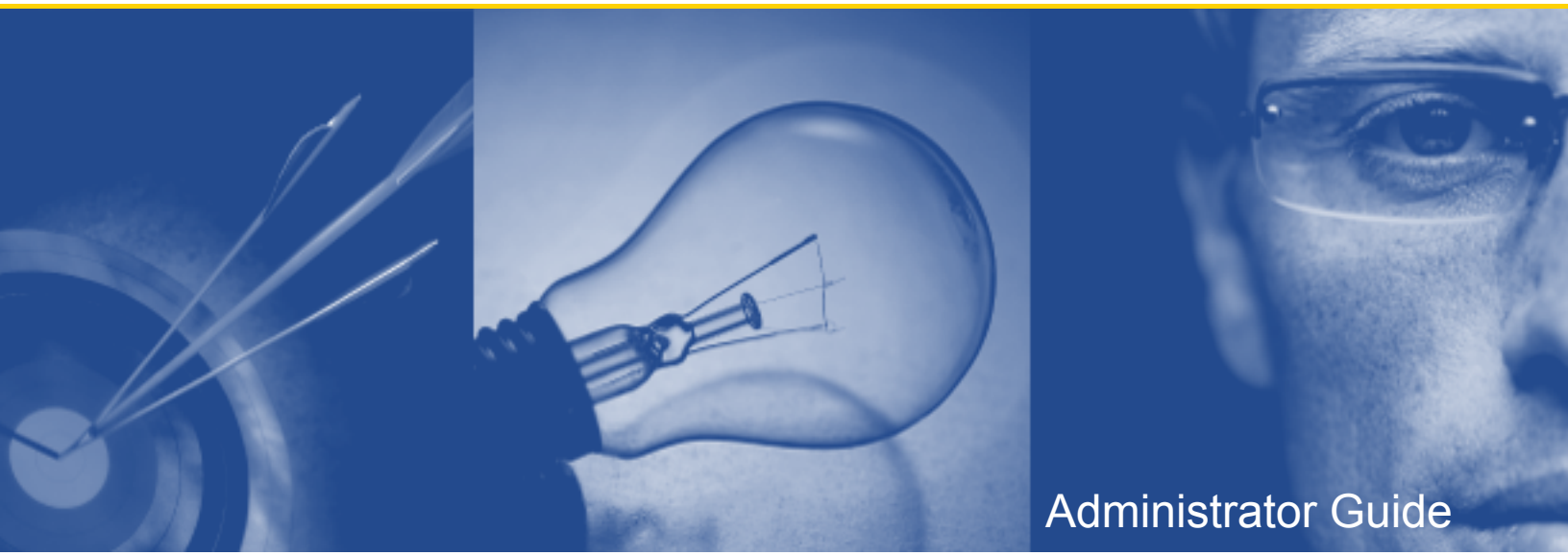
QUEST SOFTWARE®

Quest ActiveRoles Quick Connect 4.5



Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
USA
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Third Party Contributions

Quest ActiveRoles Quick Connect contains some third party components (listed below). Copies of their licenses may be found on our website at www.quest.com/legal/third-party-licenses.aspx.

COMPONENT	LICENSE OR ACKNOWLEDGEMENT
.NET logging library 1.0	BSD 4.4

Quest ActiveRoles Quick Connect - Administrator Guide
Updated - May 21, 2010
Software Version - 4.5

CONTENTS

About This Guide

- Intended Audience
- Conventions
- About Quest Software
- Contacting Quest Software
- Contacting Quest Support

Intended Audience

This document has been prepared to assist you in becoming familiar with the Quest ActiveRoles Quick Connect. The Administrator Guide contains the information required to install and use the Quest ActiveRoles Quick Connect. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

ELEMENT	CONVENTION
Select	This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.
Bolded text	Interface elements that appear in Quest Software products, such as menus and commands.
Italic text	Used for comments.
Bold Italic text	Used for emphasis.
Blue text	Indicates a cross-reference. When viewed in Adobe® Reader®, this format can be used as a hyperlink.
	Used to highlight additional information pertinent to the process being described.
	Used to provide Best Practice information. A best practice details the recommended course of action for the best result.
	Used to highlight processes that should be performed with care.
+	A plus sign between two keystrokes means that you must press them at the same time.
|	A pipe sign between elements means that you must select the elements in that particular sequence.

About Quest Software

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com.for more information.

Contacting Quest Software

Email	info@quest.com
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com/

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.

1

Quick Connect Overview

- What Is Quick Connect?
- New in This Release
- Features and Benefits
- Why Use Quick Connect?
- Technical Overview

What Is Quick Connect?

In most organizations, identity information exists in many different connected data sources, such as directories, databases, or formatted dump files. This can result in the duplication of information, incompatibility of data formats, and also requires administrators to have access to multiple connected data sources. It is crucial for any modern business to maintain the organization identity information from all connected data systems in sync at all times.

Quest ActiveRoles Quick Connect (hereafter *Quick Connect*) is an application that coordinates and synchronizes the identity information between multiple connected data sources and Active Directory. Quick Connect includes the core module - *Quick Connect Sync Engine*, and a number of *connectors* used to access data in connected data sources.

Quick Connect employs the ActiveRoles Server administrative platform to automate the tasks of maintaining Active Directory objects in sync with external connected data sources. The use of advanced technologies minimizes the time required to synchronize the identity information. The following types of the synchronization operations are supported:

- Provision
- Update
- Deprovision
- Synchronization of passwords

Quick Connect also increases security through business process integration and reduces the amount of manual processing that occurs between systems when identity information changes (for example, when an employee joins or leaves the organization).

New in This Release

This new release of ActiveRoles Quick Connect considerably enhances and extends the capabilities of the product, which now include the user passwords synchronization, re-designed sync history log, etc.

Passwords Synchronization

Quick Connect can synchronize passwords between Active Directory and some categories of connected systems. Active Directory and connected systems are governed by different access policies. Consequently, users need to maintain different user accounts and different passwords on these systems. Maintaining several passwords on several different systems is a hassle for users and administrators.

Quick Connect provides for Quick Connect Capture Agent to be installed on all domain controllers in the source Active Directory connections. Capture Agent tracks changes that were made to user password in Active Directory, and then Quick Connect Sync Engine synchronizes the passwords basing on this information.

In this release, the passwords synchronization is supported for the following categories of connected systems:

- Active Directory connections
- AD LDS (ADAM)
- Sun One Directory server
- SQL Server
- Oracle database
- Novell Directory service
- IBM RACF
- Lotus Domino Server
- Google Apps service
- SAP systems

For details, refer to "Managing Passwords Synchronization" later in this paper.

Re-designed Sync History Log

The Sync History feature of the application allows you to view reports on the performed synchronization workflow runs.

The **Sync History** tab allows you to display a list of all performed synchronization workflows runs, and then view the report on the workflow run of interest. In addition to this possibility, the new version of the **Sync History** tab allows you first to filter the synchronization reports for all object pairs using some filter criteria, and then select the report to view.

For details, refer to "Using Sync History Log" later in this paper.

Other Enhancements

Below is a list of issues that were resolved and enhancements that were implemented in the latest version of Quick Connect Sync Engine.

- New: Additional rules for synchronizing multivalued attributes.
- Fixed: Incorrect behavior of the application when configuring synchronization steps: if the target container for synchronization operation was configured to be generated by a script, you cannot reconfigure the application to generate that container by a rule.
  The target container can be set on the **Target** tab of the **Synchronization Step Settings** panel.
- Fixed: In a 64-bit version of Quick Connect Sync Engine, the **About Quick Connect** dialog box provides invalid information about installed licenses. An attempt to update the installed licenses results in the "Failed to install license key" error message.
- Fixed: Incorrect behavior of the Quick Connect console UI: adding a significant number of the update rules or initial attribute population rules for one synchronization step, may result in an incorrect on-screen position of the rules control buttons (such as the **Edit**, **Copy**, **Remove** buttons, etc.).

- Fixed: Quick Connect fails to update the object attributes that conform to the LargeInteger syntax (e.g. the accountExpires attribute) returning the "The directory datatype cannot be converted to/from a native DS datatype. Invalid attribute type or type mismatch." error message.
- Fixed: When synchronizing attributes that contain the line break characters, the target synchronized attribute may contain invalid symbols.
- Fixed: After rebooting a computer running Quest Quick Connect Service, the service does not restart automatically. The QC Server Event Log contains the following Error event: "The Quest Quick Connect 4.0 service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion."
- Fixed: If Quick Connect service is restarted when running a synchronization step, the Sync History log contains no information about execution of this synchronization step.
- Fixed: Incorrect behavior of the application when updating the object attributes in the target connected system: Quick Connect fails to update an attribute if its current value and the new value to which the attribute must be set differ only by case.

Features and Benefits

The major features of ActiveRoles Quick Connect are as follows:

- Bidirectional Synchronization
- Delta Synchronization
- Group Memberships Synchronization
- Windows Powershell Scripting
- Management Shell
- Attribute Synchronization Rules
- Distinguished Name Generation Rules
- Scheduling Capabilities
- Extensibility

Bidirectional Synchronization

Quick Connect Sync Engine supports the bidirectional (two-way) synchronization of all changes in Active Directory and connected data sources since the last synchronization between the data sources. This feature helps you resolve problems that result from conflicting identity information contained in Active Directory and a number of the connected data sources used in your organization.

The bidirectional synchronization is not supported for some categories of the connected data systems, such as the delimited text files, PeopleSoft systems, and databases accessed with the OLE DB provider.

For SAP systems, the bidirectional synchronization is not supported for SAP employee objects. For SAP Employee objects, you can configure the synchronization steps only from SAP system to ActiveRoles Server.

Delta Synchronization

Quick Connect Sync Engine supports the delta synchronization mode. In this mode, the application processes only data that has changed in the connected data source or in Active Directory since the last synchronization between the data sources.

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

The delta synchronization mode is now supported only for the following categories of the connected data systems:

- Active Directory
- AD LDS (ADAM)
- Delimited text files

Group Memberships Synchronization

Quick Connect Sync Engine ensures that the group memberships information will be synchronized in all connected data systems. For example, when provisioning a group object from Active Directory to AD LDS (ADAM), you can specify rules for synchronizing between the "member" attribute in ADAM and the "edsaMember" attribute in Active Directory.

Windows PowerShell Scripting

Quick Connect Sync Engine allows administrators to configure the object attribute synchronization rules or passwords synchronization rules basing on Windows PowerShell scripts. For example, the script can build values of the target object attribute using values of the source object attribute(s). For more information, refer to "Developing PowerShell Scripts for Attributes Synchronization Steps" and "Developing PowerShell Scripts for Passwords Synchronization Steps" in ActiveRoles Quick Connect - SDK.

Management Shell

Quick Connect now includes the Quick Connect Management Shell. This is an Active Directory-specific automation and scripting shell that provides a command-line management interface for synchronizing data between connected systems and Active Directory via the Quick Connect service. The Quick Connect Management Shell is implemented as a Windows PowerShell snap-in, providing an extension to the Windows PowerShell environment. The commands provided by the Quick Connect Management Shell conform to the Windows PowerShell standards, and are fully compatible with the default command-line tools that come with Windows PowerShell.

Attribute Synchronization Rules

Quick Connect Sync Engine allows administrators to configure synchronization rules used to build values of the target object attributes. The application provides for three types of synchronization between a source and a target object:

- **Direct synchronization**: the target object attribute is equal to the specified source object attribute.

- **Script-based synchronization**: the target object attribute is generated with a Windows Powershell script.
- **Rules-based synchronization**: the target object attribute is generated basing on the specified rules that can be easily configured with the Quick Connect console.

Distinguished Name Generation Rules

When performing the provisioning operations, Quick Connect Sync Engine creates new objects in the connected data systems or Active Directory. The application allows administrators to easily configure rules used to generate distinguished names for newly created objects.

Scheduling Capabilities

Quick Connect Sync Engine allows you to schedule the execution of synchronization steps to be automatically performed on a regular basis, according to your company policy.

This functionality helps save many hours of an administrator's time.

Extensibility

Quick Connect Sync Engine employs connectors to access data in the connected data systems. A connector is a driver or provider that encapsulates interactions with a particular connected system and controls the data flow between a connected data source and ActiveRoles Server. Along with built-in connectors to basic types of external data systems, Quick Connect Sync Engine allows administrators to employ custom connectors to data systems used in your organization. The application is supplied with the Quick Connect Software Development Kit (SDK). SDK provides a documentation and samples that help administrators develop and install custom connectors.

Why Use Quick Connect?

Today’s organizations rely on Active Directory and external connected data systems such as HR systems, directories, etc. Because of this reliance controlling the business processes that interact with Active Directory and connected data systems is critical and must be done in the most secure, controlled and efficient way possible. Quick Connect Sync Engine coordinates and synchronizes the identity information between multiple connected data sources and Active Directory. Quick Connect Sync Engine provides for rules based automation of provisioning, update, and deprovisioning steps.

Automated Management of User Identity Information

Quick Connect Sync Engine automates user provisioning tasks to reduce your administrative workload and get new users up and running faster. It automates the update and deprovisioning tasks as well, so when an employee joins or leaves the organization, the related information in Active Directory and connected data systems is automatically updated, thereby reducing administrative workloads.

Improved Security

The use of the ActiveRoles Server administrative platform to perform the synchronization tasks allows the administrators to ensure that every administrative action is consistent with administrative policies and corporate security standards, which is a top priority for most organizations.

Improved Flexibility

Quick Connect Sync Engine allows you to develop custom connectors to data systems used in your organization. This feature improves the application flexibility and ensures that the identity information is always synchronized between all categories of connected data systems used in your organization.

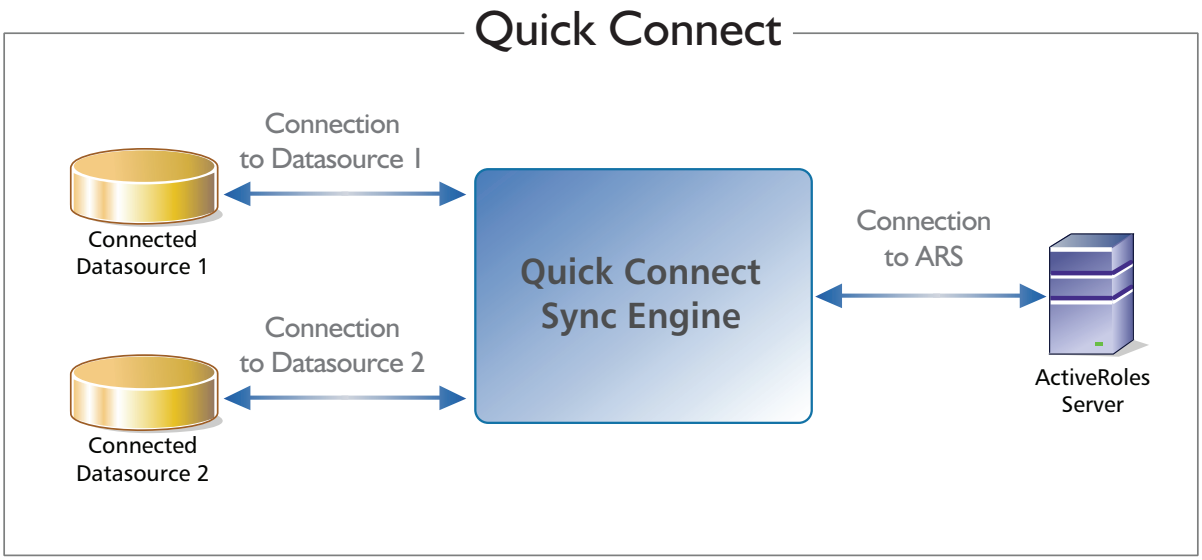
Increased Efficiency

Quick Connect Sync Engine increases the efficiency of the data management by automating synchronization tasks, such as provisioning, deprovisioning and update. The use of scripting capabilities provides a flexible way to automate administrative processes, and to integrate the administration of Active Directory and connected data systems with other business processes. By automating regular synchronization tasks, Quick Connect Sync Engine allows administrators to concentrate on strategic issues, such as planning the directory, increasing enterprise security, or supporting business-critical applications.

Technical Overview

The overall Quick Connect environment comprises *Quick Connect Sync Engine*, *Capture Agents*, *ActiveRoles Server*, *connected data systems (data sources), connectors*, *connections*, and *synchronization workflows*.

The following illustration shows how the components work together to flow data from one data source to multiple data sources.



This section describes the application environment components.

Quick Connect Sync Engine

The core module of ActiveRoles Quick Connect - Quick Connect Sync Engine is a client\server application.

The *client component* includes the interface for the Windows platform (ActiveRoles Quick Connect Administration console) that allows users to perform a defined set of administrative activities, such as creation, deletion or configuring synchronization workflows, configuring connections to target connected data systems, etc.

The *server component* includes the Quick Connect service that is a secure level between the Quick Connect console and managed resources, such as connected data systems, ActiveRoles Server and SQL Server.

In the current version of the application, the Quick Connect Sync Engine Installation program installs the client and server components only on the same computer.

Capture Agent

The Passwords Synchronization feature uses Quest ActiveRoles Capture Agents (hereafter *Capture Agents*) that can track changes made to the Active Directory user password. Capture Agents must be installed on all domain controllers for all Active Directory connections you want to use as source systems for the passwords synchronization. Quick Connect Sync Engine uses the information obtained from the agents to synchronize user passwords between Active Directory and specified connected systems.

ActiveRoles Server

ActiveRoles Server is a key component of the Quick Connect environment. It can be installed on the computer running Quick Connect Sync Engine or on any accessible network computer.

Quick Connect Sync Engine employs the ActiveRoles Server administrative platform to automate the tasks of maintaining Active Directory objects in sync with external connected data sources. ActiveRoles Server processes the integrated identity information that Quick Connect Sync Engine gathers from multiple connected data sources. All identity information is synthesized into a single object that represents the aggregated view of objects from one or several connected data sources.

Connected Data Systems

Quick Connect Sync Engine allows you to synchronize identity information from a wide variety of data sources. *Connected data system* is a data source that is connected to Quick Connect Sync Engine with a *connector* of a particular type, using particular connection parameters. After you install Quick Connect Sync Engine, you can synchronize with the connected data systems of the following categories:

- **Active Directory.** Identity information can be retrieved from Active Directory servers.
- **AD LDS (ADAM).** Identity information can be retrieved from servers running AD LDS (ADAM).

Additional connected data systems, such as Delimited text files, Microsoft SQL Server Data, LDAP Directory services, etc. are supported only if you have installed Quick Connect for Base Systems or additional connectors. For more information, refer to "Licensing" later in this document.

Connectors

Quick Connect Sync Engine employs *connectors* to access data in the connected data systems. A connector is a driver or provider that encapsulates interactions with a particular connected system. Connectors control the data flow between a connected data source and ActiveRoles Server.

There are connectors for different types of connected systems: Active Directory connector, LDAP connector and so on (see "Connected Data Systems" earlier in this paper).

Custom Connectors

Quick Connect Sync Engine provides you with flexibility for connecting to a wide range of connected data systems. In addition to connectors included when you install Quick Connect Sync Engine or Quick Connect for Base Systems, you can implement custom connectors for connected data systems used in your organization. For more information on how to implement your custom connectors, refer to ActiveRoles Quick Connect - SDK.

Connections

A connector configured for accessing the specific instance of a connected data system is referred to as *connection*.

Quick Connect Sync Engine provides the Add Connected System wizard designed to configure connectors for a wide variety of the connected data systems. For more information, see "Configuring Connections to External Data Systems" later in this document.

Synchronization Workflows

Synchronization workflow is a set of *synchronization steps* (or *synchronization operations*) that determine how to synchronize the connected data system objects with their counterparts in Active Directory. A synchronization workflow is composed of at least one synchronization step. With the Quick Connect console, you can configure any number of synchronization workflows designed to perform a specific set of synchronization steps.

Synchronization Steps

Quick Connect Sync Engine provides the Add Synchronization Step wizard that allows you to add a new synchronization step to a synchronization workflow. The wizard offers the provisioning, update and deprovisioning synchronization steps.

- **Provisioning steps**: The process of creating and connecting objects in a connected data system or in Active Directory, based on the tracked changes to objects. When creating a new object, Quick Connect Sync Engine sets initial values of the object attributes basing on the initial attribute population rules.
- **Update steps**: The process of pushing changes to an object's attributes into and out of a connected data system. This process is controlled by the *mapping rules* defined for the connected data system. For more information, refer to "Managing Objects Mapping" later in this paper.
- **Deprovisioning steps**: The process of managing or cleaning up objects after they have been disconnected from a connected data system. You may remove the objects permanently or keep them in a disconnected state.

Additional connected data systems, such as Delimited text files, Microsoft SQL Server Data, LDAP Directory services, etc. are supported only if you have installed Quick Connect for Base Systems or additional connectors. For more information, refer to "Licensing" later in this document.

2

Deploying Quick Connect

- System Requirements
- Licensing
- Upgrade and Compatibility
- Steps to Deploy Quick Connect

System Requirements

Quick Connect Sync Engine

Before installing Quick Connect Sync Engine, ensure that your environment meets the following minimum hardware and software requirements:

ITEM	REQUIREMENTS
Platform	1 GHz or higher Intel Pentium-compatible CPU.
Memory (RAM)	512 MB; 1 GB or more recommended.
Hard Disk Space	250 MB or more of free disk space. The required amount depends on the number of synchronized objects in external data sources.
Operating System	Microsoft Windows Server 2003, including x64 editions, with or without any Service Pack -OR- Microsoft Windows Server 2008, 32-bit or 64-bit architecture -OR- Microsoft Windows Server 2008 R2
ActiveRoles Server	ActiveRoles Server 6.1.0 or 6.5.0.
ActiveRoles Server ADSI Provider	ActiveRoles Server ADSI Provider 6.1.0 or 6.5.0
Microsoft SQL Server	- Microsoft SQL Server 2005 (any edition) - Microsoft SQL Server 2008 (any edition)
Microsoft .NET Framework	Microsoft .NET Framework 3.5 SP1 or later.
Windows PowerShell	Windows PowerShell 1.0 or 2.0.
Quick Connect Capture Agent	The Passwords Synchronization feature requires the Quick Connect Capture Agent installed on all domain controllers in the source Active Directory systems.

Quick Connect Capture Agent

Before installing Quick Connect Capture Agent, ensure that your system has the following software installed:

- Microsoft .NET Framework 3.5 SP1, or later

To use the Passwords Synchronization feature, you have to install and configure Capture Agents on all domain controllers in the source Active Directory data systems. For more information, see "Deploying Capture Agents" later in this document.

The Quick Connect Management Shell

Before installing the Quick Connect Management Shell, ensure that your system has the following software installed:

- Windows XP Service Pack 2, Windows 2003 Service Pack 1, or later versions of Windows, including x64 editions.
- Microsoft .NET Framework 3.5 SP1, or later
- Microsoft Windows PowerShell 1.0 or 2.0

The Quick Connect Management Shell can be installed on any network computer from which the computer running Quick Connect Sync Engine is accessible.

For more information about the Quick Connect Management Shell, refer to "Using Management Shell" and "Quick Connect Management Shell Cmdlets" later in this document.

Licensing

To use Quick Connect Sync Engine you must have ActiveRoles Server installed in your environment. Quick Connect Sync Engine does not require separate licenses.

To use additional connectors, you need to obtain an appropriate license from Quest Software.

The synchronization with the following categories of the connected data systems are subject to licensing:

- Delimited text files
- Microsoft SQL Server
- LDAP Directory service
- OLE DB
- Sun One Directory Server
- Oracle database
- Novell directory service
- IBM RACF
- Lotus Domino Server
- Google Apps Service
- SAP system
- PeopleSoft system

When installing Quick Connect for Base Systems, Quick Connect for Mainframes, Quick Connect for Online Services, Quick Connect for Lotus Notes or Quick Connect for SAP Solutions, you will be prompted to install the license key file purchased from Quest Software. For more information about licensing, refer to Release Notes applicable to connectors of your interest.

Upgrade and Compatibility

Upgrading from ActiveRoles Quick Connect 3.5

Upgrading from ActiveRoles Quick Connect 3.5 is not supported. However, you can install current version of Quick Connect and develop scenarios implemented in the Scheduled Import Wizard 3.5..

Before deploying and testing Quick Connect 4.5, we recommend that you retain a system with the Scheduled Import Wizard 3.5 and ActiveRoles Server 6.0 installed.

If you plan to use the current version of ActiveRoles Quick Connect, consider the following key aspects:

- Quick Connect now can use only ActiveRoles Server 6.5 or later while the Scheduled Import Wizard provided in Quick Connect 3.5 uses only ActiveRoles Server 6.0.
- The Quick Connect 4.X architecture differs significantly from that for Quick Connect 3.5. The import of the application configuration from Quick Connect 3.5 is not supported.
- If you want Quick Connect to support synchronization scenarios implemented in the Scheduled Import Wizard 3.5, create the appropriate synchronization steps with the Add Synchronization Step wizard (for related procedures, see "Managing Synchronization Workflows" later in this document). Note that in Quick Connect, you can create synchronization steps based on both the attribute synchronization rules and the PowerShell scripts. Whenever possible, create the rules-based synchronization steps because they accelerate the synchronization process.
- Quick Connect supports only the Windows PowerShell scripts. Note that the scripts used by the Scheduled Import Wizard 3.5 are not supported in Quick Connect. For more information about the use of PowerShell scripts, refer to ActiveRoles Quick Connect - SDK.

Upgrading from ActiveRoles Quick Connect 4.0

The Quick Connect Setup supports upgrading from ActiveRoles Quick Connect 4.0. The import of the Quick Connect 4.0 configuration is supported.

Steps to Deploy Quick Connect

The process of deploying Quick Connect includes the following steps:

- Preinstallation Steps
- Installing Quick Connect Sync Engine
- Installing and configuring connectors to external data sources (optionally): for more information, refer to Release Notes applicable to your connectors, and to "Configuring Connectors to External Data Systems" later in this paper.
- Installing and configuring Quick Connect Capture Agents (required only for the Passwords Synchronization feature): for more information, refer to "Deploying Capture Agents" later in this paper.
- Installing the Quick Connect Management Shell (optionally): for more information, refer to "Using Management Shell" later in this paper.

Preinstallation Steps

Use the following check list to ensure that you are ready to install Quick Connect Sync Engine.

ITEM TO CHECK	DESCRIPTION
Computer	The computer running Quick Connect Sync Engine must meet the hardware and software requirements listed in "System Requirements" earlier in this paper.
Microsoft SQL Server	Quick Connect Sync Engine employs Microsoft SQL Server. SQL Server can be installed on the local computer or on any network computer. The following versions of SQL Server are supported: • Microsoft SQL Server 2005 (any edition) • Microsoft SQL Server 2008 (any edition)
ActiveRoles Administration Service	Quick Connect Sync Engine employs ActiveRoles Administration Service v. 6.1.0 or 6.5.0. It can be installed on the local computer or on any network computer. For more information, refer to Quest ActiveRoles Server - Quick Start Guide. **Important** You need to ensure that ActiveRoles Administration Service has at least one managed domain. For information about how to add managed domains, refer to Quest ActiveRoles Server - Administrator Guide.
ActiveRoles Server ADSI Provider	The ActiveRoles Server ADSI Provider 6.1.0 or 6.5.0 must be installed on your local computer. For more information, refer to Quest ActiveRoles Server - Quick Start Guide.
Microsoft SQL Server 2008 Native Client	Microsoft SQL Server 2008 Native Client must be installed on your local computer.

ITEM TO CHECK	DESCRIPTION
Quick Connect Service account	Quick Connect service will run under this account. For Quick Connect Sync Engine to function properly, this account must have administrator rights on the computer running the Quick Connect service. For example, the Quick Connect Service account can be a member of the local Administrators group. In addition, Quick Connect Sync Engine uses this account when accessing managed resources, such as SQL Server or ActiveRoles Administration Service, unless an override account is specified.
Account used for connection to SQL Server	Quick Connect Sync Engine can be configured to use Windows authentication or SQL Server authentication for connection to SQL Server. If you choose Windows authentication, the connection is established using the Quick Connect Service account. In this case, the service account must be a member of the sysadmin role on SQL Server. If you choose SQL Server authentication, the connection is established with the override account you are prompted to specify when installing the application. This account must be a member of the sysadmin role on SQL Server.
Account used for connection to ActiveRoles Administration Service	Quick Connect Sync Engine can be configured to use the Quick Connect Service account or an override Windows account for connection to ActiveRoles Administration Service.

Installing Quick Connect Sync Engine

To install Quick Connect Sync Engine

1. On a computer running a 32-bit edition of Windows, run the delivered "QuickConnectSyncEngine_x86.msi"
   -- OR --
   on a computer running a 64-bit edition of Windows, run the delivered "QuickConnectSyncEngine_x64.msi."

   The ActiveRoles Quick Connect Sync Engine Installation wizard starts.
2. On the **Welcome** page, click **Next**.
3. On the **License Agreement** page, select the **I accept the license agreement** check box and click **Next**.
4. On the **User Information** page, specify your personal information and click **Next**.
5. On the **Custom Setup page**, ensure that all features you want to install are selected, and then click **Next**. The following features are available:
   - **SDK**: Installs documentation and samples to help develop connectors to your custom connected systems.
   - **Quick Connect Sync Engine**: Installs the Quick Connect console and service components. *Quick Connect console* is a user interface providing an access to all functions of ActiveRoles Quick Connect. *Quick Connect Service* is a secure layer between Quick Connect console and managed resources, such as ActiveRoles Administration Service, SQL Server and the connected data sources. Quick Connect Service manages the data flows between connected data sources and Active Directory.
   - **Administrative Templates**: Installs the Group Policy Administrative templates used for deploying Capture Agents and configuring Quick Connect service parameters used for the passwords synchronization feature. For more information, see "Deploying Capture Agents" and "Configuring Capture Agents and Quick Connect services to use the custom certificate" later in this document.
6. On the **Quick Connect Service Account Information** page, specify the name and password of the domain user account to be used as logon account for Quick Connect Service, and then click **Next**.
7. On the **Database and Connection Settings** page, complete the **Database** area:
   - in **SQL Server**, type the name of SQL Server in the form <*Computer*>\<*Instance*> (for named instance) or **<**Computer**>** (for default instance).
   - In the **Configuration data store** and **Temporary data store** text boxes, type names of the configuration SQL databases or leave the default names (*QCConfiguration* and *QCExecutionData*). Setup will create the configuration databases on the SQL Server instance specified in the **SQL Server** text box.
8. Complete the **Connection** area:
   - To have the application connect to SQL Server using the Quick Connect Service account, click **Use the Quick Connect Service** account.
   - To have the application connect to SQL Server using a SQL Server login, click **Use the following SQL Server login** and specify the login name and password.
9. On the **ActiveRoles Service Connection Settings** page, complete the **ActiveRoles Service** area: in **ActiveRoles Service computer**, type the DNS name of the computer running ActiveRoles Administration Service you want the application to use.
10. Complete the **Connection** area:
    - To have the application connect to ActiveRoles Administration Service using the Quick Connect Service account, click **Use the Quick Connect Service account**.
    - To have the application connect to ActiveRoles Administration Service using an override account, click **Use the following Windows account** and specify the login name and password.
11. On the **Ready to Install the Application** page, review the installation settings you are going to use. To proceed with the installation process, click **Next**.
12. On the Completion page, click **Finish** to close the wizard.

Deploying Capture Agents

To use the Passwords Synchronization feature, you have to install and configure Capture Agents on all domain controllers in the source Active Directory data systems. This section explains how you can install and configure Quick Connect Capture Agents (hereafter *Capture Agents*).

Capture Agents track changes made to the Active Directory user password. Quick Connect Sync Engine uses the information obtained from the agents to synchronize user passwords between Active Directory and specified connected systems.

Installing Capture Agents

You can install Capture Agents by using one of the following methods:

- Manually installation of agents on each domain controller of a domain of interest.
- Remote installation of agents on all domain controllers of a domain of interest using Group Policy.

To manually install Capture Agent

1. On a domain controller running a 32-bit edition of Windows, run the delivered "QuickConnectCaptureAgent_x86.msi"
   -- OR --
   on a domain controller running a 64-bit edition of Windows, run the delivered "QuickConnectCaptureAgent_x64.msi"
   The Quest ActiveRoles Quick Connect Capture Agent Setup wizard starts.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select the **I accept the terms in the license agreement** check box and click **Next**.
4. On the **Destination Folder** page, specify the installation folder for Capture Agent, and click **Next**.
5. On the **Ready to Install Quest ActiveRoles Quick Connect Capture Agent** page, click **Next** to proceed with the installation process.
6. On the Completion page, click **Finish** to close the wizard.

To install Capture Agents using Group Policy, consider two scenarios: one basic scenario and one advanced scenario.

Basic Scenario

In the basic scenario, you install Capture Agents only on 32-bit or 64-bit domain controllers. All domain controllers are within the Domain Controllers built-in folder and the "Default Domain Controllers Policy" built-in Group Policy object is linked to the Domain Controllers folder.

To install Capture Agents using Group Policy

1. Save the required delivered Capture Agent installation package (the QuickConnectCaptureAgent_x86.msi or the QuickConnectCaptureAgent_x64.msi file, respectively) to a folder on a network share.

   Important*: The folder on the network share must be accessible from all domain controllers where you want to install Capture Agents.*

2. Using Group Policy Editor, open the "Default Domain Controllers Policy" Group Policy object stored in the domain where you want to install Capture Agents.

For information about how to open and use Group Policy Editor, refer to the Group Policy Editor documentation.

3. In the console tree of Group Policy Object Editor, under **Computer Configuration,** click **Software Settings**.
4. In the details pane, click **Software Installation**, on the **Action** menu, point to **New**, and then click **Package**.

   *The **Open** dialog box opens.*
5. Using the **Open** dialog box, open the Capture Agent installation package.
6. In the **Deploy Software** dialog box that opens, select **Assigned**, and then click **OK**.
7. For changes to take effect, refresh the Group Policy settings, using the **GPupdate** command:
   - At the command prompt, type **GPupdate /force**

Advanced Scenario

In the advanced scenario, your domain has both 32-bit and 64-bit domain controllers. To install Capture Agents on all domain controllers using Group Policy, you perform the following steps:

1. Save the delivered Capture Agent installation packages (the QuickConnectCaptureAgent_x86.msi and the QuickConnectCaptureAgent_x64.msi file, respectively) to a folder on a network share.

   ***Important**: The folder on the network share must be accessible from all domain controllers where you want to install Capture Agents.*
2. Using Active Directory Users and Computers, do the following:
   - Move all 32-bit and 64-bit domain controllers to separate Active Directory containers, such as the "DC32bit" and "DC64bit" Organizational Units.
   - Create new Group Policy objects, such as GPO32 and GPO64, and link them to the DC32bit and DC64bit Organizational Units, respectively.
   - For the "GPO32" and "GPO64" Group Policy objects, perform Steps 2 to 6 from the previous procedure (use the QuickConnectCaptureAgent_x86.msi and the QuickConnectCaptureAgent_x64.msi file, for GPO32 and GPO64, respectively).

   For detailed instructions, refer to the ActiveRoles Directory Users and Computers documentation.
3. For changes to take effect, refresh the Group Policy settings, using the **GPupdate** command:
   - At the command prompt, type **GPupdate /force**

If you cannot move the 32-bit and 64-bit domain controllers to separate directory folders, manually install Capture Agents on each domain controller using the "To manually install Capture Agent" procedure earlier in this section.

Configuring Capture Agents

Capture Agent uses a set of parameters that control its behavior. The actions performed by Capture Agent may vary depending on parameter values.

The following table lists the Capture Agent parameters.

PARAMETER	DESCRIPTION	DEFAULT VALUE
Maximum connection point age	Determines the period of time (in hours) that a connection point is valid.	24 hours
Set interval between attempts to reconnect to service	Capture Agent tracks changes that were made to user password in Active Directory, and then tries to send information on changed password to Quick Connect service. This parameter determines the time interval (in minutes) between attempts 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. **Note**: During this period Capture Agent keeps passwords in an encrypted file.	7 days
Set certificate	Specifies a thumbprint of certificate used to encrypt the data transfer channel between Capture Agent service and Quick Connect service. The certificate must be accessible both for Capture Agent and Quick Connect Service. For more information, refer to "Using Certificates" later in this paper	If this parameter is not set, a default built-in certificate will be used.
Connection point 1 to **Coneection point 7**	Determines the location of Quick Connect Service to which Capture Agent sends passwords to synchronize. Quick Connect Service specified in this setting is added to a list of available Quick Connect services.	If these parameters are not set, Capture Agent will search the "CN=QuickConnect,CN=Quest Software,CN=System,DC=<*do main name*>" container for available Quick Connect services.

Before using the Passwords Synchronization feature, you can optionally set the Capture Agent parameters to any appropriate values.

If you do not set the parameters, Capture Agent will use default values listed in the above table.

You can configure Capture Agent to use:

- *A unique set of parameters for all domain controllers* in a domain using Group Policy.
- *A specific set of parameters for some of domain controllers* by setting the appropriate registry keys on each domain controller.

Setting Capture Agent Parameters Using Group Policy

You can specify a unique set of parameters for all domain controllers in a domain by adding an Administrative Template delivered with the Quest ActiveRoles Sync Engine installation to Group Policy object(s) linked to Active Directory contaiter(s) where domain controllers reside.

Let us consider two scenarios: a **basic scenario** and an **advanced scenario** similar to the scenarios discussed in "Installing Capture Agents" earlier in this paper.

In the **basic scenario**, you add the Administrative Template to the "Default Domain Controllers Policy" Group Policy object while in the **advanced scenario**, you add the Administrative Template to the GPO32 and GPO64 Group Policy objects linked to the Active Directory containers where the 32-bit and 64-bit domain controllers reside. Use the following procedure:

To add an Administrative Template to a Group Policy object

1. On any computer from the domain of interest, start Group Policy Object Editor, and connect to the Group Policy object, such as the "Default Domain Controllers Policy", GPO32 or GPO64.

   For information about how to open and use Group Policy Editor, refer to the Group Policy Editor documentation.

2. In the Group Policy Object Editor console, expand the Group Policy object to which you have connected, expand the **Computer Configuration** node, and then click **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 delivered Administrative Template (the CaptureAgentService.adm file).

