Trial Guide

Directory and Resource Administrator
Exchange Administrator

September 2010

Legal Notice

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

Contents

About This Book and the Library

The *Trial Guide* helps you quickly set up and evaluate the NetIQ Directory and Resource Administrator product (DRA) and the NetIQ Exchange Administrator product (ExA). It outlines steps necessary to install DRA and ExA. It also describes the important features of DRA and ExA, and how those features can benefit users.

Intended Audience

This book provides information for individuals responsible for understanding DRA and ExA concepts.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

User Guide

Provides conceptual information about DRA and ExA. This book also provides an overview of the DRA and ExA user interfaces and the Help.

Administrator Guide

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

Help

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

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 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
Installing the Trial Version of DRA and ExA

To see DRA and ExA in action, you can install the trial version of the product in a test environment and use this guide to explore the user interface and other product features.

Why You Should Install and Trial DRA and ExA

DRA and ExA help you control and manage Active Directory and Microsoft Exchange. With these products, you can:

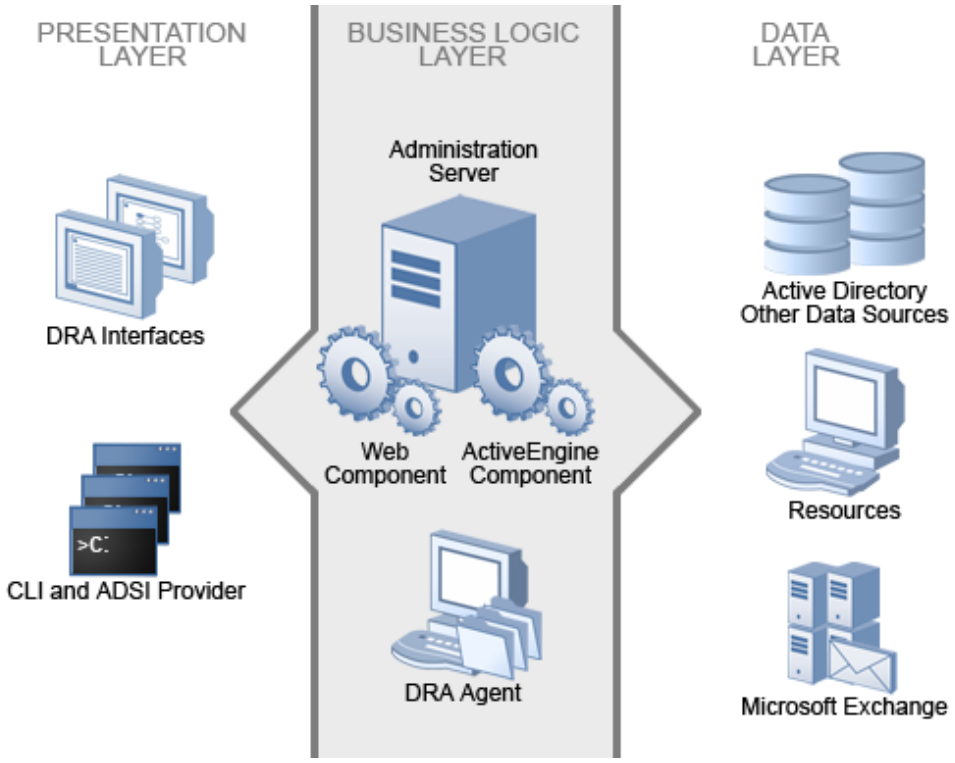
- Reduce the number of Administrator user accounts
- Provide granular delegation of permissions
- Ensure every action is logged, including before and after values of changed properties
- Enable safe distribution of data content ownership throughout your organization
- Enable unified administration of users, groups, mailboxes, resources, and other data through one consistent user interface
- Enable trigger-based automation that can cause changes outside the directory whenever the directory changes
- Provide content control by verifying the information you enter
- Create temporary group assignments that control users' access and permissions to specific resources

Using DRA and ExA to control and manage Active Directory provides benefits not available when using native or other Active Directory tools.

Understanding DRA and ExA Architecture

To evaluate DRA and ExA, install these products in a test or evaluation environment on a computer in a Microsoft Windows Server 2003, Microsoft Windows Server 2008, or Microsoft Windows Server 2008 R2 Active Directory domain with Microsoft Exchange Server 2003 or later installed. The following sections provide additional requirements for a successful product evaluation and describe the installation and configuration process. DRA may require additional software or hardware in other installation requirements. For more information, see the *Installation Guide*.

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 for 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, 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 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 intended for Help Desk personnel, data owners, and occasional administrators who perform administration tasks in addition to their primary job functions.

NetIQ Reporting Center Console

Allows administrators to view and deploy Management reports that include the following types of reports:

- activity reports that show who has done what using DRA
- configuration and environmental reports that list groups and membership, as well as disabled user accounts
- summarization reports that show change activity summaries and trend reports

Many of these reports can be viewed in a graphical representation.

Command-Line Interface

Allows administrators to make modifications from the command line to implement broad administration changes.

DRA ADSI Provider

Allows administrators to develop custom user interfaces and applications, as well as custom policy and automation triggers.

Business Logic Layer

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

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

Administration Server

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

This layer includes the following components:

ActiveEngine Component

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

NetIQ DRA Core

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

DRA Agents (optional)

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

Log Archive Service

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

Web Component

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

Data Layer

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

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

Understanding the Evaluation Process

Install DRA and ExA in a test environment for this evaluation. Before installing or starting the product, you should have a working knowledge of Active Directory, Microsoft Windows Server technology, and Microsoft Exchange Server technology. Use the Installation Checklist to ensure your environment meets all the requirements. The checklist also guides you through installing and configuring the product for evaluation before you start the guided tour.

Installation Checklist

The following checklist helps you track each task as you complete it and provides a reference to detailed steps for each task.

	Step	See Section
☐	1. Ensure the evaluation computer meets all the requirements.	For more information, see “Requirements” on page 5.
☐	2. Ensure you have a trial license.	For more information, see “Licensing Considerations” on page 8.

	Step	See Section
☐	3. Create the account you want to use as the Administration server service account.	For more information, see "Permission Considerations" on page 7.
☐	4. Create the local domain security group you want to use as the ADAM Admin account.	For more information, see "Permission Considerations" on page 7.
☐	5. Set up your environment and install any requisite software.	For more information, see "Setting Up Your Environment" on page 9.
☐	6. Install DRA and ExA on one computer.	For more information, see "Installing DRA and ExA for Evaluation" on page 10.
☐	7. Log on to the evaluation computer and start DRA and ExA.	For more information, see "Starting the DRA and ExA Consoles" on page 15.

Requirements

For evaluation, install both the Administration server and client components on a Microsoft Windows Server 2003 or Microsoft Windows Server 2008 domain controller with Microsoft Exchange Server 2003 or later installed. You can also install Microsoft Exchange Server 2003 or later on a separate server. Ensure your Microsoft Exchange Server computer and your Administration server computer are located in the same domain. The DRA and ExA evaluation computer must meet the following requirements.

Category	Requirement
Hardware	1 GHz or faster Intel Core processor 4 GB memory 500 MB temporary disk space on C Drive and 4 GB on drive where Installation folder resides
Operating System	Microsoft Windows Server 2003 Standard/Enterprise/Datacenter Edition 32-bit (x86) or 64-bit (x64) Service Pack 2 Microsoft Windows Server 2003 R2 Standard/Enterprise/Datacenter Edition 32-bit (x86) or 64-bit (x64) Service Pack 2 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter Edition 32-bit (x86) or 64-bit (x64) Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter Edition 64-bit (x64) For the most recent information about software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.
DRA Reporting (for optional Management reports)	SQL Server 2005 Service Pack 1, Service Pack 2, or Service Pack 3 SQL Server 2005 Reporting Services SQL Server 2005 Integration Services Microsoft Visual C++ 2008 Redistributable Microsoft Internet Information Services (IIS) ASP.NET installed and configured in the Default Web Site properties Named Pipes enabled

Category	Requirement
Enabled Support	NetBIOS Protocol DCOM Active scripting enabled in Internet Explorer to run the setup program. Microsoft Windows and Microsoft Exchange in English and Japanese One of the following versions of Microsoft Data Access Component (MDAC): • MDAC 2.6 • MDAC 2.6 Service Pack 1 • MDAC 2.6 Service Pack 2 • MDAC 2.7 • MDAC 2.7 Service Pack 1 • MDAC 2.8 • MDAC 2.8 Service Pack 1 Microsoft.NET Framework 3.5 Service Pack 1 Microsoft Message Queuing (MSMQ) Microsoft Core XML Services (MSXML) For the most recent information about third party software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.
Web Component	Microsoft Internet Information Services 6.0, 7.0, or 7.5 Microsoft Internet Explorer 6.0, 7.0, or 8.0 W3SVC service To enable Web Console support on 64-bit operating systems, configure IIS to support 32-bit worker processes in the Worker Process Isolation mode on 64-bit operating systems. For more information, see the NetIQ Knowledge Base available at http://support.netiq.com/dra or access the following Microsoft Knowledge Base articles: • http://support.microsoft.com/kb/894435 • http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0aafb9a0-1b1c-4a39-ac9a-994adc902485.mspx?mfr=true • http://msdn2.microsoft.com/en-us/library/zwk9h2kb.aspx
Microsoft Exchange Tools	To use ExA, install the Microsoft Exchange management tools version that matches the version of your Microsoft Exchange Server on the Administration server. To manage Exchange 2010 objects, also install the following on the Administration server: • Windows Remote Management (WinRM) 2.0 • Windows PowerShell 2.0
Microsoft Exchange Server	To install and use ExA, your Microsoft Exchange server must have LDAP support enabled and one of the following versions of Microsoft Exchange Server installed on a server in the same domain as the Administration server: • Microsoft Exchange Server 2003 Standard/Enterprise Edition Service Pack 2 • Microsoft Exchange Server 2007 Service Pack 2 • Microsoft Exchange Server 2010 with Update Rollup 4
Environment	Member of a Microsoft Windows Server 2003, Microsoft Windows Server 2008, or Microsoft Windows Server 2008 R2 native domain

DRA Considerations

Consider the following points when installing DRA for evaluation purposes:

- If the Administration server computer is not connected to a network, you may need to install the Microsoft Loopback Adapter. The error message `Network Path Not Found Error 53` may indicate that you have not correctly installed the Loopback Adapter.

- DRA and ExA log audit events in the secure, compressed log archive. If you also want DRA and ExA to log events in the Windows Application event log, you must enable this feature after installing the products. If you choose to enable logging to the Application event log, you may want to increase the size of the Application event log. For more information about enabling logging to the Application event log and increasing the size of the Application event log, see "Setting Up Your Environment" on page 9.

Note
DRA may require additional software or hardware in other installation environments. For more information, see the *Installation Guide*.

Microsoft Exchange Server Requirements

To install and use ExA, your Microsoft Exchange server must have LDAP support enabled and one of the following versions of Microsoft Exchange software installed:

- Microsoft Exchange Server 2003 Standard/Enterprise Edition Service Pack 2
- Microsoft Exchange Server 2007 Service Pack 2
- Microsoft Exchange Server 2010 with Update Rollup 4

Permission Considerations

To install DRA, you must log on with an account that has administrator permissions on the computer. To run the evaluation utilities, you must be a member of the local Administrators group in the evaluation domain.

When you install DRA and ExA, the setup program prompts you for the following accounts:

Administration server service account

Allows you to access the evaluation domain and the Microsoft Exchange server. This account should be a member of the group you use as the ADAM admin account.

ADAM Admin Account

Allows you access to your ADAM instance. This account should be a local security group.

Create these accounts using Active Directory Users and Computers (ADU&C). Note the passwords for these accounts since the setup program prompts for the account name and password during installation.

To fully evaluate DRA and ExA, ensure the accounts meet the following requirements:

Account	DRA Requirement	ExA Requirement
Administration server service	Part of an ActiveView with power to View All Objects.	• Exchange Full Administrator permissions on the Exchange organization for the evaluation domain • Member of the Account Operators group • For Exchange Server 2007 environments, must have Exchange Recipient Administrators and Exchange Server Administrators roles delegated through the Exchange 2007 Management Console • For Exchange Server 2010 environments, must be a member of the Organization Management and Recipient Management security groups
ADAM Admin Account	• Local domain security group or user account • Member of the domain you want to manage	None

The feature demonstrations in the *Trial Guide* focus on Microsoft Exchange Server 2003 management. DRA and ExA also support Microsoft Exchange Server 2007 and Microsoft Exchange Server 2010 management. For more information, see the *Installation Guide*.

In addition, the feature demonstrations assume that you manage Microsoft Windows 2003 domains. You can also manage multiple subtrees of a Microsoft Windows 2003 domains, Microsoft Windows 2008 domains, and Microsoft Windows 2008 R2 domains. For more information about setting up DRA to manage subtrees, see the *Installation Guide*.

Production Installation Differences

For evaluation, install DRA and ExA and all required software on one computer. For production installations, you may want to install the DRA Administration server and the clients on separate computers. Using the Custom installation option, you can install DRA components on different computers. Custom configurations may have additional requirements. For more information about production hardware and software requirements, see the *Installation Guide*.

Licensing Considerations

To preview the trial versions of DRA and ExA, use the trial license key included in the installation kit. Select the trial license key when you install DRA.

You have a full 30 days to use and explore the product with the trial license. To continue using DRA and ExA after the trial period, contact your NetIQ sales representative.

Setting Up Your Environment

Before you install DRA and ExA for evaluation, ensure the evaluation environment supports the product requirements so you can fully participate in the feature demonstrations.

To reduce the complexity of your evaluation environment, you should install DRA and ExA on a Microsoft Windows 2003 or Microsoft Windows 2008 domain controller.

To prepare your evaluation environment:

1. Ensure your evaluation environment supports the product requirements. For more information about product requirements, see "Requirements" on page 5.
2. Check the permissions and properties of your Administration server service account and DRA Admin account. For more information about account permissions, see "Permission Considerations" on page 7.
3. Create and share a folder named `Home` on the local hard drive of your evaluation computer and assign `Change` permissions to `Everyone`. During the feature demonstrations, DRA uses this folder to automatically create home directories for new user accounts. For more information about creating and configuring a share, see the Microsoft Windows Help.
4. Ensure your user account has a mailbox-enabled Microsoft Exchange user account.

   One of the DRA feature demonstrations uses an automation trigger script that sends an email notification to the person performing the demonstration. To view this email message, enable a Microsoft Exchange mailbox for your evaluation user account. This mailbox should be SMTP or MAPI-compliant. Open Microsoft Outlook and log on to this mailbox to see the email notification. For more information about enabling a Microsoft Exchange mailbox, see the Microsoft Exchange Help.
5. Check the Application event log configuration.

   If you plan to enable logging entries to the Application event log, check your Application event log configuration parameters. By default, Microsoft Windows Server 2003 allocates only 512KB to the Application event log and overwrites entries more than seven days old. Depending on the duration of the tests you plan, you may want to modify these values so you do not lose DRA or ExA log entries. For more information about configuring the Application event log, see the Microsoft Windows Help.
6. Enable logging entries to the Application event log if you want to duplicate the audit events that DRA stores in the log archive.

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.

Installing the Product Preview Utilities

To evaluate DRA or ExA, you need to manage objects. The product preview kit provides the NetIQ DRA-ExA Product Preview AD Populator and the NetIQ DRA-ExA Product Preview DRA Populator utilities to help generate evaluation data.

The AD Populator utility generates the following Active Directory objects:

- Account objects
  - User accounts
  - Groups
  - Contacts
  - Computers
- Organizational units (OUs)
- Microsoft Exchange mailboxes

The DRA Populator utility configures your evaluation environment by creating Assistant Admins, ActiveViews, policies, and automation triggers.

To install the evaluation kit utilities:

1. Log on to the evaluation computer with an account that has administrator permissions in this domain. For more information about the evaluation user account, see "Permission Considerations" on page 7.
2. Run the `Setup.exe` file in the `Evaluation Utilities` folder of the DRA installation kit.
3. On the Welcome window, click **OK**.
4. Click the computer icon to begin installing the utilities.
5. Click **Continue** to accept the default program group for the utilities.
6. After installing the product preview utilities, click **OK**.

Installing DRA and ExA for Evaluation

You can install DRA and ExA when the evaluation computer meets all the requirements and you have completed setting up your environment. For more information about preparing the evaluation computer, see "Installation Checklist" on page 4 and "Setting Up Your Environment" on page 9.

To install DRA and ExA for evaluation:

1. Log on to the evaluation computer with an account that has local administrator permissions. For more information about the evaluation user account, see "Permission Considerations" on page 7.
2. Run `Setup.exe` in the root folder of the installation kit.
3. Click **Check Version** on the Trial Setup tab of the setup program.

   The Check Version feature compares the product version in the installation kit with the newest available product version on the Web site. If you do not have the latest product version, contact your NetIQ sales representative or download a trial version from the NetIQ Web site (www.netiq.com).
4. Click **Begin Trial Setup** on the Trial Setup tab.
5. Click **Next**, and then click **Next** again.
6. Select the products you want to install, and then click **Next**.
7. Click **Add Licenses**.
8. Browse to the folder that contains your license key file.
9. Select your license key file, and then click **Open**.
10. Click **Next**.
11. Review the terms of the License Agreement. If you agree to the terms of the License Agreement, click **Accept**.
12. Click **Next**.
13. Type the name you want to use for the ADAM instance in the **Instance Name** field or accept the default name, and then click **Next**.
14. Type the LDAP and SSL port numbers you want to use in the **LDAP Port number** and **SSL port number** fields or accept the defaults, and then click **Next**.
15. Type the name of the ADAM admin account you created for this evaluation in the **ADAM Administrator Group** field. Specify the fully qualified account name using a pre-Windows 2000 format, such as `EvalDomain\ADAM Admin`. Do not use a DNS domain name (`EvalDomain.com\DRAServiceAccount`) or a User Principle Name (UPN) (`DRAServer@EvalDomain.com`).
16. Click **Next**.
17. Type the name and password of the service account you created for this evaluation in the **Account name** and **Password** fields. If the account is a domain account, enter the fully qualified account name using the pre-Windows 2000 format, such as `EvalDomain\DRAServiceAccount`. Do not use a DNS domain name (`EvalDomain.com\DRAServiceAccount`) or a User Principle Name (UPN) (`DRAServer@EvalDomain.com`).
18. Click **Next**.
19. ***If you want to evaluate the optional DRA Management reports***, on the NetIQ Reporting Center Installer dialog, select **Yes** to install NetIQ Reporting Center.
20. Click **Next**.
21. Click **Next**.
22. Click **Select** to specify the domain you want to use for this evaluation. Ensure your evaluation computer is in the specified domain.

