User Guide

Directory and Resource Administrator
Exchange Administrator

September 2010

Legal Notice

NetIQ Directory Resource Administrator and Exchange Administrator are protected by United States Patent No. 6,792,462.

Contents

Chapter 3
Managing User Accounts 21

Chapter 4
Managing Groups 33

Chapter 7
Managing Exchange Mailboxes 55

Chapter 8
Managing Computers 65

Chapter 9
Managing Services 71

Chapter 10
Managing Printers and Print Jobs 75

Chapter 11
Managing Shares 85

Chapter 12
Managing Advanced Queries 89

Chapter 13
Managing Connected Users 93

Chapter 14
Managing Devices 95

Chapter 15
Managing Event Logs 97

Chapter 16
Managing Open Files 101

Chapter 17
Managing the Recycle Bin 103

Chapter 18
Generating Reports 105

About This Book and the Library

The *User Guide* provides conceptual information about Directory and Resource Administrator (DRA) and Exchange Administrator (ExA). This book defines terminology, provides quick tours of all user interfaces, and guides users step-by-step through administration and Exchange tasks.

Intended Audience

This book provides information for individuals responsible for performing directory, resource, and Exchange administration tasks within 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.

Administrator Guide

Provides conceptual information about the DRA and ExA. This book defines terminology and includes implementation scenarios.

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [*value*]	• Optional parameters of a command
Braces, such as {*value*}	• Required parameters of a command
Logical OR, such as *value1* | *value2*	• Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please 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, please 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, please visit http://community.netiq.com.

Chapter 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.

Key benefits of DRA include:

Policy and regulation compliance

> Involves the assessment, operation, and control of systems and resources in accordance with security standards, best practices, and regulatory requirements and provides logging and auditing capabilities that help demonstrate compliance.

Operational integrity

> Prevents malicious or incorrect changes that affect the performance and availability of systems and services by providing granular access control for administrators and managing access to systems and resources.

Process enforcement

Maintains the integrity of key change management processes that help you improve productivity, reduce errors, save time, and increase administration efficiency.

What are DRA and ExA?

DRA and ExA are comprehensive account and resource management products for the key Microsoft identity and messaging platforms, Active Directory and Exchange. Using a flexible, rules-based management model, both DRA and ExA deliver capabilities that streamline administration, increase security, assure operational integrity, and ease the challenges of regulatory compliance for your Active Directory and Microsoft Exchange messaging environments.

An enterprise-scale directory and resource management product, DRA controls and manages Active Directory administration. Its powerful policy-based management, coupled with its safe, distributed administration, dramatically reduces administration efforts and costs. DRA provides increased data security while protecting the integrity of your Active Directory content.

ExA extends the power and flexibility of DRA to include Microsoft Exchange management. Within the context of account administration, you can manage mailboxes, Microsoft Exchange permissions, contacts, and distribution lists. DRA and ExA provide a single, integrated solution for controlling and managing complex IT environments.

What DRA and EXA Provide

DRA and ExA allow you to manage your enterprise within the context of a dynamic security model. This model ensures that your enterprise management and security remains current as your enterprise changes and evolves.

DRA and ExA provide advanced delegation and robust, policy-based administration features that improve the security and efficiency of your Microsoft Windows environment. They provide a secure, integrated administration solution for the following environments:

- Microsoft Windows 2000 Server Active Directory, Microsoft Windows Server 2003 Active Directory, and Microsoft Windows Server 2008 Active Directory
- Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, and Microsoft Exchange Server 2010

DRA and ExA offer significant flexibility using patented ActiveView technology and granular delegation. An ActiveView is a dynamic set of objects, such as user accounts or computers, that you want an administrator to collectively manage. ActiveViews can include or exclude objects from multiple domains, OUs, and groups into virtual containers for easy administration. With ActiveViews, administrators only sees the objects they can manage, without exposing them to the other objects present across the managed environment.

Granular delegation lets you securely distribute specific tasks, such as resetting a user password or modifying Microsoft Exchange mailbox rights. The flexibility of ActiveViews helps eliminate many of the problems associated with managing data in difficult-to-change, hierarchical structures.

DRA and ExA also help you assure compliance with internal policies and with regulatory requirements. For example, DRA offers dual-key security, so you can require two people to independently confirm portions of the same workflow. You can delegate one administrator to send a user account to the Recycle Bin, and another administrator to review the action and either approve the decision or revoke the change. DRA provides additional reports, logging, and auditing capabilities to help you demonstrate compliance with policies and with regulatory requirements.

With the Web Console, DRA and ExA provide out-of-the-box relief where you want to delegate administrative tasks, but do not want to deploy the product console. For example, you may want employees to manage their personal information, or provide limited privileges to a Help Desk organization. This easy-to-use, task-based interface significantly reduces administration time and lets you securely delegate specific tasks without additional training. You can quickly and easily customize the scope of the administration tasks you want to make available from the Web Console

These technologies seamlessly join and manage data from multiple sources across your enterprise, including Active Directory, Microsoft Exchange, and computer resources. To further expand these benefits, DRA and ExA let you apply policies to directory updates that can extend beyond the directory itself to other applications and databases, making the task of enterprise management easy.

DRA lets you define administration policies that it then automatically propagates and enforces for all DRA users, increasing security and reducing administration costs. This model is dynamic, so as your enterprise changes, objects inherit the appropriate level of security.

DRA and ExA help you automate and streamline many routine administration tasks, such as creating a user account and home share for a new employee. While many automated Active Directory administration tasks are provided out-of-the-box, you can also extend DRA and ExA using well-known standard interfaces such as the Active Directory Service Interfaces (ADSI) and Windows Terminal Server (WTS). DRA and ExA also provide tools, such as automation triggers and the DRA Software Development Kit (SDK), so you can integrate enterprise administration with your current business systems.

DRA supports both 32-bit and 64-bit platforms, ensuring you can run DRA in any Microsoft Windows environment. 64-bit platforms provide you with increased scalability, increased performance, reduced query time, and more effective use of memory.

Using state-of-the-art technology, these products provide the features you need to create a more secure, productive, and manageable Active Directory and Microsoft Exchange environment.

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

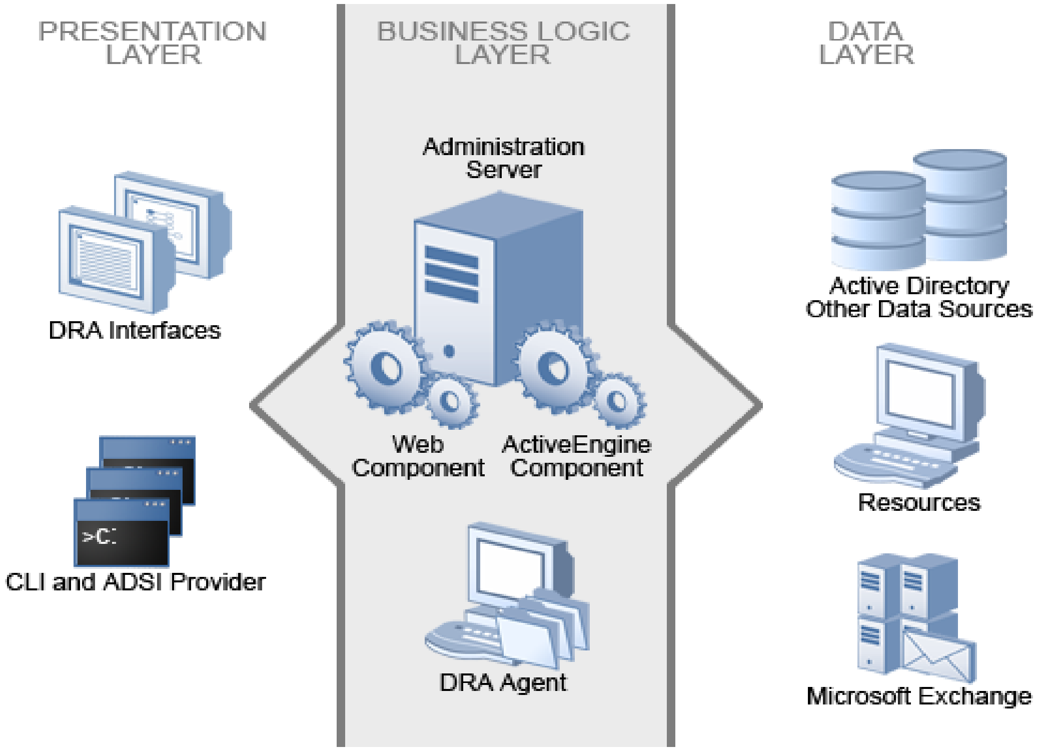
Managing any data set that contains inconsistencies creates security risks and may interfere with efficient operations. You can publish naming policies and permission guidelines for different accounts, but users may not remember to follow the guidelines. DRA can automatically enforce your policies, ensuring 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.

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. 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.

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. 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.

Chapter 2

Working with the User Interfaces

The user interfaces for DRA and ExA address a variety of administration needs. These interfaces include:

Web Console

Allows you to perform common account and resource administration tasks through a Web-based interface. This simple interface allows the occasional administrator to easily perform everyday administration tasks. You can access the Web Console from any computer running Internet Explorer.

Account and Resource Management Console

Allows you to administer objects in any managed domain. Through the Account and Resource Management console, you can view and modify accounts, resources, temporary group assignments, and Microsoft Exchange mailboxes. This interface addresses enterprise management needs from basic administration to advanced Help Desk issues.

NetIQ Reporting Center Console

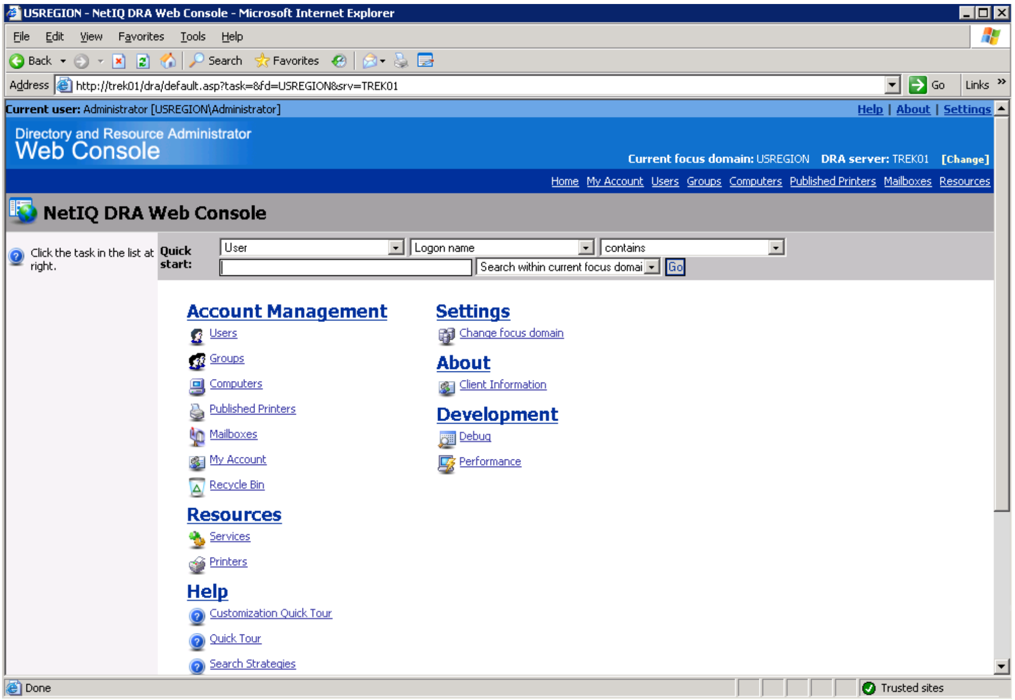
Allows you to view and deploy Management reports so you can audit your enterprise security and track administration activities. Management reports include activity reports, configuration reports, and summarization reports. Many of these reports can be viewed in a graphical representation.

Web Console

The Web Console is a Web-based user interface that provides quick and easy access to many user account, group, computer, resource, and Microsoft Exchange mailbox tasks. You can also manage general properties of your own user account, such as the street address or cell phone number.

The Web Console is easy to learn and simple to use, which makes it a great tool for occasional or beginning administrators. The Web Console provides step-by-step help as it guides you through each task. When you complete a task, it displays links to other related tasks, so you can quickly address an entire workflow. The Web Console displays a task only if you have the power to perform that task.

The following figure shows the Web Console home page.


USREGION - NetIQ DRA Web Console - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://trek01/dra/default.asp?task=&fd=USREGION&srv=TREK01
Go Links
Current user: Administrator [USREGION\Administrator]
Help | About | Settings
Directory and Resource Administrator
Web Console
Current focus domain: USREGION DRA server: TREK01 [Change]
Home My Account Users Groups Computers Published Printers Mailboxes Resources
NetIQ DRA Web Console
Click the task in the list at right.
Quick start:
User
Logon name
contains
Search within current focus domai
Go
Account Management
Users
Groups
Computers
Published Printers
Mailboxes
My Account
Recycle Bin
Resources
Services
Printers
Help
Customization Quick Tour
Quick Tour
Search Strategies
Settings
Change focus domain
About
Client Information
Development
Debug
Performance
Done
Trusted sites

Starting the Web Console

You can start the Web Console from any computer running Internet Explorer. To start the Web Console, specify the appropriate URL in your Web browser address field or use the link provided in the Account and Resource Management console. For example, if you installed the Web component on the HOUserver computer, type `http://HOUserver/dra` in the address field of your Web browser.

Note

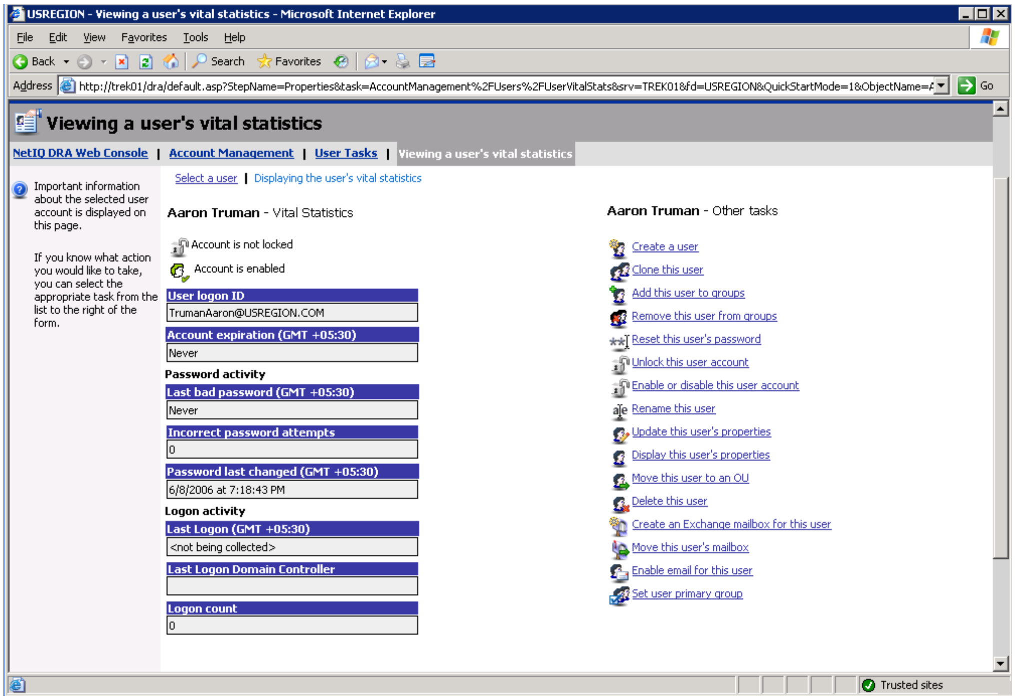
To display the most current account and Microsoft Exchange information in the Web Console, set your Web browser to check for newer versions of cached pages at every visit.

You can also start the Web Console from the DRA program group, and from the File menu in the Account and Resource Management console and the Delegation and Configuration console.

Using Quick Start to Solve Issues

Quick Start allows you to quickly and easily resolve account issues. You can view vital statistics and properties for a specific user account, computer, or group. You can then link to the appropriate task, such as resetting the password for a user account, which addresses your problem.

