



Quest[®] ActiveRoles Server 6.5



What's New

**© 2009 Quest Software, Inc.
ALL RIGHTS RESERVED.**

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

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

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.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BusinessInsight, ChangeAuditor, ChangeManager, DeployDirector, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, ERDisk, Foglight, GPOAdmin, Imceda, IntelliProfile, InTrust, Invirtus, iToken, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogAdmin, MessageStats, Monosphere, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportAdmin, RestoreAdmin, SelfServiceAdmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer Pro, vPackager, vRanger, vRanger Pro, vSpotlight, vStream, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, Vizioncore vTraffic, Vizioncore vWorkflow, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Disclaimer

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

Quest ActiveRoles Server - What's New
Updated - August 31, 2009
Software Version - 6.5

CONTENTS




INTENDED AUDIENCE	4
CONVENTIONS	4
ABOUT QUEST SOFTWARE, INC.	5
CONTACTING QUEST SOFTWARE	5
CONTACTING QUEST SUPPORT	5
INTRODUCTION	6
NEW FEATURES OF ACTIVEROLES SERVER 6.5	7
NEW FEATURES OF ACTIVEROLES SELF-SERVICE MANAGER	8
WORKFLOWS	8
ABOUT WORKFLOW PROCESSES	9
POLICY EXTENSIONS	10
DESIGN ELEMENTS	10
GROUP DEPROVISIONING	11
UNDO DEPROVISIONING	13
GROUP OWNERS	14
GROUP PUBLICATION	16
MEMBERSHIP SELF-MANAGEMENT	17
EXPLORING THE MY ACCESS PAGE	18
KEYWORD SEARCH	19
DEFINING KEYWORDS FOR GROUPS	19
SEARCHING FOR GROUPS BY KEYWORD	19
RECYCLE BIN	20
RESTORING DELETED ACTIVE DIRECTORY OBJECTS	20
DELEGATING OPERATIONS ON DELETED OBJECTS	21
APPLYING POLICY OR WORKFLOW RULES ON DELETED OBJECTS	22
SUPPORT FOR EXCHANGE SERVER 2010	22
UPGRADE FROM AN EARLIER VERSION	23
COMPONENTS COMPATIBILITY	24
UPGRADE ISSUES	24
IMPACT ON ACTIVEROLES SERVER REPLICATION	24
IMPACT ON CUSTOM SOLUTIONS	24
IMPACT ON DYNAMIC GROUPS	24
IMPACT ON MAILBOX POLICIES	24
IMPACT ON CREDENTIALS OF OVERRIDE ACCOUNTS	25

Intended Audience

This document has been prepared to assist you in becoming familiar with the Quest ActiveRoles Server. The What's New contains the information required to install and use the Quest ActiveRoles Server. 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.
<i>Italic text</i>	Used for comments.
<i>Bold Italic text</i>	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, Inc.

Quest Software, Inc., a two-time winner of Microsoft's Global Independent Software Vendor Partner of the Year award, delivers innovative products that help organizations get more performance and productivity from their applications, databases Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows management solutions simplify, automate secure and extend Active Directory, Exchange Server, SharePoint, SQL Server, .NET and Windows Server as well as integrating Unix, Linux and Java into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

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

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](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf).

Note: This document is only available in English.

Introduction

Quest® ActiveRoles Server helps you manage, automatically provision, reprovision and deprovision users quickly, efficiently and securely in Active Directory and beyond. ActiveRoles Server provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service, to achieve practical user and group lifecycle management for the Windows enterprise.

The newest version, ActiveRoles Server 6.5, adds significant value: workflows to coordinate processes of directory data management, including change approval and notification; policy extensions that make it easy to create, deploy and use custom policy types; the ability to deprovision groups; increased self-service capabilities for users to administer their membership in groups; the ability to assign multiple owners to a single group; and support for the Active Directory Recycle Bin feature of Windows Server 2008 R2, with a point-and-click interface for restoring deleted objects.

This document presents the key new features in the latest version of ActiveRoles Server and ActiveRoles Self-Service Manager, and briefly describes the functionality of each. Information about other new features along with instructions on how to start using new features can be found in the *ActiveRoles Server Feature Guide*.

New Features of ActiveRoles Server 6.5

This new release of ActiveRoles Server extends and enhances the capabilities of the product, which now include workflows, policy extensions, deprovisioning of groups, self-service for users to join or leave groups, and restoration of deleted objects. The key new features of ActiveRoles Server 6.5 are:

- **New Edition of Self-Service Manager** An optional add-on module for ActiveRoles Server, ActiveRoles Self-Service Manager now provides the ability for regular users to self-manage their memberships in Active Directory groups and distribution lists. For more information, see [New Features of ActiveRoles Self-Service Manager](#) later in this document.
- **Workflows** A rich workflow system provides a powerful and convenient way to add new logic to directory data management and provisioning processes in ActiveRoles Server, including change approval, e-mail notification, and custom actions implemented by using script technologies such as Microsoft Windows PowerShell.
- **Windows PowerShell Scripting** Custom policies and workflow activities can be created using Windows PowerShell—a command-line shell and scripting language designed especially for system administration. ActiveRoles Server provides an environment for authoring PowerShell-based script modules, and leverages the Windows PowerShell runtime for executing policies and activities that use PowerShell-based script modules.
- **Policy Extensions** ActiveRoles Server offers a programmatic framework along with user interfaces that make it easy to create, deploy and use new types of administration policy performing custom provisioning or deprovisioning actions, in addition to the built-in policy types that ship with ActiveRoles Server.
- **Group Deprovisioning** ActiveRoles Server now provides for the Deprovision function on groups, enabling a group to be made temporarily unusable. For example, when a compliance review is not completed for a group within required time frame, which may pose a potential threat, deprovisioning can be applied on that group as a remediation measure.
- **Recycle Bin** ActiveRoles Server builds on Active Directory Recycle Bin, a new feature of Windows Server 2008 R2, to facilitate the restoration of deleted objects. By providing the ability to undo deletions in Active Directory quickly and easily, ActiveRoles Server minimizes the time, costs, and user impact associated with accidental deletions of directory data.
- **Support for Windows Server 2008 R2** All ActiveRoles Server components can run on Windows Server 2008 R2. ActiveRoles Server can be successfully used in Active Directory environments with domain controllers running Windows Server 2008 R2 and Active Directory domain or forest functional level of Windows Server 2008 R2.
- **Support for SQL Server 2008** ActiveRoles Server supports Microsoft SQL Server 2008, to take advantage of high availability, industry-leading performance, improved security, and other significant enhancements engineered into this new technology from Microsoft. Any edition of SQL Server 2008 can be used as a database or reporting services platform for ActiveRoles Server.
- **Support for Exchange Server 2010** ActiveRoles Server helps you streamline and secure your administration of Exchange Server 2010 through the use of role-based delegation, policy-based administration, flexible administrative views, and comprehensive console and Web-based interfaces to perform recipient management tasks.

