ActiveRoles Quick Connect

What's New

Version 3.1

QUEST SOFTWARE®

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

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

www.quest.com
e-mail: legal@quest.com

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

Trademarks

ActiveRoles Quick Connect – What's New
Updated – September 15, 2006
Software version – 3.1

CONTENTS

About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate and secure Active Directory, Exchange and Windows, as well as integrate Unix and Linux into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

E-mail: info@quest.com

Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Web site: www.quest.com

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 support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles and 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: support.quest.com/pdfs/Global Support Guide.pdf

INTRODUCTION

ActiveRoles Quick Connect extends the capabilities of ActiveRoles Server, automating the management of user account lifecycle in Active Directory and beyond. ActiveRoles Quick Connect version 3.1 retains and improves upon the enterprise-class features of version 3.0, including:

- **Scheduled Import Wizard** to automate the management of Active Directory user accounts based on identity information from external data sources.
- **MIIS Integration** to provide an identity management solution that combines the capabilities of Quest ActiveRoles Server and Microsoft Identity Integration Server (MIIS).

Scheduled Import Wizard automates the tasks of maintaining Active Directory user accounts in sync with external data sources such as HR and ERP systems. It enables quick and efficient propagation of identity information from external data sources to Active Directory, automating the management tasks such as:

- Provisioning users with user accounts and access to resources, based on ActiveRoles Server AutoProvision policies
- Deprovisioning of user accounts, along with revocation of user access to resources, based on ActiveRoles Server Deprovision policies

MIIS Integration links ActiveRoles Server with Microsoft Identity Integration Server to automate provisioning, ongoing management, and deprovisioning of Active Directory users along with the management of user-related data in identity information repositories.

By combining MIIS with ActiveRoles Server, MIIS Integration provides the ability to leverage security, policy-based automation, and reporting benefits of ActiveRoles Server in a MIIS-based environment, and helps streamline and simplify user management tasks in Active Directory and beyond.

The new version of ActiveRoles Quick Connect capitalizes on the capabilities of ActiveRoles Server version 6.0, which include:

- Deprovision Policies
- AutoProvision Policies

The following sections elaborate on these new capabilities, as applied to ActiveRoles Quick Connect. The document also provides an overview of the major new features of Quick Connect version 3.0, inherited by the new version of this product.

NEW FEATURES INCLUDED IN VERSION 3.1

Designed to run on top of Quest ActiveRoles Server 6.0, ActiveRoles Quick Connect 3.1 benefits from the new capabilities of ActiveRoles Server, including:

- **Deprovision Policies.** Scheduled Import Wizard leverages the Deprovision Policies feature of ActiveRoles Server to automate the deprovisioning of user accounts, mailboxes and home folders, and to update security and distribution lists so that deprovisioned user accounts cannot access resources.
- **AutoProvision Policies.** Scheduled Import Wizard leverages the AutoProvision Policies feature of ActiveRoles Server to automatically generate user logon names and e-mail aliases, and to provision new users with resources such as Exchange mailboxes, home folders, and group memberships.

Deprovision Policies

With the earlier versions of the Scheduled Import Wizard, the deprovisioning-related operations are performed via custom, script-based policies. Now, it is also possible to use the Deprovision policies included in ActiveRoles Server for that purpose. ActiveRoles Server comes with a default policy to automate commonly-used deprovisioning tasks, and provides a point-and-click interface for managing the Deprovision policies so that these can be configured and applied without writing a single line of code.

Thus, once the Scheduled Import Wizard detects that a given user account is subject to deprovisioning, it requests ActiveRoles Server to perform all operations prescribed by the Deprovision policies. The following sections summarize the Deprovision policies that can be leveraged by the Scheduled Import Wizard.

User Account Deprovisioning

Modify deprovisioned user accounts so that they cannot be used to log on. A policy can be configured to:

- Disable deprovisioned user accounts
- Set user passwords to random values
- Set user logon names to random values
- Rename deprovisioned user accounts
- Update other properties of deprovisioned user accounts

Group Membership Removal

Remove deprovisioned user accounts from groups. A policy can be configured to remove such accounts from security groups, mail-enabled groups, or both.

It is also possible to configure a policy not to remove deprovisioned accounts from selected groups, or to specify that such accounts need not be removed from any security groups or mail-enabled groups.

