage alerts** link below the workflow for which you want to create or edit an alert.

   The **Manage alerts** link is only available on workflows that include one or more synchronization steps.
3. In the **Manage Workflow Alerts** dialog box, do one of the following:
   a. If you want to create a new alert, click the **Add** button under the **Workflow alerts** list.
   b. If you want to edit an existing alert, select that alert in the **Workflow alerts** list, and then click the **Edit** button under the list.
4. Use the following options in the dialog box that opens to specify alert settings, and then click **OK**:
   - **When this event occurs**. Select an event that will trigger the alert. You can select one of the following:
     - **Workflow run completes (with or without errors)**. Triggers the alert upon the workflow run completion regardless of any errors encountered in the run.
     - **Workflow run completes with errors**. Triggers the alert only when the workflow run completed with errors.
   - **Send email to**. Type the email addresses of the recipients to which you want to send a notification email message when the selected event occurs. When specifying multiple email addresses, use a semicolon as a separator.
   - **Email message subject**. Type the text you want to include into the notification email message subject.
   - **Ignore mapping errors**. Select this check box if you want the alert to skip mapping errors in workflow runs. This check box is only available when you select **Workflow run completes with errors** in the **When this event occurs** option.
   - **Ignore non-fatal errors in**. Select this check box if you want this alert to skip non-fatal errors in workflow runs. A non-fatal error causes a workflow run to partially succeed. A fatal error causes a workflow run to fail. If you select this check box, you must also select one of the following options:
   - **All workflow steps**. Causes the alert to skip non-fatal errors in all steps of the workflow.
   - **The specified workflow steps**. Causes the alert to skip non-fatal errors in the workflow steps you specify in the text box below. Type workflow step numbers separated by commas (example: 1, 3, 5). To specify a range of steps, use a dash as a separator (example: 1, 3, 5-8).

This check box is only available when you select **Workflow run completes with errors** in the **When this event occurs** option.

5. Use the **Send email using this outgoing mail profile** list to select the settings to be used for sending notification emails generated by the alerts in the **Workflow alerts** list.

   To configure the current outgoing mail profile, click the **Properties** button. For more information, see Managing outgoing mail profiles.
6. When you are finished, click **OK** to close the **Manage Workflow Alerts** dialog box.

Deleting a workflow alert

To delete an alert

1. In the Quick Connect Administration Console, open the **Workflows** tab.
2. Click the **Manage alerts** link below the workflow for which you want to delete an alert.

   The **Manage alerts** link is only available on workflows that include one or more synchronization steps.
3. In the **Workflow alerts** list, select the alert you want to delete, and then click the **Delete** button under the list.

Managing outgoing mail profiles

To create, edit, or delete an outgoing mail profile, in the Quick Connect Administration Console, click the **Settings** menu in the upper right corner, and then click the **Mail Profiles**. Then, follow the appropriate procedure below.

To create a profile

1. Click the **Add** button below the list of profiles, and then specify the settings you want to use. For the descriptions of the settings you can specify, see Outgoing mail profile settings.
2. When you are finished, click **OK**.

To edit a profile

1. In the list, select the outgoing mail profile you want to edit.
2. Click the **Edit** button below the list of profiles, and then specify the settings you want to use. For the description of the settings you can specify, see Outgoing mail profile settings.
3. When you are finished, click **OK**.

To delete a profile

1. In the list, select the outgoing mail profile you want to delete.
2. Click the **Delete** button below the list of profiles.

Outgoing mail profile settings

In each outgoing mail profile, you can use the following settings:

- **Profile name**. Type a descriptive name with which you want to identify the profile.
- **Outgoing SMTP server**. Type the fully qualified domain name of the SMTP mail server you want to use for sending notification emails.
- **This server requires an encrypted connection (SSL)**. Select this check box if the specified mail server requires an encrypted connection.
- **This server requires authentication**. Select this check box if the specified mail server requires authentication, and then type the user name and password with which you want to access the server.
- **Sender email address**. Type the email address you want to use as the originating address in the notification emails.
- **Sender name**. Type the sender name you want to display in the From field to the recipients of the notification emails.

Mapping objects

About mapping objects

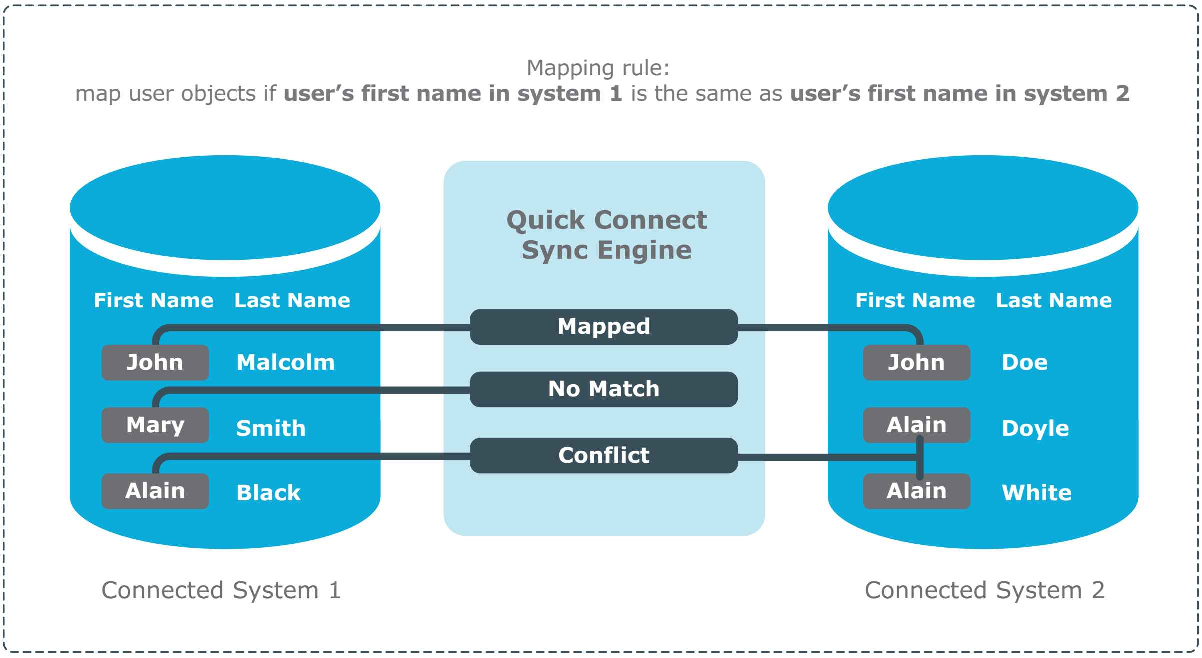
Object mapping allows you to establish one-to-one relationships between objects in two connected data systems. By using object mapping, you can determine what objects will participate in data synchronization operations you run between these two data systems.

Quick Connect maps objects automatically when running the provisioning steps of a synchronization workflow. In this case, one-to-one relationship is automatically established between source objects and their counterparts created in the target connected system during the provision operation. In some cases, however, you may need to manually map objects. For example, you should configure object mapping before running a synchronization workflow that includes updating or deprovisioning steps. By doing so, you provide One Identity Quick Connect Sync Engine with the information on which objects need to be updated or deprovisioned in the target data system.

To map objects, you can use *mapping pairs* and *mapping rules*. A *mapping pair* allows you to establish a relationship between a certain object type in one connected system and its counterpart in the other connected system. A *mapping rule* allows you to define the scope of conditions where the objects belonging to the object types specified in a particular mapping pair will be mapped. For a mapping pair you can create multiple mapping rules, each defining a specific mapping condition. In order your mapping rules take effect, you need to run them. After you run a mapping rule, One Identity Quick Connect Sync Engine reads data in the connected data systems for which the rule is configured, and then maps the objects that meet the conditions specified in the mapping rule.

The following example shows how a mapping rule works:

Object Mapping



In this example, one-to-one relationship is established between the user object John Malcolm in Connected System 1 and the user object John Doe in Connected System 2: the first names of these user objects match, and thus the condition specified in the mapping rule is met. Now, if you configure a synchronization workflow for these systems and populate it with synchronization steps, identity information will be synchronized between these two user objects, since they are *mapped*. The direction of synchronization depends on which of these two connected data systems acts as the synchronization source and which is the target.

The next sections cover the following:

- Steps to map objects
- Steps to unmap objects

Steps to map objects

You can map objects in two data systems to which One Identity Quick Connect Sync Engine is connected. To map objects in two connected data systems, complete the following steps:

- Step 1: Create mapping pairs
- Step 2: Create mapping rules
- Step 3 (optional): Change scope for mapping rules
- Step 4: Run map operation

Step 1: Create mapping pairs

In this step, you create mapping pairs that specify the types of objects you want to map in two connected systems. You can create as many mapping pairs as necessary.

To create a mapping pair

1. In the Quick Connect Administration Console, open the **Mapping** tab.
2. Click the name of the connection for which you want to map objects.
3. Click **Add mapping pair**.
4. On the **Specify source** page, next to **Connected system object type**, click **Select**, and then select the type of object you want to map.
5. Click **Next**.
6. On the **Specify target** page, do the following:
    a. Next to **Target connected system**, click **Specify**, and then specify the other connected system where you want to map objects.

    b. Next to **Connected system object type**, click **Select**, and then select the type of object you want to map.
7. Click **Finish** to create the mapping pair.

