Directory and Resource Administrator Exchange Administrator

User Guide

June 2017

NetIQ

Legal Notice

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

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

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

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

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

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

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

Contents

About This Book and the Library

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

Intended Audience

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

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

Administrator Guide

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

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

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

Conventions

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

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

About NetIQ Corporation

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

Contacting Sales Support

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

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

.

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

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

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

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

1 Introduction

NetIQ Enterprise Administration solutions provide enterprise customers with the ability to safely and securely delegate administrative privileges across their Windows server, Active Directory, Group Policy, Office 365, Skype, and Exchange server environments. Combined with detailed auditing of and reporting on administrative activities, NetIQ Enterprise Administration solutions provide organizations with unprecedented levels of accountability while reducing the costs associated with daily operations, internal policy, and regulatory compliance activities.

Organizations have increasingly relied upon Active Directory for the central management of identities and for the authentication and authorization of those identities to the network and IT services. With the introduction of Office 365, organizations have come to depend more and more on maintaining a single point of control over on-premises and cloud directory and messaging administration. However, assuring the security, availability and integrity of Active Directory and Office 365 requires more than just delegating permissions or changing group memberships. IT Governance and auditors also require proof that policies and procedures are enforced, that changes are tracked, and that administrators are not able to manage beyond the scope of their responsibilities.

NetIQ Directory and Resource Administrator (DRA) delivers an unparalleled ability to control who can manage what within Active Directory and Office 365 while protecting the consistency and integrity of its information by validating all administrative changes. Through granular delegation of permissions, robust change management policies, and automation that simplifies workflows, DRA reduces down time and operational risks to Active Directory and Office 365 that are posed by the consequences of malicious or accidental changes.

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

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

Key benefits of DRA include:

Policy and regulation compliance

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

Operational integrity

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

Process enforcement

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

What are DRA and ExA?

DRA and ExA are comprehensive account and resource management products for the key Microsoft identity and messaging platforms, Active Directory, Office 365, and Exchange. Using a flexible, rules-based management model, both DRA and ExA deliver capabilities that streamline administration, increase security, assure operational integrity, and ease the challenges of regulatory compliance for your Active Directory, Office 365, and Microsoft Exchange messaging environments.

An enterprise-scale directory and resource management product, DRA controls and manages Active Directory and Office 365 administration. Its powerful policy-based management, coupled with its safe, distributed administration, dramatically reduces administration efforts and costs. DRA provides increased data security while protecting the integrity of your Active Directory and Office 365 content.

ExA extends the power and flexibility of DRA to include Microsoft Exchange, Office 365, and Skype management. Within the context of account administration, you can manage mailboxes, Microsoft Exchange permissions, contacts, and distribution lists. DRA and ExA provide a single, integrated solution for controlling and managing complex IT environments.

What DRA and EXA Provide

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

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

Environment	Supported Versions		
Microsoft Windows Server Active Directory	2012	2012 R2	2016
Microsoft Exchange Server	2013	2016	Microsoft Exchange Online

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

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

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

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

These technologies seamlessly join and manage data from multiple sources across your enterprise, including Active Directory, Office 365, Microsoft Exchange, and computer resources. To further expand these benefits, DRA and ExA let you apply policies to directory updates that can extend beyond the directory itself to other applications and databases, making the task of enterprise management easy.

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

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

DRA supports the 64-bit platform, which provides you with increased scalability, increased performance, reduced query time, and more effective use of memory.

