NetIQ® Directory and Resource Administrator™ and NetIQ® Exchange Administrator™

Product Overview

July 2017

Legal Notice

NetIQ Directory and Resource Administrator is protected by United States Patent No(s): 6,792,462.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2017 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About this Book and the Library

The *Product Overview* provides information about new features of the NetIQ Directory and Resource Administrator product (Directory and Resource Administrator) and the NetIQ Exchange Administrator product (Exchange Administrator). This book defines terminology and includes implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

User Guide

Provides conceptual information about DRA and ExA. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

Administrator Guide

Provides conceptual information about the Directory and Resource Administrator (DRA) and Exchange Administrator (ExA) products. This book defines terminology and.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for fields on most windows.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Introduction

NetIQ Enterprise Administration solutions provide enterprise customers with the ability to safely and securely delegate administrative privileges across their Windows server, Active Directory, Group Policy and Exchange server environments. Combined with detailed auditing of and reporting on administrative activities, NetIQ Enterprise Administration solutions provide organizations with unprecedented levels of accountability while reducing the costs associated with daily operations, internal policy, and regulatory compliance activities.

Organizations have increasingly relied upon Active Directory for the central management of identities and for the authentication and authorization of those identities to the network and IT services. However, assuring the security, availability and integrity of Active Directory requires more than just delegating permissions or changing group memberships. IT Governance and auditors also require proof that policies and procedures are enforced, that changes are tracked, and that administrators are not able to manage beyond the scope of their responsibilities.

NetIQ Directory and Resource Administrator (DRA) delivers an unparalleled ability to control who can manage what within Active Directory while protecting the consistency and integrity of its information by validating all administrative changes. Through granular delegation of permissions, robust change management policies, and automation that simplifies workflows, DRA reduces down time and operational risks to Active Directory that are posed by the consequences of malicious or accidental changes.

NetIQ Exchange Administrator (ExA) extends the powerful features of DRA to provide seamless management of Microsoft Exchange. Through a single, common user interface, ExA delivers policy-based administration for the management of directories, mailboxes and distribution lists across your Microsoft Exchange environment.

Together, DRA and ExA provide the solutions you need to control and manage your Active Directory, Microsoft Windows, and Microsoft Exchange environments.

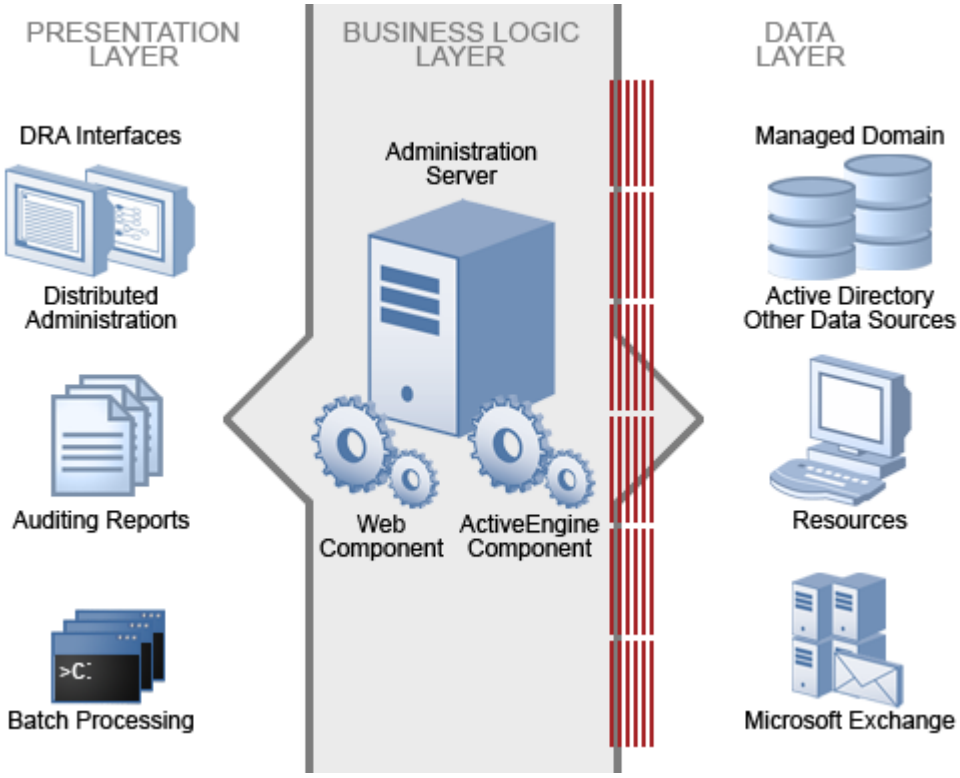
How DRA and ExA Work

DRA and ExA support several open, extensible standards and services. DRA and ExA include the following user-friendly interfaces for Active Directory and Microsoft Exchange:

- Account and Resource Management Console
- Delegation and Configuration Console
- Web Console
- Command-Line Interface (CLI)
- Active Directory Service Interfaces (ADSI)
- Windows Terminal Server (WTS)

These products use the same native interfaces as the native Active Directory and Microsoft Exchange administration consoles. Therefore, DRA and ExA are as secure and reliable as Active Directory and Exchange. These products do not modify Active Directory in any way.

DRA and ExA support a three-tiered architecture that efficiently distributes workload into three functional layers, namely the presentation layer, business logic layer, and data layer. Each layer addresses different processes and functions and enables fast performance and reduced network load.



Presentation Layer

The Presentation layer provides a variety of user interfaces to meet various needs, including distributed administration, auditing and reporting, and batch processing across domains. This layer includes the following interfaces:

Delegation and Configuration Console

Allows administrators to define the security model and associated policies, delegate network administration, report on changes, and perform all administration tasks in an object-oriented workflow. This console is intended for full-time system administrators.

Account and Resource Management Console

Allows Help Desk personnel and departmental administrators to perform various day-to-day user administration and provisioning tasks. This console is intended for Help Desk personnel in their primary job function.

Web Console

Allows users to quickly and easily perform common tasks, such as changing an account password or modifying personal information, from a task-based interface. The Web Console is a Web client for Help Desk personnel, data owners, and occasional administrators who perform occasional administration tasks in addition to their primary job functions.

NetIQ Reporting Center Console

Allows administrators to view and deploy Management reports that include activity reports, configuration reports, and summarization reports. Many of these reports can be viewed in a graphical representation.

Command-Line Interface

Allows an administrator to make modifications from the command-line to implement broad administration changes.

DRA ADSI Provider

Allows administrators develop custom user interfaces and applications, as well as custom policy and automation trigger scripts.

Business Logic Layer

The Business Logic layer establishes a virtual firewall, buffering users from direct interaction with the Data layer. This layer performs the central processing and provides information to the user interfaces. The Business Logic layer also manages Web services, business rules and policy, content integrity, embedded best practices, and transactions across data sources in your enterprise.

The Business Logic layer consists of the NetIQ Administration server (Administration server) and DRA agents. These components work together to efficiently collect information from computers in the managed domains.

Administration Server

The Business Logic layer consists of the NetIQ Administration server (Administration server). The Administration server uses transaction processing to identify and authenticate administrators, enforce policy, automate operations, and log all administration activity. To provide fault tolerance, load balancing, and continuous operation, you can install secondary Administration servers on one or more computers. The Administration server runs as a secure Windows service.

This layer includes the following components:

ActiveEngine component

Runs as a service under an administrator account within the Active Directory. The ActiveEngine component accepts requests from multiple clients in the Presentation layer, and then validates and processes these requests. This component interacts with the Data layer components to retrieve or manage the appropriate information.