23. On the Component Selection window, ensure you select the previously specified domain, and then click **OK**.
24. ***If the installer prompts you to add the service account to the Account Operators group***, click **Yes**.
25. Click **Next**.
26. Type the name of the Domain Admin account for the evaluation domain in the **Account name** field. Specify the fully qualified account name using pre-Windows 2000 format, such as `EvalDomain\administrator`.
27. Click **Next**.
28. Accept the default settings, and then click **Next**.
29. ***If you are installing ExA***, select the version of Microsoft Exchange you want to use for this evaluation, and then click **Next**.
30. Click **Next** to start installing the product components.
31. ***If the setup program prompts for services to be stopped***, click **Continue**.
32. Click **Finish**.
33. On the Administration Server Initialization window, click **OK**.
34. If you selected **Yes** in Step 19, the NetIQ Reporting Center setup program starts.

Tip

Ensure you have the following information available and then continue the steps in this procedure:

- SQL Server computer name
- SQL Server account name and password with Sysadmin privilege to create the reporting database

35. Click **Next**.
36. On the Component Selection dialog, select **Configuration Database**, **Web Service**, and **Console**, and click **Next**.
37. Follow the instructions until the installation completes, and click **Finish**.

Note

If you need to run the Reporting Center setup program at a later time to install the console on a separate server or to modify your installation, run one of the following files in the Intel folder of your installation kit:

- `netiqreportingcentersetup_x86.exe` to install on 32-bit operating systems
- `netiqreportingcentersetup_x64.exe` to install on 64-bit operating systems

Generating Sample Data for Evaluation

Use the NetIQ DRA-ExA Product Preview AD Populator and NetIQ DRA-ExA Product Preview DRA Populator utilities to generate sample data for your evaluation environment. For more information about installing these utilities, see "Installing the Product Preview Utilities" on page 10.

Generating Active Directory Objects

The AD Populator program generates user accounts, groups, contacts, organizational units, and computer accounts. AD Populator also supplies many additional user account properties that you can view in the Account and Resource Management console, the Delegation and Configuration console, and the Web Console. Run AD Populator *after* you install DRA or ExA.

To run AD Populator:

1. Log on to the evaluation computer with the user account you set up for this evaluation. For more information about the evaluation user account, see "Permission Considerations" on page 7.
2. Run **AD Populator** from the program folder where you installed it. By default, DRA installs the AD Populator program in the NetIQ DRA-ExA Product Preview program group.
3. On the AD Population tab, click **OK** to use the default values.
4. Click **OK**.
5. After AD Populator completes successfully, click **OK**.
6. Click **Exit**.
7. Run the incremental cache refresh so DRA and ExA recognize the new Active Directory objects. For more information about running an incremental cache refresh, see "Performing an Immediate Incremental Accounts Cache Refresh" on page 14.

Generating DRA Objects

The DRA Populator generates ActiveViews, Assistant Admins, policies, and automation triggers for you to use during your evaluation. Run DRA Populator *after* you install DRA and run the AD Populator program. Once you start DRA Populator, it runs without further input from you.

To run DRA Populator:

1. Log on to the evaluation computer with the user account you set up for this evaluation. For more information about the evaluation user account, see "Permission Considerations" on page 7.
2. Run **DRA Populator** from the program folder where you installed it. By default, DRA installs the DRA Populator program in the DRA-ExA Product Preview program group.
3. When the DRA Populator prompts you to create ActiveViews, click **OK**.
4. After DRA Populator completes successfully, click **OK**.
5. Run the incremental cache refresh so DRA and ExA recognize the new ActiveViews, policies, and automation triggers. For more information about running an incremental cache refresh, see Performing an Immediate Incremental Accounts Cache Refresh.

Notes

- DRA Populator generates ActiveViews based on the departmental and regional OUs created by AD Populator.
- The policies and automation triggers defined by DRA Populator apply only to objects in the top level OU you specified when you ran AD Populator.

Performing an Immediate Incremental Accounts Cache Refresh

The accounts cache refresh does not include objects that are unavailable during the refresh time. After you run the DRA Populator and AD Populator programs, DRA and ExA do not immediately display the new objects, policies, and automation triggers. You should perform an immediate incremental accounts cache refresh to view these objects in DRA and ExA. To refresh the accounts cache, you must have the appropriate powers. For more information, see the *Administrator Guide*.

To perform an immediate incremental accounts cache refresh:

1. Start the Delegation and Configuration console. By default, DRA installs the Delegation and Configuration console in the Directory and Resource Administrator folder of the NetIQ Administration program group.
2. In the left pane, expand **Directory and Resource Administrator > Configuration Management**.
3. Click **Managed Domains**.
4. In the right pane, select the domain for which you want to refresh the accounts cache.
5. On the Tasks menu, click **Refresh Accounts Cache > Incremental Refresh**.
6. Click **Yes**.
7. Click **OK**.

Enabling and Configuring DRA Management Reports

To see DRA Management reports in Reporting Center, you must enable and configure the data collectors that make audit data available to Reporting Center. If you chose to install the optional reporting components, complete these steps to enable and configure Management reports.

To enable and configure Management reports:

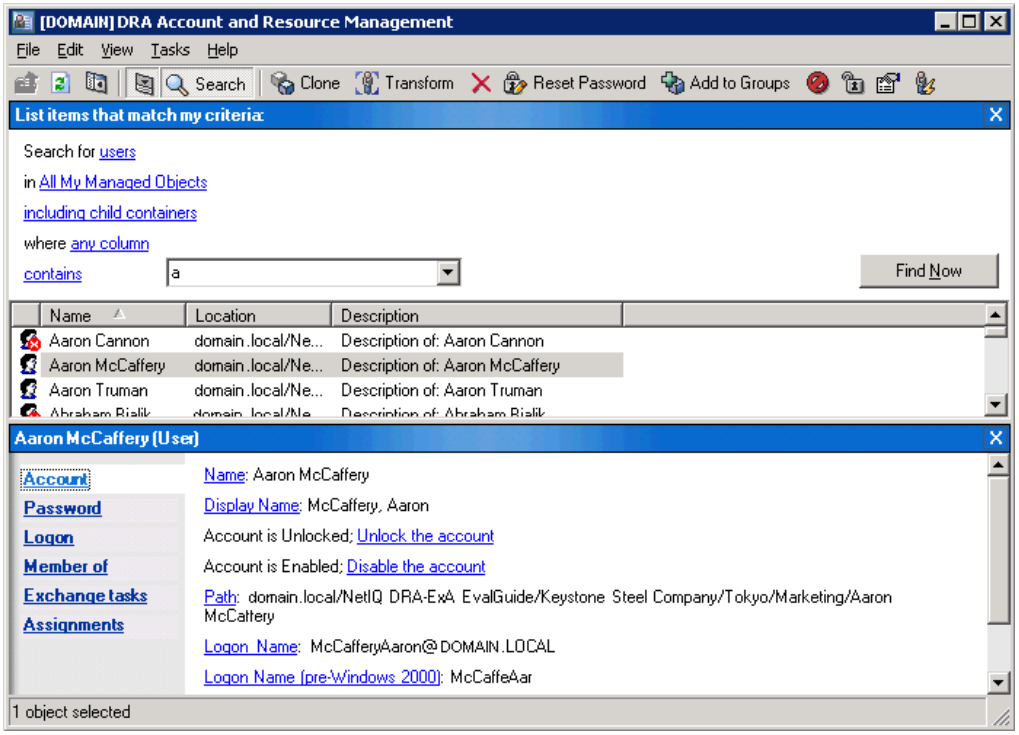
1. Start the Delegation and Configuration console.
2. In the left pane, expand **Directory and Resource Administrator > Configuration Management**.
3. Click **Update Reporting Service Configuration**.
4. On the Storage Server tab, select **Enable DRA Reporting support**.
5. Click **Browse** in the Server Name field and select the computer where SQL Server is installed.
6. On the Credentials tab, specify the appropriate credentials to use for the SQL Server interactions.
7. If this is the same account that can be used to create the database and initialize the schema, select the **Use the above credentials for creating a database and initializing the database schema** check box.
8. If you want to specify a different account for creating a database, on the Admin Credentials tab, specify that user account and password.
9. Click **OK**.
10. On the Active Directory Collector tab, click **General**.
11. Select **Enable data collection**.
12. Click **Browse** in the Server Name field and select the Administration server you want to use for data collection.
13. Complete the Active Directory Collector Configuration Wizard.

14. When you schedule the collector schedule for the first time, set it for daily collection a few minutes later than when you are configuring it. Doing this gives you the shortest time to wait for data to populate reports.
15. Click **Finish** when you have completed all required fields.
16. On the DRA Collector tab, click **General**.
17. Select **Enable data collection**.
18. Click **Browse** in the Server Name field and select the Administration server you want to use for data collection.
19. Complete the DRA Collector Configuration Wizard.
20. When you schedule the collector schedule for the first time, set it for daily collection a few minutes later than when you are configuring it. Doing this gives you the shortest time to wait for data to populate reports.
21. Click **Finish** when you have completed all required fields.
22. On the Management Reports Collector tab, click **Enable activity data collection**, and then click **OK**.

Starting the DRA and ExA Consoles

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

To start the Account and Resource Management console, click **Account and Resource Management** in the Directory and Resource Administration folder of the NetIQ Administration program group. The Account and Resource Management console starts, as shown in the following figure:

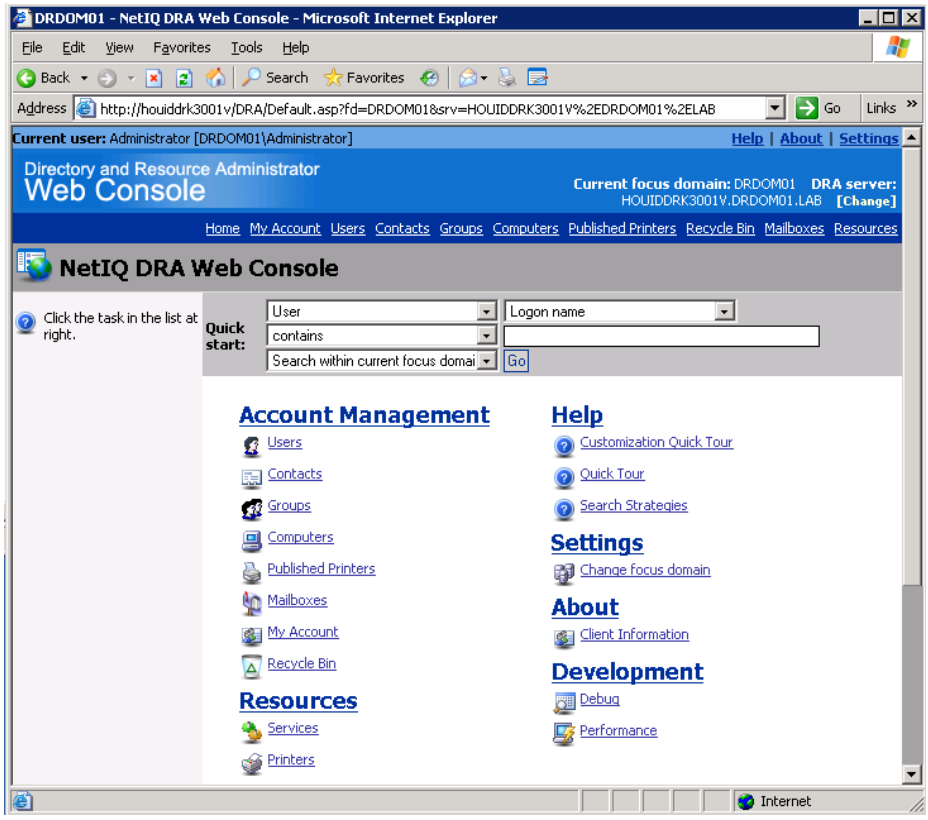


The Delegation and Configuration console lets administrators define the security model and associated policies, delegate network administration, and perform all administration tasks in an object-oriented workflow. This console is intended for full-time system administrators.

To start the Delegation and Configuration console, click **Delegation and Configuration** in the Directory and Resource Administration folder of the NetIQ Administration program group. The Delegation and Configuration Console opens, as shown in the following figure:

The Web Console lets Help Desk personnel perform common account and resource administration tasks using an easy-to-use, task-based interface. The Web Console is intended for Help Desk organizations and others who need a simple interface that allows them to easily perform everyday administration tasks.

To start the Web Console, click **Web Console** in the Directory and Resource Administration folder of the NetIQ Administration program group. The Web Console opens, as shows in the following figure:



Chapter 2
Exploring DRA and ExA

The following concepts and guided tour of DRA and ExA demonstrate the features and benefits of using the products. Ensure you complete all the tasks identified in the installation chapter before continuing. For more information, see "Installing the Trial Version of DRA and ExA" on page 1.

Understanding Active Directory Administration

The dual nature of Active Directory as a data store for confidential information, as well as a gateway to other systems, makes it particularly attractive and vulnerable to malicious and inadvertent security attacks. Protecting the Active Directory from internal and external threats is a constant challenge. With powerful policy-based privilege and content management, as well as extensive auditing and reporting capabilities, DRA secures Active Directory, protects the integrity of its data, and plays a key role in meeting your organization's regulatory compliance objectives. ExA leverages these benefits to provide seamless Microsoft Exchange management. Together, DRA and ExA provide the solutions you need to control and manage your Active Directory, Microsoft Windows, and Microsoft Exchange environments. DRA and ExA offer the following advantages over using native or other tools:

- Let you reduce the number of highly privileged accounts
- Let you create multiple forests for the most rigorous security needs
- Enforce a strong password policy
- Let you use Group Policy pervasively
- Implement change control
- Implement dual-key authorization for important changes
- Implement centralized auditing and monitoring
- Let you temporarily remove inactive or expired user accounts

Many automated Active Directory administration tasks are provided out-of-the-box, but DRA and ExA also support a wide spectrum of open, extensible standards so you can extend your administration model. The extensible standards include 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 and ExA give you the administrative power and flexibility to extend native Active Directory delegation across geographic, operating system, and organizational unit (OU) hierarchical boundaries by using patented *ActiveView* technology. Using a rules-based architecture, DRA automatically enforces and propagates policies across Windows systems, ensuring data integrity enforcement and increasing security.

Understanding ActiveViews

An ActiveView represents a set of objects. When you create or modify an ActiveView, you specify rules that define which objects you want to manage as a collection. The ActiveView rule also associates Assistant Admins (AAs) with roles and powers to manage this collection of objects.

ActiveViews allow you to implement a security model with the following features:

- Is independent from your Active Directory structure
- Allows you to assign powers and define policies that correlate to your existing workflows
- Provides automation to help you further integrate and customize enterprise administration tasks
- Responds dynamically to change

An ActiveView represents a set of objects within one or more managed domains. You can include an object in more than one ActiveView. You can also include many objects from multiple domains or OUs.

Dynamic Sets of Objects

An ActiveView provides real-time access to specific objects within one or more domains or OUs. You can add or remove objects from an ActiveView without changing the underlying domain or OU structure.

You may think of an ActiveView as a virtual domain or OU, or the result of a select statement or database view for a relational database. ActiveViews can include or exclude any set of objects, contain other ActiveViews, and have overlapping content. ActiveViews can contain objects from different domains, trees, and forests. You can configure ActiveViews to meet your enterprise management needs.

ActiveViews can include the following types of objects:

- Accounts:
  - User accounts
  - Groups
  - Computers
  - Contacts
  - Published printers
  - Published printer print jobs
- Directory objects:
  - Organizational units
  - Domains
  - Member servers
- Other objects:
  - ActiveViews
  - Self Administration
  - Direct Reports
  - Managed Groups
- Resources:
  - All resources

- Connected users
- Devices
- Event logs
- Open files
- Printers
- Print jobs
- Services
- Shares

You can specify the objects that DRA includes in an ActiveView by querying the object attributes. As your enterprise changes or grows, ActiveViews change to include or exclude the new objects. You can use ActiveViews to reduce the complexity of your model, provide the security you need, and give you far more flexibility than other enterprise management tools.

Flexible Rules

An ActiveView can consist of rules that include or exclude objects, such as user accounts, groups, OUs, contacts, resources, and ActiveViews. In addition, ActiveView rules can specify security and policy objects. When you specify a wildcard character in a rule specification, the rule includes all objects that match the specified value. This flexibility makes ActiveViews dynamic.

When you add a rule to an AA group using wildcards, the rule includes all computer accounts that match the specified pattern. Wildcard matching makes administration dynamic because accounts are automatically included when they match the rule. When you use wildcards, you do not need to reconfigure the ActiveViews as your organization changes.

Quick Tour of the Web Console

The Web Console lets you perform common account and resource administration tasks using 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.