Repeat the above steps to create mapping pairs for as many object types as necessary.

Step 2: Create mapping rules

Once you have created a mapping pair, you can configure mapping rules for that pair. Mapping rules define the conditions where the objects that belong to the object types specified in the mapping pair will be mapped. One Identity Quick Connect Sync Engine maps objects only if all mapping rules specified for a mapping pair are met.

To add a new mapping rule

1. In the Quick Connect Administration Console, open the **Mapping** tab.
2. Click the name of the connection for which you want to create a mapping rule.
3. Click the mapping pair for which you want to create a mapping rule.
4. Click **Add mapping rule**.
5. Use the **Define Mapping Rule** dialog box to define the condition where the objects in the connected systems are to be mapped. To do so, click the down arrow on the button next to each of the two provided options and select one of the following:
    - **Attribute**. Allows you to select an attribute in the connected system.
    - **Rule**. Allows you to set up a list of rules to generate a value for the connected system. For details, see Using value generation rules.

- **PowerShell Script**. Allows you to type a Windows PowerShell script that generates a value for the connected system.

6. When you are finished, click **OK** to create the mapping rule.

Step 3 (optional): Change scope for mapping rules

Each mapping rule applies to a scope of objects. By default, this scope includes all objects that belong to the object types specified in the mapping rule. If necessary, you can narrow the scope specified for a particular mapping rule or you can revert to the default scope.

To change the scope of a mapping rule

1. Go to the mapping pair that includes the mapping rule whose scope you want to change:
   a. In the Quick Connect Administration Console, open the **Mapping** tab.
   b. Click the name of the appropriate connection.
   c. Click the appropriate mapping pair entry.
2. Locate the mapping rule whose scope you want to change. Use the following elements provided for each mapping rule entry:
   a. **Mapping scope for system 1**. Shows the mapping rule scope applicable to the data system shown on the left part of the mapping pair entry.
   b. **Mapping scope for system 2**. Shows the mapping rule scope applicable to the data system shown on the right part of the mapping pair entry.

   These elements can take one of the following values:

   a. **Default**. Indicates that the mapping rule applies to all objects of the specified type.
   b. **Custom**. Indicates that the mapping rule scope is narrowed down and only applies to some objects of the specified type.
3. Change the mapping rule scope as necessary:
   a. Click the value displayed next to **Mapping scope for system 1** or **Mapping scope for system 2**, and then specify the scope you want to use.
   b. When you are finished, click **OK**.

Step 4: Run map operation

Once you have created mapping rules for a mapping pair, you need to run the map operation in order to apply these rules and map objects that belong to the mapping pair. There are two methods to run the map operation: you can manually run the map operation once or you can create a recurring schedule to automatically run the map operation on a regular basis.

The latter method is recommended when you want to use Quick Connect to synchronize passwords from an Active Directory domain to other connected systems.

Running mapping rules on a recurring schedule allows you to properly map newly-created Active Directory user objects to their counterparts in the connected systems where you automatically synchronize passwords with the Active Directory domain. If you do not run mapping rules on a regular basis, some passwords may become out of sync because of the changes that inevitably occur to your environment.

For example, new user objects are created, some user objects are deleted, but Quick Connect cannot detect these changes and synchronize passwords for the newly-created users before you apply the mapping rules. In this scenario, the best way to ensure Quick Connect synchronizes all passwords is to apply your mapping rules on a regular basis. You can accomplish this task by creating a recurring schedule for applying your mapping rules.

To run the map operation once

1. In the Quick Connect Administration Console, open the **Mapping** tab.
2. Click the name of the connection for which you want to run the map operation.
3. Click the mapping pair for which you want to run the map operation.
4. Click **Map now.**
5. In the dialog box that opens, click one of the following:

    - **Full Map**. With this option, One Identity Quick Connect Sync Engine retrieves the data required to map objects from the connected data systems.
    - **Quick Map**. With this option, One Identity Quick Connect Sync Engine first tries to map objects by using the data that is available in the local cache. If the local cache is missing or cannot be used to map objects, then One Identity Quick Connect Sync Engine retrieves the required data from the connected data systems.

    Wait for the map operation to complete.

    After the map operation completes, the Quick Connect Administration Console displays a report that provides information about the objects that participated in the map operation. At this stage, the application does not map the objects. To map the objects, you need to commit the map operation result.

    You can click the number that is provided next to an object category name in the report to view the details of objects that belong to that category.
6. Review the report about the objects that participated in the map operation, and then click **Commit** to map the objects.

To automatically run the map operation on a recurring schedule

1. In the Quick Connect Administration Console, open the **Mapping** tab.
2. Click the name of the connection for which you want to create a recurring mapping schedule.

3. Click the mapping pair for which you want to run the map operation on a recurring schedule.
4. Click **Schedule mapping**.
5. In the dialog box that opens, select the **Schedule the task to run** check box, and then specify a schedule for the map operation.

   It is recommended to schedule the map operation to run once in every 6 hours.
6. If several One Identity Quick Connect Sync Engine instances are installed in your environment, under **Run the task on**, select the computer that hosts the instance you want to use for running the map operation.
7. Click **OK** to activate the schedule.

   The results of a scheduled map operation always apply automatically, you do not need to commit the changes.

   When performing a scheduled map operation, One Identity Quick Connect Sync Engine always retrieves the required data from the connected data systems and never uses the data available in the local cache.

Steps to unmap objects

You can unmap the objects that were mapped earlier.

To unmap objects

1. In the Quick Connect Administration Console, open the **Mapping** tab.
2. Click the name of the connection for which you want to unmap objects.
3. Click the mapping pair that specifies the objects types you want to unmap.
4. Click **Unmap now** and wait until the unmap operation completes.

   After the unmap operation completes, the Quick Connect Administration Console displays a report which provides information about the objects that participated in the unmap operation. At this stage, the application does not unmap the objects. To unmap them, you need to commit the result of the unmap operation.

   You can click the number provided next to an object category name in the report to view the details of objects that belong to that category.
5. Review the report on the objects that participated in the unmap operation, and then click **Commit** to unmap the objects.

7

Automated password synchronization

About automated password synchronization

If your enterprise environment has multiple data management systems, each having its own password policy and dedicated user authentication mechanism, you may face one or more of the following issues:

- Because users have to remember multiple passwords, they may have difficulty managing them. Some users may even write down their passwords. As a result, passwords can be easily compromised.
- Each time users forget one or several of their numerous access passwords, they have to ask administrators for password resets. This increases operational costs and translates into a loss of productivity.
- There is no way to implement a single password policy for all of the data management systems. This too impacts productivity, as users have to log on to each data management system separately in order to change their passwords.

With Quick Connect, you can eliminate these issues and significantly simplify password management in an enterprise environment that includes multiple data management systems.

Quick Connect provides a cost-effective and efficient way to synchronize user passwords from an Active Directory domain to other data systems used in your organization. As a result, users can access other data management systems using their Active Directory domain password. Whenever a user password is changed in the source Active Directory domain, this change is immediately and automatically propagated to other data systems, so each user password remains in sync in the data systems at all times.

You need to connect One Identity Quick Connect Sync Engine to the data systems in which you want to synchronize passwords through special connectors supplied in Quick Connect packages (also known as *bundles*). For a list of data systems in which you can synchronize passwords by using a particular Quick Connect package, see the *Quick Start Guide* supplied with that package.

Steps to automate password synchronization

> NOTE: For instructions on how to automate password synchronization between two Active Directory domains, see the Quick Start Guide supplied with Quick Connect Express for Active Directory.

To automatically synchronize passwords from an Active Directory domain to another data system, complete these steps:

1. Install Capture Agent on each domain controller in the Active Directory domain you want to be the source for password synchronization operations.

   Capture Agent tracks changes to the user passwords in the source Active Directory domain and provides this information to the Quick Connect Service (a component of the One Identity Quick Connect Sync Engine), which in turn synchronizes passwords in the target connected systems you specify.

   For more information on how to install Capture Agent, see Managing Capture Agent.

2. Connect the One Identity Quick Connect Sync Engine to the Active Directory domain where you installed Capture Agent in step 1.

   Alternatively, you can configure a connection to Quest ActiveRoles Server that manages the source Active Directory domain.

3. Connect the One Identity Quick Connect Sync Engine to the data system where you want to synchronize user object passwords with those in the source Active Directory domain.

   - For some target data systems (such as SQL Server and Oracle Database) you must specify the data you want to participate in the password synchronization by configuring an SQL query. For more information, see the section titled “Using an SQL Query to Specify Data in a Connected System” in the *Quick Start Guide* supplied with the Quick Connect package that provides connectors for those data systems.
   - If the target data system is an LDAP directory service accessed via the generic LDAP connector, you must specify the target object type for which you want to

synchronize passwords and the attribute where you want to store object passwords.

4. Ensure that user objects in the source Active Directory domain are properly mapped to their counterparts in the target connected system.

   For more information about mapping objects, see Mapping objects.

   Quick Connect automatically maps objects between the source Active Directory domain and the target connected system if you configure synchronization workflows to manage the provision and deprovision operations between the source AD domain (or Quest ActiveRoles Server that manages that domain) and the target connected system.

   For more information on synchronization workflows, see Synchronizing identity data.

5. Create a password synchronization rule for the target connected system.

   For more information, see Creating a password sync rule.