New Features of ActiveRoles Self-Service Manager

With this new release of ActiveRoles Server, the capabilities of ActiveRoles Self-Service Manager—an optional add-on module for ActiveRoles Server—have been extended to enable self-service users to view or change their own memberships in groups. The key new features of ActiveRoles Server 6.5 that are specific to Self-Service Manager include the following:

- **Membership Self-Management** With Self-Service Manager, users can add or remove themselves from groups. This gives users the ability to manage their own memberships in groups without having to involve IT or Help Desk staff. The request to join or leave a group is granted only after owner approval.
- **Group Owners** In ActiveRoles Server, the owners of a group can be given rights to view or change the group, to review and attest the group, and, if the group requires owner approval for joining, to approve requests to join it. It is possible to assign multiple group owners, to load balance the management of groups.
- **Group Publication** In ActiveRoles Server, groups can be published for self-service so as to make them joinable by others based on owner approval. A user can submit a request for membership in a published group, which has to be approved by a group owner. This simplifies the task of joining groups while ensuring proper control over group memberships.
- **Keyword Search** A keyword search mechanism helps organize and locate groups in Self-Service Manager. The owner of a group or an IT administrator can associate the group with multiple keywords most likely to describe the group to someone looking for it. Self-service users may then rely on keywords to find and distinguish groups they are interested in.

Workflows

ActiveRoles Server provides a rich workflow system for directory data management automation and integration. Based on Microsoft's Windows Workflows Foundation technology, this workflow system enables IT to define, automate and enforce management rules quickly and easily. Workflows extend the capabilities of ActiveRoles Server by delivering a framework that enables combining versatile management rules such as provisioning and de-provisioning of identity information in the directory, enforcement of policy rules on changes to identity data, routing data changes for approval, e-mail notifications of particular events and conditions, as well as the ability to implement custom actions using script technologies such as Microsoft Windows PowerShell.

Suppose you need to provision user accounts based on data from external systems. The data is retrieved and then conveyed to the directory by using a service such as ActiveRoles Quick Connect that works in conjunction with ActiveRoles Server. A workflow can be created to coordinate the operations in account provisioning. For example, different rules can be applied for creating or updating accounts held in different containers.

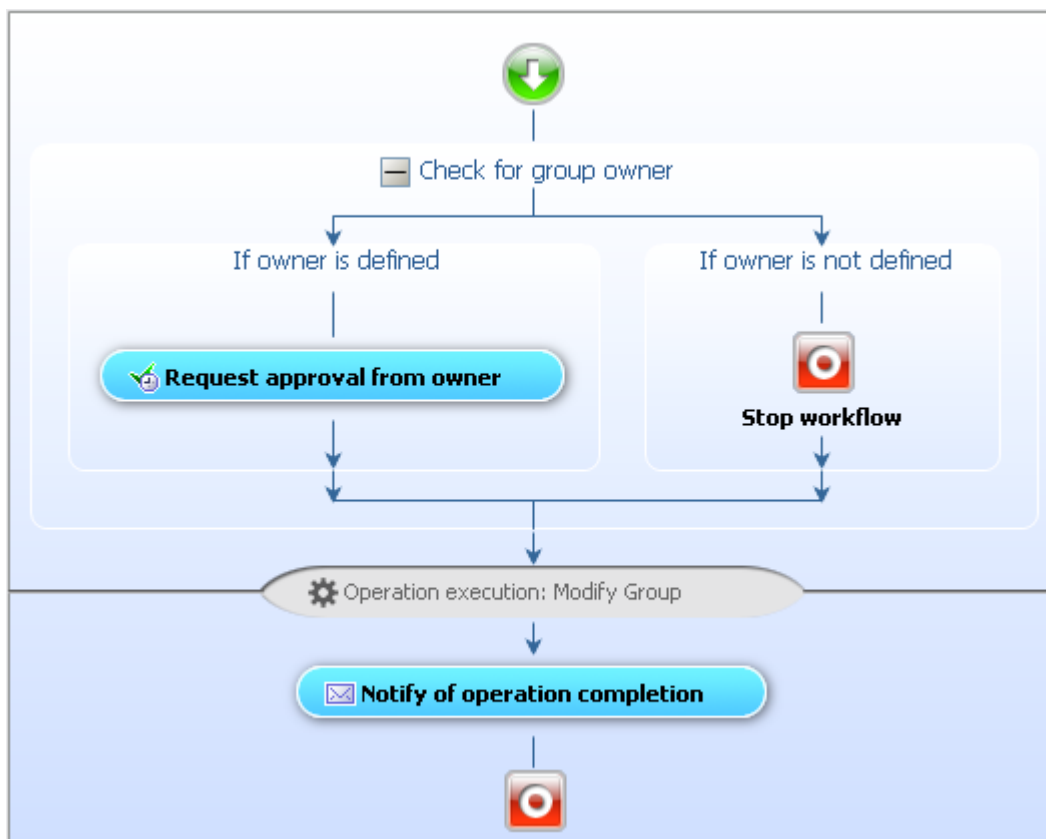
Workflows may also include approval rules that require certain changes to be authorized by designated persons (approvers). When designing an approval workflow, the administrator specifies which kind of operation causes the workflow to start, and adds approval rules to the workflow. The approval rules determine who is authorized to approve the operation, the required sequence of approvals, and who needs to be notified of approval tasks or decisions.