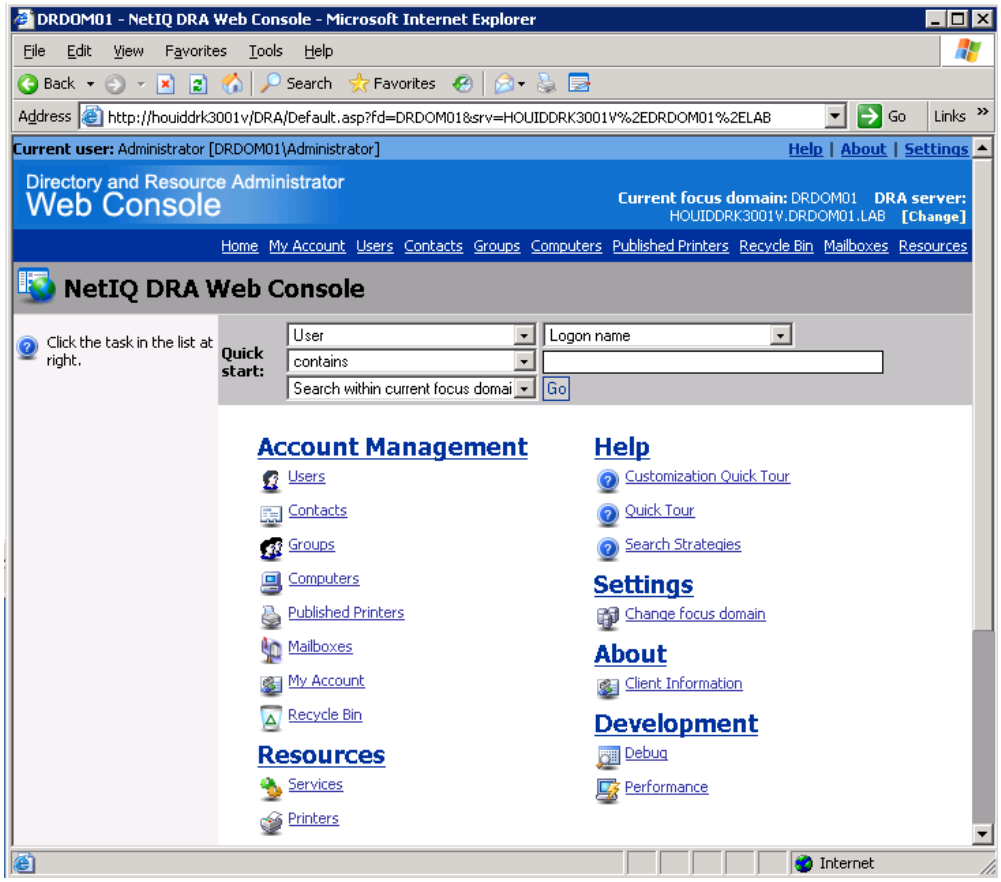
Starting the Web Console

You can start the Web Console from the NetIQ Administration program group, the Account and Resource Management Console, the Delegation and Configuration Console, or your internet browser.

To start the Web Console from your internet browser:

1. Open Internet Explorer.
2. In the **Address** field, type `http://`*`ComputerName`*`/dra`, where *`ComputerName`* is the name of the server computer where you installed DRA and ExA.
3. Press **Enter**.

The Web Console displays the home page, as shown in the following figure.



Available Tasks

The Web Console lets you perform various tasks for:

- Users
- Groups
- Computers
- Contacts
- Published Printers
- Services
- Printers
- Mailboxes
- My Account
- Recycle Bin
- Settings
- About
- Development

The next few tasks will help you create a user account, group, and computer account. You can easily perform other tasks by going through these basic tasks.

Creating a User Using the Web Console

The Web Console lets you to perform most of the user-related tasks. The Web Console displays only the tasks for which you have the appropriate permissions. This task shows how you create a user account and apply password settings using the Web Console.

To create a user account:

1. On the Web Console home page, click **Users**.
2. On the User Tasks page, click **Create a user**.
3. Type the user name in the **First name** and **Last name** fields.
4. Type the logon account name in the **Logon name** field.
5. Clear the **Suggest a password** for me check box.
6. Type the new password in the **Password** fields.
7. Select the **User must change password at next logon** check box.
8. Clear the **User cannot change password** and **Password never expires** check boxes.
9. Click **Create User,** and then click **OK**.

Creating a Group Using the Web Console

The Web Console lets you to perform most of the group-related tasks. The Web Console displays only the tasks for which you have the appropriate permissions. This task shows how you create a group using the Web Console.

To create a group:

1. On the Web Console home page, click **Groups**.
2. On the Group Tasks page, click **Create a group**.
3. Type the group name in the **Group name** field.
4. Click **Distribution group** and **Global group**.
5. Click **Create Group**, and then click **OK**.

Creating a Computer Account Using the Web Console

The Web Console lets you to perform most of the computer account-related tasks. The Web Console displays only the tasks for which you have the appropriate permissions. This task shows how you create a computer account using the Web Console.

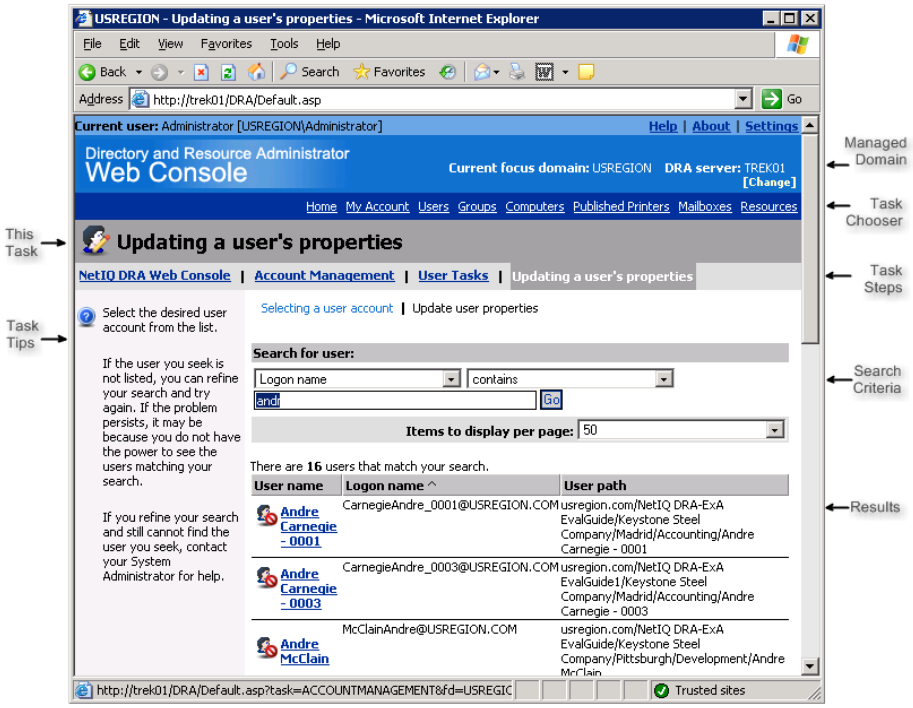
To create a computer account.

1. On the Web Console home page, click **Computers**.
2. On the Computer Tasks page, click **Create a computer**.
3. Type `TrialComputer-1` in the **Computer name** field.

4. Clear the **Allow Pre-Windows 2000 computers to use this account** check box.
5. To specify the user account or group that can use this computer account, complete the following steps:
   a. Click **Browse**.
   b. Specify the user account or group attributes, and then click **Go**.
   c. Select the appropriate user account or group from the list.
6. Click **Create Computer**, and then click **OK**.

Using the Web Console

The Web Console guides occasional administrators step-by-step through many routine administration tasks. The following figures provide a brief tour of some Web Console features and navigation tools.



The Web Console provides a number of features to help beginners or occasional administrators navigate through routine administration tasks.

This Task

Displays the current step you are performing.

Task Tips

Gives hints or tips for what to do next or how to find the information you need.

Managed Domain

Displays the name of the domain whose objects you are managing.

Task Chooser

Lets you select another task or return to the Web Console home page.

Task Steps

Lists the sequence of steps for the current task, and lets you select another step in this sequence.

Search Criteria

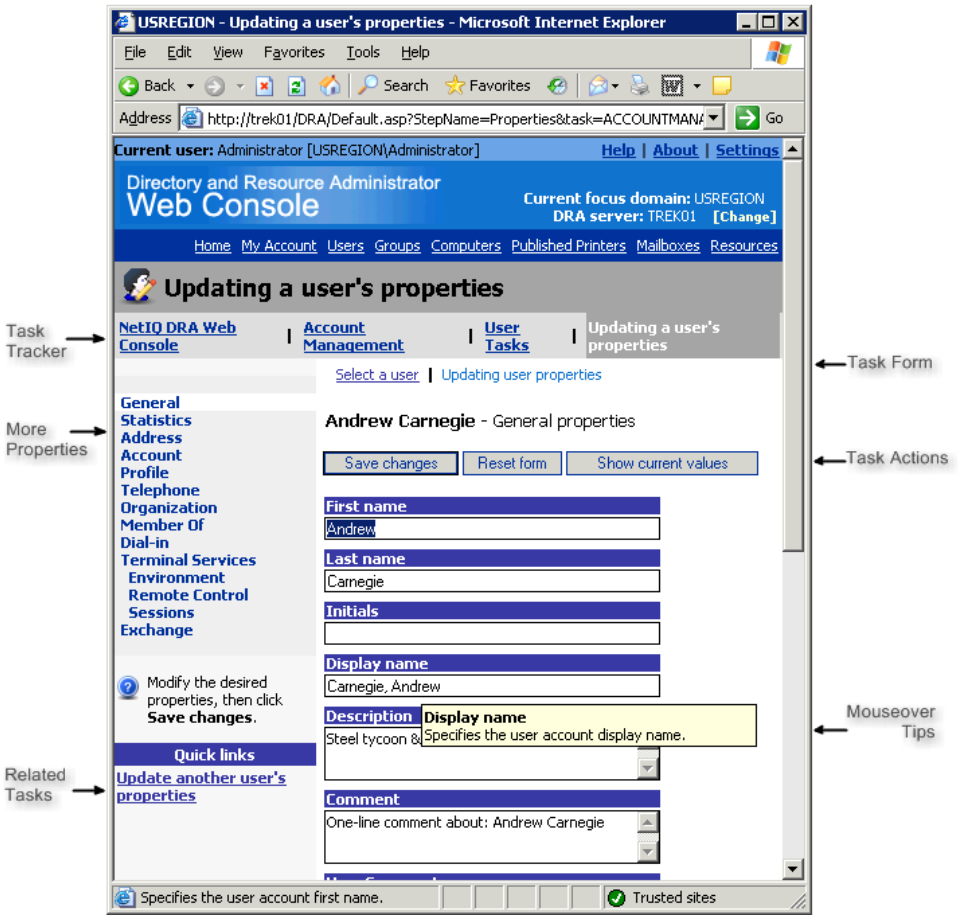
Offers a quick way to find the specific object you are managing. To start your search, specify your criteria, and then click **Go**.

You can search for objects based on a specific property value, such as the **Name** or **Logon name**. For example, you can search for a user whose name begins with Andrew. You can also type a few letters and add a wildcard, such as *, ?, or #, to narrow or broaden your search. For example, type `*ATL*` to find all user accounts or groups whose names contain the character string ATL anywhere in the name.

Results

Displays items that match your search criteria.

The following figure identifies additional navigation features found on some other task pages of the Web Console:



Task Tracker

Keeps track of the steps you took to arrive at the current task. Click any highlighted item to return to a previous step.

More Properties

Displays links to additional property pages for the selected user account, group, or mailbox. For example, you can view and manage group membership properties for a specific user account.

Related Tasks

Lists other tasks similar to the current task that you may want to perform.

Task Form

Displays information, such as user account properties, for this step in the task.

Task Actions

Provides the actions you can take at this step in the task. For example, you can show the current property values for the selected user account, letting you compare updates to previous values before you apply your changes.

Tips

Displays helpful information when you move the pointer over an item.

Solving Account Issues Using the Web Console

Companies want Help Desk technicians to provide high levels of service by quickly and effectively addressing account issues. With the Web Console, you can quickly access vital statistics about a specific user account, diagnose the issue, and perform the necessary actions to resolve it.

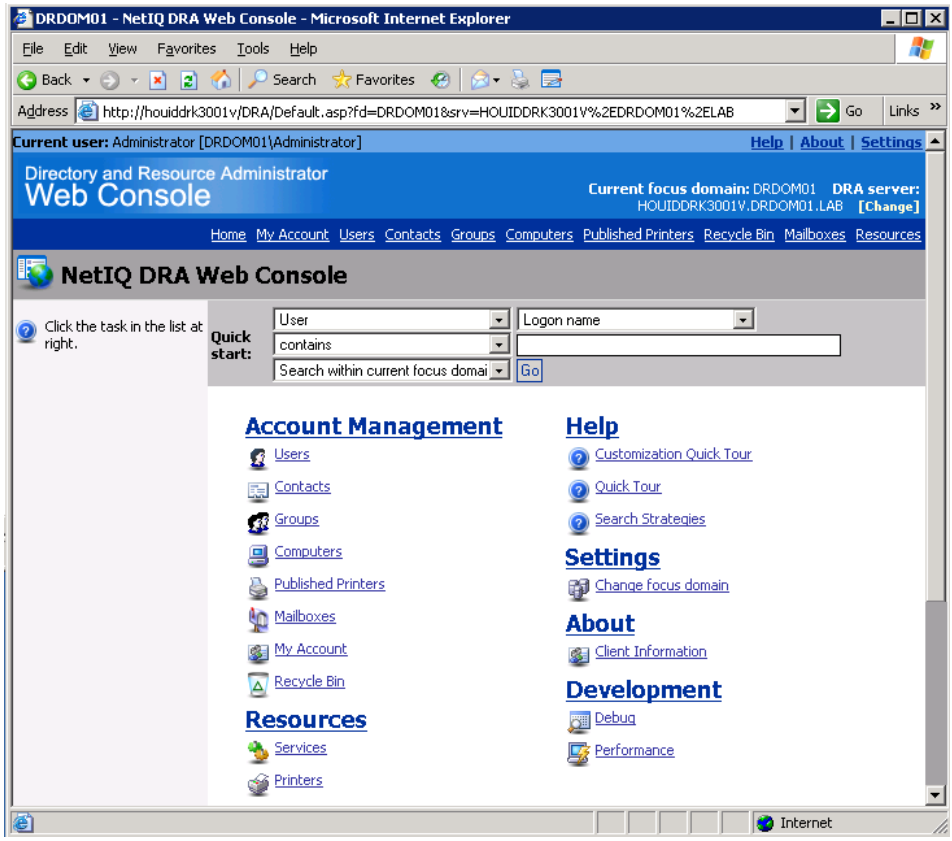
DRA provides the following vital statistics:

- Whether the account is locked out
- Whether the account is enabled
- Password activity
- Logon activity

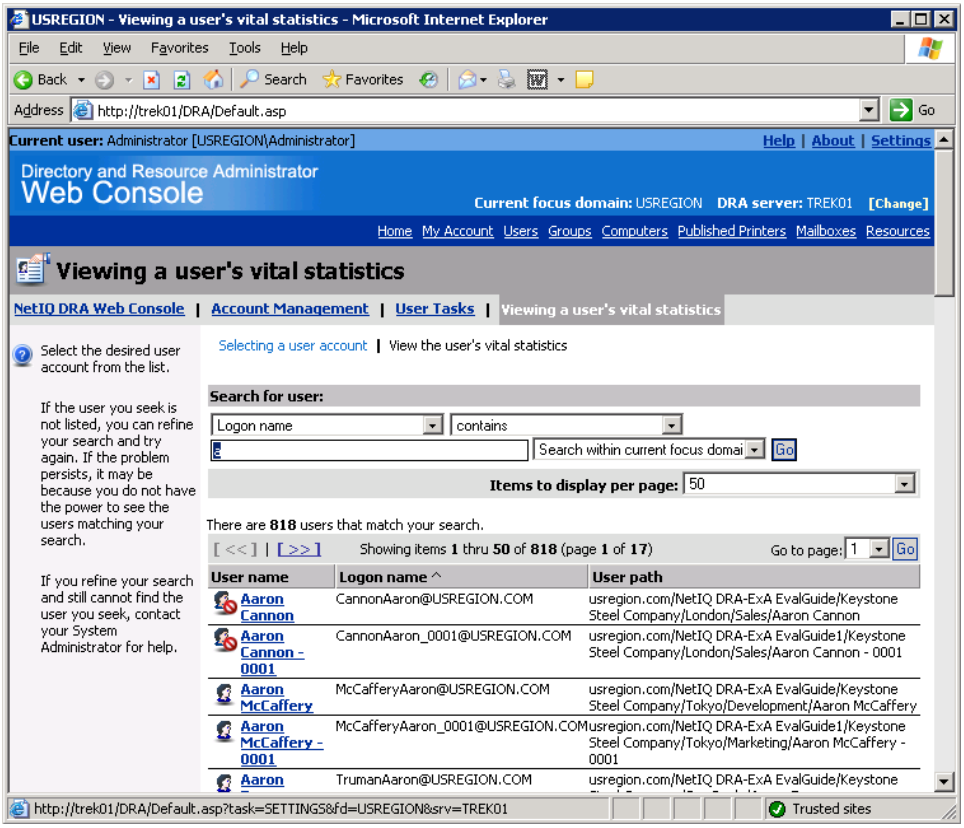
This task shows you how to check whether a user account is locked out.

To check whether a user account is locked out using the Web Console:

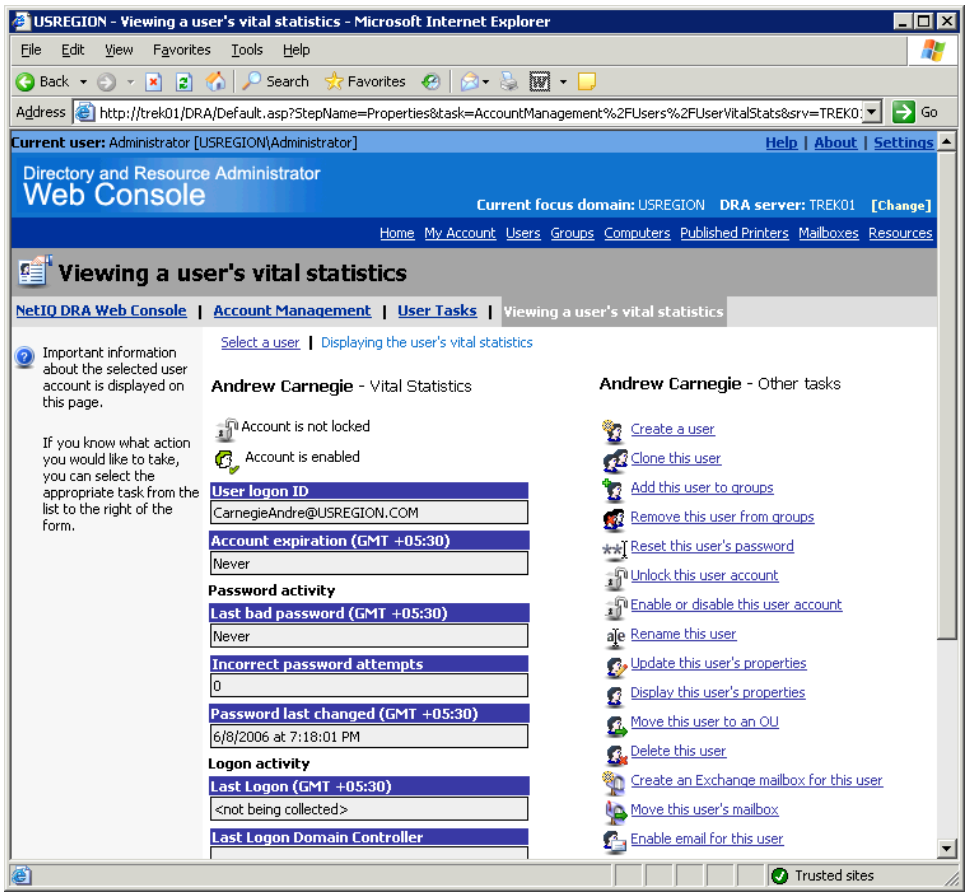
1. On the Web Console home page, use **Quick Start** to specify your search criteria, and then click **Go**.