After you complete the above steps, the One Identity Quick Connect Sync Engine starts to automatically track user password changes in the source AD domain and synchronize passwords in the target connected system.

If necessary, you can fine-tune the password synchronization settings by completing these optional tasks:

- Modify the default Capture Agent settings.

  For more information, see Configuring Capture Agent.

- Modify the default Quick Connect Service settings related to password synchronization.

  For more information, see Configuring Quick Connect Service.

- Specify a custom certificate for encrypting the password sync traffic between the Capture Agent and the Quick Connect Service. By default, a built-in certificate is used for this purpose.

  For more information, see Specifying a custom certificate for encrypting password sync traffic.

- Configure the One Identity Quick Connect Sync Engine to automatically run your PowerShell script after the password synchronization completes.

  For more information, see Using PowerShell scripts with password synchronization.

Managing Capture Agent

Capture Agent is required to track changes to the user passwords in the Active Directory domain you want to be the authoritative source for password synchronization operations. To synchronize passwords, you must install Capture Agent on each domain controller in the source Active Directory domain.

Whenever a password changes in the source Active Directory domain, the agent captures that change and provides the changed password to the One Identity Quick Connect Sync

Engine. In turn, the One Identity Quick Connect Sync Engine uses the provided information to synchronize passwords in the target connected systems according to your settings.

In this section:

- Installing Capture Agent manually
- Using Group Policy to install Capture Agent
- Uninstalling Capture Agent

Installing Capture Agent manually

You can use this method to manually deploy Capture Agent on each domain controller in the source Active Directory domain.

To manually install Capture Agent

1. Run one of the following files supplied with the One Identity Quick Connect Sync Engine installation package:
    - On a 32-bit domain controller, run the file **QuickConnectCaptureAgent_x86.msi**.
    - On a 64-bit domain controller, run the file **QuickConnectCaptureAgent_x64.msi**.
2. Step through the wizard to complete the agent installation.

Using Group Policy to install Capture Agent

You can use this method to automatically deploy Capture Agent on each domain controller in the source Active Directory domain. This method is applicable in the following scenarios only:

Table 14: Prerequisites by scenario

Supported scenario	Prerequisites
Scenario 1: AD domain includes either 32- or 64-bit domain controllers	All the domain controllers must be held in a single organizational unit (for example, the built-in **Domain Controllers** OU). At least one group policy object must be linked to the OU holding the domain controllers (for example, the built-in **Default Domain Controllers Policy Group Policy** object).
Scenario 2: AD domain includes	The domain controllers must be held in two separate

Supported scenario	Prerequisites
both 32- and 64-bit domain controllers	organizational units, each containing domain controllers of the same bitness. At least one group policy object must be linked to each of the two organizational units.

The next steps apply to both these scenarios.

To install Capture Agent by using Group Policy

1. Save the **QuickConnectCaptureAgent_x86.msi** and **QuickConnectCaptureAgent_x64.msi** files supplied in the Quick Connect installation package to a network share accessible from each domain controller in the source Active Directory domain.
2. Depending on your scenario, complete the steps in the table:

Table 15:
Steps by scenario

Scenario 1: AD domain includes either 32- or 64-bit domain controllers	Scenario 2: AD domain includes both 32- and 64-bit domain controllers
1. Use Group Policy Editor to open the group policy object linked to the OU holding the domain controllers on which you want to install Capture Agent. 2. In the Group Policy Object Editor console tree, do one of the following: a. In Windows Server 2003 or Windows Server 2003 R2, expand the **Computer Configuration** node, and then select **Software Settings**. b. In a later version of Windows Server, expand the **Computer Configuration** node, then expand **Policies**, and select **Software Settings**. 3. In the details pane, click **Software Installation**, on the **Action** menu point to **New**, and then click **Package**.	1. Use Group Policy Object Editor to open the group policy object linked to the OU holding the 32-bit domain controllers. 2. Do one of the following in the Group Policy Object Editor console tree: a. In Windows Server 2003 or Windows Server 2003 R2, expand the **Computer Configuration** node, and then select **Software Settings**. b. In a later version of Windows Server, expand the **Computer Configuration** node, then expand **Policies**, and select **Software Settings**. 3. In the details pane, click

Scenario 1: AD domain includes either 32- or 64-bit domain controllers	Scenario 2: AD domain includes both 32- and 64-bit domain controllers
4. Use the dialog box to open one of the following files: a. **QuickConnectCaptureAgent_x86.msi** if all your domain controllers are 32-bit. b. **QuickConnectCaptureAgent_x64.msi** if all your domain controllers are 64-bit. 5. In the **Deploy Software** dialog box, select **Assigned**, and then click **OK**.	**Software Installation**, on the **Action** menu point to **New**, and then click **Package**. 4. Use the dialog box to open the **QuickConnectCaptureAgent_x86.msi** file. 5. In the **Deploy Software** dialog box, select **Assigned**, and then click **OK**. 6. Repeat steps 1-5 for the group policy object linked to the OU holding the 64-bit domain controllers. Use the **QuickConnectCaptureAgent_x64.msi** file to install Capture Agent on these domain controllers.

Run the following command at a command prompt to refresh the Group Policy settings:

```
gpupdate /force
```

Uninstalling Capture Agent

To uninstall Capture Agent

1. On the computer where Capture Agent is installed, open the list of installed programs:
   - In Windows Server 2003 or Windows Server 2003 R2, open **Add or Remove Programs** in Control Panel.
   - In a later version of Windows, open **Programs and Features** in Control Panel.
2. In the list of installed programs, select **Dell One Identity Quick Connect Capture Agent**.
3. Uninstall the agent:
   - In Windows Server 2003 or Windows Server 2003 R2, click **Remove**.
   - In a later version of Windows, click **Uninstall**.
4. Follow the on-screen instructions to uninstall Capture Agent.

Managing password sync rules

To synchronize passwords from an Active Directory domain to other connected systems, you need to create and configure a password synchronization rule for each target connected system where you want to synchronize passwords.

A password synchronization rule allows you to specify the following:

- The Active Directory domain you want to be the source for password synchronization operations.
- The source object type for password synchronization operations (typically, this is the user object type in Active Directory).
- The target connected system in which you want to synchronize passwords with the source Active Directory domain.
- The target object type for password synchronization operations.

Optionally, you can configure a password synchronization rule to modify attribute values of the target connected system objects whose passwords are being synchronized.

This section covers:

Creating a password sync rule

To create a password sync rule

1. In the Quick Connect Administration Console, open the **Password Sync** tab.
2. Click **Add password sync rule**.
3. On the **Specify source for password sync** page, do the following:
   a. In the **Source connected system** option, specify the Active Directory domain you want to be the source for password synchronization operations. Alternatively, you can select the ActiveRoles Server instance that manages such an Active Directory domain.
   b. In the **Connected system object type** option, select the object type you want to be the source for password synchronization.
4. Click **Next**.
5. On the **Specify target for password sync** page, do the following:
   a. In the **Target connected system** option, specify the target connected system in which you want to synchronize passwords.

b. In the **Connected system object type** option, select the object type you want to be the target for password synchronization.

c. Optionally, you can click the **Password Sync Settings** button and then use the following tabs to configure more password sync settings:

    - **Password Sync Retry Options**. Use this tab to specify how many times you want Quick Connect to retry the password synchronization operation in the event of a password synchronization failure. You can select one of the following options:
    - **Unlimited number of times**. Causes Quick Connect to retry the password synchronization operation until it succeeds.
    - **This maximum number of times**. Specify the maximum number of times you want Quick Connect to retry the password synchronization operation.

- **Password Transformation Script**. Use this tab to type a PowerShell script that transforms source Active Directory user passwords into object passwords for the target connected system. Use this item if you want the object passwords in the source and target connected systems to be different. If you do not want to transform passwords, leave the text box blank.
- **Rules to Modify Object Attributes**. Use this tab to specify rules for modifying attribute values on the target connected system objects. These rules will only apply to the objects on which One Identity Quick Connect Sync Engine modifies passwords in the target connected system.

d. When you are finished, click **OK**.

6. Click **Finish** to create the password sync rule.

Deleting a password sync rule

To delete a password sync rule

1. In the Quick Connect Administration Console, open the **Password Sync** tab.
2. Locate the rule you want to delete, and then click **Delete this rule** below the rule.

Modifying settings of a password sync rule

You can modify the following settings of an existing password sync rule:

- Specify how many times you want the One Identity Quick Connect Sync Engine to retry the password synchronization operation in the case of a password synchronization failure.
- Specify a PowerShell script to transform a source Active Directory user password into an object password in the target connected system.

- Specify rules to modify the attributes of the target connected system objects on which Quick Connect changes passwords.

To modify the settings of a password sync rule

1. In the Quick Connect Administration Console, open the **Password Sync** tab.
2. Click the **Password sync settings** link below the password sync rule you want to modify.
3. In the dialog box that opens, use the following tabs:
    - **Password Sync Retry Options**. Use this tab to specify how many times you want Quick Connect to retry the password synchronization operation in the event of a password synchronization failure. You can select one of the following options:
        - **Unlimited number of times**. Causes Quick Connect to retry the password synchronization operation until it succeeds.
        - **This maximum number of times**. Specify the maximum number of times you want Quick Connect to retry the password synchronization operation.
    - **Password Transformation Script**. Use this tab to type a PowerShell script that transforms source Active Directory user passwords into object passwords for the target connected system. Use this tab if you want the object passwords in the source and target connected systems to be different. If you do not want to transform passwords, leave the text box blank.
    - **Rules to Modify Object Attributes**. Use this tab to specify rules for modifying attribute values on the target connected system objects. These rules will only apply to the objects on which One Identity Quick Connect Sync Engine modifies passwords in the target connected system.
4. When you are finished, click **OK** to save your changes.