The following figure shows the vital statistics page for a user account.


USREGION - Viewing a user's vital statistics - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
http://trek01/dra/default.asp?StepName=Properties&task=AccountManagement%2FUsers%2FUserVitalStats&srv=TREK01&fd=USREGION&QuickStartMode=1&ObjectName=A
Go
Trusted sites

Viewing a user's vital statistics

NetIQ DRA Web Console | Account Management | User Tasks | Viewing a user's vital statistics

Select a user | Displaying the user's vital statistics

Important information about the selected user account is displayed on this page.

If you know what action you would like to take, you can select the appropriate task from the list to the right of the form.

Aaron Truman - Vital Statistics

Account is not locked

Account is enabled

User logon ID: TrumanAaron@USREGION.COM

Account expiration (GMT +05:30): Never

Password activity

Last bad password (GMT +05:30): Never

Incorrect password attempts: 0

Password last changed (GMT +05:30): 6/8/2006 at 7:18:43 PM

Logon activity

Last Logon (GMT +05:30): <not being collected>

Last Logon Domain Controller:

Logon count: 0

Aaron Truman - Other tasks

- Create a user
- Clone this user
- Add this user to groups
- Remove this user from groups
- Reset this user's password
- Unlock this user account
- Enable or disable this user account
- Rename this user
- Update this user's properties
- Display this user's properties
- Move this user to an OU
- Delete this user
- Create an Exchange mailbox for this user
- Move this user's mailbox
- Enable email for this user
- Set user primary group

Account and Resource Management Console

The Account and Resource Management console provides access to all tasks, addressing enterprise management needs from basic administration to advanced Help Desk issues. Through the Account and Resource Management console, you can perform all account and resource management tasks and manage Microsoft Exchange mailboxes.

The Account and Resource Management console contains the following nodes:

All My Managed Objects

Allows you to manage objects, such as user accounts, groups, contacts, and resources, for each domain in which you have some power.

Temporary Group Assignments

Allows you to manage group memberships for users who only need group membership for a specific time period.

Advanced Search Queries

Allows you to manage advanced queries available on the Administration server.

Recycle Bin

Allows you to manage deleted user accounts, groups, contacts, and resources, for any Microsoft Windows domain where the Recycle Bin is enabled.

When you start the Account and Resource Management console, you initially connect to the best available Administration server in the local domain. The best-available Administration server is the closest server, which is typically a server in the network site. By seeking the best available Administration server, DRA provides a quicker connection and improved performance.

To start the Account and Resource Management console interface, click **Account and Resource Management** in the Directory and Resource Administrator program folder. The following sections provide common tasks for the Account and Resource Management console.

Connecting to an Administration Server

The best-available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to the next available server in the managed domain or managed subtree. You can also specify the Administration server to which you want to connect.

When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you are logged on to a domain that is not managed by an Administration server, or if DRA cannot connect to the Administration server for that domain, DRA may display an error message. Ensure the Administration server is available and try again.

To connect to an Administration server:

1. On the File menu, click **Connect to DRA server**.
2. Click **Connect to this DRA server**.
3. Type the name of the Administration server, using the following format: *`computername`*.
4. Click **OK**.

Connecting to a Managed Domain or Computer

By default, the Account and Resource Management console connects to a managed domain or computer by using the best-available Administration server. The best-available Administration server is the closest server, which is typically a server in the network site. If the site does not include an Administration server, DRA connects to one of the servers managing the domain of the client computer. However, you can specify the domain or computer to which you want to connect. You can also specify which Administration server you want DRA to use.

When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you attempt to log on to a domain or computer that is not managed by an Administration server, or if DRA cannot connect to the Administration server for your managed domain or computer, DRA may display an error message. Ensure the Administration server is available and try again.

To connect to a managed domain or computer:

1. On the File menu, click **Connect to DRA server**.
2. Select the appropriate option, and then type the name of the managed domain or computer.
3. For example, to connect to the HOULAB domain, click C**onnect to a DRA server that manages this domain**, and then type `HOULAB`.
4. To specify an Administration server for the managed domain or computer, click **Advanced**, and then select the appropriate option.
5. Click **OK**.

Modifying the Console Title

You can modify the information displayed in the title bar of both the Delegation and Configuration console and the Account and Resource Management console. For convenience and clarity, you can add the user name with which the console was launched and the Administration server to which the console is connected. In complex environments in which you need to connect to multiple Administration servers using different credentials, this feature helps you quickly discern which console you need to use.

To modify the console title bar:

1. Start the Account and Resource Management console.
2. Click **View > Options**.
3. Select the Window Title tab.
4. Specify the appropriate options, and then click **OK**. For more information, click the **?** icon.

Customizing List Columns

You can select which object properties DRA displays in list columns. This flexible feature allows you to customize the user interface, such as lists for search results, to better meet the specific demands of administrating your enterprise. For example, you can set columns to display the user logon name or group type, letting you quickly and effectively find and sort the data you need.

To customize list columns:

1. Select the appropriate node. For example, to choose which columns display when viewing search results on managed objects, select **All My Managed Objects**.
2. On the View menu, click **Choose Columns**.
3. From the list of properties available for this node, select the object properties you want to show.
4. To change the column order, select a column, and then click **Move Up** or **Move Down**.
5. To specify the column width, select a column, and then type the appropriate number of pixels in the provided field.
6. Click **OK**.

Using Custom Tools

DRA enables you to seamlessly integrate the DRA interface with other products by using the custom tools feature. Using custom tools, you can execute external applications, launch scripts, open a web page, and enter parameters for any object from within the DRA interface. For example, if you select a computer in your domain, you can launch any of the custom tools defined and enabled for computers by your DRA Administrator.

To use custom tools:

1. Start the Account and Resource Management console.
2. In the left pane, expand **All My Managed Objects**.
3. To specify the object for which you want to use the custom tool, complete the following steps:
   a. ***If you know the object location***, select the domain and OU that contains this object.
   b. In the search pane, specify the object attributes, and then click **Find Now**.

   c. In the list pane, select the appropriate object.

4. On the Tasks menu, click **Custom Tools**.

   Note

   When you try to select custom tools for an object, if DRA does not display any custom tools for that object, it implies your DRA administrator has not enabled custom tools for that object.

   ---

5. Select the appropriate custom tool.

Executing Saved Advanced Queries

Using advanced queries, you can search for users, contacts, groups, computers, printers, OUs, and any other object that DRA supports. If you have the Execute Saved Advanced Queries power, you can execute advanced queries available in the **Saved Queries** list for any container in the Account and Resource Management console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

To execute saved advanced queries:

1. Start the Account and Resource Management console.
2. In the left pane, expand **All My Managed Objects**.
3. Select the appropriate container. For example, if you want DRA to search for user account information, select **Users**.
4. To view the advanced search pane, click **Advanced Search**.
5. In the advanced search pane, select an advanced query from the **Saved Queries** list.
6. Click **Load Query**, and then click **Find Now**.

Reporting on Object Changes

You can view real-time change information for objects in your domains by generating Activity Detail reports. For example, you can view a list of changes made to an object or by an object during a specified time period. You can also export and print Activity Detail reports.

To report on object changes:

1. Find the objects that match your criteria.
2. Right-click on an object, and select **Reporting > Changes made to objectName** or **Reporting > Changes made by objectName**.
3. Select the start and end dates to specify the changes you want to view.
4. ***If you want to change the number of rows to be displayed***, type a number over the default value of 250.

   Note

   The number of rows displayed applies to each Administration server in your environment. If you include 3 Administration servers in the report and use the default value of 250 rows to display, up to 750 rows can be displayed in the report.

   ---

5. ***If you want to include only specific Administration servers in the report***, select **Restrict query to these DRA servers** and type the server name or names you want the report to include. Separate multiple server names with commas.

6. Click **OK**.

Reporting on Object Lists

You can export or print data from object lists. With this feature, you can quickly and easily report on and distribute general information about your managed objects.

When you export an object list, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page

---

Note
You can also select multiple items in a list and then copy these items to a text application, such as Notepad.

To report on object lists:

1. Find the objects that match your criteria.
2. To export this object list, click **Export List** on the File menu.
3. To print this object list, click **Print List** on the File menu.
4. Specify the appropriate information to save or print this list.

Reporting on Object Details

You can export or print data from details tabs that list object attributes, such as group memberships. With this feature, you can quickly and easily report on and distribute frequently needed details about specific objects.

When you export an object details tab, you can specify the file location, name, and format. DRA supports HTML, CSV, and XML formats, so you can export this information to database applications or post list results to a Web page.

To report on object details:

1. Find the object that matches your criteria.
2. On the View menu, click **Details**.
3. In the details pane, select the appropriate tab.
4. To export these object details, click **Export Details** List on the File menu.
5. To print these object details, click **Print Details List** on the File menu.
6. Specify the appropriate information to save or print this list.

Restoring Console Settings

DRA allows you to resize windows and persists your window sizes. DRA also persists many other settings, including the last Administration server to which you connect, the columns you add or remove from list results, and column widths. If you want to restore these settings to the original setting with which you installed DRA, the Restore Default Settings option allows you to do so.

To restore default console settings:

1. Start the appropriate console.
2. Click **View > Options**.
3. Select the Saved Settings tab.
4. Review the information provided on the window, and then click **Restore Default Settings**. For more information, click the **?** icon.

Using Special Characters

You cannot use the following special characters when naming user accounts, groups, contacts, OUs, computers, ActiveViews, AA groups, roles, policies, or automation triggers. These naming restrictions apply to the name of the object as well as the name of the rule that defines the object.

Naming user accounts, groups, and computers

When specifying a pre-Windows 2000 name, you cannot use the following special characters:

Backslash	\
Colon	:
Comma	,
Double quote	"
Equal sign	=
Forward slash	/
Greater than	>
Left bracket	[
Less than	<
Plus sign	+
Right bracket	]
Semi colon	;
Vertical bar	|

When naming user accounts, groups, and computers in Microsoft Windows domains, you can use any special character.

Naming contacts and OUs

When naming contacts and OUs, you can use any special character.

Naming ActiveViews, AA groups, and roles

When naming ActiveViews, AA groups, and roles, you cannot use the backslash (\).

Naming policies and automation triggers

When naming policies and automation triggers, you cannot use the backslash (\).

You can include wildcard characters (`*, ?, and #`) when naming Microsoft Windows objects. Use wildcard characters when creating rules to narrow or broaden the context of a rule.

Using Wildcard Characters

DRA and ExA support wildcard characters in many fields in the DRA consoles and in CLI commands. Wildcards allow you to define rules that match multiple objects to a specific condition or standard, such as a naming convention. You can use wildcards instead of regular expressions to narrow or broaden the scope of the rule. Wildcard matching is not case-sensitive. You can also use the question mark (?), asterisk (*), or number sign (#) wildcard characters as normal characters by prefixing a backslash (\) to the particular wildcard character. For example, to search for `abc*`, type the search text `abc\*`.

DRA and ExA support the following wildcard characters. You cannot use wildcard characters in names.

Match Item	Character	Definition
Any character	Question mark ?	Matches exactly one character
Any digit	Number sign #	Matches one digit
Any character, 0 or more matches	Asterisk *	Matches zero or more characters

The following table provides examples of wildcard character specifications and what they match and do not match.

Example	Matches	Does Not Match
Den???	Denton and Dennis	Denison
El ????o	El Campo and El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA and ExA do not support wildcard specifications that contain logical operations.

Viewing Your Assigned Powers and Roles

Roles and powers define how you manage objects. A role is a set of powers that provides the permissions required to perform a specific administration task, such as creating a user account or moving shared directories.

The DRA Admin assigns roles, adds you to specific AA groups, and associates you with ActiveViews (sets of domain objects you can manage). You can view these assignments through the Account and Resource Management console and the Delegation and Configuration console. You do not need any auxiliary powers to view the roles and powers assigned to you.

For more information about the DRA security model, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator.*

To view your assigned powers and roles:

1. On the File menu, click **DRA Properties**.
2. Click **Powers**.
3. Select the appropriate view. For example, click **Flat View** to see a table of your AA group memberships, assigned powers and roles, and associated ActiveViews.

4. Expand the appropriate item. For example, under **Has Power** column, expand **Roles and Powers** to view the individual roles or powers assigned to you.

5. Click **OK**.

Viewing the Product Version Number and Installed Hotfixes

You can view the product version number and installed hotfixes from the DRA Properties window. This window provides version numbers and lists of installed hotfixes for the Administration server and the DRA client computer.

To view the product version number and installed hotfixes:

1. On the File menu, click **DRA Properties**.

2. Click **General**.

3. View the information you need. For more information about a particular field, click the **?** icon.

4. Click **OK**.

Suppressing the License Warning Message

DRA provides you with an option to suppress the license warning message that appears when you reach the remaining user count threshold limit. DRA allows you to set the threshold limit for the number of remaining licensed users in the registry, which overrides the remaining user count threshold limit value available in the license file. DRA suppresses the license warning message until you reach the threshold limit you have set in the registry. The value you set as the threshold limit in the registry is optional and you can still use the threshold limit available in the license file.

Warning

Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To update the threshold limit value in the registry:

1. Click **Start > Run**. The Run dialog box is displayed.

2. In the **Open** field, type `regedit` and then click **OK**. The Registry Editor window is displayed.

3. In the left pane, expand `HKLM\SOFTWARE\Mission Critical Software\OnePoint\Administration\License`.

   Note

   If you are editing the registry on a 64-bit operating system, expand `HKLM\Software\WOW6432Node` instead of `HKLM\Software`. The rest of the path remains the same.

4. In the right pane, right-click and select **New > DWORD value**.

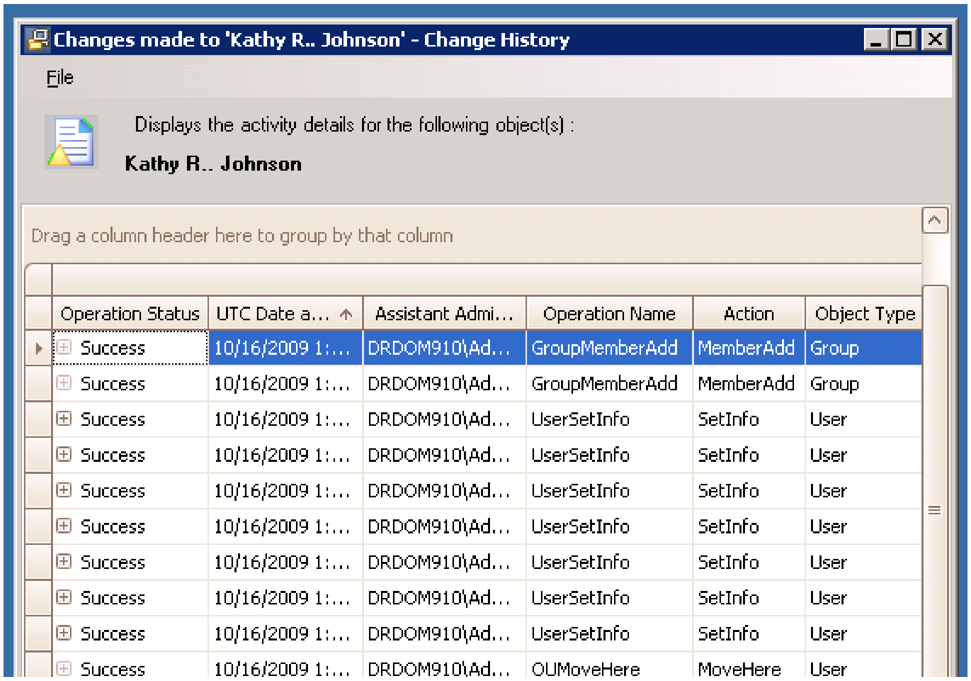
5. Name the `DWORD value` as "`WarnThreshold`" and set the value that you wish to warn at. For example, if you set this value to 10, then DRA will not warn you until your license has less than 10 users left.

DRA Reporting

DRA Reporting provides built-in, ready-to-use reports that let you quickly track duplicate accounts, last account logons, Microsoft Exchange mailbox details, and much more. Reporting also provides real-time details of changes made in your environment, including before and after values for changed properties. You can export, print, or view reports, or publish them to SQL Server Reporting Services.