   *By default, the CaptureAgentService.adm file is stored in the **[Quick Connect installation folder]\Quick Connect Capture Agent\Administrative Templates** folder.*

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

   ***Note**: The names of group policy settings correspond to names of the Capture Agent parameters listed in the table above.*

6. For changes to take effect, refresh the Group Policy settings, using the **GPupdate** command:
   - At the command prompt, type **GPupdate /force**

Setting Capture Agent Parameters in the Domain Controller Registry

Optionally, you can override the Capture Agent parameters for a specific domain controller. To do this, you must make some changes to the Windows Registry on the domain controller.

Do not edit the registry unless you have no alternative. The registry editor bypasses standard safeguards, allowing settings that can damage your system, or even require you to reinstall Windows. If you must edit the registry, back it up first and see the registry reference.

To set parameters in the domain controller registry

1. On the domain controller, start the Regedit.exe tool.
   Registry Editor opens.
2. Using Registry Editor, add the following registry keys:
   - HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService
   - HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService\Connection Points
   - HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService\Certificate
3. Under the newly created keys, add the entries listed in the following tables.

Under the **HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService** registry key, add the following entries:

ENTRY NAME	DATA TYPE	VALUE
CPUpdateTimeSpan	REG_DWORD	The period of time (in hours) that a connection point is valid.
RetryTimeSpan	REG_DWORD	The time interval (in minutes) between attempts to reconnect to Quick Connect service.
KeepPasswordTimeSpan	REG_DWORD	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.

Under the **HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService\Connection Points** registry key, add the following registry keys:

- Connection Point 1
- Connection Point 2
- *etc... (the number of such keys must be equal to the number of connection points)*

Under each newly created registry key, add the following entries:

ENTRY NAME	DATA TYPE	VALUE
CONFIGURATION.SERVER_URL	REG_SZ	Quick Connect service URL (e.g.: net.tcp://MyComp/Quest.QuickConnect.Server/PasswordService)
CONFIGURATION.PROJECT	REG_SZ	Connected System ID.

Under the **HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService\Certificate** registry key, add the following entries:

ENTRY NAME	DATA TYPES	VALUES
FindValue	REG_SZ	Specifies a thumbprint of certificate used to encrypt the data transfer channel between Capture Agent service and Quick Connect service. For information about how to retrieve the certificate thumbprint, refer to "Configuring Capture Agents and Quick Connect services to use the custom certificate" later in this paper.

The values of parameters specified in Registry keys override values of the same parameters specified using Group Policy.

If you have specified parameters in Registry keys, setting those parameters with the use of Group Policy takes no effect.

3

Using Quick Connect Sync Engine

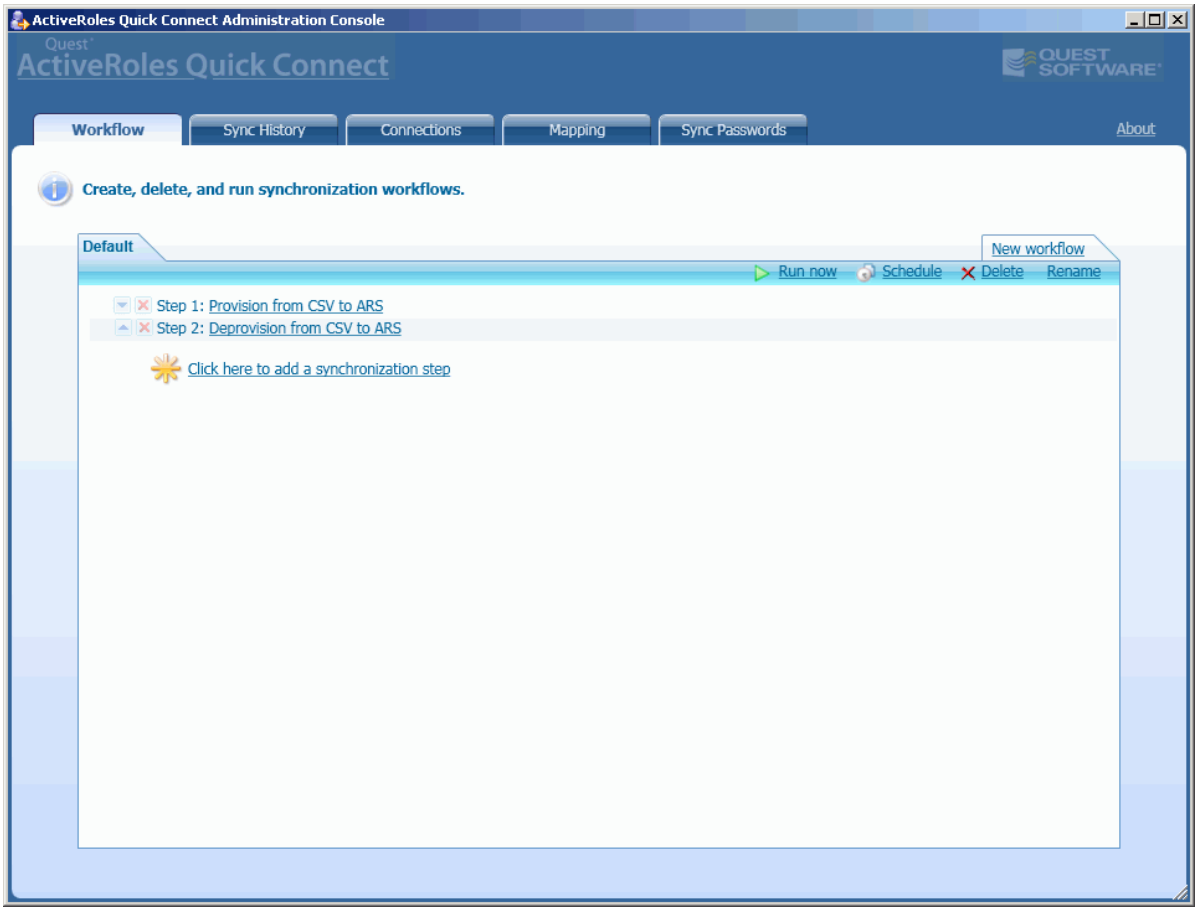
- Getting Started
- Managing Synchronization Workflows
- Configuring Connections
- Using Sync History Log
- Managing Objects Mapping
- Managing Passwords Synchronization
- Using the QCconfig Command-line Tool

Getting Started

The Quick Connect Sync Engine client component is implemented as a user-friendly console (hereafter the *Quick Connect console*) to ensure intuitive operation and close integration with the Windows operating system.

To start the Quick Connect console, click **Start**, point to **All Programs** -> **Quest Software**-> **ActiveRoles Quick Connect**, and then click **ActiveRoles Quick Connect Administration Console**.

The Quick Connect console is similar to the following screen:



The console includes the following tabs:

- **Workflow**: Provides for creation, deletion and running the synchronization workflows.
- **Sync History**: Contains the history information about the synchronization workflows runs.
- **Connections**: Provides for configuring connection settings for ActiveRoles Server and connected data systems.
- **Mapping**: Provides for creation, deletion, and running mapping rules.
- **Sync Passwords**: Provides for configuring settings for synchronization of user passwords between Active Directory and connected systems.

Managing Synchronization Workflows

The **Workflow** tab allows you to create new synchronization workflows, modify, delete, rename, run or schedule existing workflows.

Creating a New Synchronization Workflow

To create a new synchronization workflow

1. In the Quick Connect console, open the **Workflow** tab.
2. Click **New workflow**.
   *The **Create New Synchronization Workflow** dialog box opens.*
3. In the **Synchronization workflow name** text box, type the name for new synchronization workflow, and then click **OK**.
   The Quick Connect console adds a tab for the newly created synchronization workflow.

A synchronization workflow is composed of at least one *synchronization step*. You can add synchronization steps to an existing synchronization workflow using the Add Synchronization Step wizard.

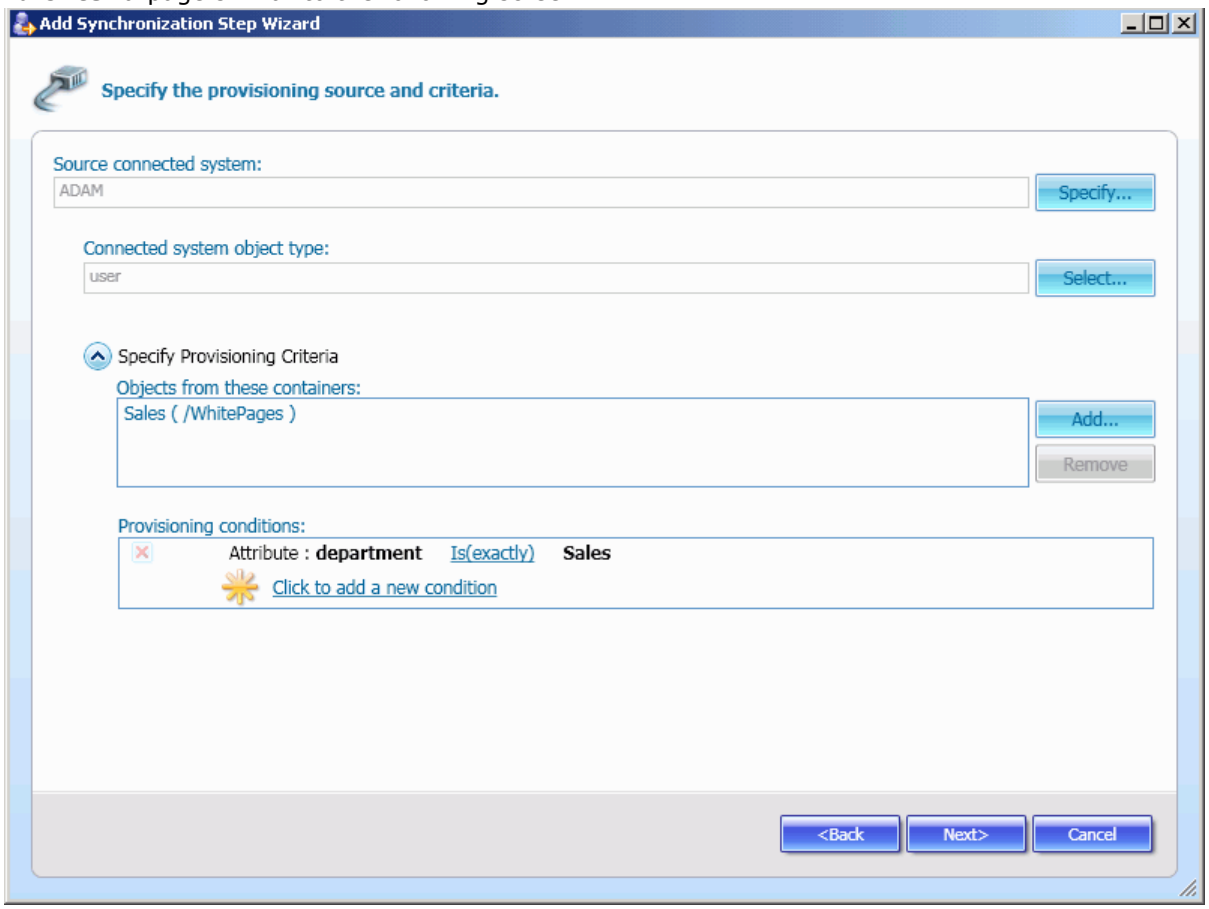
- To start the Add Synchronization Step wizard, click the **Click here to add a synchronization step** link available on the tab for the workflow to which you want to add a new synchronization step.

When started, the wizard displays the **Select an operation** page where you can select the synchronization operation (step) *type*, such as the provision, deprovision or update operation, and the synchronization operation *direction*: for example, you can select the provisioning from a connected system to ActiveRoles Server or vice versa. Alternatively, you can select an existing synchronization step, if any.

The next pages of the wizard depend on the type of the selected synchronization operation. The following sections detail the steps required to add the provisioning, deprovisioning and update operations.

Configuring Provisioning Step

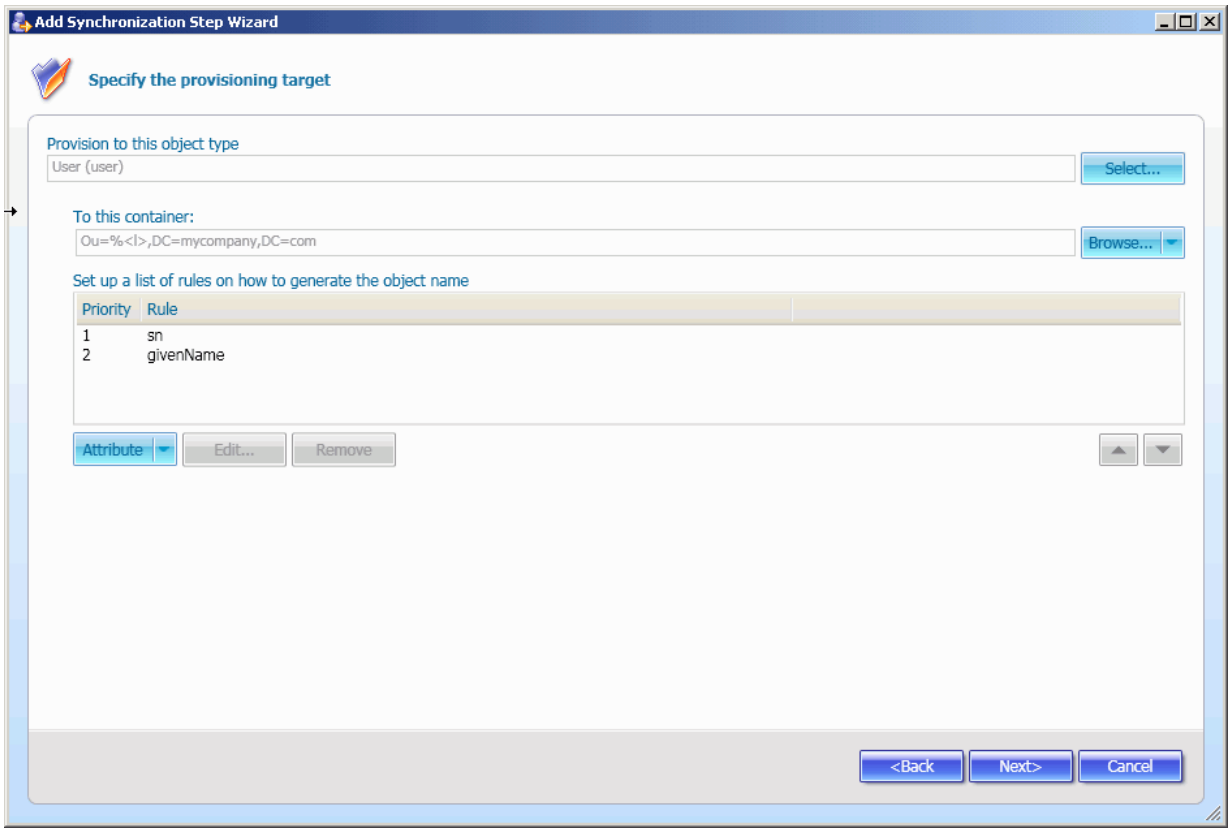
If you select to add a new provisioning step, the wizard displays the **Specify the provisioning source and criteria** page similar to the following screen:



Use this page to specify the connected data system and the object type from which to provision. Optionally, specify the provisioning criteria used to select the connected system objects that will participate in the provisioning process. This page defines the following elements:

- **Source connected system**: Displays the name of a connection to the source connected data system. Click **Specify** to start the Add Connected System wizard that will help you create a new connection to the connected data system. For more information, refer to "Creating a Connection" later in this document.
- **Connected system object type**: Specifies the connected system object type that will participate in the synchronization process. To select the object type, click **Select**, and then complete the **Select Object Type** dialog box.
- **Objects from these containers**: Specifies a list of containers in the source data system. Only objects from selected containers will participate in the synchronization process. To modify the list, use the **Add** and **Remove** buttons.
- **Provisioning conditions**: Specifies a list of conditions to which the connected system objects must match to participate in the provisioning process. To specify a new condition, click the **Click to add a new condition** link, and then complete the **Add Condition** dialog box.

The next is the **Specify the provisioning target** page similar to the following screen:



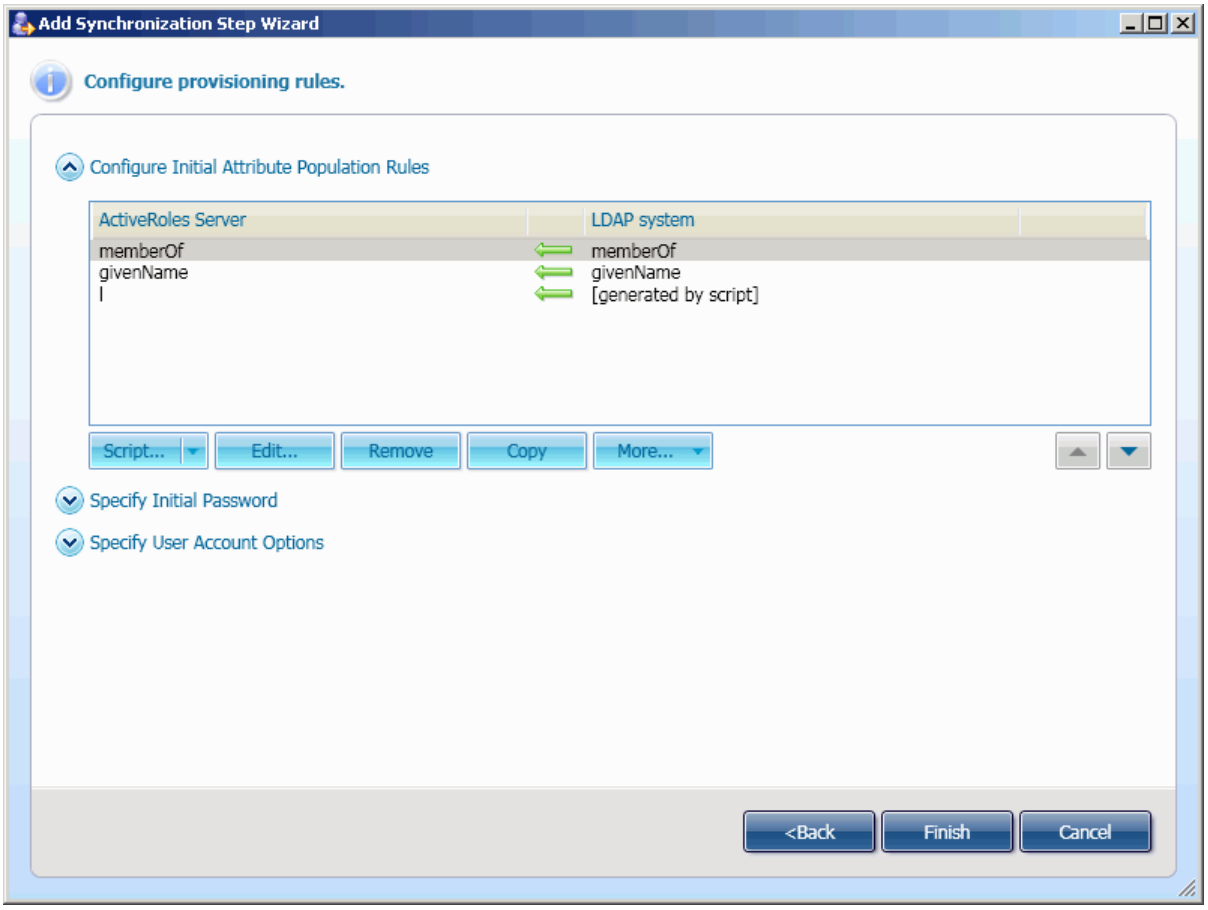
Use this page to do the following:

- Specify the type of objects in the target data system with which to synchronize;
- Specify the parent container(s) in the target data system where the objects reside;
- Configure rules used to generate the object name in the target connected data system.

This page defines the following elements:

- **Provision to this object type:** Allows you to specify the target object type to which to provision. To select the object type, click **Select**, and then complete the **Select Object Type** dialog box.
- **To this container**: Allows you to specify the container(s) in the target data system where the objects will be created. For more information, see "Specifying Target Container" later in this paper.
- **Set up a list of rules on how to generate the object name**: Allows you to specify a list of rules on how to generate the target object name. For more information, see "Generating Object Name" later in this paper.

The next is the **Configure the provisioning rules** page similar to the following screen:



You can use this page to perform the following operations:

- *Configuring rules for initial population of the target object attributes*: These rules determine how to generate values of the target object attributes. For details, see "Synchronization Rules for Multivalued Attributes" later in this paper.
- *Specifying options for generating user password and the user account options* (available only for provisioning the user objects).
- *Configuring additional rules for initial population of the linked attributes*, such as the "member" attribute of the user object. For details, refer to "Synchronization of Group Memberships" later in this paper.
- *Configuring additional rules for initial population of multivalued attributes*, such as the "otherTelephone" attribute of the user object. For details, refer to "Synchronization Rules for Multivalued Attributes" later in this paper.

This page also allows you to import and export population rules from\to XML files.

To export a population rule to a file

1. From the list of configured attribute population rules, select a rule to export.
2. Click **More**, and then click **Export**.
   *The **Save As** dialog box opens.*
3. Using the **Save As** dialog box, specify an XML file where to store the rule.

To import a population rule from a file

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

Configuring Update Step

If you select to add a new update step, the wizard displays the **Specify source for the update** page. Use this page to specify the connected data system type, the object type from which to update and the update criteria.

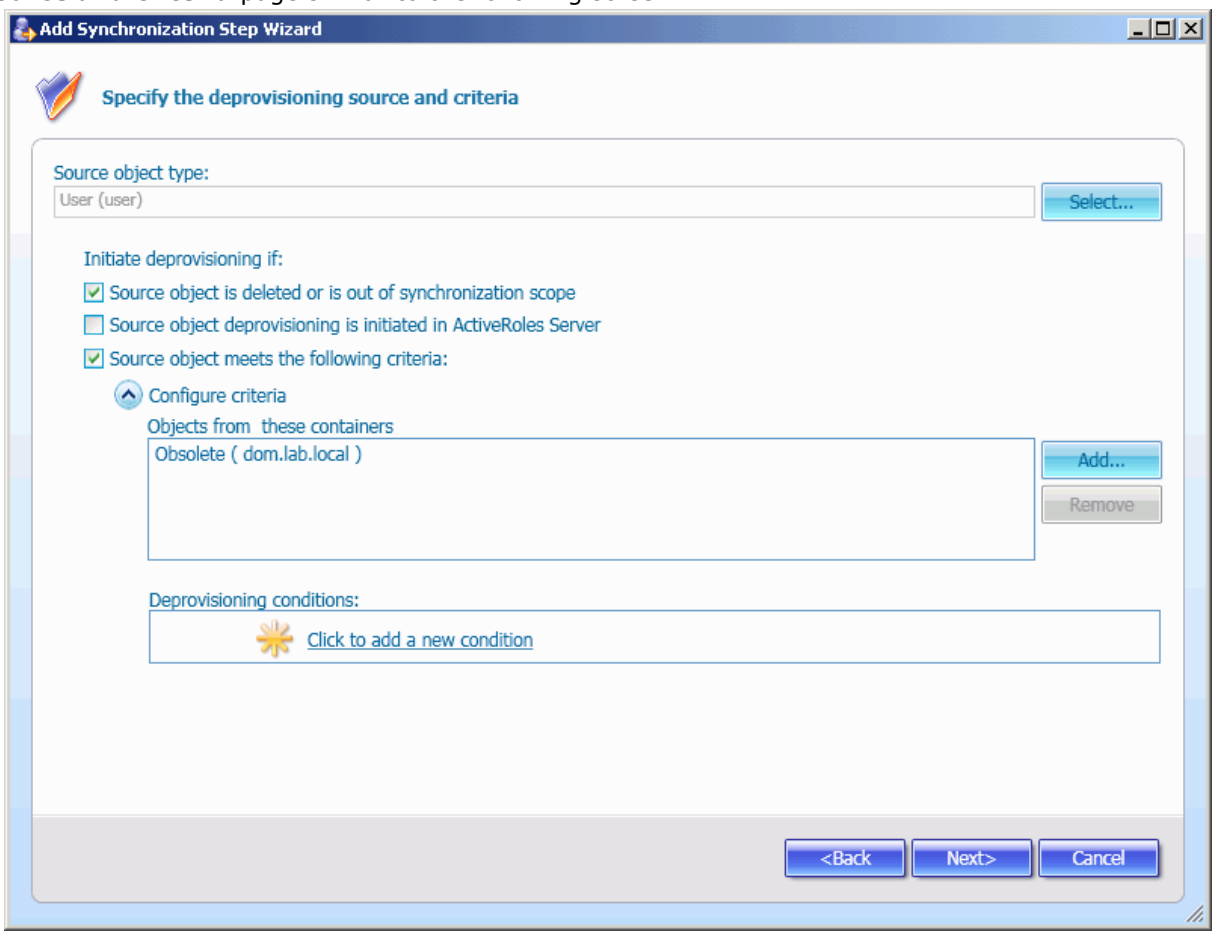
The next is the **Specify target for the update step** page. Use this page to specify the class and location of objects in the target data system to update.

The next is the **Configure rules for the update step** page. Use this page to optionally configure the following rules:

- **Attribute update rules**: Specify how to update the target objects attributes. For details, see "Attribute Transformation Rules" and "Synchronization of Group Memberships" later in this paper.
- **Object location rules**: Specify a parent container for the target objects to update. For details, see "Specifying Target Container" later in this paper.
- **Object name generation rules**: Specify how to generate the target object name. For details, see "Generating Object Name" later in this paper.

Configuring Deprovisioning Step

If you select to add a new deprovisioning step, the wizard displays the **Specify the deprovisioning source and criteria** page similar to the following screen:



Use this page to specify the source object class for the deprovisioning operation and the deprovisioning criteria.

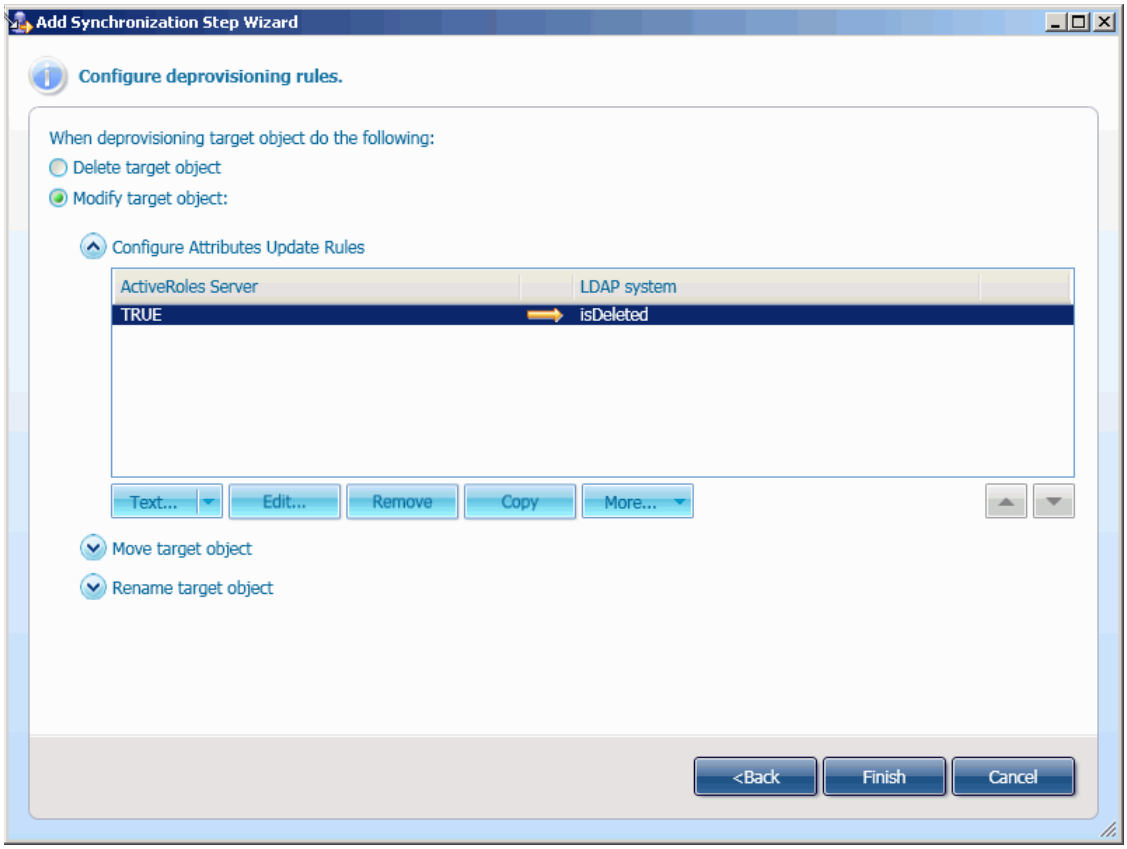
This page defines the following elements:

- **Source object type**: Allows you to specify the source object class for the deprovisioning operation. To select the object class, click **Select**, and then complete the **Select Object Class** dialog box.
- **Initiate deprovisioning if**: Allows you to specify criteria the source objects must meet to initiate deprovisioning in the target data system. You can optionally select or leave cleared the following check boxes:
  - **Source object is deleted or is out of synchronization scope**: Initiates the deprovisioning operation in the target data system if the source object is deleted or is out of synchronization scope.
  - **Source object deprovisioning is initiated in ActiveRoles Server**: Initiates the deprovisioning operation in the target data system if the source object deprovisioning is initiated in ActiveRoles Server. For more information, refer to Quest ActiveRoles Server - Administrator Guide. Note that this check box is only available when deprovisioning from ActiveRoles Server to a connected data system.

- **Source object meets the following criteria**: Specifies additional criteria the source object must meet to initiate a deprovisioning operation in the target data system. To configure the criteria, expand **Configure criteria**, and then use the **Add** and **Remove** buttons to set up a list of containers in the source data system. If a source object resides within any container from the list and meets conditions specified under **Deprovisioning conditions**, if any, Quick Connect initiates the deprovisioning operation in the target data system.

The next is the **Specify target for the deprovisioning step** page. Use this page to specify the target connected data system type and object type to deprovision.

The next is the **Configure the deprovisioning rules** page similar to the following screen:



Use this page to specify how to deprovision the target object. This page defines the following elements:

- **Delete target object**: Select this option to delete the target object when deprovisioning.
- **Modify target object**: Select this option to ensure that the deprovision operation will modify the target object using the rules configured under the following items:
  - **Configure Attributes Update Rules**: Specifies how to modify the target object attributes. For details, see "Attribute Transformation Rules" and "Synchronization of Group Memberships" later in this paper.
  - **Move target object**: Specifies the container(s) in the target data system to which the target object will be moved. For details, see "Specifying Target Container" later in this paper.
  - **Rename target object**: Specifies a list of rules on how to generate the target object name. For details, see "Generating Object Name" later in this paper.

Configuring Synchronization Rules

When configuring the provisioning, deprovisioning or update step, the Add Synchronization Step wizard allows you to define additional synchronization rules. You can configure the synchronization rules of the following categories:

- Rules specifying a container in a target data system
- Target object name generation rules
- Group memberships synchronization rules
- Synchronization rules for multivalued attributes
- Attribute transformation rules

Specifying Target Container

When provisioning, deprovisioning or updating objects, the Add Synchronization Step wizard allows you to define container(s) in the target data system where the objects will be created or to which the object will be moved. You can cause Quick Connect to put all objects into the same target container or configure rules that define individual target containers for each object to provision/deprovision/update.

On the **Configure provisioning rules**, **Configure deprovisioning rules** or **Configure rules for update step** page, you can use the following procedures.

To specify the same target container for all objects to provision/deprovision/update

- Click **Browse**, and then select the container using the **Select Container** dialog box.

To specify individual target containers for objects to provision/deprovision/update

Click the arrow to the side of the **Attribute** button, and then select one of the following items:

- **Script**: Allows you to compose a PowerShell script that calculates the target container name, such as the container DN. The source of this calculation is based on the target object properties. For example, your script can designate different Organizational Units for users living in different cities (see the scenario "Provisioning Users from Connected System to Active Directory" later in this paper.) For more information about PowerShell scripts, refer to "Developing PowerShell Scripts for Synchronization Rules" in ActiveRoles Quick Connect - SDK.
- **Rules**: Allows you to configure a set of rules used to calculate the target container name. For details, refer to "Configuring Attribute Generation Rule" below.

Generating Object Name

When provisioning, deprovisioning or updating objects in the target data system, the Add Synchronization Step wizard allows you to create a list of rules on how to generate the object name. The object name format depends on the category of the target data system. For example, for Active Directory, the object name is the object distinguished name.

To specify rules on how to generate the object name

1. Under **Set up a list of rules on how to generate the object name**, do one of the following:
   - Click **Attribute**: Ensures that the target object name will be equal to the value of the specified object attribute.
   - Click the arrow to the side of the **Attribute** button, and then select **Rules:** Allows you to configure a set of rules used to obtain a value to which the object name must be equal. For details, refer to "Configuring Attribute Generation Rule" below.
   - Click the arrow to the side of the **Attribute** button, and then select **Script**: Allows you to compose a PowerShell script that calculates the target object name. For details, refer to "Developing PowerShell Scripts for Synchronization Rules" in ActiveRoles Quick Connect - SDK.
2. Optionally, repeat Step 1 to add a new name generation rule to the list.

You can optionally copy/paste existing object name generation rule, by performing the following steps:

1. In the **Set up a list of rules on how to generate the object name** list, right-click a rule, and then on the shortcut menu, click **Copy** to copy the rule to the application Clipboard.
2. In the rules list, right-click an entry, and then click **Paste** on the shortcut menu.
   This adds the rule from the Clipboard to the rules list.

How it works?

When the list of rules includes several entries, Quick Connect first tries to create the target object with the name calculated using the rule N 1 in the list. If the object with that name already exists, Quick Connect tries to create the target object with the name calculated using the rule N 2, etc.

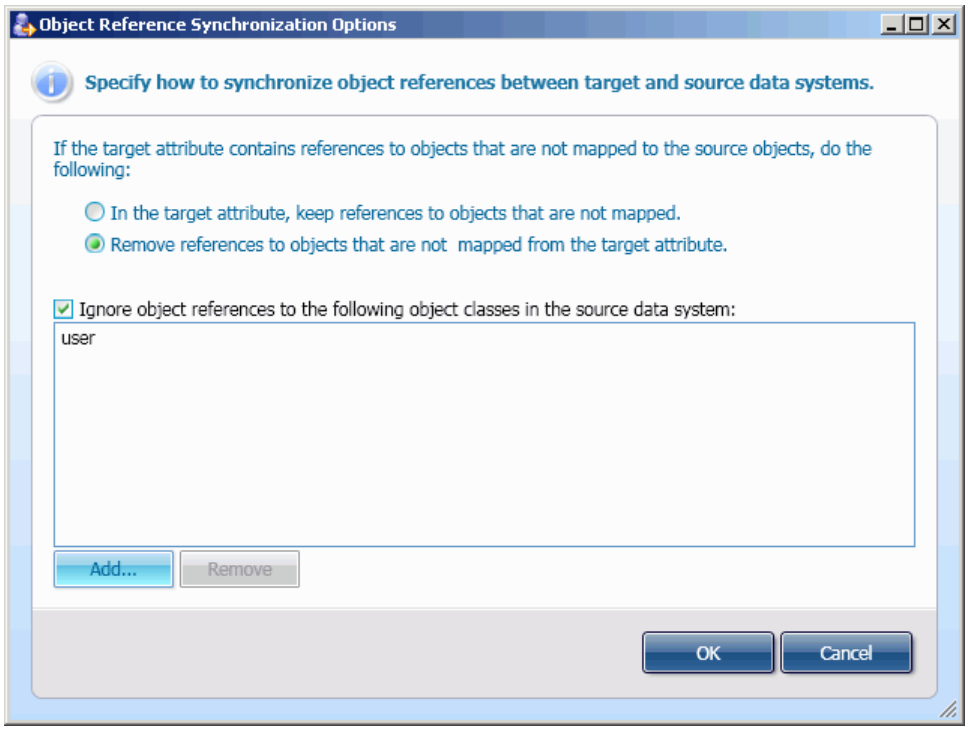
Synchronization of Group Memberships

When configuring synchronization rules using the Add Synchronization Step wizard, you can configure additional rules applied to a synchronization of group memberships. For example, when provisioning a group object from Active Directory to AD LDS (ADAM), you can specify rules for synchronizing between the "member" attribute in ADAM and the "edsaMember" attribute in Active Directory.

To specify rules for synchronization between the "edsaMember" and "member" attributes when provisioning the group objects, perform the following steps:

1. On the **Configure the provisioning rules** page, expand **Configure Initial Attribute Population Rules**, and then click **Attribute** to add the **edsaMember** => **member** pair to the list.
2. From the list, select the **edsaMember** => **member** pair, click **More**, and then click **Options**.

   *The **Object References Synchronization Options** dialog box similar to the following screen opens:*



   This dialog box allows you to specify how to synchronize references to the target system objects that are not mapped to their counterparts in the source system (for details, refer to "Managing Objects Mapping" later in this document). To specify rules for the object references synchronization, use the following elements:

   - **In the target attribute, keep references to objects that are not mapped**: Select this option to ensure that the "member" attribute of the target group will keep references to objects that are not mapped to their counterparts in the source group.
   - **Remove references to objects that are not mapped from the target attribute**: Select this option to ensure that the "member" attribute of the target group will not contain any references to objects that are not mapped to their counterparts in the source group.
   - **Ignore object references to the following object classes in source data system:** Select this check box and then use the **Add** and **Remove** buttons to specify a list of the object classes that will not participate in the group memberships synchronization.