Fine-tuning automated password synchronization

This section provides information about the optional tasks related to configuring the automated password synchronization from an Active Directory domain to connected data systems.

In this section:

- Configuring Capture Agent
- Configuring Quick Connect Service
- Specifying a custom certificate for encrypting password sync traffic
- Using PowerShell scripts with password synchronization

Configuring Capture Agent

Capture Agent has a number of parameters you can modify. After you install the agent, each of these parameters is assigned a default value, as described in the following table:

Table 16: Capture Agent parameters

Parameter	Description	Default value
Maximum connection point age	Determines the period of time (in hours) during which a connection between Capture Agent and Quick Connect Service remains valid.	24 hours
Set interval between attempts to reconnect to service	Determines the time interval (in minutes) during which Capture Agent tries to reconnect to Quick Connect Service.	10 minutes
Set time period for attempts to connect to service	Determines the period of time (in days) during which Capture Agent tries to connect to Quick Connect Service to send the information about changed user passwords. During this period Capture Agent stores the user passwords to be synchronized in an encrypted file.	7 days
Set certificate	Specifies a certificate for encrypting the password sync data transferred between Capture Agent and Quick Connect Service. For more information, see Specifying a custom certificate for encrypting password sync traffic.	By default, a built-in certificate is used.

Parameter	Description	Default value
Connection Point 1	Define the Quick Connect Service instances to which Capture Agent provides information about changed user passwords.	If none of these parameters is set, Capture Agent looks for available instances of the Quick Connect Service in the following container: CN=QuickConnect,CN=One Identity,CN=System,DC=*<DomainName>*
Connection Point 2		
Connection Point 3		
Connection Point 4		
Connection Point 5		
Connection Point 6		
Connection Point 7		

You can modify the default values of these parameters by using Group Policy and the Administrative Template supplied with the One Identity Quick Connect Sync Engine. The next steps assume that all the domain controllers where the Capture Agent is installed are held within organizational units.

Complete these steps to modify the default Capture Agent settings:

- Step 1: Create and link a Group Policy object
- Step 2: Add administrative template to Group Policy object
- Step 3: Use Group Policy object to modify Capture Agent settings

Step 1: Create and link a Group Policy object

Create a new Group Policy object. Link the object to each organizational unit holding the domain controllers on which the Capture Agent is installed. For more information, see the documentation for your version of the Windows operating system.

Step 2: Add administrative template to Group Policy object

1. Use Group Policy Object Editor to connect to the Group Policy object you created in step 1.
2. In the Group Policy Object Editor console, expand the Group Policy object, and then do one of the following:
    - In Windows Server 2003 or Windows Server 2003 R2, expand the **Computer Configuration** node, and then select **Administrative Templates**.
    - In a later version of Windows Server, expand **Computer Configuration**, expand **Policies**, and then select **Administrative Templates**.
3. On the **Action** menu, point to **All Tasks**, and click **Add/Remove Templates**.

   The **Add/Remove Templates** dialog box opens.

4. In the **Add/Remove Templates** dialog box, click **Add**, and then use the **Policy Templates** dialog box to open the Administrative Template (CaptureAgentService.adm file) supplied with the One Identity Quick Connect Sync Engine.

   The CaptureAgentService.adm file is located in <One Identity Quick Connect Sync Engine installation folder>**\Quick Connect Capture Agent\Administrative Templates**.

Step 3: Use Group Policy object to modify Capture Agent settings

1. In Windows Server 2003 or Windows Server 2003 R2, under **Computer Configuration\Administrative Templates\Quick Connect**, select **Quick Connect Capture Agent Service**.

   In a later version of Windows Server, under **Computer Configuration\Policies\Administrative Templates\Classic Administrative Templates (ADM)\Quick Connect**, select **Quick Connect Capture Agent Service**.
2. In the details pane, configure the appropriate Group Policy settings.

   The names of Group Policy settings correspond to the names of the Capture Agent parameters provided in the table in Configuring Capture Agent.
3. Run the following command at a command prompt for the changes to take effect:

   ```
   gpupdate /force
   ```

Configuring Quick Connect Service

You can modify the default values of the Quick Connect Service parameters related to password synchronization. These parameters and their default values are described in the next table.

Table 17: Quick Connect Service parameters

Parameter	Description	Default Value
Set interval between attempts to reset password	The Capture Agent sends information on changes made to Active Directory user passwords to the Quick Connect Service. After receiving this information,	10 minutes

Parameter	Description	Default Value
	the Quick Connect Service tries to reset passwords in the target connected systems specified. This parameter determines the time interval (in minutes) between attempts to reset passwords in the target connected systems.	
Set service connection point update period	The Quick Connect Service publishes its connection point in Active Directory. This parameter determines the frequency of updates (in minutes) of the Quick Connect Service connection point.	60 minutes
Set certificate	This parameter specifies the thumbprint of the certificate used to encrypt the password sync traffic between Capture Agent and Quick Connect Service. The same certificate must be used for the Capture Agent and the Quick Connect Service.	By default, a built-in certificate is used.

You can modify the Quick Connect Service parameters using Group Policy and the Administrative Template supplied with the One Identity Quick Connect Sync Engine.

To modify the Quick Connect Service parameters using Group Policy

1. On the computer running the Quick Connect Service, start Group Policy Object Editor, and then connect to the **Local Computer Policy** Group Policy object.
2. In the Group Policy Object Editor console, expand the **Local Computer Policy** node, expand the **Computer Configuration** node, and select **Administrative Templates**.
3. On the **Action** menu, point to **All Tasks**, and click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, click **Add**, and then use the **Policy Templates** dialog box to open the **PasswordService.adm** file that holds the Administrative Template.

   By default, the PasswordService.adm file is stored in <Quick Connect installation folder>**\Quick Connect Capture Agent\Administrative Templates**

5. Under **Computer Configuration\Administrative Templates\Quick Connect**, select **Quick Connect Password Service**, and then in the details pane, configure the appropriate group policy settings.

   The names of group policy settings correspond to the names of the Quick Connect Service parameters provided in the table in Configuring Capture Agent.

6. For the changes to take effect, refresh the Group Policy settings by running the following command at a command prompt: **gpupdate /force**

Specifying a custom certificate for encrypting password sync traffic

By default, Quick Connect uses a built-in certificate to encrypt password sync traffic between the Capture Agent and the Quick Connect Service. If necessary, you can use a custom certificate for this purpose.

This section illustrates how to use a custom certificate for encrypting the password synchronization traffic in Windows Server 2003.

Complete the following steps:

- Step 1: Obtain and install a certificate
- Step 2: Export custom certificate to a file
- Step 3: Import certificate into certificates store
- Step 4: Copy certificate’s thumbprint
- Step 5: Provide certificate’s thumbprint to Capture Agent
- Step 6: Provide certificate’s thumbprint to Quick Connect Service

Step 1: Obtain and install a certificate

To obtain and install a certificate, you have to make a certificate request. There are two methods to request a certificate in Windows Server 2003:

- **Request certificates using the Certificate Request Wizard**. To request certificates from a Windows Server 2003 enterprise certification authority, you can use the Certificate Request Wizard.
- **Request certificates using the Windows Server 2003 Certificate Services Web interface**. Each certification authority that is installed on a computer running Windows Server 2003 has a Web interface that allows the users to submit certificate requests. By default, the Web interface is accessible at **http://servername/certsrv**, where **servername** refers to the name of the computer running Windows Server 2003.

This section provides steps to request certificates using the Windows Server 2003 Certificate Services Web interface. For detailed information about the Certificate Request Wizard, refer to the documentation on Certification Authority.

To request a certificate using the Windows 2003 Certificate Services Web interface

1. Use a Web browser to open to **http://servername/certsrv**, where **servername** refers to the name of the Web server running Windows Server 2003 where the certification authority that you want to access is located.
2. On the **Welcome** Web page, click **Request a certificate**.
3. On the **Request a Certificate** Web page, click **advanced certificate request**.
4. On the **Advanced Certificate Request** Web page, click **Create and submit a certificate request to this CA**.
5. On the Web page that opens, do the following:
    a. Select the **Store certificate in the local computer certificate store** check box.
    b. Under **Additional Options**, select the **PKCS10** option, and in the **Friendly Name** text box, specify a name for your certificate (such as My QC Certificate).

    Keep default values for all other options.
6. Click **Submit**.
7. On the **Certificate Issued** Web page, click **Install this certificate**.

After you install the certificate, it becomes available in the Certificates snap-in, in the **Personal/Certificates** store.

Step 2: Export custom certificate to a file

In this step, you export the issued certificate to a file. You will need the file to install the certificate on each domain controller running Capture Agent and on each computer running Quick Connect Service.

To export the certificate

1. On the computer where you installed the certificate in step 1, open the Certificates - Local Computers snap-in.
2. In the console tree, click the **Personal/Certificates** store.
3. In the details pane, click the issued certificate you want to export.
4. On the **Action** menu, point to **All Tasks**, and then click **Export**.
5. Step through the wizard.
6. On the **Export Private Key** page, select **Yes, export the private key**, and then click **Next**.