Directory and Resource Administrator provides two methods of generating reports that allow you to collect and review user account, group, and resource definitions in your domain. **Activity Detail reports**, viewed through the Delegation and Configuration console, provide real-time change information for objects in your domain. For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports.

The following figure shows a sample Activity Detail report:



Displays the activity details for the following object(s) :

Kathy R.. Johnson

Drag a column header here to group by that column

Operation Status	UTC Date a...	Assistant Admi...	Operation Name	Action	Object Type
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	OUMoveHere	MoveHere	User

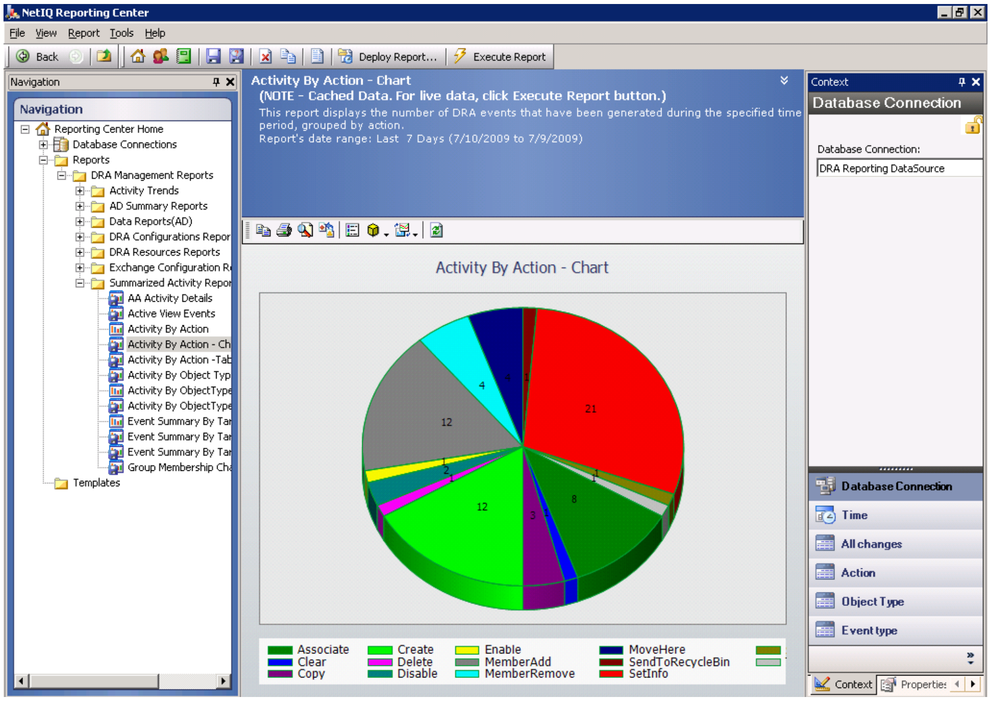
Optional **DRA Management reports**, viewed through the NetIQ Reporting Center (Reporting Center), provide activity, configuration, and summarization information about events in your managed domains. Some Management reports are available as graphical representations of the data. These built-in reports can also be customized to give you exactly the information you need.

For example, you can view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting allows you to view details about the DRA security model, such as ActiveView and AA group definitions.

You must install and configure the optional Management reports before you can view these reports. For more information about installing reporting components, see the *Installation Guide*. For more information about DRA Reporting, see “Generating Reports” on page 105.

Start Reporting Center Console in the NetIQ > Reporting Center program group.

The following figure shows the Reporting Center interface with DRA Management reports selected.



Activity By Action - Chart

(NOTE - Cached Data. For live data, click Execute Report button.)

This report displays the number of DRA events that have been generated during the specified time period, grouped by action.

Report's date range: Last 7 Days (7/10/2009 to 7/9/2009)

Database Connection: DRA Reporting DataSource

Chapter 3

Managing User Accounts

Microsoft Windows relies on the user account type to determine access permissions for the associated user account. A user account can be global or local. DRA also supports InetOrgPerson objects, but recognizes InetOrgPerson objects as normal users.

Global user account

A user account that can be used in any domain that trusts the domain in which the user account was created. You can grant specific permissions to a user account. You can also make a user account a member of a group and then assign permissions to that group. Grouping user accounts helps simplify the process of managing network permissions for many user accounts.

Local user account

A user account that is restricted to the computer on which it was created. Local user accounts allow users from NetWare, LAN Manager, and IBM LAN Server environments to use resources in a Microsoft Windows computer.

User Accounts in Trusted Domains

Microsoft Windows stores user account and group definitions in the directory of the managed domain. Therefore, an Administration server cannot modify the directory information from a trusted domain unless that domain is also managed by DRA.

For example, in the Account and Resource Management console, you may see user accounts and groups that you cannot modify. These user accounts and groups are defined in domains trusted by one of the managed domains. However, you can add accounts and groups from a trusted domain to other groups in the managed domain.

To modify user accounts or groups in a managed domain, you must first connect to the Administration server managing that domain. You must also have the appropriate powers to modify those user accounts or groups. For more information about specific user account administration tasks, see “User Account Management Tasks” on page 22.

User Account Management Tasks

This section guides you through administering user accounts in the Account and Resource Management console. With the appropriate powers, you can perform various user account management tasks, such as creating and deleting accounts. If you select multiple user accounts, you can perform selected tasks in one operation, such as deleting, moving, or adding users to a group. The Tasks menu indicates which tasks you can perform when you select single or multiple user accounts.

You also can perform these tasks using the Web Console or CLI. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Creating a User Account

You can create user accounts in the managed domain or managed subtree. You can also modify properties, create a mailbox, enable email, and specify group memberships for the new account.

Notes

- Your company may have a naming convention enforced through policy that determines the name you can assign to the new user account.
- By default, DRA places the new user account in the Users OU of the managed domain.
- You cannot create InetOrgPerson objects in DRA.

To create a user account:

1. In the left pane, expand **All My Managed Objects**.
2. Select the location where you want to create this account.

   For example, if you want to create this account in a specific OU of the managed domain, expand the domain and then select the appropriate OU.
3. On the Tasks menu, click **New > User**.
4. On each tab, specify the appropriate settings and properties for the new user account, and then click **Next**.
5. Review the summary, and then click **Finish**.

Cloning a User Account

By cloning a user account, you can quickly create user accounts based on other accounts with similar properties. When you clone a user account, DRA populates the Clone User Wizard with values from the selected account. You can also modify properties, enable email, and specify group memberships for the new account.

Note

When you clone an InetOrgPerson object, you create a user account.

To clone a user account:

1. In the left pane, expand **All My Managed Objects.**
2. To specify the user account you want to clone, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.

    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Clone**.
4. On each tab, specify the appropriate settings and properties for the new user account, and then click **Next**.
5. Review the summary, and then click **Finish**.

Managing User Account Properties

You can manage the properties of user accounts in the managed domain or managed subtree. The powers you have determine which properties you can modify for a user account. If you installed ExA and enabled Microsoft Exchange support, you can modify the associated mailbox properties while managing user accounts.

Notes

- You cannot modify mailbox properties of user accounts managed on member servers.
- If home directory policies are enabled, DRA automatically modifies the home directory of a user account when you manage that account. For example, when you change the home directory location, DRA attempts to create the specified home directory and move the contents of the previous home directory to the new location. DRA also applies the assigned ACLs from the previous directory to the new directory. For more information, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator.*

To manage user account properties:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to modify, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. ***If you selected a single user account***, on the appropriate tab, change the properties and settings you want to modify.
5. ***If you selected multiple user accounts***, complete the following steps:

    Note

    You can manage selected property values on the General, Address, Account, Profile, and Organization property pages for user accounts. If you are also managing Microsoft Exchange mailboxes, when you select multiple user accounts, you can perform selected Exchange tasks, such as creating or cloning mailboxes.

    a. On the appropriate tab, click the pencil icon next to the property or setting you want to modify.
    b. Change the property or settings you want to modify. Changing the property or settings value applies the same value to all selected objects.
    c. Click **Apply**.

   d. ***If you want to copy the contents of the Results window***, click the copy to clipboard icon on the lower left of the window.

   e. Click **OK**.

6. To save changes before you modify other properties, click **Apply**.

7. Click **OK**.

Managing Your Own Account

You can manage your own account by modifying general properties, such as your telephone number. Before you manage your account, ensure you have the appropriate power.

To manage your own account:

1. In the left pane, expand **All My Managed Objects**.

2. Use the search pane to find your account.

3. In the list pane, select your account.

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

5. On the appropriate tab, change the properties and settings you want to modify.

   To save these changes before you modify other properties, click **Apply**.

6. Click **OK**.

Renaming a User Account

You can rename user accounts in the managed domain or managed subtree. Changing the user logon name also changes the name of the mailbox associated with the user account.

To rename a user account:

1. In the left pane, expand **All My Managed Objects**.

2. To specify the user account you want to rename, complete the following steps

   a. ***If you know the account location***, select the domain and OU that contains this user account.

   b. In the search pane, specify the account attributes, and then click **Find Now**.

   c. In the list pane, select the appropriate user account.

3. On the Tasks menu, click **Rename**.

4. Change the appropriate naming properties.

5. Click **OK**.

Enabling a User Account

You can enable a user account in the managed domain or managed subtree. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies this change.

Note

When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties. For more information, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator.*

To enable a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to enable, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Enable User Account**.
4. To apply this change at a specific domain controller, click **Specify domain controller**, and select the appropriate domain controller.
5. Click **Yes**.

Disabling a User Account

You can disable a user account in the managed domain. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies this change.

Note

When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties. For more information, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator.*

To disable a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to disable, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Disable User Account**.
4. To apply this change at a specific domain controller, click **Specify domain controller**, and select the appropriate domain controller.
5. Click **Yes**.

Unlocking a User Account

You can unlock a user account in the managed domain or managed subtree.

Because DRA retrieves the user account status from the accounts cache, the user interface may indicate that the selected account is unlocked when it is actually locked. DRA allows you to unlock a user account even if the account status indicates it is currently unlocked. You can also specify a domain controller when unlocking a user account using the DRA console without having to reset the user account password. For more information about the accounts cache refresh, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator*.

To quickly unlock a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to unlock, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Unlock User Account**.

Resetting a User Account Password

You can reset the password for an account in the managed domain or managed subtree. The powers you have determine the fields you can change for that user account.

When you reset the password for a user account, DRA automatically unlocks the account. You can select whether DRA generates a new password for the user account. You can also modify several password-related options for the account. If you are managing a Microsoft Windows account, you can specify the domain controller at which DRA applies these changes.

Note

When you apply this change to a specific domain controller, DRA also applies this change to the default domain controller for this managed domain. To verify which default domain controller DRA is using, view the domain properties. For more information, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator*.

To quickly reset a user account password:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose password you want to reset, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Reset password**.
4. Specify the new password and select the appropriate account options.

   If you request a generated password, record the password DRA displays. If you specify a domain controller, record which domain controller you chose. DRA generates a password based on the Password Policy defined in the domain of the user account.

5. To apply this change at a specific domain controller, click **Specify domain controller**, and select the appropriate domain controller.

6. Click **OK**.

Copying a User Account to Another ActiveView

You can copy a user account to another ActiveView. This action is called **transferring** a user account. To copy a user account to another ActiveView, you need the Copy User to Another ActiveView power in both the source and target ActiveViews. Transferring a user account to another ActiveView does not remove the user account from the source ActiveView.

To copy a user account to another ActiveView:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to copy to another ActiveView, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Transfer**.
4. Specify the appropriate ActiveViews.
5. Click **OK**.

Moving a User Account to Another Container

You can move a user account to another container, such as an OU, in the managed domain or managed subtree.

To move a user account to another container:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to move to another container, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Move**.
4. Select the appropriate container.
5. Click **OK**.

Deleting a User Account

You can delete a user account in the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a user account permanently removes the user account from the Active Directory. If the Recycle Bin is enabled for that domain, deleting a user account moves the user account to the Recycle Bin.

For more information about using the Recycle Bin, see "Managing the Recycle Bin" on page 103.

Warning
When you create a user account, Microsoft Windows assigns a Security Identifier (SID) to that account. The SID is not generated from the account name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a user account, you cannot return access capabilities for that account by creating a new user account with the same name.

To delete a user account:

1. In the left pane, expand **All My Managed Objects.**
2. To specify the user account you want to delete, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Specifying Group Membership for User Accounts

You can add or remove user accounts from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this account belongs.

To specify group membership for user accounts:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to manage, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. In the details pane, click **Member of**. To view the details pane, click **Details** on the View menu.
4. To check a group to which the user account already belongs, select the group, and then click **Properties**.
5. To add the user account to a group, complete the following steps:
    a. Click **Add to Groups**.
    b. Find and select the appropriate group, and then click **OK**.
6. To remove the user account from a group, select the group, and then click **Remove**.

Transforming User Accounts

DRA offers you the ability to quickly and efficiently transform user accounts. When the individual associated with a user account transitions to new job responsibilities, you can use the transform capabilities of DRA. Taking advantage of job role templates, you can quickly add, remove, or update the group memberships associated with an account. Whether an individual is promoted, changes departments, or leaves the company, the ability to transform a user account will save you time, money, and guesswork.

Understanding the Transformation Process

You can use the transform user account capabilities to fulfill any of the following needs:

- Remove group memberships from a user account
- Add group memberships to a user account
- Change user properties
- Remove particular group memberships while adding other group memberships to a user account

Consider the following process before attempting to transform a user account:

1. Decide whether you need to add, remove, or both add and remove group memberships.
2. Review your current subtractive and additive templates to ensure you have the necessary template user accounts.
3. If necessary, create any required template accounts.
4. Complete the Transform User wizard.

As DRA transforms a user, the group memberships designated by the subtractive template are removed from the user account, while those memberships designated by the additive template are assigned to the user account. DRA leaves any memberships outside of the subtractive or additive templates intact. For example, an individual in your outside sales department is transferred from US sales to European sales. Within your organization, you have both distribution groups and security groups that are unique for these sales teams and a number that are shared across all sales teams. The US sales team has the US Hotspots DL and the US Sales Mang DL distribution groups while the European sales team has Euro Hotspots and Euro Sales Mang distribution groups. Both teams are members of the Global Sales Sec security group, but also have individual site-specific security groups.

Your subtractive template, named US Sales Template, would be assigned the following group memberships:

- US Hotspots DL
- US Sales Mang DL
- Global Sales Sec
- US Sec

Your additive template, named Euro Sales Template, would be assigned the following group memberships:

- Euro Hotspots DL
- Euro Sales Mang DL

- Global Sales Sec
- Euro Sec

During the transformation process, the user account of the transferred sales person is first removed from all the group memberships designated by the US Sales Template, and then added to all the group memberships designated by the Euro Sales Template. If this individual was also a member of the Poker Players distribution group, this group membership remains untouched.

The following powers allow an Assistant Admin to further modify a user account during the transformation process:

- Modify Address Properties while Transforming a User Account
- Modify Description while Transforming a User Account
- Modify Office while Transforming a User Account
- Modify Telephone Properties while Transforming a User Account

You can also restrict the ability to add or remove group memberships by giving an Assistant Admin only one of the following powers:

- Add a user to groups found in a template
- Remove a user from groups found in a template

You can use either of these power-based limiting options to create a layer of security within your organization. By allowing certain individuals the power to only remove groups found in a template, you can create interim user accounts. These interim accounts can then be reviewed before a different Assistant Admin uses an additive template account to grant the new group memberships.

Creating User Transformation Templates

Transformation of user accounts is directly tied to the roles and job ladders of your organization. Consider creating a template for each role or job within your company. DRA makes no distinction between a user account template used as subtractive versus additive. Create a single template user account for each role within your organization. During the transformation, you select the template as subtractive or additive. Selecting a template as subtractive does not stop the same template from being used as additive in a future transformation.

To create a user transformation template, you must have the powers to create a user account and assign that user account to the appropriate groups. These powers can be obtained through associating your account with the Create and Delete User Accounts and the Group Administration roles in the appropriate ActiveViews or through the assigning of individual powers.

Transforming User Accounts

Transforming a user account allows you to add, remove, or both add and remove user account group memberships. Use this workflow to help you when individuals transition from one job responsibility to another within your organization. You must have the Transform a User role or a role that contains the appropriate powers to transform user accounts.