Synchronization Rules for Multivalued Attributes

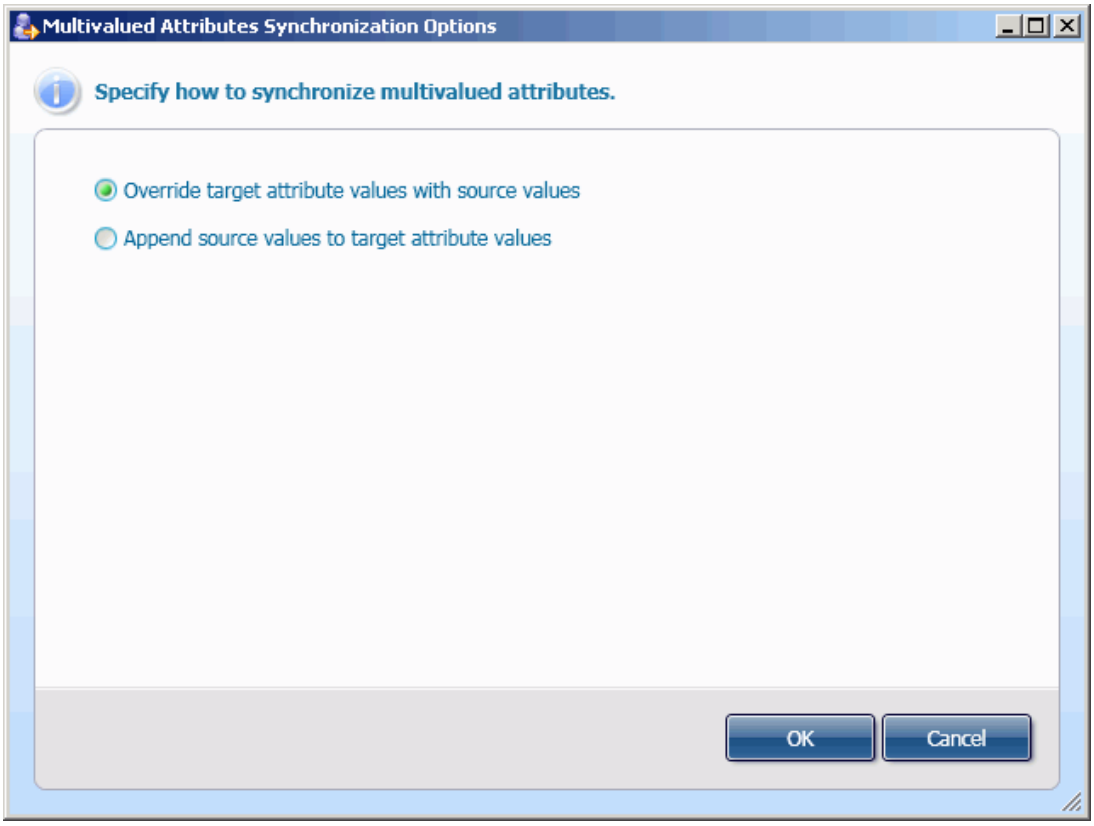
When configuring synchronization steps, you can configure additional rules applied to a synchronization of multivalued attributes. For example, when provisioning or updating a user object from Active Directory to AD LDS (ADAM), you can specify additional rules for synchronizing between the "otherTelephone" attribute in Active Directory and the same attribute in AD LDS using the following procedure.

Optionally, you can configure several synchronization rules for the same object pair. In this scenario, use the **Multivalued Attributes Synchronization Options** dialog box (see below) to specify how to process the attributes values defined in each synchronization rule.

To specify a rule for synchronization between the "otherTelephone" attributes when provisioning the user objects

1. In the Add Synchronization Step wizard, on the **Configure the provisioning rules** page, expand **Configure Initial Attribute Population Rules**, and then click **Attribute** to add the **otherTelephone** => **otherTelephone** pair to the list.
2. From the list, select the **otherTelephone** => **otherTelephone** pair, click **More**, and then click **Options**.

   *The **Multivalued Attributes Synchronization Options** dialog box opens.*



In this dialog box, select one of the following options, and then click **OK**:

- **Override target attribute values with source values**: The target attribute values will be replaced with values in the source attribute.
- **Append source values to target attribute values**: The target attribute values will be kept. The source attribute values will be appended to existing values.

Attribute Transformation Rules

The provisioning, deprovisioning, and update rules configured with the Add Synchronization Step wizard may include subrules that transform attribute values by calculating a target attribute value (or attribute values, in the case of a multivalued attribute).

For example, when configuring provisioning rules, on the **Configure provisioning rules** page, the attribute transformation rules can be configured under **Configure Initial Attribute Population Rules** by completing the following steps:

1. Expand **Configure Initial Attribute Population Rules**.
2. Click the arrow to the side of the **Attribute** button, and then select one of the following values from the list:
   - **Rule**: Defines the *Rule-Based* transformation rule used to obtain a value to which the target attribute must be equal. For details, refer to "Configuring Rules-based Synchronization" later in this document.
   - **Script**: Defines the *Script-Based* transformation rule. Allows you to type a PowerShell script that calculates the target attribute value. For details, refer to "Developing PowerShell Scripts for Synchronization Rules" in ActiveRoles Quick Connect SDK.
   - **Text**: Defines the *Constant-Based* transformation rule. Allows you to set the specified target attribute to a constant text value.
   - **Empty**: Sets the specified target attribute to an empty value. For multivalued attributes, this rule allows you to clear all entries stored in a multivalued attribute.

You can optionally copy/paste existing Attribute Transformation rule (such as an Initial Attribute Population rule or an Attribute Update Rule), by performing the following steps:

1. In the rules list, right-click a rule, and then on the shortcut menu, click **Copy** to copy the rule to the application Clipboard.
2. In the rules list, right-click an entry, and then click **Paste** on the shortcut menu.
   This adds the rule from the Clipboard to the rules list.

Configuring Rules-based Synchronization

After you select **Rules** using the split button on the **Configuring provisioning rules**, **Configuring deprovisioning rules** or **Configuring update rules** page, the application displays the **Configure Rule-based synchronization** dialog box. This dialog box allows you to configure a generation rule to build the target attribute value.

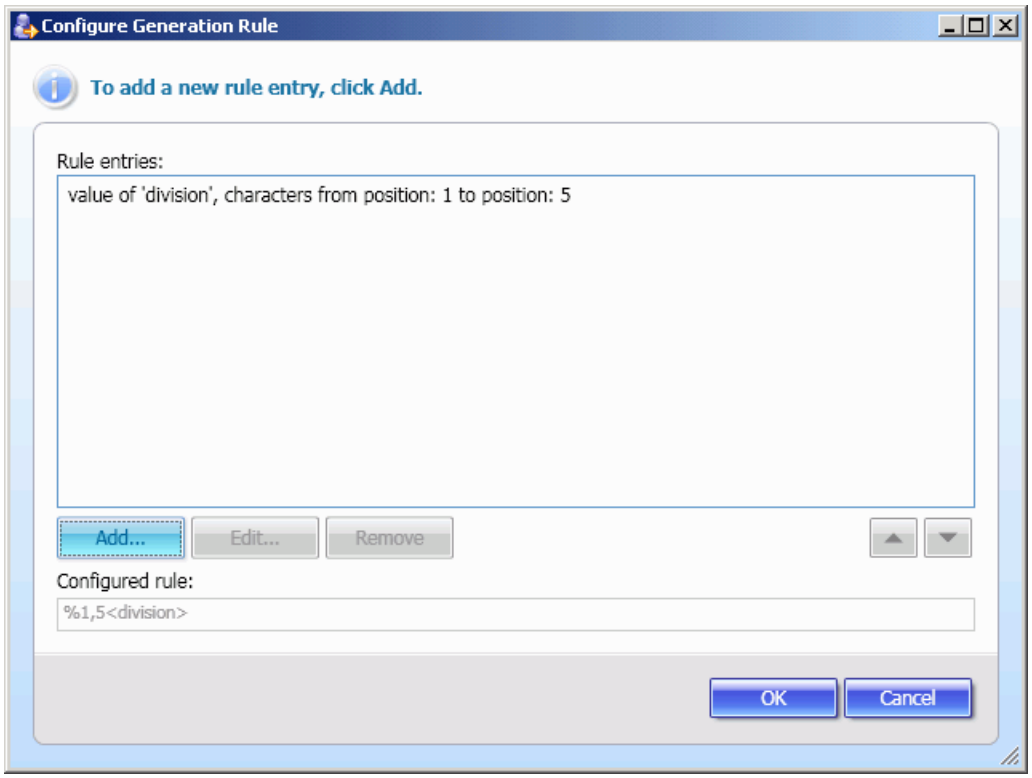
To complete the Configure Rule-based synchronization dialog box

1. Click **Select**, and use the **Select Object Attribute** dialog box that opens to select the target attribute to build.
2. Click **Configure**, and then complete the **Configure Generation Rule** dialog box that opens. When finished, click **OK**

   *For information about how to complete the **Configure Generation Rule** dialog box, refer to "Configuring Attribute Generation Rule" later in this paper.*

Configuring Attribute Generation Rule

The **Configure Generation Rule** dialog box similar to the following screen:



This dialog box allows you to add new generation rule entries, edit or remove existing entries using the **Add**, **Edit** or **Remove** button, respectively.

To remove an existing rule entry

- From the **Rule entries** list, select the entry, and then click **Remove**.

To edit an existing rule entry

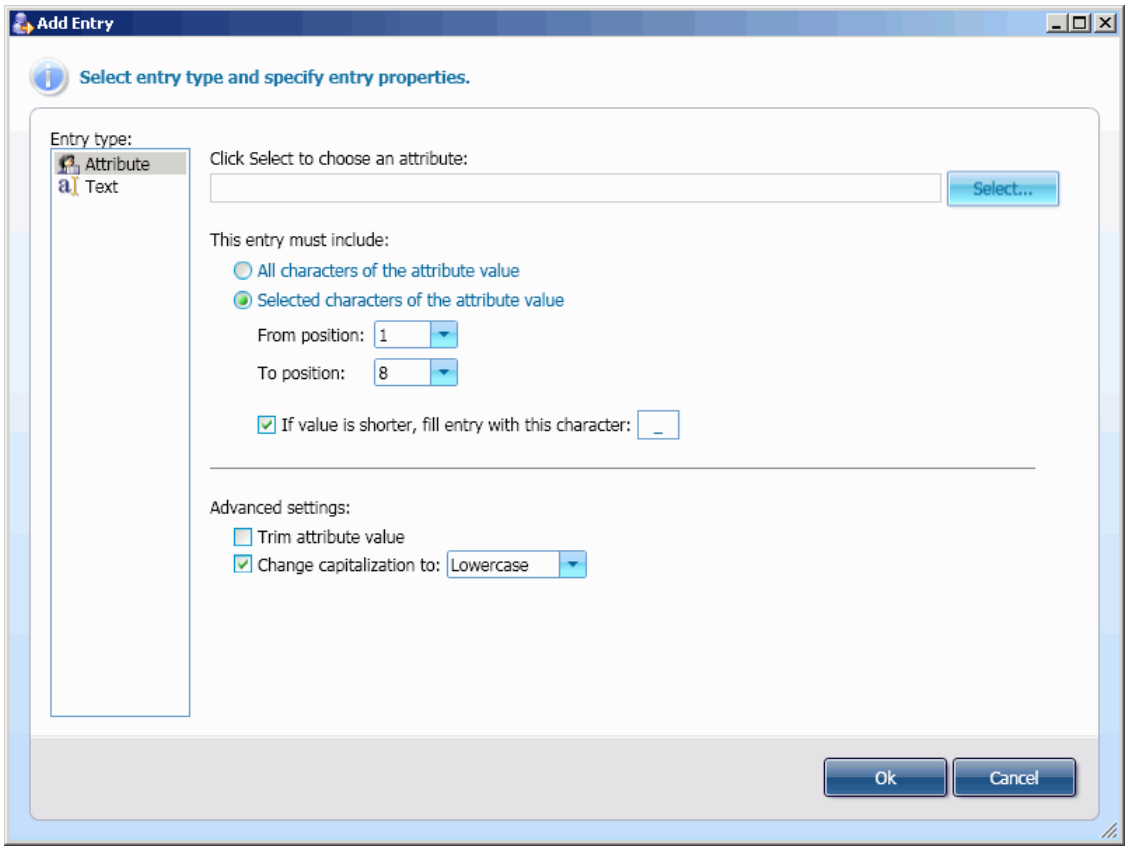
1. From the **Rule entries** list, select the entry, and then click **Edit.**
   *The **Add Entry** dialog box opens.*
2. Configure an entry to include in the rule using one of the appropriate procedures for the entry configuring outlined below.

To add a new rule entry

1. Click **Add.**
   *The **Add Entry** dialog box opens.*
2. Configure an entry to include in the rule using one of the appropriate procedures for the entry configuring outlined below.

Configuring Rule Entries

Use one of the following procedures to configure an entry in the **Add Entry** dialog box. The **Add Entry** dialog box is similar to the following screen:



To configure a Text Entry

1. Under **Entry type**, click **Text**.
2. In the **Configure value to include the following text** text box, type the text string you want the value to include.
3. Click **OK**.

To configure an Attribute based entry

1. Under **Entry type**, click **Attribute**.
2. Click **Select**, click the attribute to include in the value, and then click **OK**.
3. If you want the entry to include the entire value of the attribute, click **All characters of the attribute value**. Otherwise, click **Selected characters of the attribute value**, and specify characters to include in the entry using the **From position** and **To position** lists.
4. Optionally, use **If value is shorter, fill entry with this character** to specify the character that will fill the entry.
5. Optionally, specify **Advanced settings**.
6. When finished, click **OK**.

Modifying Synchronization Step Settings

Once you have created a synchronization step, you can view or modify its settings.

To view or modify settings of a synchronization step

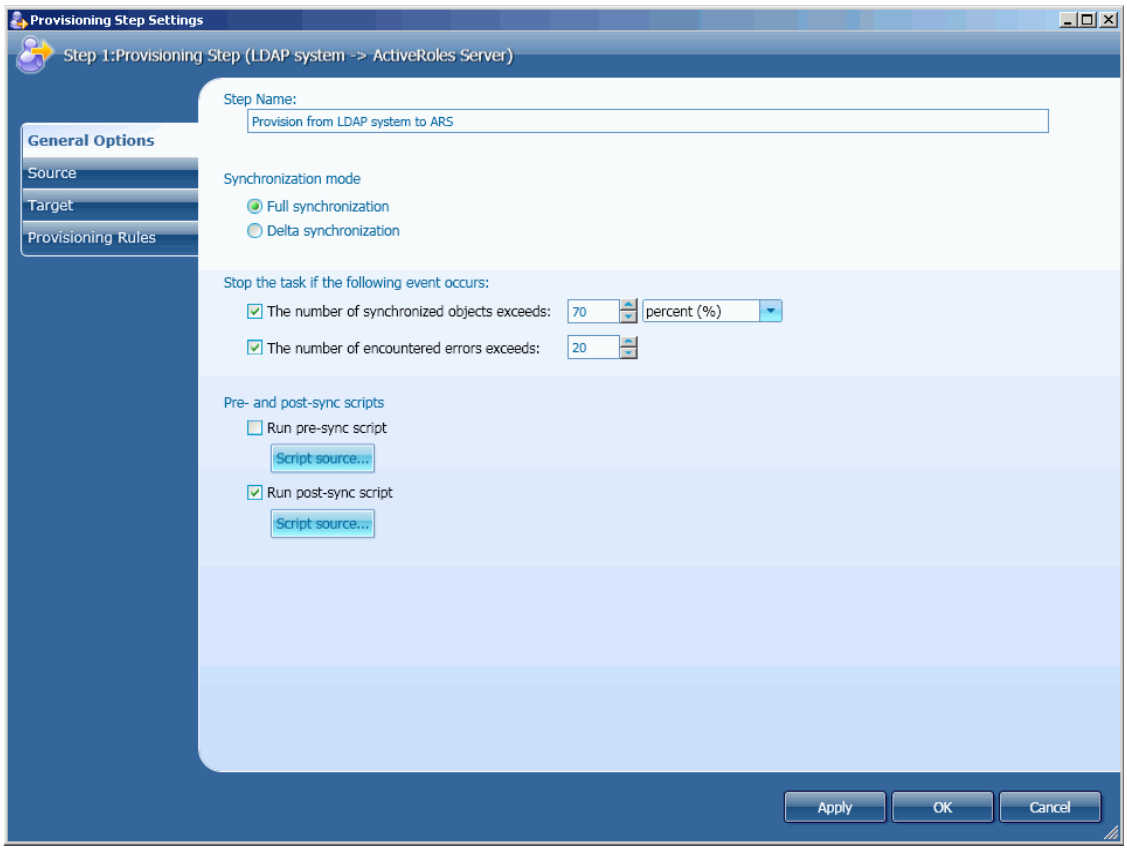
1. In the Quick Connect console, open the tab with the synchronization workflow that includes the synchronization step you want to examine.
2. Click the synchronization step.

   *The **Step Settings** dialog box opens.*
3. Use the tabs in the ***Step Settings*** dialog box to view and modify the synchronization step settings.

The tabs in the **Step Settings dialog** box, except the **General Options** tab, provide the same options as the wizard for creating the synchronization step. For information about the options specific to each type of the synchronization step, use instructions found in "Managing Synchronization Workflows" earlier in this paper.

The General Options Tab

In the **Step Settings** dialog box, the **General Options** tab is similar to the following screen:



The **General Options** tab allows you to view and modify the following settings of a synchronization step:

- **Step Name**: type the new step name in the **Step Name** text box.
- **Synchronization mode**: Under **Synchronization mode,** you can select **Full synchronization** (default mode) or **Delta Synchronization**. In the delta synchronization mode, the application processes only data that has changed in the connected data source or in Active Directory since the last synchronization between the data sources.
- *Stop Threshold*: Under **Stop the task if the following event occurs,** optionally specify a maximum number of objects that can be synchronized during one synchronization step, and a maximum number of the encountered errors.

  Quick Connect Sync Engine stops the synchronization step execution if any of these numbers exceeds the specified threshold values.
  Note that you may set an explicit maximum number of objects or a maximum percent of the total number of objects in the source data system.

- *Pre- and post-sync scripts execution: You* can optionally specify the PowerShell scripts to run before starting the synchronization step and after the step terminates. For example, you can develop scripts that add information on the synchronization step to the application log or send a emaIl notification about a planned synchronization step to an Administrator. To add your script, select the **Run pre-sync script** or **Run post-script** check box, click **Script source**, and then type the script source in the **Script Editor** dialog box. For information about how to develop the PowerShell scripts, refer to Quick Connect SDK.

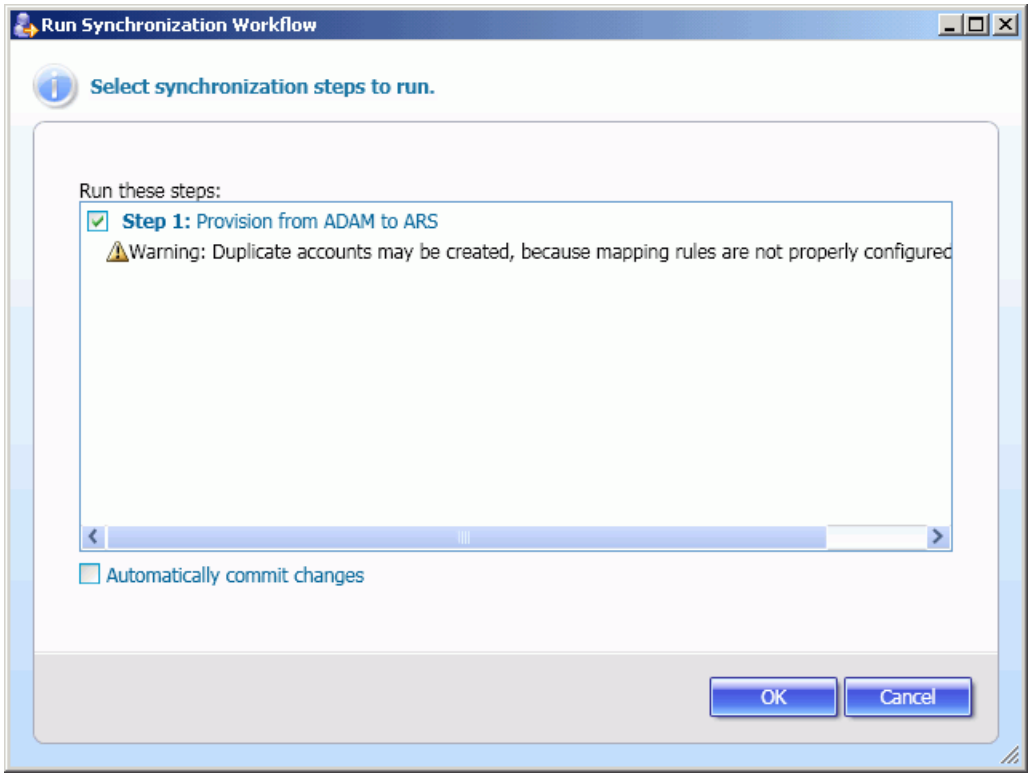
Running Synchronization Workflows

Quick Connect Sync Engine stores information on the created synchronization workflows in the application configuration database. Using the Quick Connect console you can run the selected synchronization workflow manually or schedule it to start at a specific time in the future.

To run a synchronization workflow

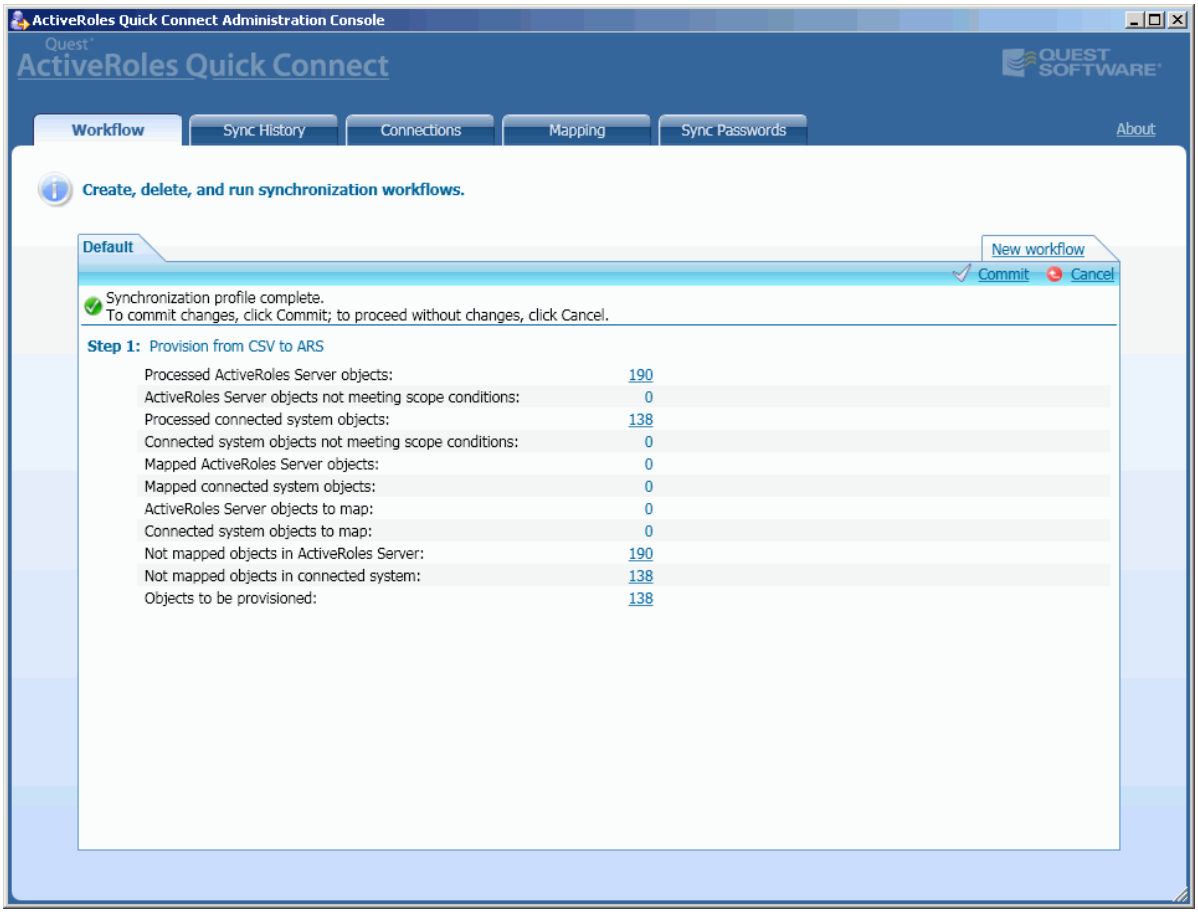
1. In the Quick Connect console, open the tab with the synchronization workflow to run, and then click **Run now**.

   *The **Run Synchronization Workflow** dialog box opens. This dialog box is similar to the following screen:*



2. In the **Run Synchronization Workflow** dialog box, select check boxes next to synchronization steps you want to run, optionally, select the **Automatically commit changes** check box, and then click **OK**.

   After the workflow execution is completed, the console displays the synchronization operation report similar to the following screen:

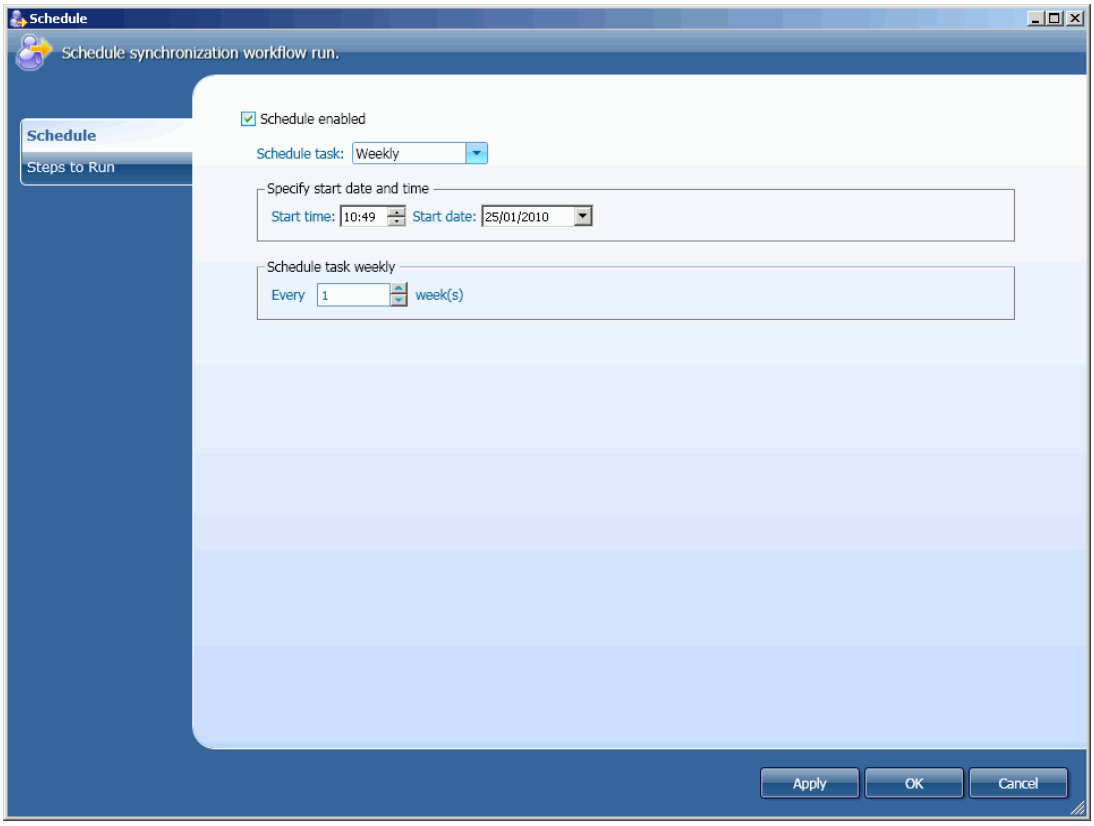


   To get more information on the objects that participate in the synchronization process, click links available in the column 2 of this report.

3. If you left the **Automatically commit changes** check box cleared, do the following:
   to commit changes, click **Commit**
   -- OR --
   to proceed without changes, click **Cancel**.
   If you select the **Automatically commit changes** check box, click **Cancel** to close the synchronization operation report.

To schedule the execution of a synchronization workflow

1. In the console, open the tab with the synchronization workflow to run, and then click **Schedule**.
   *The application displays the **Schedule** dialog box similar to the following screen:*



2. In the **Schedule** dialog box, on the **Schedule** tab, select the **Schedule enabled** check box, and then specify when you want the workflow execution to start. When finished, click **OK**.
3. In the **Schedule** dialog box, on the **Steps to Run** tab, select check boxes next to synchronization steps you want to run.

Configuring Connections

The **Connections** tab allows you to configure settings for connections to external data systems and ActiveRoles Server. This tab is divided into the **ActiveRoles Server** and **Connected systems** areas that allow you to configure or modify settings that Quick Connect Sync Engine uses to establish connections to ActiveRoles Server and external data systems, respectively.

Creating a Connection

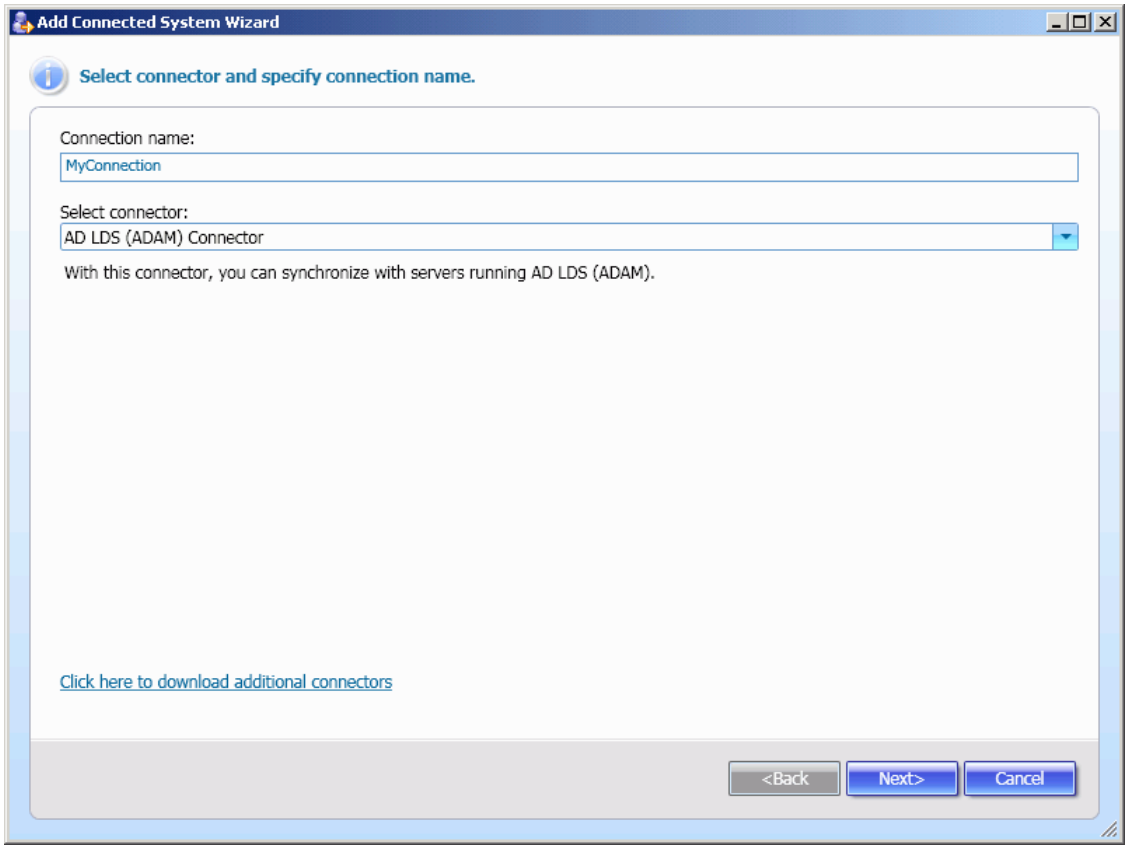
Quick Connect Sync Engine provides for the Add Connected System wizard. The wizard adds a specific external data system to the Quick Connect environment, and configures a connection to that connected data system. You can manually start the wizard using the following procedure:

To start the Add Connected System wizard

1. In the Quick Connect console, open the **Connections** tab.
2. Click the **Click to add a new connected system** link.

Quick Connect Sync Engine automatically runs the Add Connected System wizard after you select the type of the connected data system in the Add Synchronization Workflow wizard (see "Managing Synchronization Workflows" earlier in this paper).

When started, the Add Connected System wizard displays the **Select connector and specify connection name** page similar to the following screen:



From the **Select connector** list, select the desired connector. For information about supported types of connected data systems, refer to "Connected Data Systems" earlier in this paper. In the **Connection name** text box, type the new connection name such as *MyConnection*. When finished, click **Next** to proceed with the wizard.

The next page(s) depend(s) on the category of the external data system to which you want to establish a connection. For details, see "Configuring Connections to Active Directory and AD LDS" and "Configuring Connections to External Data Systems" later in this document.

The next is the **Specify attributes used to uniquely identify an object in the connected system** page. On this page, from the **Available attributes** list, select attributes you want to identify the object in the connected data system, and then click **Add**. When finished, click **Finish** to close the wizard.

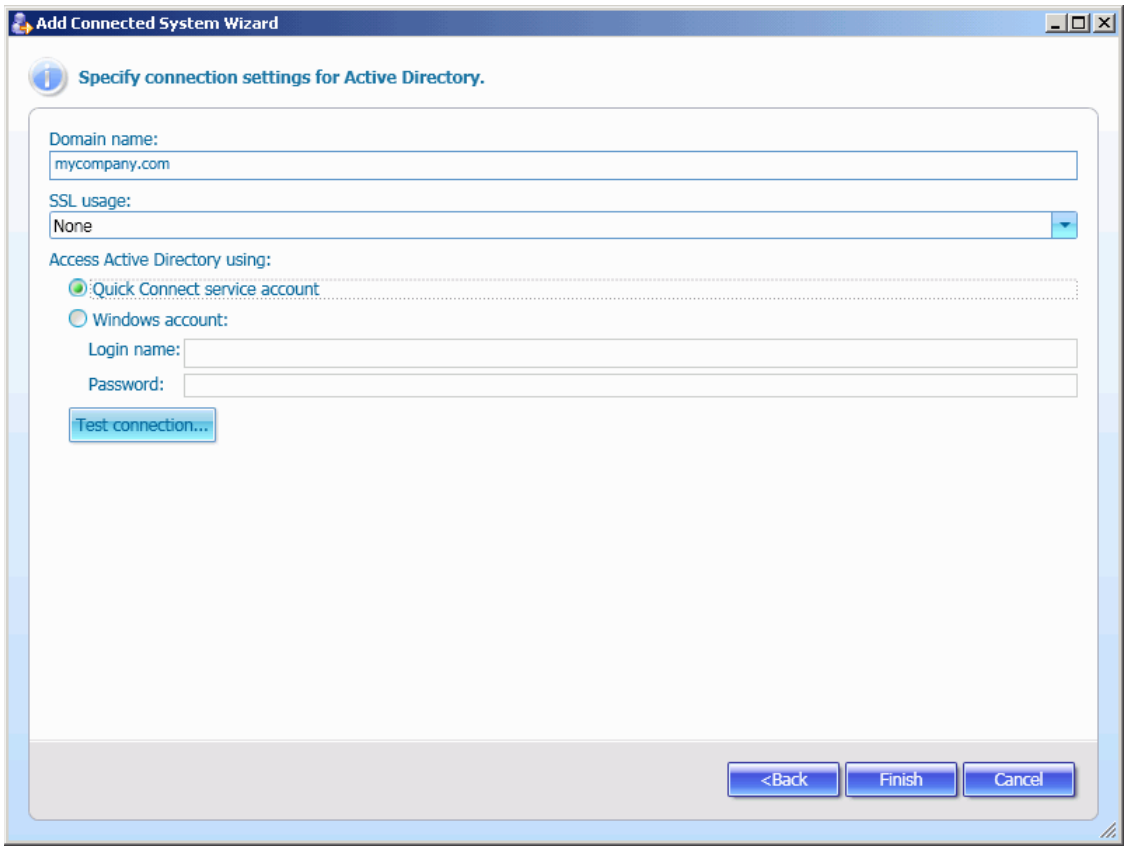
The **Specify attributes used to uniquely identify an object in the connected system** page is displayed only when you create a connection to a Delimited text file, Generic LDAP system, SQL database, Oracle database or a database accessed with OLE DB provider.

Configuring Connections to Active Directory and AD LDS

This section details procedures for configuring connections to Active Directory and AD LDS (ADAM).

Configuring Connection to Active Directory

To establish a connection to Active Directory, complete the **Specify connection settings for Active Directory** page similar to the following screen:

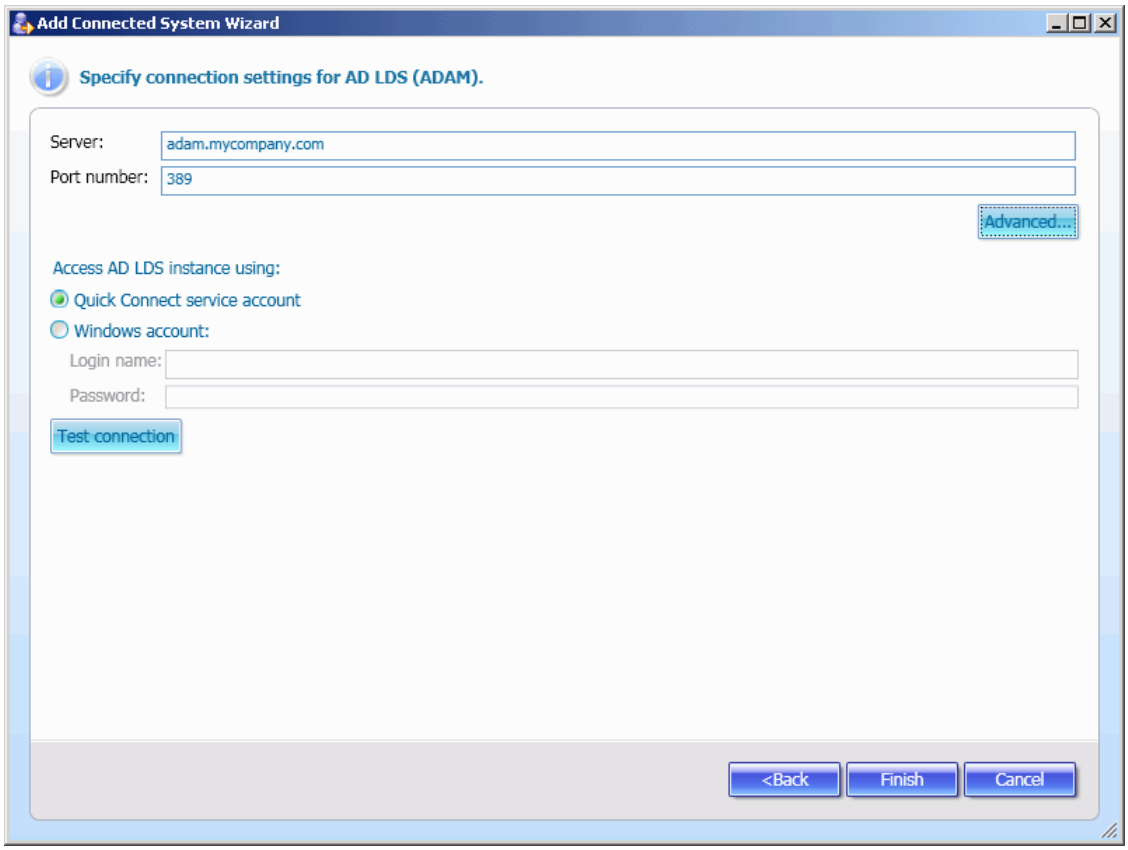


The elements of the page are defined as follows:

- **Domain name**: Type the fully qualified DNS name of the domain to which to connect.
- **SSL usage**: Specify whether to use the Secure Sockets Layer (SSL) protocol to access the domain. In the list, click one of the following options:
  - **Do not use**: SSL will not be used.
  - **Force use**: SSL must be used.
  - **Use if available**: SSL will be used if it is available.
- **Quick Connect service account**: When selected, specifies that Quick Connect Sync Engine accesses the domain in the security context of the Quick Connect service account.
- **Windows account**: Select this option, and then specify the login name and password of the user account under which the application will access the domain.
- **Test connection**: Optionally, click to verify whether the application can access the domain using the specified parameters.