NetIQ DRA Core

Runs as a service under an administrator account. The NetIQ DRA Core service collects data from Active Directory and DRA for reporting requests. Additionally, the service generates Activity Detail reports when they are requested from clients in the Presentation layer. This service interacts with the Data layer components to retrieve or manage the appropriate information.

DRA Agents (optional)

DRA collects information for reporting on last logon statistics using DRA agents, which you can optionally install on domain controllers of managed domains.

Log Archive Service

Runs as a service under an administrator account within the Active Directory. The log archive service tracks all DRA activity, compresses the data, and stores it on the Administration server in a secure, tamper-resistant repository. The service also categorizes the audit events and summarizes events based on these categories.

Web component

Runs on a standard Internet Information Server (IIS) computer to provide administration capabilities across your Intranet. The Web component communicates between the ActiveEngine component and the Web Console. This component is required only if you use the Web Console.

Data Layer

The Data layer comprises every network data source. The Administration server manages data stored in the Active Directory and Microsoft Exchange directory. The Data layer can also include other enterprise data sources, such as a Human Resources database. All these data sources provide important information about your enterprise. When the Administration server receives a request from the Business Logic layer, the server validates this request and allows a client to access and modify this data. This additional layer of authentication ensures that your business data remains protected and secure.

DRA and ExA help you use and manage these data sources. These products also let you define and enforce the business rules and policies that can help you keep these data sources current and correct.

How DRA and ExA Help You

Managing Active Directory and Microsoft Exchange mailboxes offers specific challenges for administrators. You can benefit from using DRA and ExA regardless of where your enterprise is in the Microsoft Windows evolution.

Provide Regulatory Compliance

DRA and ExA provide a number of features to help you maintain compliance with the ever-increasing number of regulations your organization must meet. For example, DRA provides the following features:

Recycle Bin

Holds certain inactive objects, like user accounts, groups, contacts, and computer accounts to meet retention policy requirements and helps restore these objects to their original state.

Dual-Key Tasks

Let you require task confirmation by two independent administrators to complete the action.

Policy Enforcement and Automation

Help you define and enforce change management processes, access control, and auditing.

Naming Convention Enforcement

Controls data entries so they comply with specific conventions you establish and maintain data consistency.

Transform User Tasks

Help you control access to resources, pruning unnecessary permissions and adding appropriate permissions when users in your organization change positions.

By providing granular access control and change management for Microsoft Windows permissions, your organization can document its compliance with regulations that affect your industry.

Maintain Control of Active Directory

Using DRA and ExA, you can reduce the number of privileged accounts and provide much more granular access control for administrators, Help Desk personnel, and even your employees. Tightly managing access and permissions helps protect your Microsoft Windows environment from the risks of power escalation or inadvertent security threats. With over 60 roles and more than 300 granular powers, you can always delegate *who can do what to whom or what* to exactly the right person.

DRA and ExA help you maintain control by logging all administrator actions and presenting information in clear and comprehensive reports. DRA includes logging before and after values of changed properties and stores data in a tamper-resistant, write-once technology that stands up to the rigors of chain of custody processes. This accountability helps you meet internal and external audit goals. The Recycle Bin lets you disable unused objects but store information about them to meet retention policy requirements.

Increase Administration Efficiency

DRA allows you to create and use a management model that reflects how you think and work rather than confining you to an inflexible directory topology. For example, IT planners can use the Delegation and Configuration Console to design a dynamic ActiveView security model and delegate administration to span OUs, domains, trees, or forests.

By providing multiple user interfaces, DRA lets you easily delegate other operations to the correct administrator in your organization. IT administrators can manage the logically grouped user accounts, computers, mailboxes, and resources in their ActiveViews using the Account and Resource Management Console. Help Desk personnel can use the Web Console to manage routine user account and mailbox changes.

The DRA dynamic security and management model and role-based user interfaces help streamline Active Directory management and increase efficiency for every level of administrator in your organization. Because DRA and ExA each support multiple versions of Microsoft Windows and Microsoft Exchange, the products provide a unified administrative interface for your entire Microsoft Windows and Microsoft Exchange environment.

Reduce Administration Costs

Automation and extensibility features make DRA and ExA the perfect choice as you seek ways to reduce administration expense. By automating repetitive and complex tasks and using granular delegation, you can enhance your security efforts, improve regulatory compliance, and distribute account administration duties to reduce costs and improve service.

The following features help you automate, streamline, control, audit, and unify user account, computer, mailbox, and resource administration:

- Automation triggers that automatically perform specific tasks before and after an administrator action is completed

- Support for automated, rules-based provisioning of Active Directory based on external datasources
- Scriptable LDAP-compatible ADSI provider so you can query Active Directory and run scripts to automate your routine processes
- SDK that supports multiple development languages, making customized workflows accessible to most organizations
- Domain controller-directed actions let you unlock accounts or reset passwords in near real time to minimize end-user down time caused by replication delay

DRA and ExA can help you slash administrative costs enforcing business and security policies.

Ensure Data Integrity

Managing any data set that contains inconsistencies creates security risks and may interfere with efficient operations. You can publish naming policies and permission guidelines for different accounts, but users may not remember to follow the guidelines. DRA can automatically enforce your policies, ensuring Active Directory consistency and reducing data clutter. DRA and ExA help enforce best practices for change management, access control, and auditing to help you maintain a trouble-free and consistent Active Directory environment.

2 What’s New in This Release

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem.

Feature 1

Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Using Feature 1

At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga.

1. Open.
2. Click.
3. Close.

Feature 2

Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Using Feature 2

At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga.

1. Open.
2. Click.
3. Close.

3 Implementing DRA

This chapter includes scenarios for implementing DRA to solve your top business needs.

Introduction

This will be an introduction to the chapter if needed.

Scenario for Implementing Dynamic Administration across Multiple OUs

This scenario creates and assigns an ActiveView named All Engineering Resources. The All Engineering Resources ActiveView contains resources in multiple OUs for engineering departments across your company. The All Engineering Resources ActiveView allows you to manage these resources collectively even though they are located in different departments or OUs. Your ActiveView could also contain resources across multiple domains and forests, but for simplicity in this example, we will keep it a single domain scenario.

You can also add separate resource ActiveViews to the All Engineering Resources ActiveViews. If these ActiveView names share a common prefix or suffix, you can specify them through a wildcard rule based on a naming convention. For example, to easily add existing ActiveViews to a new ActiveView, name your engineering ActiveViews with an ENG prefix.

Adding one ActiveView to another is called **nesting**. By using nested ActiveViews in your security model, you can divide administration power and scope into smaller pieces and then assemble these pieces to meet different needs. Each ActiveView ensures that the Assistant Admin (AA) works with a complete and accurate set of objects at the appropriate level of power and scope.

To implement this scenario, you must complete the following actions first

1. Log on to the Administration server or DRA client computer with an account that has DRA Admin or Manage Security Model powers in the appropriate domain.
2. Start the Delegation and Configuration console, and then connect to the primary Administration server.

Using the Delegation Wizard to Distribute Administration across OUs

The Delegation Wizard allows you to easily and securely distribute administration across your enterprise. This task includes the following actions:

Specifying ENG Admins AA Group

This action adds a specific person to the ENG Admins AA group. You can specify more than one person, or add members of another group, such as an Active Directory group. You must define AA groups if you plan to limit the scope of policies and triggers. You cannot scope policies and triggers using Active Directory groups.

This action also sets general AA group properties so you can easily audit delegations in your security model.

Assigning Resource Administration Role

This action assigns the built-in Resource Administration role, which includes the powers your AAs need to manage various resources, such as modifying computer accounts, stopping services, or pausing print jobs.