User Account Relocation

Move deprovisioned user accounts to a certain organizational unit. The policy configuration specifies the organizational unit to move such accounts to. A policy can also be configured not to move deprovisioned user accounts.

Exchange Mailbox Deprovisioning

Deprovision Microsoft Exchange resources for deprovisioned user accounts. A policy can be configured to:

- Hide mailboxes from the global address list (GAL)
- Prevent non-delivery reports (NDR) from being sent
- Grant the user’s manager read-only access to the user’s mailbox
- Grant selected users or groups read-only access to the user’s mailbox
- Disallow forwarding messages to alternate recipients
- Forward all incoming messages to the user's manager

Home Folder Deprovisioning

Deprovision home folders for deprovisioned user accounts. A policy can be configured to:

- Remove the user’s permissions on the user’s home folder
- Grant the user’s manager read-only access to the user’s home folder
- Grant selected users or groups read-only access to the user’s home folder
- Make a selected user or group the owner of the user’s home folder
- Delete the user’s home folder when the user account is deleted

User Account Permanent Deletion

Schedule deprovisioned user accounts for permanent deletion. The policy configuration specifies the number of days (retention period) before the user account is deleted. A policy can also be configured so that the deprovisioned user accounts are not deleted automatically.

Script Execution

Run a certain script upon processing of a deprovision request. Scripting allows custom actions to be included in the user deprovision process. A script can be associated with the deprovision operation so that the policy runs it when the operation is requested or after the operation is completed.

Notification Distribution

Have a policy send a notification message to certain e-mail recipients upon processing of a deprovision request. It is possible to customize the list of recipients, the message subject, and the message body.

Report Distribution

Have a policy send an auto-generated report to certain e-mail recipients upon completion of processing of a deprovision request. The report includes a list of actions taken during the deprovisioning of the user account and the details of the deprovisioning activity. It is possible to customize the list of recipients and the message subject.

AutoProvision Policies

With the earlier versions of the Scheduled Import Wizard, provisioning-related operations such as generation of user logon names and e-mail aliases are normally performed by using custom scripts defined as part of user account creation rules. Creation of Exchange mailboxes and home folders for newly provisioned user accounts also required the use of scripting in many real-life scenarios.

The new version of the Scheduled Import Wizard makes it possible to use the AutoProvision policies included in ActiveRoles Server 6.0, to generate user logon names and e-mail aliases, provision users with Exchange mailboxes and home folders, and add users to appropriate security and distribution lists. ActiveRoles Server provides a point-and-click interface for managing those policies so that they can be configured and applied without writing a single line of code. The following sections summarize the AutoProvision policies that can be leveraged by the Scheduled Import Wizard.

User Logon Name Generation

Automatically generate the user logon name (pre-Windows 2000) to assign to the new user account, based on other properties of the account. A policy can be configured to automatically add an incremental numeric value in the event of a naming conflict, thereby ensuring uniqueness of the generated name.

E-mail Alias Generation

Automatically generate the e-mail alias to assign to the new user account. A policy can be configured to generate the alias based on pre-selected properties of the account, such as the first and last names or using a custom rule-based selection of properties. Custom rules allow an incremental numeric value to be added in the event of a naming conflict, to ensure uniqueness of the alias.

Exchange Mailbox AutoProvisioning

Automatically select a mailbox store, to provision the new user account with a mailbox on Microsoft Exchange Server. A policy defines a single store, or a set of stores, in which creation of mailboxes is allowed, and specifies a rule to distribute mailboxes among multiple stores either by using the round-robin method or by automatically selecting a store with the least number of mailboxes.

Group Membership AutoProvisioning

Automatically add the new user account the specified groups if the properties of the account meet the specified conditions. ActiveRoles Server checks the user account against conditions, and adds it to the appropriate groups based on the check results.

Home Folder AutoProvisioning

Automatically create a home folder or share, and assign it to the new user account. A policy determines the server on which to create home folders and shares, specifies naming conventions for home folders and shares, and defines the user access rights to the newly created home folders and shares.

NEW FEATURES INCLUDED IN VERSION 3.0

The new version of ActiveRoles Quick Connect inherits and improves upon the features of the previous version, including:

- **MIIS Integration.** Enables bi-directional synchronization of user accounts, groups and other directory data between ActiveRoles Server and Microsoft Identity Integration Service (MIIS).
- **Broad out-of-the-box connectivity.** Provides the ability to synchronize identity information from a wide variety of data sources, including directories, databases, and flat files.