Configuring Connection to AD LDS (ADAM)

To establish a connection to an AD LDS (ADAM) instance, complete the **Specify connection settings for AD LDS (ADAM)** page similar to the following screen:



The elements of the page are defined as follows:

- **Server**: Type the fully qualified DNS name (for example, adam.mycompany.com) of the computer on which the instance is running.
- **Port number**: Type the Lightweight Directory Access Protocol (LDAP) communication port number in use by the instance (the default communication port for LDAP is 389).
- **Advanced**: Click to specify advanced options to access ADAM service.
- **Quick Connect service account**: When selected, specifies that Quick Connect Sync Engine accesses the specified ADAM instance in the security context of the Quick Connect service account.
- **Windows account**: Select this option, and then specify the login name and password of the user account under which the application will access the ADAM instance.
- **Test connection**: Optionally, click to check the connection to the specified data source. If the connection fails, ensure that the settings are correct.

Modifying Connection Settings

The **Connections** tab is divided into the **ActiveRoles Server** and **Connected systems** areas that allow you to view or modify settings for connections to ActiveRoles Server and external data systems, respectively.

ActiveRoles Server

Using links available in this area, you can modify settings that Quick Connect Sync Engine uses to establish a connection to ActiveRoles Server. The following links are available:

- **ActiveRoles Administration service**: Displays the name of the ActiveRoles Administration service to which Quick Connect Sync Engine is connected.

When Quick Connect Sync Engine is configured to use any ActiveRoles Administration service from the specified replication group, this link displays the name of the computer running the ActiveRoles Administration service that is the Publisher of this replication group. For more information, see the description of the **General** tab below.

- **Connection account**: Displays the user account that Quick Connect Sync Engine uses to connect to ActiveRoles Administration service.
- **Synchronization scope**: Specifies the directory containers that will participate in the synchronization process. If this setting is not configured, the synchronization process affects all objects belonging to all domains and AD LDS (ADAM) instances managed by ActiveRoles Administration service to which Quick Connect Sync Engine is connected.

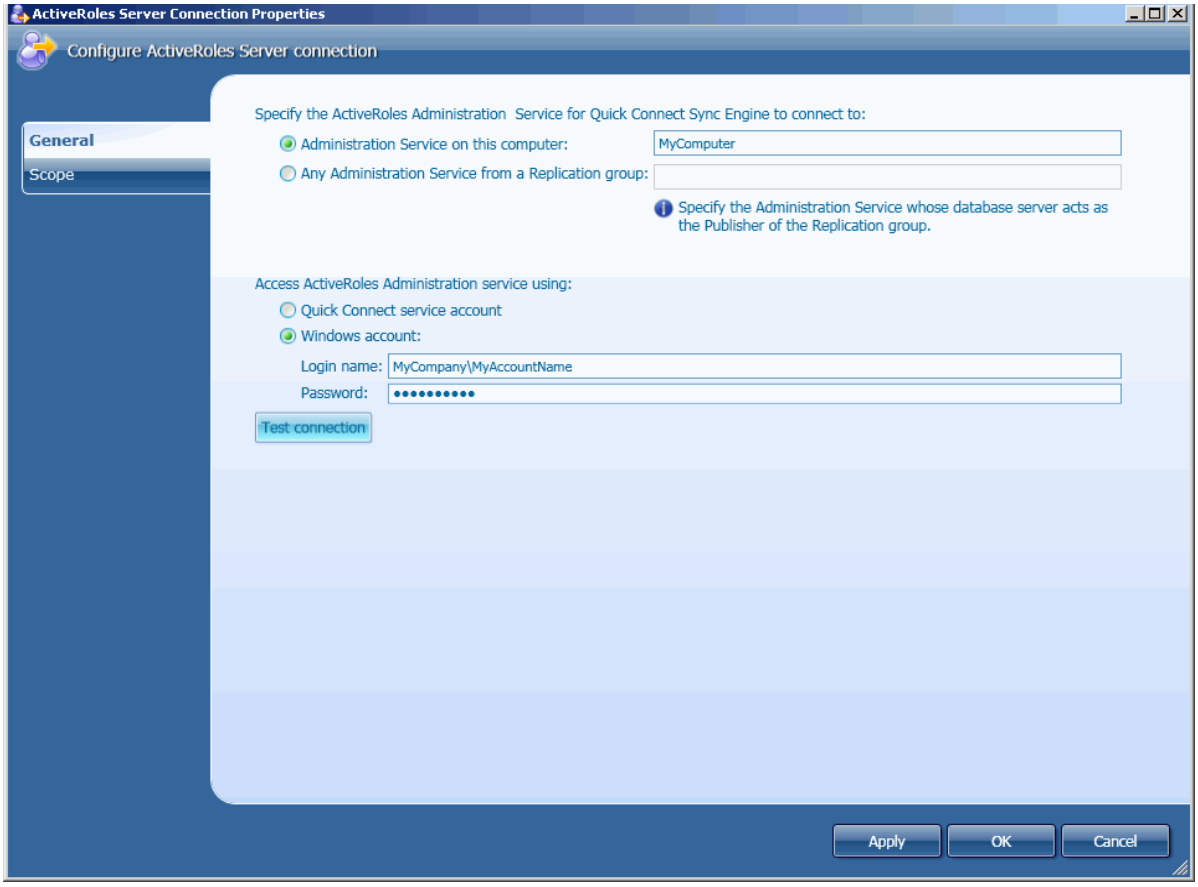
To view or modify these settings, click any above mentioned link.

Clicking the **Synchronization scope** link causes the Quick Connect console to display the **Scope** tab of the **ActiveRoles Server Connection Properties** panel.

The **Scope** tab allows you to specify the directory containers that will participate in the synchronization process. If this setting is not configured, the synchronization process affects all objects belonging to all domains and AD LDS (ADAM) instances managed by ActiveRoles Administration service to which Quick Connect Sync Engine is connected.

Clicking the **ActiveRoles Administration service** or **Connection account** link causes the Quick Connect console to display the **General** tab of the **ActiveRoles Server Connection Properties** panel.

The **General** tab is similar to the following screen:



The elements of the **General** tab are defined as follows:

- **Administration Service on this computer**: Select this option, and then specify the name of the computer running the ActiveRoles Administration service you want Quick Connect Sync Engine to use.
- **Any Administration Service from a Replication group**: Select this option, and then specify the name of the computer running the ActiveRoles Administration service that is the Publisher of a Replication group.

  When this option is selected, Quick Connect Sync Engine can use any available Administration Service from the specified Replication group.
- **Quick Connect service account**: When selected, specifies that Quick Connect Sync Engine accesses the Administration Service in the security context of the Quick Connect service account.
- **Windows account**: Select this option, and then specify the login name and password of the user account under which Quick Connect Sync Engine will access the Administration Service.
- **Test connection**: Optionally, click to verify whether Quick Connect Sync Engine can access the Administration Service using the specified parameters.

For information about how to modify settings that Quick Connect Sync Engine uses to access SQL Server, refer to "Using the QCconfig Command-line Tool" later in this paper.

Connected Systems

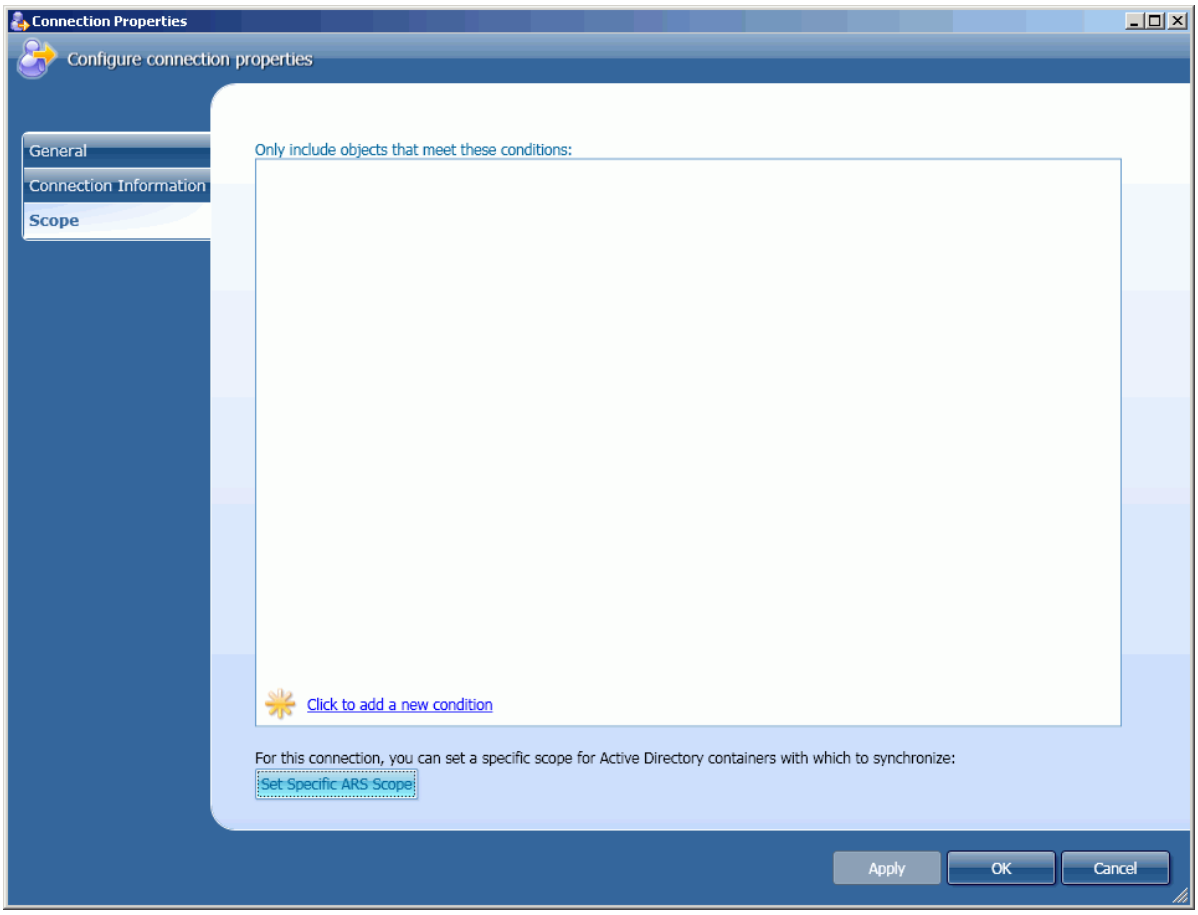
This area lists external data systems that are currently connected to Quick Connect Sync Engine. In the list, each data system is identified by the connection name. In this area, you can create a new connection to an external data system and change settings of an existed connection.

To create a new connection, click the **Click to add a new connected system** link, and then complete the Add Connected System wizard. For more information, refer to "Creating a Connection" earlier in this paper.

To change the connection settings, in the **Connected systems** list, click the connection, and then use the **Connection Properties** panel that opens. This panel depends on the type of the selected connected data system. The tabs in the **Connection Properties** panels, except the **Password** and **Scope** tabs, provide the same options as the Add Connected System wizard (see "Creating a Connection" earlier in this paper). For more information about the **Password** tab, refer to "Managing Passwords Synchronization" later in this paper.

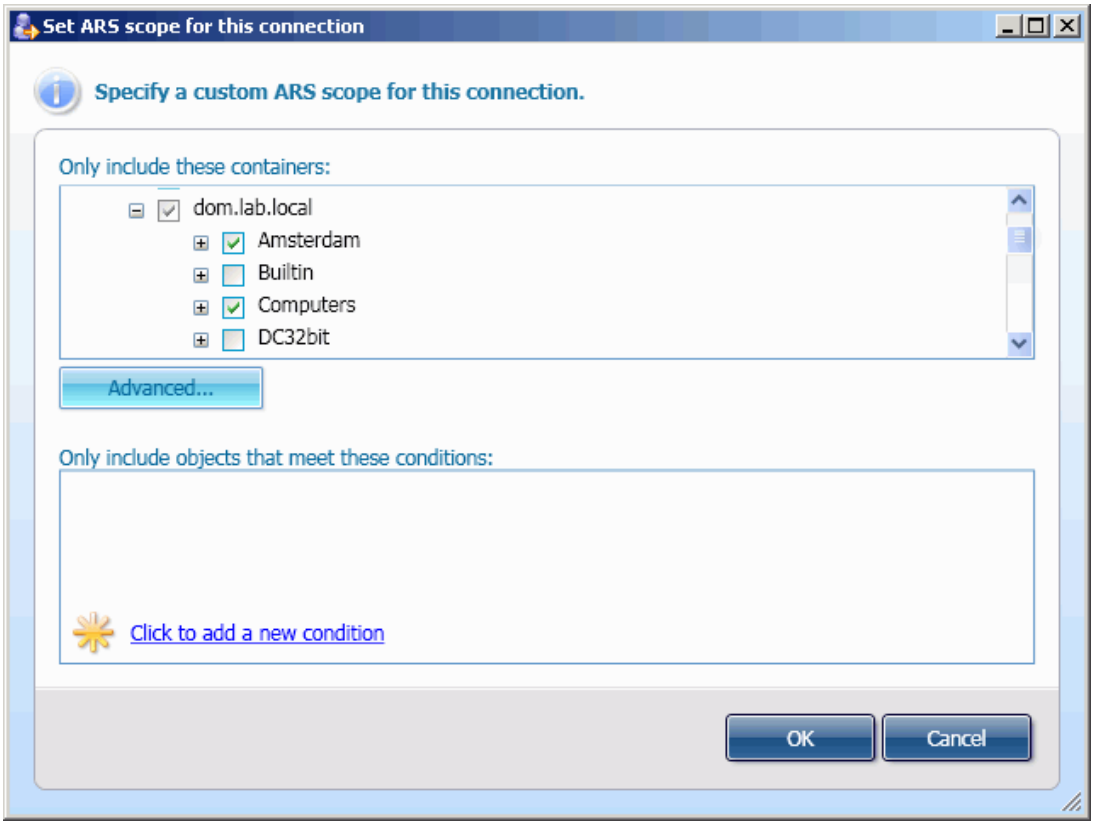
The **Scope** tab allows you to define the scope of connected system objects and Active Directory objects that will participate in the synchronization operations related to this connection.

This tab depends on the connected system category. For example, for SQL Server or Oracle connector, the **Scope** tab is similar to the following screen:



The elements of the **Scope** tab are defined as follows:

- **Only include objects that meet these conditions**: Lists conditions, to which the connected system objects must match to participate in the synchronization process. To specify a new condition, click the **Click to add a new condition** link, and then complete the **Add Condition** dialog box that opens.
- **Set Specific ARS Scope**: Clicking this button displays the **Set ARS scope for this connection** dialog box similar to the following screen:



The elements of this dialog box allows you to define a scope of Active Directory objects that will participate in the synchronization operations related to this connection.

The use of this feature helps you increase flexibility of the synchronization operations for different connections.

Using Sync History Log

The **Sync History** tab lists links to reports on the performed synchronization operations. Using this tab, you can view reports on all performed synchronization workflows runs or filter reports using specified filter criteria. You can also clear the Sync History log.

Viewing Synchronization Reports

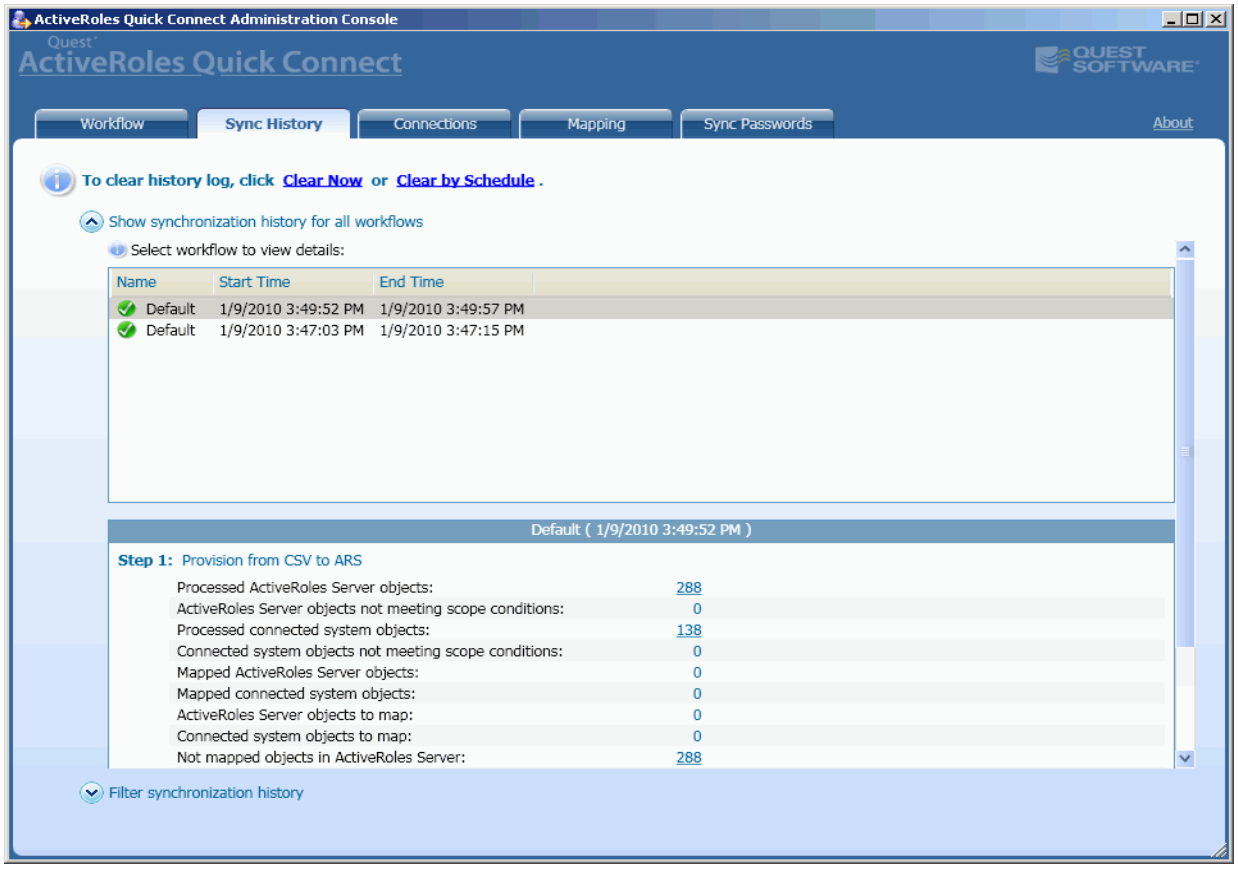
You can display a list of all performed synchronization workflows runs, and then view the report on the workflow run of interest. You can also first filter the synchronization reports for all object pairs using some filter criteria, such as the synchronization operation type, the class of objects participating in the synchronization operation, etc., and then select the report to view.

To view a report from the full list of reports

- On the **Sync History** tab, click **Show synchronization history for all workflows**, and in the workflow runs list, click the desired report.

  *The report is displayed in the lower pane of the **Sync History** tab.*

A report on the synchronization workflow run is similar to the following screen:

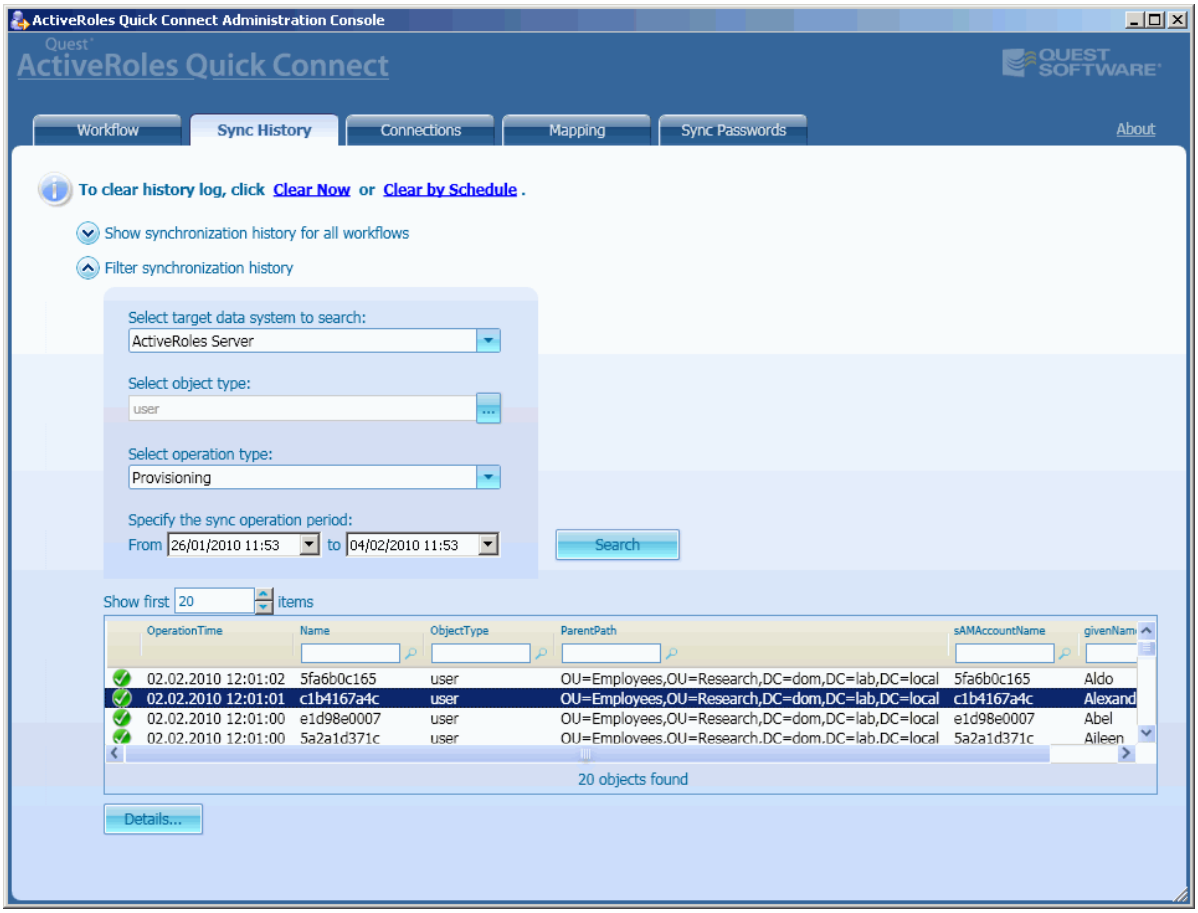


For detailed information, click links in Column 2 of the report. For example, clicking the link next to **Processed ActiveRoles Server objects**, displays the list of the 110 Active Directory objects processed in this synchronization run.

To view a report for a synchronized pair of objects

1. On the **Sync History** tab, click **Filter synchronization history**, specify the filter criteria, and then click **Search**.

   *The list of synchronized pairs of objects that match the specified criteria is displayed beneath the **Sync History** tab:*



2. To view a report on a synchronized pair of objects, in the list, double-click the object pair or click **Details**.

Clearing Sync History Log

You can immediately clear the sync history log or schedule this operation to start at a specific time in the future.

To clear Sync History log

1. On the **Sync History** tab, click the **Clear Now** link.
   *The **Clear Sync History** dialog box opens.*
2. In the **Clear Sync History** dialog box, do the following:
   - Select **Clear all entries** to delete all entries in the sync history log.
   - Select **Clear entries older than** to delete entries older than the specified days. To delete old entries from the log, decrease the number of days.
   - Click **OK** to close the dialog box.

To schedule Sync History log clearing

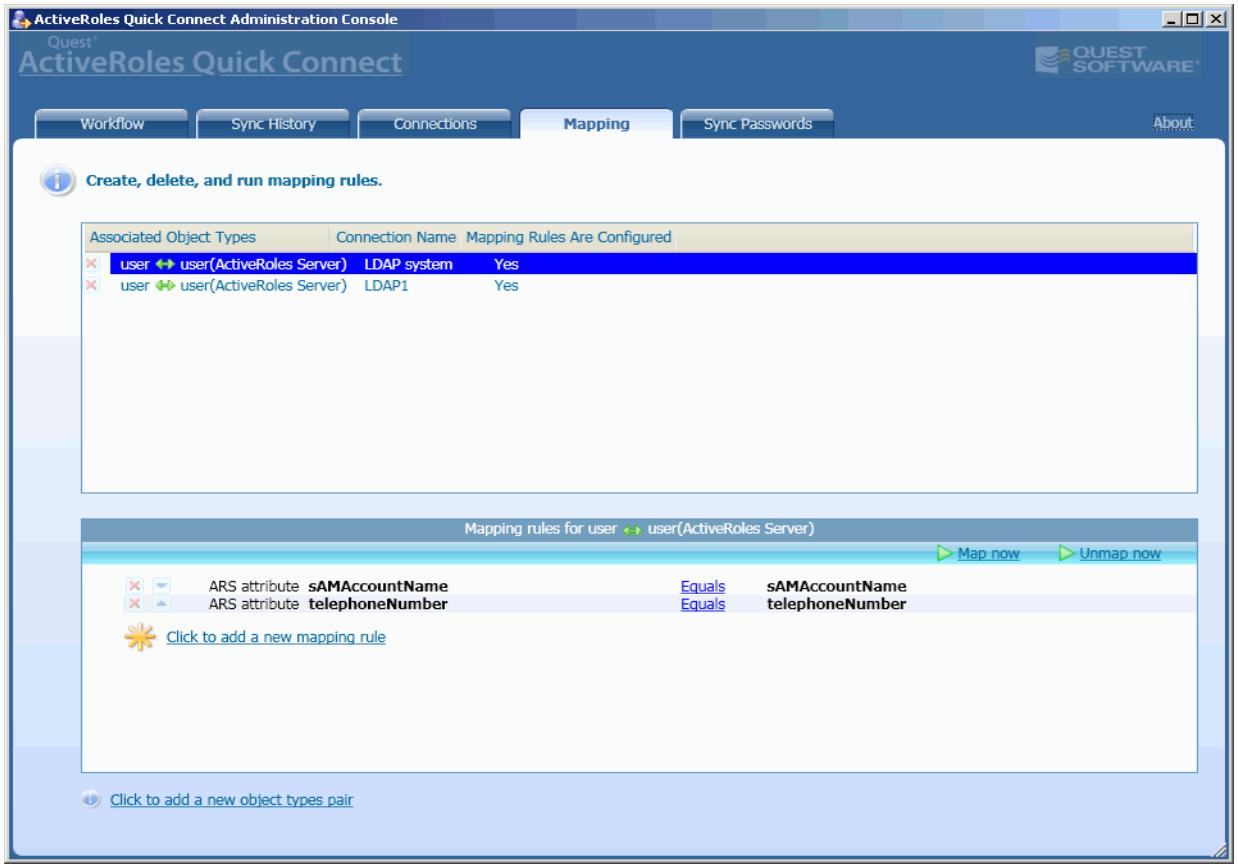
1. On the **Sync History** tab, click the **Clear by Schedule** link.
   *The **Clear Sync History** dialog box opens.*
2. In the **Clear Sync History** dialog box, select the **Schedule enabled** check box, and then specify when you want the workflow execution to start. When finished, click **OK**

Managing Objects Mapping

Quick Connect Sync Engine uses mapping to establish one-to-one relationships between objects in connected data systems and their counterparts in Active Directory.

In the Quick Connect console, the **Mapping** tab allows you to view and modify mapping rules for all available connected data systems. You can also manually configure the mapping.

The **Mapping** tab is similar to the following screen:



The **Mapping** tab is divided into two areas. The upper area displays the pairs of the associated object types that already participate in synchronization processes configured on the **Workflow** tab. if any. For example, if you have configured the User accounts provision from Active Directory to a connected data system, this area will contain an entry similar to one in the following table:

ASSOCIATED OBJECT TYPES	CONNECTION NAME	MAPPING RULES ARE CONFIGURED
user <-> user (ActiveRoles Server)	LDAP system	Yes

If the **Mapping Rules Are Configured** column displays **Yes**, clicking the entry causes the lower area to display all mapping rules configured for the pair of the associated object types.

Using the **Mapping** tab, you can create, modify, delete existing mapping rules, and add new pairs of the associated object types.

When Use Mapping Rules?

When performing a provisioning step, Quick Connect Sync Engine automatically maps the connected system objects to Active Directory objects using the appropriate provisioning rules. Thus, mapping rules are not mandatory for provisioning steps.

Before performing a synchronization workflow that includes the update or deprovisioning steps, you should establish one-to-one relationships between objects in the connected data system and Active Directory. Thus, in some cases, you have to configure mapping rules for performing the update and deprovisioning steps.

Adding an Associated Object Types Pair

By default, the upper area of the **Mapping** tab includes a list of all pairs of the associated object types that already participate in synchronization workflows configured on the **Workflow** tab. Optionally, you can add any new object types pair to this list, and then configure mapping rules for the newly created pair.

To add an associated object types pair

1. On the **Mapping** tab, click the **Click to add a new object types pair** link.
   The Associate Object Types wizard starts.
2. Follow instructions provided in the wizard.

After you complete the Associate Object Types wizard, the Quick Connect console adds the newly created pair of the associated object types to the upper area of the **Mapping** tab. You can optionally configure mapping rules for that object types pair. For details, see "Configuring Mapping Rules" below.

Configuring Mapping Rules

Once a pair of the associated object types is created, you can optionally configure mapping rules for that pair. Mapping rules determine some conditions to which values of attributes of objects in the connected data system and Active Directory must meet. If all mapping rules configured for an associated object types pair are met, Quick Connect Sync Engine establishes one-to-one relationship between an object in the connected data system and its counterpart in Active Directory. Such objects are called *mapped* objects.

To add a new mapping rule

1. In the upper area of the **Mapping** tab, select the object types pair for which you want to create a new mapping rule.

   *The lower part of the **Mapping** tab displays all mapping rules configured for the selected object type pair, if any.*

2. Click the **Click to add a new mapping rule** link.

   *The **Add Rule** dialog box opens. This dialog box allows you to specify an attribute of the ActiveRoles Server object and a value to which the attribute must be equal.*

3. In the **Add Rule** dialog box, to select the ActiveRoles Server attribute from the list of available attributes, click **Select** next to **ActiveRoles Server object attribute**, and then complete the **Select Object Attribute** dialog box.
   - OR -
   To define an advanced mapping rule, click the arrow to the side of the **Attribute** button, and then click **Script**.
   *This opens the **Script Editor** dialog box where you can type a PowerShell script that returns a name of the ActiveRoles Server object attribute to use in the mapping rule. For details, refer to "Developing PowerShell Scripts for Synchronization Rules" in ActiveRoles Quick Connect - SDK.*

4. In the **Add Rule** dialog box, to specify the value to which the ActiveRoles Server object attribute must be equal, click **Attribute**, and then complete the **Select Object Attribute** dialog box.
   - OR -
   To define an advanced mapping rule, click the arrow to the side of the **Attribute** button, and then select one of the following values from the list:
   - **Rules**: Defines the Attribute Generation rule used to obtain a value to which the attribute of ActiveRoles Server object (see Step 3) must be equal. For details, refer to "Configuring Attribute Generation Rule" earlier in this document.
   - **Script**: Allows you to type a PowerShell script that calculates a value to which the attribute of ActiveRoles Server object (see Step 3) must be equal. For details, refer to "Developing PowerShell Scripts for Synchronization Rules" in ActiveRoles Quick Connect - SDK.

Running Mapping Rule

Once you have configured mapping rules for an associated object types pair, you may run the rules. When running a mapping rule, Quick Connect Sync Engine uses that rule to establish one-to-one relationships between objects in the appropriate connected data system and their counterparts in Active Directory. This operation is named "mapping."

To start mapping operation

1. In the Quick Connect console, open the **Mapping** tab.
2. From the list of the associated object types pairs, displayed in the upper area of the **Mapping** tab, select the appropriate object types pair.
3. In the lower part of the **Mapping** tab, click **Map now**.

   The mapping operation for the select object types pair starts.

The report on the mapping operation results is displayed in the lower part of the **Mapping** tab. Use this report to view a list of objects mapped in the connected data system and Active Directory. The report displays the number of objects to map in Active Directory and in connected data system next to **ActiveRoles Server objects to map** and **Connected systems objects to map**, respectively.

To apply the mapping operation results

- In the lower part of the **Mapping** tab, click **Commit**.

Unmapping

Optionally, you can cancel all mappings for the selected associated object types pair. This operation is named "unmapping."

To perform unmapping operation

1. In the Quick Connect console, open the **Mapping** tab.
2. From the list of the associated object types pairs, displayed in the upper area of the **Mapping** tab, select the object types pair for which you want to cancel all existing mappings.
3. In the lower part of the **Mapping** tab, click **Unmap now**.

   The unmapping operation for the select object types pair starts.

The unmapping operation clears all mappings established for the selected associated object types pair.

Managing Passwords Synchronization

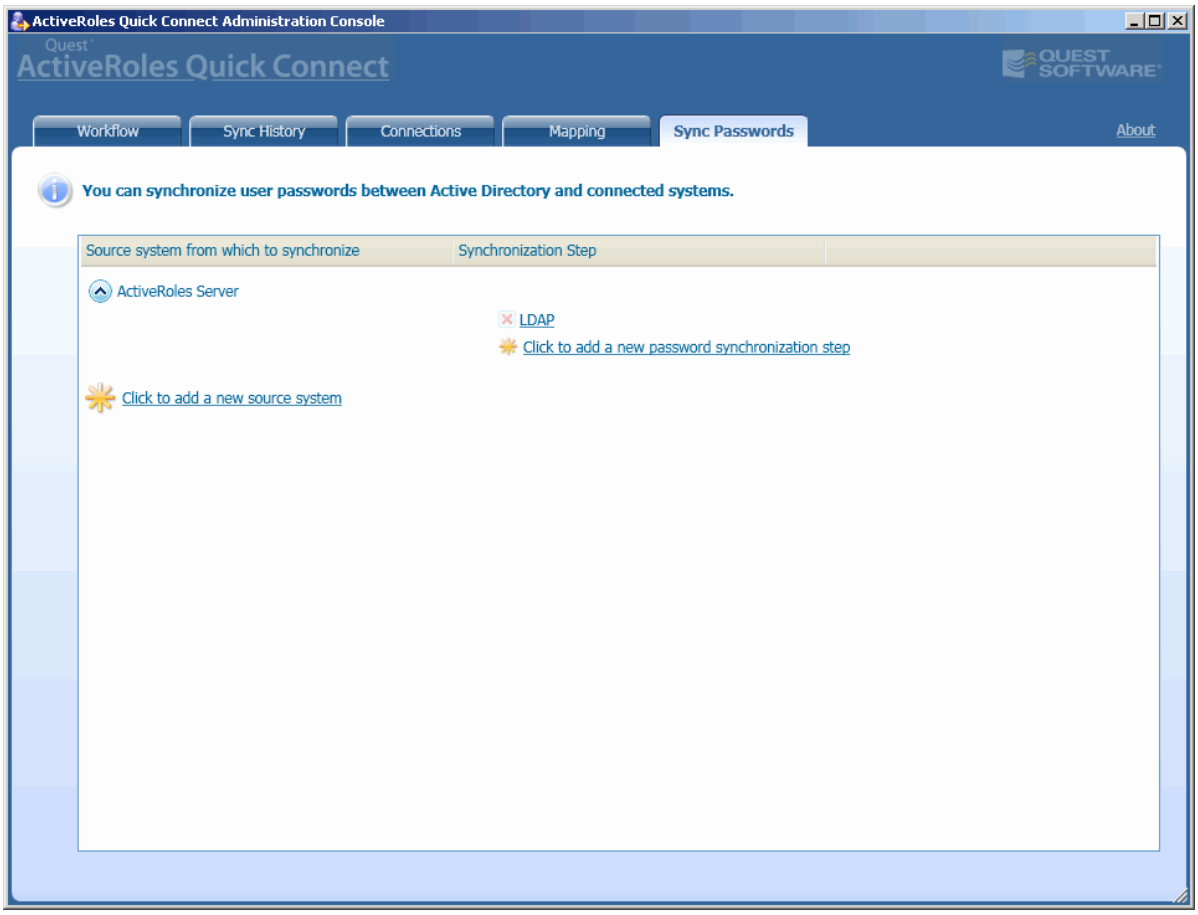
Quick Connect provides for user passwords synchronization between Active Directory and some categories of connected systems. The passwords synchronization is supported for the following categories of connected systems:

- Active Directory connections
- AD LDS (ADAM)
- Sun One Directory server
- SQL Server
- Oracle database
- Novell Directory service
- IBM RACF
- Google Apps service
- SAP systems
- Lotus Domino Server

For Lotus Domino Server, to synchronize Active Directory user's password with the local copy of Lotus Notes ID file stored on the user's workstation, Quick Connect uses Quest Quick Connect for Lotus Notes: Password Sync Client (hereafter *Password Sync Client*).