To transform a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to manage, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.

   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.

3. Click **Tasks > Transform**.
4. Review the Welcome window, and then click **Next**.
5. On the Select User Template window, use **Browse** to the select the appropriate subtractive template user.
6. ***If you want to review the properties of the subtractive template user account***, click **View**.
7. Use **Browse** to the select the appropriate additive template user.
8. ***If you want to review the properties of the additive template user account***, click **View**.
9. ***If you have the appropriate powers***, you can check **Change other properties of the user** and select properties to modify. Click **Next** to navigate through the properties available. For more information, click **?**.
10. Click **Next**.
11. Review the Summary window, and then click **Finish**.

Chapter 4

Managing Groups

As an Assistant Admin (AA), you can use DRA and ExA to manage groups and modify group properties. Groups allow you to give specific permissions to a defined set of user accounts. Groups let you control which data and resources a user account can access in any domain.

You can manage groups of any type and scope. For example, you can nest groups, allowing one group can inherit permissions from another group. You can also effectively control group memberships across domains by adding groups from trusted domains to other groups in the managed domain and by managing temporary group assignments.

Group Contents

Groups can contain the following objects:

- User Accounts (UA)
- Contacts (CON)
- Computers (CPT)
- Global Groups (GG)
- Local Groups (LG)
- Universal Groups (UG)
- Foreign Security Principals (FSP)

Depending on your network environment, groups can only contain certain objects. The following table indicates what type of objects a group can contain when groups are in the same domain or in a trusted domain, mixed mode or native mode domain environment.

	Local Groups		**Global Groups**		**Universal Groups**	
Domain	**Same**	**Trusted**	**Same**	**Trusted**	**Same**	**Trusted**
Mixed Mode	UA CON CPT GG LG UG FSP	UA CON CPT GG UG FSP	UA CON CPT FSP	None	UA CON CPT GG FSP	UA CON CPT GG LG FSP

	Local Groups		**Global Groups**		**Universal Groups**	
Domain	**Same**	**Trusted**	**Same**	**Trusted**	**Same**	**Trusted**
Native Mode	UA CON CPT GG LG UG FSP	UA CON CPT GG UG FSP	UA CON CPT GG FSP	None	UA CON CPT GG UG FSP	UA CON CPT GG UG FSP

Group Types

In mixed mode and native mode domains, you can create the following group types:

Security Groups

Let you assign rights and permissions to a collection of members and manage their permissions collectively. Each security group is assigned a Security Identifier (SID).

Distribution Groups

Let you identify a set of user accounts and contacts to use as an Exchange distribution list. Distribution groups are not assigned SIDs.

Group Scope

In mixed or native mode domains, you can define the group scope as domain local, global, or universal. With group type and scope combined in mixed mode domains, you can create groups with several different types and scopes, including the following groups:

- Domain local security groups
- Domain local distribution groups
- Global security groups
- Global distribution groups
- Universal distribution groups

You can use universal security groups only in native mode domains.

Group Scopes in Mixed and Native Modes

A mixed mode domain has some limitations on the use of group types and scopes. For example, you can create universal distribution groups, but you cannot create universal security groups. You can only nest distribution groups in a mixed mode domain. Once you create a group, you cannot change the type or scope or convert the group to another type or scope.

In a native mode domain, groups are more flexible than in mixed mode domains. You can use universal groups for security or distribution. You can nest any type of group in a universal group. You can freely convert groups between security and distribution group scopes. You can convert global and domain local groups to universal group types with a few exceptions.

The following table compares some aspects of group scope in mixed mode domains and in Microsoft Windows native mode domains.

Group Scope	Mixed Mode Domains	Microsoft Windows Native Mode Domains
Domain Local	Groups can contain user accounts and global groups from any domain. You can include these groups only in other domain local groups and permission lists in the same domain.	Groups can contain user accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain. You can convert domain local groups that do not contain other domain local groups to universal groups.
Global	Groups can contain user accounts from the same domain and any domain can reference a domain that trusts the domain in which it was created. You can assign a global group permissions for anywhere in the network. Global groups cannot contain other groups.	Groups can contain the same objects as in mixed mode domains, except global groups can contain other global groups from the same domain. You can convert global groups that are not a member of any other global groups to universal groups.
Universal	You can only create universal distribution groups in a mixed mode domain.	Groups can contain members from any domain in the forest. Universal groups can appear in ACLs anywhere in the forest, and can contain other universal groups, global groups, and user accounts.

Group Management Tasks

This section guides you through administering groups in the Account and Resource Management console. With the appropriate powers, you can perform various group management tasks, such as modifying group memberships. If you select multiple groups, you can perform selected tasks in one operation, such as deleting, moving, or adding members to a group. The Tasks menu indicates which tasks you can perform when you select single or multiple groups.

You also can perform these tasks using the Web Console or CLI. For more information about your assigned powers, see “Viewing Your Assigned Powers and Roles” on page 17.

Adding Accounts to Groups

You can add user accounts, contacts, and computers to a managed group. For more information about nesting groups, see "Adding Groups to Other Groups" on page 36.

Notes

- This task adds multiple accounts to a selected group. You can add a single account to a group by selecting the appropriate account and then clicking **Add to groups** on the Tasks menu.
- If adding an account to another group increases your powers for the account, DRA does not permit you to add the account.

To add an account to a group:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group to which you want to add accounts, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Add members**.
4. Find and select the appropriate accounts. You can select more than one account type, such as a contact and a user account.
5. Click **OK**.

Adding Groups to Other Groups

You can nest groups by adding a group to another managed group. When a group is nested in another group, the child group can inherit permissions from the parent group.

Note

If adding a group to another group increases your powers for the source group, DRA does not permit you to add the group.

To add a group to another group:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to add within another group, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Add to Groups**.
4. Find and select the appropriate group. You can select more than one group from different OUs or managed domains.
5. Click **OK**.

Managing Group Properties

You can manage properties for local and global groups. The powers you have determine which properties you can modify for a group in the managed domain or managed subtree. If you installed ExA and enabled Microsoft Exchange support, you can modify distribution list properties while managing groups.

To manage group properties:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to manage, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Properties**.
4. ***If you selected a single group***, on the appropriate tab, change the properties and settings you want to modify.
5. ***If you selected multiple groups***, complete the following steps:

    Note
    You can manage selected property values on the General and Managed by property pages for groups.

    a. On the appropriate tab, click the pencil icon next to the property or setting you want to modify.
    b. Change the property or settings you want to modify. Changing the property or settings value applies the same value to all selected objects.
    c. Click **Apply**.
    d. ***If you want to save the contents of the Results window***, click **Export** on the lower left corner of the window.
    e. Click **OK**.
6. To save your changes before you modify other properties, click **Apply**.
7. Click **OK**.

Creating a Group

You can create a group in the managed domain or managed subtree. You can also modify properties, such as group members, for the new group.

Notes

- Your company may have a naming convention enforced through policy that determines the name you can assign to the new group.
- By default, DRA places the new group in the Users OU of the managed domain.

To create a group:

1. In the left pane, expand **All My Managed Objects**.
2. Select the location where you want to create this group.

For example, if you want to create this group in a specific OU of the managed domain, expand the domain and then select the appropriate OU.

3. On the Tasks menu, click **New > Group**.
4. On each tab, specify the appropriate settings and properties for the new group, and then click **Next**.
5. Review the summary, and then click **Finish**.

Specifying Group Members

You can add or remove user accounts, contacts, computers, or other groups from the managed group. DRA allows you to only remove foreign security principals. You can also view or modify properties of existing group members, except for foreign security principals.

When you remove members from a group, DRA does not delete the objects. When you add members to a group, you must have the power to modify the objects you want to add.

Note
You cannot add user accounts or groups to any of the Windows special groups (Administrators, Account Operators, Backup Operators, or Server Operators) unless you are a Windows administrator or a member of that specific special group.

To manage group members:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group whose members you want to modify, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. In the details pane, click **Members**. To view the details pane, click **Details** on the View menu.
4. To check an existing group member, select the object, and then click **Properties**.
5. To add an object to this group, complete the following steps:
    a. Click **Add Members**.
    b. Find and select the appropriate object, and then click **OK**.
6. To remove an object from this group, select the object, and then click **Remove**.

Specifying Group Membership for Groups

You can add or remove a group from other groups in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this group belongs.

To manage group memberships:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group whose membership you want to modify, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.

    c. In the list pane, select the appropriate group.

3. In the details pane, click **Member of**. To view the details pane, click **Details** on the View menu.
4. To check a group, select the group, and then click **Properties**.
5. To add this group to another group, complete the following steps:
    a. Click **Add to Groups**.
    b. Find and select the appropriate group, and then click **OK**.
6. To remove this group from another group, select the group, and then click **Remove**.

Setting Group Membership Security Permissions

You can set Active Directory security permissions for group memberships. These permissions specify who can view (read) and modify (write) group memberships using Microsoft Outlook. These settings let you more effectively secure distribution lists and security groups in your environment. You cannot modify inherited security permissions.

Note

When you manage group membership security, disabled permissions may indicate inherited permissions.

To set group membership security permissions:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group whose membership you want to secure, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Properties**.
4. Click **Membership security**.
5. Select the user account or group you want to grant or deny security permissions. To specify a different user account or group, click **Add**.
6. Under Permissions, select the appropriate security settings:
    - To allow the selected user account or group the ability to view this group membership, click **Allow** under **Read members**.
    - To deny the selected user account or group the ability to view this group membership, click **Deny** under **Read members**.
    - To allow the selected user account or group the ability to modify this group membership, click **Allow** under **Write members**.
    - To deny the selected user account or group the ability to modify this group membership, click **Deny** under **Write members**.
7. To remove all security permissions from a user or group, select the appropriate user or group, and then click **Remove**.

8. To check if a user or group has security permissions, select the appropriate user or group, and then click **Properties**.
9. Click **OK**.

Setting Group Ownership

You can set the ownership of any Microsoft Windows distribution or security groups. You can grant the group ownership permission to a user account, group, or contact. Granting group ownership allows the specified user account, group, or contact to modify the membership of this group.

Note

DRA disables the **Manager can update membership list** check box when group membership is hidden from the Microsoft Exchange server. To enable this check box, click **Expose Group Membership** on the Exchange tab of the Group Properties window. For more information, see "Exposing Group Memberships in Distribution Lists" on page 42.

To set group ownership:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group whose ownership you want to set, complete the following steps:
   a. ***If you know the group location***, select the domain and OU that contains this group.
   b. In the search pane, specify the group attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Properties**.
4. Click **Managed by**.
5. To specify a different manager for this group, click **Change**.
6. Select the **Manager can update membership list** check box, and then click **OK**.

Cloning a Group

You can clone both local groups and global groups in managed domains. Cloning groups creates new groups of the same type and attributes as the original group. DRA also attempts to add all members from the original group to the new group.

By cloning a group, you can quickly create groups based on other groups with similar properties. When you clone a group, DRA populates the Clone Group Wizard with values from the selected group. You can also modify properties for the new group.

Notes

- Your company may have a naming convention enforced through policy that determines the name you can assign to the new group.
- By default, DRA places the new group in the Users OU of the managed domain.

To clone a group:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to clone, complete the following steps:
   a. ***If you know the group location***, select the domain and OU that contains this group.
   b. In the search pane, specify the group attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Clone**.
4. On each tab, specify the appropriate settings and properties for the new group, and then click **Next**.
5. Review the summary, and then click **Finish**.

Renaming a Group

You can rename groups in the managed domain or managed subtree.

To rename a group:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to rename, complete the following steps:
   a. ***If you know the group location***, select the domain and OU that contains this group.
   b. In the search pane, specify the group attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Rename**.
4. Change the appropriate naming properties.
5. Click **OK**.

Deleting a Group

You can delete local and global groups in the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a group permanently removes the group from the Active Directory. If the Recycle Bin is enabled for that domain, deleting a group moves the group to the Recycle Bin and disables the group properties.

For more information on the Recycle Bin, see "Managing the Recycle Bin" on page 103.

Warning

When you create a group, Microsoft Windows assigns a Security Identifier (SID) to that group. The SID is not generated from the group name. Microsoft Windows uses SIDs to record privileges in access control lists (ACLs) for each resource. If you delete a group, you cannot return access capabilities for that group by creating a new group with the same name.

To delete a group:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to delete, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Moving a Group to Another Container

You can move a group to another container, such as an OU, in the managed domain or managed subtree.

To move a group to another container:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to move to another container, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Move**.
4. Select the appropriate container.
5. Click **OK**.

Exposing Group Memberships in Distribution Lists

You can expose group memberships in distribution lists for groups in the managed domain or managed subtree.

To expose group memberships in distribution lists:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group you want to modify, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Exchange Tasks**.
4. Click **Expose Group Membership**.
5. Click **Finish**, and then click **Done**.

Hiding Group Memberships from Distribution Lists

You can hide group memberships in distribution lists for groups in the managed domain or managed subtree.

Note

Hide Group Membership option is disabled for Microsoft Exchange 2007 distribution lists.

To hide group memberships in distribution lists:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the group want to modify, complete the following steps:
    a. ***If you know the group location***, select the domain and OU that contains this group.
    b. In the search pane, specify the group attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate group.
3. On the Tasks menu, click **Exchange Tasks**.
4. Click **Hide Group Membership**.
5. Click **Finish**, and then click **Done**.

Temporary Group Assignment Tasks

Temporary group assignments allow you to manage group memberships for users who only need group membership for a specific time period. This section guides you through administering temporary group assignments in the Account and Resource Management console. With the appropriate powers, you can perform tasks such as creating new temporary group assignments or removing expired temporary group assignments. You can perform these tasks only on the primary Administration server. The Tasks menu indicates which tasks you can perform when you select single or multiple temporary group assignments.

For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Temporary Group Assignment Properties

You can manage properties for temporary group assignments or saved expired temporary group assignments only on the primary Administration server. The powers you have determine which properties you can modify for a temporary group assignment.

To manage temporary group assignment properties:

1. In the left pane, expand **Account and Resource Management**.
2. Select **Temporary Group Assignment**.
3. ***If you want to specify global properties for all temporary group assignments***, complete the following steps:
    a. On the Tasks menu, click **Properties**.
    b. Change the properties and settings you want to modify.

   c. To save your changes, click **Apply**.

4. ***If you want to specify the properties for a temporary group assignment***, complete the following steps:
   a. In the list pane, select the appropriate temporary group assignment.
   b. On the Tasks menu, click **Properties**.
   c. On the appropriate tab, change the properties and settings you want to modify.

      To save your changes before you modify other properties, click **Apply**.
5. Click **OK**.

Creating a New Temporary Group Assignment

You can create a temporary group assignment only on the primary Administration server. You can also modify properties, such as schedules, for the new temporary group assignment.

To create a temporary group assignment:

1. In the left pane, expand **Account and Resource Management**.
2. Select **Temporary Group Assignment**.
3. On the Tasks menu, click **New Temporary Group Assignment**.
4. On each tab, specify the appropriate settings and properties for the new temporary group assignment, and then click **Next**.
5. Review the summary, and then click **Finish**.

Managing User Accounts in a Temporary Group Assignment

You can add or remove user accounts from temporary group assignments on the primary Administration server.

Note
You can only manage user accounts for temporary group assignments that are not yet active.

To manage user accounts in a temporary group assignment:

1. In the left pane, expand **Account and Resource Management**.
2. Select **Temporary Group Assignment**.
3. In the list pane, select the appropriate temporary group assignment.
4. On the Tasks menu, click **Properties**.
5. Click **Group Members**.
6. ***If you want to remove a user account***, select the user account and click **Remove**.
7. ***If you want to add a new user account***, complete the following steps:
   a. Click **Add > User**.

    b. Find and select the appropriate user account, and then click **OK**.

8. Click **Apply**, and then click **OK**.

Rescheduling a Temporary Group Assignment

You can reschedule temporary group assignments only on the primary Administration server. You can also reschedule a saved expired temporary group assignment.

Note

When a temporary group assignment expires, DRA automatically deletes it, unless you saved it for future use.