By delivering e-mail notifications, workflows extend the reach of management process automation throughout the enterprise. Notification activities in a workflow let people be notified via e-mail about events, conditions or tasks awaiting their attention. For example, approval rules can notify of change requests pending approval, or separate notification rules can be applied to inform about data changes in the directory. Notification messages include all necessary supporting information, and provide hyperlinks enabling message recipients to take actions using a standard Web browser.

About Workflow Processes

The logic of an automated management process can be implemented by using administrative policies in ActiveRoles Server. Yet creating and maintaining complex, multi-step processes in that way can be challenging. Workflows provide a different approach, enabling IT administrators to define a management process graphically. This can be faster than building the process by applying individual policies, and it also makes the process easier to understand, explain and change.

The diagram below shows a workflow process created in the ActiveRoles Server console. In this simple example, upon a request to add a user to a certain group, the workflow first checks to see if the group has an owner. If the group has no owner, the requested changes are denied and the workflow is complete; otherwise, the changes are submitted to the group owner for approval. When approval is received, ActiveRoles Server applies the changes, adding the user to the group. On the process diagram, this step is referred to as **Operation execution**. If the owner rejects the changes, the workflow finishes on the previous (approval) step so that the changes are not applied. After the changes are made, the workflow sends an e-mail notification to the person who requested the changes, and then finishes.



In the above example, the workflow manages the process of adding a user to a group according to the rules defined at design time. The rules constitute the workflow definition, and include the activities that occur within the process and the relationships between activities. An activity in a process definition can be a pre-defined function available out of the box, such as a request for approval or a notification of conditions that require user interaction, or it can be a custom function created using script technologies.

A workflow process is started when the requested changes meet the conditions specified in the workflow definition. In the above example, the conditions might be set up so that the workflow starts whenever an ActiveRoles Server user has made changes to the membership list of a certain group. Once the conditions are fulfilled, the workflow process starts to drive the changes through the workflow definition, performing automated steps and, if necessary, requesting human interaction such as approval.

For more information, see the “Workflows” chapter in the *ActiveRoles Server Administrator Guide*.

Policy Extensions

In previous versions of ActiveRoles Server, administrators could configure policies of only pre-defined types. The list of policy types in the ActiveRoles Server console was restricted to the types available out of the box, such as **Home Folder AutoProvisioning** or **User Account Deprovisioning**. There was no way to extend the list by adding new types of policy.

Each policy type determines a certain policy action (for example, creating a home folder for a user account) together with a collection of policy parameters to configure the policy action (for example, parameters that specify the network location where to create home folders). The latest version of ActiveRoles Server builds upon this concept, providing the ability to implement and deploy custom types of policy. It enables custom policy types to be created as necessary, and listed along with the pre-defined policy types, allowing administrators to configure policies that perform custom actions determined by those new types of policy.

ActiveRoles Server allows the creation of custom policies based on the **Script Execution** built-in policy type. However, creating and configuring a script policy from scratch can be time-consuming. Custom policy types provide a way to mitigate this overhead. Once a custom policy type is deployed that points to a particular script, administrators can easily configure and apply policies of that type, having those policies perform the actions determined by the script. The policy script also defines the policy parameters specific to the policy type.

Custom policy types provide an extensible mechanism for deploying custom policies. This capability is implemented by using the Policy Type object class. Policy Type objects can be created by using the ActiveRoles Server console, with each object representing a certain type of custom policy.

Design Elements

The policy extensibility feature is designed around two interactions: policy type deployment and policy type usage.

Policy Type Deployment

The deployment process involves the development of a script that implements the policy action and declares the policy parameters; the creation of a Script Module containing that script; and the creation a Policy Type object referring to that Script Module. To deploy a policy type to a different environment, an administrator can export the policy type to an export file in the source environment and then import the file in the destination environment. Using export files makes it easy to distribute custom policy types.

Policy Type Usage

This is the process of configuring policies. It occurs when an administrator creates a new Policy Object or adds policies to an existing Policy Object. For example, the wizard for creating a Policy Object includes a page that prompts to select a policy. The page lists the policy types defined in ActiveRoles Server, including the custom policy types. If a custom policy type is selected, the wizard provides a page for configuring the policy parameters specific to that policy type. Once the wizard is completed, the Policy Object contains a fully functional policy of the selected custom type.

ActiveRoles Server provides a graphical user interface, complete with a programming interface, for creating and managing custom policy types. Using those interfaces, ActiveRoles Server policies can be extended to meet the needs of a particular environment. ActiveRoles Server also has a deployment mechanism by which administrators put new types of policy into operation.

Since policy extension involves two interactions, ActiveRoles Server provides solutions in both areas. The Administration Service maintains policy type definitions, exposing policy types to its clients such as the ActiveRoles Server console or ADSI Provider. The console can be used to:

- Create a new custom policy type, either from scratch or by importing a policy type that was exported from another environment.
- Make changes to the definition of an existing custom policy type.
- Add a policy of a particular custom type to a Policy Object, making the necessary changes to the policy parameters provided for by the policy type definition.

Normally, an ActiveRoles Server expert develops a custom policy type in a separate environment, and then exports the policy type to an export file. An ActiveRoles Server administrator deploys the policy type in the production environment by importing the export file. After that, the ActiveRoles Server console can be used to configure and apply policies of the new type.

For more information, see the "Policy Extensibility" section in the *ActiveRoles Server Administrator Guide*.

Group Deprovisioning

ActiveRoles Server now provides for the Deprovision function on groups, enabling a group to be made temporarily unusable. For example, when Attestation Review for a group is not completed in a timely manner, which may pose a potential threat, group deprovisioning can be used as a remediation measure.

As applied to a group, deprovisioning refers to a set of changes being made in order to prevent the use of the group. What changes to make is determined by deprovisioning policies. ActiveRoles Server comes with a default deprovisioning policy, and allows new deprovisioning policies to be created and configured as needed.

Both the ActiveRoles Server console and Web Interface provide the **Deprovision** command on groups. When performing this command, ActiveRoles Server makes all the changes prescribed by the deprovisioning policies and creates a detailed report about the changes that were made along with information about success or failure of each change.

One more way to apply deprovisioning on groups is to configure Attestation Review in ActiveRoles Server so that the groups not attested within required time frame are automatically deprovisioned. Attestation Review also provides the option to let an IT administrator manually deprovision such groups.