2. Click the user account for which you want to view vital statistics.



3. Use these vital statistics to diagnose whether the user account is locked out.



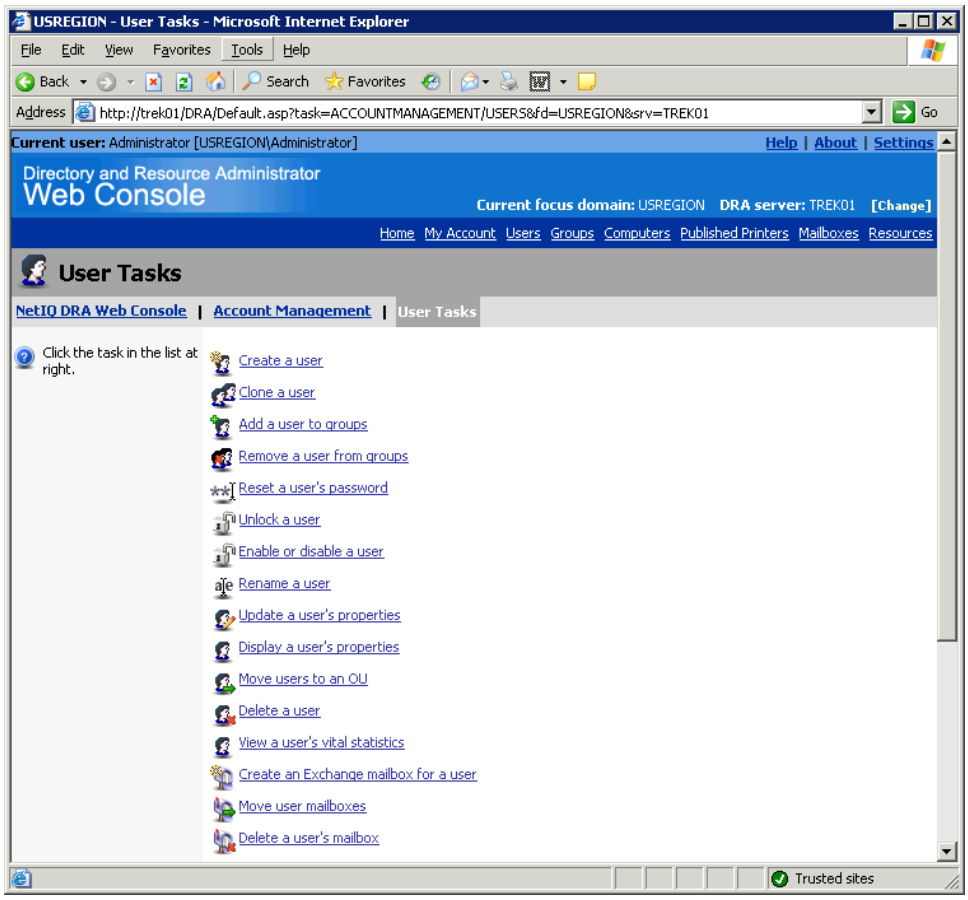
To immediately take corrective action and resolve the issue, click the appropriate task link under **Other tasks**.

Resetting a Password Using the Web Console

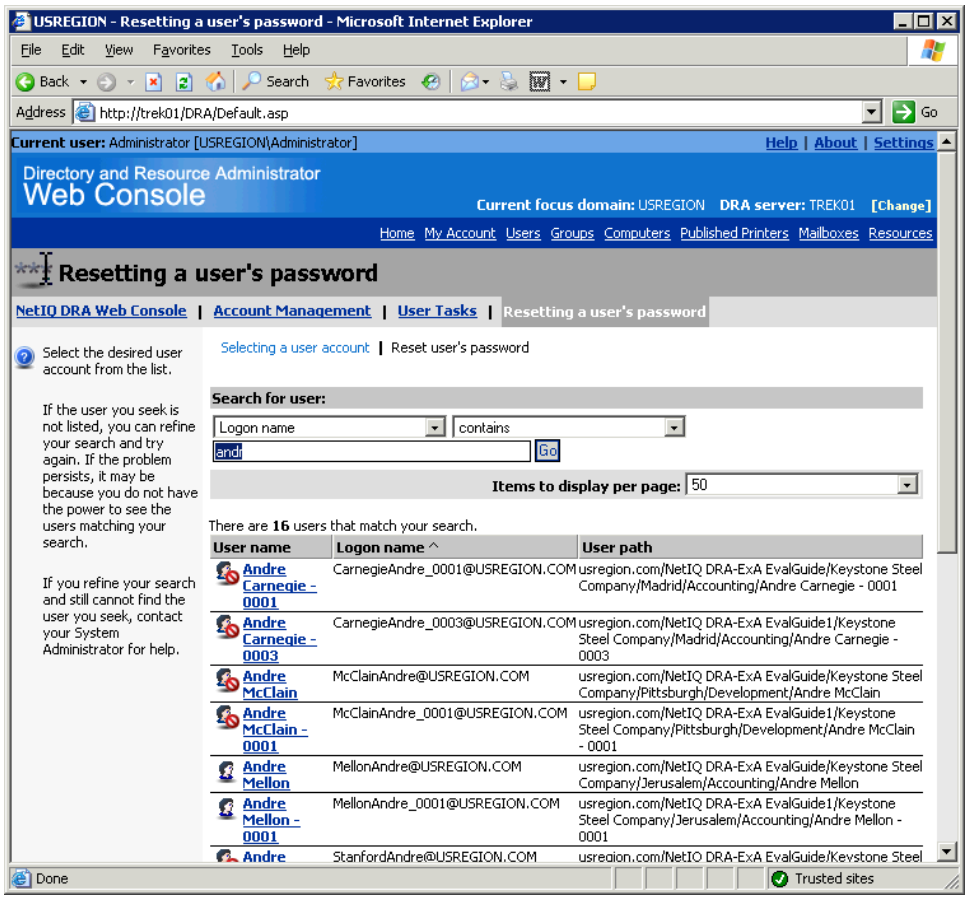
Delegating routine tasks such as resetting passwords to departmental users can reduce the workload for system administrators. The Web Console secures and automates tasks so you can securely delegate them.

To reset a password for a user account using the Web Console:

1. On the Web Console home page, click **Users**.
2. On the User Tasks page, click **Reset a user's password**.

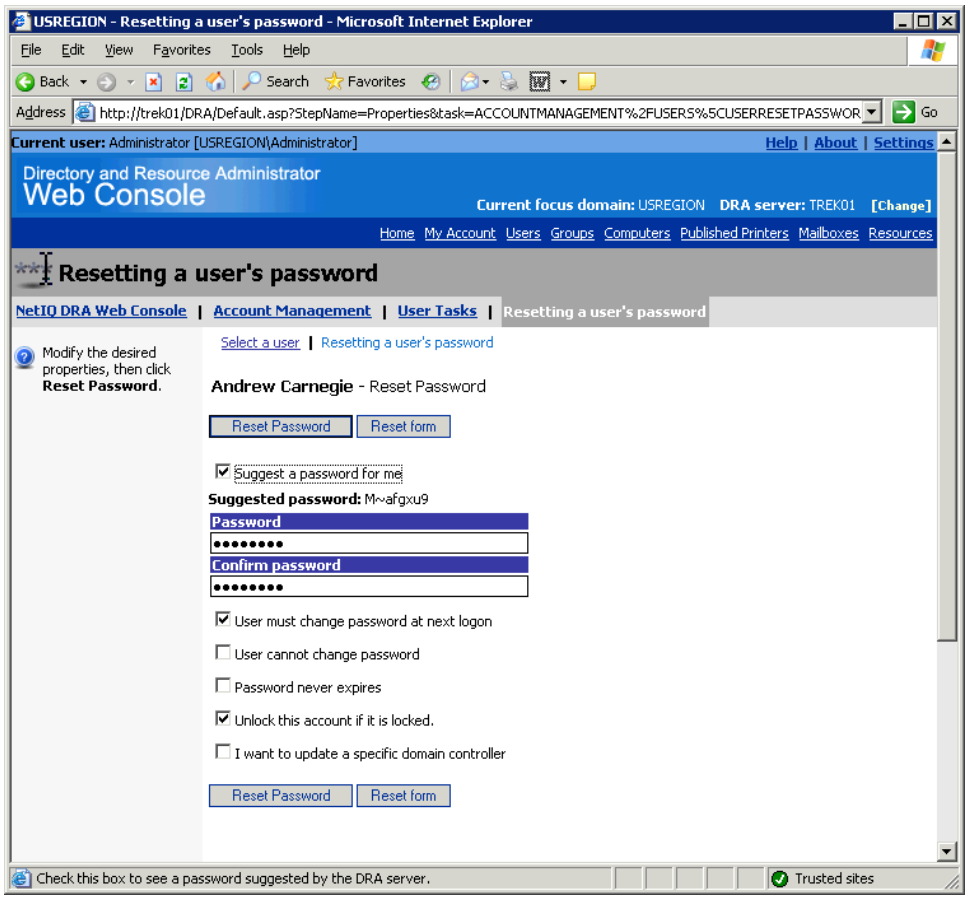


3. Specify your search criteria, and then click **Go**.



4. Select the user account that requires a password change.
5. Clear the **Suggest a password for me** check box.
6. Type the new password in the **Password** and **Confirm password** fields.
7. Select the **User must change password at next logon** check box.
8. Select the **Unlock this account if it is locked** check box.

9. Click **Reset Password**, and then click **OK**.



After DRA resets the account password, DRA performs the following additional tasks that you selected:

- Unlocks the user account if it is locked out
- Sets the flag that requires the user to change the account password at next logon

Using ActiveViews to Manage Objects

DRA ActiveViews allow you to collectively manage Active Directory, Microsoft Windows 2003 objects, or Microsoft Windows 2008 objects in ways that make the most sense for your organization. Rules define ActiveViews, making them dynamic, changing as your enterprise does. For example, you can define an ActiveView that includes or excludes any set of objects, including other ActiveViews. Then, as your network changes, the rules ensure automatic inclusion or exclusion of new objects in the proper ActiveViews.

ActiveViews can overlap, contain other ActiveViews, and include objects from different domains, trees, OUs, and forests. ActiveViews can also contain objects that are outside the Active Directory, such as printers and shares. You can collect objects in ActiveViews without changing the underlying domain or OU structure. This task shows you how to create a simple ActiveView and delegate power to create and delete groups.

To create an ActiveView and delegate power:

1. Start the Delegation and Configuration console.
2. In the right pane under Common Tasks, click **Delegate Administration**.
3. On the Welcome tab, click **Next**.
4. Click **Add > Users**.
5. Search for the user account you want to delegate power to. For example, to delegate power to Andrew Carnegie, type `Andrew` in the provided field, and then click **Find Now**.
6. Select **Andrew Carnegie**.
7. Click **Add**, and then click **OK**.
8. Click **Next**.
9. Click **Add > Roles**.
10. Search for the role you want to assign to the user account. For this demonstration, search for **Create and Delete Groups**.
11. Select **Create and Delete Groups**.
12. Click **Add**, and then click **OK**.
13. Click **Next**.
14. Click **Add > Domains, OUs, and Containers**.
15. Expand *`DomainName`* **> NetIQ DRA-EXA Product Preview > Keystone Steel Company > London**, where *`DomainName`* is the name of your domain.
16. Select **Accounting**, click **Add**, and then click **OK**.
17. Click **Next**.
18. Type `London Sales` in the **Name** field.
19. Type `Product Preview ActiveView Description` in the **Description** field. Note that you can include both a comment and a description for ActiveViews. The Delegation and Configuration Console displays the description in the ActiveView list.
20. Click **Next**. You can review the managed objects by clicking the links under **Analysis of Managed Objects**.
21. Click **Finish**.

Generating Reports to Audit Actions

DRA Activity Detail reports include detailed, historical data telling you what was changed, when it was changed, and who made the changes. Before and after values give you a detailed view of changes in your environment. Powers in DRA specify who can run these reports and who can export them. The ability to run reports is also based on objects that the Assistant Admin can see. Reports selections dynamically change depending on the object selected.

To run an Activity Detail report:

1. Start the Account and Resource Management Console.
2. In the Search pane, enter criteria to find a user or group you created with the Web Console.
3. Click Find Now.
4. Right-click over the user or group in the Results pane, and click **Reporting > Changes made to objectName**.
5. Click **OK** and view the report in the new window.

As you search for various objects, right-click and select **Reporting** to see the different reports that are available for different objects. For example, group reports include changes made to a group, members added to a group, and members removed from a group.

Configuring Home Directory Policy and Automation Triggers

You can quickly and easily automate many tasks using DRA, including setting home directory policy and automating home directory and share creation. DRA supports Distributed File System (DFS) paths or partitions and NetApp Filer during creation of user home directories or configuration of home directory policies for users in allowable parent paths.

User account management often requires administrators to perform the following tasks after creating a new user account:

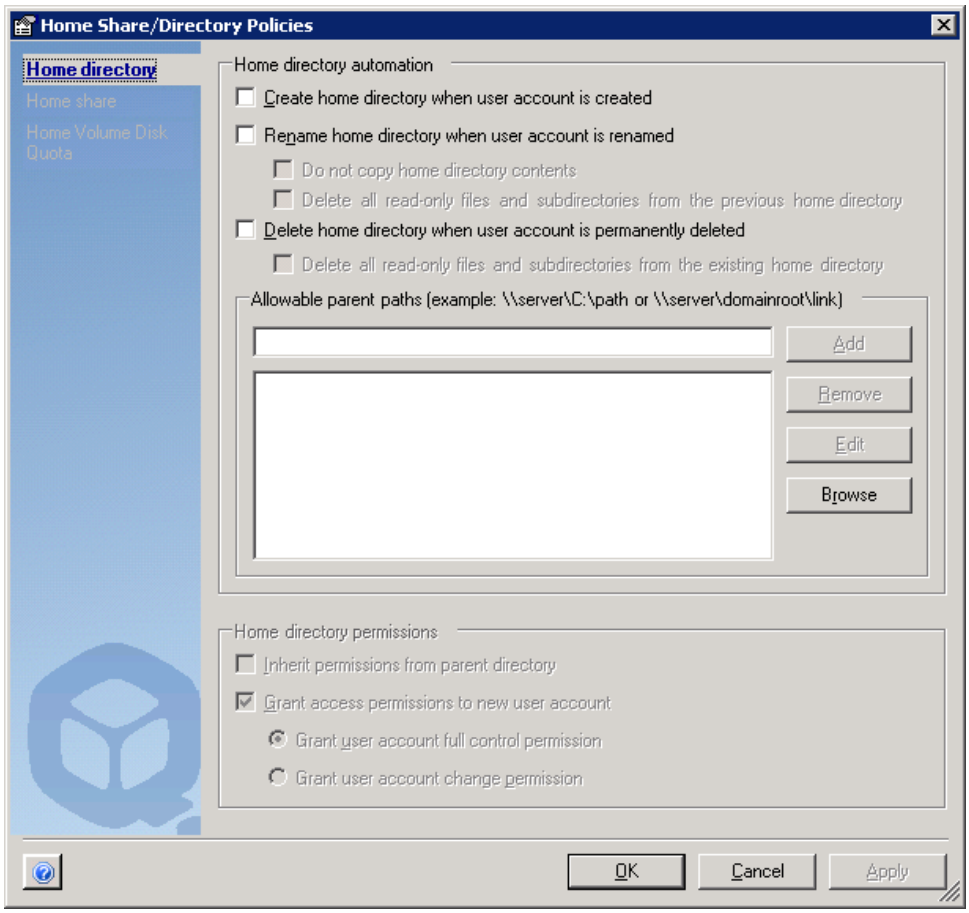
- Create a home directory
- Set the access permissions for the home directory
- Set a disk quota for the disk volume housing the home directory
- Create a home share

With DRA, you can automate these tasks without scripting. In the following task, you activate automation and policy for home directory, home share, and home directory disk quotas using the Delegation and Configuration Console.