If you plan to use the passwords synchronization feature for Lotus Domino Server, you must install Password Sync Client on each user's workstation. For information about how to install and configure this application, refer to Quest Quick Connect for Lotus Notes: Password Sync Client - Quick Start Guide.

In the Quick Connect console, the **Sync Passwords** tab allows you to configure the passwords synchronization feature. The **Sync Passwords** tab is similar to the following screen:



The elements of this tab are defined as follows:

- **Click to add a new passwords synchronization step**: Starts the Add Password Synchronization Step wizard. The wizard allows you to add a target connected system with which to synchronize the passwords and configure the passwords synchronization settings. For more information, refer to "Configuring Passwords Synchronization Steps" later in this paper.
- **Click to add a new source system**: Starts the Add Connected System wizard. The wizard adds a source data system for the passwords synchronization. For more information, refer to "Creating a Connection" earlier in this paper.

Prerequisites for Using the Passwords Synchronization

For passwords synchronization to function properly, before configuring the passwords synchronization steps, consider the following key aspects:

ITEM	DESCRIPTION
Quick Connect Capture Agent	Capture Agent tracks changes made to the Active Directory user password, and then sends information about those changes to Quick Connect Sync Engine that uses this information for synchronizing user passwords between Active Directory and specified connected systems. You must install and configure Capture Agents on all domain controllers in data systems that serve as source systems for passwords synchronization. For more information, refer to "Deploying Capture Agents" earlier in this document.
Certificate	For sending passwords from the source domain controllers to Quick Connect service, Capture Agent uses channels encrypted with a certificate. You can configure Capture Agents and Quick Connect service to use your custom certificate or use a built-in certificate delivered with the Quick Connect Sync Engine installation. For more information, refer to "Using Certificates" later in this paper.
Target connected data system	Before configuring the passwords synchronization with a target connected data system, you must specify appropriate settings on the **Password** tab of the **Connection Properties** panel for connection to that data system. These settings depend on the data system category. For more information, refer to "Passwords Synchronization Settings for Connected Data Systems" later in this paper.
Mapping user objects	All user objects in the source data system whose passwords you want to synchronize, must be properly mapped to their counterparts in the target connected data system. For more information, refer to "Managing Objects Mapping" earlier in this document.

Using Certificates

For encrypting channels used for sending password information from Capture Agents to Quick Connect service, Quick Connect uses a certificate. This section covers the following subjects:

- Using a built-in certificate
- Using a custom certificate

Using a Built-in Certificate

You can configure Quick Connect to use a default built-in certificate delivered with the Quick Connect Sync Engine installation. To do this, do not configure the Certificate parameter of Capture Agent and Quick Connect service. Let Quick Connect use the default value of this parameter. For information about configuring parameters of Capture Agent, see "Configuring Capture Agents" earlier in this document.

Using a Custom Certificate

To configure Quick Connect to use your custom certificate, consider the following key aspects:

- Requesting a certificate.
- Exporting the issued certificate to a file.
- Importing the certificate from the file.
- Configuring Capture Agents and Quick Connect service to use the same custom certificate.

This section details steps related to these key aspects.

Requesting a certificate

To issue a certificate, you have to make a certificate request. There are two primary ways to explicitly request certificates in a Windows Server 2003 operating system:

- *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 located in the Certificates snap-in.
- *Request certificates using the Windows Server 2003 Certificate Services Web pages*: Each certification authority that is installed on a computer running Windows Server 2003 has Web pages that users can access to submit certificate requests. By default, these pages are located at **http://servername/certsrv**, where the *servername* refers to the name of the computer running Windows Server 2003.

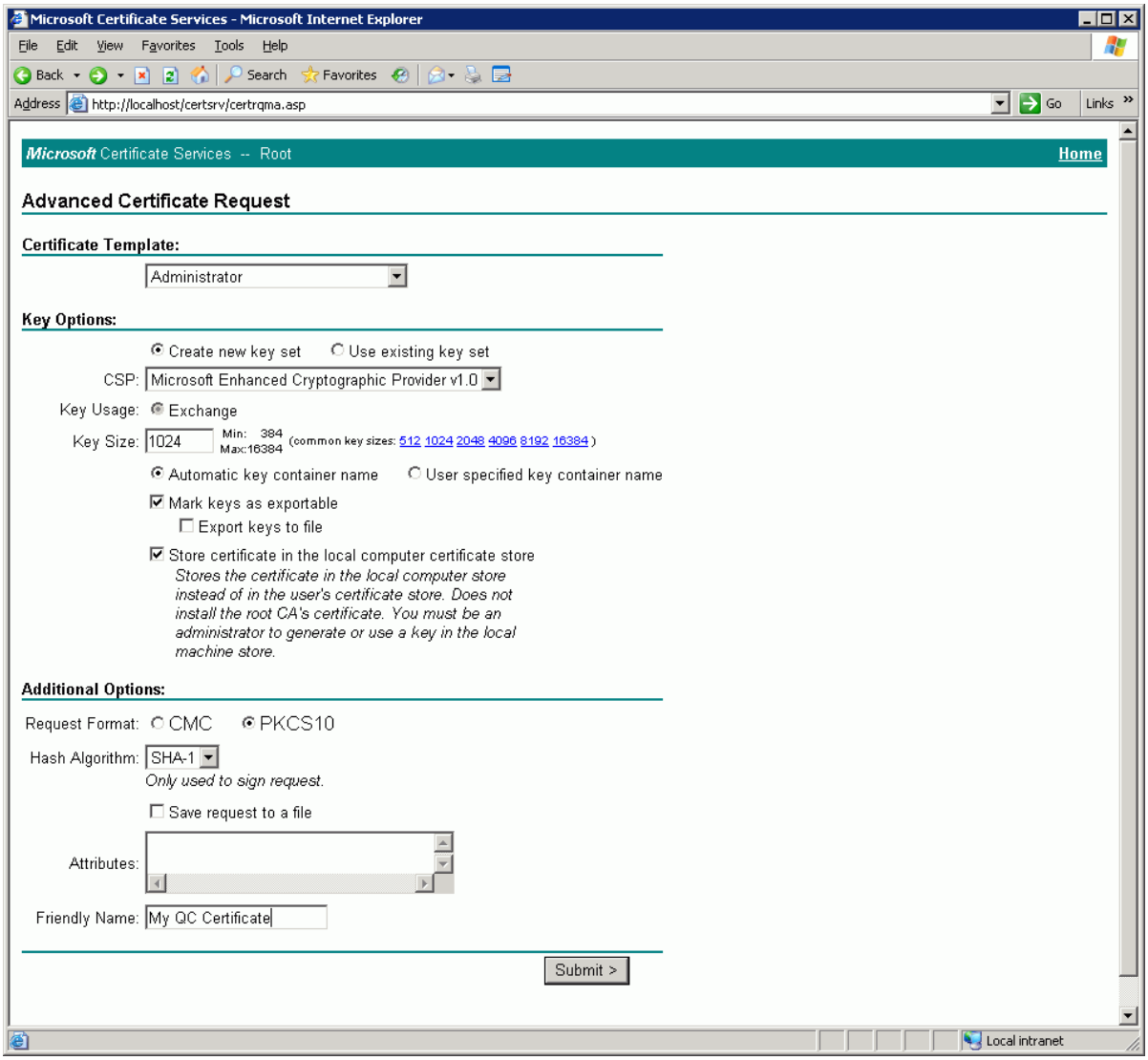
In this document, we detail steps to request certificates using the Windows Server 2003 Certificate Services Web page. For detailed information about the Certificate Request wizard, refer to the documentation on Certification Authority.

To request a certificate using the Windows 2003 Certificate Services web pages

1. Open Internet Explorer and connect to *http://servername/certsrv*, where the *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**.

   The page similar to the following screen opens:



   On this Web page, use default values, except the following fields that you have to specify:

   - Select the **Store certificate in the local computer certificate store** check box.
   - Under **Additional Options**, select the **PKCS10** option, and in the **Friendly Name** text box, specify any name for your certificate (such as My QC Certificate).

5. Click **Submit**.
6. On the **Certificate Issued** Web page, click **Install this certificate**.

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

Exporting the issued certificate to a file

You have to export the issued certificate *with the private key* to a file that will be used to install this certificate on all domain controllers running Capture Agents and on all computers running Quick Connect service.

To export the certificate with the private key

1. On the computer where you have installed the certificate, 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**.

   The Certificate Export wizard starts.
5. On the **Welcome** page, click **Next**.
6. On the **Export Private Key** page, select the **Yes, export the private key** option, and then click **Next**.

   Note that this option will appear 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, in **Password,** 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, in **File name**, type a file name and path for the PKCS #12 file that will store the exported certificate and 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.

Importing the Certificate

You must import your certificate to the **Personal\Certificates** certificate store in the Certificates snap-in on *all domain controllers running Capture Agents* and on *all computers running Quick Connect services* that will participate in the passwords synchronization. You can import the certificate using the Certificate - Local Computers snap-in.

For Capture Agents to function properly, you must import your certificate only to the **Personal\Certificates** store.

To import a 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**.
   The Certificate Import wizard starts.
4. On the **Welcome** page, click **Next**.
5. On the **File to Import** page, in **File name**, type the file name containing the certificate to be imported. or click **Browse** and navigate to 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.

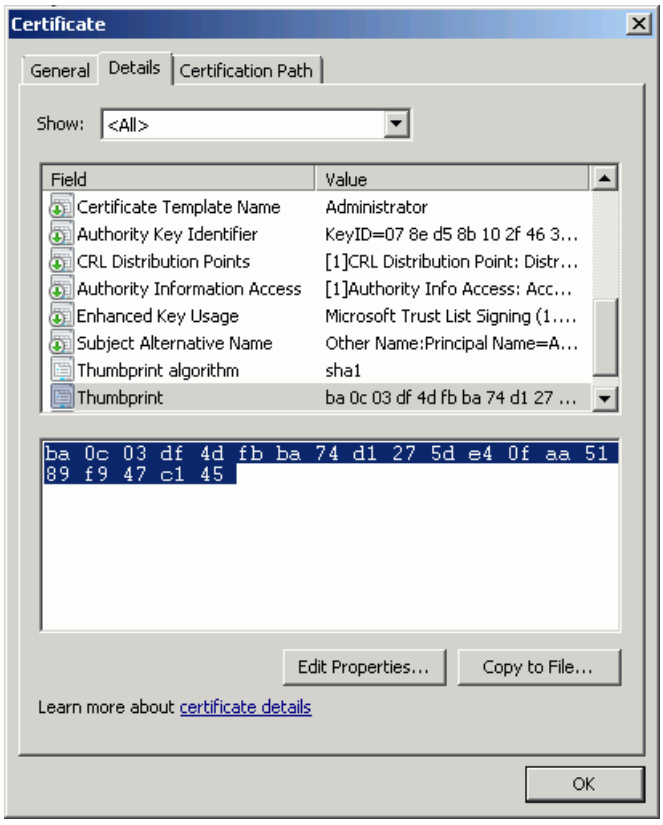
Configuring Capture Agents and Quick Connect services to use the custom certificate

After you import custom certificate, you must configure Capture Agents and Quick Connect services to use that certificate for encrypting/decrypting the password information that Capture Agent sends to Quick Connect service.

In Quick Connect, the certificates are identified with the *certificate thumbprint*. To retrieve the thumbprint of the imported certificate, use the following procedure.

To retrieve a certificate's thumbprint

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.
   *The **Certificate** dialog box opens.*
5. In the **Certificate** dialog box, click the **Details** tab, scroll through the list of fields, and then click Thumbprint.
   *The Thumbprint value (hexadecimal characters) is displayed in the box beneath the **Details** tab:*



6. Copy the hexadecimal characters from the box to Clipboard.
   You will use the certificate's thumbprint value for configuring Capture Agent and Quick Connect service.

Configuring Capture Agent

The procedure for configuring Capture Agent depends on the way used for specifying the Capture Agent parameters. After installing Capture Agent, you may specify the Capture Agent parameters using Group Policy or using the Windows Registry. For detailed information, refer to "Configuring Capture Agents" earlier in this paper.

If Capture Agent uses parameters specified using Group Policy, perform the following steps:

1. On any computer from a domain where Capture Agents are installed, open the Group Policy Object Editor console, and connect to the Group Policy object that defines the Capture Agent settings.

   For example, in the basic scenario, connect to the "Default Domain Group Policy" Group Policy object, while in the advanced scenario, connect to the GPO64 and GPO32 Group Policy objects. For detailed information, refer to "Configuring Capture Agents" earlier in this paper.

2. In the Group Policy Object Editor console, expand the Group Policy object to which you connected, expand the **Computer Configuration** node, click **Administrative Templates**, expand the **Administrative Templates\Quick Connect** node, and then click **Quick Connect Capture Agent Service**.
3. In the details pane, double-click **Certificate**.

   *The **Certificate Properties** dialog box opens.*

4. In the **Certificate Properties** dialog box, open the **Setting** tab, select the **Enabled** option, and then paste the certificate's thumbprint (see Step 6 of the procedure above) in the **Thumbprint** text box. When finished, click **OK**.
5. For changes to take effect, refresh the Group Policy settings, using the **GPupdate** command:
   - At the command prompt, type **GPupdate /force**

If Capture Agent uses parameters specified in the Windows Registry, perform the following steps:

1. On the domain controller running Capture Agent, start the Regedit.exe tool.

   Registry Editor opens.

2. Using Registry Editor, open the "HKLM\SOFTWARE\Quest Software\Quick Connect\CaptureAgentService\Certificate" registry key.
3. In the details pane, double-click the **FindValue** value, and then set this value to the certificate's thumbprint name (see the "To retrieve a certificate's thumbprint" procedure earlier in this document).

Configuring Quick Connect Service

After installing Quick Connect Sync Engine, you can optionally configure the Quick Connect service parameters related to the Passwords Synchronization feature.

The following table lists the Quick Connect service parameters.

PARAMETER	DESCRIPTION	DEFAULT VALUE
Set interval between attempts to reset password	Capture Agents send information on changes made to Active Directory user passwords to Quick Connect service. After receiving this information, Quick Connect service tries to reset passwords in target connected systems for which the passwords synchronization feature is enabled. This parameter determines the time interval (in minutes) between attempts to reset passwords in the target connected systems. If you do not specify the parameter value, the default value (10 minutes) is used.	10 minutes
Set service connection point update period	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. If you do not specify this parameter, the default value (60 minutes) is used.	60 minutes
Set certificate	This parameter specifies the thumbprint of the certificate used to encrypt the data transfer channel between Capture Agent service and Quick Connect service. The same certificate must be used for Capture Agent and Quick Connect Service. If you do not specify this parameter, the default built-in certificate will be used instead.	If this parameter is not set, a default built-in certificate will be used.

If you do not set these parameters, Quick Connect service will use default values listed in the Default Values column of the table.

You can set the Quick Connect service parameters in one of the following ways:

- Setting parameters using Group Policy
- Setting parameters in Windows Registry on the computer running Quick Connect service

To specify the Quick Connect service parameters using Group Policy

1. On the computer running Quick Connect service, start Group Policy Object Editor, and then connect to the "Local Computer Policy" Group Policy object.

   For information about how to open and use Group Policy Editor, refer to the Group Policy Editor documentation.

2. In the Group Policy Object Editor console, expand the **Local Computer Policy** node, expand the **Computer Configuration** node, and then click **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 delivered Administrative Template (the PasswordService.adm file).

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

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.

   ***Note**: The names of group policy settings correspond to names of the Quick Connect service parameters listed in the table above.*

6. For changes to take effect, refresh the Group Policy settings, using the **GPupdate** command:
   - At the command prompt, type **GPupdate /force**

To specify the Quick Connect service parameters in Windows Registry

1. On the computer running the Quick Connect service, start the Regedit.exe tool.

   Registry Editor opens.

2. Using Registry Editor, add the following registry keys:
   - HKLM\SOFTWARE\Quest Software\Quick Connect\PasswordService
   - HKLM\SOFTWARE\Quest Software\Quick Connect\PasswordService\Certificate
3. Under the newly created keys, add the entries listed in the following tables.

Under the **HKLM\SOFTWARE\Quest Software\Quick Connect\PasswordService** registry key, add the following entries:

ENTRY NAME	DATA TYPE	VALUE
FailedRequestSpreadTime	REG_DWORD	The time interval (in minutes) between attempts to reset passwords in the target connected systems.
ConnectionPointUpdateSpreadTime	REG_DWORD	The frequency of updates (in minutes) of the Quick Connect service connection point.

Under the **HKLM\SOFTWARE\Quest Software\Quick Connect\PasswordService\Certificate** registry key, add the following entries:

ENTRY NAME	DATA TYPE	VALUE
FindValue	REG_SZ	The thumbprint of the certificate used to encrypt the data transfer channel between Capture Agent service and Quick Connect service. For information about how to retrieve the certificate thumbprint, refer to "Configuring Capture Agents and Quick Connect services to use the custom certificate" earlier in this paper.

The values of parameters specified in Registry keys override values of the same parameters specified using Group Policy.

If you have specified parameters in Registry keys, setting those parameters with the use of Group Policy takes no effect.

Passwords Synchronization Settings for Connected Data Systems

Before configuring a passwords synchronization step for an external connected data system, you should first create a connection to that data system (see "Creating a Connection" earlier in this paper), and then specify appropriate settings on the **Password** tab of the **Connection Properties** panel. The **Password** tab depends on the connected data system category.

This section helps you configure settings available on the **Password** tab for various connected systems.

To open the Password tab

1. In the Quick Connect console, open the **Connections** tab.
2. Under **Connected systems**, click the connection to the connected system with which you want to synchronize passwords.

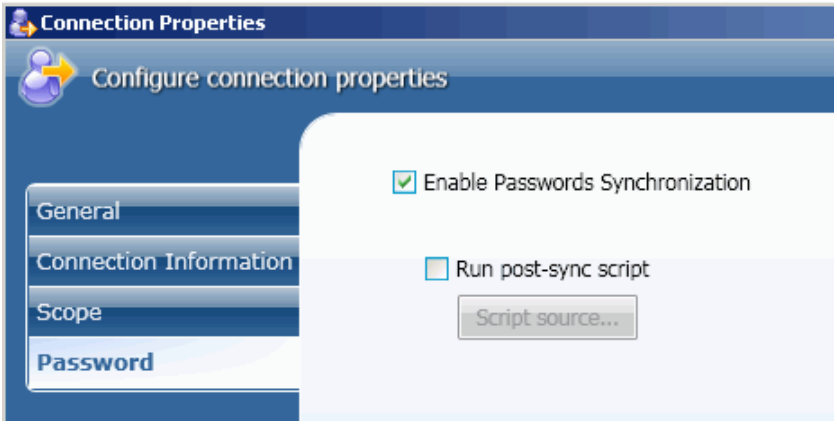
   *The **Connection Properties** panel opens.*
3. Click the **Password** tab.

The **Password** tab exists only for connections to external data systems for which the passwords synchronization feature is available.

To enable the passwords synchronization for a selected data system, ensure that on the **Password** tab, the **Enable Passwords Synchronization** check box is selected.

Connection to Active Directory, Sun One, Novell, SAP, Google Apps, and RACF

For connections to Active Directory, Sun One, Novell, SAP, Google Apps and IBM RACF data systems, the **Password** tab is similar to the following screen:



On this tab, you can enable or disable the passwords synchronization for this connection and optionally specify your custom PowerShell script to run after completing the passwords synchronization operation.

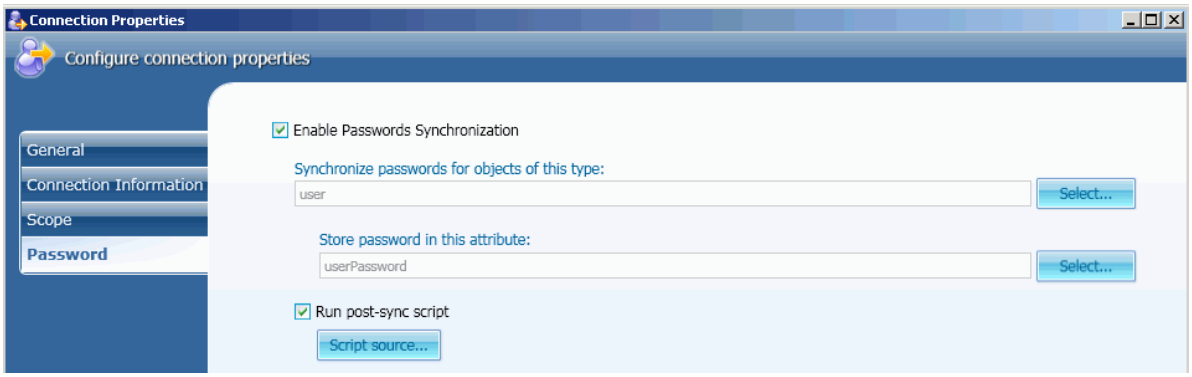
The elements of this tab are defined as follows:

- **Enable Passwords Synchronization**: Select this check box to enable the passwords synchronization for this Active Directory connection.
- **Run post-sync script**: Select this check box, and then click **Script source** to specify a Powershell script to run after completing the passwords synchronization for this connection.

  *Type the script text in the **Script Editor** dialog box that opens.*

Connection to LDAP Directory System

For connections to LDAP directory systems, the **Password** tab is similar to the following screen:



On this tab, you can enable or disable the passwords synchronization for this connection, specify the type of objects in the LDAP system for which you want to synchronize the passwords and the object attribute that will store the object password. Optionally, you can specify your custom PowerShell script to run after completing the passwords synchronization operation.

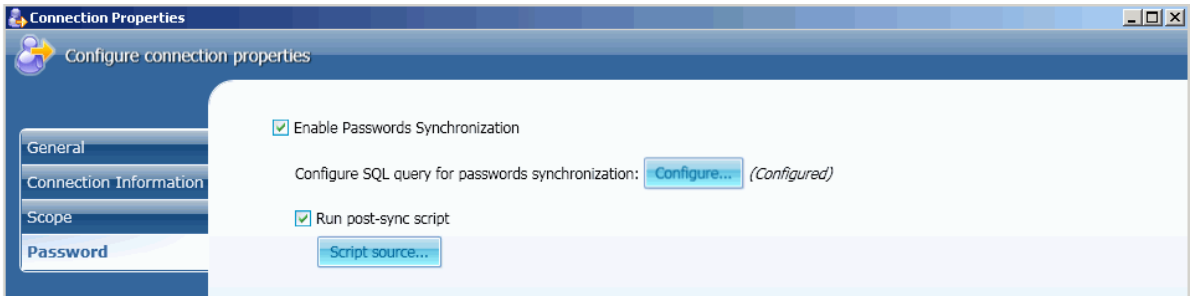
The elements of this tab are defined as follows:

- **Enable Password Synchronization**: Select this check box to enable the passwords synchronization for this LDAP connection.
- **Synchronize passwords for objects of this type**: Click **Select** next to this text box, and then use the **Select Object Type** dialog box to specify the type of objects that will participate in the passwords synchronization.
- **Store password in this attribute**: Click **Select** next to this text box, and then use the **Select Object Attribute** dialog box to specify the object attribute that will contain the password.
- **Run post-sync script**: Select this check box and then click **Script source** to specify a Powershell script to run after completing the passwords synchronization for this connection.

  *Type the script text in the **Script Editor** dialog box that opens.*

Connection to SQL, Oracle Data Systems

For connections to SQL and Oracle data systems, the **Password** tab is similar to the following screen:



On this tab, you can enable or disable the passwords synchronization for this connection, specify a SQL query used to set password in the target connected data system, and optionally, specify your custom PowerShell script to run after completing the passwords synchronization operation.

The elements of this tab are defined as follows:

- **Enable Password Synchronization**: Select this check box to enable the passwords synchronization for this LDAP connection.
- **Configure SQL query for passwords synchronization**: Click **Configure**, and then in the **Query Editor** dialog box that opens, specify your custom SQL query used to synchronize passwords between Active Directory users and their counterparts on SQL Server. For a sample query, see "Sample SQL Queries" below.
- **Run post-sync script**: Select this check box and then click **Script source** to specify a Powershell script to run after completing the passwords synchronization for this connection.

  *Type the script text in the **Script Editor** dialog box that opens.*

Sample SQL Queries

The following sample SQL queries can be used to synchronize passwords between Active Directory and a SQL or Oracle data system, respectively.

SQL Data System

Suppose that you have configured a connection to a SQL Server using the following SQL query for selection of SQL Server data:

```
select * from sys.server_principals
```

The SQL query for selection of data must be specified on the **Connection Information** tab of the **Connection Properties** panel for connection to SQL Server. For more information, refer to "Configuring Connection to SQL Server" later in this document.

In this scenario, you can use the following query for passwords synchronization:

```
EXEC sp_password null, @newPassword, @name
```

Oracle Data System

Suppose that you have configured a connection to an Oracle database using the following SQL query for selection of data:

```
select * from all_users
```

The SQL query for selection of data must be specified on the **Connection Information** tab of the **Connection Properties** panel for connection to Oracle Database. For more information, refer to "Configuring Connection to Oracle Database" later in this document.

In this scenario, you can use the following SQL query for passwords synchronization:

```
call  dbms_utility.exec_ddl_statement('ALTER USER ' || :USERNAME || ' IDENTIFIED BY ' ||
:newPassword)
```

In this query: the *USERNAME* refers to the name of attribute that uniquely identifies an object in the Oracle database; the *newPassword* refers to the name of attribute that stores the password.

Running Post-Sync Scripts

Optionally, on the **Password** tab, you can specify a PowerShell script that will start after completing the passwords synchronization operation.

To specify a post-sync script

1. In the Quick Connect console, open the **Connections** tab.
2. Under **Connected systems**, click the target connection system for which the passwords synchronization feature is available.

   *The **Connection Properties** panel opens.*
3. In the **Connection Properties** panel, open the **Password** tab, select the **Run post-sync script** check box, and then click **Script Source**.

   *The **Script Editor** window opens.*
4. In the **Script Editor** window, type the script text, and then click OK.

Sample Script

This sample PowerShell script implements the following scenario: after completing the passwords synchronization operation, the script sends a notification e-mail message that informs an administrator about resetting password for an object in the target connected system. The message contains the names of Active Directory object and its counterpart in the target connected system.

```
#---- 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)
```

For more information about the use of PowerShell for development of scripts related to Quick Connect, refer to ActiveRoles Quick Connect - SDK.

Configuring Passwords Synchronization Steps

In Quick Connect, the passwords synchronization operation between Active Directory users and objects in a target connected system is referred to as a *passwords synchronization step*.

Quick Connect Sync Engine provides for the Add Passwords Synchronization Step wizard that helps you configure the passwords synchronization step.

You can add a new passwords synchronization step for an existing source data system or you can modify settings of existing passwords synchronization steps.

To add a new passwords synchronization step

1. In the Quick Connect console, open the **Sync Passwords** tab.
2. Under **Select source system from which to synchronize**, click an existing source data system for passwords synchronization
   -- OR --
   click the **Click to add new source system** link, complete the Add Connected System wizard that starts (see "Creating a Connection" earlier in this paper), and then click a newly added source data system.
3. Under **Synchronization Step**, click **Click to add a new passwords synchronization step**.

   The Add Password Synchronization Step wizard starts.
4. On the **Specify synchronization source** page, click **Select**, and then complete the **Select Object Type** dialog box that opens. When finished, click **Next**.
5. On the **Specify the synchronization target** page, do the following and then click **Finish**:
   - Click **Specify**, and then complete the Add Connected System wizard that starts to specify the target connected system for passwords synchronization.
   - Click **Select**, and then use the **Select Object Type** dialog box that opens to specify the type of objects in the target connected data system with which to synchronize the passwords.
   - Optionally, click **Set Synchronization Options**, and then complete the **Synchronization Options** dialog box that opens. For details, see "Setting Passwords Synchronization Options" later in this paper.

To modify settings of an existing passwords synchronization step

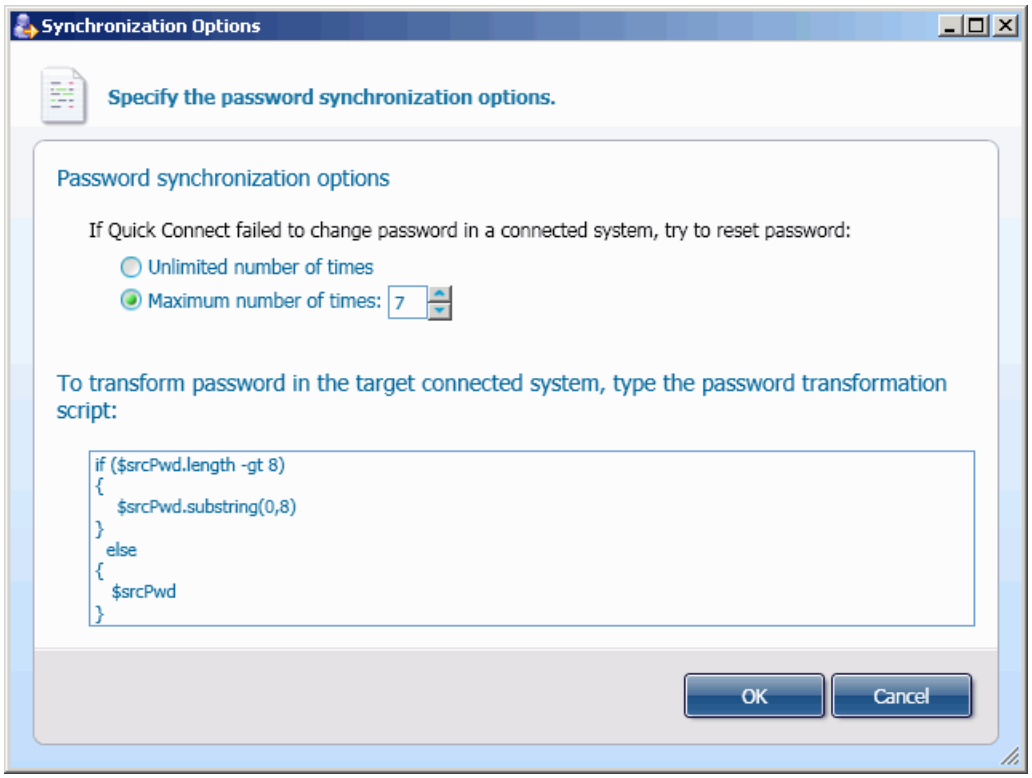
1. In the Quick Connect console, open the **Sync Passwords** tab.
2. Under **Select source system from which to synchronize**, click an existed source data system.
3. Under **Synchronization Step**, click the existing passwords synchronization step you want to modify.

   *The **Passwords synchronization step properties** panel opens.*

4. In the **Passwords synchronization step properties** panel, open the **Target** tab.
5. Click **Set Synchronization Options**, and then complete the **Synchronization Options** dialog box that opens. For details, see "Setting Passwords Synchronization Options" below.

Setting Passwords Synchronization Options

To set passwords synchronization options, complete the **Synchronization Options** dialog box similar to the following screen:



The elements of this dialog box are defined as follows:

- **Unlimited number of times**: Select this option to allow Quick Connect Sync Engine to reset passwords in the target data system unlimited number of times.
- **Maximum number of times**: Select this option, and then specify a maximum number of attempts to reset passwords in the target data system
- **To transform password in the target connected system, type the password transformation script**: Provides a space for you to type your custom PowerShell script that will build passwords in the target connected system. For more information and sample scripts, refer to "Developing PowerShell Scripts for Passwords Synchronization Steps" in Quest Quick Connect - SDK.

  Important: If you do not want to transform passwords, leave this area cleared.

How It Works?

Once you have properly configured the passwords synchronization, this feature functions automatically and no operator intervention is required.

Each time you changed a user password in a source data system, Quick Connect Capture Agents track this change and sends the changed password to Quick Connect service(s) specified in the Capture Agent settings. Basing on this information Quick Connect service resets the user passwords in all target connected systems specified in the passwords synchronization steps configured for the source data system.

Capture Agent uses encrypted channels to send passwords from the source domain controllers to Quick Connect service. To encrypt channels, you can use a built-in certificate or you can configure Capture Agent to use your custom certificate. For more information, refer to "Using Certificates" earlier in this document.

Using the QCconfig Command-line Tool

Quick Connect provides for the command-line tool designed to configure parameters that Quick Connect Sync Engine uses for accessing SQL Server and ActiveRoles Administration service. The command-line tool is the QuickConnectServerHost.exe executable file that defines the command-line parameters.

To run the QCconfig command-line tool

1. Switch to the "[Program Files]\Quest Software\ActiveRoles Quick Connect\Service" folder.
2. At the Command Prompt, run the QuickConnectServerHost.exe file by specifying the required parameters. The command syntax is described below.

Syntax

```
QuickConnectServerHost.exe /DBSERVERNAME <DBSERVERNAME> /DBNAME_CONFIGURATION
<DBNAME_CONFIGURATION> /DBNAME_EXECUTIONDATA <DBNAME_EXECUTIONDATA>
/DBAUTHENTICATIONMODE <0 | 1> /DBLOGIN <DBLOGIN> /DBPASSWORD <DBPASSWORD> /ARSSERVERNAME
<ARSSERVERNAME> /ARSLOGIN <ARSLOGIN> /ARSPASSWORD <ARSPASSWORD>
```

Parameters

PARAMETER	DESCRIPTION
DBSERVERNAME	The name of SQL Server to connect to in the form: <*Computer*>\<*Instance*> (for named instance) or <*Computer*> (for default instance).
DBNAME_CONFIGURATION	The name of the SQL database for storing the application configuration data (default name is QC40Configuration).
DBNAME_EXECUTIONDATA	The name of the SQL database for storing temporary data (default name is QC40ExecutionData).
DBAUTHENTICATIONMODE	The authentication mode the Quick Connect service uses for connection to SQL Server. Specify one of these values: • "0" - SQL authentication mode • "1" - Windows authentication mode
DBLOGIN	SQL Server login for connection to SQL Server. **Important:** This parameter is used only for the SQL authentication mode.
DBPASSWORD	Password for SQL Server login. **Important:** This parameter is used only for the SQL authentication mode.
ARSSERVERNAME	The fully qualified DNS name of the computer running the ActiveRoles Administration service to connect to.
ARSLOGIN	The user logon name of the account the Quick Connect service uses for connection to ActiveRoles Administration service.
ARSPASSWORD	Password for the user logon name specified in ARSLOGIN.

You can set separately the parameters for accessing SQL Server and ActiveRoles Administration service. For example, if you want to change only the SQL Server access parameters, you must specify all DB* parameters. In this case, the ARS*parameters are optional.

Scenario: Change Credentials for Connection to SQL Server

This scenario explains how to use the QCconfig command-line tool to reconfigure Quick Connect Sync Engine to use a different login and password or a different authentication mode for connection to SQL Server.

When installing Quick Connect Sync Engine, you configure how Quick Connect Service connects to the SQL Server instance that maintains the application configuration database. Suppose that the login used for connection to SQL Server is deleted, has the password modified, or no longer belongs to the **sysadmin** fixed role at the SQL Server instance. In this case, you should reconfigure Quick Connect Sync Engine to use a different login and password.

The key aspects of the scenario are as follows:

- Assume that Quick Connect Sync Engine is connected to the default instance of SQL Server running on the *mySQL.mycompany.com* computer.
- Assume that you do not change default names for the application configuration database and for the database used for storing temporary data (*QC40Configuration* and *QC40ExecutionData*, respectively).
- Also assume that you want Quick Connect Sync Engine to use the "*sb*" login and the "*iYght6U08*" password " to access SQL Server.

To implement this scenario, perform these steps:

1. Switch to the "[Program Files]\Quest Software\ActiveRoles Quick Connect\Service" folder.

   A typical path is as follows: C:\Program Files\Quest Software\ActiveRoles Quick Connect\Service
2. At the command prompt, type the following syntax, and then press ENTER:

```
QuickConnectServerHost.exe /DBSERVERNAME mySQL.mycompany.com /DBNAME_CONFIGURATION
QC40Configuration /DBNAME_EXECUTIONDATA QC40ExecutionData /DBAUTHENTICATIONMODE 0
/DBLOGIN sb /DBPASSWORD iYght6U08
```

3. For changes to take effect, restart the *Quest Quick Connect* service with Services tool provided by Windows System Tools.

4

Configuring Connections to External Data Systems

- About External Data Systems
- Configuring Connection to Delimited Text File
- Configuring Connection to LDAP Directory Service
- Configuring Connection to SQL Server
- Configuring Connection to Sun One Directory Server
- Configuring Connection to Oracle Database
- Configuring Connection to Novell Directory Service
- Configuring Connection to IBM RACF
- Configuring Connection to Lotus Domino Server
- Configuring Connection to Google Apps Service
- Configuring Connection to SAP System
- Configuring Connection to PeopleSoft System

About External Data Systems

Along with connectors to Active Directory and AD LDS (ADAM) installed with the core module of Quick Connect - *Quick Connect Sync Engine*, you can install and configure additional connectors to specific external data systems.

This section details procedures for configuring connections to specific external data systems using the Add Connected System wizard. For information about how to run the wizard, refer to "Configuring Connections" earlier in this paper.

To install connectors described in this section, you need to obtain a license from Quest Software. For details, refer to "Licensing" earlier in this paper.

When configuring a connection to an external data system, the data system must be up and running, otherwise the configure operation will fail.