To reschedule a temporary group assignment:

1. In the left pane, expand **Account and Resource Management**.
2. Select **Temporary Group Assignment**.
3. In the list pane, select the appropriate temporary group assignment.
4. On the Tasks menu, click **Properties**.
5. Click **Schedule**.
6. Specify new start and end times. If the temporary group assignment is active, you can only specify the end time.
7. ***If you want to save a temporary group assignment for future use***, select the **Keep this temporary assignment for future use** check box.
8. Click **OK**.

Deleting a Temporary Group Assignment

You can delete any temporary group assignment on the primary Administration server.

To delete a temporary group assignment:

1. In the left pane, expand **Account and Resource Management**.
2. Select **Temporary Group Assignment**.
3. In the list pane, select the appropriate temporary group assignment.
4. On the Tasks menu, click **Delete**.
5. Click **Yes**.

Chapter 5

Managing OUs and the Active Directory

An organizational unit (OU) is a container in the Active Directory. OUs can contain user accounts, groups, computers, contacts, and other OUs. However, an object can only be a member of one OU at a time. OUs cannot contain objects from other domains. In Microsoft Windows, an OU may be the smallest unit in which you can use your administration powers.

Built-in Containers

In addition to OUs, Microsoft Windows creates built-in containers automatically. You can neither rename these containers nor create another OU with the names of these containers. There may be additional limits on what objects these containers may contain. DRA presents only the valid options for each type of OU, object, or container.

OU Management Tasks

This section guides you through administering OUs in the Account and Resource Management console. With the appropriate powers, you can perform various OU management tasks, such as moving an OU to another container. You also can perform these tasks using the CLI. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing OU Properties

You can manage properties for OUs. The powers you have determine which properties you can modify for an OU in the managed domain or managed subtree.

To manage OU properties:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU you want to manage, complete the following steps:
    a. ***If you know the OU location***, select the domain or OU that contains this OU.
    b. In the search pane, specify the container attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate OU.
3. On the Tasks menu, click **Properties**.

4. On the appropriate tab, change the properties and settings you want to modify.

   To save these changes before you modify other properties, click **Apply**.

5. Click **OK**.

Creating an OU

You can create an OU in the managed domain or managed subtree. You can also modify general properties, such as the OU description.

To create an OU:

1. In the left pane, expand **All My Managed Objects**.
2. Select the location where you want to create this OU.

   For example, if you want this new OU to be a child of a specific OU in the managed domain, expand the domain and then select the appropriate parent OU.

3. On the Tasks menu, click **New > OU**.
4. On each tab, specify the appropriate settings and properties for the new OU, and then click **Next**.
5. Review the summary, and then click **Finish**.

Cloning an OU

You can create a new OU by cloning an existing OU from the managed domain or managed subtree. You can also modify general properties for new OU, such as the OU description. Cloning an OU does not clone the objects contained in the OU.

To clone an OU:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU you want to clone, complete the following steps:
   a. ***If you know the OU location***, select the domain or OU that contains this OU.
   b. In the search pane, specify the container attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate OU.
3. On the Tasks menu, click **Clone**.
4. On each tab, specify the appropriate settings and properties for the new OU, and then click **Next**.
5. Review the summary, and then click **Finish**.

Opening the Active Directory Tree to an OU Location

You can quickly and easily open the Active Directory tree to the location of a specific OU in the managed domain or managed subtree.

To open the Active Directory tree:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU, complete the following steps:
    a. In the search pane, specify the container attributes, and then click **Find Now**.
    b. In the list pane, select the appropriate OU.
3. On the Tasks menu, click **Open in Tree**.
4. In the left pane, the tree opens to the location of the selected OU.

Moving an OU to Another Container

You can move an OU to a different container in the managed domain. When managing a subtree of a domain, you can move OUs within the hierarchy of that subtree.

Notes

- If moving an OU to another container increases your powers for the moved OU, DRA does not permit you to move the OU.
- You can also move an OU by dragging it to the new location.

To move an OU to another container:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU you want to move, complete the following steps:
    a. ***If you know the OU location***, select the domain or OU that contains this OU.
    b. In the search pane, specify the container attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate OU.
3. On the Tasks menu, click **Move**.
4. Select the appropriate container.
5. Click **OK**.

Renaming an OU

You can quickly and easily rename an OU in the managed domain or managed subtree.

Note

When you rename objects, including OUs, consider the naming restriction. The names of OUs cannot contain leading or trailing spaces.

To rename an OU:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU you want to rename, complete the following steps:
    a. ***If you know the OU location***, select the domain or OU that contains this OU.
    b. In the search pane, specify the container attributes, and then click **Find Now**.

    c. In the list pane, select the appropriate OU.

3. On the Tasks menu, click **Rename**.
4. Change the appropriate naming properties.
5. Click **OK**.

Deleting an OU

You can delete OUs from the managed domain or managed subtree. You can only delete empty OUs. If an OU contains objects, you cannot delete the OU. In order to delete an OU that contains objects, delete all of the objects first, and then delete the OU.

To delete an OU:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the OU you want to delete, complete the following steps:
    a. ***If you know the OU location***, select the domain or OU that contains this OU.
    b. In the search pane, specify the container attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate OU.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Chapter 6

Managing Contacts

DRA and ExA allows you to manage many network objects, including contacts and the associated email addresses. Contacts are available only in mixed mode or native Microsoft Windows domains. Contacts do not have a Security Identifier (SID), as do user accounts and groups. Use contacts to add members to distribution lists or groups without granting them access to the network services.

You can add contacts to security or distribution groups in mixed and native mode domains. Because security groups can be used as distribution lists in Microsoft Windows, you may want to add contacts to these groups. Having a contact in a global security group does not prevent the group from being converted to a universal security group when you migrate to a native mode Microsoft Windows domain.

Contact Management Tasks

This section guides you through administering contacts in the Account and Resource Management console. With the appropriate powers, you can perform various contact management tasks, such as cloning a contact. If you select multiple contacts, you can perform selected tasks in one operation, such as deleting, moving, or adding contacts to a group. The Tasks menu indicates which tasks you can perform when you select single or multiple contacts.

You also can perform these tasks using the Web Console or CLI. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Contact Properties

You can manage contact properties. The powers you have determine which properties you can modify for a contact in the managed domain. If you installed ExA and enabled Exchange support, you can modify email address properties while managing the contacts.

To manage contact properties:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to manage, complete the following steps:
   a. ***If you know the contact location***, select the domain and OU that contains this contact.
   b. In the search pane, specify the contact attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate contact.
3. On the Tasks menu, click **Properties**.

4. ***If you selected a single contact***, on the appropriate tab, change the properties and settings you want to modify.
5. ***If you selected multiple contacts***, complete the following steps:

   Note
   You can manage selected property values on the General, Address, and Organization property pages for contacts.

   ---

   a. On the appropriate tab, click the pencil icon next to the property or setting you want to modify.
   b. Change the property or settings you want to modify. Changing the property or settings value applies the same value to all selected objects.
   c. Click **Apply**.
   d. ***If you want to copy the contents of the Results window***, click the copy to clipboard icon on the lower left of the window.
   e. Click **OK**.
6. To save your changes before you modify other properties, click **Apply**.
7. Click **OK**.

Creating a Contact

You can create contacts in the managed domain or managed subtree. You can also modify properties, enable email and specify email addresses, and specify group memberships for the new contact.

To create a contact:

1. In the left pane, expand **All My Managed Objects**.
2. Select the location where you want to create this contact.

   For example, if you want to create this contact in a specific OU of the managed domain, expand the domain and then select the appropriate OU.
3. On the Tasks menu, click **New > Contact**.
4. On each tab, specify the appropriate settings and properties for the new contact, and then click **Next**.
5. Review the summary, and then click **Finish**.

Cloning a Contact

By cloning a contact, you can quickly create contacts based on other contacts with similar properties. When you clone a contact, DRA populates the Clone Contact Wizard with values from the selected contact. You can also modify properties, enable email and specify email addresses, and specify group memberships for the new contact.

To clone a contact:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to clone, complete the following steps:
   a. ***If you know the contact location***, select the domain and OU that contains this contact.
   b. In the search pane, specify the contact attributes, and then click **Find Now**.

    c. In the list pane, select the appropriate contact.
3. On the Tasks menu, click **Clone**.
4. On each tab, specify the appropriate settings and properties for the new contact, and then click **Next**.
5. Review the summary, and then click **Finish**.

Managing Group Memberships for Contacts

You can add or remove contacts from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this contact belongs.

To specify group membership for contacts:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to manage, complete the following steps:
    a. ***If you know the contact location***, select the domain and OU that contains this contact.
    b. In the search pane, specify the contact attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate contact.
3. In the details pane, click **Member of**. To view the details pane, click **Details** on the View menu.
4. To check a group to which the contact already belongs, select the group, and then click **Properties**.
5. To add the contact to a group, complete the following steps:
    a. Click **Add**.
    b. Find and select the appropriate group, and then click **OK**.
6. To remove the contact from a group, select the group, and then click **Remove**.

Moving a Contact to Another OU

You can move a contact to another container, such as an OU, in the managed domain or managed subtree.

To move a contact to another container:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to move to another container, complete the following steps:
    a. ***If you know the contact location***, select the domain and OU that contains this contact.
    b. In the search pane, specify the contact attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate contact.
3. On the Tasks menu, click **Move**.
4. Select the appropriate container.
5. Click **OK**.

Renaming a Contact

You can quickly and easily rename a contact in the managed domain or managed subtree.

To rename a contact:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to rename, complete the following steps:
    a. ***If you know the contact location***, select the domain and OU that contains this contact.
    b. In the search pane, specify the contact attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate contact.
3. On the Tasks menu, click **Rename**.
4. Change the appropriate naming properties.
5. Click **OK**.

Deleting a Contact

You can delete a contact from the managed domain or managed subtree. If the Recycle Bin is disabled for that domain, deleting a contact permanently removes the contact from the Active Directory. If the Recycle Bin is enabled for that domain, deleting a contact moves the contact to the Recycle Bin.

For more information on the Recycle Bin, see "Managing the Recycle Bin" on page 103.

To delete a contact:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the contact you want to delete, complete the following steps:
    a. ***If you know the contact location***, select the domain and OU that contains this contact.
    b. In the search pane, specify the contact attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate contact.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Chapter 7

Managing Exchange Mailboxes

DRA and ExA let you manage Microsoft Exchange mailboxes as an extension of user account properties. This integration allows you to simplify your administration workflows so you can effectively administer Exchange properties.

You can manage Microsoft Exchange mailboxes for user accounts in the managed domain or managed subtree. Each aspect of managing Microsoft Exchange mailboxes requires different powers. The powers you have control which mailbox properties you can modify, or whether you can create, clone, view, or delete Microsoft Exchange mailboxes. You can also manage mailbox rights and permissions associated with a user account, allowing you to control the security of your Microsoft Exchange environments. If you do not have the required power to modify a tab or field for the selected mailbox, DRA disables the tabs and fields that you cannot modify.

Mailbox Management Tasks

This section guides you through administering Microsoft Exchange mailboxes in the Account and Resource Management console. With the appropriate powers, you can perform various user account management tasks, such as creating and deleting mailboxes. You also can perform these tasks using the Web Console or CLI. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Creating a Mailbox

You can create a Microsoft Exchange mailbox for an existing user account. You can also modify properties for the new mailbox.

Note

When you create a mailbox, ExA generates the necessary proxy strings based on your Exchange policy settings. Microsoft Exchange also generates default proxy strings. As a result, when you view the properties of the newly created mailbox, you see both types of proxy strings.

To create a Microsoft Exchange mailbox:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account for whom you want to create a mailbox, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.

3. On the Tasks menu, click **Exchange Tasks**.
4. Click **Create a Mailbox**.
5. On each tab, specify the appropriate settings and properties for the new mailbox, and then click **Next**.
6. Review the summary, and then click **Finish**.

Moving a Mailbox

You can move a Microsoft Exchange mailbox for a user account to another mailbox store or Microsoft Exchange server.

To move a Microsoft Exchange mailbox:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to move, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Exchange Tasks**.
4. Click **Move Mailbox**.
5. Select the new Exchange server and mailbox store to which you want to move the mailbox, and then click **Next**.
6. Review the summary, and then click **Finish**.

Managing Mailbox Properties

You can manage properties for Microsoft Exchange mailboxes as you manage the associated user accounts. The powers you have determine which mailbox properties you can modify.

Note
You cannot modify mailbox properties of user accounts managed on member servers.

To manage Microsoft Exchange mailbox properties:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to manage, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.

4. On the appropriate Exchange tab, change the properties and settings you want to modify.

   To save these changes before you modify other properties, click **Apply**.

5. Click **OK**.

Setting Mailbox Security Permissions

You can specify which user accounts, groups, or computers you want to grant or deny the ability to send and receive email using a specific Microsoft Exchange mailbox. These settings let you more effectively secure your Exchange environment. You cannot modify inherited security permissions.

Note
When you manage mailbox security, disabled permissions may indicate inherited permissions.

To set mailbox security:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to secure, complete the following steps:
   a. ***If you know the account location***, select the domain and OU that contains this user account.
   b. In the search pane, specify the account attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Mailbox security**.
5. Select the user account, group, or computer you want to grant or deny the mailbox permissions. To specify a different user account, group, or computer, click **Add**.
6. Under Permissions, select the appropriate security settings.
   - To allow the selected user account, group, or computer to receive messages using this mailbox, click **Allow** under **Receive as**.
   - To deny the selected user account, group, or computer the ability to receive messages using this mailbox, click **Deny** under **Receive as**.
   - To allow the selected user account, group, or computer to send messages using this mailbox, click **Allow** under **Send as**.
   - To deny the user account, group, or computer the ability to send messages using this mailbox, click **Deny** under **Send as**.
7. Click **OK**.

Removing Mailbox Security Permissions

You can remove mailbox security permissions from a user account, group, or computer associated with a Microsoft Exchange mailbox. Removing mailbox security permissions prevents the user account, group, or computer account from sending and receiving email through the specified mailbox. You cannot remove inherited security permissions.

To remove mailbox security:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox security you want to change, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Mailbox security**.
5. Select the user account, group, or computer you want to prevent from using this mailbox, and then click **Remove**.
6. Click **OK**.

Setting Mailbox Rights

You can grant or deny other user accounts, groups, or computers rights to a specific Microsoft Exchange mailbox. These settings let you more effectively secure your Exchange environment. You cannot modify inherited mailbox rights.

Note
When you manage mailbox rights, disabled permissions may indicate inherited permissions.

To set mailbox rights:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to secure, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Mailbox rights**.
5. Select the user account, group, or computer you want to grant or deny the mailbox rights. To specify a different user account, group, or computer, click **Add**.
6. Under Permissions, select the appropriate settings for the mailbox right.
7. Click **OK**.

Removing Mailbox Rights

You can remove mailbox rights from user accounts, groups, or computers associated with a specific Microsoft Exchange mailbox. Removing mailbox rights prevents the user account, group, or computer account from using the specified mailbox. You cannot remove inherited mailbox rights.

To remove mailbox rights:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to secure, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Mailbox rights**.
5. Select the user account, group, or computer you want to prevent from using the mailbox, and then click **Remove**.
6. Click **OK**.

Deleting a Mailbox

You can delete a mailbox associated with a user account in the managed domain or managed subtree. Deleting a mailbox also deletes all messages in the mailbox.

To delete a mailbox:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to delete, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Exchange Tasks**.
4. Click **Delete Mailbox**.
5. Click **Finish**.

Adding an Email Address

You can specify email addresses for mailboxes associated with user accounts in your managed domain or managed subtree. You can also assign email addresses to user accounts who do not yet have mailboxes. When managing Microsoft Exchange mailboxes, you can add only the email address types defined by your proxy generation policies.

To add an email address:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account to whom you want to assign an email address, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.

    c. In the list pane, select the appropriate user account.

3. On the Tasks menu, click **Properties**.
4. To specify a new email address for a Microsoft Window account that does not have a Microsoft Exchange mailbox, complete the following steps:
    a. Click **Exchange Tasks**, and then click **Establish Email Addresses**.
    b. Specify the appropriate properties and settings for this new email address. To review the summary, click **Next**.
    c. Click **Finish**.
5. To specify a new email address for an account that has a mailbox, complete the following steps:
    a. Click **Email**.
    b. Click the add icon at the top of the window.
    c. Specify the appropriate properties and settings for this new email address, and then click **OK**.
6. Click **OK**.