ActiveRoles Server offers a number of policy types to control the group deprovisioning process:

- Group Object Deprovisioning
- Group Object Relocation
- Group Object Permanent Deletion
- Notification Distribution
- Report Distribution
- Script Execution

Group Object Deprovisioning

Group object deprovisioning policy specifies the changes to make to the group object in Active Directory in order to prevent the use of the group. It is intended to perform the following tasks when deprovisioning a group:

- **Hide the group from the Global Address List (GAL)**, to prevent access to the group from Exchange Server client applications such as Microsoft Outlook. This task is applicable to distribution groups or mail-enabled security groups.
- **Change the type of the group from Security to Distribution**, to revoke access rights from the group. This task is applicable only to security groups.
- **Rename the group**, to distinguish deprovisioned groups by name. This task can be configured to compose a name based on other properties of the group.
- **Remove members from the group**, to revoke user access to resources controlled by the group. This task has the option to specify the members that should not be removed from the group.

In addition, the policy can be configured to change or clear any other properties of a group, such as the pre-Windows 2000 name, e-mail addresses, or description.

Group Object Relocation

Group relocation policy is intended to perform the task of moving deprovisioned groups to specified organizational units. Moving deprovisioned groups to a different location removes such groups from the control of the administrators that are responsible for management of the organizational units in which those groups originally reside. This policy can also be configured not to move deprovisioned groups.

Group Object Permanent Deletion

Group deletion policy is intended to perform the task of deleting deprovisioned groups. Deprovisioned groups are retained for a specified amount of time before they are permanently deleted. This policy can also be configured not to delete deprovisioned groups. One more option is to delete deprovisioned groups immediately to Active Directory Recycle Bin.

When processing a request to deprovision a group, ActiveRoles Server uses this policy to determine whether to schedule the deprovisioned group for deletion. When scheduled for deletion, a group is permanently deleted after a certain time period, referred to as retention period. The retention period option specifies the number of days to retain deprovisioned groups. ActiveRoles Server permanently deletes a group after the specified number of days has passed since the group was deprovisioned.

One more option of group deletion policy is to delete deprovisioned groups to Active Directory Recycled Bin. With this option, ActiveRoles Server checks to see whether Recycle Bin is enabled in the domain of the group (this requires the Active Directory forest functional level of Windows Server 2008 R2), and then, if Recycle Bin is enabled, deletes the deprovisioned group immediately. Should the need arise to recover a group that was deprovisioned to Recycle Bin, ActiveRoles Server can be used to restore (un-delete) the group from Recycle Bin and then perform the Undo Deprovisioning operation on that group.

Notification Distribution Policy

Notification distribution policy is intended to send an e-mail notification upon a request to perform the deprovisioning operation. The primary purpose is to notify designated persons about a deprovisioning request, so they could take additional deprovisioning-related actions if necessary. The policy specifies the notification recipients and message, and determines the outgoing mail server (SMTP). The subject and the body of the message may include auto-text fields (tokens) to customize the message, making it more meaningful to the recipients.

A notification message cannot be considered as an indication of success or failure of the deprovisioning operation. It only indicates that a deprovisioning operation has been requested. To inform of deprovisioning results, ActiveRoles Server offers report distribution policy.

Report Distribution Policy

Report distribution policy is intended to send a report on deprovisioning results upon completion of a deprovisioning operation. The report includes a list of actions taken during the deprovisioning operation. For each action, the report informs of whether the action is completed successfully, and provides information about the action results.

The policy specifies the report recipients, the subject of the report message, and whether to send a report if no errors occurred. Similar to the notification messages, the message subject can be configured to include auto-text fields (tokens). Report messages are delivered via e-mail by using SMTP transport.

Script Execution Policy

Script execution policy can be used to run supplementary scripts upon requests to deprovision groups. Scripting allows custom actions to be included in the group deprovisioning process. A script can be associated with a deprovision operation so that the policy runs it when the operation is requested or after the operation is completed.

Undo Deprovisioning

ActiveRoles Server provides the ability to restore deprovisioned groups. The purpose of this operation, referred to as *Undo Deprovisioning*, is to roll back the changes that were made to a group by the Deprovision operation. When a deprovisioned group needs to be restored (for example, a group was deprovisioned accidentally), Undo Deprovisioning allows the group to be quickly returned to the state it was in before the changes were made.

Undo Deprovisioning rolls back the changes that were made to the group in accord with the standard deprovisioning policies. For example, assume the deprovisioning policy is configured so that Deprovision operation:

- Removes all members from the group
- Renames the group
- Moves the group to a certain container

In this case, the Undo Deprovisioning operation:

- Restores the original membership list of the group, as it was at the time of deprovisioning
- Renames the group, restoring the original name of the group
- Moves the group to the container that held the group at the time of deprovisioning

Similar behavior is in effect for the other deprovisioning policies:

- If the Deprovision operation hides the group from the Global Address List (GAL), Undo Deprovisioning restores the visibility of the group in the GAL.
- If the Deprovision operation changes the group type from Security to Distribution, Undo Deprovisioning sets the group type back to Security.
- If the Deprovision operation changes any other properties of the group, Undo Deprovisioning restores the original property values.

Both the ActiveRoles Server console and Web Interface provide the **Undo Deprovisioning** command on deprovisioned groups. When selected on a deprovisioned group, this command originates a request to restore the group. Upon receipt of the request, ActiveRoles Server performs all necessary actions to undo the results of deprovisioning on the group, and provides a detailed report of the actions that were taken along with information about success or failure of each action.

Group Owners

An owner of a group is a person designated to perform certain management tasks on that group, such as:

- Add or remove members from the group
- Act as an approver to allow or deny changes to the group requested by other people (for example, requests to join or leave the group)
- Act as an attestor to review and certify the membership list of the group in the course of Attestation Review
- Deprovision or un-deprovision the group, if necessary

With earlier versions of ActiveRoles Server the owner of a group was the same as the manager, that is, the user specified by the "Managed By" property of the group. This resulted in two major shortcomings:

- It was possible to designate only a single person as the owner of a single group
- The owner of a group had to belong to the same domain as the group itself

The latest version of ActiveRoles Server removes these limitations by offering the "Secondary Owners" property on groups. This is a multi-valued property that can identify several users or groups as owners of a single group. In addition, the "Managed By" property can now be set not only to a user but also to a group.