To enable home directory, share policy, and automation:

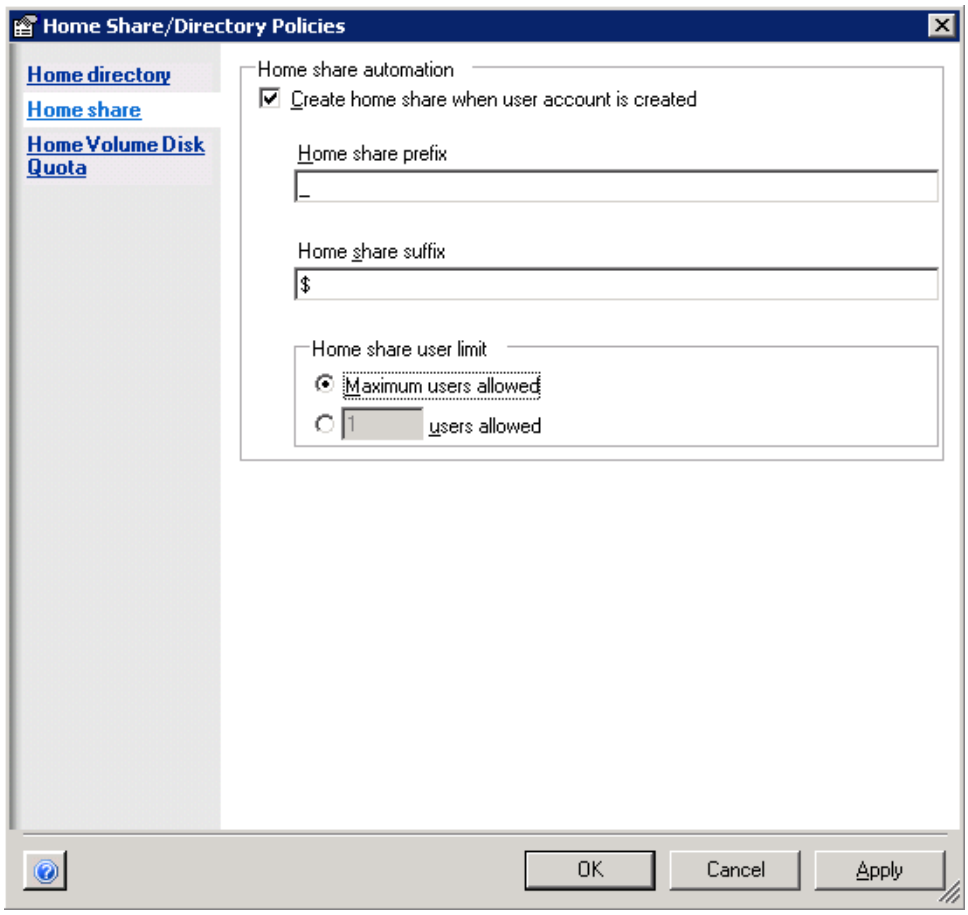
1. Start the Delegation and Configuration console.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Click **Policy and Automation Management**.
4. Under Common Tasks in the right pane, click **Configure Home Directory Policies**.

On the Home directory tab, DRA provides several policy options, as shown in the following figure.



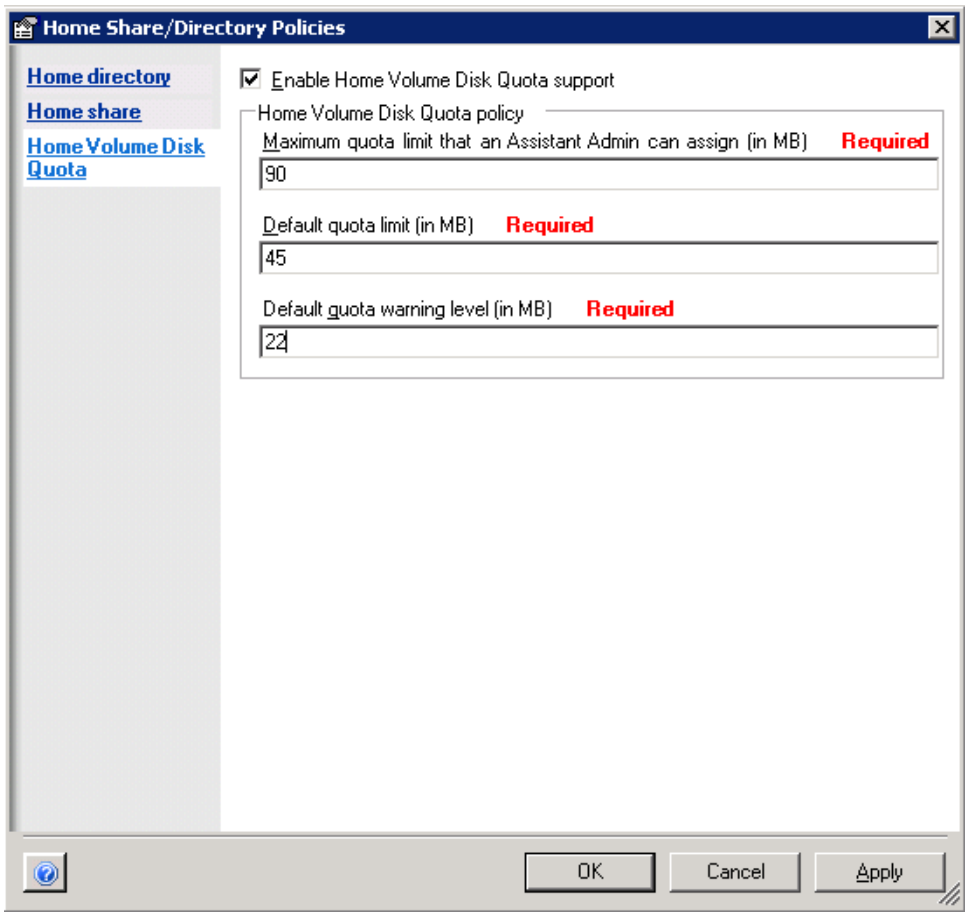
5. Under **Home directory automation**, select **Create home directory when user account is created**. Select or clear other items for the results you want.
6. Under **Allowable parent paths**, specify the root path of the home directory using the `\\server name\C:\path to root directory` syntax.
   - To specify a DFS path, use the `\\server\root\<link>` format, where root can be either the managed domain or a standalone root directory.
   - To specify a NetApp Filer, use: `\\FilerName\adminshare:\volumerootpath\directorypath`
7. Under **Home directory permissions**, select **Inherit permissions from parent directory** and **Grant access permissions to new user account**.

8. Click the Home share tab, as shown in the following figure.



9. Under **Home share automation**, select **Create home share when user account is created**. This option instructs DRA to automatically create a home share when you create or clone a user account.
10. Type an underscore (_) in the **Home share prefix** field so you can easily identify user shares.
11. Type a dollar sign **($)** in the **Home share suffix** field to hide user shares.

12. Click the Home Volume Disk Quota tab, as shown in the following figure.



13. Select **Enable Home Volume Disk Quota support**.
14. Specify `90` as the maximum quota limit.
15. Specify `45` as the default quota limit.
16. Specify `22` as the default quota warning level.
17. Click **Apply**, and then **OK** to save changes and complete the home directory policy and automation configuration.

In this brief task, you configured DRA to enforce policies and automate tasks critical to efficient user account administration. Now, any time an administrator uses the Account and Resource Management console, the Delegation and Configuration console, or the Web Console to create or clone a new user account, DRA automatically completes these additional tasks:

- Creates a home directory
- Assigns the access permissions you specified to the home directory
- Adds the underscore prefix to the beginning of the home share name
- Adds the dollar sign suffix to the end of the home share name
- Limits disk quota size to 90 MB for home directories
- Assigns a default disk quota size of 45 MB
- Assigns a quota warning level of 22 MB

Prefixes and suffixes help you distinguish home shares. The prefix ensures DRA groups all home shares together in a sorted list. Using the $ suffix ensures DRA hides the shares. Hiding home shares helps secure your servers and data.

With home directory, share, and disk quota policy and automation in place, if administrators or casual users know how to create or clone a new user account, you do not need to teach them how to do these more complicated tasks. DRA completes these tasks automatically, according to the guidelines and policies you establish.

Creating a Property Validation Policy

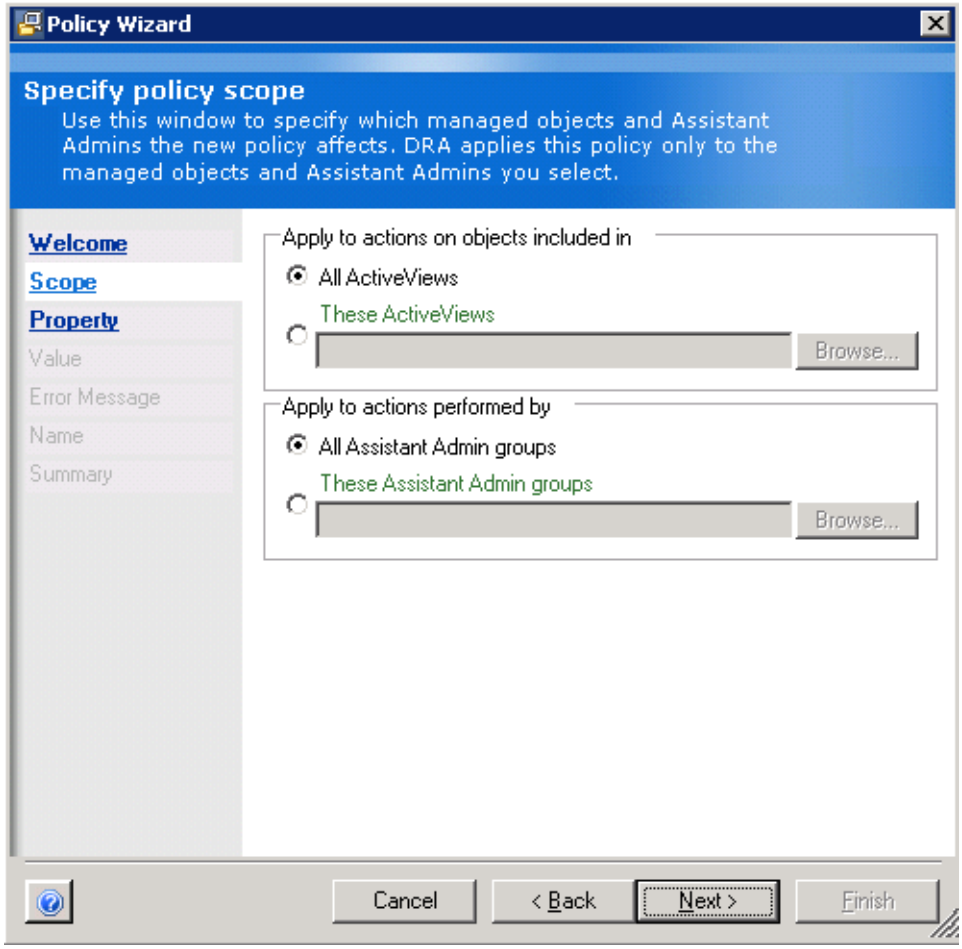
DRA has a built-in feature that lets you validate a property for many types of entries. For example, you may want to limit the value for **Department** to discrete settings, such as `Sales` or `Development`, or the value for **Location** to `Glasgow` and `Pittsburgh`.

In other cases, you may want to constrain a value to a particular entry format, such as for mailbox auto-reply messages or telephone numbers. For example, you could define a validation format for telephone numbers so that an entry must include an area code and a hyphen to delimit the number into area code, exchange, and extension, such as 412-555-1234. You can use this feature to maintain consistency in your Active Directory and help control directory pollution.

To create a validation policy for the user telephone number format:

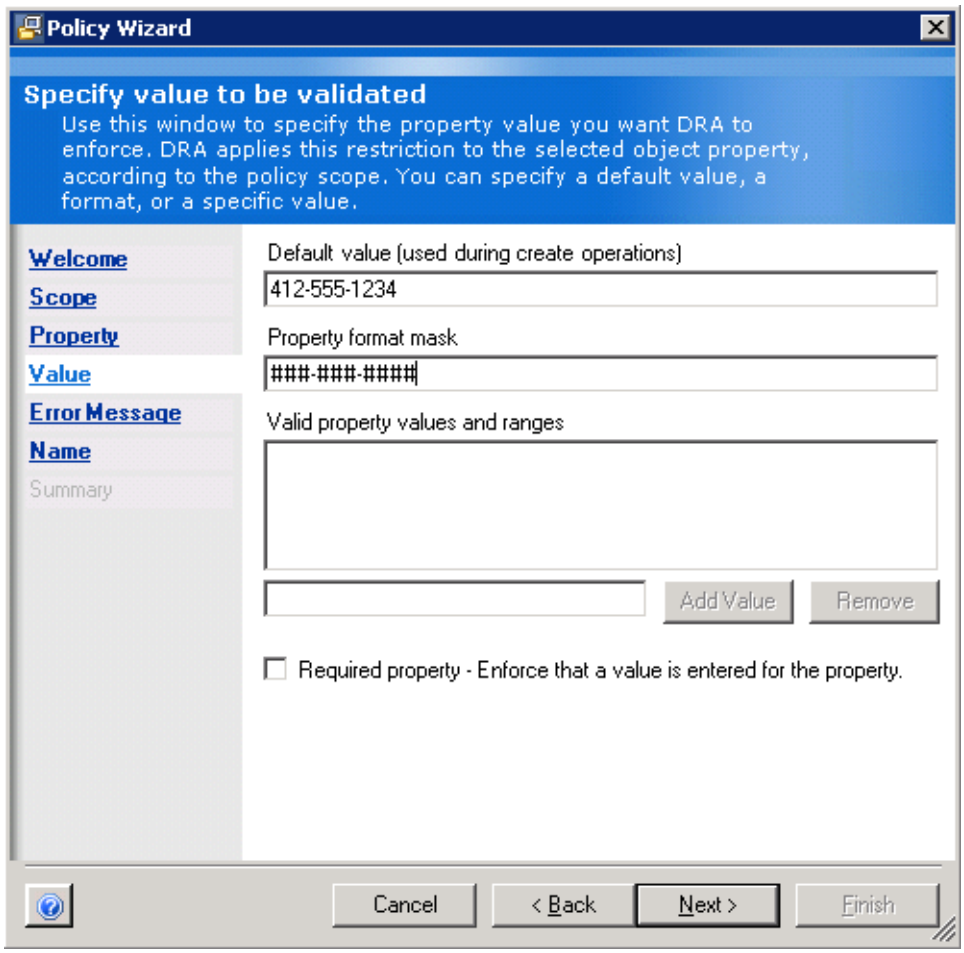
1. Start the Delegation and Configuration console.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Expand **Policy and Automation Management**.
4. Click **Policy**.
5. On the Tasks menu, click **New Policy > Create Policy to Validate a Specific Property**.
6. On the Welcome tab, click **Next**.

7. By default, DRA enforces the new policy in all ActiveViews and for all Assistant Admin groups, as shown in the following figure. You can change the policy scope to affect specific ActiveViews and specific Assistant Admin groups. Click **Next**.



8. In the **Class** field, select **User**.
9. Click **Browse** to choose a property to validate.
10. Search for and select **telephoneNumber**.
11. Click **Add**, and then click **OK**.
12. Click **Next**.
13. Type a number in the **Default value** field, such as `412-555-1234`. You may want to set this to your company's main telephone number. When a new user account is created, if no other telephone number is specified, DRA inserts this value for the **Telephone Number** property.

14. Type `###-###-###` in the **Property format mask** field, as shown in the following figure. This mask allows you to specify telephone numbers in the following format: `123-456-7890`.



15. Click **Next**.
16. On the Error Message tab, type an error message in the **Error message** field that explains how to correct the entries to match the format. For example, you might type `The telephone number you typed was not in the proper format. Type telephone numbers in the following format: 777-555-1212.`
17. Click **Next**.
18. Type `North America phone number format 1` for **Policy name**, and then click **Next**.
19. Review the information on the Summary tab, and then click **Finish**.

In this task, you defined a policy that limits telephone number entries to a common North America telephone number format. Use this same technique to limit other types of entries for many classes of objects. Then, as you delegate tasks among other administrators, or casual users, DRA helps maintain consistent data.

Defining a Custom Tool

DRA enables you to create custom tools that seamlessly integrate the DRA interface with other products. Using custom tools, you can execute external applications, launch scripts, and open a web page.

DRA supports two types of custom tools:

- Custom tools that launch common desktop utilities, such as Microsoft Office
- Custom tools that you create and distribute to each DRA client computer

DRA enables you to easily distribute custom tools you create to each DRA client by using the DRA file replication feature. The DRA file replication feature allows you to quickly and easily upload one or more files to an Administration server and then replicate these files between additional Administration servers and every configured DRA client computer in your environment.

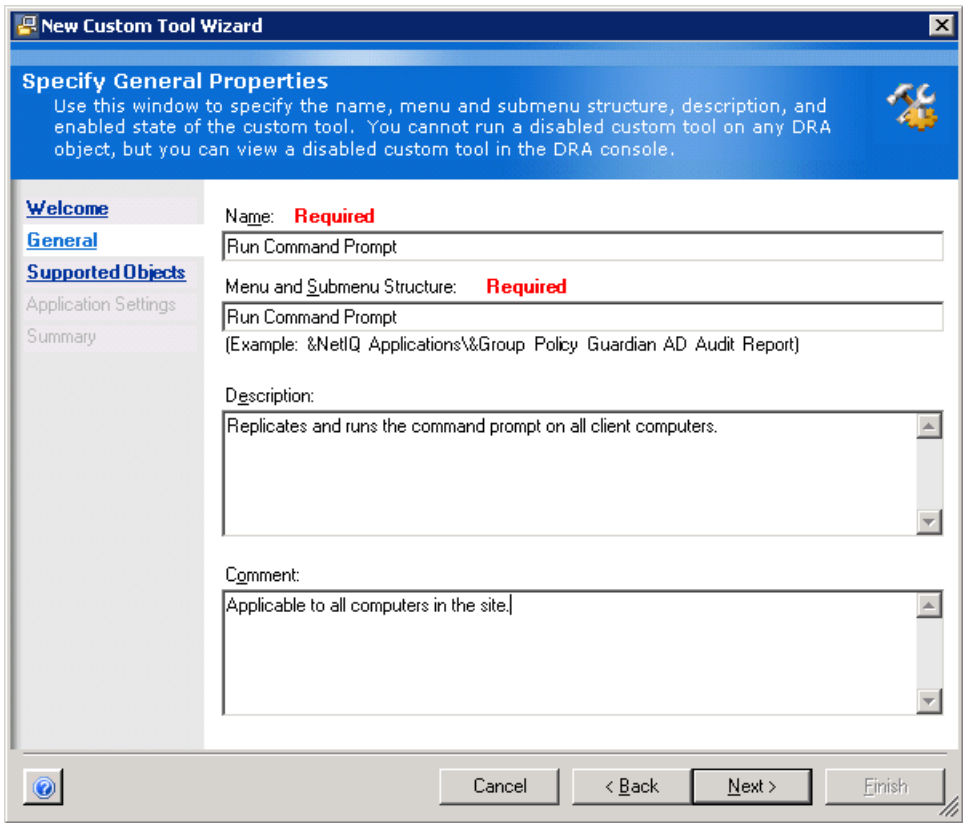
Creating a Custom Tool

You can quickly and easily use DRA to create a custom tool that allows Assistant Admins to run the command prompt on a specific computer from the DRA console.