Define All Engineering Resources ActiveView

This action creates an All Engineering Resources ActiveView by including resources from multiple OUs. Specifying an exact domain or OU name improves performance. If you use a group naming convention, you can specify a wildcard value instead. This action also sets general ActiveView properties so you can easily audit delegations in your security model.

You can create AA groups, roles, and ActiveViews before you use the Delegation Wizard to set up your security model. If you are managing a larger environment, you may want to design the scope of your security model before you begin implementation. For more information, see “Scenario for Implementing a Help Desk” on page 19 and “How to Create a Security Model” in the *Administrator Guide*.

To use the Delegation Wizard to manage resources in multiple OUs:

1. In the left pane, click **Delegation Management**.
2. Under Common Tasks in the right pane, click **Delegate Administration**.
3. To specify the Assistant Admin, complete the following steps, and then click **Next**.
   - **3a** On the Assistant Admins tab, click **Add > Users**.
   - **3b** Select the appropriate user account, such as `JSmith`, and then click **OK**.
   - **3c** To save this selection as a new AA group, click **Save this selection**, and then type the appropriate details. For example, you may want to track the following information when you audit or report on your security model configuration.

AA Group Property	Example Information
Name	ENG Admins
Description	Contains any AA who needs to manage objects in engineering OUs
Comment	Members manage engineering objects, such as resources

4 To specify the built-in Resource Administration role, click **Add > Roles** on the Roles and Powers tab, and then click **Next**.

5 To define an ActiveView that includes resources from multiple OUs, complete the following steps for each OU, and then click **Next**.

5a On the ActiveViews tab, click **Add > Objects that match a rule**.

5b Under Resources, click **All Resources**.

5c Select the specific OU that contains the resources you want to manage, and then click **OK**.

6 On the ActiveView Name tab, specify the appropriate details about this new ActiveView, and then click **Next**. For example, you may want to track the following information when you audit or report on your security model configuration.

ActiveView Property	Example Information
Name	All Engineering Resources
Description	Contains resources managed by engineering ActiveViews
Comment	Use to manage all engineering resources

7 Review the summary, and then click **Finish**.

Result: AAs Manage One Dynamic Set of Objects

Because you included resources from different engineering departments, your AAs can manage resources across multiple OUs without changing the underlying configuration of your Active Directory structure. Because your AAs are assigned a built-in role, they can now manage resources for engineering departments across your company regardless of their location.

To implement this scenario in your own security model, identify which OUs you want to include and which AAs you want to grant power in the new ActiveView. You can also create any ActiveView, AA group, or role you need. Before delegating power to an AA group, ensure that this group contains the appropriate user accounts.

If you want to be more granular in granting powers, you can go back and adjust resource rules to include only specific resources. For example, specify services matching "SQL" on those computers to restrict this ActiveView to include only these specific resources on the computers.

Scenario for Implementing a Help Desk

This scenario allows the Houston Help Desk AA group to reset passwords, modify description fields, and unlock user accounts at the Houston facility.

The scenario starts by creating the Houston Help Desk AA group and a Help Desk role. This new role includes the powers to reset passwords, modify description fields, and unlock user accounts. You can create this role by cloning the existing Help Desk Administration role. You can also specify which powers to include in the new Help Desk role, customizing it to fit your particular Help Desk needs.

By using groups and roles to delegate Help Desk tasks, this security model can more effectively respond to change and growth. For example, if you use a naming convention for Houston Help Desk employee user accounts, you can define the Houston Help Desk AA group through a wildcard specification. Then, when a new Help Desk employee is hired, that user account is automatically

added to the Houston Help Desk AA group and given the appropriate powers. With the model in this scenario, your new employee can immediately begin securely administering accounts for the Houston facility.

You can also implement this scenario through the Delegation Wizard. For more information, see "Scenario for Implementing Dynamic Administration across Multiple OUs" on page 17.

To implement this scenario, you must complete the following actions first

1. Log on to the Administration server or DRA client computer with an account that has DRA Admin or Manage Security Model powers in the appropriate domain.
2. Start the Delegation and Configuration console, and then connect to the primary Administration server.

Step 1: Define General Help Desk Role

This step creates a custom Help Desk role by cloning and modifying the built-in Help Desk Administration role. This built-in role already includes many of the powers required for this scenario. You can also define the Help Desk role by creating a new role and then adding the required powers.

TIP: This new role is not specific to the Houston Help Desk. You can reuse the General Help Desk role for other Help Desks at other facilities. For example, you can assign the General Help Desk role to the San Jose Help Desk, giving the San Jose Help Desk group the same set of powers. By reusing roles, you can ensure uniform administration across your company.

This step consists of the following actions:

Adding powers to your custom role

Because you cloned the Help Desk Administration role, your custom Help Desk role does not contain all the powers you want.

Removing unwanted powers from your custom role

Because you cloned the Help Desk Administration role, your custom Help Desk role contains some unnecessary powers.

Specifying Help Desk role properties

This action sets general role properties so you can easily audit delegations in your security model.

To define the Help Desk role:

1. Expand **Delegation Management** in the left pane.
2. Click **Roles**.
3. Select the **Help Desk Administration** role in the right pane.
4. On the Tasks menu, click **Clone**.
5. On the Included Roles and Powers tab, click **Add > Powers** to include the Modify User Comment power.
6. Remove the following powers. Select these powers from the provided list, and then click **Remove**.
   - Disable User Account
   - Enable User Account
   - View All Exchange Properties

7 On the General tab, specify the following information about this new role:

   7a In the **Name** field, type `Help Desk`.

   7b In the **Description** field, type `Reset passwords, unlock user accounts, view user account properties, modify user account descriptions`.

   7c In the **Comment** field, type `Use this role instead of Help Desk Administration`.

8 On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.

9 Click **Finish**.

Step 2: Define Houston Help Desk AA Group

This step creates a new AA group. If you already have a Help Desk group, you can specify the existing group. You can then modify the group definition to include the appropriate user accounts.

TIP: To improve performance, use group membership to add user accounts to an AA group. For more information, see “Optimizing Your ActiveView Rules” in the *Administrator Guide*.

This step consists of the following actions:

Adding members to the Houston Help Desk AA group

This action uses a naming convention to specify user accounts from the Houston Help Desk department. It assumes all accounts for the Houston Help Desk personnel start with HouHD. You can specify any appropriate user accounts or groups.

Specifying Houston Help Desk AA group properties

This action sets general AA group properties so you can easily audit delegations in your security model.

To define the Houston Help Desk AA group:

1 Click **Delegation Management** in the left pane.

2 On the Tasks menu, click **New > New Assistant Admin Group**.

3 On the Group Members tab, add Houston Help Desk employees to the AA group by completing the following steps:

   3a Click **Add > Objects that match a rule**.

   3b Click **All users > Users Matching Wildcard**.

   3c Type `HouHD*`, and then click **OK**.

   3d In the Name field, type `All Houston Help Desk Employees`.

   3e Click **OK**.

4 On the General tab, specify the following information about this new AA group:

   4a In the **Assistant Admin Name** field, type `Houston Help Desk`.

   4b In the **Description** field, type `Contains employees of the Houston Help Desk`.

   4c In the **Comment** field, type `Members manage all Houston user accounts in the Houston Help Desk AV`.

5 On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.

6 Click **Finish**.

Step 3: Define Houston Users ActiveView

This step creates and defines a new ActiveView. If you already have a ActiveView that includes user accounts from the appropriate OU, you can use this existing ActiveView.