The owners of a group are specified on the **Managed By** page for that group, in the ActiveRoles Server console or Web Interface. The page displays the name and other properties of the manager, and includes a separate area for designating secondary owners. In ActiveRoles Server, the manager is also referred to as the primary owner.

The **Managed By** page can be used to view or change the primary owner or secondary owners:

- The primary owner (manager) of a group can be a user or group from the same domain as the group itself. When the primary owner is set to a group, any member of that group may act as the primary owner.
- One or more secondary owners may be assigned to a single group, with each of the secondary owners being a user or group from any managed domain. This capability is especially useful in a resource forest topology where resources, such as Exchange distribution groups, are located in a forest other than the forest that holds the accounts of the owners. When a secondary owner is a group, then any member of that group may act as a secondary owner.

The **Managed By** page can also be used to specify whether the primary owner (manager) or secondary owners are authorized to add or remove members from the group. It is possible to do this separately for the primary and secondary owners: thus, only the primary owner or only the secondary owners might be allowed to change the group membership list.

Another way to delegate group management tasks to owners of a group is to use built-in accounts that represent group owners. By selecting the **Primary Owner (Managed By)** or **Secondary Owners** built-in account as the delegated account in the Delegation of Control Wizard, you effectively delegate control of a group to the users or groups identified as the primary owner or secondary owners of that group, respectively. In this way you can authorize group owners to deprovision or un-deprovision the groups that they own.

The Approval and Notification activities in ActiveRoles Server Workflow provide separate options for the primary or secondary owners to act as approvers or receive notifications. Supported are several types of approval:

- **Single approval** One level of approval is required, whether that be the primary owner or any one of the secondary owners. It is possible to configure approval workflow so that only the primary owner can approve changes to the group, or only secondary owners can approve changes.
- **Multiple approvals in serial order** Approvals by both the primary owner and one of the secondary owners are required, with a subsequent approval not taking place until its antecedent is approved.
- **Multiple approvals in parallel order** Approvals by both the primary owner and one of the secondary owners are required, but all owners are contacted at once with the request. The process does not continue until the primary owner and any one of the secondary owners have approved the requested changes to the group.

Notification can be configured so that different owners are notified of different events. For each event type, it is possible to specify whether only the primary owner, only the secondary owners, or both the primary and secondary owners receive notifications about events of that type.

When setting up Attestation Review, you can choose who is authorized to review and certify the groups to be attested. It is possible to configure Attestation Review so that only the primary owners, only secondary owners, or both the primary and secondary owners are allowed to perform attestation. With multiple owners, the review of a group is considered complete once any of the designated owners has certified the group.

ActiveRoles Server provides the capability to view all groups for which a given user is assigned as a primary or secondary owner, from a single page in the ActiveRoles Server console or Web Interface. The **Managed Resources** page on a user account lists the groups owned by that user, and gives an indication of the ownership type on each group:

- **Primary** The user is the only manager of the group, specified by the "Managed By" property.
- **Primary-Inherited** The user belongs to the group specified by the "Managed By" property. Every member of such a group has the rights that are granted to the primary owner.
- **Secondary** The user is a secondary owner, specified by the "Secondary Owners" property.
- **Secondary-Inherited** The user belongs to a group specified by the "Secondary Owners" property. Every member of such a group has the rights that are granted to the secondary owners.

By using the **Managed Resources** page, an IT administrator can detect issues with assigning group owners. For example, it is easy to identify the groups for which a given user is assigned as both the primary owner and a secondary owner.

Group Publication

With the latest release of ActiveRoles Server, group publication is used to provide end-users with controlled access to their group memberships through ActiveRoles Self-Service Manager. Publishing a group makes the group joinable by other people based on owner approval. Self-Service Manager enables users to submit requests to join or leave published groups, while ensuring that requests are granted only after approval by group owners.

Approval workflow complements group publication, empowering group owners to control changes to group memberships. By enabling group owners to approve or reject membership requests, ActiveRoles Server helps reduce the burden of verifying whether or not a particular person should be allowed to join a particular group. This burden is shifted from IT staff to group owners who are in the best position to justify the need for group membership changes.

Group publication is accomplished through adding groups to a built-in Managed Unit called "Published Groups" that has security and workflow controls configured to ensure the appropriate behavior of the published groups in ActiveRoles Server. A certain property of groups, called "Is Published," determines which groups are members of that Managed Unit. When publishing a group, ActiveRoles Server sets the "Is Published" property on that group, thereby causing the group to be automatically added to the "Published Groups" Managed Unit.

To facilitate group publication, both the ActiveRoles Server console and Web interface provide the **Publish** command on groups. The command is complemented by a dialog box that enables you to review and, if necessary, change a number of settings prior to starting the Publish operation. These include the group description, keywords and notes. In that dialog box, it is possible to choose whether changes to the group require approval and who should approve the changes: the primary owner, a secondary owner, or both.

The **Properties** dialog box for a group includes the **Publish** tab where you can see whether the group is published. From that tab you can also publish or unpublish the group as well as specify who you want to approve changes to the group. The **Unpublish** command on a published group provides another way stop publishing the group, which effectively removes the group from the "Published Groups" Managed Unit.

By default, the "Published Groups" Managed Unit has an Access Template applied to it that gives the authenticated users the right to add or remove their own accounts from groups. This Access Template, called "Self-Service - My Memberships Management," defines the following permissions as applied to the group object type:

- **Add/Remove self as member** Enables a user to add or remove the user's own account from membership of a group.
- **List, Read All Properties** Enables users to view a group.

Note that this Access Template does not authorize a user to view a list of groups of which that user is a member—the "Member Of" list. An additional Access Template needs to be applied in order to enable the use of the **My Access** page in Self-Service Manager. The page is intended to display the "Member Of" list for the current user, so users must be given Read access to the "Member Of" property of their own accounts. This can be accomplished by applying the "Self-Service - My Account Management" Access Template to an Organizational Unit or Managed Unit that holds user accounts, with the rights assigned to the built-in account called "Self."