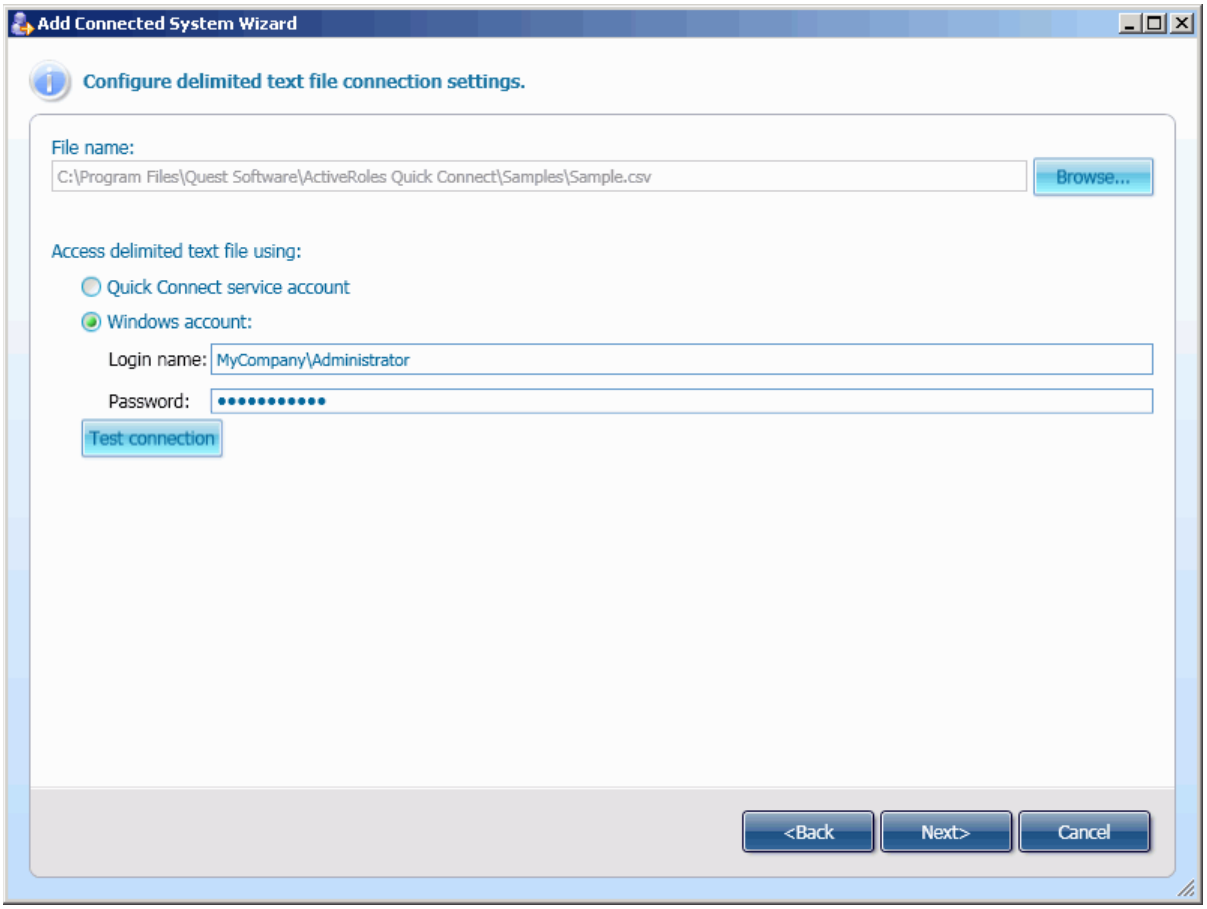
In this release of Quick Connect, the following categories of data systems are supported:

- Delimited text file
- LDAP Directory service
- Microsoft SQL Server
- Sun One Directory server
- Relational databases accessed with an OLE DB provider
- Oracle database
- Novell Directory service
- IBM RACF
- Lotus Domino Server
- Google Apps service
- SAP system
- PeopleSoft system

Configuring Connection to Delimited Text File

When establishing a connection to a DTF, the wizard prompts you to complete the **Configure delimited text file connection settings** and the **Confirm delimited text file format** pages.

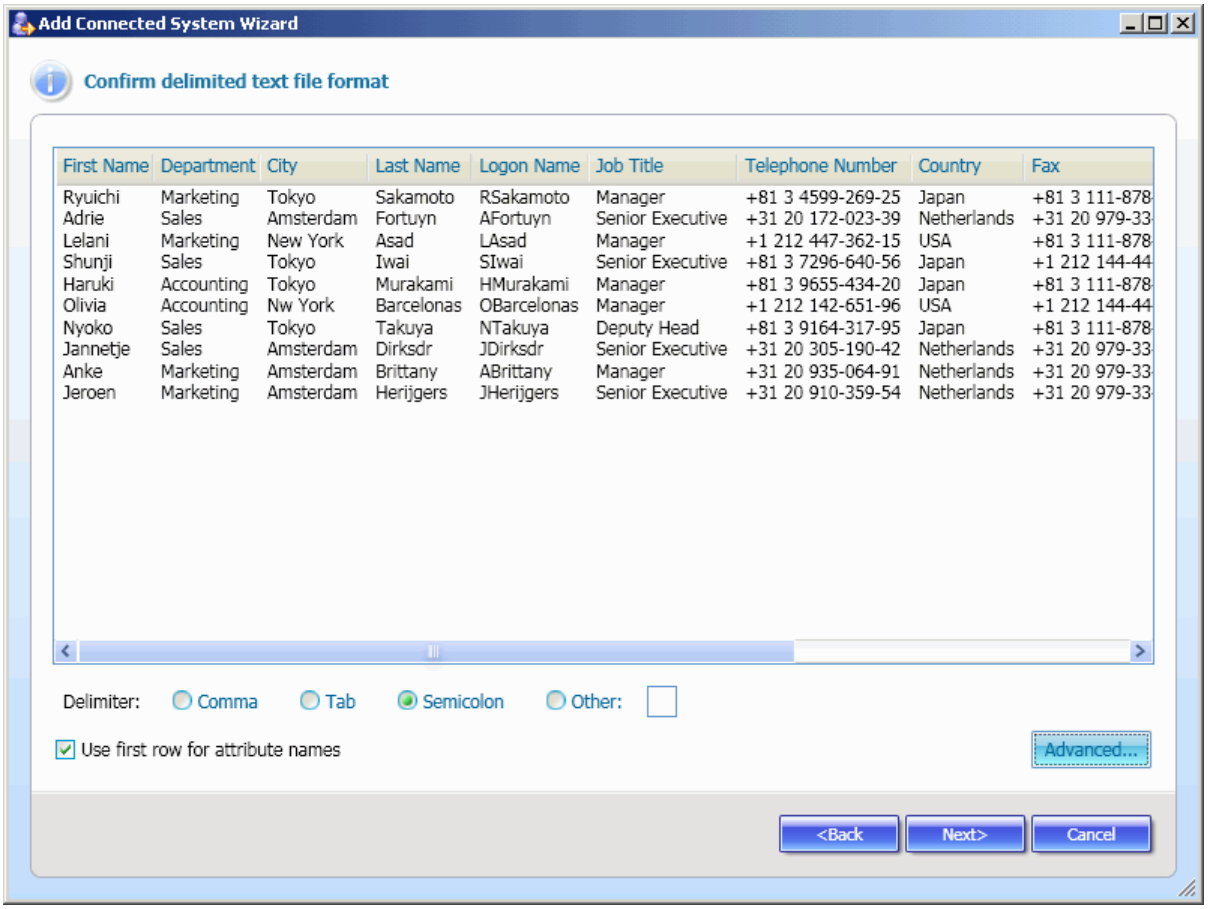
The **Configure delimited text file connection settings** page allows you to specify a delimited text file and an account under which the application will access the file. This page is similar to the following screen:



On this page, do the following:

1. Click **Browse**, and then select the DT file with the **Open** dialog box.
2. Under **Access delimited text file using**, do one of the following:
   - Select the **Quick Connect service account** option to have Quick Connect Sync Engine to access the specified DT file in the security context of the Quick Connect service account.
   - Select the **Windows account** option and then specify the login name and password of the user account under which the application will access the DT file.
3. Optionally, click **Test connection** to attempt a connection to the specified DT file. If the connection fails, ensure that the settings are correct.
4. Click **Next** to proceed to the **Confirm delimited text file format** page.

The **Confirm delimited text file format** page allows you to confirm the file format and optionally, specify the data delimiter. This page is similar to the following screen:



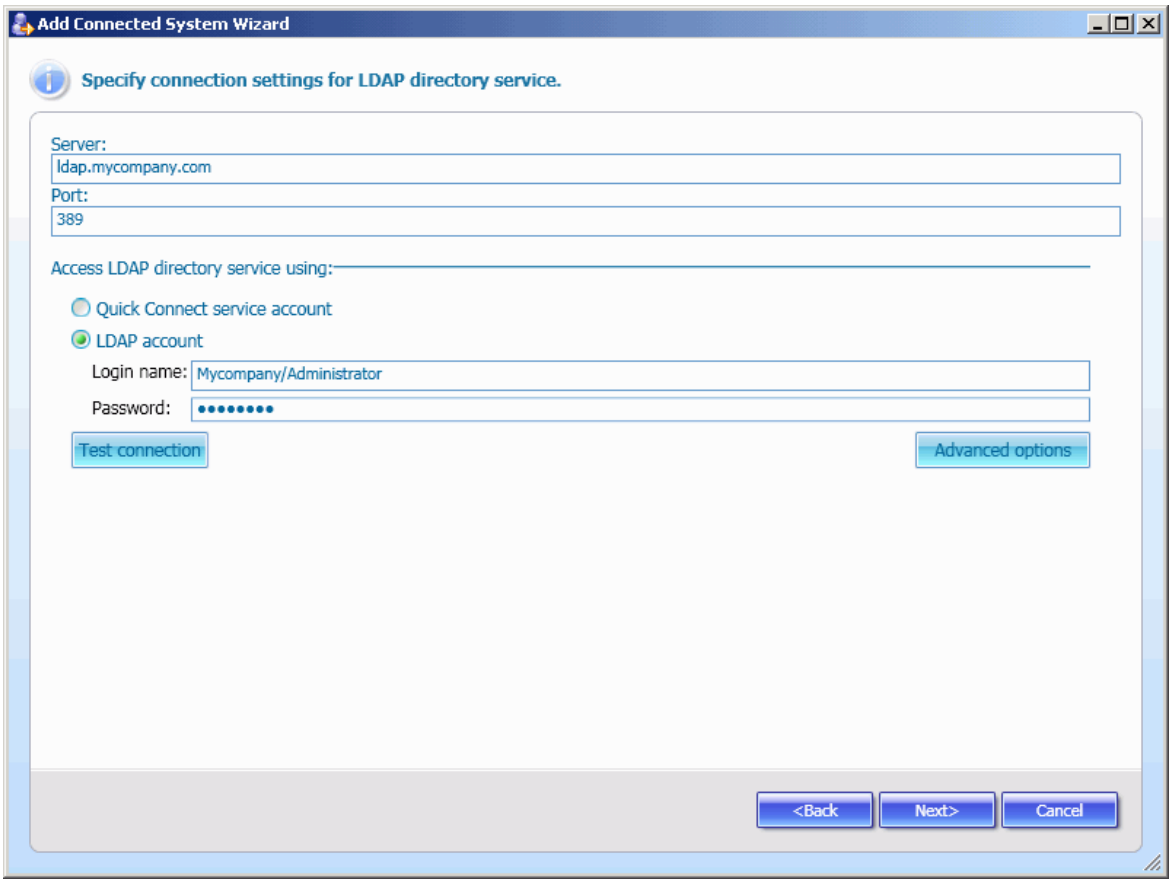
On this page, do the following:

1. Set delimiter for the selected DT file. To do this, select one of the following delimiters: **Comma**, **Tab**, **Semicolon**
   -- OR --
   to set your custom delimiter, click **Other,** and then type the delimiter in the text box next to **Other**.
2. If the first line of the DT file contains the attributes names, select the **Use first row for attribute names** check box. Otherwise, leave this check box cleared.
3. Optionally, click **Advanced** to specify advanced options for the delimited text file, such as the page encoding.
4. Click **Next**, and follow the provided instructions to complete the wizard.

Configuring Connection to LDAP Directory Service

When establishing a connection to an LDAP directory service, the wizard prompts you to complete the **Specify connection settings for LDAP directory service** and the **Specify directory partitions that will participate in synchronization process** pages.

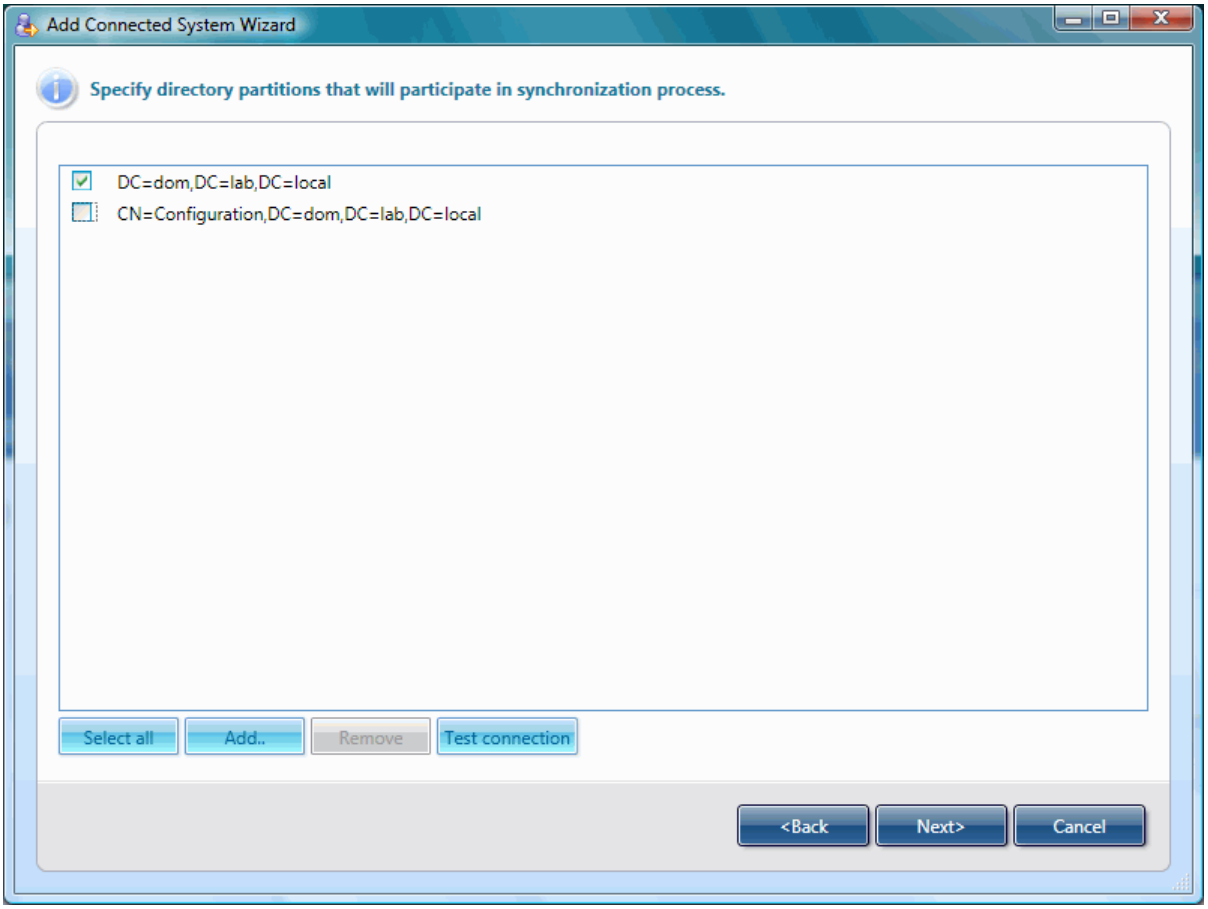
On the **Specify connection settings for LDAP directory service** page, you can specify the LDAP service to connect and an account under which the application will access the LDAP service. This page is similar to the following screen:



On this page, do the following:

1. In the **Server** text box, type the fully qualified DNS name of the computer running the service.
2. In the **Port** text box, type the LDAP communication port number in use by the service.
3. Under **Access LDAP directory service using**, do one of the following:
   - Select the **Quick Connect service account** option to have Quick Connect Sync Engine to access the LDAP directory service in the security context of the Quick Connect service account.
   - Select the **LDAP account** option and then specify the login name and password of the user account under which the application will access the LDAP directory service.
4. Optionally, click **Advanced options** to specify advanced options to access the service.
5. To proceed to the **Specify directory partitions that will participate in synchronization process** page, click **Next**

On the **Specify directory partitions that will participate in synchronization process** page, select check boxes next to the names of directory partitions in the LDAP connected system you want to participate in the synchronization process. This page is similar to the following screen:



You can modify the list of directory partitions displayed on this page, using the **Add** or **Remove** button.

After you complete this page, click **Next** and follow the provided instructions to complete the Add Connected System wizard.

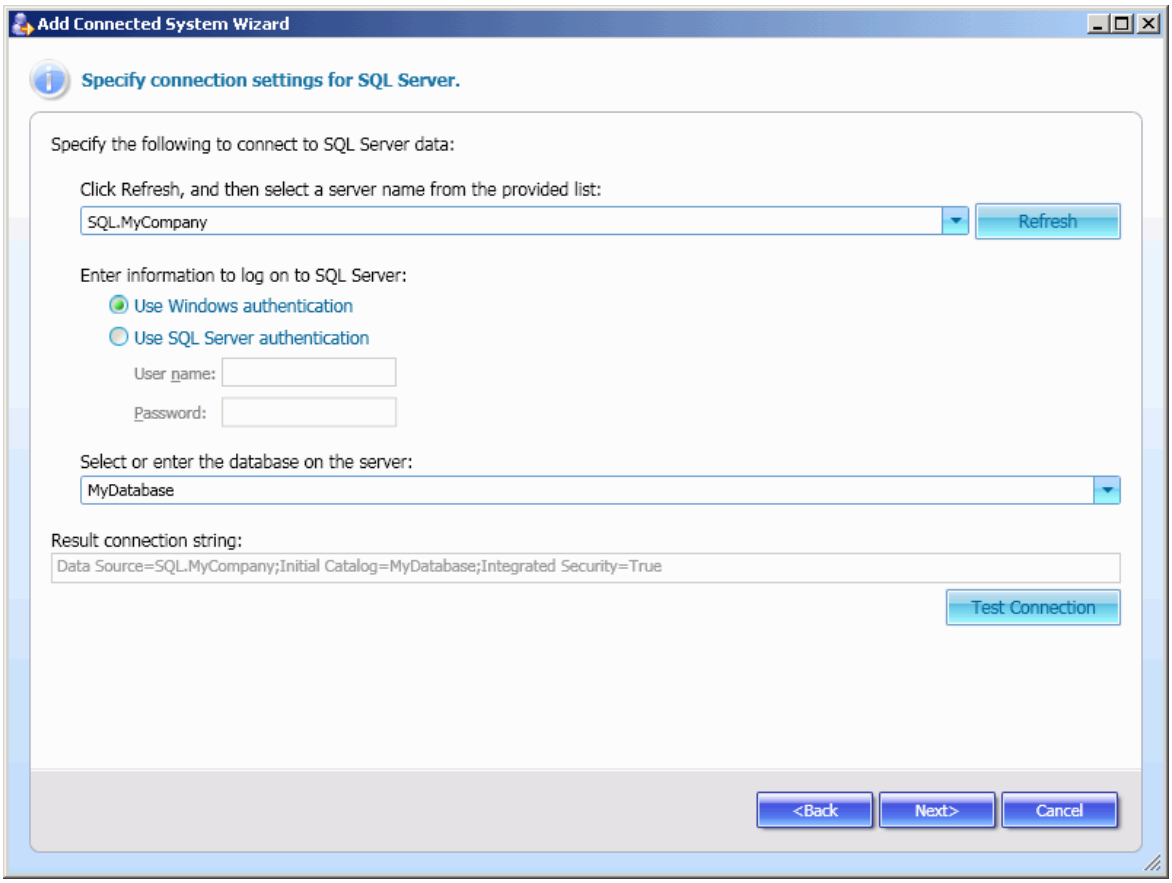
Note: Every object in a connected system has a naming attribute from which the object name is formed. By default, after you create a connection to an LDAP directory service, the naming attribute for all object classes is "uid."
Optionally, you can change the naming attribute for specified object classes by performing the following steps:

1. In the ActiveRoles Quick Connect Administration Console, open the **Connections** tab, and then under **Connected Systems**, click the created connection to an LDAP directory service.
2. In the **Connection Properties** dialog box that opens, click **Connection Information**, and then expand **Naming Attributes**.
3. Using the **Add**, **Edit** and **Remove** buttons, redefine the naming attributes for the desired object classes
4. When finished, click **OK** to apply the changes and close the **Connection Properties** dialog box.

Configuring Connection to SQL Server

When establishing a connection to SQL server, the wizard prompts you to complete the **Specify connection settings for SQL Server** and the **Specify how to select data from SQL Server database** pages.

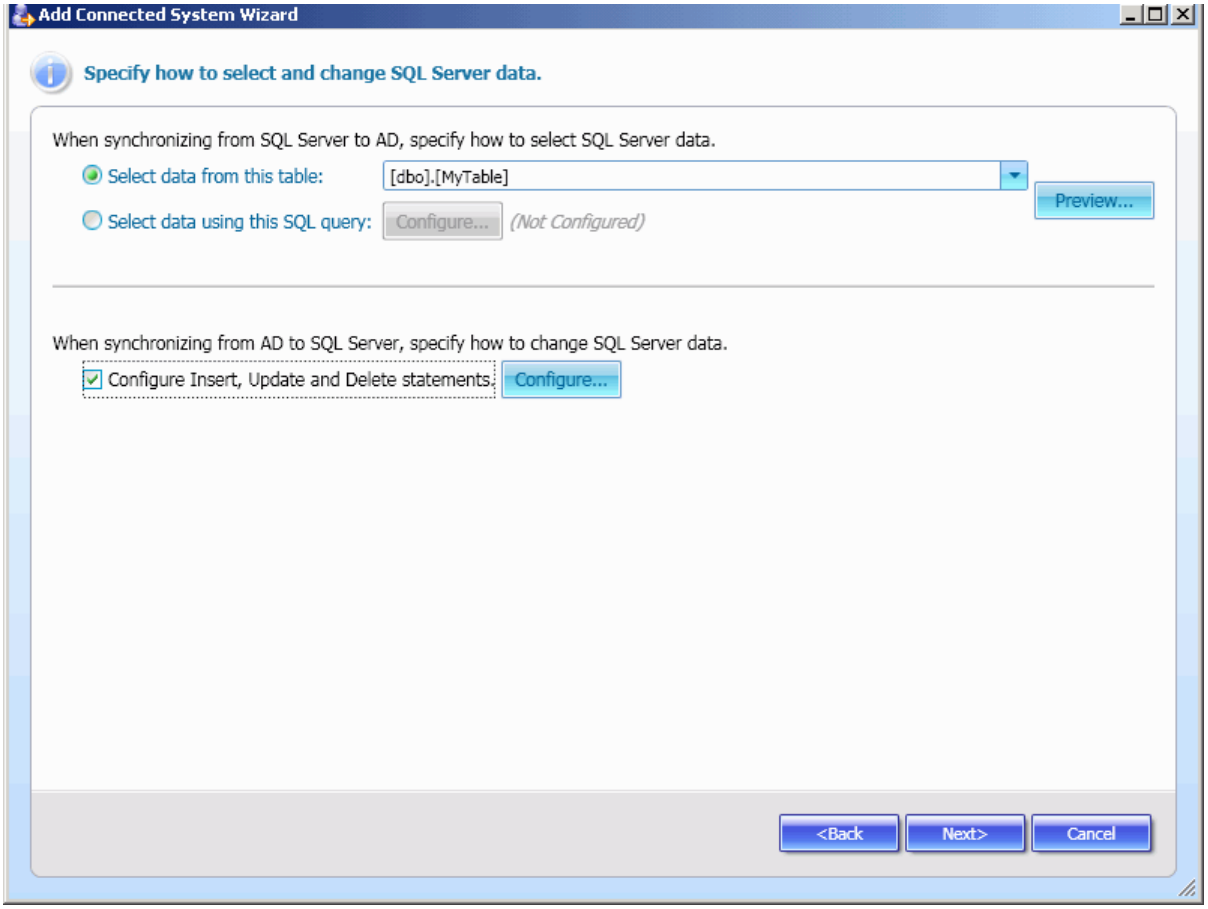
On the **Specify connection settings for SQL Server** page, you can specify a SQL server to connect, a database on the server with which to synchronize, and an information to log on to SQL server. This page is similar to the following screen:



On this page, do the following:

1. Click **Refresh**, and then select a server name from the provided list.
2. Under **Enter information to log on to SQL Server**, select **Use Windows authentication** to access SQL Server using the Quick Connect service account
   -- OR --
   select **Use SQL Server authentication** to use a supplied user name and password to authenticate your logon information to SQL Server data.
3. Under **Select or enter the database name on the server,** click the arrow to select the database name from the provided list or type the database name in the text box.
4. Optionally, click **Test connection** to attempt a connection to the specified data source.
   If the connection fails, ensure that the settings are correct.
5. Click **Next** to proceed to the **Specify how to select data from SQL Server database** page.

On the **Specify how to select and change SQL Server database** page, you can specify a set of SQL Server tables and columns in those tables that can participate in a synchronization process. You can also specify how Quick Connect will change SQL Server data when synchronizing from Active Directory to SQL Server. This page is similar to the following screen:



On this page, do the following:

1. To let Quick Connect synchronize with all columns of a specified table, select **Select data from this table,** click the arrow, and then select the table from the provided list
   -- OR --
   In advanced scenarios (for example, to let Quick Connect synchronize with data from several tables), select **Select data using this SQL query**, click **Configure**, and then type the appropriate SQL query in the **Query Editor** dialog box that opens.
2. If you plan to synchronize from Active Directory to SQL Server, select the **Configure Insert, Update and Delete statements** check box, click **Configure**, and then specify the Insert, Update and Delete SQL statements using the **Configure SQL Statements** dialog box that opens. For details and sample queries, refer to "Specifying SQL Queries" later in this paper.
3. Click **Next,** and follow the provided instructions to complete the wizard.

Specifying SQL Queries

This section explains how to create SQL queries used to specify how to change the SQL Server data when synchronizing from Active Directory to SQL Server.

In all sample queries, **Id** refers to an attribute (a column name in an SQL Server table) that uniquely identifies an object in your SQL database.

These examples can be used only for configuring connectors to Microsoft SQL Server 2005.

How to Insert an Object into a Table

This sample illustrates how to create a query that inserts an object with specified attributes into the table SQLConnTest1. The table has the following structure: *CREATE TABLE [SQLConnTest1]([Id] [bigint] IDENTITY(1,1),[attr1] [nchar](64),[attr2] [nchar](64)))*.

Insert the following SQL query into the **Configure SQL Statements** dialog box:

```
INSERT into SQLConnTest1(Id) values(@Id)
```

How to Create a SQL Server Account

This sample illustrates how to create a SQL Server account, and then retrieve the UniqueID attribute for that account.

To define the scope where to create the SQL Server account, insert the following query in the **Query Editor** dialog box:

```
SELECT sid as Id,name as login from sys.server_principals
```

Insert the following SQL query into the **Configure SQL Statements** dialog box:

```
EXEC sp_addlogin @login, @newPassword;
EXEC sp_adduser @login,@login,'db_owner';
SELECT sid as Id from sys.server_principals where name=@login;
```

The names of attributes (i.e. column name in SQL Server table) used in SQL queries cannot contain space characters. For example, you cannot use names such as "user password."

Configuring Connection to OLE DB Provider

This section describes steps to configure a connection to a database using an OLE DB provider with the use of the Add Connected System wizard.

You can configure connections only to relational databases.

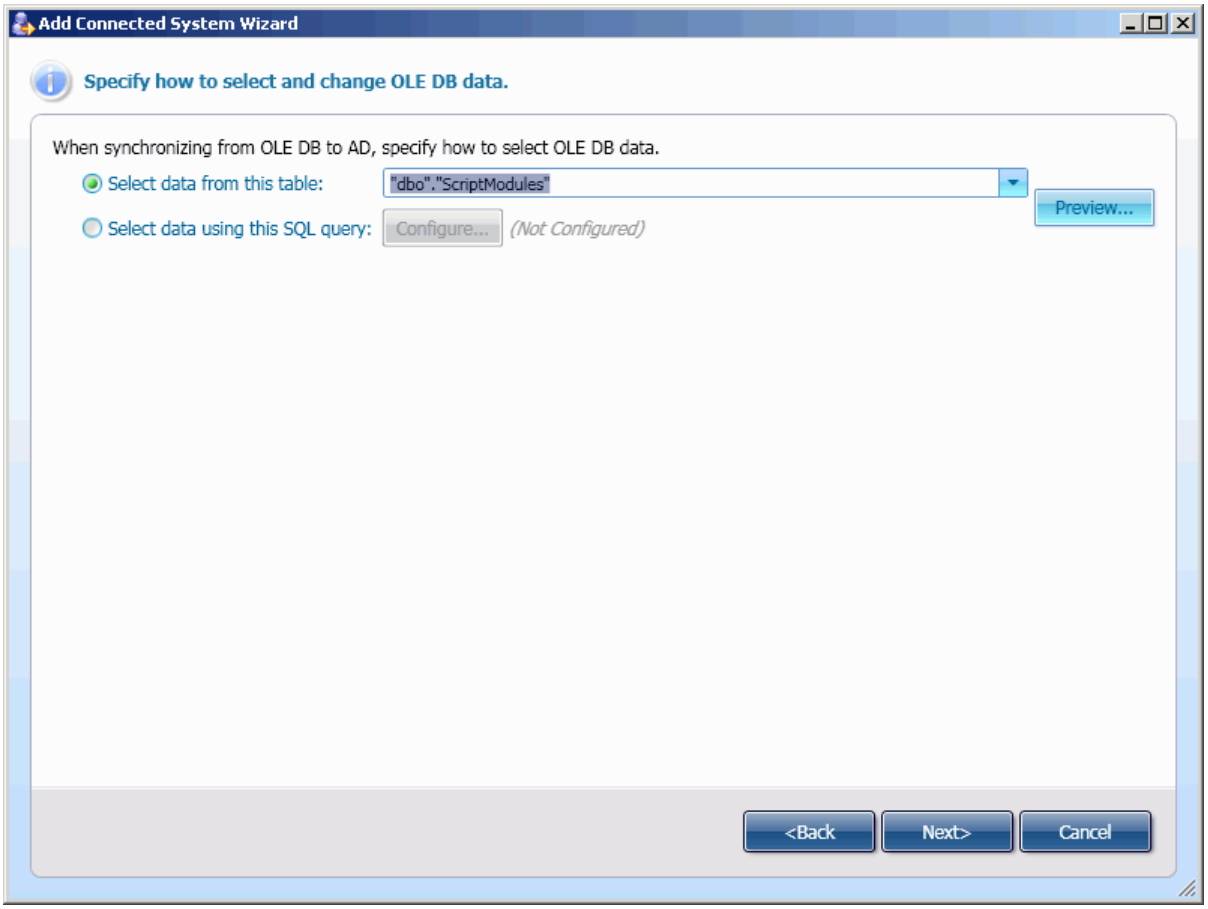
The wizard prompts you to complete the **Select OLE DB provider for the type of data to access and specify required connection settings** and **How to select and change OLE DB data** pages.

The **Select OLE DB provider for the type of data to access and specify required connection settings** page allows you to build OLE DB connection string with the use of Microsoft Data Link.

Steps to complete the **Select OLE DB provider for the type of data to access and specify required connection settings** page:

1. Click **Configure**.
   *The **Data Link Properties** property sheet opens.*
2. In **Data Link Properties**, click the **Provider** tab, and then select the appropriate OLE DB provider for your database from the provided list.
3. Click the **Connection** tab that depends on the type of the database to access. Follow the provided instructions to complete the **Connection** tab. For more information, click **Help**.
4. Optionally, complete the **Advanced** and **All** tabs. When finished, click **OK** to close the **DataLink Properties** property sheet.
5. Click **Next**, to proceed to the **How to select and change OLE DB data** page.

On the **How to select and change OLE DB data** page, you can specify a set of database tables and columns in those tables that can participate in a synchronization process. You can also specify how Quick Connect will change data in the connected database when synchronizing from Active Directory to the connected database. This page is similar to the following screen:



On this page, do the following:

1. To let Quick Connect synchronize with all columns of a specified table, select **Select data from this table,** click the arrow, and then select the table from the provided list
   -- OR --
   In advanced scenarios (for example, to let Quick Connect synchronize with data from several tables), select **Select data using this SQL query**, click **Configure**, and then type the appropriate SQL query in the **Query Editor** dialog box that opens.
2. Click **Next,** and follow the provided instructions to complete the wizard.

Configuring Connection to Sun One Directory Server

This section describes steps to configure a connection to a Sun One directory Server using the Add Connected System wizard.

The wizard prompts you to complete the **Specify connection settings for Sun One Directory Server** page. This page is similar to the **Specify connection settings for AD LDS (ADAM)** page displayed when configuring connection to ADAM (see "**Configuring Connection to AD LDS (ADAM)**" earlier in this paper).

Steps to complete the **Specify connection settings for Sun One Directory Server** page:

1. In the **Server** text box, type the fully qualified DNS name (for example, sun.mycompany.com) of the computer running the server.
2. In the **Port** text box, type the Lightweight Directory Access Protocol (LDAP) communication port number in use by the server.
3. Optionally, click **Advanced** to specify advanced options to access the server.
4. Under **Access Sun One Directory Server using**, specify the login name and password of the user account under which the application will access Sun One directory server.
5. Optionally, click **Test connection** to attempt a connection to the specified Sun One Directory Server. If the connection fails, ensure that the settings are correct.
6. Click **Next**, and follow the provided instructions to complete the wizard.

Configuring Connection to Oracle Database

This section describes steps to configure a connection to an Oracle database using the Add Connected System wizard.

The wizard prompts you to complete the **Specify settings for connection to Oracle Server** and **Specify how to select data from Oracle database** pages. These pages are similar to pages used to configure a connection to SQL Server (see "Configuring Connection to SQL Server" earlier in this paper).

You can configure connections only to Oracle Database 8g or later.

Steps to complete the **Specify settings for connection to Oracle Server** page:

1. Under **Select or enter an Oracle service name**, type the Oracle service name or select it from the provided list. Refresh the list by clicking **Refresh.**
2. Under **Enter information to log on to Oracle Server**, specify the login name and password of the user account under which the application will access the Oracle service.
3. Optionally, click **Test connection** to attempt a connection to the specified Oracle service.

   If the connection fails, ensure that the settings are correct. For example, spelling errors and case sensitivity can cause failed connections.
4. Click **Next** to proceed to the **Specify how to select data from Oracle database** page.

Steps to complete the **Specify how to select data from Oracle database** page:

1. To cause Quick Connect to select data from the specified table, select S**elect data from this table**, click the arrow, and then select the table from the provided list
   -- OR --
   To cause Quick Connect to select data using a specified query, select **Select data using this SQL query**, click **Configure**, and then type the SQL query in the **Query Editor** dialog box that opens.
2. When synchronizing from Active Directory to Oracle, select the **Configure Insert, Update and Delete statements** check box, click **Configure**, and then specify the Insert, Update and Delete SQL statements using the **Configure SQL Statements** dialog box that opens.
   See "Sample SQL Query" later in this paper.
3. Click **Next**, and follow the provided instructions to complete the wizard.

Sample SQL Query

This section provides a sample SQL query that illustrates how to create an object with specified attributes in your Oracle database when provisioning from Active Directory to Oracle. The query inserts the newly created object into the table SQLConnTest1. The table has the following structure: *CREATE TABLE "SQLConnTest1"("Id" number,"attr1" nchar(64), "attr2" nchar(64))*.

In this sample, Id refers to an attribute that uniquely identifies an object in your Oracle database.

Insert the following SQL query into the Configure SQL Statements dialog box:

```
Insert into SQLConnTest1(attr1) values(@attr1) returning Id into :Id
```

Configuring Connection to Novell Directory Service

This section describes steps to configure a connection to Novell Directory Service using the Add Connected System wizard.

The wizard prompts you to complete the **Specify connection settings for Novell Directory Service** page. This page is similar to the **Specify connection settings for AD LDS (ADAM)** page displayed when configuring connection to ADAM (see "Configuring Connection to AD LDS (ADAM)" earlier in this paper).

Steps to complete the **Specify connection settings for Novell Directory Service** page:

1. In the **Server** text box, type the fully qualified DNS name (for example, novell.mycompany.com) of the computer running the Novell Directory Service.
2. In the **Port** text box, type the Lightweight Directory Access Protocol (LDAP) communication port number in use by the server.
3. Optionally, click **Advanced** to specify advanced options to access the server.
4. Under **Access Novell Directory Service using**, specify the login name and password of the user account under which the application will access Novell Directory Service.
5. Optionally, click **Test connection** to attempt a connection to the specified Novell Directory service. If the connection fails, ensure that the settings are correct.
6. Click **Next**, and follow the provided instructions to complete the wizard.

Configuring Connection to IBM RACF

This section describes steps to configure a connection to IBM Resource Access Control Facility ((RACF) using the Add Connected System wizard.

The wizard prompts you to complete the **Specify connection settings for ActiveRoles Quick Connect for Mainframes (bridge)** page. This page is similar to the **Specify connection settings for AD LDS (ADAM)** page displayed when configuring connection to ADAM (see "Configuring Connection to AD LDS (ADAM)" earlier in this paper). On this page you can configure settings for connection to ActiveRoles Quick Connect for Mainframes (bridge) 3.5.5 (referred to as *LDAP Bridge*) delivered with the Quick Connect for Mainframes installation package. LDAP Bridge is an LDAP gateway that provides access to RACF.