NOTE

- Wildcard specifications allow you to include objects from several domains or OUs while making your security model more dynamic. If you need to manage objects across multiple domains or OUs, and you have established naming conventions, wildcard specifications may be more appropriate for your enterprise.
-
- If you select **Domains Matching Wildcard**, the Administration server populates the ActiveView based on the domain type. For Microsoft Windows domains, the Administration server matches the computer name portion of the DNS name. For example, if you specify a wildcard of `*mkg*`, the ActiveView will include objects from a domain with the DNS `mkg01.north.acme.com`. The ActiveView will not include objects from a domain with the DNS `prodserver.north.mkg.acme.com`.

This step consists of the following actions:

Adding user accounts from the Houston OU

This action adds user accounts from a specific OU. Specifying an exact domain or OU name improves performance. However, if you want to add multiple OUs or domains, you can use a wildcard specification instead.

Specifying Houston Users ActiveView properties

This action sets general ActiveView properties so you can easily audit delegations in your security model.

To define the Houston Users ActiveView:

1. Click **Delegation Management** in the left pane.
2. On the Tasks menu, click **New > New ActiveView**.
3. On the Rules tab, add user accounts from the Houston OU by completing the following steps:
   - **3a** Click **Add > Objects that match a rule**.
   - **3b** Click **Users**.
   - **3c** Click **any OU > Specific OU**.
   - **3d** Select the Houston OU, and then click **OK**.
   - **3e** In the Name field, type `Include Houston user accounts`.
   - **3f** Click **OK**.
4. On the General tab, specify the following information about this new ActiveView:
   - **4a** In the **ActiveView Name** field, type `Houston Users`.
   - **4b** In the **Description** field, type `Contains user accounts from the Houston OU`.
   - **4c** In the **Comment** field, type `Used by Houston Help Desk to manage all Houston user accounts`.
5. On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.
6. Click **Finish**.

Step 4: Assign Houston Help Desk AA Group, Help Desk Role, and Houston Users ActiveView

This step assigns the Houston Help Desk AA group to the Houston Users ActiveView, and delegates the powers included in the custom Help Desk role. If you do not complete this assignment, delegation does not occur and the Houston Help Desk AA group will not be able to managed accounts specified by the Houston Users ActiveView.

To assign the Houston Help Desk AA group to the Help Desk role and the Houston Users ActiveView:

1. Click **Delegation Management** in the left pane.
2. Click **Delegate Administration** under Common Tasks in the right pane.
3. On the Assistant Admins tab, specify the Houston Help Desk AA group by completing the following steps:
   - **3a** Click **Add**, and then click **Advanced > Assistant Admin Groups**.
   - **3b** Select the Houston Help Desk AA group.
   - **3c** Click **OK**.
4. On the Roles and Powers tab, specify the General Help Desk role by completing the following steps:
   - **4a** Click **Add > Roles**.
   - **4b** Select the General Help Desk role.
   - **4c** Click **OK**.
5. On the ActiveViews tab, specify the Houston Users ActiveView by completing the following steps:
   - **5a** Click **Add > ActiveViews**.
   - **5b** Select the Houston Users ActiveView.
   - **5c** Click **OK**.
6. Review the summary, and then click **Finish**.

Result: Help Desk Team Can Perform Requested Tasks

Because you created an ActiveView that contains user accounts from the Houston OU, your AAs can manage these accounts from a single interface. Because your AAs are associated with a role, they can perform the expected Help Desk services you need to provide to the Houston facility. As the company grows, you can assign this role to Help Desk departments at other facilities, enforcing consistent permissions across the company.

To implement this scenario in your own security model, first identify what jobs need to be accomplished and who needs to accomplish them. These answers will help you determine which roles, AA groups, and ActiveViews you need. You can create any ActiveView, AA group, or role. Before delegating power to an AA group, ensure that this group contains the appropriate user accounts.

ActiveViews for Microsoft Exchange Management

This scenario implements a Microsoft Exchange Templates ActiveView that allows AAs in Minneapolis to create mail-enabled user accounts with consistent, set properties by using a template to clone user accounts with mailboxes.

This scenario starts by creating the User Admins AA group and creating a new role: the Clone and Move User role. This new role includes powers to clone a user account with a Microsoft Exchange mailbox, view the account and mailbox properties, and copy the new user account to another ActiveView.

To accommodate different account configurations for different departments, you can create individual templates for each department or location. You can also use this scenario as a basis for creating other object templates.

By using templates, this security model ensures data consistency across the enterprise while streamlining the administration workflow. Template objects allow your AAs to quickly and easily create objects with the appropriate properties and settings. You can also establish policies, such as property validation, to further secure your enterprise data and maintain data integrity.

To prepare for this scenario:

1. Create a Templates OU to contain your template objects.
2. Create a template user account and set the appropriate properties.

   If an existing user account already has the appropriate properties set, you can clone this account and modify the new template account as needed.
3. Create a template Microsoft Exchange mailbox for this user account and set the appropriate properties. If an existing mailbox already has the appropriate properties set, you can clone this mailbox, modify the new template mailbox as needed, and assign the template mailbox to the template account.

You can also implement this scenario through the Delegation Wizard. For more information, see “Scenario for Implementing Dynamic Administration across Multiple OUs” on page 17.

To implement this scenario:

1. Log on to the Administration server or DRA client computer with an account that has DRA Admin or Manage Security Model powers in the appropriate domain.
2. Start the Delegation and Configuration console, and then connect to the primary Administration server.

Step 1: Define Clone and Transfer User Role

This task creates a new role. If you already have a similar role, you can clone the existing role to create this new role. You can then modify the role definition to include the appropriate powers.

This step consists of the following actions:

Adding roles and powers to your custom role

This action ensures your new role contains the appropriate roles and powers for this scenario.

Specifying Clone and Move User role properties

This action sets general role properties so you can easily audit delegations in your security model.

TIP

- To allow an AA to modify properties for the cloned user account and mailbox, assign the appropriate powers, such as Modify General Exchange Mailbox Properties.
- This new role is not specific to the Minneapolis Admins. You can reuse the Clone User with Mailbox role for other AAs at other facilities. For example, you can assign the Clone User with Mailbox role to the New York AAs, giving these AAs the same set of powers. By reusing roles, you can ensure uniform administration across your company.

To define the Clone and Move User role:

1. Click **Delegation Management** in the left pane.
2. On the Tasks menu, click **New > New Role**.
3. On the Included Roles and Powers tab, complete the following steps:
   - **3a** Click **Add > Roles** to include the Clone User with Mailbox role.
   - **3b** Click **Add > Powers** to include the Copy User to Another ActiveView power.
   - **3c** Click **Next**.
4. On the General tab, specify the following information about this new role:
   - **4a** In the **Name** field, type `Clone and Move User`.
   - **4b** In the **Description** field, type `Contains powers to clone user accounts with mailboxes and move these accounts to another ActiveView`.
   - **4c** In the **Comment** field, type `Use to create new accounts with mailboxes by cloning template user accounts and mailboxes`.
5. On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.
6. Click **Finish**.

Step 2: Define User Admins AA Group

This step creates a new AA group that includes members of the Minneapolis Admins group. This new AA group is not specific to the Minneapolis Admins. To expand the scope and flexibility of your security model, you can add other user accounts and groups to this AA group, or associate this AA group with other roles and ActiveViews.

This step consists of the following actions:

Defining the User Admins AA group

This action uses a group membership definition to specify user accounts in the Minneapolis Admins group. Using a group membership definition to add user accounts to another group improves performance. For more information, see “Optimizing Your ActiveView Rules” in the *Administrator Guide*.

Specifying User Admins AA group properties

This action sets general AA group properties so you can easily audit delegations in your security model.