The workflow rules on the published groups are defined by using two pre-defined workflow definitions:

- **Approval by Primary Owner (Manager)** Workflow to enforce the rule that changes to a group must be approved by the primary owner (manager) of the group.
- **Approval by Secondary Owner** Workflow to enforce the rule that changes to a group must be approved by any of the secondary owners of the group.

Each of these workflow definitions is configured to start the approval workflow upon a request to add or remove a member from a group. The workflow start conditions also include a filter to consider the approval options on the group: the first workflow starts if the group is configured to require approval by the primary owner; the second workflow starts if approval by a secondary owner is required.

With group publication, ActiveRoles Server helps reduce administrative overhead and improve productivity by empowering end users to perform group membership management tasks in a framework with delegated self-service. Tight security and approval workflow controls protect the published groups from unwanted access and ensure the accuracy of the membership lists, while Self-Service Manager provides a convenient, easy-to-use interface for managing groups and group memberships.

Membership Self-Management

This new release of ActiveRoles Server extends the capabilities of ActiveRoles Self-Service Manager to let users view or change their memberships in Active Directory groups and Exchange distribution lists. A new section has been added to Self-Service Manager that lists the security and distribution groups of which the current user is a member, enabling the user to join or leave groups as needed.

With the **My Access** section, Self-Service Manager empowers end users to manage their own access needs without involving the help desk and other IT departments. End users can now easily request membership in appropriate security groups allowing access to resources or particular distribution lists where e-mail communication takes place. Group owners can accept or deny requests to join or leave the groups they own, thereby ensuring tight control of group membership lists.

By enabling users to manage their own memberships, Self-Service Manager increases productivity of end users, while freeing up IT from repetitive tasks. Whenever users need additional access to business resources, they can promptly gain the necessary access rights through membership in the appropriate groups. The capabilities provided by ActiveRoles Server for administrative tasks delegation, enforcement of policy rules and approvals, and change tracking ensure that group membership lists are managed in a secure and compliant manner.

Exploring the My Access Page

When you open the **My Access** page in Self-Service Manager, you see a summary screen that lists the security and distribution groups (distribution lists) of which you are a member. With a single click, you can remove yourself from a group you select from the list. With another click, you can examine any of the listed groups in detail.

By default, the **My Access** page lists the groups to which you belong as a direct member. The list can be extended to include all groups of which you are a member, whether directly or indirectly. For example, you might be a direct member of group A which is, in turn, a member of group B. Normally, the list includes only group A, but it is possible to change this behavior so that the list includes both group A and group B.

You can remove yourself from only those groups to which you belong as a direct member. For the groups from which you cannot remove yourself, the check box next to the group name is unavailable. You cannot remove yourself from the groups in which you have indirect membership. Likewise, you cannot do this for your primary group. The name of the primary group is displayed in the lower part of the page.

The **My Access** page lists the groups in which you are a regular member and the groups in which you are a temporal member. Regular members remain in the group for an indefinite period of time whereas temporal members are scheduled to be automatically added or removed from the group at a certain point in time. In the list, an icon of a small clock overlays the icon for the groups in which you are a temporal member. It is possible to hide or display the groups to which you are scheduled to be added in the future. The icons identifying such groups are shown in orange. By changing temporal membership settings on a selection of groups, you can choose the time for you to join or leave those groups.

You can use the **My Access** page to join or leave groups. However, your ability to add or remove yourself from a particular group is restricted with your access rights on that group. By default, average users do not have sufficient rights to add or remove themselves from an arbitrary group. To allow users to join or leave a group, group owners or IT administrators have to give the users the appropriate rights. Normally, this is accomplished by publishing the group to Self-Service Manager. The **My Access** page is mainly intended to enable average users to join or leave published groups. Note that Self-Service Manager obeys all approval rules associated with groups, so your request to join or leave a group may be granted immediately or will be granted when the necessary approvals are performed.

Keyword Search

ActiveRoles Server introduces a new property of groups: keywords. The keywords property on a group can hold multiple string values, which are words or phrases used to identify the group for searching. By using keywords, group owners can optimize search results so as to expose the groups important to self-service users.

ActiveRoles Server provides keyword search mechanism to help organize and expose groups in Self-Service Manager. Users can search for groups by the keywords assigned to each group, in addition to other properties such as the group name, type, or description. With the keyword search capability, self-service users can easily find groups even if they do not know or remember the exact group names.

Making best use of this search capability requires careful thought and consideration when group owners are publishing groups. It is advisable to enter the keywords most likely to describe each group to someone looking for it.

The keyword scheme also lets group owners or IT administrators categorize groups hierarchically. For example, "Accounting" groups might be further subdivided with keywords such as "Accounts Receivable" and "Payroll." By looking for appropriate keywords, a user can find all groups with the "Accounting" keyword, or just a subset with the "Payroll" keyword.

Defining Keywords for Groups

Users who have read and write access to the **Keywords** attribute on a group can view, add, remove or change keywords for that group by using the ActiveRoles Server console or Web Interface.

In the ActiveRoles Server console, the keywords assigned to a group can be administered:

- On the **General** tab in the **Properties** dialog box for that group
- In the dialog box displayed by the **Publish** command on that group

In the Web Interface, the keywords assigned to a group can be administered:

- On the **General** tab of the **General Properties** page for that group
- On the page displayed by the **Publish** command on that group

Searching for Groups by Keyword

In Self-Service Manager, users can submit requests to join groups. Keywords help self-service users locate and select groups they want to join. When searching for groups, the **Select Object** dialog box in Self-Service Manager considers keywords along with group names, so that the search results contain the groups with the names or keywords matching the search string. In addition, the **Keywords** column provides a way to refine the list of search results by filtering groups with particular keywords.

ActiveRoles Server administrators or help-desk technicians can also rely on keywords when searching for groups with the ActiveRoles Server console or Web Interface. In the console, the **Find** dialog box provides the **Keywords** search option for the **Groups** category. Likewise, the **Keywords** option is available on the **Search** page for groups, in the Web Interface site for Administrators and in the Web Interface site for Help Desk.

Recycle Bin

ActiveRoles Server builds on Active Directory Recycle Bin, a new feature of Active Directory Domain Services in Microsoft Windows Server 2008 R2, to facilitate the restoration of deleted objects. When Recycle Bin is enabled, ActiveRoles Server makes it easy to undo accidental deletions, reducing the time, costs, and user impact associated with the recovery of deleted objects in Active Directory.