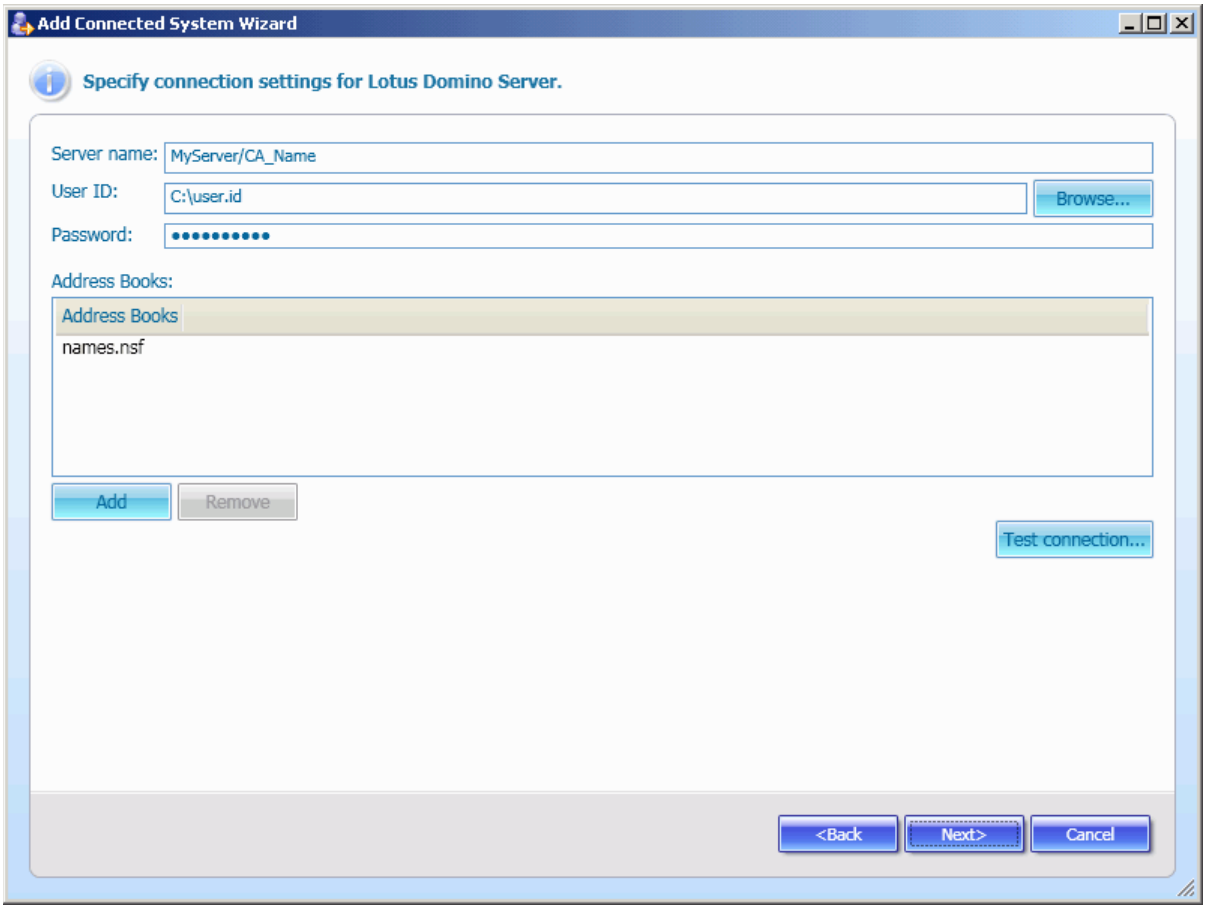
Steps to complete the **Specify connection settings for ActiveRoles Quick Connect for Mainframes (bridge)** page:

1. In the **Server** text box, type the fully qualified DNS name of the computer running the LDAP Bridge.
2. In the **Port** text box, type the LDAP communication port number in use by the LDAP Bridge.
3. Under **ActiveRoles Quick Connect for Mainframes (bridge)**, specify the login name and password of the user account under which the application will access the LDAP Bridge.
4. Optionally, click **Advanced options** to specify advanced options to access the LDAP Bridge.
5. Click **Next**, and follow the provided instructions to complete the wizard.

Configuring Connection to Lotus Domino Server

When configuring a connection to Lotus Domino Server, the wizard prompts you to complete the **Specify connection settings for Lotus Domino Server** and the **Specify Organizational Units** pages.

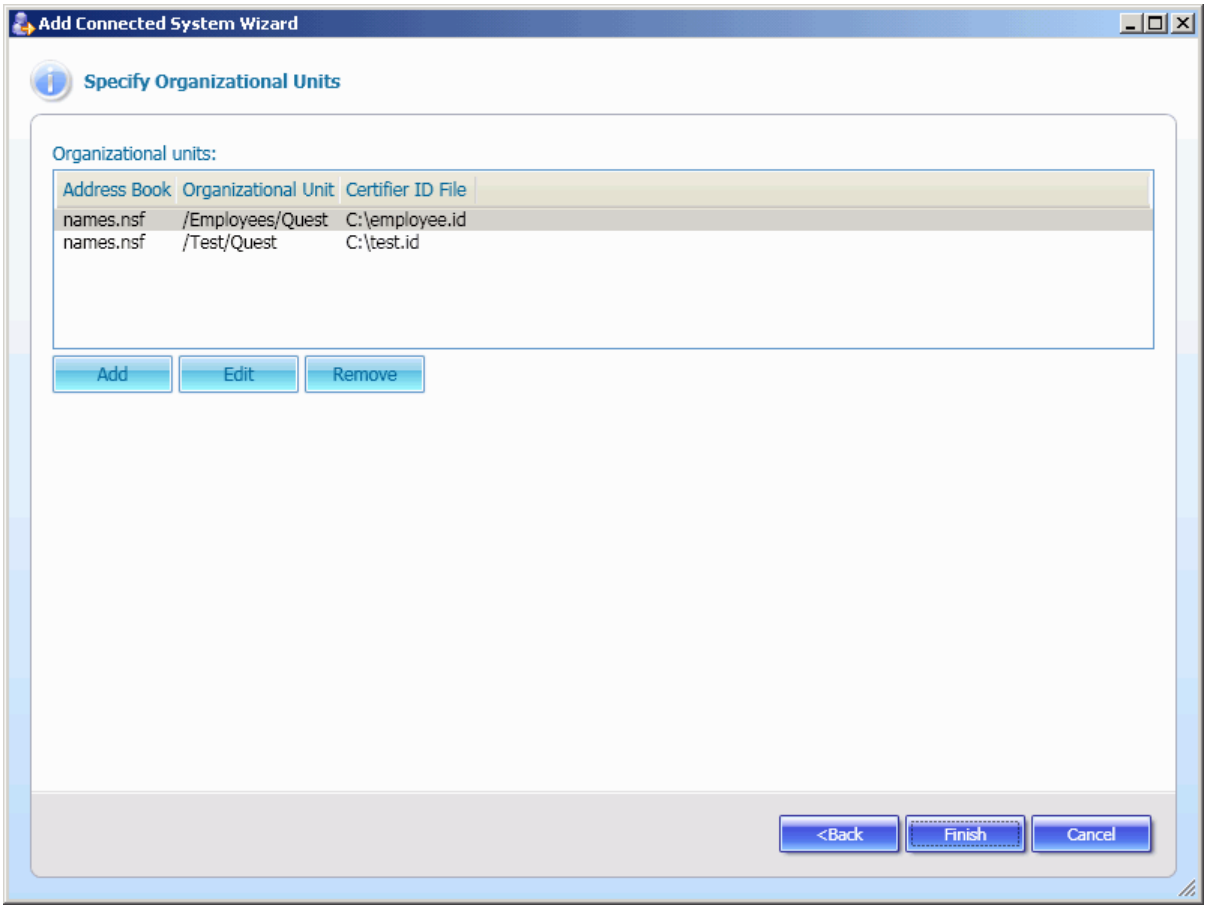
On the **Specify connection settings for Lotus Domino Server** page, you can specify a Lotus Domino server to connect, a User ID file, and address books with which to synchronize. This page is similar to the following screen:



On this page, do the following:

1. In **Server name**, type the hierarchical server name, such as *<ServerName>/<Certificate authority's name>*.
2. In **User ID file**, type the path to your User ID file, or click **Browse** to select this file.
   Make sure that you have a properly configured Connection document for this User ID file in Lotus Notes.
3. In **Password,** type the User ID file password.
4. Optionally, click **Add** to add a new address book to the **Address Books** list.
   Only address books from this list can participate in the synchronization process.

On the **Specify Organizational Units** page, for each address book, you can select Organizational Units that will participate in the synchronization process. This page is similar to the following screen:



The **Organizational units** list contains Organizational Units that will participate in the synchronization process. In the list, each entry contains 3 items: an address book name, an Organizational Unit name, and the path to the Certifier ID file for the Organizational Unit.

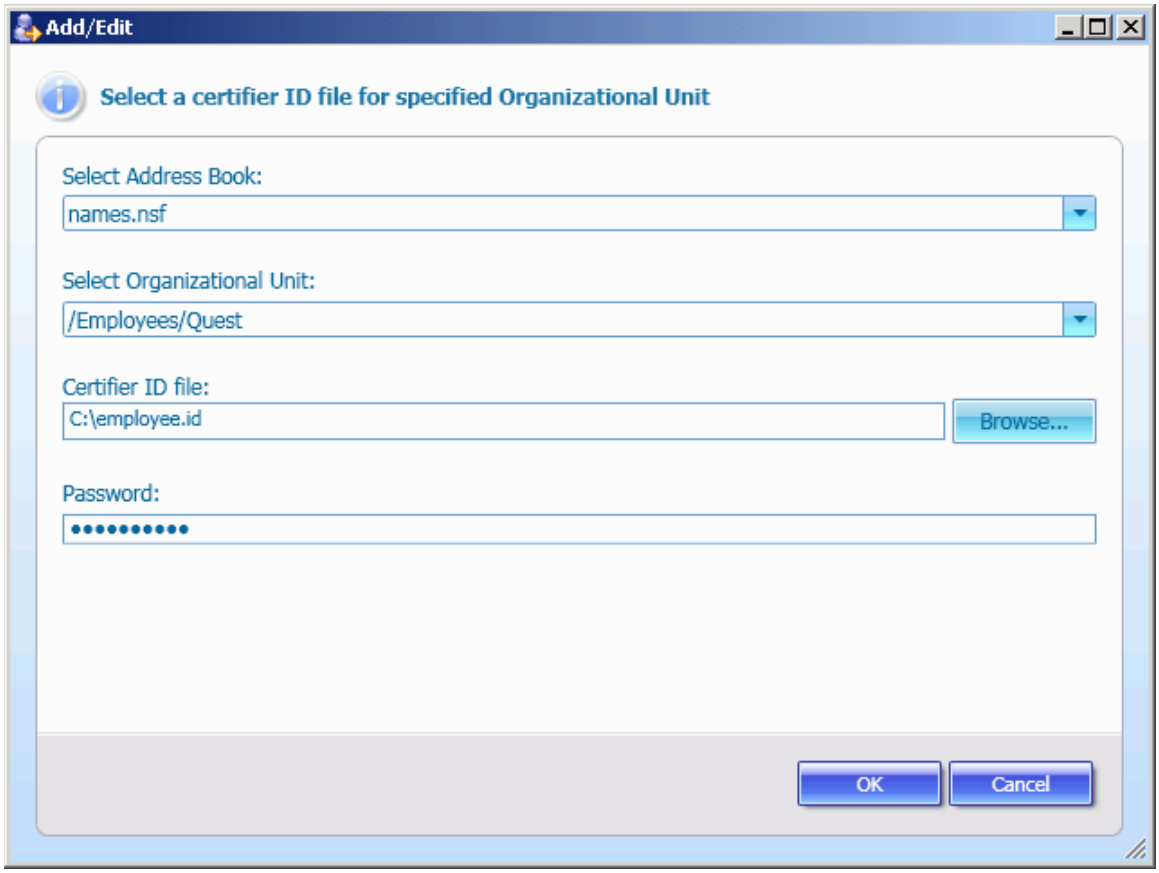
To specify the **Organizational units** list, use the following elements:

- **Add**: Opens the **Add/Edit** dialog box that allows you to add a new Organizational Unit to the **Organizational Units** list.
- **Edit**: Opens the **Add/Edit** dialog box that allows you to change settings for Organizational Unit currently selected from the **Organizational Units** list.
- **Remove**: Removes the currently selected Organizational Unit from the **Organizational Units** list.

Once you have configured a connection to Lotus Domino Server, you can modify the **Organizational units** list using the **Connection Information** tab of the **Connection Properties** pane for created connection. For more information, see "Connected Systems" earlier in this document.

If you have deleted an Organizational Unit (Certifier) on Lotus Domino Server, the Organizational Unit remains displayed in the **Organizational units** list on the **Connection Information** tab. In this case, you should manually remove deleted Organizational Units from the list.

Clicking the **Add** or **Edit** button displays the **Add/Edit** dialog box similar to the following screen:



In this dialog, do the following:

1. From the **Select Address Book** list, select the address book that contains an Organizational Unit to add.

   Note that this list contains only Address Books added on the **Specify connection settings for Lotus Domino Server** page.
2. From the **Select Organizational Unit** list, select the Organizational Unit.
3. In **Certifier ID file,** type the path to Certifier ID file for the selected Organizational Unit, or click **Browse** to select this Certifier ID file.
4. In **Password,** type the appropriate password for the Certifier ID file, and then click **OK** to close the dialog box.

Using the Lotus Domino Connector

The Lotus Domino connector allows you to synchronize between *Person objects*, *Group objects and Certifier objects* in Lotus Domino system, and *User objects, Group objects and Organizational Unit objects*, respectively, in Active Directory.

This section provides additional information that will help you effectively use the Lotus Domino connector. The following subjects are covered:

- Configuring Synchronization Steps
- Extending the Connector Schema

Configuring Synchronization Steps

Quick Connect extends the Lotus Domino Server Schema so that additional operational attributes can be handled for Person objects and Certifier objects. To populate values of those attributes, on the **Configure provisioning rules** page provided by the Add Synchronization Step wizard, configure the appropriate Initial Attribute Population rules. For related information, refer to "Configuring Provisioning Step" earlier in this paper.

Attributes Used for Provisioning Person Objects

The following table lists operational attributes used to configure a provision of Person objects from Active Directory to Lotus Domino Server. The names of additional operational attributes begin with *LN*.

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
Comment	A value for the comment field in the Domino Directory record.		
LNCertifierName	The certifier name when a Notes ID file is not used.		
LNCreateMailDb	Specifies whether a mail database is created.	FALSE	**TRUE** or **FALSE**
LNEnforceUniqueShortName	Specifies whether a short name must be unique. **Important** When this attribute is set to TRUE, you must set the **ShortName** attribute (this attribute is described in this table, later in this document) using an appropriate Initial Attribute Population rule.	FALSE	**TRUE** or **FALSE**
LNGroupList	Specifies a list of groups to which a user belongs during registration.		
LNIDExpiration	The expiration date for creation of ID files (in the DateTime format).	Now + 2 years.	Any desired date.
LNIDIsNorthAmerican	Specifies whether an ID file is North American.	TRUE	**TRUE** or **FALSE**

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
LNIDType	The type of the ID file to create.	172 - a hierarchical ID	**171** - a flat ID **172** - a hierarchical ID **173** - a flat or hierarchical ID depending on whether the certifier is flat or hierarchical.
LNIsRoamingUser	Indicates whether a user is a roaming user.	FALSE	**TRUE** or **FALSE**
LNMailACLManager	Specifies a name assigned to Manager access in the mail database ACL. The mail database owner may or may not be a Manager depending on MailOwnerAccess.		
LNMailCreateFTIndex	Specifies whether to create a full-text index for the mail database.	TRUE	**TRUE** or **FALSE**
InternetAddress	Specifies the user's Internet name for sending and receiving mail. When empty string, the registration process generates an Internet name.		
LNMailOwnerAccess	Specifies the mail database ACL setting for the owner.	0 **-** Manager	**0** - Manager **1** - Designer **2** - Editor
LNMailQuotaSizeLimit	Specifies the maximum size of the user's mail database (in megabytes). If 0 (zero), sets no size limit.	0	Any appropriate value.
LNMailQuotaWarningThreshold	Specifies a threshold size (in megabytes) for the user’s mail database. If the database size exceeds this value, the user receives a corresponding warning. Setting this value to 0 (zero) does not specify a threshold size.	0	Any appropriate value.
LNMailReplicaServers	Specifies a list of servers to which the mail database will replicate. This property applies only to clustered servers.		
MailSystem	Sets type of the mail system.	0	**0** - Lotus Notes **1** - POP **2** - IMAP **3** - Domino Web Access **4** - Other Internet **5** - Other **6** - None

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
LNMailTemplateName	Specifies the name of the template for the design of the mail file. When empty, a standard template is used. For example, in Release 6 the standard template is MAIL6.NTF.		
LNNoIDFile	Specifies whether to create an ID file during a registration.	FALSE	**TRUE** or **FALSE**
LNIDFile	Specifies the ID file name.		
LNMinPasswordStrength	Specifies a level of complexity assigned to the password for an ID file.	0	**0** (password is optional); **1** (password of any length is acceptable); **2, 3** (very weak password); **4-6** (weak password); **7, 8** (recommended complexity levels for users); **9-12** (strong password, recommended for servers and certifiers); **13-16** (highest complexity level, recommended for servers and certifiers).
Policy	Specifies the name of an explicit policy.		
LNRegistrationLog	The log file used when creating the ID files. No logging occurs if this parameter is an empty string, otherwise the information will log to the CERTLOG.NSF file saved in the Domino data directory on the registration server.		
RoamCleanPer	Specifies the interval (in days) for cleaning up data on Notes clients set up for roaming users.	0	

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
RoamCleanSetting	Specifies the clean-up process for data on Notes clients set up for roaming users.	0 - roaming data is never deleted.	**0** - roaming data is never deleted. **1** - roaming data is deleted every <*N*> days, where *N* is specified by the **LNRoamingCleanupPeriod** attribute. **2** - roaming data is deleted upon Notes shutdown. **3** - a user will be prompted to delete roaming data when exiting Notes. The user can also choose an individual clean-up or not. The user can also decline being prompted in the future.
LNRoamingServer	Specifies the server on which the user's roaming data is stored. If this property is empty, the roaming server defaults to the user's mail server.		
LNRoamingSubdir	Specifies the subdirectory that contains the user's roaming data.		
LNStoreIDInAddressBook	Specifies whether the ID file is stored into the server's Domino Directory.	TRUE	**TRUE** or **FALSE**
LNStoreIDInMailfile	Specifies whether the ID file is stored into the user's mail file. This property applies only to Domino Web Access and allows the Notes users to read their encrypted mail when using Domino Web Access.	FALSE	**TRUE** or **FALSE**
LNSynchInternetPassword	Specifies whether to synchronize the user's Internet password with the password for the Lotus Notes client ID. If the user changes the password for the Lotus Notes client ID file, the Internet password automatically (but not immediately) changes to match it.	FALSE	**TRUE** or **FALSE**
LNUpdateAddressBook	Specifies whether to update the server entry in the Lotus Domino Directory when creating the ID file.	TRUE	**TRUE** or **FALSE**
LNUseCertificateAuthority	Specifies whether the certificate authority (CA) is used for registration.	FALSE	**TRUE** or **FALSE**

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
LNUserType	Specifies the type of client to be created.	**176** - full client	**174** - Mail client **175** - Desktop client **176** - Default, full client
Location	A value for the location field in the Domino Directory record.		
MailAddress	The forwarding domain for the user's mail file.		
MailDomain	Lotus Notes domain of the specified person's mail address.		
MailFile	Sets path to the mail file.	"mail\<***ShortName*** *value*>.nsf" This default value is set only if the **LNCreateMailDb** attribute is set to TRUE.	Any name (the maximum name length is 8 characters). For example, if you set this attribute to "mbox", the "mail\mbox.nsf" mail file will be created.
ShortName	The Person object short name.	*First letter of the first name, followed by the last name* (only if the **FirstName** and **LastName** attributes of Person object are specified in the Initial Attribute Population rules) --- OR --- *First eight alphanumeric characters of the CN value of Person object.*	

Attributes Used for Provisioning Person Objects with Lotus Mailbox

The following table lists the Person object attributes and Initial Attribute Population rules that you can use to configure a provision of Person objects with Lotus mailbox from Active Directory to Lotus Domino.

For information about the Attribute Population Rule type, refer to "Attribute Transformation Rules" earlier in this paper.

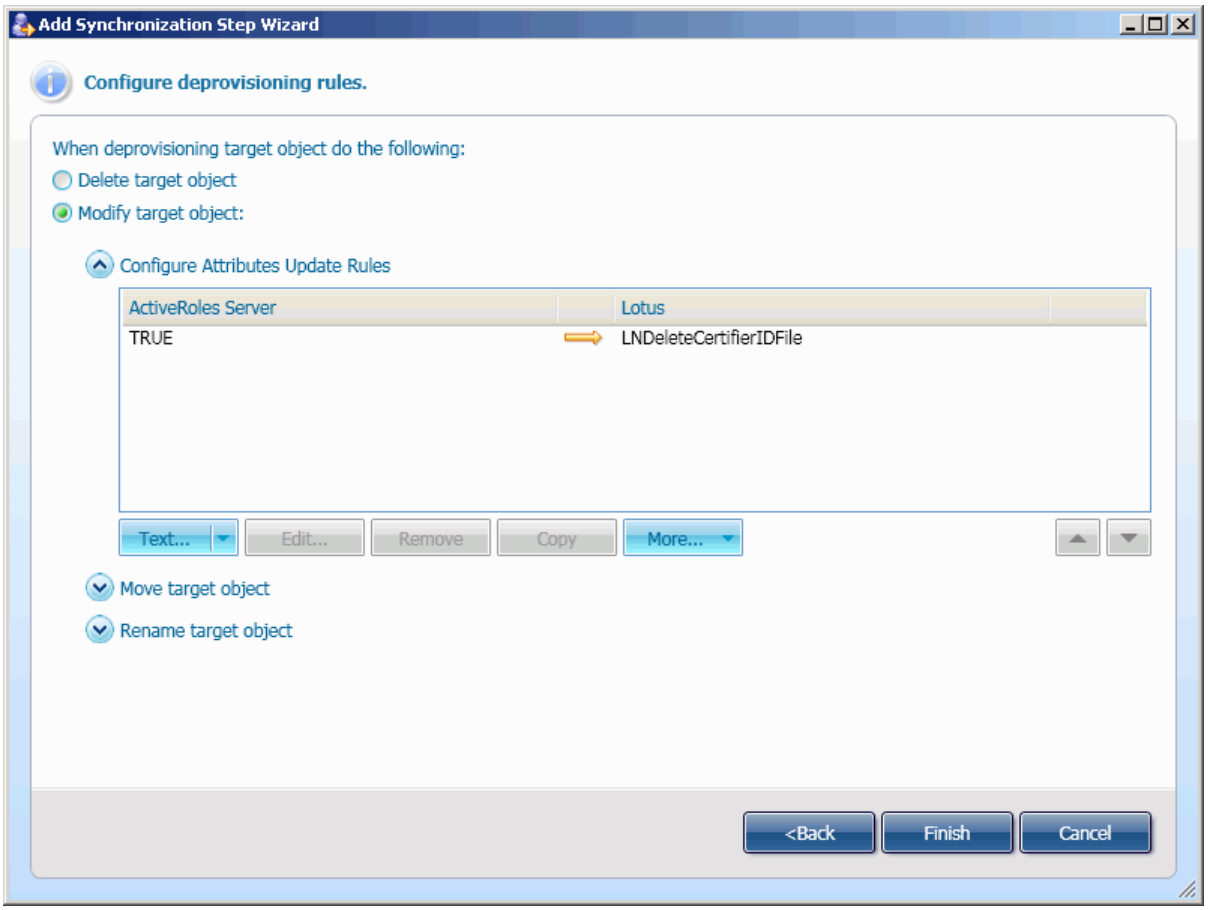
LOTUS ATTRIBUTE NAME	ACTIVE DIRECTORY ATTRIBUTE NAME, A CONSTANT OR A RULE	ATTRIBUTE POPULATION RULE TYPE
FirstName	**givenName**	Attribute-based
MiddleInitial	**initials**	Attribute-based
LastName	**sn**	Attribute-based
LNCreateMailDB	**true**	Constant-based
InternetAddress	**mail**	Attribute-based
MailSystem	**0**	Constant-based
MailServer	The Lotus mail server address, for example: **CN=lotus-server-10/O=mycompany**	Constant-based
MailAddress	**%<givenName>%<initials>%<sn>**	Rule-based
MailDomain	The Lotus Notes domain name. For example: **nyt**	Constant-based

Attributes Used for Deprovisioning Certifier Objects

The following table lists operational attributes used to configure a deprovision of Certifier objects.

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
LNDeleteCertifierIDFile	Specifies whether to delete the Certifier ID file when deprovisioning Certifier object.	FALSE	**TRUE** or **FALSE**

When you create a deprovisioning synchronization step, on the **Configure deprovisioning rules** page of the Add Synchronization Step wizard, you can specify how to deprovision Certifier objects. This page is similar to the following screen:



When configuring settings on this page, take into account the following behaviors:

- If yoy select the **Delete target object** option, the Certifier object will be deleted, but the corresponding Certifier ID file remains unless you manually delete it.
- If you select the **Modify target object** option, and then specify the Text-type rule that sets the **LNDeleteCertifierIDFile** attribute to TRUE, both the Certifier object and the corresponding Certifier ID file will be deleted.

Provisioning Certifier Objects

When provisioning Certifier objects, take into account the following points:

- Certifier ID file for newly provisioned certifier is always created into the Lotus directory that stores the Certifier ID for parent certifier.
- The passwords for newly provisioned certifier ID and its parent certifier ID are the same.

Attributes Used for Provisioning Group Objects

The following table lists operational attributes used to configure a provision of Lotus Domino Group objects.

ATTRIBUTE NAME	DESCRIPTION	DEFAULT VALUE	POSSIBLE VALUES
GroupType	Specifies the type of the newly created Lotus Domino group.	**1**	**0**: Multi-purpose, **1**: Mailing list only **2**: Access Control List only **3**: Deny List only 4: Servers only

Extending the Connector Schema

The Lotus Domino connector configuration information is stored into the *<%Quick Connect Installation folder%>\Service\Connectors\DominoConnector\ConnectorConfig.xml* XML configuration file discussed in "Configuration XML File Format" in Quick Connect SDK. The configuration file contains general information about the connector, such as the connector ID, description, assembly name, etc. In addition to general information, this file contains the SelfConfig element that includes XML child elements (between the *<SelfConfig>* and *</SelfConfig>* tags) specific to the Lotus Domino connector. These elements allows you to customize the Lotus Domino connector by extending the connector schema.

How the Application Reads the Connector Schema?

After you create a new connection to Lotus Domino Server, Quick Connect reads the schema for all Person and Group objects residing within Organizational Units (Certifiers) that participate in the synchronization process. These Organizational Units can be specified on the **Specify Organizational Units** page of the Add Connected System wizard (see "Configuring Connection to Lotus Domino Server" earlier in this paper).

You can optionally extend the Lotus Domino connector schema by modifying the SelfConfig element into the ConnectorConfig.xml file.

XML Elements Used to Extend the Lotus Domino Connector Schema

This section provides a list of XML elements you can use to extend the Lotus Domino connector schema.

For each element, the list includes the element name, description, parent element, child elements and attributes, if any.

All elements described in this section must be inserted into the ConnectorConfig.xml file. between the **<SelfConfig>** and **</SelfConfig>** tags.

Element Name: ***SchemaExtension***

Element Description: Contains definitions of attributes and object classes that extend the connector schema.

Parent Element: ***SelfConfig***

Child Elements: ***SchemaAttributeDefinition***, ***SchemaClassDefinition***

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
dominoObjectCount	Specifies the number of the Lotus Domino objects of each class (Persons, Groups and Certifiers) from which the connector reads the schema. When set to **-1**, the connector reads the schema from all found the Lotus Domino objects. Minimum value: **5**

Element Name: ***SchemaAttributeDefinition***

Element Description: Describes a new attribute that extends the connector schema. Note that one attribute can be assigned to several object classes.

Parent Element: ***SchemaExtension***

Child Elements: **None**

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
name	Specifies the attribute name.
displayName	Specifies the attribute display name.
attributeType	Specifies the syntax to which the attribute conforms. Possible values: • String • Boolean • Integer • LargeInteger • DateTime • Binary • ObjectReference
isSingleValue	When **TRUE**, the attribute is single valued.

Element Name: ***SchemaAttributeDefinition***

Element Description: Describes a new attribute that extends the connector schema. Note that one attribute can be assigned to several object classes.

Parent Element: ***SchemaExtension***

Child Elements: **None**

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
name	Specifies the attribute name.
displayName	Specifies the attribute display name.
attributeType	Specifies the syntax to which the attribute conforms. Possible values: • String • Boolean • Integer • LargeInteger • DateTime • Binary • ObjectReference
isSingleValue	When **TRUE**, the attribute is single valued.

Element Name: ***SchemaClassDefinition***

Element Description: Describes a Lotus Domino object class.

Parent Element: ***SchemaExtension***

Child Elements: ***Attributes***

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
name	Specifies the class name. The supported Lotus Domino object classes: • Person • Group • Certifier
displayName	Specifies the class display name.

Element Name: ***Attributes***

Element Description: Describes a collection of attributes to assign to the object class specified in the parent element ***SchemaClassDefinition***.

Parent Element: ***SchemaClassDefinition***

Child Elements: ***Attribute***

Attributes: None

Element Name: ***Attribute***

Element Description: Contains the attribute name to assign to the object class specified in the parent element ***SchemaClassDefinition***. Note that this attribute must be defined using the ***SchemaAttributeDefinition*** element described earlier in this section.

Parent Element: ***Attributes***

Child Elements: None

Attributes: None

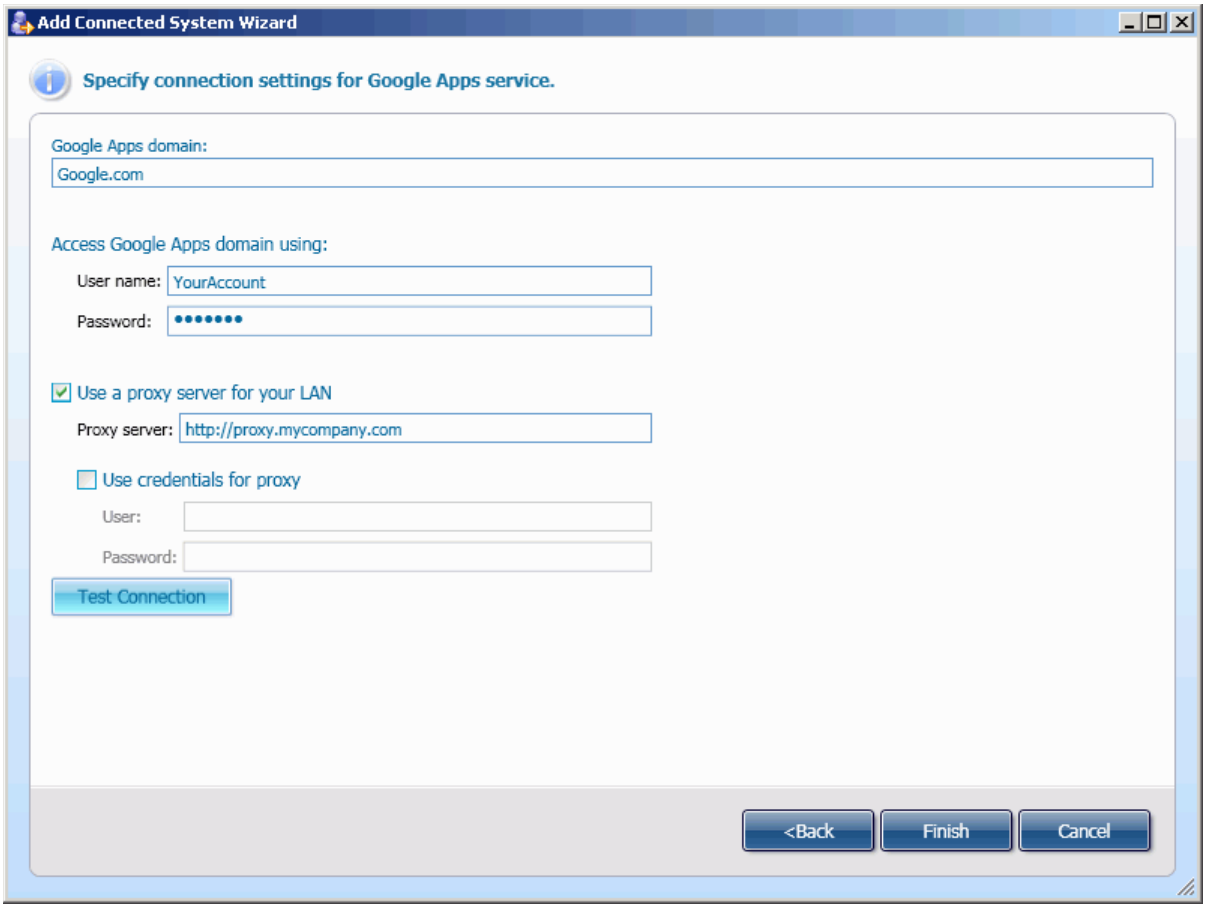
Sample of Use

To clarify the procedure of the Lotus Domino connector schema extension, consider the following snippet of the ConnectorConfig.xml file that contains only the SelfConfig section. This section extends the connector schema by assigning the NoteID and Form attributes to Lotus Group objects.

```
<SelfConfig>
   <!-- Causes Quick Connect to read the connector schema only from 6 first objects
        of each class found in Organizational Units participating in synchronization
    -->
  <SchemaExtension dominoObjectsCount="6">
     <!-- New attributes used to extend the connector schema -->
     <SchemaAttributeDefinition name="NoteID" displayName="NoteID" syntax="String"
singleValue="true" />
     SchemaAttributeDefinition name="Members" displayName="Members"
attributeType="ObjectReference" isSingleValued="false" />)
     <SchemaClassDefinition name="Group" displayName="Group">
         <!-- Assign new attributes to Lotus Groups -->
         <Attributes>
            <Attribute>NoteID</Attribute>
            <Attribute>Members</Attribute>
         </Attributes>
       </SchemaClassDefinition>
  </SchemaExtension>
</SelfConfig>
```

Configuring Connection to Google Apps Service

When configuring a connection to Google Apps service, the wizard prompts you to complete the **Specify connection settings for Google Apps service** page. On this page, you can specify the domain name, the user account used to contact the Google Apps domain. If your LAN uses a proxy-server, specify the proxy-server parameters. The **Specify connection settings for Google Apps service** page is similar to the following screen:



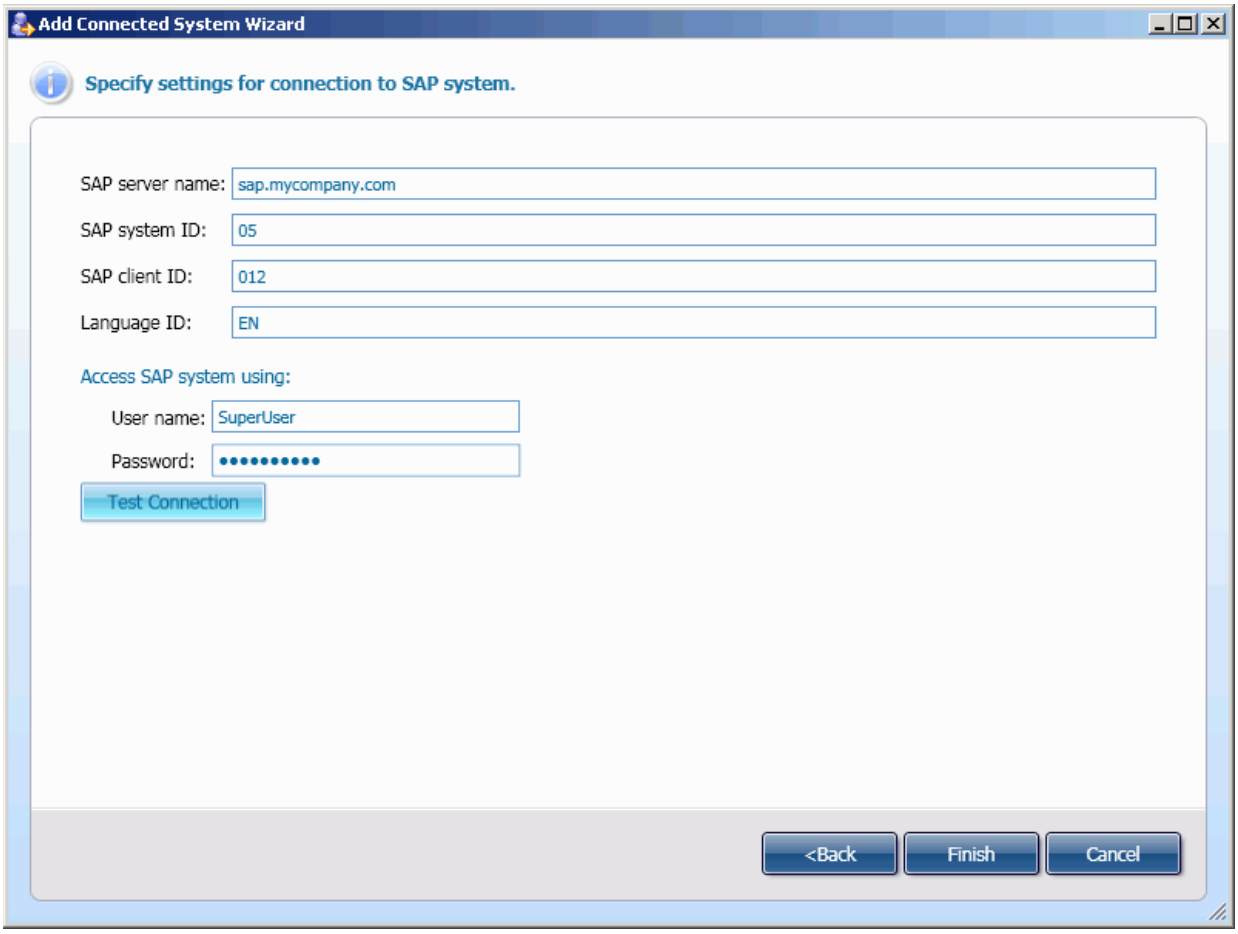
On this page, do the following:

1. In **Google Apps domain**, specify the name of the Google Apps domain to connect to.
2. Under **Access Google Apps domain using**, specify the user account and password under which the application will access the Google Apps domain.
3. If your LAN uses a proxy-server, select the **Use a proxy server for your LAN** option, and in **Proxy server**, enter the proxy server address.
4. If your proxy server requires authentication, select the **Use credentials for proxy** check box, and then in **User** and **Password**, specify the user account and password used to access the proxy-server.
5. Optionally, click **Test Connection** to check the connection to the specified Google Apps service.

   If the connection fails, ensure that the settings are correct.

Configuring Connection to SAP System

When configuring a connection to a SAP system, the wizard prompts you to complete the **Specify settings for connection to SAP system** page. On this page, you can specify the SAP server to connect and the connection parameters. The **Specify settings for connection to SAP system** page is similar to the following screen:



On this page, do the following, and then click **Finish**:

- In **Sap server name**, specify DNS name of the server running the SAP system to connect to.
- In **SAP system ID**, specify the SAP system ID.
- In **Sap client ID**, specify the SAP system client ID.
- In **Language ID**, specify the ID for the language used by the SAP system.
- In **User name** and **Password**, specify the user name on the SAP system, used to access the SAP system, and the password, respectively.