To define the User Admins AA group:

1. Click **Delegation Management** in the left pane.
2. On the Tasks menu, click **New > New Assistant Admin Group**.

3 On the Group Members tab, click **Add > Groups** to include the Minneapolis Admins group.

4 On the General tab, specify the following information about this new AA group:

4a In the **Name** field, type `User Admins`.

4b In the **Description** field, type `Includes user accounts from the Minneapolis Admins administrator group`.

4c In the **Comment** field, type `Use for user administration only`.

5 On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.

6 Click **Finish**.

Step 3: Define User Mailbox Templates ActiveView

This step creates and defines a new ActiveView. If you already have a similar ActiveView, you can create a new ActiveView by cloning the existing ActiveView. You can then modify the ActiveView definition to include the appropriate template accounts.

NOTE: This step assumes you created a Template OU that contains various template objects, including a template user account with a Microsoft Exchange mailbox.

This step consists of the following actions:

Adding template user account

This action adds a specific template user account from a Templates OU in a specific domain. Specifying an exact account and OU name improves performance but, if you use a naming convention, you can specify a wildcard value instead. For more information, see “Optimizing Your ActiveView Rules” in the Administrator Guide.

Specifying the Users built-in container as the target container

This action allows AAs to create the new user accounts in the Users built-in container.

Specifying Exchange Templates ActiveView properties

This action sets general ActiveView properties so you can easily audit delegations in your security model.

To define the Exchange Templates ActiveView:

1 Click **Delegation Management** in the left pane.

2 On the Tasks menu, click **New > New ActiveView**.

3 On the Rules tab, add the appropriate template accounts by completing the following steps:

3a Click **Add > Objects that match a rule**.

3b Click **User**.

3c Click **any User > Specific User**.

3d Select the template user account, and then click **OK**.

3e In the **Name** field, type `Include template user with Exchange mailbox`.

3f Click **OK**.

4 To specify the target container, complete the following steps:

4a On the Rules tab, click **Add > Target containers for create operations**.

4b Select the appropriate OU, such as the Users built-in container, and then click **OK**.

5 On the General tab, specify the following information about this new ActiveView:

5a In the **Name** field, type `User Mailbox Templates`.

5b In the **Description** field, type `Contains template user accounts with Exchange mailboxes from the Templates OU`.

5c In the **Comment** field, type `Used by the User Admins AA group to create mailbox-enabled user accounts`.

6 On the Summary tab, clear the checkbox allowing you to automatically launch the Delegation Wizard.

7 Click **Finish**.

Step 4: Assign Clone and Move User Role, User Admins AA Group, and User Mailbox Templates ActiveView

This step assigns the User Admins AA group to the User Mailbox Templates ActiveView, and delegates the powers included in the custom Clone and Move User role. If you do not complete this assignment, delegation does not occur and the User Admins AA group will not be able to clone user accounts specified by the User Mailbox Templates ActiveView.

To assign the User Admins AA group to the Clone and Move User role and the User Mailbox Templates ActiveView:

1 Click **Delegation Management** in the left pane.

2 Click **Delegate Administration** under Common Tasks in the right pane.

3 On the Assistant Admins tab, specify the User Admins AA group by completing the following steps:

3a Click **Add**, and then click **Advanced > Assistant Admin Groups**.

3b Select the User Admins AA group.

3c Click **OK**.

4 On the Roles and Powers tab, specify the Clone and Move User role by completing the following steps:

4a Click **Add > Roles**.

4b Select the Clone and Move User role.

4c Click **OK**.

5 On the ActiveViews tab, specify the User Mailbox Templates ActiveView by completing the following steps:

5a Click **Add > ActiveViews**.

5b Select the User Mailbox Templates ActiveView.

5c Click **OK**.

6 Review the summary, and then click **Finish**.

Result: Use Preset Template to Clone User Accounts and Mailboxes

Because you created an ActiveView that contains a mail-enabled template user account with set properties, you can reduce the administration workload and ensure consistency across your enterprise. Because the Minneapolis AAs are members of a generic AA group, you can quickly and easily assign these AAs to other tasks. As the company grows or responsibilities change, you can add other AAs to this AA group, immediately providing access to the necessary tasks.

NOTE

- To ensure data consistency across your enterprise, you can use property validation policies to limit which values the AA can enter for account and mailbox properties. For more information about property validation policy, see “Implementing Default Policies” in the *Administrator Guide*.
- You can use proxy generation rules to automate the creation of email addresses. For more information about automating email address management, see “Proxy Generation Policy” in the *Administrator Guide*.

To implement this scenario in your own security model, first identify what jobs need to be accomplished and who needs to accomplish them. These answers will help you determine which roles, AA groups, and ActiveViews you need. You can also create any ActiveView, AA group, or role. Before delegating power to an AA group, ensure this group contains the appropriate user accounts.

Scenario for Including the Recycle Bin in Your Security Model

This scenario allows you to restore accounts to the Chicago OU from the Recycle Bin or delete these accounts from the Recycle Bin.

The scenario starts when you create the Recycle Bin AA group. This group includes the AAs who will be responsible for restoring users, groups, contacts, and computer accounts to the Chicago OU. You can create this group by cloning an existing AA group. You can also modify Recycle Bin AA group membership, customizing it to fit your particular needs.

The scenario also creates a Midwest ActiveView that includes the Chicago OU and delegates the following powers to the Recycle Bin group:

- Delete User from Recycle Bin
- Restore User from Recycle Bin
- Delete Group from Recycle Bin
- Restore Group from Recycle Bin
- Delete Computer from Recycle Bin
- Restore Computer from Recycle Bin
- Delete Contact from Recycle Bin
- Restore Contact from Recycle Bin
- View All Recycle Bin Objects

By creating an ActiveView that delegates Recycle Bin administration for the appropriate OUs, this security model can more effectively respond to change and growth. For example, if you use a naming convention for your OUs, you can define the ActiveView through a wildcard specification. Then, when

you create a new OU in the managed domain, DRA automatically adds the OU to the corresponding ActiveView. Also, because this scenario separates Recycle Bin administration from account management, you can delegate other powers over specific sets of accounts without granting power to permanently delete accounts.

With the model in this scenario, your AAs can immediately restore deleted accounts from any OU in any domain, and you can maintain a secure Active Directory.

To implement this scenario, you must complete the following tasks:

1. Log on to the Administration server or DRA client computer with an account that has DRA Admin or Manage Security Model powers in the appropriate domain.
2. Start the Delegation and Configuration console, and then connect to the primary Administration server.
3. Enable the Recycle Bin for the appropriate domain.

Using the Delegation Wizard to Implement the Recycle Bin

The Delegation Wizard allows you to easily and securely distribute administration across your enterprise. This task includes the following actions:

Specifying the Recycle Bin AA group

This task adds a specific user to the Recycle Bin AA group. You can specify more than one user, or add members of another group. For example, you could use a naming convention to specify users from the Houston Help Desk department. For more information about incorporating a help desk into your security model, see the Getting Started Guide.

This action also sets general AA group properties so you can easily audit delegations in your security model.

Specifying Recycle Bin powers

This task delegates the following powers from the Recycle Bin powers:

- Delete User from Recycle Bin
- Restore User from Recycle Bin
- Delete Group from Recycle Bin
- Restore Group from Recycle Bin
- Delete Computer from Recycle Bin
- Restore Computer from Recycle Bin
- Delete Contact from Recycle Bin
- Restore Contact from Recycle Bin
- View All Recycle Bin Objects

Adding the Chicago OU to the Midwest Recycle Bin ActiveView

This task adds a specific OU and its contents. Specifying an exact domain or OU name improves performance, but you can specify a wildcard value instead. This action sets general ActiveView properties so you can easily audit delegations in your security model.