This option is available only if the private key is marked as exportable and you have access to the private key.

7. On the **Export File Format** page, do the following, and then click **Next**:
   - To include all certificates in the certification path, select the **Include all certificates in the certification path if possible** check box.
   - To enable strong protection, select the **Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)** check box.
8. On the **Password** page, use the **Password** text box to type a password to encrypt the private key you are exporting. In **Confirm password**, type the same password again, and then click **Next**.
9. On the **File to Export** page, use the **File name** text box to specify the PKCS #12 file to which you want to export the certificate along with the private key, and click **Next**.
10. On the Completion page, revise the specified settings and click **Finish** to create the file and close the wizard.

Step 3: Import certificate into certificates store

In this step, you import the certificate to the **Personal\Certificates** certificate store by using the Certificates snap-in. You must complete this step on each domain controller running Capture Agent and on each computer running the Quick Connect Service that will participate in the password synchronization.

To import the certificate

1. Open the Certificates - Local Computers snap-in.
2. In the console tree, click the **Personal\Certificates** logical store.
3. On the **Action** menu, point to **All Tasks** and then click **Import**.
4. Step through the wizard.
5. On the **File to Import** page, in **File name**, type the file name containing the certificate to be imported or click **Browse** and to locate and select the file. When finished, click **Next**.
6. On the **Password** page, type the password used to encrypt the private key, and then click **Next**.
7. On the **Certificate Store** page, ensure that the **Place all certificates in the following store** option is selected, and the **Certificate store** text box displays **Personal**, and then click **Next**.
8. On the **Completion** page, revise the specified settings and click **Finish** to import the certificate and close the wizard.

Step 4: Copy certificate’s thumbprint

In this step, you copy the thumbprint of your custom certificate. In the next steps, you will need to provide the thumbprint to Capture Agent and Quick Connect Service.

To copy the thumbprint of your custom certificate

1. Open the Certificates - Local Computer snap-in.
2. In the console tree, click the **Personal** store to expand it.
3. Click the **Certificates** store to expand it.
4. In the details pane, double-click the certificate.
5. In the **Certificate** dialog box, click the **Details** tab, and scroll through the list of fields to select **Thumbprint**.
6. Copy the hexadecimal value of Thumbprint to Clipboard.

   You will need the copied thumbprint value to configure the Capture Agent and Quick Connect Service.

Step 5: Provide certificate’s thumbprint to Capture Agent

This step assumes that:

- The same Group Policy object is linked to each OU holding the domain controllers on which the Capture Agent is installed. For more information on how to create and link a Group policy object, see the documentation for your version of Windows.
- The CaptureAgentService.adm administrative template file is linked to that Group Policy object.

  For instructions on how to add an administrative template file to a Group Policy object, see Step 2: Add administrative template to Group Policy object

To provide the thumbprint to Capture Agent

1. On any computer joined to the domain where Capture Agent is installed, open Group Policy Object Editor, and connect to the Group Policy object to which you added the Administrative Template in Step 2: Add administrative template to Group Policy object.
2. In the Group Policy Object Editor console, expand the Group Policy object, and then expand the **Computer Configuration** node.
3. Expand the **Administrative Templates\Quick Connect** node to select **Quick Connect Capture Agent Service**.
4. In the details pane, double-click **Set certificate**.

5. In the **Certificate Properties** dialog box, open the **Set certificate properties** tab, select the **Enabled** option, and then paste the certificate's thumbprint (the one you copied in Step 4: Copy certificate's thumbprint) in the **Thumbprint** text box. When finished, click **OK**.
6. For the changes to take effect, refresh the Group Policy settings by running the following command at a command prompt: **gpupdate /force**

Step 6: Provide certificate's thumbprint to Quick Connect Service

Perform the next steps on each computer running the Quick Connect Service that participates in the password sync operations.

To provide the thumbprint to Quick Connect Service

1. On the computer running the Quick Connect Service, start Group Policy Object Editor, and then connect to the **Local Computer Policy** Group Policy object.
2. In the Group Policy Object Editor console, expand the **Local Computer Policy** node, expand the **Computer Configuration** node, and select **Administrative Templates**.
3. On the **Action** menu, point to **All Tasks**, and click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, click **Add**, and then use the **Policy Templates** dialog box to open the **PasswordService.adm** file that holds the Administrative Template.

   By default, the PasswordService.adm file is stored in <Quick Connect installation folder>**\Quick Connect Capture Agent\Administrative Templates**
5. Under **Computer Configuration\Administrative Templates\Quick Connect**, select **Quick Connect Password Service**.
6. In the details pane, double-click **Set certificate**.
7. In the **Certificate Properties** dialog box, open the **Set certificate properties** tab, select the **Enabled** option, and then paste the certificate's thumbprint (the one you copied in Step 4: Copy certificate's thumbprint) in the **Thumbprint** text box. When finished, click **OK**.
8. For the changes to take effect, refresh the Group Policy settings by running the following command at a command prompt: **gpupdate /force**

Using PowerShell scripts with password synchronization

Optionally, you can configure the One Identity Quick Connect Sync Engine to run your custom PowerShell script before, after, or instead of the password synchronization operation. To do so, create a connection handler. For instructions, see Using connection handlers.

Example of a PowerShell script run after password synchronization

```
#---- Specify the SMTP Server name in your organization ----
$SmtpServer = "smtpServerName"
$smtp = new-object system.net.mail.smtpClient($SmtpServer)
$mail = new-object System.Net.Mail.MailMessage
# ---- Set the sender mail ----
$mail.From = "yourmail@mydomain.com"
# ---- Set the destination mail ----
$mail.To.Add("Administrator@mydomain.com")
# --- Specify the message subject ----
$mail.Subject = "Password was changed"
# ---- Set the message text ----
$body = "The passwords were synchronized for the following object pair: "
$body = $body + $srcObj.Name + "->" + $dstObj.Name
$mail.Body = $body
# ---- Send mail ----
$smtp.Send($mail)
```

Description: After the password synchronization is complete, this script sends a notification email message informing the administrator that the specified object password has been modified in the target connected system. The message provides the names of the source Active Directory object and its counterpart in the target connected system.

Synchronization history

About synchronization history

Quick Connect Administration Console provides the Synchronization History feature that allows you to view the details of completed synchronization workflow runs, password sync rule runs, and map and unmap operations.

The synchronization history also helps you troubleshoot synchronization issues by providing information on the errors that were encountered during synchronization workflow runs, password sync rule runs, or map and unmap operations.

You can also selectively clean up entries from the synchronization history.

To access the synchronization history, use the **Sync History** tab in the Quick Connect Administration Console.

In this chapter:

- Viewing workflow history
- Viewing mapping history
- Searching Synchronization History
- Cleaning up synchronization history

Viewing workflow history

You can use the **Sync History** tab in the Quick Connect Administration Console to view a list of completed synchronization workflow runs. This list provides such information as the names of completed workflows, the dates when each workflow run started and completed, and which Quick Connect Service instance was used to run each workflow.

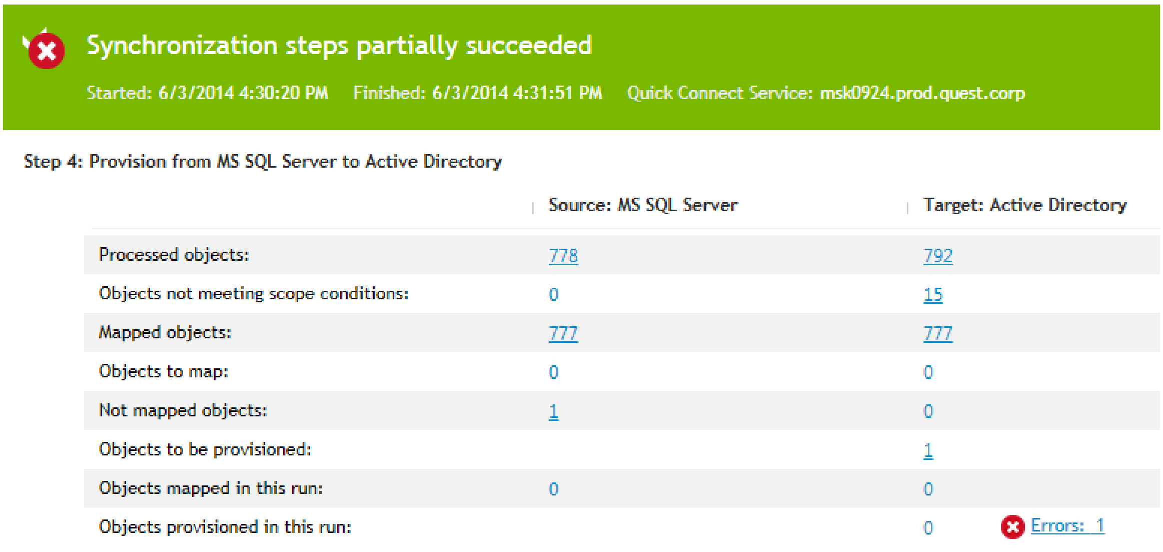
You can click a workflow run entry in the list to view detailed information about the workflow steps that were run, objects that participated in that run, and errors encountered during the run, if any.