Specifying an Email Address

You can modify email addresses for mailboxes associated with user accounts in the managed domain or managed subtree.

To change an email address:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account for whom you want to modify an email address, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Email**.
5. Select the email address type you want to modify, and then click the edit icon at the top of the window.
6. In the **Email Address** field, type the new address, and then click **OK**.
7. Click **OK**.

Specifying a Reply Address

You can set reply addresses for a mailbox associated with a user account in the managed domain or managed subtree. You can set several reply addresses for a mailbox. However, you cannot set more than one email address type as a reply address. For example, you cannot specify more than one Internet address as a reply address.

To specify a reply address:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to modify, complete the following steps:
    a. ***If you know the account location***, select the domain and OU that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Email**.
5. Select the email address type you want to use as the reply address. To specify a different email address type, click the add icon at the top of the window.
6. Click the appropriate icon at the top of the window for setting the email address as the reply address.
7. Click **OK**.

Deleting an Email Address

You can delete an email address by removing the address from the mailbox.

To delete an email address:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account for whom you want to delete an email address, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Email**.
5. Select the email address type you want to delete, and then click the remove icon at the top of the window.
6. Click **OK**.

Setting Delivery Options

You can specify which mailboxes the user can use to send messages, set forwarding options, and specify recipient limits.

To set delivery options:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to modify, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.

    c. In the list pane, select the appropriate user account.

3. On the Tasks menu, click **Properties**.
4. Click **Delivery options**.
5. Specify the appropriate options for the mailbox of this user account.
6. Click **OK**.

Setting Delivery Restrictions

By setting delivery restrictions, you can limit the size of incoming and outgoing messages and the acceptance incoming messages to a specific mailbox.

To set delivery restrictions:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to modify, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Delivery restrictions**.
5. Specify the appropriate restrictions for the mailbox of this user account.
6. Click **OK**.

Setting Storage Limits

You can specify storage limits, such as warnings based on the size of a mailbox. You can also specify retention times for deleted items.

To specify storage limits:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox you want to modify, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Storage limits**.
5. Specify the appropriate storage limit information.
6. Click **OK**.

Checking Mailbox Move Status

You can check the status of mailbox moves and take actions on them, such as clearing the status, canceling a move, and resuming a move that has been interrupted.

To check the status of mailbox moves:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account whose mailbox move status you want to check, complete the following steps:
    a. ***If you know the account location***, select the domain that contains this user account.
    b. In the search pane, specify the account attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate user account.
3. On the Tasks menu, click **Properties**.
4. Click **Move Mailbox Status**.
5. View the details and status of the mailbox move and select an action, if needed.
6. Click **Refresh** to update the status while the window is open.
7. Click **OK**.

Chapter 8

Managing Computers

DRA allows you to administer computers in the managed domain or managed subtree. For example, you can add or remove computer accounts in the managed domains, as well as manage the resources on each computer. When you add a computer to a domain, DRA creates a computer account in that domain for that computer. You can then connect the computer in that domain and configure the computer to use that computer account. You can also view and modify the properties of computer accounts. DRA also lets you shut down a computer and synchronize domain controllers in a managed domain.

Note

You cannot manage hidden domain controllers. The domain cache does not include hidden domain controllers. Therefore, DRA does not display hidden domain computers in lists or property windows

Computer Management Tasks

This section guides you through administering computers in the Account and Resource Management console. With the appropriate powers, you can perform various computer management tasks, such as shutting down a computer. If you select multiple computers, you can perform selected tasks in one operation, such as deleting, moving, or adding computers to a group. The Tasks menu indicates which tasks you can perform when you select single or multiple contacts.

You also can perform these tasks using the CLI and the Web Console (for Microsoft Windows domains and OUs). For more information about your assigned powers, see “Viewing Your Assigned Powers and Roles” on page 17.

Specifying Group Membership for Computers

You can add or remove computers from a specific group in the managed domain or managed subtree. You can also view or modify properties of existing groups to which this computer belongs.

To specify group membership for computers:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the computer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Member of**. To view the details pane, click **Details** on the View menu.

4. To check a group to which the computer already belongs, select the group, and then click **Properties**.
5. To add the computer to a group, complete the following steps:
   a. Click **Add to Groups**.
   b. Find and select the appropriate group, and then click **OK**.
6. To remove the computer from a group, select the group, and then click **Remove**.

Managing Computer Account Properties

You can manage computer account properties. The powers you have determine which properties you can modify for a computer in the managed domain or managed subtree.

To manage computer account properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Properties**.
4. ***If you selected a single computer***, on the appropriate tab, change the properties and settings you want to modify.
5. ***If you selected multiple computers***, complete the following steps:

   Note
   You can manage selected property values on the General, Location, and Managed by property pages for computers.

   a. On the appropriate tab, click the pencil icon next to the property or setting you want to modify.
   b. Change the property or settings you want to modify. Changing the property or settings value applies the same value to all selected objects.
   c. Click **Apply**.
   d. ***If you want to copy the contents of the Results window***, click the copy to clipboard icon on the lower left of the window.
   e. Click **OK**.
6. To save your changes before you modify other properties, click **Apply**.
7. Click **OK**.

Adding a Computer to a Domain

You can add a computer to a managed domain or managed subtree by creating a new computer account.

To add a computer to a domain:

1. In the left pane, expand **All My Managed Objects**.
2. Select the location where you want to add this computer.

   For example, if you want to create this computer in a specific OU of the managed domain, expand the domain and then select the appropriate OU.
3. On the Tasks menu, click **New > Computer**.
4. On each tab, specify the appropriate settings and properties for the new computer account, and then click **Next**.
5. Review the summary, and then click **Finish**.

Removing a Computer from a Domain

You can remove a computer from a managed domain or managed subtree by deleting the computer account.

To remove a computer from a domain:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to remove, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Shutting Down or Restarting a Computer

You can shutdown and restart a computer immediately or at a set date and time.

To shutdown or restart a computer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to shutdown or restart, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Start Shutdown**.
4. To shut down the selected computer now, click **Immediately**.
5. To shut down the selected computer at a scheduled time, click **Time**, and then specify the appropriate date and time.
6. To restart the computer after shutdown, select the **Restart after shutting down** check box.
7. Click **Start Shutdown**.

Resetting the Administrator Account Password

To reset the administrator account password for a computer, you must have the Reset Password for Local Administrator power or be associated with a role that contains this power. You can reset the administrator password for member servers in your managed domain or managed subtree. You cannot reset the administrator password for a domain controller.

To reset the administrator password:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the computer whose administrator password you want to reset, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Reset Admin Password**.
4. Specify and confirm the new password.
5. To request a generated password, select **Generate password.** Be sure to record the password DRA generates. DRA generates a password based on the Password Policy defined in the domain of the user account.
6. Click **OK**.

Resetting the Computer Account

You can reset a computer account for member servers in your managed domain or managed subtree. You cannot reset the computer account for a domain controller.

To reset the computer account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the computer account you want to reset, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Reset Account**.
4. Click **Yes**.

Deleting a Computer Account

You can delete a computer account from the managed domain or managed subtree. If you are managing a Microsoft Windows domain, you can delete computer accounts that contain other objects, such as a shared resource. If the Recycle Bin is disabled for that domain, deleting a computer account permanently removes the computer account from the Active Directory. If the Recycle Bin is enabled for that domain, deleting a computer account moves the computer account to the Recycle Bin.

For more information on the Recycle Bin, see “Managing the Recycle Bin” on page 103.

Note

You cannot delete computer accounts for member servers in the managed domain or managed subtree.

To delete a computer account:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to delete, complete the following steps:
   a. ***If you know the computer location***, select the domain or OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Delete**.
4. Click **Yes**.

Disabling a Computer Account

You can disable a computer account in the managed domain or managed subtree. Disabling a computer account prevents users on that computer from logging on to any domain.

To disable a computer account:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to disable, complete the following steps:
   a. ***If you know the computer location***, select the domain or OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Properties**.
4. On the General tab, select the **Disabled** check box.
5. Click **OK**.

Enabling a Computer Account

You can enable a computer account in the managed domain or managed subtree. Enabling a computer account allows users on that computer to log on to any domain.

To enable a computer account:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to enable, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Properties**.

4. On the General tab, clear the **Disabled** check box.
5. Click **OK**.

Managing Computer Resources

For each computer account in the managed domain or managed subtree, you can manage the associated resources, such as services, shares, devices, printers, and print jobs.

To manage computer resources:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer you want to enable, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. On the Tasks menu, click **Manage**, and then select the appropriate resource type.

Chapter 9

Managing Services

A service is a type of application that gets special treatment from the Windows operating system. Services can run even when no user is currently logged on to a computer. DRA allows Assistant Admins (AAs) with the appropriate powers to manage services through the Account and Resource Management console.

Service Management Tasks

You can manage services running on computers in the managed domain or managed subtree. You can manage services while managing other resources for that computer.

DRA allows you to start, stop, or restart a service, as well as view or modify the properties of a service. You can also modify the startup type and whether the service logs on as a system or a user account when the service starts. However, some administration tasks may not be available for specific services, depending on the service type or whether the selected service has dependencies on other services.

This section guides you through administering services in the Account and Resource Management console. With the appropriate powers, you can perform various service management tasks. You also can perform these tasks using the Web Console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Service Properties

You can manage properties for services running on computers in the managed domain or managed subtree. You can manage services while managing other resources for that computer.

To modify service properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to manage service properties, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to manage, and then click **Properties**.
5. On the appropriate tab, change the properties and settings you want to modify.
6. To save these changes before you modify other properties, click **Apply**, and then click **OK**.

Starting a Service

You can start a service on any computer in the managed domain or managed subtree.

To start a service:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to start a service, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, on the View menu click **Details**.
4. Select the service you want to start, and then click **Start**.

Starting a Service with Parameters

When you start services that accept parameters, you can specify these parameters at start up. You can start services on computers in the managed domain or managed subtree.

To start a service with parameters:

1. In the left pane, expand **All My Managed Object**s.
2. To select the computer on which you want to start a service, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to start, and then click **Start with parameters**.
5. Specify the appropriate parameters for the service startup, and then click **OK**.

Specifying the Service Startup Type

You can change the startup type of a service, such as requiring a manual startup.

To change the startup type of a service:

1. In the left pane, expand **All My Managed Object**s.
2. To select the computer on which you want to manage service properties, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service for which you want to change the startup type, and then click **Properties**.

5. On the General tab, under **Startup Type**, select the appropriate option. For example, to require a manual startup for this service, click **Manual**.
6. Click **OK**.

Specifying a Service Log On Account

You can change the service logon account to an account other than the current system account. You can specify logon accounts for services running on computers in the managed domain or managed subtree. You can specify the local system account or a specific user account.

To specify a service log on account:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer for which you want to specify a service logon account, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now.**
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to manage, and then click **Properties**.
5. Click **Log On**, and then select **This account**.
6. Specify the appropriate account name and password, and then click **OK**.

Restarting a Service

You can restart a service running on a computer in the managed domain or managed subtree.

To restart a service, you must have both the Stop a Service and Start a Service powers or be associated with a role that contains these powers, such as the Start and Stop Service role.

To restart a service:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to restart a service, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to restart, and then click **Restart**.

Stopping a Service

You can stop a service running on a computer in the managed domain or managed subtree.

To stop a service:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to stop a service, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Detail**s on the View menu.
4. Select the service you want to stop, and then click **Stop**.

Pausing a Service

You can pause a service running on a computer in the managed domain or managed subtree. Whether a service can be paused or not depends on the type of service. For example, you may not be able to pause a service that has dependent services.

To pause a service:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to pause a service, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to pause, and then click **Pause**.

Resuming a Paused Service

You can resume a service that was paused on a computer in the managed domain or managed subtree.

To resume a paused service:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to resume a service, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Services**. To access the details pane, click **Details** on the View menu.
4. Select the service you want to resume, and then click **Resume**.

Chapter 10

Managing Printers and Print Jobs

To manage printers, you manage the print queues that service those printers. DRA allows you to pause or resume, start, modify, stop, and view resource printers and published printers. DRA also lets you modify the properties and priorities of print jobs. To add or delete a printer, use the native Windows tools.

A print server is a computer on which one or more logical printers are installed. A logical printer is defined on the computer that has the printer device driver. A logical printer includes the print driver, print queue, and ports for a printer. The print server associates logical printers with printer devices.

A connected printer is defined on the computers from which documents are selected for printing. A connected printer is a connection to a print share on the network. Therefore, you can manage printers and print jobs through the associated computers.

A published printer is a printer published in Active Directory. A published printer can be a network printer that is not directly connected to a server or it can be a printer hosted by cluster server.

Printer Management Tasks

You can manage printers associated with computers in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

This section guides you through administering printers in the Account and Resource Management console. With the appropriate powers, you can perform various printer management tasks, such as stopping a printer. You also can perform these tasks using the Web Console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Printer Properties

You can manage properties for printers in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

To manage printer properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.

4. Select the printer you want to manage, and then click **Properties**.
5. On the appropriate tab, change the properties and settings you want to modify.

   To save these changes before you modify other properties, click **Apply**.
6. Click **OK**.

Pausing a Printer

You can pause a printer associated with a computer in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

To pause a printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the printer you want to pause, and then click **Pause**.

Resuming a Printer

You can resume a printer associated with a computer in the managed domain or managed subtree. DRA lets you manage printers while managing other resources for that computer.

To resume a printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the printer you want to resume, and then click **Resume**.

Print Job Management Tasks

You can manage print jobs associated with printers in the managed domain or managed subtree. Because print jobs are associated with a printer, you can manage print jobs while managing the printer.

This section guides you through managing print jobs in the Account and Resource Management console. With the appropriate powers, you can perform various print job management tasks, such as canceling a print job. You also can perform these tasks using the Web Console. The CLI allows you to manage only resource printer print jobs. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Print Job Properties

You can modify print job properties as part of your printer management workflow. Because print jobs are associated with printers, you can modify the print job while managing the corresponding printer. The print job properties you can modify depend on the type of power you have. To modify print job properties, you must be able to access the corresponding printer and computer.

To modify print job properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate printer, and then click **Manage Print Jobs**.
5. Select the print job you want to modify, and then click **Properties**.
6. Modify the appropriate properties, and then click **OK**.

Pausing a Print Job

You can pause a print job on a printer in a managed domain or managed subtree. To pause a print job, you must be able to access the corresponding printer and computer. Pausing a print job does not delete the print job from the print queue.

To pause a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
3. ***If you know the computer location***, select the domain and OU that contains this computer.
    a. In the search pane, specify the computer attributes, and then click **Find Now**.
    b. In the list pane, select the appropriate computer.
    c. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate printer, and then click **Manage Print Jobs**.
5. Select the print job you want to pause.
6. Click **Pause**.

Resuming a Print Job

You can resume a print job that was paused. To resume a print job, you must be able to access the corresponding printer and computer.

To resume a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate printer, and then click **Manage Print Jobs**.
5. Select the print job you want to resume.
6. Click **Resume**.

Restarting a Print Job

You can restart a print job that was stopped. To restart a print job, you must be able to access the corresponding printer and computer.

To restart a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate printer, and then click **Manage Print Jobs**.
5. Select the print job you want to restart.
6. Click **Restart**.

Canceling a Print Job

You can cancel a print job that is in the printer queue. When you cancel a print job, DRA permanently deletes the print job from the printer queue. To cancel a print job, you must be able to access the corresponding printer and computer.

To cancel a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose printer you want to manage, complete the following steps:

   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Printers**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate printer, and then click **Manage Print Jobs**.
5. Select the print job you want to cancel.
6. Click **Cancel**.

Published Printer Management Tasks

You can manage published printers in the managed domain or managed subtree. You can add or search for any printer that is published in the Active Directory or printers that are hosted by cluster server.

This section guides you through administering published printers in the Account and Resource Management console. With the appropriate powers, you can perform various printer management tasks, such as stopping a printer. You also can perform these tasks using the Web Console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Published Printer Properties

You can manage properties for published printers in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

To manage published printer properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to manage, complete the following steps:
   a. ***If you know the published printer location***, select the domain and OU that contains this printer.
   b. In the search pane, specify the printer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate printer.
3. On the Tasks menu, click **Properties**.
4. On the appropriate tab, change the properties and settings you want to modify.
5. To save these changes before you modify other properties, click **Apply**.
6. Click **OK**.