TIP

- You can create AA groups, roles, and ActiveViews before you use the Delegation Wizard to set up your security model. If you are managing a larger environment, you may want to design the scope of your security model before you begin implementation. For more information, see How to Create a Security Model and the Getting Started Guide.
- If you are implementing the Recycle Bin to manage accounts from multiple OUs or multiple domains, include these OUs and domains in this ActiveView.

To use the Delegation Wizard to restrict group management:

1. In the left pane, click **Delegation Management**.
2. Under Common Tasks in the right pane, click **Delegate Administration**.
3. Click **Next**.
4. To specify the Assistant Admin, complete the following steps, and then click **Next**.
   - **4a** On the Assistant Admins tab, click **Add > Users**.
   - **4b** Select an appropriate user account, and then click **OK**.
   - **4c** To save this selection as a new AA group, click the **Save this selection as an Assistant Admin Group** check box, and then type the necessary details. For example, you may want to track the following information when you audit or report on your security model configuration.

AA Group Property	Example Information
Name	Recycle Bin
Description	Contains any AA who needs to restore and delete accounts from Recycle Bin
Comment	Members manage all accounts in the Recycle Bin

5. To specify the appropriate Recycle Bin powers, complete the following steps, and then click **Next**.
   - **5a** On the Roles and Powers tab, click **Add > Powers** to specify the following powers:
     - Delete User from Recycle Bin
     - Restore User from Recycle Bin
     - Delete Group from Recycle Bin
     - Restore Group from Recycle Bin
     - Delete Computer from Recycle Bin
     - Restore Computer from Recycle Bin
     - Delete Contact from Recycle Bin
     - Restore Contact from Recycle Bin
     - View All Recycle Bin Objects
   - **5b** Click **OK**.

6 To define an ActiveView that includes the accounts you want to delete through the Recycle Bin, complete the following steps, and then click **Next**.

   6a On the ActiveViews tab, click **Add > Domains, OUs, and Containers**.

   6b Select the appropriate OU.

   6c Click **OK**.

7 On the ActiveView Name tab, specify the appropriate details about this new ActiveView, and then click **Next**. For example, you may want to track the following information when you audit or report on your security model configuration.

Active View Property	Example Information
Name	Midwest Recycle Bin
Description	Contains the Chicago OU
Comment	Use to delegate power to the Recycle Bin AA group for all Chicago accounts

8 Review the summary, and then click **Finish**.

Result: Securely Manage Deleted User Accounts

Because you created an ActiveView that contains accounts from the Chicago OU, you can delegate additional powers so your AAs can effectively manage accounts in this OU. As your enterprise needs change, you can give different AA groups different powers over the same set of accounts. Because you created an ActiveView that contains the Chicago OU, you can provide Recycle Bin administration for the appropriate accounts without compromising your Active Directory security. As the company grows, you can include OUs from other domains, implementing the Recycle Bin across your company while maintaining control through a single point of reference.

To implement this scenario in your own security model, first identify which domains require secure account deletion and which OUs contain these accounts. These answers help you determine which roles, AA groups, and ActiveViews you need. You can also create any ActiveView, AA group, or role. Before assigning powers to an AA group, ensure that this group contains the appropriate user accounts.

Scenario for Restricting Management of Groups in an ActiveView

This scenario creates an Atlanta Groups ActiveView that allows specific AAs to modify group memberships for the Marketing and Sales departments in Atlanta. In this scenario, the assigned AAs can fully manage the Atlanta Marketing group but cannot clone, move, or change group membership for the Atlanta Sales group.

By restricting management of an object, you can further control the power an AA has to modify that object. Restrictions provide an extra layer of security.

To implement this scenario, you must complete the following actions first:

1. Log on to the Administration server or DRA client computer with an account that has DRA Admin or Manage Security Model powers in the appropriate domain.
2. Start the Delegation and Configuration console, and then connect to the primary Administration server.

Using the Delegation Wizard to Restrict Group Management

The Delegation Wizard allows you to easily and securely distribute administration across your enterprise. This task includes the following actions:

Adding JSmith to the Atlanta Group Admins AA group

This action adds a specific person to the Atlanta Group Admins AA group. You can specify more than one person, or add members of another group. This action also sets general AA group properties so you can easily audit delegations in your security model.

Specifying the Manage Group Memberships role

This action specifies the built-in Manage Group Memberships role, which provides the powers your AAs need to add and remove objects from groups.

Defining Atlanta Groups ActiveView

This action adds the Atlanta Marketing and Sales groups in the Atlanta OU to the Atlanta Groups ActiveView. Specifying an exact domain or OU name improves performance. If you use a group naming convention, you can specify a wildcard value instead. This action also sets general ActiveView properties so you can easily audit delegations in your security model.

You can create AA groups, roles, and ActiveViews before you use the Delegation Wizard to set up your security model. If you are managing a larger environment, you may want to design the scope of your security model before you begin implementation. For more information, see the Getting Started Guide and How to Create a Security Model.

To use the Delegation Wizard to restrict group management:

1. In the left pane, click **Delegation Management**.
2. Under Common Tasks in the right pane, click **Delegate Administration**.
3. To specify the Assistant Admin, complete the following steps, and then click **Next**.
   - **3a** On the Assistant Admins tab, click **Add > Users**.
   - **3b** Select the appropriate user account, such as `JSmith`, and then click **OK**.
   - **3c** To save this selection as a new AA group, click **Save this selection**, and then type the appropriate details.

For example, you may want to track the following information when you audit or report on your security model configuration.

AA Group Property	Example Information
Name	Atlanta Group Admins
Description	Contains any AA who needs to manage Atlanta groups
Comment	Members manage user accounts in the Atlanta groups

4 To specify the built-in Manage Group Memberships role, click **Add > Roles** on the Roles and Powers tab, and then click **Next**.

5 To define an ActiveView that restricts group management, complete the following steps, and then click **Next**.

- **5a** On the ActiveViews tab, click **Add > Groups**.
- **5b** Select the Atlanta Marketing and Atlanta Sales groups from the Atlanta OU, and then click **OK**.
- **5c** Select the ActiveView rule you want to restrict, such as the rule that includes the Atlanta Sales group.
- **5d** Click **Options > Restrict Usage**.
- **5e** Select the appropriate restriction. For example, you can prevent the Atlanta Sales group from being cloned, moved, or added to other groups.

6 On the ActiveView Name tab, specify the appropriate details about this new ActiveView, and then click **Next**.

For example, you may want to track the following information when you audit or report on your security model configuration.

Active View Property	Example Information
Name	Atlanta Groups
Description	Contains groups from the Atlanta OU
Comment	Used by the Atlanta Group Admins AA group to manage group memberships

7 Review the summary, and then click **Finish**.

Result: Use One ActiveView to Restrict Actions on Multiple Groups

Because you created an ActiveView that contains groups from the Atlanta OU, your AAs can manage these groups from a single interface. Because you set restrictions on some groups but not others, you can control how the AAs manage different objects in the same ActiveView. These restrictions provide flexibility as well as additional security, so you do not need to implement multiple ActiveViews to address your group administration needs.

To implement this scenario in your own security model, first identify what jobs need to be accomplished and who needs to accomplish them. These answers will help you determine which roles, AA groups, and ActiveViews you need. You can also create any ActiveView, AA group, or role. Before assigning powers to an AA group, ensure this group contains the appropriate user accounts.

Implementing Custom User Interface Extensions

You can customize and extend the DRA consoles by implementing user interface extensions. User interface extensions allow you to add proprietary account and OU properties, such as Active Directory schema extensions and virtual attributes, to specific wizards and property windows. These extensions allow you to customize DRA to meet your specific requirements. Using the New Custom Page wizard in the Delegation and Configuration console, you can quickly and easily create a custom page to extend the appropriate user interface.