To view the details of a completed workflow run

1. In the Quick Connect Administration Console, open the **Sync History t**ab.
2. Click **Workflow History**.
3. If you want to filter the list of completed workflows, use the following elements:
    - **Show items completed**. Use this element to specify the time period when the workflows you want to view completed.
    - **Maximum number of items to show**. Specify the maximum number of completed workflows you want to view.

   You can sort the list of completed workflows by clicking the column titles in the list. Also you can filter the list of completed workflows by typing keywords in the text boxes provided below the column titles.
4. To view detailed information about a list entry, select that list entry, and then click the **Details** button.

   The details provided for each list entry look similar to the following:



✖ Synchronization steps partially succeeded

Started: 6/3/2014 4:30:20 PM Finished: 6/3/2014 4:31:51 PM Quick Connect Service: msk0924.prod.quest.corp

Step 4: Provision from MS SQL Server to Active Directory

	Source: MS SQL Server	Target: Active Directory	
Processed objects:	778	792	
Objects not meeting scope conditions:	0	15	
Mapped objects:	777	777	
Objects to map:	0	0	
Not mapped objects:	1	0	
Objects to be provisioned:		1	
Objects mapped in this run:	0	0	
Objects provisioned in this run:		0	✖ Errors: 1

To view detailed information about the objects that belong to a certain object category, click the number displayed next to the object category name in the **Source** or **Target** column.

To view detailed information about encountered errors, click the link displaying the number of errors.

Viewing mapping history

You can use the **Sync History** tab in the Quick Connect Administration Console to view the detailed information about a particular completed map or unmap operation. By doing so, you can view a list of attributes for each object that participated in the map or unmap operation.

To view the details of a mapped pair of objects

1. In the Quick Connect Administration Console, open the **Sync History** tab.
2. Click **Mapping History**.
3. If you want to filter the list of completed map and unmap operations, use the following elements:
    - **Show items completed**. Specify a time period when the map and unmap operations you want to view completed.
    - **Maximum number of items to show**. Specify the maximum number of completed map and unmap operations you want to view.

    You can sort the list of map and unmap operations by clicking the column titles. Also you can filter the list of map and unmap operations by typing keywords in the text boxes provided below the column titles.
4. To view detailed information about a list entry, select that list entry, and then click the **Details** button.

Searching synchronization history

You can use the **Sync History** tab in the Quick Connect Administrative Console to search for completed provision, deprovision, update, and sync passwords operations in the synchronization history. You can search by such criteria as target connected system on which the operation was run, type of object that participated in the operation, and period during which the operation completed.

To search the synchronization history for completed operations

1. In the Quick Connect Administration Console, open the **Sync History** tab.
2. Click **Search**.

3. Use the following options to specify your search criteria:
    a. **Target connection**. Select the connected system for which you want to search for completed provision, deprovision, update, and sync passwords operations.
    b. **Object type**. Select the object type for which you want to search for completed provision, deprovision, update, and sync passwords operations.
    c. **Show items completed**. Specify the time period during which the operation you want to search for completed.
    d. **Maximum number of items to show**. Specify the maximum number of completed provision, deprovision, update, and sync passwords operations you want to view in the list.

    You can sort the search results by clicking the column titles in the search results list. Also you can filter the search results by typing keywords in the text boxes provided below the column titles.
4. To view detailed information about an entry in the search results list, select that entry, and then click the **Details** button.

Cleaning up synchronization history

You can selectively delete entries from the workflow history and object mapping history. To delete entries, you can either run the cleanup operation once or you can create a recurring schedule to run the cleanup operation on a regular basis.

To run the cleanup operation once

1. In the Quick Connect Administration Console, open the **Sync History** tab.
2. Click **Clean up now**.
3. Specify what entries you want to delete.
4. Click **OK** to delete the entries from the synchronization history.

To create a recurring schedule for the cleanup operation

1. In the Quick Connect Administration Console, open the **Sync History** tab.
2. Click **Schedule cleanup**.
3. In the dialog box that opens, select the **Schedule the task to run** check box, and then specify a schedule for the cleanup operation.
4. If several One Identity Quick Connect Sync Engine instances are deployed in your environment, under **Run the task on**, select the computer that hosts the instance you want to use for running the cleanup operation.
5. Click **OK** to activate the schedule.

To disable a scheduled cleanup operation

1. In the Quick Connect Administration Console, open the **Sync History** tab.
2. Click **Schedule cleanup**.
3. In the dialog box that opens, clear the **Schedule the task to run** check box, and then click **OK**.

Scenarios of use

About scenarios

This section provides some use case scenarios that help you familiarize yourself with Quick Connect. The scenarios illustrate how to create and run synchronization workflows and their steps to update and provision user information from a Human Resources database represented by a delimited text file to an Active Directory domain.

The scenarios are:

- Scenario 1: Provision users from a .csv file to an Active Directory domain. In this scenario, Quick Connect provisions user accounts from a Comma Separated Values (.csv) file that includes a Human Resources (HR) database to individual Organizational Units in an Active Directory domain, depending on the city where each user is based.
- Scenario 2: Use a .csv file to update user accounts in an Active Directory domain. In this scenario, Quick Connect updates user accounts in an Active Directory domain based on the changes made to the Human Resources (HR) database saved in a Comma Separated Values (.csv) file.

- Scenario 3: Synchronizing data between One Identity Manager Custom Target Systems and an Active Directory domain. In this scenario, Quick Connect updates data in One Identity Manager based on the changes made in Active Directory domain.
- Scenario 4: Deprovisioning between One Identity Manager Custom Target Systems and an Active Directory domain. In this scenario, Quick connect deprovisioning synchronized objects in One Identity Manager processed from the Active Directory domain.
- Scenario 5: Provisioning of Groups between One Identity Manager Custom Target Systems and an Active Directory domain. In this scenario, Quick Connect provisions group objects to be synchronized to One Identity Manager from Active Directory domain.
- Scenario 6: Enabling Delta Sync mode between One Identity Manager Custom Target Systems and an Active Directory domain. In this scenario, Quick Connect updates data in One Identity Manager based on the changes made in Active Directory domain in the delta sync mode.

Before you proceed with these sample scenarios (Scenario 1 and Scenario 2), perform the following steps:

1. Make sure you have installed the Quick Connect for Base Systems package. For the installation instructions, see the Quick Connect for Base Systems documentation.
2. Make sure you have properly configured the connection to the target Active Directory domain in the Quick Connect Administration Console.
3. Create the Employees Organizational Unit (OU) at the root of the target Active Directory domain.
4. In the Employees OU, create the following OUs:
    - New York
    - Tokyo
    - Amsterdam
    - OtherCities

Scenario 1: Provision users from a .csv file to an Active Directory domain

The following scenario demonstrates how to provision user accounts from a Human Resources (HR) database to an Active Directory domain. The HR database is represented by a sample Comma Separated Values (.csv) file supplied with the Quick Connect for Base Systems package. Depending on the user city, accounts will be provisioned to one of the following OUs:

- Employees\New York
- Employees\Tokyo

- Employees\Amsterdam
- Employees\OtherCities

This scenario includes the following steps:

- Step 1: Create a workflow
- Step 2: Create a provisioning step
- Step 3: Run the created provisioning step
- Step 4: Commit changes to Active Directory

Step 1: Create a workflow

To create a new synchronization workflow

1. Start the Quick Connect Administration Console.
2. Open the **Workflows** tab, and then click **Add workflow**.
3. Type a descriptive name for the workflow being created, and then click **OK** to create the workflow.

Step 2: Create a provisioning step

This section provides instructions on how to:

- Connect Quick Connect to the source Comma Separated Values (.csv) file and target Active Directory domain.
- Create a new provisioning step and configure its settings, for example, specify the object attributes to provision.
- Develop a Windows PowerShell script that returns the name of an Active Directory container for provisioned user accounts.

Preview a list of user accounts to be provisioned.

To create a provisioning step

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow you created in Step 1: Create a workflow.
2. Click **Add synchronization step**.
3. On the **Select an action** page, select **Provision**, and then click **Next**.
4. On the **Specify source and criteria** page, click **Specify**, click **Add new connected system**, and then step through the wizard to add the sample Comma Separated Values (.csv) file as a connected system:

a. Use the **Connection name** box to type a descriptive name for the connection being created.

b. In the **Use the specified connector** list, select **Delimited Text File Connector**. Click **Next**.

c. Click **Browse** to locate and select the sample Comma Separated Values (.csv) file supplied with the Quick Connect for Base Systems package. This file is located in the folder *<One Identity Quick Connect Sync Engine installation folder>***\Samples**.

d. Step through the wizard until you are on the **Specify attributes to identify objects** page.

e. In the **Available attributes** list, select **Employee ID**, click **Add**, and then click **Finish**.

5. Click **Next**.

   a. On the **Specify target** page, click **Specify**, and then step through the wizard to add the target Active Directory domain as a connected system:

   b. Use the **Connection name** box to type a descriptive name for the connection being created.

   c. In the **Use the specified connector** list, select **Active Directory Connector**. Click **Next**.

6. Use the **Domain name** box to type the FQDN name of the target Active Directory domain. If necessary, adjust other connection settings on this page as appropriate. Click **Finish**.