Using the SAP Connector

This section provides additional information about configuring synchronization steps using the SAP connector.

The SAP connector allows you to synchronize between *SAP User objects*, *SAP Employee objects* in SAP system, and *User objects* in Active Directory.

For *SAP Employee objects*, the bidirectional synchronization is not supported, i.e. for SAP Employee objects, you can configure the synchronization steps only from SAP system to ActiveRoles Server.

Populating Mandatory Attributes of SAP User Objects

The following SAP user attributes must be populated with *non-empty values* when provisioning User objects from ActiveRoles Server to SAP Systems:

- UserName
- LastName

To populate values of those attributes, on the **Configure provisioning rules** page provided by the Add Synchronization Step wizard, configure the appropriate Initial Attribute Population rules.

For example, you can configure the Initial Attribute Population rules that map the **sAMAccountName** and **sn** attributes of the source Active Directory user to the **UserName** and **LastName** attributes of the target SAP User, respectively.

For more information and related procedures, refer to "Configuring Provisioning Step" earlier in this paper.

Assigning SAP User Roles

In SAP systems, a role defines an activity set and all the sources of information and services that an individual SAP user needs in order to achieve a desired business objective. For more information about SAP user roles, refer to SAP documentation.

When provisioning user objects from ActiveRoles Server to SAP system, you can assign SAP roles to newly provisioned users using the Initial Attribute Population rules (for more information, see "Configuring Provisioning Step" and "Synchronization Rules for Multivalued Attributes" earlier in this paper.)

For example, to assign the SAP_BC_SRV_USER and SAP_BC_BASIS_MONITORING roles to all newly provisioned SAP users, start the Add Synchronization Step wizard, specify the provision from ActiveRoles Server to SAP system, and follow the provided instructions. On the **Configuring provisioning rules** page of the wizard, perform the following steps:

1. Expand **Configure Initial Attribute Population Rules**, click the arrow to the side of the **Attribute** button, and then click **Text**.

   *The **Constant-based Synchronization** dialog box opens.*

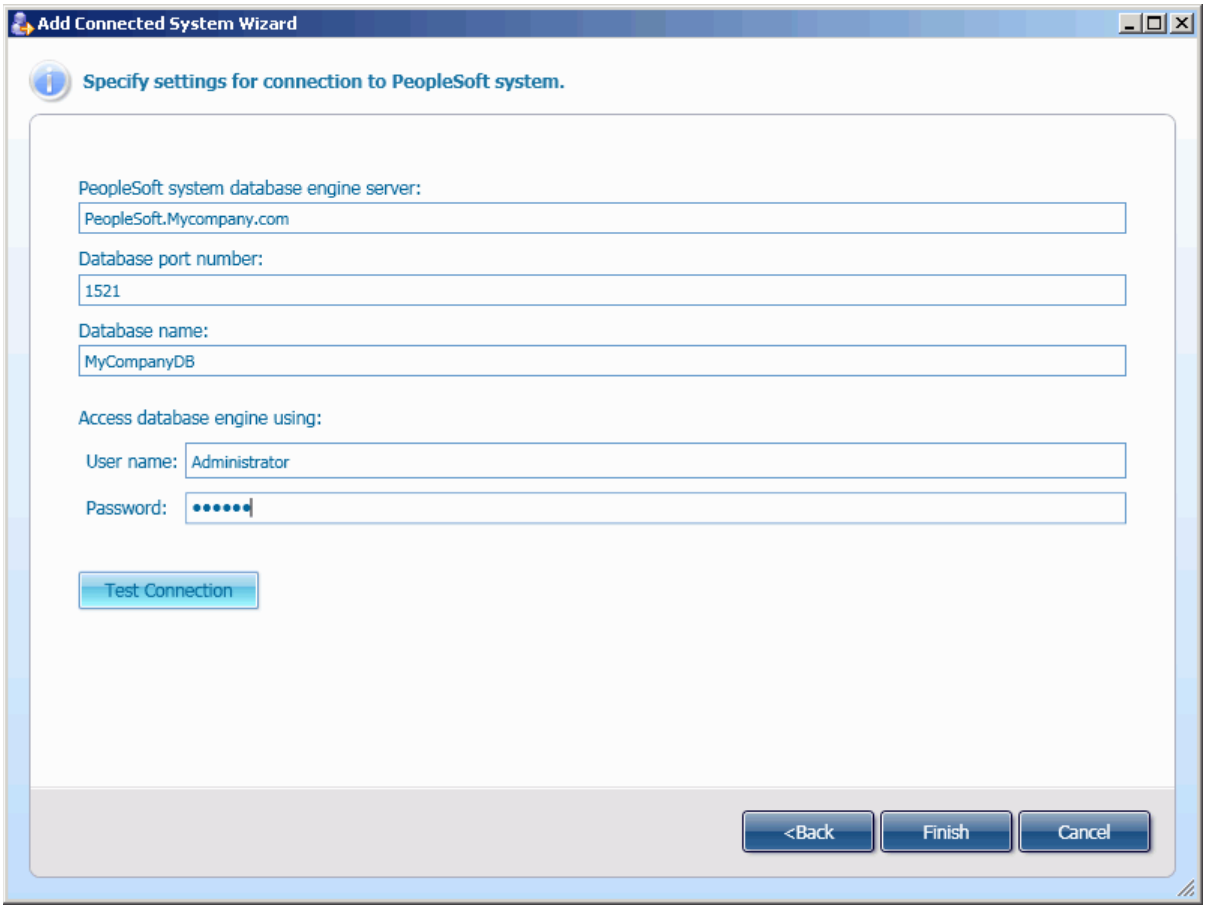
2. In the **Constant-based Synchronization** dialog box, to add the SAP_BC_SRV_USER role, do the following:
   - In the **Constant value** text box, type SAP_BC_SRV_USER.
   - Click **Select,** in the **Select Object Attribute** dialog box that opens, select **UserRoles**, click **OK** to close the **Select Object Attribute** dialog box, and then click **OK** to close the **Constant-based Synchronization** dialog box.
3. Under **Configure Initial Attribute Population Rules**, select the rule you created for SAP_BC_SRV_USER, click **More**, and then click **Options**.

   *The **Multivalued Attributes Synchronization Options** dialog box opens.*
4. In the **Multivalued Attributes Synchronization Options** dialog box, select the **Append source values to target attribute values** option, and then click **OK** to close this dialog box.
5. Repeat Steps 2 to 4 to add the SAP_BC_BASIS_MONITORING role.
6. Expand **Specify Initial Password**, and then specify how to generate password for newly created SAP user.
7. Click **Finish** to complete the Add Synchronization Step wizard.

After you run the synchronization step created using the procedure above, the provisioned SAP users will take the SAP_BC_SRV_USER and SAP_BC_BASIS_MONITORING roles.

Configuring Connection to PeopleSoft System

When configuring a connection to a PeopleSoft system, the wizard prompts you to complete the **Specify settings for connection to PeopleSoft system** page. On this page, you can specify the computer running the PeopleSoft system database engine to connect to, and the connection parameters. The page is similar to the following screen:



On this page, do the following, and then click **Finish**:

- In **PeopleSoft system database engine server**, specify DNS name or IP address of the computer running PeopleSoft system database engine to connect to.
- In **Database port number**, type the port number in use by the database engine.
- In **Database name**, type the name of database in use by the database engine.
- In **User name** and **Password**, specify the user name on the database engine, used to access the database engine, and the password, respectively.

Using the PeopleSoft Connector

This section provides additional information that will help you effectively use the PeopleSoft connector. The following subjects are covered:

- Configuring Synchronization Steps
- Extending the Connector Schema

Configuring Synchronization Steps

This section provides additional information about configuring synchronization steps using the PeopleSoft connector.

The PeopleSoft connector allows you to synchronize between *PeopleSoft User objects*, *PeopleSoft Employee objects* in PeopleSoft system and *User objects* in Active Directory.

The PeopleSoft connector does not support the bidirectional synchronization i.e. you can configure synchronization steps only from PeopleSoft system to ActiveRoles Server.

Extending the Connector Schema

The PeopleSoft connector configuration information is stored in XML configuration files located into the *<%Quick Connect Installation folder%>\Service\Connectors\PSConnector* folder. The following table lists the PeopleSoft connector configuration files.

FILE NAME	DESCRIPTION
ConnectorConfig.xml	Contains general information about the connector, such as the connector ID, description, assembly name, etc. The file format is discussed in "Configuration XML File Format" in Quick Connect SDK.
BaseQueries.xml	Specifies basic SQL queries used to calculate some of single-valued attributes of PeopleSoft objects. **Note** We don't recommend that you modify this file. Make all your custom changes in the **PSSchema.xml** file.
PSSchema.xml	Defines the *PeopleSoft connector schema*. The connector schema defines supported PeopleSoft object classes, attributes and display names used on the Quick Connect console User Interface. This file also specifies SQL queries used to calculate the following categories of PeopleSoft objects attributes: • Multivalued attributes. • Single-valued attributes that are not defined in the **BaseQueries.xml** file.

The information from this section will help you extend the PeopleSoft connector schema by customizing the **PSSchema.xml** file for PeopleSoft system used in your organization. The XML elements you can use in the **PSSchema.xml** file are discussed in "XML ElementsSample PSSchema.xml File" later in this document.

To add a new attribute to the connector schema, you must perform the following three basic steps:

1. **Choose a PeopleSoft object class for which you want to define a new attribute.**
   *All attributes for the object class are described using child elements of the **PSClass** element for this class.*
2. **Specify the new attribute name, display name, syntax, type.**
   *To do this, use the **PSAttribute** element that is a child element of the **PSAttributes** element for the appropriate **PSClass** element.*
3. **Specify how to calculate value(s) of a newly added attribute.**
   *To do this, use the **CustomQuery** element and its childs. The **CustomQuery** element is a child element of* **PSAttribute***.*

Sample PSSchema.xml File

To clarify the above procedure, consider the following snippet of the PSSchema.xml file that illustrates how to add the custom attribute "Status" that contains the PeopleSoft Employee status. In this scenario, the Status attribute value is calculated using XXX

<INSERT SAMPLE !!!>

For detailed description of XML elements used in this sample, refer to the “XML Elements” section later in this paper.

XML Elements

This section provides a list of XML elements you can use in the **PSSchema.xml** file. For each element, the list includes the element name, element description, parent element, child elements (if any), the element attributes (if any).

Element Name: ***PSClasses***

Element Description: Contains definitions of all supported PeopleSoft object classes. In this version, only the *PeopleSoft User* and *PeopleSoft Employee* object classes are supported.

Parent Element: ***PSClassSchema***

Child Elements: ***PSAttributes***

Attributes: None

Element Name: ***PSClass***

Element Description: Describes a PeopleSoft object class.

Parent Element: ***PSClasses***

Child Elements: ***PSAttributes***

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
name	Specifies the object class name. Possible values: • **PSUser**: specifies the PeopleSoft User object class. • **PSEmployee**: specifies the PeopleSoft Employeer object class.
displayName	Specifies the object class display name. This name is used on the application User Interface.

Element Name: ***PSAttributes***

Element Description: Describes a collection of all atributes supported for this object class.

Parent Element: ***PSClass***

Child Elements: ***PSAttribute***

Attributes: None

Element Name: ***PSAttribute***

Element Description: Describes the PeopleSoft object attribute.

Parent Element: ***PSAttributes***

Child Elements: ***CustomQuery***

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
name	Specifies the object attribute name.
displayName	Specifies the object attribute display name. This name is used on the application User Interface.
IsSingleValued	Specifies the object attribute type. Possible values: • **True**: single-valued attribute • **False**: multivalued attribute
HasInternalHandler	Specifies whether this object attribute can be processed using a special handler. In this release, this attribute must be always set to **False**.
AttributeSyntax	Specifies the object attribute syntax. Possible values: • **Integer** • **String** • **DateTime**
QueryType	Specifies the type of a SQL query used to retrieve the object attribute value. Possible values: • **None**: the query type is not specified. • **Base**: the query is defined in the **BaseQueries.xml** file. • **Custom**: the query is defined in the ***CustomQuery*** element.
AddToWebRequest	Specifies whether this object attribute can be modified using a SOAP request. In this release, this attribute must be always set to **None**.

Element Name: ***CustomQuery***

Element Description: Describes a set of SQL queries used to calculate the attribute value.

Parent Element: ***PSAttribute***

Child Elements: ***Queries***

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
QueryType	Specifies the query type. Possible values: • **Single**: Specifies that the PeopleSoft connector sends one request to retrieve the object attribute value(s) for all PeopleSoft objects from the synchronization scope. This query returns two-column SQL table. The names of columns are defined in the KeyColumn and ValueColumn attributes. • **Individual**: Specifies that the PeopleSoft connector sends individual requests to retrieve the object attribute value(s) for each PeopleSoft object from the synchronization scope. This query returns one-column SQL table that contains value(s) of the object attribute. The column name is of no importance. For parametrization of the individual query, use the following form: [@*attrName*], where the attrName refers to name of a PeopleSoft object attribute.
KeyColumn	Required only for the Single-type queries. Specifies the first column name. Set this attribute to name of the object attribute used as the unique ID.
ValueColumn	Required only for the Single-type queries. Specifies the second column name. Set this attribute to name of the object attribute values.

If the synchronization scope contains a large number of the PeopleSoft objects, the Single-type queries may consume too much memory.

The use of Individual-type queries may be a time-consuming operation.

Element Name: ***Queries***

Element Description: Describes a set of SQL queries used to calculate the object attribute value.

Parent Element: ***CustomQuery***

Child Elements: ***Query***

Attributes: None

Element Name: ***Query***

Element Description: Specifies a SQL query used to calculate the attribute value.

Parent Element: ***Queries***

Child Elements: None

Attributes:

ATTRIBUTE NAME	ATTRIBUTE DESCRIPTION
DBType	Specifies the type of the database from which the object attribute value will be calculated. In this release, the following possible values are supported: • **Any**: Any database. A generic SQL request will be used. • **Oracle**: Oracle database. An Oracle specific request will be used.
PeopleSoftVersions	This attribute is not used. In this release, this attribute must be always set to **Any**.

5

Using Management Shell

- About Management Shell
- Installing and Opening Management Shell
- Getting Help
- Cmdlet Naming Conventions
- Quick Connect Management Shell Cmdlets

About Management Shell

The Quick Connect Management Shell is an Active Directory-specific automation and scripting shell that provides a command-line management interface for synchronizing data between Active Directory and connected systems via the Quick Connect service.

The Quick Connect Management Shell is implemented as a Windows PowerShell snap-in, providing an extension to the Windows PowerShell environment. The commands provided by the Quick Connect Management Shell conform to the Windows PowerShell standards, and are fully compatible with the default command-line tools that come with Windows PowerShell.

The Quick Connect Management Shell command-line tools (cmdlets), like all the Windows PowerShell cmdlets, are designed to deal with objects—structured information that is more than just a string of characters appearing on the screen. The cmdlets do not use text as the basis for interaction with the system, but use an object model that is based on the Microsoft.NET platform. In contrast to traditional, text-based commands, the cmdlets do not require the use of text-processing tools to extract specific information. Rather, you can access portions of the data directly by using standard Windows PowerShell object manipulation commands.

Installing and Opening Management Shell

This section explains how to install and open the Quick Connect Management Shell.

Installing the Quick Connect Management Shell

The Quick Connect Management Shell is installed as an option of Quick Connect. It can be installed on the computer running Quick Connect Sync Engine or on any network computer.

To install the Quick Connect Management Shell

1. On a computer running a 32-bit edition of Windows, install the delivered file "QuickConnectManagementShell_x86.msi"
   -- OR --
   on a computer running a 64-bit edition of Windows, install the delivered file "QuickConnectManagementShell_x64.msi."
   The ActiveRoles Quick Connect Management Shell Installation wizard starts.
2. On the **Welcome** page, click **Next**.
3. On the **License Agreement** page, select the **I accept the license agreement** option and click **Next**.
4. On the **User Information** page, specify your personal information and click **Next**.
5. On the **Ready to Install the Application** page, click Next to proceed with the installation process.
6. On the Completion page, click **Finish** to close the wizard.

Opening the Quick Connect Management Shell

Before using the Quick Connect Management Shell, you are to load the Quick Connect Management Shell snap-in into Windows PowerShell. Otherwise, if you run a command (cmdlet) provided by that snap-in, you will receive an error.

To add the Quick Connect Management Shell snap-in from Windows PowerShell

1. Select **Start | All Programs | Windows PowerShell 1.0 | Windows PowerShell**.
2. At the Windows PowerShell prompt, enter the following command:
   Add-PSSnapin Quest.QuickConnect.PasswordManagerSnapin

Upon the shell start, the console may present you with a message stating that a certain file published by Quest Software is not trusted on your system. This security message indicates that the certificate the file is digitally signed with is not trusted on your computer, so the console requires you to enable trust for the certificate issuer before the file can be run. Press either **R** (Run once) or **A** (Always run). To prevent this message from appearing in the future, it is advisable to choose the second option (**A**).

Getting Help

The Quick Connect Management Shell uses the Windows PowerShell help cmdlets to assist you in finding the appropriate information to accomplish your task. The following table provides some examples of how to use the Get-Help and Get-Command cmdlets to access the help information that is available for each cmdlet in the Quick Connect Management Shell.

COMMAND	DESCRIPTION
Get-Help	When you use **Get-Help** without any parameters, you are presented with basic instructions on how to use the help system in Windows PowerShell, including Help for Quick Connect Management Shell.
Get-Help <Cmdlet>	When you use **Get-Help** with the name of a cmdlet as an argument, you are presented with the help information for that cmdlet. For example, to retrieve the help information for the **Change-QCUserPassword** cmdlet, use the following command: `Get-Help Change-QCUserPassword`
Get-Command	**Get-Command** without any parameters lists all the cmdlets that are available to the shell. You can use the **Get-Command** cmdlet with the **Format-List** or **Format-Table** cmdlet to provide a more readable display. For example, use **Get-Command | Format-List** to display the output in a list format.
Get-Command <Cmdlet>	When you use **Get-Command** with the name of a cmdlet as an argument, you are presented with information about the parameters and other components of that cmdlet. The <Cmdlet> entry allows for wildcard character expansion. For example, to retrieve information about the cmdlets with the names ending in Password, you can use the following command: `Get-Command *Password`
Get-Command -Noun <CmdletNoun>	**Get-Command -Noun** <CmdletNoun> lists all the cmdlets with the names that include the specified noun. <CmdletNoun> allows for wildcard character expansion. Thus, you can use the following command to list all the cmdlets provided by the Quick Connect Management Shell: `Get-Command -Noun QC*`

Cmdlet Naming Conventions

All cmdlets are presented in verb-noun pairs. The verb-noun pair is separated by a hyphen (-) without spaces, and the cmdlet nouns are always singular. The verb refers to the action that the cmdlet performs. The noun identifies the entity on which the action is performed. For example, in the **Change-QCUserPassword** cmdlet name, the verb is **Change** and the noun is **QCUserPassword**. All the Quick Connect Management Shell cmdlets have the nouns prefixed with QC, to distinguish the Quick Connect Management Shell cmdlets from those provided by PowerShell itself or by other PowerShell snap-ins. You can use the following command to list all cmdlets found in the Quick Connect Management Shell:

```
Get-Command Quest.QuickConnect.PasswordManagerSnapin\*
```

Quick Connect Management Shell Cmdlets

This section provides the reference information about the command-line tools (cmdlets) that are provided by the Quick Connect Management Shell.

In this release, the following cmdlets are supported:

- Change-QCUserPassword
- Reset-QCUserPassword

Change-QCUserPassword

Change the user password in connected systems.

Syntax

```
Change-QCUserPassword [-ServiceName <String>] -Identity <Object> -OldPassword
<SecureString> -NewPassword <SecureString> [-ConnectedSystem <String[]>]
[<CommonParameters>]
```

Parameters

PARAMETER	DESCRIPTION
ServiceName	Specify the name of the computer where the Quick Connect service is installed.
Identity	Specify the object GUID for the user account for which you want to change the password.
OldPassword	Specify the old password for the user.
NewPassword	Specify the new password for the user.
ConnectedSystem	Specify the comma-separated list of the connected systems where the user identity information exists.

Detailed Description

This cmdlet changes the user password in the connected data systems specified with the ConnectedSystem parameter. The ConnectedSystem parameter contains a comma-separated list of the connected data systems where to change the user password. If the ConnectedSystem parameter is not set, the cmdlet will change the password in all available connected data systems where the user identity information exists.

Examples

Example 1

This example illustrates how to change the password from "oldPass" to "newPass" for the user account identified with the "BA48B22F-07B3-46C8-B94D-A6D79D922D3E" object GUID. The cmdlet will change the user password in all available connected data systems where the user identity information exists. The Quick Connect service is running on the localhost.

```
C:\PS> $Identity = new-object Guid("BA48B22F-07B3-46C8-B94D-A6D79D922D3E")  $secNewPass
= ConvertTo-SecureString "newPass" -AsPlainText -force $secOldPass =
ConvertTo-SecureString "oldPass" -AsPlainText -force

C:\PS> Change-QCUserPassword  -Identity $Identity -OldPassword $secOldPass -NewPassword
$secNewPass
```

Example 2

This example illustrates how to change the password from "oldPass" to "newPass" for the user account identified with the "BA48B22F-07B3-46C8-B94D-A6D79D922D3E" object GUID. This cmdlet will change the user password only in the "System1" and "System2" connected systems. The Quick Connect service is running on the "qcservice1" server.

```
C:\PS> $Identity = new-object Guid("BA48B22F-07B3-46C8-B94D-A6D79D922D3E")  $ServiceName
= "qcservice1.domain.com"  $secNewPass = ConvertTo-SecureString "newPass" -AsPlainText
-force $secOldPass = ConvertTo-SecureString "oldPass" -AsPlainText -force

C:\PS> Change-QCUserPassword  -ServiceName "qcservice1.domain.com" -Identity $Identity
-OldPassword $secOldPass -NewPassword $secNewPass -ConnectedSystem "System1","System2"
```

Reset-QCUserPassword

Reset the user password in connected systems.

Syntax

```
Reset-QCUserPassword [-ServiceName <String>] -Identity <Object> -UserPassword
<SecureString> [-ConnectedSystem <String[]>] [<CommonParameters>]
```

Parameters

PARAMETER	DESCRIPTION
ServiceName	Specify the name of the computer where the Quick Connect service is installed.
Identity	Specify the object GUID for the user account for which you want to reset the password.
UserPassword	Specify the new password for the user.
ConnectedSystem	Specify the comma-separated list of the connected systems where the user identity information exists.

Detailed Description

This cmdlet resets the user password in the connected data systems specified with the ConnectedSystem parameter. The ConnectedSystem parameter contains a comma-separated list of the connected data systems where to reset the user password. If the ConnectedSystem parameter is not set, the cmdlet will reset the password in all available connected systems where the user identity information exists.

Examples

Example 1

This example illustrates how to reset the user password to "userPass." The user object GUID is set to "BA48B22F-07B3-46C8-B94D-A6D79D922D3E." This cmdlet will reset the user password in all available connected data systems where the user identity information exists. The Quick Connect service is running on the localhost.

```
C:\PS> $Identity = new-object Guid("BA48B22F-07B3-46C8-B94D-A6D79D922D3E")  $newPass =
ConvertTo-SecureString "userPass" -AsPlainText -force
C:\PS> Reset-QCUserPassword  -Identity $Identity -UserPassword $newPass
```

Example 2

This example illustrates how to reset the user password to "userPass." The user object GUID is set to "BA48B22F-07B3-46C8-B94D-A6D79D922D3E." This cmdlet will reset the user password only in the "System1" and "System2" connected data systems. The Quick Connect service is running on the qcservice1 server.

```
C:\PS> $Identity = new-object Guid("BA48B22F-07B3-46C8-B94D-A6D79D922D3E")  $secPass =
ConvertTo-SecureString "userPass" -AsPlainText -force

C:\PS> Reset-QCUserPassword  -ServiceName "qcservice1.domain.com" -Identity $Identity
-UserPassword $secPass -ConnectedSystem "System1","System2"
```

6

Scenarios of Use

- About Scenarios
- Provisioning Users from Connected System to Active Directory
- Update User Accounts in Active Directory Using a Delimited Text File

About Scenarios

This section contains sample scenarios that illustrate how to create and run synchronization workflows including the steps to update and provision user information from an HR database represented by a delimited text file to Active Directory. These scenarios will assist you in becoming familiar with ActiveRoles Quick Connect.

The following sample scenarios are considered:

- *Provisioning user accounts from a connected data system to Active Directory*: In this scenario, Quick Connect provisions user accounts from the HR database to separate Organizational Units in Active Directory, depending on the user city.
- *Updating user accounts in Active Directory using information from a connected data system*: In this scenario, Quick Connect updates user accounts in Active Directory, when the information on employees is changed in the HR database.

Before using sample scenarios, perform the following steps:

1. Make sure that you have installed Quick Connect for Base Systems. For more information, refer to the "Getting Start" section in Quick Connect for Base Systems - Release Notes.
2. Start ActiveRoles Server console and connect to ActiveRoles Administration Service that Quick Connect Sync Engine uses.
3. Add at least one managed domain.
4. In the managed domain, create the following Organizational Units (OUs):
   - "Employees" (at the root of the domain)
   within the "Employees" OU, create the following OUs:
   - "New York"
   - "Tokyo"
   - "Amsterdam"
   - "OtherCities"

Note: For detailed instructions on how to install and use ActiveRoles Server and ActiveRoles Server console, refer to Quest ActiveRoles Server - Quick Start Guide and Quest ActiveRoles Server - Administrator Guide.

Provisioning Users from Connected System to Active Directory

The following scenario demonstrates how to provision user accounts from a Human Resource database (HR database) to Active Directory. The HR database is represented by an export file (a delimited text file) available in Quick Connect Sync Engine release package. Depending on the user city, accounts will be provisioned to the Employees\New York, Employees\Tokyo, Employees\Amsterdam or Employees\OtherCities OU.

Creation of Provisioning Step

This section explains how you can create a synchronization workflow that includes a synchronization step to provision user accounts from the HR database to Active Directory.

The scenario demonstrates the following techniques:

- How to start the Add Synchronization Step wizard
- How to create a new connection to a delimited text file using the Add Connected System wizard.
- How to configure settings for provisioning step, such as the list of attributes to provision.
- How to develop a PowerShell script that returns the name of an Active Directory container for provisioned user accounts.
- How to preview a list of user accounts to provision.

To add a new synchronization step to the Default workflow, perform the following steps:

1. Start Quick Connect Administration console.
2. Open the **Workflow** tab and then in the **Default** pane, click **Click here to add a synchronization step**.
   The Add Synchronization Step wizard starts.
3. On the **Select an operation** page, select the **Provision** option and then select **Provisioning from connected system to ActiveRoles Server**. When finished, click **Next**.
4. On the **Specify the provisioning source** page, click **Specify**.
   The Add Connected System wizard starts.
5. On the **Add a new connected system or select an existing system** page, select **Add a new connected system** and click **Next.**
6. On the **Select connector and specify connection name** page, in the **Select connector** list, click **Delimited text file connector**. In the **Connection name** text box, type HR Export. When finished, click **Next**.
7. On the **Configure delimited text file connection settings** page, click **Browse**, and then select the sample.csv file with the **Open** dialog box. To continue, click **Next**.

By default, this file is located in the "[Program Files]\Quest Software\ActiveRoles Quick Connect\Samples" folder. If necessary, under **Access delimited text file using,** change default settings used to access the sample.csv file.

8. On the **Confirm delimited text file format** page you can preview the selected file. Click **Next** to continue.

9. On the **Specify attributes used to identify an object in the connected system** page, in the **Available Attributes** list, click EmployeeID, and then click **Add.** Click **Finish**.

   The Add Connected System wizard closes.

10. On the **Specify the provisioning source and criteria** page, click **Select** next to **Connected system object type**. In the **Select Object Type** dialog box that opens, click csv-Object, and then click **OK**.
11. On the **Specify the provisioning target** page, click **Select** next to the **Provision to this object type** box. In the **Select Object Type** dialog, select the User object type and click **OK**.
12. On the **Specify the provisioning target** page, click the arrow to the side of the **Browse** button, and then select **Script**.

    *The **Script Editor** dialog box opens.*

13. In the **Script Editor** dialog box, insert the following sample code (see Note below), 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
```

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

14. On the **Specify the provisioning target** page, click **Attribute**, and in the **Select Object Attribute** dialog box that opens, select the Logon Name attribute. Click **OK**, and then click **Next**.
15. On the **Specify provisioning rules** page, expand **Configure Initial Attribute Population Rules** and click the **Attribute** button.

    The Direct Synchronization dialog box opens.

16. In the **Direct Synchronization** dialog box, click **Select** next to **Source attribute**, and then select the Logon Name attribute. Click **Select** next to Target attribute, and then select the Logon Name (Pre-Widows 2000) attribute. When finished, click **OK**.
17. Repeat Steps 15-16 for the attributes: First Name, Last Name, and City.
18. On the **Specify provisioning rules** page, expand **Specify Initial Password**, click **Text**, and in the **Set Password** dialog box, specify a password, such as P@ssword. When finished, click **OK**.
19. On the **Specify provisioning rules** page, expand **Specify User Account Options**, and then optionally change the default options used for creation of a new user account.
20. Click **Finish** to close the Add Connected System wizard.

Running Provisioning Step

To run the synchronization workflow that includes the provisioning task you just created, perform the following steps:

1. Open the **Workflow** tab, and in the **Default** pane, click **Run now**.
   The Run Synchronization Workflow dialog box opens.
2. In the **Run Synchronization Workflow** dialog box, select the **Step 1: Provision from HR Export to ARS** check box, and then click **OK** to start this task.

After the synchronization workflow is completed, under **Step 1: Provision from HR Export to ARS**, the Quick Connect console displays the provisioning report that contains counters for the processed Active Directory and connected system objects, the mapped objects, the objects to be provisioned, etc. At this stage, the application does not commit changes to Active Directory.

To view the list of user accounts to be created in the Employees OU, click the link next to the **Objects to be provisioned** counter.

To commit changes to Active Directory

- Click **Commit**.

To ensure that Quick Connect Sync Engine has created user accounts in the Employees OU, explore this OU with ActiveRoles Server console. The New York, Tokyo, Amsterdam, and OtherCities OUs must contain a number of the disabled user accounts created by Quick Connect Sync Engine.

Update User Accounts in Active Directory Using a Delimited Text File

This scenario demonstrates how to update the Active Directory user accounts, when the information on employees is changed in the Human Resource (HR) database. The HR database is represented by an export file (a delimited text file).

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.

Creation of Update Step

This section explains how you can create a synchronization workflow that includes a step to update user accounts from the HR database to Active Directory.

The scenario demonstrates the following techniques:

- How to start the Add Synchronization Step wizard
- How to select an existing connection to a delimited text file with the Add Connected System wizard.
- How to configure settings for update step, such as a list of attributes to update.

To add a synchronization step to the Default workflow, perform the following steps:

1. Start Quick Connect Administration console.
2. Open the **Workflow** tab and then in the **Default** pane, click **Click here to add a synchronization step**.
   The Add Synchronization Step wizard starts.
3. On the **Select an operation** page, select the **Update** option and then select **Update from connected system to ActiveRoles Server**. When finished, click **Next**.
4. On the **Specify source for the update step** page, click **Specify**.
   The Add Connected System wizard starts.
5. On the **Add a new connected system or select an existing system** page, select the **Select existing connected system** option; from the available connected systems list, select **HR Export**, and then click **Finish**.
   The Add Connected System wizard closes.
6. On the **Specify source for the update step** page, click **Select** next to **Connected system object type**. In the **Select Object Type** dialog box that opens, click **csv-Object**, and then click **OK**. To proceed with the wizard, click **Next**.
7. On the **Specify target for the update step** page, click **Select** and in the **Select Object Type** dialog box, select the **User** object type, and then click **OK**. To proceed with the wizard, click **Next**.
8. On the **Specify rules for the update step** page, expand **Specify Attributes Update Rules**, and then click the **Attribute** button.
9. In the **Direct Synchronization** dialog box, click **Select** next to **Source attribute**, and then select the **City** attribute. Click **Select** next to T**arget attribute**, and then also select the **City** attribute. When finished, click **OK**.
10. Repeat Steps 8-9 for the following attributes: Department, First Name, Last Name, and Telephone Number.
11. On the **Specify rules for the update step** page, click **Finish** to close the wizard.

Running Update Step

To run the synchronization workflow that includes the update task you just created, perform the following steps:

1. Open the **Workflow** tab, and then in the Default workflow pane, click **Run now**.
   *The **Run Synchronization Workflow** dialog box opens.*
2. In the **Run Synchronization Workflow** dialog box, select the **Step 2: Update from HR Export to ARS** check box, and then click **OK** to start this task.

After the synchronization workflow is completed, under **Step 2: Update from HR Export to ARS**, the Quick Connect console displays the update report that contains counters for the processed Active Directory and connected system objects, the mapped objects, the objects to be updated, etc. At this stage, the application does not commit changes to Active Directory.

To view the list of user accounts to be updated in the Employees OU, in the update report, click the link next to **Objects to be updated** counter.

To commit changes to Active Directory

- Click **Commit**.

7

Appendixes

- Appendix 1: Troubleshooting
- Appendix 2: Glossary

Appendix 1: Troubleshooting

This chapter provides information to help you troubleshoot problems if any occur when using Quick Connect Sync Engine. The following sections briefly discuss some error statements that you may encounter when using the application.

Issue TF00048480

In reports on results of synchronization tasks, you may encounter the following issue: clicking the **Errors** link next to the **ActiveRoles Server objects to map** or **Connected system objects to map** counter, displays the **Mapping Ambiguity** dialog box listing the objects that cannot be mapped because of the mapping ambiguity, but this dialog box does not allow you to resolve this issue.

Cause

This error occurs if you have not configured mapping rules for a pair of the associated object types that participate in the synchronization task.

Resolution

To resolve this issue, use the following steps:

1. In the Quick Connect console, go to the **Mapping** tab.
2. In the list of associated object types pairs, expand the pair for which the synchronization task has failed, and then click **Map now**.

   The mapping operation starts.
3. After the mapping operation is completed, in the operation report, click the **Errors** link next to the **ActiveRoles Server objects to map** or **Connected system objects to map** counter.

   *The **Mapping Ambiguity** dialog box opens.*
4. In the failed objects list, select an object, and then click **Details**.

   *The **Object Mapping** dialog box opens. This dialog box allows you to manually map the failed object to the specified object in ActiveRoles Server or in the connected system, respectively.*
5. In the **Object Mapping** dialog box, click **Search**. From the found objects list, choose an object to which you want the failed object to map, and then click **Select**.
6. To confirm the operation, click **Map**. To select another object, click **New Search**.
7. Optionally, repeat Steps 4 to 6 for other objects in the failed objects list.
8. When finished, in the **Mapping Ambiguity** dialog box, click **Close**.

Issue TF00048523

When running a synchronization workflow, you may encounter the following issue: the synchronization operation fails with this error: "The server has rejected the client credentials. The logon attempt failed."

Cause

This error occurs if you have specified invalid credentials for connection to ActiveRoles Administration Service.

Resolution

To resolve this issue, use the following steps:

1. In the Quick Connect console, go to the **Connections** tab.
2. In the **ActiveRoles Server** area, click the **ActiveRoles Administration service** link.
   *The **ActiveRoles Server Connection Properties** dialog box opens.*
3. In the **ActiveRoles Server Connection Properties** dialog box, open the **General** pane, and then specify the appropriate credentials for connection to ActiveRoles Administration service. When finished, click **OK**.

Issue TF00048818

When performing the deprovisioning step, you may encounter the following issue: the synchronization operation fails with the "The source entry is not available" error.

Resolution

To resolve this issue, when configuring the deprovisioning rules for source objects that are out of synchronization scope, avoid using the source object attributes values in the Attribute update rules, Move target object rule, Rename target object rule. These rules can be configured on the **Configure deprovisioning rules** page of the Add Synchronization Step wizard.

Issue TF00055134

When performing a synchronization step, you may encounter the following issue: the Sync History report indicates that the number of mapped objects exceeds the total number of objects in connected data system or in Active Directory. Some of ActiveRoles Server objects are mapped to several connected systems objects.

Cause

This problem occurs when some of connected system objects have UniqueID attributes that are not unique or are empty.

Resolution

To resolve this issue, specify different UniqueID attributes that meet the following requirements:

- Attributes have unique values for each object to be updated.
- The attributes values are not empty.

Appendix 2: Glossary

C

Connected data system
A directory, database, file, or other data repository. Quick Connect support several categories of the connected data systems.

Connection
A connector configured for accessing the specific instance of a connected system is referred to as *connection*. Quick Connect Sync Engine provides the Add Connected System wizard designed to configure connectors for a wide variety of the connected data systems.

Connector
Quick Connect Sync Engine employs *connectors* to access data in the connected data systems. A connector is a driver or provider that encapsulates interactions with a particular connected system. Connectors control the data flow between a connected data system and ActiveRoles Server. There is a connector for each supported connected data system type. In addition to the connectors included when you install Quick Connect Sync Engine or Quick Connect for certain data systems, you can implement the custom connectors for data sources used in your organization.

M

Mapping rules
The rules that determine the linking of a connected system object with its counterpart in Active Directory. Mapping rules allow Quick Connect to establish one-to-one relationships between objects in the connected data system and Active Directory.

P

Passwords synchronization step
Refers to an operation to perform when synchronizing passwords between Active Directory users and their counterparts in a connected data system.

S

Synchronization step
Refers to an operation to perform when synchronizing data between Active Directory and a connected data system. The following types of synchronization steps exist:
- *Provisioning step*: Creation objects in a connected data system based on information on newly created objects in Active Directory.
- *Update step*: The process of renaming or modifying objects in a connected data system based on changes to their counterparts in Active Directory.
- *Deprovisioning step*: The process of renaming, moving or deleting objects in a connected data system when deleting or modifying their counterparts in Active Directory.

Synchronization workflow
A set of synchronization steps that determine how to synchronize data between connected data systems. A *synchronization workflow* is composed of at least one synchronization step.