To create a custom tool that runs the command prompt:

1. Start the Delegation and Configuration console.
2. In the right pane under Common Tasks, click **Configure Directory and Resource Administrator**.
3. Click **Manage Custom Tools**.
4. On the Tasks menu, click **New Custom Tool**.
5. On the Welcome tab, click **Next**.

6. Type `Run Command Prompt` in the **Name** field, as shown in the following figure.



7. Notice that the **Menu and Submenu Structure** field also displays the same value that you entered in the **Name** field. If you want to change the menu item name, type a new name, such as `Launch Command Prompt`. You can also specify a submenu by typing a backslash (\) and the name of the submenu, such as `Launch Command Prompt\CMD`.

Note

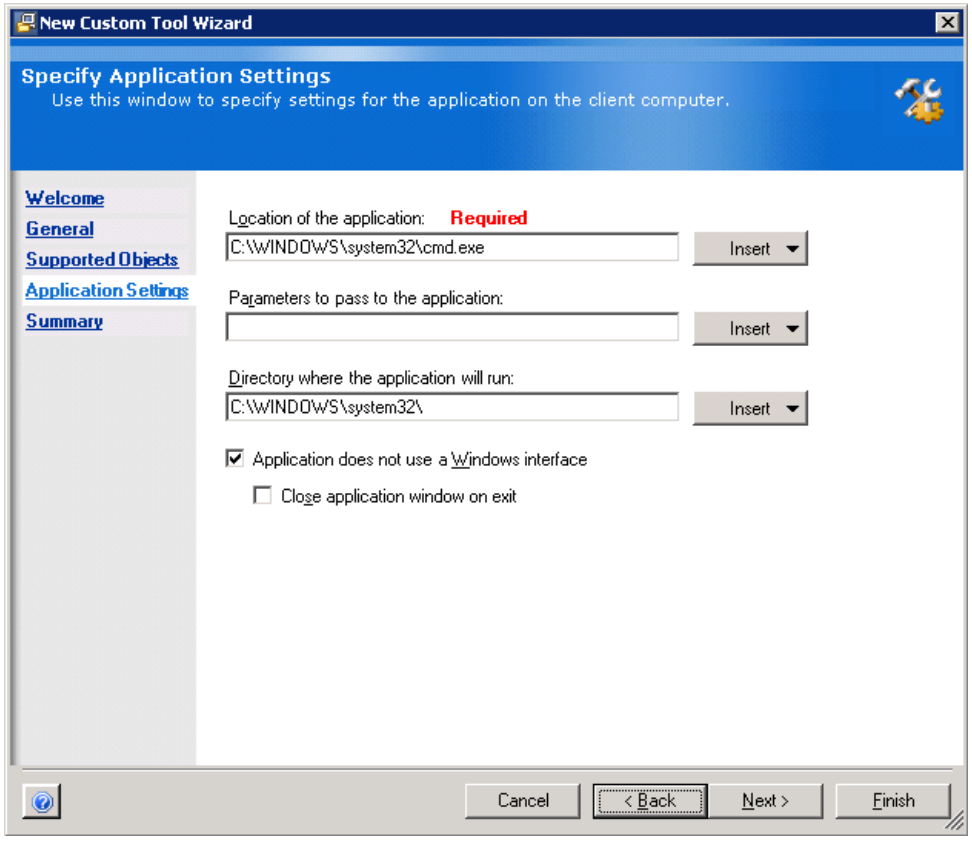
You can create shortcut keys to these new menu items by adding an ampersand (&) before the menu item name. For example, to create a shortcut key for the Launch Command Prompt menu, type `&Launch Command Prompt` in the **Menu and Submenu Structure** field.

---

8. Click **Next**.

9. Select the **Domain** and **Computer** check boxes, and then click **Next**.

10. To define the location of the external application, copy and paste, or type the full path of the application in the **Location of the application** field. For example, to specify the sample executable program to launch an antivirus application, type `C:\WINDOWS\system32\cmd.exe`, as shown in the following figure.



You can also click **Insert** and select the DRA variable as the location of the application, followed by a backslash (\), and then specify the name of the application.

11. Select the **Application does not use a Windows interface** checkbox.
12. Click **Next**.
13. Review the information on the Summary tab, and then click **Finish**.

Distributing Custom Tools Using File Replication

DRA uploads and distributes custom tools you create using the DRA file replication feature. With file replication, you can upload library files, scripts, or executable files to an Administration server and then replicate these files to other Administration server computers and DRA client computers.

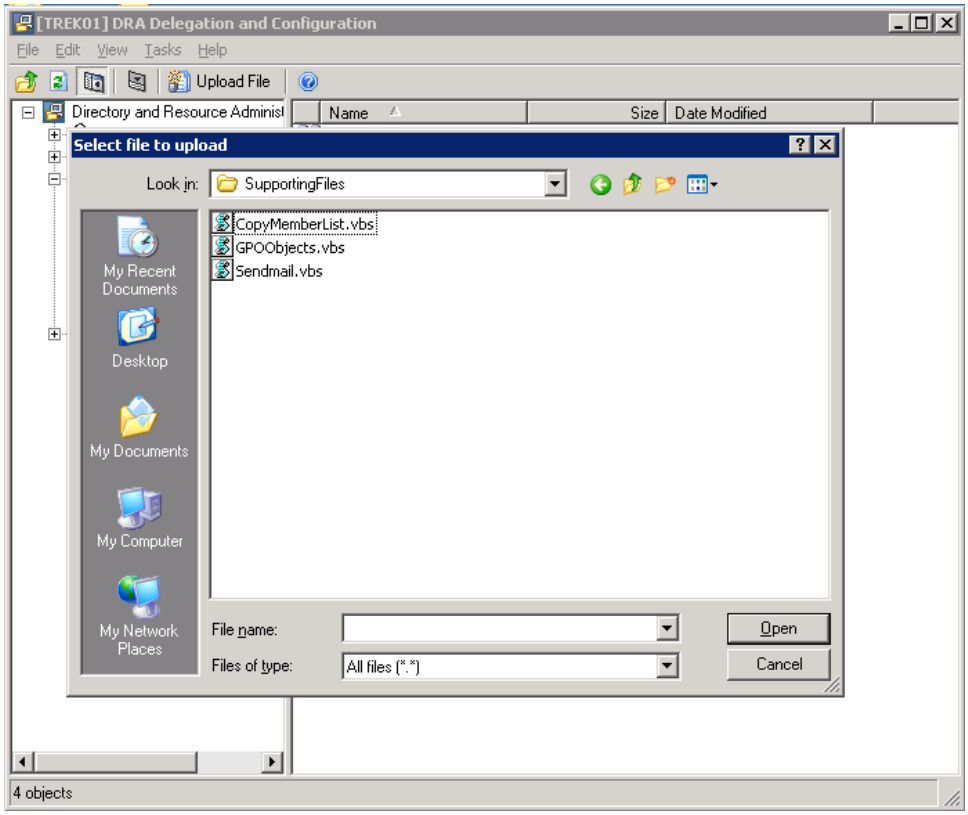
Note

Connect to the primary Administration server to perform the file replication operation. Custom tool properties and settings reside on the primary Administration server. During file replication, DRA copies only custom tool scripts or executable files to the connected DRA client computer.

To replicate custom tools:

1. Start the Delegation and Configuration console.
2. In the right pane under Common Tasks, click **Configure Directory and Resource Administrator**.

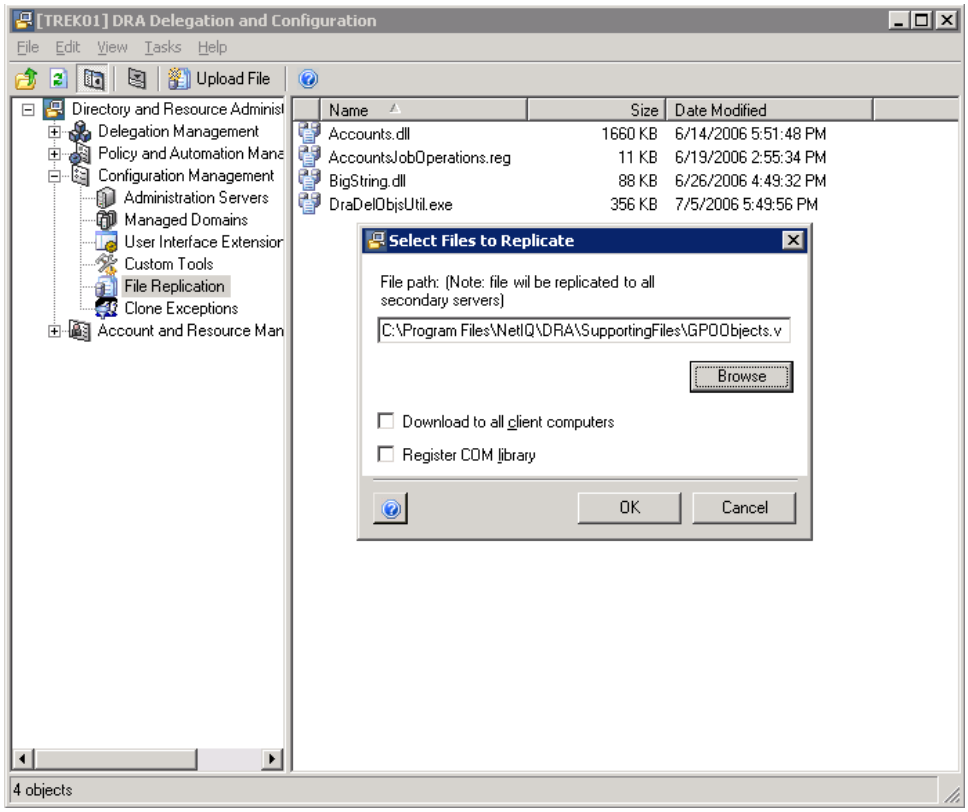
3. Click **Manage File Replication**.
4. On the Tasks menu, click **Upload File**.
5. To search for and select the file you want to upload, click **Browse**. For this demonstration, you can select one of the custom tool sample scripts already available in DRA. By default, you can find these sample scripts in the `C:\Program Files\NetIQ\DRA\SupportingFiles\` folder, as shown in the following figure.



6. ***If you want to download the selected file to all DRA client computers***, select the **Download to all client computers** check box, as shown in the following figure.

Note

If you select this option, whenever a DRA client connects to a primary or secondary Administration server, DRA downloads the file to the DRA client computer. By default, DRA downloads the file to the folder path available in the `{DRA_Replicated_Files_Path}` variable. This folder path can differ for each Administration server.



7. Do not select the **Register COM library** check box. You should only select this option when you are uploading a COM library file.

8. Click **OK**.

DRA replicates the new custom tool to secondary servers to ensure DRA clients connecting to secondary servers can access the new custom tool. DRA replicates the custom tool settings available in the primary Administration server to secondary Administration servers during the MMS replication process.

Similarly, to download custom tool settings to client computers, DRA replicates these settings from the primary Administration server to other Administration servers during the next MMS synchronization. DRA downloads the custom tool settings to the client computers when the client computers connect to the secondary Administration servers.

Using Custom Tools

You can use the new custom tool you created and uploaded to an Administration server after file replication completes. You can verify file replication completed successfully by searching for the file name in the DRAInstallDir folder on the DRA client computer.

After successful file replication, you can use the new custom tool after restarting the DRA console. When you restart the DRA console, DRA downloads the custom tool script or executable file to the DRA client computer.

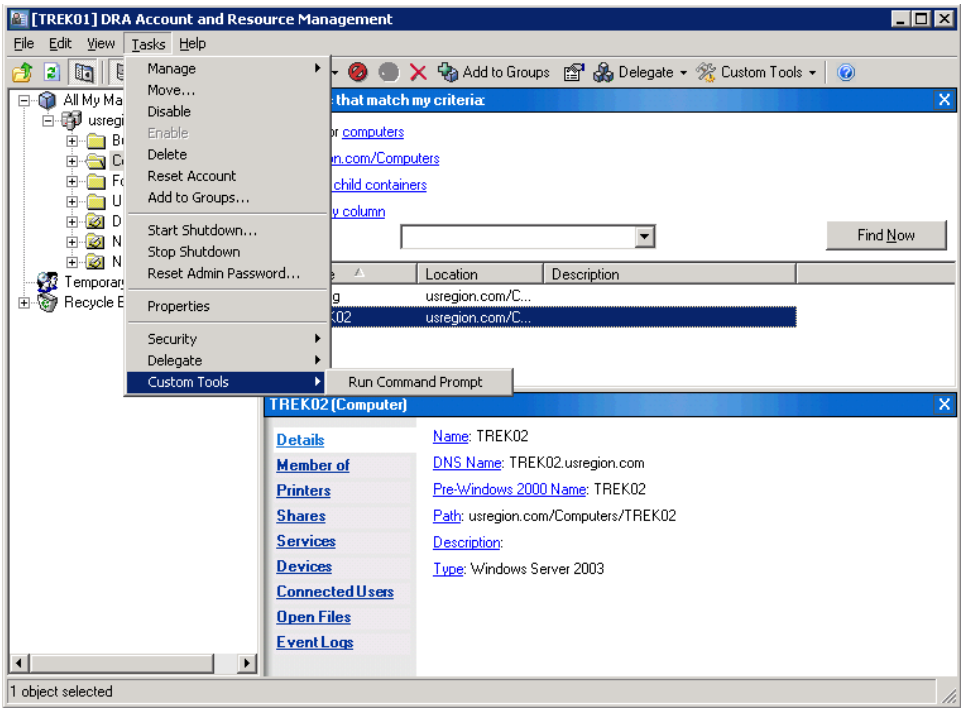
In this task, you can see how DRA makes the command prompt custom tool you created available after you restart the DRA console.

Note
You can run custom tool scripts and executable files only on DRA client computers.

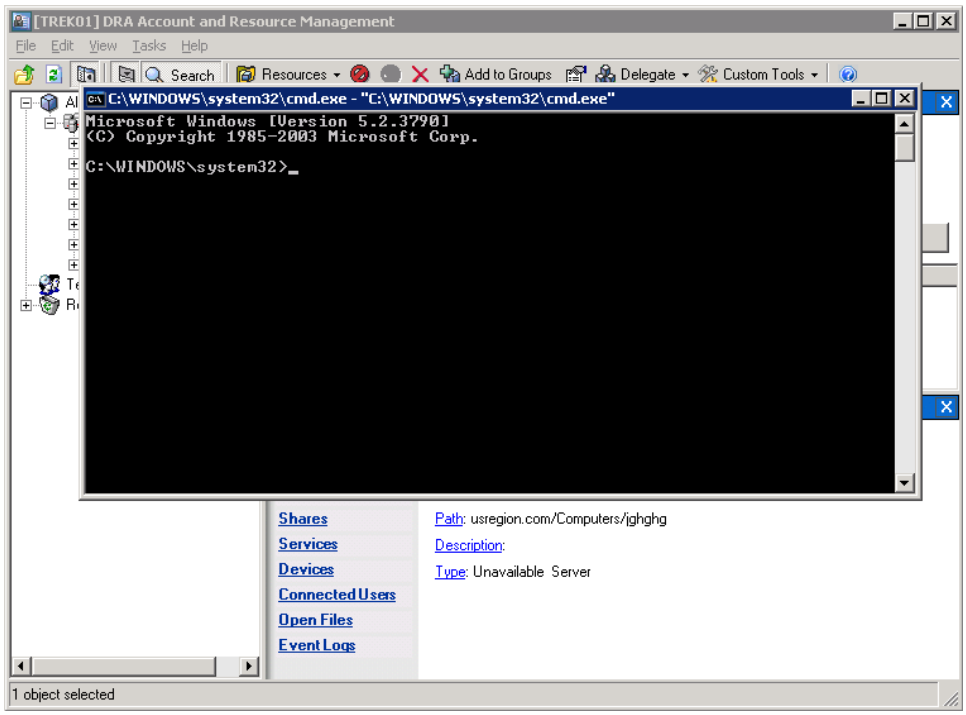
To use the command prompt custom tool:

1. Start the Account and Resource Management console.
2. On the View menu, click **Console Tree**.
3. In the left pane, expand **All My Managed Objects**.
4. To specify the computer account for which you want to use the command prompt custom tool, complete the following steps:
   a. ***If you know the computer account location***, select the domain and OU that contains this object.
   b. ***If you don't know the computer account location,*** specify the computer account attributes in the search pane, and then click **Find Now**.
   c. In the list pane, select the appropriate computer account.
5. On the Tasks menu, click **Custom Tools**, as shown in the following figure.

Note
If you try to select a custom tool for an object, if DRA does not display a custom tool for that object, your DRA administrator has not created or enabled a custom tool for that object.



6. Click **Run Command Prompt**.
7. The command prompt application runs, as shown in the following figure.



Creating a User Account

DRA allows you to generate new user accounts. You can create a user account by typing the account properties in a blank form, or you can clone an existing user account. Many customers find cloning more efficient. Using cloning, you can define several user accounts to be used as templates for each type of user account your enterprise needs. Cloning a user account template ensures that group membership, home directories, and other user account properties are consistent throughout your enterprise.

In this task, you use the Account and Resource Management console to generate a new user account. This task uses policies established by DRA Populator. In the first task, the user account you create meets the established policy and is successful. In the second task, you can see what happens when the user account you want to create does not meet policy.

In addition to creating a new user account, DRA also performs the following actions automatically:

- Checks the employee identification number (ID) against a demonstration human resources (HR) database to verify that the person is an employee. If the employee ID is not in the HR database, DRA does not create the user account.
- Checks the HR database to determine if the employee already has a user account. If the HR database indicates that the employee already has a user account, DRA does not create a new user account.
- Extracts detailed data, such as the employee's telephone number and address, from the HR database and populates the Active Directory properties.
- Generates a home directory for the user.
- Generates a home share for the user.
- Applies a disk quota to the volume containing the new user's home directory.

- Updates the HR database with the employee's user account information if the new user account is created.
- Sends email notification of the user account creation.

To interact with a sample HR database, the following tasks use a Microsoft Access MDB file installed with the product preview utilities.

Create a User Account that Meets Policy

In the following task, DRA creates a user account that meets the policy currently defined in Policy and Automation Management.

To create a new user account using the Account and Resource Management console:

1. Start the Account and Resource Management console.
2. On the View menu, click **Console Tree**.
3. Expand **All My Managed Objects**.
4. Select the location where you want to create this account.