7. Click the down arrow on the button provided next to the **Target container** option.

8. In the provided list, click **PowerShell Script**.

9. Insert the following script sample into the dialog box, and then click **OK**:

```
$userCity = $srcObj["City"]
 switch ($userCity)
{
  "New York" {$container = "OU=New York,OU=Employees,DC=mycompany,DC=com";
break}
  "Amsterdam" {$container = "OU=Amsterdam,OU=Employees,DC=mycompany,DC=com";
break}
  "Tokyo" {$container = "OU=Tokyo,OU=Employees,DC=mycompany,DC=com"; break}
  default {$container = "OU=OtherCities,OU=Employees,DC=mycompany,DC=com";
break}
}
$container
```

NOTE: Before using the script, change the "DC=mycompany",DC=com" string as appropriate to reflect your environment. For example, if you have created the Employees OU in the testlab.ttt domain, use the following string: "DC=testlab,DC=ttt".

10. Click the down arrow on the leftmost button provided below the **Rules to generate unique object name** list.
11. In the provided list, click **Attribute**.
12. Select **Logon Name**, and then click **OK**. Click **Next**.
13. Expand **Initial Attribute Population Rules**, and then create forward sync rules to synchronize the following pairs of attributes:

    Table 18: Initial attribute population rules

CSV file attribute	Synchronization direction	Active Directory attribute
Logon Name	=>	Logon Name (Pre-Windows 2000)
First Name	=>	First Name
Last Name	=>	Last Name
City	=>	City

    For information on how to create rules, see Modifying attribute values by using rules.
14. Expand **Initial Password**, click **Text**, and type a password in the **Set Password** dialog box. Click **OK**.
15. Optionally, you can expand **User Account Options** to modify the default options to create new user accounts.
16. Click **Finish** to close the wizard.

Step 3: Run the created provisioning step

To run the provisioning step

1. On the **Workflows** tab, click **Run now**.
2. In the **Select workflow steps to run** dialog box, select the check box next to the step you created, and then click **Full Run** to run the step.

   After the synchronization step run completes, the Quick Connect Administration Console displays a report that provides information about the objects that participated in the provisioning step. At this stage, the application does not commit changes to the target Active Directory domain.

NOTE: To view a list of user accounts to be created in the Employees OU, click the number next to **Objects to be provisioned**.

Step 4: Commit changes to Active Directory

- Click **Commit**.

  > NOTE: You can use the Active Directory Users and Computers tool to ensure that Quick Connect has created user accounts in the Employees OU. The New York, Tokyo, Amsterdam, and OtherCities OUs may include some disabled user accounts created by Quick Connect.

Scenario 2: Use a .csv file to update user accounts in an Active Directory domain

This scenario demonstrates how to update user accounts in an Active Directory domain when the information on employees is changed in the Human Resource (HR) database held in a Comma Separated Values (.csv) file.

> NOTE: This scenario can be used only if the Employees OU already contains user accounts created with the provisioning scenario described earlier in this document. Only accounts for previously provisioned employees will be updated.

This scenario has the following steps:

- Step 1: Create an updating step
- Step 2: Run the created updating step
- Step 3: Commit changes to Active Directory

Step 1: Create an updating step

This section explains how to create a step that updates user accounts from the HR database to the target Active Directory domain.

To add an updating step to your existing workflow

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow you have created in Step 1: Create a workflow.
2. Click **Add synchronization step**.
3. On the **Select an action** page, select **Update**, and then click **Next**.

4. On the **Specify source and criteria** page, do the following:
    a. Click **Specify**, click **Select existing connected system**, and then select the Comma Separated Values (.csv) file you connected in Scenario 1: Provision users from a .csv file to an Active Directory domain. Click **Finish**.
    b. Make sure that the object type specified in the **Source object type** box is **csv-Object**.
5. Click **Next**.
6. On the **Specify target** page, do the following:
    a. Click **Specify**, and then select the Active Directory domain you connected in Scenario 1: Provision users from a .csv file to an Active Directory domain.
    b. Make sure that the object type specified in the **Target object type** box is **User (user)**.
7. Click **Next**.
8. Expand **Rules to Modify Object Attributes**, and then create forward sync rules to synchronize the following pairs of attributes:

    Table 19: Rules to modify object attributes

CSV file attribute	Synchronization direction	Active Directory attribute
City	=>	City
Department	=>	Department
First Name	=>	First Name
Last Name	=>	Last Name
Telephone Number	=>	Telephone Number

    For information on how to create rules, see Modifying attribute values by using rules.
9. Click **Finish**.

Step 2: Run the created updating step

To run the updating step

1. On the **Workflows** tab, click **Run now**.
2. In the **Select workflow steps to run** dialog box, select the check box next to the step you created, and then click **OK** to run the step.

    After the synchronization step run completes, the Quick Connect Administration Console displays a report that provides information about the objects that participated in the provisioning step. At this stage, the application does not commit changes to the target Active Directory domain.

NOTE: To view a list of user accounts to be updated in the Employees OU, in the update report, click the number next to **Objects to be updated**.

Step 3: Commit changes to Active Directory

To commit changes to the target Active Directory domain

- Click **Commit**.

Scenario 3: Synchronizing data between One Identity Manager Custom Target Systems and an Active Directory domain

Out of the box, One Identity Quick Connect Sync Engine includes the One Identity Manager connector, which allows you to access the One Identity Manager. In this scenario, the basic purpose for the Quick Connect One Identity Manager connector is to use the connector for target systems where there is no existing native One Identity Manager connector.

Administrators can create or configure multiple Custom Target Systems in One Identity Manager. Each Target System has entities such as User Accounts, Groups, Container Structure, and so on.

NOTE: One Identity Manager does not have any specific table space for target systems that do not have a native One Identity Manager connector. The data synchronized is placed in the One Identity Manager tablespace where the tables starts with UNS.. and end with B, referred as UNS..B tables.

The following scenario shows how to use the Quick Connect One Identity Manager Connector to synchronize data between One Identity Manager Custom Target Systems and Active Directory domain.

This scenario includes the following steps:

- Step 1: Create connection to One Identity Manager
- Step 2: Configure One Identity Manager modules, Custom Target System and Container Information
- Step 3: Create Workflow for Provisioning
- Step 4: Create Provisioning
- Step 5: Specify the synchronization rules
- Step 6: Execute Workflow

- Step 7: Commit changes to One Identity Manager
- Step 8: Verify on One Identity Manager

Step 1: Create connection to One Identity Manager

To create a new connection to One Identity Manager:

1. In the Quick Connect Administration Console, open the **Connections** tab.
2. Click **Add connection**, and then use the following options:
   - **Connection name**. Type a descriptive name for the connection.
   - **Use the specified connector**. Select **One Identity Manager Connector**.
3. Click **Next**.
4. On the **Specify connection settings** page, use the following options:
   - **Application Server URL**. Specify the address of the One Identity Manager application server to which you want to connect.
   - **Authentication module**. Identifies the One Identity Manager authentication module to be used to verify the connection's user ID and password.
   - **User name**. Specify the user ID for this connection.
   - **Password**. Specify the password of the user ID for this connection.
   - **Test Connection**. Click to verify the specified connection settings.
5. Click **Next**.

Step 2: Configure One Identity Manager modules, Custom Target System and Container Information

NOTE: The One Identity Manager target systems and One Identity Manager containers are applicable only for the Target System Base module.

To select the One Identity Manager modules, Target Systems, and Containers:

1. Select the required One Identity Manager modules.
2. Select **Target System Base module** to synchronize data to One Identity Manager custom target systems (UNS..B tables). This enables you to select the target object types such as UNSAccountB, UNSGroupB, and so on.
3. Select the required One Identity Manager target system, for example *Azure*.

4. Select the required One Identity Manager container, for example *Test AD*.
5. Click **Finish** to create a connection to **One Identity Manager**.

Step 3: Create Workflow for Provisioning

To create a workflow for provisioning data synchronization to One Identity Manager:

1. Start the **One Identity Quick Connect Administration Console**.
2. Open the **Workflows** tab, and then click **Add workflow**.
3. Type a descriptive name, for example *AD to D1IM Sync* for the workflow being created, and then click **OK** to create the workflow.

Step 4: Create Provisioning

To create a provisioning step:

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow *AD to 1IM Sync*.
2. Click **Add synchronization step**.
3. On the **Select an action** dialog box, select **Provision**, and then click **Next**.
4. On the **Specify source and criteria** dialog box, click **Specify**, click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the Active Directory *Test AD* as a connected system.
5. Click **Next**.
6. On the **Specify target** dialog box, click **Specify.**
7. Click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the target One Identity Manager domain as a connected system.
8. Click **Select**, to add the required target object type.
9. On the **Select Object Type** dialog box, select the object type **UNSAccountB** from the list of object types.
10. Click **Ok.**

Step 5: Specify the synchronization rules

To specify the synchronization rules:

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow *Ad to 1IM Sync*.
2. Click the step **Provision from** *Test AD* **to One Identity Manager Connection**.
3. Click **Provisioning Rules** and then click **Initial Attribute Population Rules**.
4. Click **Forward Sync Rule** from the drop-down menu.
5. On the **Forward Sync Rule** dialog box, select the source attributes to be mapped to the target attributes, and then click **OK**.

   > ℹ NOTE: For One Identity Manager workflows, the attribute configuration rule for **CN** is mandatory, else a constraint violation error is displayed and the workflow execution does not succeed.

6. Click **Save and Continue**.

Step 6: Execute Workflow

To run the provisioning step:

1. On the **Workflows** tab, click **Run now**.
2. In the **Select workflow steps to run** dialog box, select the check box next to the step you created, and then click **Full Run** to run the step.