The use of ActiveRoles Server in conjunction with Active Directory Recycle Bin helps minimize directory service downtime caused by accidental deletions of directory data. Recycle Bin provides the ability to restore deleted objects without using backups or restarting domain controllers and a user interface featured by ActiveRoles Server expedites locating and recovering deleted objects from Recycle Bin. Flexible and powerful mechanisms provided by ActiveRoles Server for administrative tasks delegation, enforcement of policy rules and approvals, and change tracking ensure tight control of the recovery processes.

To undo deletions, ActiveRoles Server relies on the ability of Active Directory Recycle Bin to preserve all attributes, including the link-valued attributes, of the deleted objects. This makes it possible to restore deleted objects to the same state they were in immediately before deletion. For example, restored user accounts regain all group memberships that they had at the time of deletion.

ActiveRoles Server can be used to restore deleted objects in any managed domain that has Active Directory Recycle Bin enabled. This requires the forest functional level of Windows Server 2008 R2, so all the forest domain controllers must be running Windows Server 2008 R2. In a forest that meets these requirements, an administrator can enable Recycle Bin by using the Active Directory module for Windows PowerShell in Windows Server 2008 R2. For more information about Active Directory Recycle Bin, see [What's New in AD DS: Active Directory Recycle Bin](http://go.microsoft.com/fwlink/?LinkId=141392) (<http://go.microsoft.com/fwlink/?LinkId=141392>).

Once Active Directory Recycle Bin is enabled in a managed domain, ActiveRoles Server provides access to the **Deleted Objects** container that holds the deleted objects from that domain. In the ActiveRoles Server console tree or in the Web Interface tree view, the container appears at the same level as the domain itself. If multiple managed domains have Active Directory Recycle Bin enabled, then a separate container is displayed for each domain. To tell one container from another, the name of the container includes the domain name (for example, **MyDomain.MyCompany.com - Deleted Objects**).

Restoring Deleted Active Directory Objects

The task of restoring deleted objects involves two basic elements:

- Find and list deleted objects based on the appropriate search conditions
- Apply the **Restore** command on a deleted object

Find and list deleted objects

Search pages in the ActiveRoles Server console or Web Interface facilitate finding deleted objects, enabling the use of very specific queries based on any object properties. It is also possible to examine and search a list of deleted objects that were in a particular Organizational Unit or Managed Unit at the time of deletion.

The ActiveRoles Server console offers the **Deleted Objects** search category in the **Find** dialog box, which is intended to perform a search in the **Deleted Objects** container of any managed domain where Active Directory Recycle Bin is enabled. The same option is available on the search pages in the Web Interface.

To view and search a list of objects that were deleted from a particular Organizational Unit or Managed Unit, administrators can use the **View or Restore Deleted Objects** command. The command opens a page that lists the deleted objects that were direct children of the corresponding Organizational Unit or Manager Unit at the time of deletion. In the Web Interface, the list can be sorted or filtered as appropriate to locate particular objects. In the ActiveRoles Server console, the **View or Restore Deleted Objects** page can be used to search for deleted objects whose name matches a specific search string. It provides flexible matching by using support for ambiguous name resolution.

Restore a deleted object

For restoring deleted objects ActiveRoles Server offers the **Restore** command that is available from:

- A list of search results prepared using the **Deleted Objects** search category
- The **View or Restore Deleted Objects** page
- A list of objects held in the **Deleted Objects** container

In the ActiveRoles Server console the command can be found on the shortcut menu, which appears when you right-click a deleted object. In the Web Interface, the **Restore** command is available along with other commands on a menu that appears when you click a deleted object in a list.

The **Restore** command opens a page prompting to choose whether deleted child objects (descendants) of the deleted object should also be restored. This option is selected by default, which ensures that the **Restore** command applied on a deleted container object restores the entire contents of the container.

To clarify, consider an example in which an administrator accidentally deletes an Organizational Unit (OU) called Sales_Department that contains a number of user accounts for sales persons along with another OU called Admins that, in turn, contains a user account for an administrative assistant. When applying the **Restore** command on the Sales_Department OU, with the option to restore child objects, ActiveRoles Server performs the following sequence of steps:

1. Restore the Sales_Department OU
2. Restore all the deleted user accounts that were direct children of the Sales_Department OU
3. Restore the Admins OU in the Sales_Department OU
4. Restore all the deleted user accounts that were direct children of the Admins OU

If the option to restore child objects is not selected, ActiveRoles Server performs only the first step, so the restored Sales_Department OU is empty.

Delegating Operations on Deleted Objects

The delegation model based on the ActiveRoles Server Access Templates is fully applicable to the administrative tasks specific to deleted objects. A new Access Template called **All Objects - View or Restore Deleted Objects** makes it easy to delegate the following operations to selected users:

- Viewing deleted Active Directory objects
- Restoring a deleted Active Directory object

When applied to the **Deleted Objects** container, the Access Template gives the delegated users the right to view and restore any deleted object. With the Access Template applied to an Organizational Unit (OU) or a Managed Unit (MU), the delegated users are given the right to view and restore only those deleted objects that were located in that OU or MU at the time of deletion.

Applying Policy or Workflow Rules on Deleted Objects

In addition to the delegation of administrative tasks, ActiveRoles Server provides the ability to establish policy-based control over the process of restoring deleted objects. Policy rules can be used to perform additional verifications or custom script-based actions upon the restoration of deleted objects. Workflow rules can be applied so as to require approval for the restore operation or notify of the restore operation completion via e-mail.

The policy or workflow rules to control the process of restoring or otherwise managing deleted objects can be defined on:

- The **Active Directory** node in the ActiveRoles Server console - The rules defined in this way affect all deleted objects in any managed domain that has ActiveRoles Server Recycle Bin enabled.
- The node representing a domain or the **Deleted Objects** container for that domain in the ActiveRoles Server console - These rules affect all deleted objects in that domain only.
- An Organizational Unit (OU) or Managed Unit (MU) that held the object at the time of deletion - Although the deleted object no longer belongs to that OU or MU, ActiveRoles Server considers the former location of the object so that the rules applied on that location continue to affect the object after the deletion.