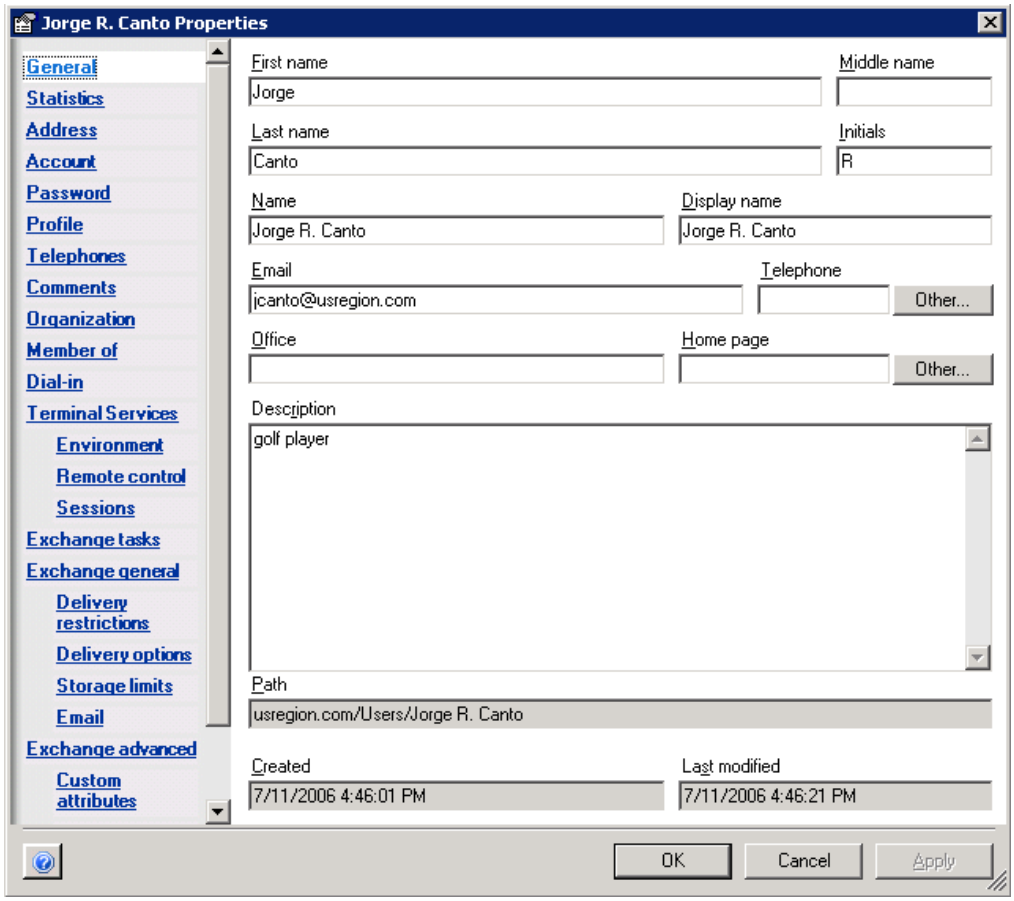
   For example, if you want to create this account in a specific OU of the managed domain, expand the domain and then select the appropriate OU.
5. On the Tasks menu, click **New > User**.
6. On the Welcome tab, click **Next**.
7. In the **Full name** field, type *x*, where *x* is the full name of the user. For this demonstration, it makes no difference what you type in this field because DRA extracts this data from the HR database. However, the wizard requires an entry in this field.
8. In the **User logon name** field, type *x*, where *x* is the user logon name.
9. In the **Employee ID** field, type **1**, and then click **Next**.
10. On the Password and Account tab, click **Next**.
11. On the Profile tab, click **Connect**.
12. Select **H:** from the list.
13. Type `\\`*`ComputerName`*`\`*`HomeShareName`*`\` in the field next to the drive letter, where *`ComputerName`* is the name of the server computer where you installed DRA and *`HomeShareName`* is the name of the home share you created when you prepared your DRA and ExA evaluation environment. For more information, see "Setting Up Your Environment" on page 9.

    Note
    When you enable home directory and share policies, you do not need to make an entry for the specific directory name in the UNC, as in `\\`*`ComputerName`*`\`*`HomeShareName`*`\`*`directoryName`*, where *`directoryName`* is the name of the user account's home directory. DRA automatically creates the directory and share based on the policy you defined. For more information, see "Configuring Home Directory Policy and Automation Triggers" on page 34.
14. Notice that the home volume disk quota entries display the values you assigned in the previous feature demonstration.
15. Click **Next**, and then click **Next** again on the Groups tab.

16. If you enabled Microsoft Exchange administration, the next tab allows you to enable the new user account for use with Microsoft Exchange. Click **Next**.
17. Review the information on the Summary tab, and then click **Finish**. DRA generates the new user account.

Use Windows Explorer to verify that DRA generated the home directory and home share. Use the Microsoft Disk Management MMC snap-in to verify that DRA assigned the home volume disk quota.

To view the new user account, select the account, and then click **Properties** on the Tasks menu. You see a fully established account, as shown in the following figure.



DRA automatically sets most user account information for you. DRA Populator creates triggers that control this automation. For more information about these triggers, see the SDK Help.

Create a User Account that Does Not Meet Policy

The previous task demonstrated how DRA can create user accounts that conform to a specified policy. This task demonstrates how DRA handles requests to create user accounts that do not conform to specified policies.

To create an invalid user account for this demonstration:

1. Start the Account and Resource Management console.
2. On the View menu, click **Console Tree**.
3. Expand **All My Managed Objects**.

4. 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.

5. On the Tasks menu, click **New > User**.
6. On the Welcome tab, click **Next**.
7. In the **Full name** field, type *x*, where *x* is the full name of the user. For this demonstration it makes no difference what you type in this field because DRA extracts this data from the HR database. However, the wizard requires an entry in this field.
8. In the **User logon name** field, type *x*, where *x* is the user logon name.
9. In the **Employee ID** field, type `1`.
10. Click the Summary tab, and then click **Finish**.
11. The Account and Resource Management console displays an error message. DRA does not create the user account if the employee already has a user account. This message also indicates that DRA automatically updated the HR database after you created the user account in the previous feature demonstration. DRA Populator creates the policies that control this validation. You can use DRA to implement similar custom policies in your enterprise.
12. Click **OK** to display the Summary tab again.
13. Click the General tab.
14. In the **Employee ID** field, type `999`.
15. Click the Summary tab.
16. Click **Finish**.
17. This time the Account and Resource Management console displays an error message. This error indicates that the user account is not created because the particular employee ID does not exist in the HR database.
18. Click **OK**.
19. Click **Cancel** and then **Yes** to conclude this feature demonstration.

DRA performed some tasks behind the scenes in the first part of this demonstration. DRA updated the HR database and sent email notifications after the user account was created. You can verify this by checking the user's Microsoft Exchange mailbox. This action is called a post-task automation trigger.

Post-task automation triggers are another powerful DRA automation feature. In this demonstration, you observed the results of the post-task trigger as well as the policy enforcement capabilities of DRA.

Restoring User Accounts with the Recycle Bin

Each Active Directory user account has its own unique security identifier (SID). Once you delete an Active Directory user account, you cannot restore it. You can recreate the same user account again in Active Directory. However, the replacement user account that you create has a different SID. After you create the replacement user account, you must go back and identify each resource to which the user account had access and assign appropriate permissions. In most enterprise environments, this is a difficult, time-consuming, and error-prone task.

The DRA Recycle Bin feature saves your organization time and money when you need to quickly restore a deleted Active Directory object. The Recycle Bin allows you to quickly restore deleted user accounts, computer accounts, groups, and contacts.

DRA enables the Recycle Bin feature by default. When you use DRA to delete an Active Directory user account, the Administration server moves the user account to a hidden OU, disables the user account, and removes the user account from all groups. If you accidentally delete a user account, you can use the Recycle Bin feature to quickly restore the user account and its associated group and Microsoft Exchange distribution list memberships.

For added dual-key security, you can require action from two Assistant Admins before DRA permanently deletes a user account. Use DRA to delegate the power to send a user account to the Recycle Bin to one Assistant Admin and the power to delete a user account from the Recycle Bin to a different Assistant Admin. This dual-key approach to deleting user accounts, computer accounts, groups, and contacts helps ensure Active Directory objects are not inappropriately or accidentally deleted.

This task shows how you can restore a deleted user account from the Recycle Bin.

DRA enables the Recycle Bin feature by default. When an Assistant Admin (AA) deletes an Active Directory user account, the Administration server moves the user account to a hidden OU, disables the user account, and removes the user account from all groups. If an AA accidently deletes a user account, you can restore the user account to active status. The process includes restoring the group and Microsoft Exchange distribution list memberships for the user account.

For added security, you can delegate one power to send a user account to the Recycle Bin and delegate another power to delete a user account that resides in the Recycle Bin. This "dual-key" security feature means you can configure the Administration server so that it requires two AAs to delete a user account.

To delete and restore a user account from the Recycle Bin:

1. Start the Account and Resource Management console.
2. Search for the user account you want to delete. For this demonstration, search for the user Andrew Carnegie by typing `Andrew` in the provided field and then clicking **Find Now**.
3. Select **Andrew Carnegie**.
4. On the Tasks menu, click **Delete**.
5. Click **Yes** when asked if you are sure you want to delete the user account.
6. To restore the user account, click **Console Tree** under the View menu.
7. In the left pane, click **Recycle Bin**.
8. Select the user account from the list.
9. On the Tasks menu, click **Restore**.
10. Click **Yes** when asked if you are sure you want to restore the user account.
11. To verify that the user account has been restored, click **All My Managed Objects** and search for Andrew Carnegie.

Managing Temporary Group Assignments

Temporary group assignments allow you to manage group memberships for users who only need group membership for a specific time period. You can manage temporary group assignments using the Delegation and Configuration console. With the appropriate powers, you can create new temporary group assignments or remove 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. DRA restricts the tasks you can perform if you select multiple temporary group assignments.

Creating a New Temporary Group Assignment

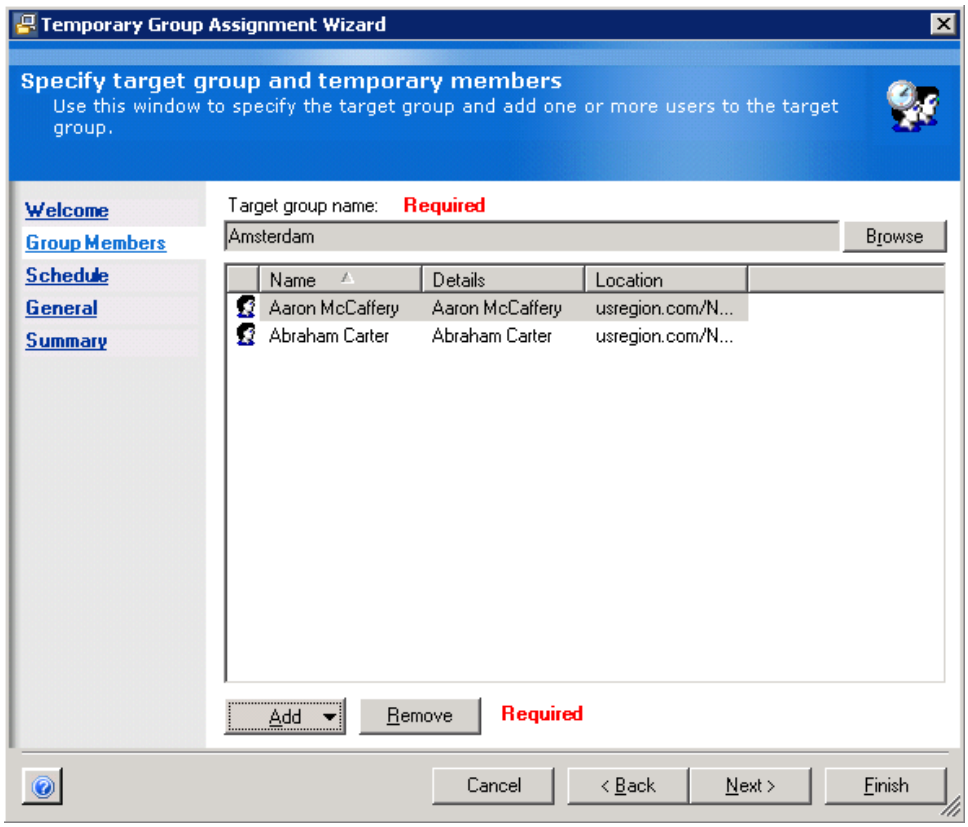
Temporary group assignments give you flexibility in deciding and tracking who has access to which resource or object and for how long. In this task, you will create a new temporary group assignment for the Amsterdam group on the primary Administration server using the Delegation and Configuration console.

Caution
When you use the temporary group assignment feature to assign a user account to a target group, if the user account is already a member of the target group, DRA prevents you from adding that user account as a temporary group assignment to the target group.

To create a temporary group assignment:

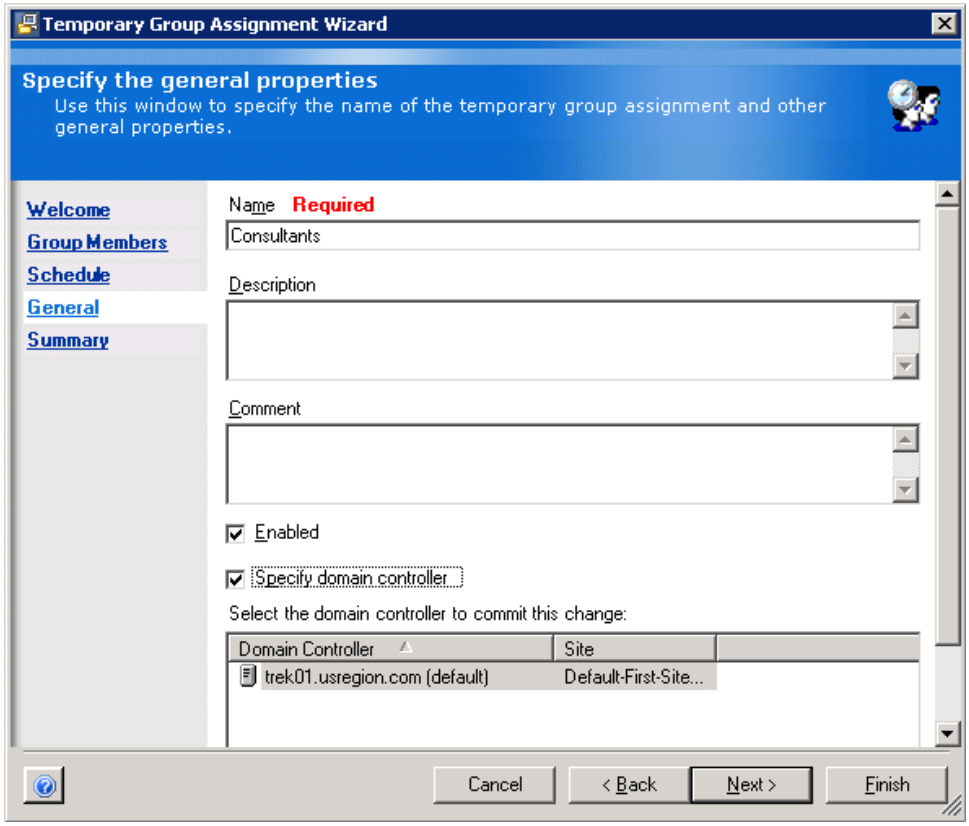
1. Start the Delegation and Configuration console.
2. In the left pane, expand **Account and Resource Management**.
3. Select **Temporary Group Assignment**.
4. On the Tasks menu, click **New Temporary Group Assignment**.
5. On the Welcome tab, click **Next**.
6. To search for and select the Amsterdam group, click **Browse**.
7. To specify the Amsterdam group for which you want to create a temporary group assignment, complete the following steps:
   a. Type `Amsterdam` in the search pane, and then click **Find Now**.
   b. In the list pane, select **Amsterdam**, and then click **Add**.
   c. Click **OK**.
8. To add user accounts to the temporary group assignment, click **Add > Users** and complete the following steps:
   a. ***If you know the user account location***, select the domain and OU that contains this user account.
   b. If you do not know the user account location, specify the user account attributes, and then click **Find Now**.
   c. In the list pane, select the **Aaron McCaffery** and **Abraham Carter**, and then click **Add**.

9. Click **OK**. You will see the selected group members, as shown in the following figure.



10. Click **Next**.
11. On the Schedule tab, in the Start Temporary Assignment area, click **Immediately**.
12. Select the **Keep this temporary group assignment for future use** check box to make the temporary group assignment available after it expires.
13. Click **Next**.
14. Type `Consultants` in the **Name** field.

15. Select the **Specify domain controller** check box and select the domain controller you will use to add or remove group members.



16. Click **Next**.
17. Review the summary, and then click **Finish**.

Rescheduling a Temporary Group Assignment

Rescheduling temporary group assignments enable you to extend or decrease the amount of time a temporary group assignment is active. This feature lets you decide how long users have access to Active Directory resources. In this task, you will reschedule a temporary group assignment.

To reschedule a temporary group assignment:

1. Start the Delegation and Configuration console.
2. In the left pane, expand **Account and Resource Management**.
3. Select **Temporary Group Assignment**.
4. In the list pane, select **Consultants**.
5. On the Tasks menu, click **Properties**.
6. Click the Schedule tab.
7. Specify a new end time.

> **Note**
> If the temporary group assignment is currently inactive, you can also specify a new start time.

8. To save a temporary group assignment for future use, select the **Keep this temporary assignment for future use** checkbox, and then click **OK**.

Note
When a temporary group assignment expires, unless you have specified that you want to keep the temporary group assignment for future use, DRA automatically deletes the temporary group assignment.

Deleting a Temporary Group Assignment

In this task, you will delete a temporary group assignment on the primary Administration server.

To delete a temporary group assignment:

1. Start the Delegation and Configuration console.
2. In the left pane, expand **Account and Resource Management**.
3. Select **Temporary Group Assignment**.
4. In the list pane, select **Consultants**.
5. On the Tasks menu, click **Delete**.
6. Click **Yes**.