Refreshing Published Printer Information

You can refresh the published printer information in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

To refresh published printer information:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to manage, complete the following steps:
   1. ***If you know the published printer location***, select the domain and OU that contains this printer.
   2. In the search pane, specify the printer attributes and then click **Find Now**.
   3. In the list pane, select the appropriate printer.

      Note
      You can refresh multiple published printers at the same time.
3. Click **Refresh**.

Pausing a Published Printer

You can pause a published printer in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

To pause a published printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to pause, complete the following steps:
   1. ***If you know the published printer location***, select the domain and OU that contains this printer.
   2. In the search pane, specify the printer attributes, and then click **Find Now**.
   3. In the list pane, select the appropriate printer.

      Note
      You can pause multiple published printers at the same time.
3. On the Tasks menu, click **Pause**.

Resuming a Published Printer

You can resume a published printer that was paused in the managed domain or managed subtree. DRA lets you manage published printers while managing other resources.

To resume a published printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to resume, complete the following steps:
   1. ***If you know the published printer location***, select the domain and OU that contains this printer.
   2. In the search pane, specify the printer attributes, and then click **Find Now**.

c. In the list pane, select the appropriate printer.

Note
You can resume multiple published printers at the same time.

---

3. On the Tasks menu, click **Resume**.

Moving a Published Printer

You can move a published printer available in one container in the managed domain to another container in the same domain. DRA lets you manage published printers while managing other resources.

To move a published printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to move, complete the following steps:
    a. ***If you know the published printer location***, select the domain and OU that contains this printer.
    b. In the search pane, specify the printer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate printer.

Note
You can move multiple published printers at the same time.

---

3. On the Tasks menu, click **Move**.
4. Select the appropriate container, and then click **OK**.

Renaming a Published Printer

You can rename a shared published printer in the Active Directory. DRA lets you manage published printers while managing other resources.

Note
Renaming a published printer in Active Directory does not change the resource printer share name or propagate the name change to the resource printer you want to manage. For example, if the resource printer name is `Emerald` and you rename the printer to `Ruby` in Active Directory, other users will see the printer name as `Ruby`, but the resource printer name will continue to be `Emerald`.

To rename a published printer:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer you want to rename, complete the following steps:
    a. ***If you know the published printer location***, select the domain and OU that contains this printer.
    b. In the search pane, specify the printer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate printer.
3. On the Tasks menu, click **Rename**.
4. Type the new printer name, and then click **OK**.

Print Job Management Tasks for Published Printers

You can manage printer jobs associated with published printers in the managed domain or managed subtree. Because print jobs are associated with a printer, you can manage print jobs while managing the published printer.

This section guides you through administering published printers in the Account and Resource Management console. With the appropriate powers, you can perform various print job management tasks, such as canceling a print job. You also can perform these tasks using the Web Console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Print Job Properties

You can modify print job properties as part of your published printer management workflow. Because print jobs are associated with printers, you can modify the print job while managing the corresponding published printer. The print job properties you can modify depend on the type of power you have. To modify print job properties, you must be able to access the corresponding published printer.

To manage print job properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer that is processing the print jobs that you want to manage, complete the following steps:
    a. ***If you know the published printer location***, select the domain and OU that contains this printer.
    b. In the search pane, specify the printer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate printer.
3. In the details pane, click **Manage Print Jobs**. To access the details pane, click **Details** on the View menu.
4. Select the print job you want to modify, and then click **Properties**.

Note
You can manage multiple print jobs of a published printer at the same time.

5. Modify the appropriate properties, and then click **OK**.

Pausing a Print Job

You can pause a print job on a published printer in a managed domain or managed subtree. To pause a print job, you must be able to access the corresponding published printer. Pausing a print job does not delete the print job from the print queue.

To pause a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer that is processing the print job that you want to pause, complete the following steps:
    a. ***If you know the published printer location***, select the domain and OU that contains this printer.

   b. In the search pane, specify the printer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate printer.
3. In the details pane, click **Manage Print Jobs**. To access the details pane, click **Details** on the View menu.
4. Select the print job you want to pause.

Note
You can pause multiple print jobs of a published printer at the same time.

---

5. Click **Pause**.

Resuming a Print Job

You can resume a print job that was paused in a managed domain or managed subtree. To resume a print job, you must be able to access the corresponding published printer.

To resume a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer that is processing the print job you want to resume, complete the following steps:
   a. ***If you know the published printer location***, select the domain and OU that contains this printer.
   b. In the search pane, specify the printer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate printer.
3. In the details pane, click **Manage Print Jobs**. To access the details pane, click **Details** on the View menu.
4. Select the print job you want to resume.

Note
You can resume multiple print jobs of a published printer at the same time.

---

5. Click **Resume**.

Restarting a Print Job

You can restart a print job that was stopped in a managed domain or managed subtree. To restart a print job, you must be able to access the corresponding published printer.

To restart a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer that is processing the print job you want to restart, complete the following steps:
   a. ***If you know the published printer location***, select the domain and OU that contains this printer.
   b. In the search pane, specify the printer attributes, and then click **Find Now**.

c. In the list pane, select the appropriate printer.

3. In the details pane, click **Manage Print Jobs**. To access the details pane, click **Details** on the View menu.
4. Select the print job you want to restart.

Note
You can restart multiple print jobs of a published printer at the same time.

---

5. Click **Restart**.

Canceling a Print Job

You can cancel a print job that is in the printer queue in a managed domain or managed subtree. When you cancel a print job, DRA permanently deletes the print job from the printer queue. To cancel a print job, you must be able to access the corresponding published printer.

To cancel a print job:

1. In the left pane, expand **All My Managed Objects**.
2. To select the published printer that is processing the print job you want to cancel, complete the following steps:
   a. ***If you know the published printer location***, select the domain and OU that contains this printer.
   b. In the search pane, specify the printer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate printer.
3. In the details pane, click **Manage Print Jobs**. To access the details pane, click **Details** on the View menu.
4. Select the print job you want to cancel.

Note
You can cancel multiple print jobs of a published printer at the same time.

---

5. Click **Cancel**.

Chapter 11

Managing Shares

A share is a way to make resources, such as files or printers, available to other users on the network. Each share has a share name that refers to a shared folder on the server. DRA manages the shares only on the computers in the managed domains. To successfully manage shares, the access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage resources. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

Share Management Tasks

You can manage shares associated with computers in the managed domain or managed subtree. Because shares are associated with a computer, you can manage shares while managing other resources for that computer.

DRA allows you to create, clone, or delete a share, as well as view and modify the properties of a share. You can modify the path or comment of a share. You can also limit the number of user accounts able to connect to a share at one time to conform to licensing agreements or to reduce activity on busy servers.

This section guides you through administering shares in the Account and Resource Management console. With the appropriate powers, you can perform various share management tasks, such as managing share properties. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Share Properties

You can manage properties for shares in the managed domain or managed subtree. DRA lets you manage shares while managing other resources for that computer.

To manage share properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to manage shares, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Shares**. To access the details pane, click **Details** on the View menu.
4. Select the share you want to manage, and then click **Properties**.

5. On the appropriate tab, change the properties and settings you want to modify.

   To save these changes before you modify other properties, click **Apply**.
6. Click **OK**.

Creating a Share

You can create a share for a computer in the managed domain or managed subtree. You can also modify properties for this share.

To create a share:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to create a share, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Shares**, and then click **New.** To access the details pane, click **Details** on the View menu.
4. On each tab, specify the appropriate settings and properties for the new share, and then click **Next**.
5. Review the summary, and then click **Finish**.

Cloning a Share

You can clone a share for a computer in the managed domain or managed subtree. By cloning a share, you can quickly create shares based on other shares with similar properties. This flexibility lets you enforce consistent settings for all shares you create in a given domain.

When you clone a share, DRA populates the Clone Share Wizard with values from the selected share. You can also modify properties for the new share.

To clone a share:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer on which you want to manage shares, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Shares**, and then click **Clone**. To access the details pane, click **Details** on the View menu.
4. On each tab, specify the appropriate settings and properties for the new share, and then click **Next**.
5. Review the summary, and then click **Finish**.

Deleting a Share

You can delete shares from computers in the managed domain or managed subtree.

To delete a share:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose share you want to delete, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Shares**. To access the details pane, click **Details** on the View menu.
4. Select the share you want to delete, and then click **Delete**.
5. Click **Yes**.

Chapter 12

Managing Advanced Queries

Regular DRA search functionality allows you to search on attributes of objects in Active Directory such as users, computers, printers, groups, and OUs. It also allows you to specify wildcard character searches. However, you cannot use DRA search functionality to search on customized attributes, like account lockout status or account expired status. Advanced search queries enable you to perform searches using customized attributes that are not available through the DRA search functionality. DRA uses LDAP to support the advanced queries feature. You can use advanced queries to search for users, contacts, groups, computers, printers, OUs, and any other object that DRA supports.

Advanced Search Query Management Tasks

DRA allows you to save, modify, copy, delete, and share advanced queries that you create. If you are familiar with the LDAP query language, you can type your LDAP query, validate the query, and share it with other AAs by saving it as a public query. If you are not familiar with the LDAP query language, you can use saved queries or import queries from the Active Directory User and Computers (ADUC) management console. You can manage advanced search queries on both the primary Administration server and secondary Administration servers.

This section guides you through administering advanced queries in the Account and Resource Management console. Different advanced query management tasks require different powers. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Creating a New Advanced Query

You can create an advanced query on either the primary Administration server or the secondary Administration server. You can also modify properties, such as the query string, for the new advanced query.

To create an advanced query:

1. In the left pane, expand **Account and Resource Management** and select **All My Managed Objects**.
2. Click the Advanced Search toolbar button.
3. Expand **Advanced Queries**.
4. Select either **Public Queries** or **My Queries**.
5. On the Tasks menu, click **New Query**.

6. Specify the appropriate settings and properties, such as the query string, for the new advanced query, and then click **OK**.

Note

Alternatively, you can create a new advanced query using the advanced search pane of a container. In the advanced search pane, select the criteria for your query, click **Find Now**, and then click **Save**.

Modifying an Advanced Query

You can change certain properties of a saved advanced query under **Public Queries** only if you have the necessary permissions to modify shared advanced queries. You can modify the properties of any query that you save under **My Queries**.

To modify an advanced query:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.
4. In the list pane, select the advanced query you want.
5. On the Tasks menu, click **Edit Query**.
6. Change the properties you want, click **Apply**, and then click **OK**.

Note

Alternatively, you can edit a saved advanced query using the advanced search pane of a container. In the advanced search pane, select an advanced query from the **Saved Queries** list, click **Load Query**, and then click **Find Now**. DRA displays the query details in the details pane and allows you to modify the query string. To save the changes to the query string, click **Save As**.

Copying an Advanced Query

You can copy advanced queries between **Public Queries** and **My Queries**. When you copy an advanced query to **Public Queries**, Assistant Admins with the necessary powers can modify and execute the advanced query.

To copy an advanced query:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.
4. In the list pane, select the advanced query you want.
5. If you want to copy an advanced query from **Public Queries**, click **Copy to My Queries** on the Tasks menu.
6. If you want to copy an advanced query from **My Queries**, click **Copy to Public Queries** on the Tasks menu.

Customizing Advanced Query Results

DRA provides you with a default set of columns in the search results list. To customize your search results, you can add or remove columns in the list of search results. You can customize the search results when you are creating a new advanced query or modifying an advanced query.

To customize advanced query results:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.
4. In the list pane, select the advanced query you want.
5. On the Tasks menu, click **Edit Query**.
6. In the Edit Query window, click **Choose Columns**.
7. ***If you want to use the default set of columns that DRA provides***, select the **Use default columns** radio button.
8. ***If you want to add or remove columns***, select the **Use specific columns** radio button.
9. Select the columns you want, and then click **OK**.

Notes

- You can view or modify object properties in the search results if you have the relevant powers.
- To change the order of the columns in the advanced search pane, click **Move Up** or **Move Down**.

Importing an Advanced Query

You can import advanced queries that you create in ADUC instead of creating these advanced queries again using DRA. You can only import advanced queries that are in XML format.

To import an advanced query:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.
4. On the Tasks menu, click **Import Query**.
5. Browse and select the appropriate advanced query, and then click **Open**.

Exporting an Advanced Query

You can export advanced queries that you create in DRA instead of creating these advanced queries again in ADUC.

To export an advanced query:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.

4. In the list pane, select the advanced query you want you want to export.
5. On the Tasks menu, click **Export Query**.
6. Browse and select the folder you want, and then click **Save**.

Deleting an Advanced Query

You can delete advanced queries under **Public Queries** only if you have the necessary permissions to delete shared advanced queries. You can delete any advanced query that is under **My Queries**.

To delete an advanced query:

1. In the left pane, expand **Account and Resource Management**.
2. Expand **Advanced Queries**.
3. Select either **Public Queries** or **My Queries**.
4. In the list pane, select the advanced query you want to delete.
5. On the Tasks menu, click **Delete**.
6. Click **Yes**.

Chapter 13

Managing Connected Users

A session is established whenever a user connects to a particular resource on a remote computer. A connected user is a user connected to a shared resource on the network.

DRA manages the connected users only on the computers in the managed domains. The access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage connected users. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

Connected User Management Tasks

You can view and disconnect users from resources on the network. When you disconnect a session, it does not log the user out or keep the user from connecting to the resource again.

This section guides you through administering connected users in the Account and Resource Management console. With the appropriate powers, you can perform these connected user management tasks. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Disconnecting a User

You can disconnect a connected user from a computer in the managed domain or managed subtree. You must be able to access the computer and this open session. Disconnecting a connected user ends the open session.

To disconnect a connected user:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Connected Users**. To access the details pane, click **Details** on the View menu.
4. Select the user account you want to disconnect, and then click **Disconnect**.

Refreshing the List of Connected Users

To ensure you are viewing the latest information about open sessions on a computer, manually refresh the list of connected users. You must be able to access the computer and this open session.

To refresh the list of connected users:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Connected Users**. To access the details pane, click **Details** on the View menu.
4. Click **Refresh**.

Chapter 14

Managing Devices

A device is any piece of equipment attached to a network, such as a computer, printer, modem, or any other peripheral equipment.

Although a device may be installed on your computer, Windows cannot recognize the device until you install and configure the appropriate driver. A device driver enables a specific piece of hardware to communicate with the operating system.

DRA allows you to configure and manage the devices only on the computers in the managed domains. The access account must have administrator permissions, such as being a member of the local Administrators group, on all computers where you want to manage devices. To assign these permissions, add the access account to the native Domain Admins group in the domain of the computer.

Device Management Tasks

The built-in resource roles provide a range of powers to let you manage devices. DRA lets you manage devices while managing other resources for that computer.

This section guides you through administering devices in the Account and Resource Management console. With the appropriate powers, you can perform various device management tasks, such as stopping a device. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Managing Device Properties

You can modify the properties of a device on a specific computer. Modifying the device properties for a device allows you to modify the startup type for a device.

To modify device properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose device you want to modify, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Devices**. To access the details pane, click **Details** on the View menu.

4. Select the appropriate device, and then click **Properties**.
5. Change the appropriate device properties, and then click **OK**.

Starting a Device

You can start a device on a specific computer in the managed domain or managed subtree.

To start a device:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose device you want to start, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Devices**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate device, and then click **Start**.

Stopping a Device

You can stop a device on a specific computer in the managed domain or managed subtree.

To stop a device:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose device you want to stop, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Devices**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate device, and then click **Stop**.

Chapter 15

Managing Event Logs

An event is an important system or application occurrence. The Windows operating system records information about events in event log files. There may be several event logs stored on each computer. Use the native Windows Event Viewer to view event logs. DRA manages the event logs only on the computers in the managed domains.

DRA records user-initiated operations in the log archive, a secure repository. You have the option to have DRA also record user-initiated operations in the Windows Event Log in addition to recording the information in the DRA log archive. For more information, see "How DRA Uses Log Archives" on page 106.