For example, an administrator could create a workflow to require approval for the restoration of any user account that was deleted from a certain Organizational Unit (OU). The workflow definition would contain an appropriate approval rule, and have that OU specified as the target container in the workflow start conditions.

Support for Exchange Server 2010

ActiveRoles Server now supports the Exchange recipient management tasks for the earlier versions of Microsoft Exchange Server and Exchange Server 2010 alike. ActiveRoles Server helps you streamline and secure your administration of Exchange Server 2010, through the use of role-based delegation, policy-based administration, flexible administrative views, and comprehensive console and Web-based interfaces to perform recipient management tasks.

Managing Exchange recipients

You can perform recipient management tasks using both the ActiveRoles Server console and the Web Interface. These interfaces support Exchange tasks on mailboxes, mail users and contacts, mail-enabled security and distribution groups, and dynamic (query-based) distribution groups, so you can create, view, and modify Exchange recipients on Exchange Server 2010 the same way you do with earlier versions of Exchange Server.

Delegating recipient management tasks

The ActiveRoles Server delegation model is fully applicable to the management tasks on Exchange Server 2010 recipients. A rich suite of Exchange-specific Access Templates, available out of the box, makes it easy to delegate the management of recipient properties, the use of the Exchange Tasks Wizard, and the management of message settings. Also provided are Access Templates that specify access to individual Exchange-related properties of users, groups, and contacts.

Auto-provisioning of Exchange mailboxes

The provisioning policies included with ActiveRoles Server enable automation of Exchange mailbox creation and management. Exchange Mailbox AutoProvisioning policies can be configured to ensure that mailboxes are created in appropriate mailbox databases, including those of Exchange Server 2010. E-mail Alias Generation policies can be used to automatically assign appropriate e-mail aliases when provisioning mailboxes.

Auto-provisioning of Exchange distribution lists

The Group Family feature of ActiveRoles Server automates the creation of security and distribution groups, including mail-enabled groups or distribution lists. Group Family automatically creates groups and maintains group membership lists in compliance with configurable rules, allowing group membership to be defined as a function of recipient properties in the directory. Group Family also allows for creation of new groups based on new values encountered in recipient properties.

De-provisioning of user mailboxes

The deprovisioning policies included with ActiveRoles Server can be used to automate revocation of user access to Exchange resources on Exchange Server 2010 as well as on earlier versions of Exchange Server. Exchange Mailbox Deprovisioning policies can be configured so that deprovisioning a user causes ActiveRoles Server to make all the necessary changes to deprovision the Exchange resources for that user, such as removing the mailbox from the Global Address List, providing designated persons with access to the mailbox, and adjusting the message forwarding settings on the mailbox.

Exchange resource forest management

An optional add-on application for ActiveRoles Server, ActiveRoles Exchange Resource Forest Manager provides synchronized provisioning and a single console for management of user and mailbox attributes even when mailbox and user accounts are in separate forests. By providing unified user and mailbox management, ActiveRoles Server improves security, saves time and saves money while helping organizations comply with regulatory requirements.

Upgrade from an Earlier Version

If an earlier version of the product is already installed, the Setup program first uninstalls all features of the old version, and then installs the features you have selected from the new version.

Setup allows you to import configuration data stored by the previous version. When upgrading the Administration Service, you have the option to copy all data from the old database to the new one. In this way, Setup ensures that the configuration settings, including all permission and policy definitions and assignments, are identical to those used in the earlier installation.

For more information on how to install or upgrade ActiveRoles Server, see the *ActiveRoles Server Quick Start Guide*.

Components Compatibility

When upgrading ActiveRoles Server components to the new version, keep in mind that the components of the earlier version may not work in conjunction with the components you have upgraded. The new Administration Service is only compatible with the ActiveRoles Server console (MMC Interface) and Web Interface of version 6.5. Earlier versions of the user interfaces will not work with the new Administration Service and thus need to be upgraded. The user interfaces of ActiveRoles Server 6.5 are only compatible with the Administration Service version 6.5. Therefore, to use the ActiveRoles Server console or Web Interface version 6.5, you first need to upgrade the Administration Service.

Upgrade Issues

Impact on ActiveRoles Server Replication

The upgrade process of the Administration Service does not preserve the replication settings. An upgrade can only be performed if the Administration Service is not configured for replication. Before upgrading the Administration Service, you should ensure that it is not configured as a Subscriber or Publisher. Replication for the new Administration Service needs to be configured after the upgrade.

Impact on Custom Solutions

An upgrade of ActiveRoles Server components may affect custom solutions, if any, that rely on the functions of ActiveRoles Server. Custom solutions (such as scripts or other modifications) that work fine with the earlier version of ActiveRoles Server may cease to work after the upgrade. Prior to attempting an upgrade, you should test the existing solutions with the new version of ActiveRoles Server in a lab environment to verify that the solutions continue to work. Should any compatibility issues arise during the test process, you can contact Quest Professional Services for paid assistance with those solutions.

Impact on Dynamic Groups

Beginning with version 6.0, the Administration Service uses a new mechanism for managing Dynamic Groups, so you must upgrade your existing Dynamic Groups after upgrading the Administration Service from version 5.2. For that purpose, the script **DGUpgrade6x.vbs** must be executed on the computer running the Administration Service upgraded to version 6.5. You can find the **DGUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder.

Impact on Mailbox Policies

Beginning with version 6.0, the Administration Service uses a new mechanism for managing mailbox policies, so you must upgrade your existing mailbox policies after upgrading the Administration Service from version 5.2. For that purpose, the script **ExchangePolicyUpgrade6x.vbs** must be executed on the computer running the Administration Service you have upgraded to version 6.5. You can find the **ExchangePolicyUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder.

Impact on Credentials of Override Accounts

Beginning with version 6.0, the Administration Service uses a new, improved algorithm for encrypting security-sensitive data, such as credentials of override accounts. After an upgrade of the Administration Service from version 5.2, ActiveRoles Server cannot read the data that was encrypted earlier. As a result, if a managed domain was registered so that ActiveRoles Server uses an override account rather than the service account to access the domain, the credentials of the override account are lost. You have to re-enter the passwords of the override accounts (if any) after the upgrade. For instructions, refer to the "Upgrading the Administration Service 5.2" section in the *ActiveRoles Server Quick Start Guide*.