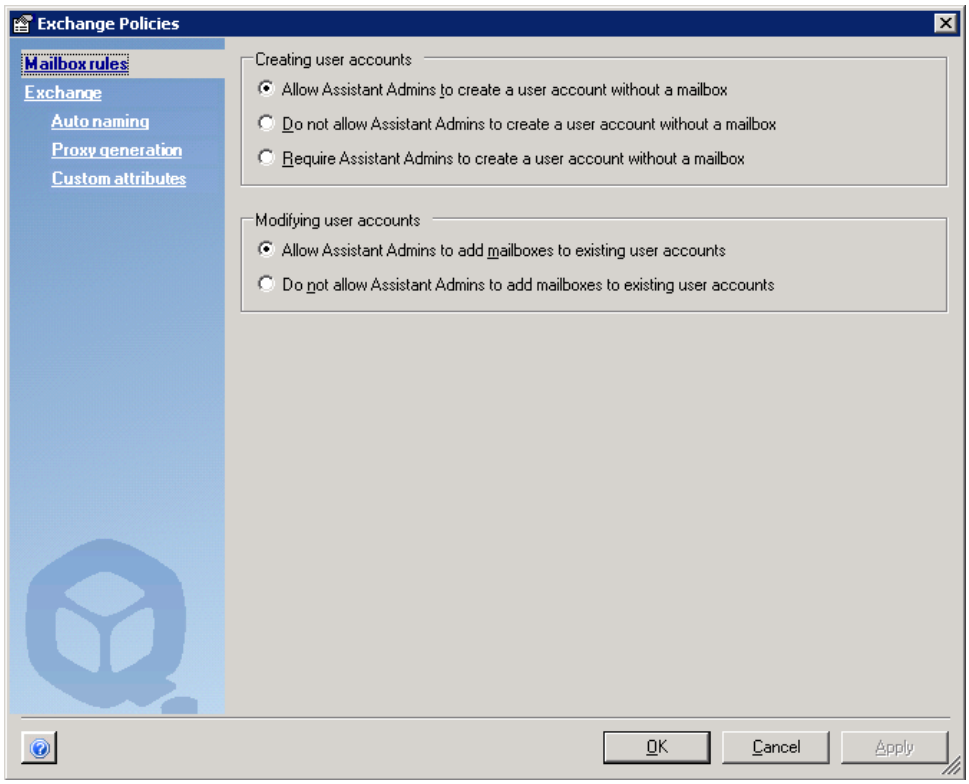
Setting Microsoft Exchange Policies

ExA automates tasks and enforces policies for Microsoft Exchange mailboxes and tasks. ExA offers several policies for effective Microsoft Exchange management. The following task shows how easy it is to configure Microsoft Exchange 2003 mailbox policies using the Delegation and Configuration console. ExA also supports Microsoft Exchange 2007 and Microsoft Exchange 2010. For more information, see the *User Guide*.

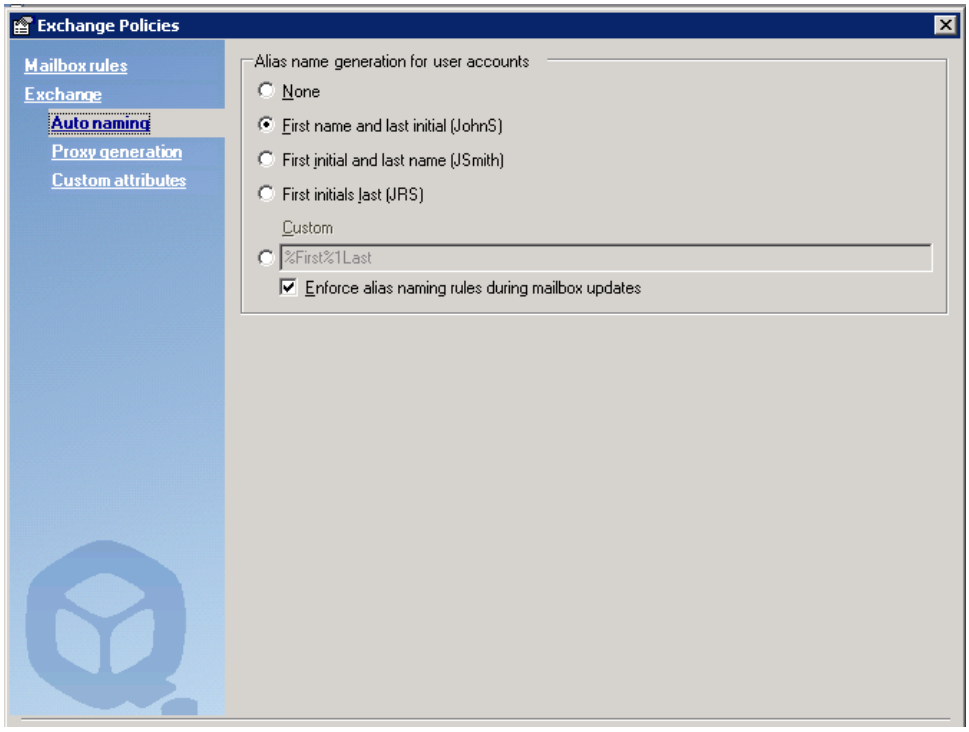
To create Microsoft Exchange 2003 mailbox policies:

1. Start the Delegation and Configuration console.
2. In the left pane, expand **Directory and Resource Administrator**.
3. Click **Policy and Automation Management**.
4. On the Tasks menu, click **Configure Exchange Policies**.
5. Select the **Enable Exchange 2003 Administration support** check box.

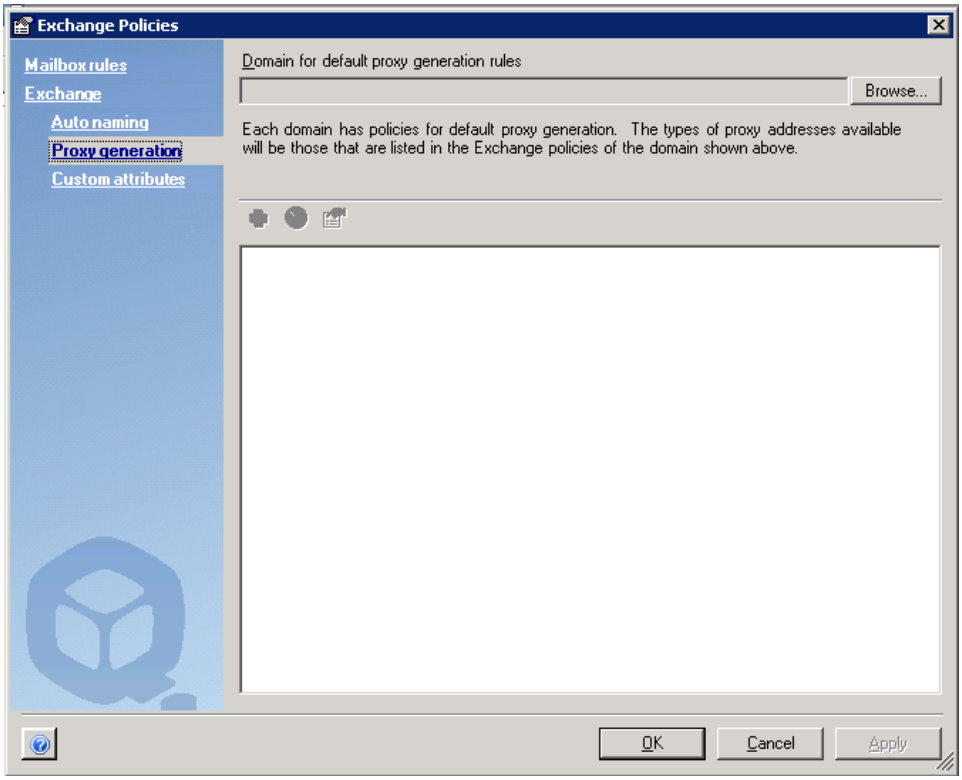
6. Click the Mailbox rules tab. This tab lets you enable or disable support for Microsoft Exchange mailboxes. The policies you define on this tab govern how mailboxes are handled when Assistant Admins create and modify user accounts, as shown in the following figure.



7. Under the Exchange tab, click the Auto naming tab. The policies you define on this tab govern the formats for the mailbox alias, as shown in the following figure.



8. Under the Exchange tab, click the Proxy generation tab. From this window, you can specify the proxy addresses generated when ExA creates a mailbox. You can specify any number of proxy addresses for an address type, as shown in the following figure.



For example, you can define a proxy address that uses the format `%1First%Last@domain.com`. Using this definition, DRA automatically generates the email address `Carnegie_Andrew@Pittsburgh.com` when you create an account for Andrew Carnegie in the Pittsburgh domain.

9. After you create your Microsoft Exchange 2003 mailbox policies, click **OK**.

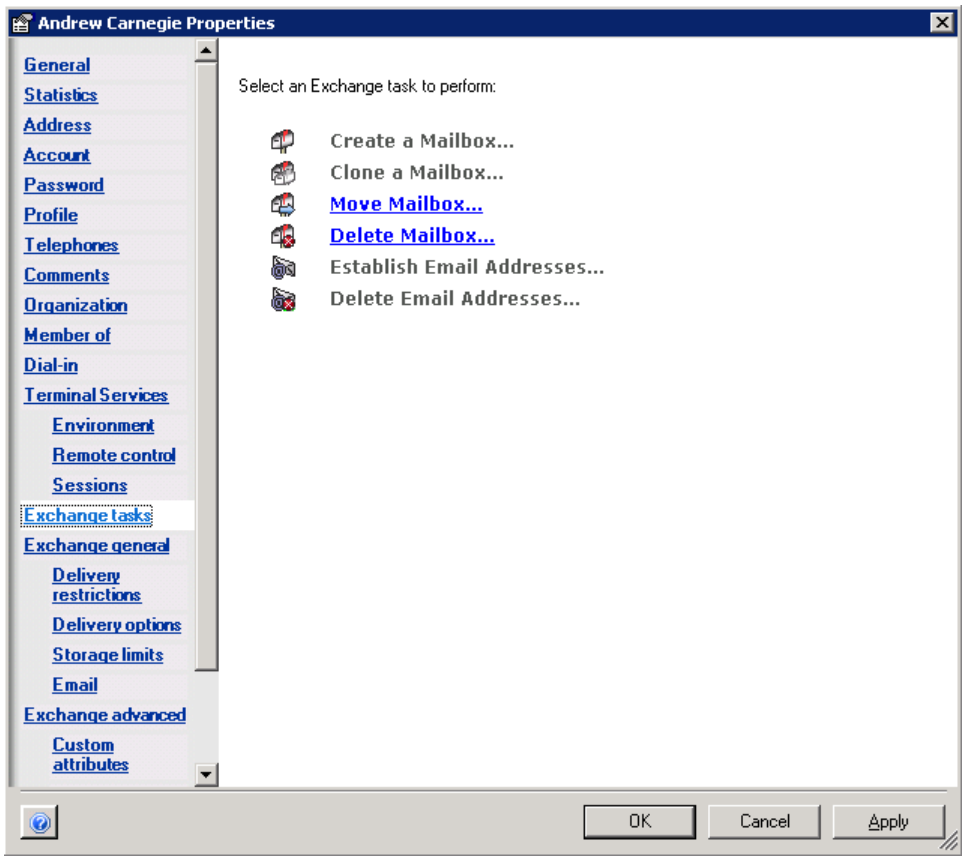
Integrated Microsoft Exchange Mailbox Administration

When you enable Microsoft Exchange mailbox administration, ExA treats Microsoft Exchange mailboxes as an extension of the user account. You can then manage Microsoft Exchange mailbox properties using the same interface that DRA uses for managing user account properties. This task illustrates ExA managing Microsoft Exchange mailboxes.

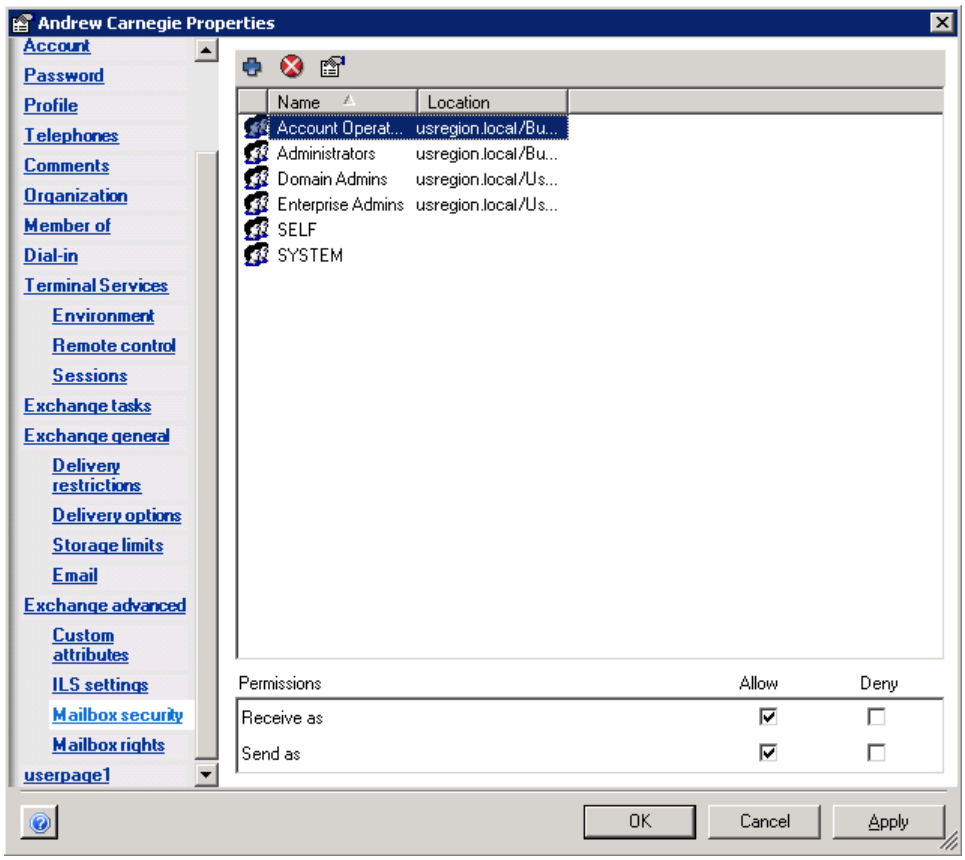
To manage Microsoft Exchange mailbox properties:

1. Start the Account and Resource Management console.
2. Search for the user account you want to manage. For this task, search for the user Andrew Carnegie by typing `Andrew` in the search pane and then clicking **Find Now**.
3. Select **Andrew Carnegie**.
4. On the Tasks menu, click **Properties**.

5. Click the Exchange tasks tab. ExA displays the available Exchange tasks for the specified user account, as shown in the following figure.



6. Under the Exchange advanced tab, click the Mailbox security tab. ExA displays the Exchange permissions for mailbox security.



7. Click other tabs to view additional mailbox properties. Note that ExA automatically supplies information that was entered for this user when the user account was created.

8. When you are done managing Microsoft Exchange mailbox properties, click **OK**.

Automation and Policy in Action

The following demonstration shows how DRA can help validate and automate address changes. When an employee changes location, items like building address and group memberships also need to change. Adding and removing user accounts from the appropriate groups and Microsoft Exchange distribution lists can be time-consuming. In this demonstration, DRA performs the following tasks:

- Validates that a correct location has been specified
- Updates the other address-related properties for the new location
- Adds and removes the user account from the appropriate groups, based on the specified location

To update an address for a user:

1. Start the Account and Resource Management console.

2. Search for the user account you want to manage. For this task, search for the user Andrew Carnegie by typing `Andrew` in the search pane and then clicking **Find Now**.

3. Select **Andrew Carnegie**.

4. On the Tasks menu, click **Properties**.
5. Click the Member of tab and note the group membership for this user.
6. Click the Address tab.
7. In the **City** field, change `Pittsburgh` to `Cleveland`, and then click **Apply**. A confirmation message dialog displays to indicate that Cleveland was an invalid location. This dialog also shows a list of valid locations.
8. Click **OK**.
9. Change `Cleveland` to `London`, and then click **OK**.
10. Select **Andrew Carnegie**.
11. On the Tasks menu, click **Properties**.
12. Click the Address tab. Notice that the city is London.
13. Click the Member of tab. Notice that the user account has moved from the Pittsburgh group to the London group.

Viewing Reports in Directory and Resource Administrator and Exchange Administrator

If you installed the optional reporting components, including NetIQ Reporting Center, you can view a summary of changes you made with DRA in your environment. You must enable reporting in the DRA Configuration Management console and enable and configure schedules for the data collectors in DRA to run before you can see reports with data in Reporting Center. For more information, see "Enabling and Configuring DRA Management Reports" on page 14.

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 start Reporting Center:

1. Log on to the computer that is running the Reporting Center Console.
2. Click **Start > Programs > NetIQ > Reporting Center > Reporting Center Console**.
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.

Removing Evaluation Data and DRA and ExA Programs

After you have evaluated DRA, ExA, the Account and Resource Management console, the Delegation and Configuration console, and the Web Console, you may want to remove the evaluation data, evaluation programs, and the DRA and ExA products from your evaluation computer.

To remove evaluation data and programs:

1. Close the Delegation and Configuration console, the Account and Resource Management console, and the Web Console.
2. Remove the Active Directory test objects generated by AD Populator by completing the following steps:
   a. Start the Active Directory Users and Computers MMC snap-in.
   b. Select **NetIQ DRA-ExA Product Preview**, the top level OU you created when you installed AD Populator, and click **Delete** on the Action menu.
   c. Click **Yes** to delete the OU.
   d. Click **Yes** to confirm the deletion of the OU and its contents.
3. Uninstall AD Populator and DRA Populator by completing the following steps:
   a. Start **Add/Remove Programs** in the Control Panel window.
   b. Select **NetIQ DRA-ExA Evaluation Guide Utilities** and click **Change/Remove**.
   c. Click **Yes**, and then click **OK**.
4. Uninstall DRA and ExA by completing the following steps:
   a. Start **Add/Remove Programs** in the Control Panel window.
   b. Select **NetIQ Administration Products** and click **Change/Remove**.
   c. Click **Remove All**.
   d. On the Remove Registry Entries window, click **Yes** and then click **Next**.
   e. Click **Next**, and then click **Continue**.
   f. Click **Finish**.