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

2 Working with the User Interfaces

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

Web Console

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

Account and Resource Management Console

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

PowerShell

NetIQ Reporting Center Console

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

Web Console

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

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

Starting the Web Console

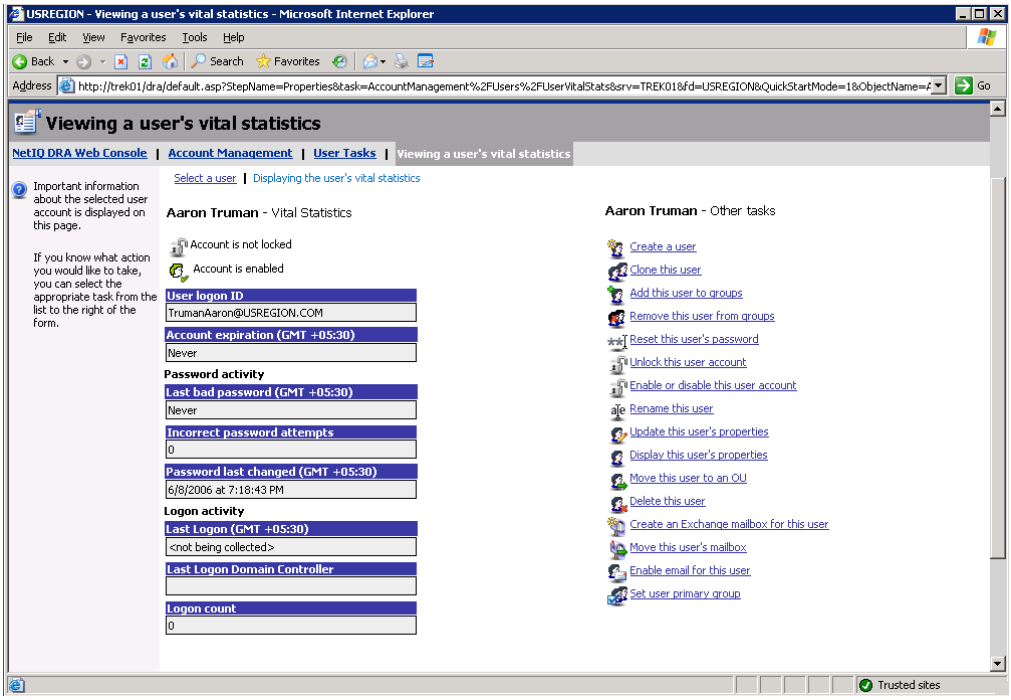
You can start the Web Console from any computer running Internet Explorer, Chrome, or Firefox. To start the Web Console, specify the appropriate URL in your Web browser address field. For example, if you installed the Web component on the HOUserver computer, type `http://HOUserver/draclient` in the address field of your Web browser.

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

Using Quick Start to Solve Issues

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

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



Customizing the Web Console

You can quickly and easily customize the Web Console in the following ways:

Create or modify property pages

For example, you can modify the user property page to display a military rank field.

Modify provided tasks

For example, you can modify the update user's properties task to include a new field that manages a proprietary setting. You can hide specific tasks you do not want Assistant Admins (AAs) to use regardless of their delegated powers. You can also publish reports generated from Directory and Resource Reporting.

Develop new tasks

For example, you can develop a new update user's properties task that meets your unique administration needs. You can replace provided tasks with custom tasks without losing built-in functionality.

Modify workflows

For example, you can modify the Web Console framework and navigation, changing how AAs step through a given task. This flexibility allows you to add, remove, or move steps to create the exact solution you require.

Modify Aegis forms

Deploy multiple Web Console applications

You can install and configure multiple Web Console applications. For example, you can deploy one custom Web Console application for your Houston facility and another custom Web Console application for your Atlanta facility. Each application can support a unique set of tasks that meet the specific needs of your facility. For more information, see the Deploying DRA in Unique Environments Technical Reference. For more information about customizing the Web Console, see the Directory and Resource Administrator Software Development Kit.

Account and Resource Management Console

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

The Account and Resource Management console contains the following nodes:

All My Managed Objects

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

Temporary Group Assignments

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

Advanced Search Queries

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

Recycle Bin

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

To start the Account and Resource Management console interface, click **Account and Resource Management** in the Directory and Resource Administrator program folder.