If your AAs require unique powers to securely manage the custom page, you can also create and delegate custom powers. For example, you may want to limit user account management to properties on the custom page only. For more information, see Understanding Power Creation.

How User Interface Extensions Work

User interface extensions are custom pages DRA displays in the appropriate wizard and properties windows. You can configure custom pages to expose Active Directory attributes, schema extensions, and virtual attributes in the Delegation and Configuration console and the Account and Resource Management console.

When you select any supported Active Directory attribute, schema extension, or virtual attribute, you can use custom pages in the following ways:

- Limit AAs to manage a well-defined and controlled set of properties. This property set can include *standard properties* and schema extensions. Standard properties are Active Directory attributes exposed by default through the Accounts and Resource Management console.
- Expose Active Directory attributes other than the standard properties managed by DRA.
- Extend the Account and Resource Management console and Delegation and Configuration console to include proprietary properties.

You can also configure how DRA displays and applies these properties. For example, you can define user interface controls with default property values.

DRA applies custom pages to all applicable managed objects in your enterprise. For example, if you create a custom page to add Active Directory schema extensions to the Group Properties window, DRA applies the properties on this page to each managed group in a domain supporting the specified schema extensions. Each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

You cannot disable individual windows or tabs in the existing user interface. An AA can select a property value using either the default user interface or a custom page. DRA applies the most recently selected value for a property.

DRA provides a full audit trail for user interface extensions. DRA logs the following data to the Application event log:

- Changes to custom pages
- Creation and deletion of custom pages
- Exposed schema extension, Active Directory attributes, and virtual attributes included on custom pages

You can also run change activity reports to monitor configuration changes for the user interface extensions.

Implement and modify user interface extensions (custom pages) from the primary Administration server. During synchronization, DRA replicates user interface extension configurations across the Multi-Master Set.

Supported Custom Pages

Each custom page you create allows you to select a set of Active Directory properties, schema extensions, or virtual attributes and expose these properties as a custom tab. You can create the following types of custom pages:

Custom User Page

Allows you to display custom tabs in the following windows:

- User Properties window
- Create User wizard
- Clone User wizard

Custom Group Page

Allows you to display custom tabs in the following windows:

- Group Properties window
- Create Group wizard
- Clone Group wizard

Custom Computer Page

Allows you to display custom tabs in the following windows:

- Computer Properties window
- Create Computer wizard

Custom Contact Page

Allows you to display custom tabs in the following windows:

- Contact Properties window
- Create Contact wizard
- Clone Contact wizard

Custom OU Page

Allows you to display custom tabs in the following windows:

- OU Properties window
- Create OU wizard
- Clone OU wizard

Supported User Interface Controls

When you add an Active Directory attribute, schema extension, or virtual attribute to a custom page, you also configure the user interface control with which an AA inputs the property value. For example, you can specify property values in the following ways:

- Define specific value ranges
- Set default property values
- Indicate whether a property is required

You can also configure the user interface control to display proprietary information or instructions. For example, if you define a specific range for an employee identification number, you can configure the text box control label to display **Specify employee identification number (001 to 100)**.

Each user interface control provides support for a single Active Directory attribute, schema extension, or virtual attribute. Configure the following user interface controls based on the property type:

Type of Active Directory attribute	Supported User Interface Controls
Boolean	Check box
Date	Calendar control
Integer	Text box (default) Selection list
String	Text box (default) Selection list Object selector
Multivalued String	Selection list

Implementing User Interface Extensions

User interface extensions, such as custom pages, allow you to extend and customize the user interface. For each customization you want to configure, create a custom page and assign the appropriate power or role to the AA.

To implement user interface extensions:

1. To ensure DRA recognizes your Active Directory attributes, schema extension attributes, or virtual attributes, restart the NetIQ Administration Service service on each Administration server.

2 Identify the type of custom page you want to create and the properties you want AAs to manage with this custom page. You can select any Active Directory attribute, including schema extension attributes and attributes in existing DRA wizards and property windows or any virtual attribute you create. However, each custom page requires a unique set of properties. You cannot add an Active Directory attribute to more than one custom page.

   Custom pages do not replace the existing user interface. For more information, see "How User Interface Extensions Work" on page 34 and "Supported Custom Pages" on page 35.

3 Determine how you want AAs to specify these properties. For example, you may want to limit a specified property to three possible values. You can define an appropriate user interface control for each property. For more information, see "Supported User Interface Controls" on page 36.

4 Determine whether your AAs need proprietary information or instructions to successfully manage these properties. For example, determine whether Active Directory requires a syntax for the property value, such as a distinguished name (DN) or an LDAP path.

5 Identify the order in which these properties should display on the custom page. You can change the display order at any time.

6 Determine how DRA should use this custom page. For example, you can add a user custom page to the New User wizard and the User Properties window.

7 Using your answers from Step 1 on page 36 through Step 5 on page 37, create the appropriate custom pages. For more information, see "Creating User Interface Extensions" on page 37.

8 Determine whether your AAs need a custom power to manage the properties on this page. For example, if you add a custom page to the User Properties window, delegating the Modify All User Properties power may give an AA too much power. Create any custom powers needed to implement your custom page. For more information, see Understanding Power Creation.

9 Use the Assignments tab on the AA details pane to verify that your AAs have the appropriate powers for the correct set of objects. If you created custom powers for this custom page, delegate those powers to the appropriate AAs.

10 Distribute information about the user interface extensions you implemented to the appropriate AAs, such as your Help Desk.

To implement user interface extensions, you must have the powers included in the DRA Administration role. For more information about custom pages, see "How User Interface Extensions Work" on page 34.

Creating User Interface Extensions

You can create different user interface extensions by creating different custom pages. By default, new custom pages are enabled.

When you create a custom page, you can disable it. Disabling a custom page hides it from the user interface. If you are creating multiple custom pages, you may want to disable the pages until your customizations are tested and complete.

NOTE: Computer accounts inherit Active Directory attributes from user accounts. If you extend your Active Directory schema to include additional attributes for user accounts, you can select these attributes when you create a custom page to manage computer accounts.

To create a user interface extension:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 On the Task menu, click **New**, and then click the appropriate menu item for the custom page you want to create. For example, to create a custom page for the Computer Properties window, click **New > Computer Page**.

4 On the General tab, type the name of this custom page.

DRA enables custom pages by default when you create them. You might prefer to create custom pages without enabling them and then enable them later.

5 ***If you want to disable this page,*** clear the **Enabled** check box.

6 For each property you want to include on this custom page, complete the following steps:

6a On the Properties tab, click **Add**.

6b To select a property, click **Browse**.

6c In the **Control label** field, type the property name DRA should use as the label for the user interface control. Ensure the control label is user-friendly and highly descriptive. You can also include instructions, valid value ranges, and syntax examples.

6d Select the appropriate user interface control from the **Control type** menu.

6e Select where in the Account and Resource Management console you want DRA to display this custom page.

6f To specify additional attributes, such as minimum length or default values, click **Advanced**.

6g Click **OK**.

7 Continue to add, edit, remove, and change the order in which DRA displays these properties on the custom page.

8 Click **Finish**.

If you disabled the user interface extension while you were creating it, you must enable the extension so that DRA displays the custom properties on the wizards and windows you specified in the user interface extension properties.

NOTE: To ensure each custom page exposes a unique set of properties, DRA does not enable custom pages that contain properties exposed on other custom pages.

To enable a user interface extension:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 In the list pane, select the appropriate user interface extension.