Event Log Types

Computers running Microsoft Windows record additional information in various logs. The logs are briefly described as follows:

ACWebpart	Records events logged by the NetIQ Reporting Center.
ADAM	Records events logged by the ADAM repository.
Application	Records events logged by an application on the computer, such as a service startup or failure. For example, DRA and ExA store events in the Application log.
Directory service	Records events related to domain controllers maintaining the security database.
File replication service	Records events related to file replication services provided by the operating system.
NetIQ DRA Core service	Collects data from Active Directory and DRA for reporting requests and generates Activity Detail reports when they are requested.
Security	Records events that include logon attempts, file and directory access, and security policy changes that are based on the audit policy options.
System	Records events logged by the Windows system components, such as the failure of a driver or services starting and stopping.

Event Log Management Tasks

You can specify the maximum size of an event log file and what happens to an event log when it becomes full. The properties window also displays the name of the log, the log file path and filename, when the log was created, when it was last modified, and when it was last accessed. If you choose to back up the log file, DRA saves the event log with a unique file name in a standard location on the selected computer.

DRA lets you manage event logs while managing other resources for that computer. This section guides you through administering shares in the Account and Resource Management console. With the appropriate powers, you can perform various share management tasks, such as changing event log properties. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Enabling and Disabling Windows Event Log Auditing for DRA

When you install DRA, audit events are not logged in the Windows event log by default. You can enable this type of logging by modifying a registry key.

Warning

Be careful when editing your Windows Registry. If there is an error in your Registry, your computer may become nonfunctional. If an error occurs, you can restore the Registry to its state when you last successfully started your computer. For more information, see the Help for the Windows Registry Editor.

To enable event auditing:

1. Click **Start** > **Run**.
2. Type `regedit` in the **Open** field and click **OK**.
3. Expand the following registry key:
   `HKLM\Software\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`

   Note

   If you are editing the registry on a 64-bit operating system, expand `HKLM\Software\WOW6432Node` instead of `HKLM\Software`. The rest of the path remains the same.
4. Click **Edit** > **New** > **DWORD Value**.
5. Enter `IsNTAuditEnabled` as the key name.
6. Click **Edit** > **Modify**.
7. Enter `1` in the **Value data** field and click **OK**.
8. Close Registry Editor.

To disable event auditing:

1. Click **Start** > **Run**.
2. Type `regedit` in the **Open** field and click **OK**.

3. Expand the following registry key:
   `HKLM\Software\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`

   Note
   If you are editing the registry on a 64-bit operating system, expand `HKLM\Software\WOW6432Node` instead of `HKLM\Software`. The rest of the path remains the same.

   ---

4. Select the `IsNTAuditEnabled` key.
5. Click **Edit > Modify**.
6. Enter `0` in the **Value data** field and click **OK**.
7. Close Registry Editor.

Managing Event Log Properties

You can modify event log properties for a specific computer.

To modify event log properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose event log you want to modify, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Event Logs**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate event log, and then click **Properties**.
5. Change the appropriate log size properties.
6. Click **OK**.

Viewing Event Log Entries

You can view entries in a specific event log for a computer in the managed domain or managed subtree. When you view an event log, DRA launches the native Windows Event Viewer.

To view event log properties:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose event log you want to view, complete the following steps:
   a. ***If you know the computer location***, select the domain and OU that contains this computer.
   b. In the search pane, specify the computer attributes, and then click **Find Now**.
   c. In the list pane, select the appropriate computer.
3. In the details pane, click **Event Logs**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate event log, and then click **Launch Event Viewer**.

Clearing the Event Log

You can clear entries in a specific event log for a computer in the managed domain or managed subtree. You can also save the event log entries before clearing the log.

Warning

Clearing an event log is an irreversible action. You cannot recover a cleared event log unless you save the event log before you clear the event log.

To clear event logs:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose event log you want to clear, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Event Logs**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate event log, and then click **Clear**.
5. ***If you want to save the current event log entries before clearing the log***, click **Yes**. Note the location where DRA saves the event log file, and then click **OK**.
6. ***If you want to clear the log without saving the event log entries***, click **No**.

Chapter 16

Managing Open Files

An open file is a connection to shared resources, such as files or pipes. A pipe is an inter-process communication mechanism that allows one process to communicate with another local or remote process.

DRA manages open files only on computers in the managed domain and managed subtree. Because open files are associated with a computer, you can manage open files while managing other resources for that computer. For example, you may want to close open files when you shut down a system or install a new device or service. You can also monitor which files users access most often, helping you better assess file security.

Open File Management Tasks

This section guides you through administering open files in the Account and Resource Management console. With the appropriate powers, you can close an open file or view open files for a specific computer. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Closing a File

You can close open files from resources on the network. It is a good idea to notify users when you intend to close open files. They may need time to save their data. To close an open file, you must be able to access the corresponding computer.

To close open files:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose open file you want to close, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Open Files**. To access the details pane, click **Details** on the View menu.
4. Select the appropriate open file, and then click **Close**.

Refreshing the List of Open Files

To ensure you are viewing the latest information about open sessions on a computer, manually refresh the list of connected users. To refresh the open file list, you must be able to access the corresponding computer.

To refresh open files:

1. In the left pane, expand **All My Managed Objects**.
2. To select the computer whose open file you want to list, complete the following steps:
    a. ***If you know the computer location***, select the domain and OU that contains this computer.
    b. In the search pane, specify the computer attributes, and then click **Find Now**.
    c. In the list pane, select the appropriate computer.
3. In the details pane, click **Open Files**. To access the details pane, click **Details** on the View menu.
4. Click **Refresh**.

Chapter 17

Managing the Recycle Bin

The Recycle Bin provides a safety net by allowing you to delete user accounts, groups, contacts, and computer accounts on a temporary basis. You can then restore these objects to their original state with all data, such as SIDs, ACLs, and group memberships intact or permanently delete these objects. This flexibility provides a safer way to manage user accounts, groups, contacts, and computer accounts.

Recycle Bin Tasks

By default, the Recycle Bin is enabled. This means that when you delete an object, that object is automatically retained in the Recycle Bin until you take further action. Use the Recycle Bin to permanently delete objects, restore objects, or view disabled object properties. For more information about the Recycle Bin, see the *Administration Guide for Directory Resource Administrator and Exchange Administrator*.

If you have the appropriate powers, you can delete user accounts, groups, contacts, and computer accounts to the Recycle Bin using the Web Console, Account and Resource Management console, or Delegation and Configuration console. If you have the appropriate powers, you can also restore these deleted objects from the Recycle Bin using the Web Console, Account and Resource Management console, or Delegation and Configuration console. For more information about your assigned powers, see "Viewing Your Assigned Powers and Roles" on page 17.

Restoring an Object from the Recycle Bin

You can restore deleted objects back to the containers from which you deleted the objects. DRA restores these objects to their original state with all data, such as SIDs, ACLs, and group memberships intact. An object can be a user account, group, contact, or computer account.

To restore an object from the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. Select the appropriate domain.
3. In the right pane, select the object you want to restore.

   Note
   You can restore multiple similar objects at the same time. For example, you can restore multiple user accounts at the same time.

4. To check the object before you restore it, click **Properties** on the Tasks menu.
5. On the Tasks menu, click **Restore**.

Restoring All Objects

You can restore all objects from the Recycle Bin for a managed domain. You can restore objects from the Recycle Bin for a specific domain or across all managed domains. To restore objects from a Recycle Bin for a specific domain, the Recycle Bin must be enabled for that domain.

To restore all objects from the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. To restore objects from the Recycle Bin for a specific domain, select the appropriate domain.
3. On the Tasks menu, click **Restore All**.

Deleting an Object from the Recycle Bin

You can permanently delete objects from the Recycle Bin for a managed domain. Once you delete an object from the Recycle Bin, you cannot restore the object. An object can be a user account, group, contact, or computer account.

To delete an object from the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. Select the appropriate domain.
3. In the right pane, select the object you want to delete.

Note
You can delete multiple similar objects at the same time. For example, you can delete multiple user accounts at the same time.

4. To check the object before you delete it, click **Properties** on the Tasks menu.
5. On the Tasks menu, click **Delete**.

Emptying the Recycle Bin

You can empty the Recycle Bin for a managed domain. Emptying the Recycle Bin permanently deletes any objects currently in the Recycle Bin. You can empty the Recycle Bin for a specific domain or across all managed domains. To empty a Recycle Bin for a specific domain, the Recycle Bin must be enabled for that domain. Once you empty the Recycle Bin, you cannot restore the deleted objects.

To empty the Recycle Bin:

1. In the left pane, expand **Recycle Bin**.
2. To empty the Recycle Bin for a specific domain, select the appropriate domain.
3. On the Tasks menu, click **Empty Recycle Bin**.

Chapter 18

Generating Reports

Auditing user actions is among the most important aspects of a sound security implementation. To allow you to review and report on Assistant Admin (AA) actions, DRA logs all user operations in the log archive on the Administration server computer. DRA provides clear and comprehensive reporting that includes before and after values of the audited events so that you can see exactly what changed.

Understanding DRA Reporting

DRA Reporting provides two methods of generating reports that allow you to see the latest changes in your environment and to collect and review user account, group, and resource definitions in your domain.

Activity Detail reports

Accessed through the ARM console and the Delegation and Configuration console, these reports provide real-time change information for objects in your domain.

DRA Management reports

Accessed through NetIQ Reporting Center (Reporting Center), these reports provide activity, configuration, and summarization information about events in your managed domains. Some reports are available as graphical representations of the data.

For example, you can view a list of changes made to an object or by an object during a specified time period using Activity Detail reports. You can also view a graph showing the number of events in each managed domain during a specified time period using Management reports. Reporting also allows you to view details about the DRA security model, such as ActiveView and AA group definitions.

DRA disables functions and reports that your license does not support. You must also have the appropriate powers to run and view reports. Therefore, you may not have access to some reports.

Activity Detail reports are available as soon as you install DRA through the ARM console and the Delegation and Configuration console to provide the latest details on your network changes.

DRA Management reports can be installed and configured as an optional feature and are viewed in Reporting Center. When you enable and configure data collection, DRA collects information about audited events and exports it to a SQL Server database on a schedule that you define. When you connect to this database in Reporting Center, you have access to over 60 built-in reports:

- Activity reports that show who did what, and when
- Configuration reports that show the state of AD or DRA at a specific point in time
- Summarization reports that show activity volume

For more information about configuring data collection for Management reports, see the *Administrator Guide*.

How DRA Uses Log Archives

To allow you to review and report on Assistant Admin (AA) actions, DRA logs all user operations in the log archive on the Administration server computer. User operations include all attempts to change definitions, such as updating user accounts, deleting groups, or redefining ActiveViews. DRA also logs specific internal operations, such as Administration server initialization and related server information. In addition to logging these audit events, DRA logs the before and after values for the event so that you can see exactly what changed.

DRA uses a folder, **NetIQLogArchiveData**, called a **log archive** to securely store archived log data. DRA archives the logs over time and then deletes older data to make room for newer data through a process called grooming.

DRA uses the audit events stored in the log archive files to display Activity Detail reports, such as showing what changes have been made to an object during a specified time period. You can also configure DRA to export information from these log archive files to a SQL Server database that NetIQ Reporting Center uses to display Management reports.

DRA always writes audit events to the log archive. You can enable or disable having DRA write events to the Windows event logs as well. For more information, see "Enabling and Disabling Windows Event Log Auditing for DRA" on page 98.

For more information about DRA auditing, see the *Administrator Guide*.

Understanding Dates and Times

DRA uses the **Short date style** and **Time style** specified in the Regional Settings application in Control Panel for report display. DRA reports show UTC date and time as well as local date and time for events. DRA reports support the following date formats:

- `m/d/yy`
- `m-d-yy`
- `m/d/yyyy`
- `m-d-yyyy`
- `mm/dd/yy`
- `mm-dd-yy`
- `mm/dd/yyyy`
- `mm-dd-yyyy`
- `dd/mm/yy`
- `dd-mm-yy`
- `dd/mm/yyyy`
- `dd-mm-yyyy`

DRA Reporting Tasks

To generate DRA Management reports, install Reporting Center and enable data collection in DRA. For more information about enabling data collection, see the *Administrator Guide*. To generate Activity Detail reports, right-click over any object and click **Reporting** to see your choices for reports on that object. The following sections guide you through the various Reporting tasks.

Viewing Activity Detail Reports

Activity Detail reports display information about changes in your environment. You can view or print a report, as well as save a report in Excel, CSV, or TXT format. To view or print reports, you must be associated with the Reporting Administration role.

When viewing reports, enter criteria to specify the time period you want to display information about. You can also choose to view a report limited to changes made on specific DRA servers, and you can limit the number of rows to be included in the report. If the report size exceeds one of the following limits, DRA displays a message stating that the report is not complete:

- Size exceeds 500 MB
- Time needed to query all DRA servers exceeds 5 minutes
- Number of rows to be displayed exceeds 1000

You have the option of viewing the report containing only the information retrieved before reaching one of these limits, or you can change the report criteria to view a report that meets these limits.

To view a report:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the object for which you want to view a report, complete the following steps:
    a. ***If you know the object location***, select the domain and OU that contains this object.
    b. In the search pane, specify the object attributes, and then click **Find Now**.
3. In the list pane, right-click the object and click **Reporting**.
4. Select the type of report, such as **Changes made to objectName** or **Changes made by objectName**. The available reports vary depending on the type of object you have selected.
5. Select the start and end dates to specify the changes you want to view.
6. ***If you want to change the number of rows to be displayed***, type a number over the default value of 250.

    Note
    The number of rows displayed applies to each Administration server in your environment. If you include 3 Administration servers in the report and use the default value of 250 rows to display, up to 750 rows can be displayed in the report.

7. ***If you want to include only specific Administration servers in the report***, select **Restrict query to these DRA servers** and type the server name or names you want the report to include. Separate multiple server names with commas.

8. Click **OK**.

Note
DRA might take up to 5 seconds to display recent changes in reports. Therefore, wait at least 5 seconds after making a change before you attempt to view a report that contains the change.

Exporting Activity Detail Reports

You can export Activity Detail reports in the following formats: XLS, CSV, and TXT. The default format is Microsoft Excel format.

To export Activity Detail reports:

1. In the report window, on the File menu, click **Preview and Export**.
2. In the Preview window, on the File menu, click **Export Document > Excel File**.
3. Select your export options and click **OK**.
4. In the Save as window, type a name for the file and click **Save**.

Printing Activity Detail Reports

To print reports, you must be associated with the Reporting Administration role. You can view or print Activity Detail reports, as well as save a report in various formats.

To print Activity Detail reports:

1. In the report window, on the File menu, click **Preview and Export**.
2. In the Preview window, on the File menu, click **Print**.

Viewing Management Reports

You must install DRA Reporting and configure the DRA data collectors to be able to view Management reports in Reporting Center. For more information about installing DRA Reporting and configuring the DRA Collectors, see the *Installation Guide*.

When you log on to the Reporting Center, the Web Service uses IIS to validate the account credentials according to the way you configured the Web Service during installation.

To view Management reports:

1. Log on to the computer that is running the Reporting Center Console.
2. Start **Reporting Center Console** in the NetIQ > Reporting Center program group.
3. Provide the required information in the Logon dialog box and click **Logon**.
4. In the Navigation pane, expand **Reports > DRA Management Reports**.
5. Expand the report categories until you find a report you want to view.
6. Click the report name in the Navigation pane and the report will load in the center Results pane, displaying cached data.
7. ***If you want to see the report using the latest data,*** click **Execute Report** in the Results Pane.

You can change the default context settings to display different report results. For more information about context settings in Reporting Center, see the *Administrator Guide*.

Customizing Management Reports

More than 60 Management reports are shipped with DRA. Reporting Center gives you the flexibility to customize and deploy these reports in many ways. For more information about customizing and deploying Management reports in Reporting Center, see the *Administrator Guide*.

To customize a Management report:

1. View a report that is similar to a report you want to create. For more information, see "Viewing Management Reports" on page 108.
2. Customize the report by changing the report properties and context settings to display the information you want.
3. Click **Execute Report**.
4. On the Report menu, click **Save Report As** and specify a report title and location to save the new report.
5. Click **Save**.

For more information about working with Management reports in Reporting Center, see the *Administrator Guide*.