   After the synchronization step run completes, the Quick Connect Administration Console displays a report that provides information about the objects that participated in the provisioning step. At this stage, the application does not commit changes to the target One Identity Manager domain.

Step 7: Commit changes to One Identity Manager

To commit the changes to One Identity Manager:

- Click **Commit**.

A message *All changes committed* is displayed. The changes are committed from the source Active Directory *Test AD* to the target One Identity Manager.

Step 8: Verify on One Identity Manager

To verify if the data is synchronized to One Identity Manager:

- Open the **One Identity Manager** console and verify that all the users from the AD are synchronized with One Identity Manager as per the provisioning rules that were set.

Scenario 4: Deprovisioning between One Identity Manager Custom Target Systems and an Active Directory domain

The Deprovisioning operation in data synchronization using Quick Connect Sync Engine allows you to modifies or removes objects in the target data system after their counterparts have been disconnected from the source data system. Quick Connect Sync Engine can be configured to remove target objects permanently or change them to a specific state. To specify the objects that will participate in the deprovision operation you can use object mapping rules. This scenario describes how to create a deprovisioning step for a workflow to modify or delete the synchronized objects in the target system based on the deprovisioning criteria that is set.

To create a deprovisioning step:

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow *AD to 1IM Sync*.
2. Click **Add synchronization step**.
3. On the **Select an action** dialog box, select Dep**rovision**, and then click **Next**.
4. On the **Specify source and criteria** dialog box, click **Specify**, click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the Active Directory *Test AD* as a connected system.
5. Specify a deprovisioning criteria by selecting one of the following:
   - Source object is deleted or out of synchronization scope
   - Source object deprovisioning is initiated in connected system
   - Source object meets these criteria - Add the criteria for the source objects to be deprovisioned in the target system
6. Click **Next**.
7. On the **Specify target** dialog box, click **Specify.**

8. Click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the target One Identity Manager domain as a connected system.
9. Click **Select**, to add the required target object type.
10. On the **Select Object Type** dialog box, select the object type **UNSAccountB** from the list of object types and click **Ok.**
11. On the **Specify deprovisioning action** dialog box, select the one of the following action to deprovision:
    - Delete target objects
    - Initiate the object deprovisioning in <*target system*>
    - Modify target objects - Click Forward Synch rule and select the attributes to modify the object attributes.
12. Click **Next.**

    The Deprovisioning step with the rules for the specified deprovisioning action is created.

Scenario 5: Provisioning of Groups between One Identity Manager Custom Target Systems and an Active Directory domain

One Identity Quick Connect Sync Engine allows you to ensure that group membership information is in sync in all connected data systems. For example, when provisioning a group object from an Active Directory domain to One Identity Manager domain, you can configure rules to synchronize the Member attribute from the source to the target domain.

This scenario describes how to create a provisioning step for a workflow to synchronize group objects between the source and target systems.

To create a group provisioning step:

1. In the Quick Connect Administration Console, open the **Workflows** tab, and then click the workflow *AD to 1IM Sync*.
2. Click **Add synchronization step**.
3. On the **Select an action** dialog box, select **Provision**, and then click **Next**.
4. On the **Specify source and criteria** dialog box, click **Specify**, click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the Active Directory *Test AD* as a connected system.
5. In **Specify object type** field, click **Select** and from the **Select Object type** list, select **Group** and then click **OK**.

6. In the **Provisioning Criteria** section, click Add.
7. On the **Select Container** dialog box, from the containers list, select the required container and click OK.
8. Click **Next**.
9. On the **Specify target** dialog box, click **Specify.**
10. Click **Add new connected system** or **Select existing connected system**, and then step through the wizard to add the target One Identity Manager domain as a connected system.
11. Click **Select**, to add the required target object type.
12. On the **Select Object Type** dialog box, select the object type **UNSGroupB** from the list of object types.
13. Click **Ok.**

    The Group provisioning step is created.

Scenario 6: Enabling Delta Sync mode between One Identity Manager Custom Target Systems and an Active Directory domain

The Delta processing mode of the Quick Connect Sync Engine allows you to synchronize identities between the source and the target systems for only the data that has changed in the source and target connected systems since their last synchronization.

This scenario describes how to enable the delta processing mode between the source (Active Directory domain) and target (One Identity Manager) systems.

To enable the delta processing mode:

1. Step 1: Create a workflow for provisioning data synchronization between the source (Active Directory) and target (One Identity Manager) system.
2. Step 2: Create a provisioning step for the workflow to provision users from the source system to target system.
3. Click on the synchronization step for provision of users.
4. In the **General Options** tab, specify the delta process mode:
    - Under **Source Connected System** select the option **Process delta from last run**.
    - Under **Target Connected System** select the option **Process delta from last run**.
    - Click **Save and continue** .

NOTE: Before any data has been processed from the source to the target system, the initial synchronization of data is always performed in the **Process all delta** mode.

5. Step 3: Run the created provisioning step.

   The data for the users added or updated to the source since the previous run, is displayed under Processed Objects.

A

Appendices

Appendix A: Developing PowerShell scripts for attribute synchronization rules

You can configure synchronization rules for steps performing such as provisioning, deprovisioning, or update synchronization rules. One Identity Quick Connect Sync Engine provides a user interface (Quick Connect Administration Console) that allows you to set up a direct or rules-based synchronization rule without any coding (for more information, refer to the Quick Connect Administrator Guide).

However, to set up a script-based synchronization rule, you must develop a Windows PowerShell script that will build values of the target object attributes using values of the source object attributes.

This section provides some reference materials on using the Windows PowerShell Script Host feature and provides the sample script.

Accessing source and target objects using built-in hash tables

One Identity Quick Connect Sync Engine synchronizes data between the source and target objects using the pre-configured synchronization rules.

In the PowerShell scripts used to set up the script-based synchronization rules, you can employ the **$srcObj** and **$dstObj** built-in associative arrays (hash tables) that allow the scripts to access the current values of attributes of the source and target objects, respectively. The array keys names are names of the object attributes.

For more information about the use of the associative arrays, refer to Windows PowerShell documentation.

In addition to **$srcObj** and **$dstObj**, Quick Connect defines the **$Request** built-in hash table. The **$Request** key names are also names of the object attributes. The **$Request** hash table contains new values of the target object attributes to which the target object attributes must be set after completing the synchronization process.

To clarify the use of built-in hash tables, let us consider the following scenario: you synchronize between the "mail" attributes of user objects in an LDAP directory (source connected system) and ActiveRoles Server (target connected system) using the following synchronization rule: the value of the "mail" attribute in the target connected system must be equal to that in the source connected system concatenated with current date.

For example, before the synchronization process started, the source object had the "mail" attribute: **JDoe@mail1.mycompany.com**, the target object had the "mail" attribute: J**Doe@mail2009.mycompany.com**. After the synchronization process completes, the target user will have the following mail: **JDoe@mail1.mycompany.com (5 December, 2012)** (if you performed the synchronization process on 5 December, 2012.

The following code snippet illustrates the use of built-in hash tables:

```
#Returns "JDoe@mail1.mycompany.com

$strSourceMail=$srcObj["mail"]

#Returns JDoe@mail2009.mycompany.com

$strTargetMail=$DstObj["mail"]

#Returns JDoe@mail1.mycompany.com (5 January, 2010)

$strNewMail=$Request["mail"]
```

Example script

The following script illustrates the use of **$srcObj**.

A provisioning task (provisioning step of a synchronization workflow as applied to Quick Connect) causes One Identity Quick Connect Sync Engine to provision user identity information from a delimited text file to Active Directory using the following provisioning rule: the "co" attribute in all provisioned users must be set to the name of country where the user lives. The script-based provisioning rule calculates the "co" attribute value basing on the user's city (the "City" attribute in the connected data source).

The following script implements the described scenario:

```
# --- Retrieve the City attribute of the user object in connected data source.

$userCity = $srcObj["City"]

# --- Determine the user's country

switch ($UserCity)

{

"New York" {$country = "United States"; break}
"Paris" {$country = "France"; break}
"Tokyo" {$country = "Japan"; break}
default {$country = "Unknown"}
}
# --- Return the user country. The script-based provisioning rule
# --- assigns this value to the "co" attribute in the provisioned user object.
$country
# End of the script
```

Appendix B: Using a PowerShell script to transform passwords

You can use a Windows PowerShell script in a password sync rule to transform passwords. This section provides some reference materials on how to write a Windows PowerShell script for password transformation.

Accessing source object password

To synchronize passwords between the source Active Directory domain and the target connected data system, One Identity Quick Connect Sync Engine uses the password sync rules you configure. In a password rule settings, you can type a PowerShell script that transforms source Active Directory user passwords into object passwords for the target connected system. For example, you can use such a script if you want the object passwords in the source and target connected systems to be different.

When developing a PowerShell script to transform passwords, you can employ the **$srcPwd** built-in associative array (hash table) that allows the scripts to access the source object password. The **$srcPwd** returns a string that contains the object password.

Example script

To clarify the use of **$srcPwd**, consider a scenario where the target object password in the target connected data system must include only 8 first characters of the source object password in the source Active Directory domain.

The following scripts implements the described scenario:

```
if($srcPwd.length -gt 8)
```

```
{
$srcPwd.substring(0,8)
}
else
{
$srcPwd
}
# End of the script
```

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

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