4 On the Tasks menu, click **Enable**.

Identifying Active Directory Attributes Managed With User Interface Extensions

You can quickly identify which Active Directory properties, schema extensions, or virtual attributes are managed using a particular user interface extension.

To identify Active Directory properties managed using user interface extensions:

1 In the left pane, expand **Directory and Resource Administrator**.

2 Expand **Configuration Management**, and then click **User Interface Extensions**.

3 In the list pane, select the appropriate user interface extension.

4. In the details pane, click the **Properties** tab. To view the details pane, click **Details** on the View menu.
5. To verify how DRA displays and applies a property, select the appropriate Active Directory attribute, schema extension, or virtual attribute from the list, and then click the **Properties** icon.

Using Policy to Enforce Naming Standards

If you have enabled Microsoft Exchange support, Exchange Administrator allows you to use policies to enforce naming standards.

ExA provides several policies to help you more effectively manage Microsoft Exchange objects. Microsoft Exchange policy allows you to automate mailbox management, enforce naming conventions for aliases and mailbox stores, automatically generate email addresses, and configure Microsoft Exchange support.

These policies help you streamline your workflows and maintain data integrity. For example, you can specify how ExA manages mailboxes when you create, modify, or delete user accounts. To define and manage Microsoft Exchange policies, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role.

Enabling Microsoft Exchange Support

Enabling Microsoft Exchange support allows you to leverage ExA features, such as Microsoft Exchange policies and integrated mailbox and mail-enabled object management. You can enable or disable Microsoft Exchange support for each Administration server. You can also enable support for Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, and Microsoft Exchange Server 2010 on the same Administration server.

To enable Microsoft Exchange support, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product. For more information about Microsoft Exchange requirements, see the *Administration Installation Guide*.

To enable Exchange Administrator:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Select **Enable Exchange Policy** and click **Apply**.

   DRA verifies which versions of the Exchange management tools are installed on the Administration Server and enables the options that allow you to select Exchange support for the appropriate versions.
4. ***If Enable Exchange Policy was already selected and the options that allow you to select Exchange support are not enabled,*** click Refresh to have DRA verify which versions of the Exchange management tools are installed on the Administration Server.
5. To enable Exchange administration support, select the option to enable support of the version of Exchange you intend to manage with this Administration server.
6. ***If you want to use Exchange Server 2010 management tools to manage all versions of Exchange objects in your environment,*** select **Update objects using Exchange 2010**.

NOTE: Managing an object in the Exchange Server 2010 Exchange Control Panel can upgrade the object. As a result, earlier versions of Exchange management tools can no longer manage the object. If you have Exchange environments that you intend to manage with earlier versions of Exchange management tools, do not select this option.

7 Click **OK**.

Automated Naming Policy

Automated naming policy allows you to specify automated naming rules for specific properties of a mailbox. These options allow you to establish naming conventions and quickly generate standard values for the display name, directory name, and alias properties. ExA allows you to specify substitution strings, such as `%First` and `%Last`, for several automated naming options.

When ExA generates a directory name or alias, it checks whether the generated value is unique. If the generated value is not unique, ExA appends a hyphen (-) and a two digit number, starting with `-01`, to make the value unique. When ExA generates a display name, it does not check whether the value is unique.

ExA supports the following substitution strings for automatic naming and proxy generation policies:

`%First`	Indicates the value of the First name property for the associated user account.
`%Last`	Indicates the value of the Last name property for the associated user account.
`%Initials`	Indicates the value of the Initials property for the associated user account.
`%Alias`	Indicates the value of the Alias mailbox property.
`%DirNam`	Indicates the value of the Directory name mailbox property. When generating email addresses for Microsoft Exchange mailboxes, ExA does not support proxy generation strings that specify the `%DirName` variable.
`%UserName`	Indicates the value of the User name property for the associated user account.

You can also specify a number between the percent sign (`%`) and the substitution string name to indicate the number of characters to include from that value. For example, `%2First` indicates the first two characters from the **First** name property of the user account.

Each automatic naming rule or proxy generation policy can contain one or more substitution strings. You can also specify characters in each rule as a prefix or suffix for a specific substitution string, such as a period and space (`.`) following the `%Initials` substitution string. If the property for the substitution string is blank, ExA does not include the suffix for that property.

For example, consider the following auto naming rule for the **Display** name property:

```
%First %1Initials. %Last
```

If the **First** name property is `Susan`, the **Initials** property is `May`, and the **Last** name property is `Smith`, ExA sets the **Display** name property to `Susan M. Smith`.

If the **First** name property is `Michael`, the **Initials** property is blank, and the **Last** name property is `Jones`, ExA sets the **Display** name property to `Michael Jones`.

Specifying Automated Mailbox Naming Policy

To specify automated mailbox naming options, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify automated mailbox naming policy:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Auto naming** under the **Exchange** tab.
4. Specify the appropriate name generation information.

   For more information about supported substitution strings for auto naming rules, see “Automated Naming Policy” on page 40.
5. Select **Enforce alias naming rules during mailbox updates**.
6. Click **OK**.

Specifying Proxy Generation Policy

Proxy generation policy allows you to specify rules for default proxies (email addresses) for mailboxes. When ExA generates a proxy, it checks whether the generated proxy is unique in the Microsoft Exchange server, the global catalog server, and Microsoft Exchange mailboxes. If the proxy is not unique, ExA appends a hyphen (-) and a two digit number, starting with `-01`, to make the proxy unique. If ExA cannot generate a unique proxy, it logs an error message in the application event log and does not create the specified proxy. The proxy generation rule is to create the secondary SMTP address and not to set the primary SMTP address. ExA applies this policy when you create a user account or modify user account properties.

To specify default email address policy, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify default email address policy:

1. In the left pane, click **Policy and Automation Management**.
2. Under Common Tasks in the right pane, click **Configure Exchange Policies**.
3. Click **Proxy generation** under the **Exchange** tab.
4. Specify the domain of the Microsoft Exchange server.
   - **4a** Click **Browse**.
   - **4b** Specify additional search criteria as needed, and then click **Find Now**.
   - **4c** Select the domain to configure, and then click **OK**.
5. Specify the proxy generation rules for the selected domain.
   - **5a** Click **Add**.
   - **5b** Select a proxy type. For example, click **Internet Address**.
   - **5c** Accept the default value or type a new proxy generation rule, and then click **OK**.

     For more information about supported substitution strings for proxy generation rules, see “Automated Naming Policy” on page 40

6 Click **Custom attributes** to edit the custom name of custom mailbox properties.

   6a Select the attribute and click the **Edit** button.

   6b In the Attribute Properties window, enter the attribute name in the **Custom name** field, and click **OK**.

7 Click **OK**.

NOTE: DRA Policy Admins must have the Manage Custom Tools power to modify custom attributes in the Microsoft Exchange policy.

Specifying Mailbox Rules

Mailbox rules let you specify how ExA manages mailboxes when AAs create, clone, modify, or delete user accounts. Mailbox rules automatically manage Microsoft Exchange mailboxes based on how the AA manages the associated user accounts.

NOTE: When enabling the **Do not allow Assistant Admins to create a user account without a mailbox** option in Microsoft Windows domains, ensure the AA has power to either clone or create a user account. Enabling this option requires AAs to create Windows user accounts with a mailbox.

To specify mailbox rules, you must have the appropriate powers, such as those included in the built-in Manage Policies and Automation Triggers role, and your license must support the ExA product.

To specify mailbox rules:

1 In the left pane, click **Policy and Automation Management**.

2 Under Common Tasks in the right pane, click **Configure Exchange Policies**.

3 Click **Mailbox rules**.

4 Select the mailbox policies you want ExA to enforce when you create or modify user accounts.

5 Click **OK**.