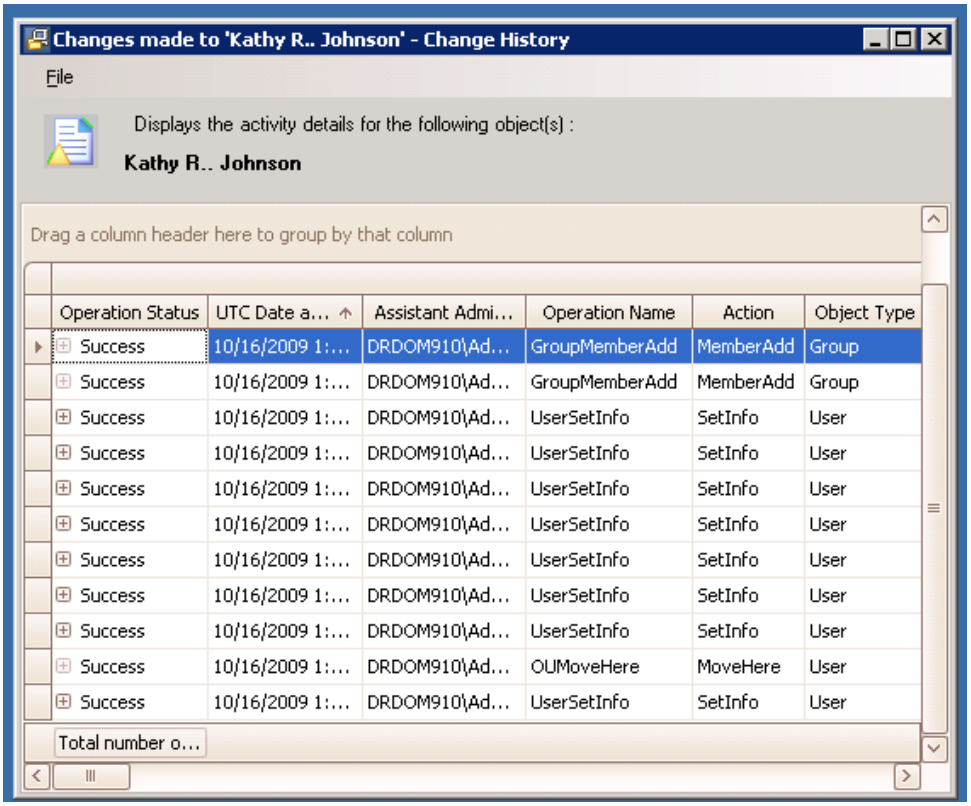
When you start the Account and Resource Management console, you initially connect to the best available Administration server in the local domain. The best-available Administration server is the closest server, which is typically a server in the network site. By seeking the best available Administration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

DRA Reporting

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

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

The following figure shows a sample Activity Detail report:



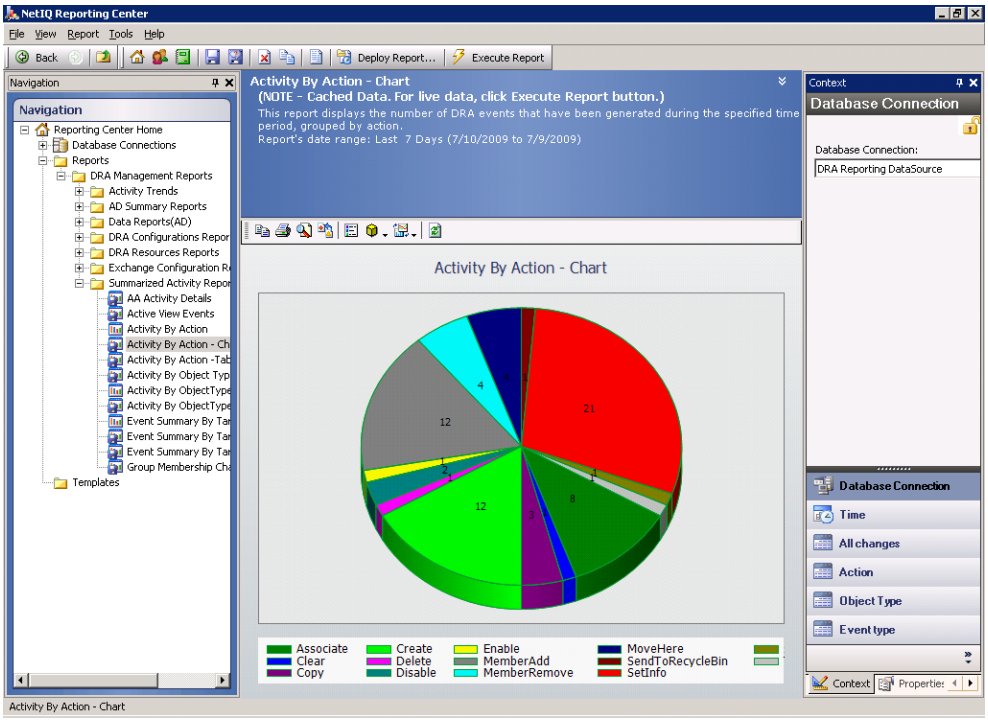
Optional **DRA Management reports**, viewed through the NetIQ Reporting Center (Reporting Center), provide activity, configuration, and summarization information about events in your managed domains. Some Management reports are available as graphical representations of the data. These built-in reports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

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

You must install and configure the optional Management reports before you can view these reports. For more information about installing reporting components, see the *Installation Guide*. For more information about DRA Reporting, see “DRA Reporting” on page 16.

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

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



Understanding DRA Reporting

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

Activity Detail reports

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

DRA Management reports

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

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

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

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

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

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

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

How DRA Uses Log Archives

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

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

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

DRA always writes audit events to the log archive. You can enable or disable having DRA write events to the Windows event logs as well.

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

Understanding Dates and Times

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

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

- `dd/mm/yyyy`
- `dd-mm-yyyy`

3 Managing User Accounts, Groups, and Contacts

Managing User Accounts

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

Global user account

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

Local user account

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

User Accounts in Trusted Domains

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

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

To modify user accounts or groups in a managed domain, you must first connect to the Administration server managing that domain. You must also have the appropriate powers to modify those user accounts or groups.

Transforming User Accounts

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

Understanding the Transformation Process

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

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

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

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

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

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

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

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

- Euro Hotspots DL
- Euro Sales Mang DL
- Global Sales Sec
- Euro Sec

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

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

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

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

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

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

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

Creating User Transformation Templates

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

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

Transforming User Accounts

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

To transform a user account:

1. In the left pane, expand **All My Managed Objects**.
2. To specify the user account you want to manage, complete the following steps:
   - 2a ***If you know the account location***, select the domain and OU that contains this user account.
   - 2b In the search pane, specify the account attributes, and then click **Find Now**.
   - 2c In the list pane, select the appropriate user account.
3. Click **Tasks > Transform**.
4. Review the Welcome window, and then click **Next**.
5. On the Select User Template window, use **Browse** to the select the appropriate subtractive template user.
6. ***If you want to review the properties of the subtractive template user account***, click **View**.
7. Use **Browse** to the select the appropriate additive template user.
8. ***If you want to review the properties of the additive template user account***, click **View**.

9 ***If you have the appropriate powers***, you can check **Change other properties of the user** and select properties to modify. Click **Next** to navigate through the properties available. For more information, click **?**.

10 Click **Next**.

11 Review the Summary window, and then click **Finish**.

Managing Groups

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

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

Group Contents

Groups can contain the following objects:

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

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

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

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

Group Types

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

Security Groups

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

Distribution Groups

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

Group Scope

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

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

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

Group Scopes in Mixed and Native Modes

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

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

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

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

Temporary Group Assignments

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

Managing Dynamic Distribution Groups

A dynamic distribution group is a mail-enabled Active Directory group object that you can create to expedite the mass sending of email messages and other information.