The following sections provide an overview of these distinguishing features of the ActiveRoles Quick Connect 3.x releases.

MIIS Integration

The MIIS Integration feature enables ActiveRoles Server and Microsoft Identity Integration Server (MIIS) to be used in conjunction with one another to automate user management tasks such as the provisioning, ongoing administration and deprovisioning of Active Directory users, along with the management of user-related data in identity information repositories.

The capabilities of MIIS Integration are summarized in the sections that follow.

User Provisioning in Active Directory

For organizations that rely on MIIS for enterprise provisioning, MIIS Integration facilitates the user provisioning in Active Directory based on users' digital identities in corporate data stores. With the ability to export identity information from MIIS to Active Directory via ActiveRoles Server, MIIS Integration makes it possible to have MIIS populate Active Directory in compliance with the rules and policies defined in ActiveRoles Server, thus leveraging the security, rules-based automation, and reporting benefits of ActiveRoles Server.

User Management in Other Directories

By providing the ability to import directory data from ActiveRoles Server to MIIS, the MIIS Integration feature allows the administrative capabilities of ActiveRoles Server to be extended to non-Windows environments. Through the use of a rich suite of Management Agents available with MIIS out of the box, MIIS can be configured to automatically update multiple identity information stores, such as other directories, with directory data that flows from ActiveRoles Server.

User Self Management

By allowing MIIS to leverage ActiveRoles Server for updating identity information stores, MIIS Integration makes it possible to delegate user self-management tasks that include the management of user-related data in repositories other than Active Directory. When used in conjunction with MIIS, ActiveRoles Server provides the ability to give users limited and controlled access not only to their personal information in Active Directory but also to certain portions of their identity information stored outside Active Directory.

Operations Monitoring

Since MIIS Integration makes it possible for MIIS to communicate with Active Directory via ActiveRoles Server, the change tracking features of ActiveRoles Server, such as Management History, can be used to monitor the changes made by MIIS to Active Directory data. ActiveRoles Server provides a clear log documenting the changes that have been made by MIIS to directory data, such as user accounts or groups. The log includes entries detailing actions performed, success or failure of the actions, as well as which attributes were changed.

Point-and-click Configuration

The ActiveRoles Server console can be used to examine and adjust the rules and policies controlling data management actions that supplement data flows between MIIS and Active Directory via ActiveRoles Server. By leveraging the point-and-click interface featured by the console, administrators can configure a wide variety of rules and policies without writing a single line of code.

Broad Out-of-the-box Connectivity

The Scheduled Import Wizard automates the management of user account lifecycle by retrieving identity information from a data source and propagating that information to Active Directory. This process allows user accounts to be created, updated, or deprovisioned based on the state of data source objects.

The Scheduled Import Wizard is capable of synchronizing identity information from a wide variety of data sources. Out-of-the-box connectivity to directories and databases as well as flat-file access gives you the power to automate the tasks of maintaining Active Directory user accounts in sync with disparate sources of identity information in your company.

The Scheduled Import Wizard provides for connectivity to data sources of the following categories:

- **Delimited text file.** Identity information can be retrieved from a text file representing a point-in-time snapshot of a data repository.
- **Active Directory Application Mode (ADAM).** Identity information can be retrieved from servers running ADAM.
- **Sun and Netscape directory servers.** Identity information can be retrieved from Sun ONE Directory Server 5.2, formerly known as iPlanet directory server.
- **LDAP compatible directory.** Identity information can be retrieved from servers running a Lightweight Directory Access Protocol (LDAP) directory service.
- **Microsoft SQL Server database.** Identity information can be retrieved from databases hosted on Microsoft SQL Server 2000 or Microsoft SQL Server 2005.
- **Oracle database.** Identity information can be retrieved from Oracle Database 9i Release 2 or Database 10g Release 2 servers.
- **OLE DB or ODBC compatible database.** Identity information can be retrieved from arbitrary databases. The database must be accessible via an OLE DB provider or Open Database Connectivity (ODBC) interfaces, such as those included with Microsoft Data Access Components (MDAC). Virtually all database management systems in use today can be accessed through ODBC.