The membership list for a dynamic distribution group is calculated each time a message is sent to the group, based on the filters and conditions that you define. This differs from a regular distribution group, which contains a defined set of members. When an email message is sent to a dynamic distribution group, it is delivered to all recipients in the organization that match the criteria defined for that group.

DRA supports the following features:

- Audit and UI reporting

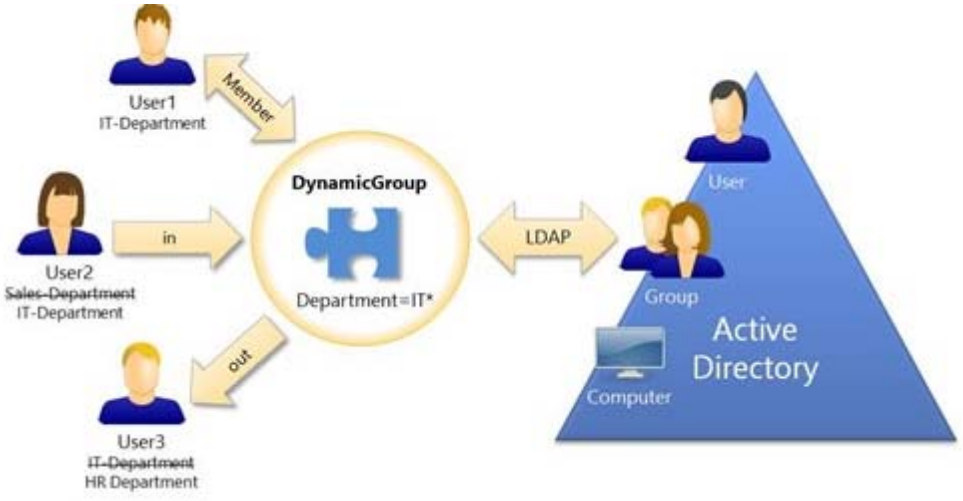
- Enumeration support for dynamic distribution groups
- NetIQ Reporting Center (NRC) report for dynamic distribution groups
- Trigger operation support for dynamic distribution groups
- UI extension support for Exchange dynamic distribution groups

Managing Dynamic Groups

A dynamic group is one whose membership changes based on a defined set of criteria. Until now dynamic groups were only possible in the Exchange environment, but now they can also be created in the Active Directory setting.

The graphic below describes a typical use for an Active Directory dynamic group. There are three dynamic groups in the graphic. Each group has a set of criteria that determines who can be added to the group and who can not. Each group controls access to a specific set of files, folders, and applications.

TIP: You can create a *static member list* that contains permanent members of the dynamic group; you can also create an *excluded member list* that denies those users membership in the dynamic group.



User2 has recently joined the IT department. When the IT department's dynamic group is updated, she will be added to the group. When the Sales department's dynamic group is updated, User2 will be removed from its members list.

TIP: You can refresh a dynamic group's member list by right-clicking it and selecting **Update Members**.

User3, who has left the IT department for the HR department, will be removed from the IT department dynamic group and added to the HR department dynamic group.

Managing Contacts

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

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

4 Managing Exchange Mailboxes

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

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

5 Managing Resources

Managing OUs and the Active Directory

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

Built-in Containers

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

Managing Computers

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

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

---

Managing Services

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

Managing Printers and Print Jobs

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

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

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

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

Managing Shares

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

Managing Advanced Queries

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

Managing Connected Users

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

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

Managing Devices

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

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

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

Managing Event Logs

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

DRA records user-initiated operations in the log archive, a secure repository. You have the option to have DRA also record user-initiated operations in the Windows Event Log in addition to recording the information in the DRA log archive. For more information, see “How DRA Uses Log Archives” on page 18.

Managing Open Files

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

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

Managing the Recycle Bin

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