Installation Guide

Directory and Resource Administrator
Exchange Administrator

February 2012

Legal Notice

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

Contents

About This Book and the Library

The *Installation Guide* provides planning, installation, licensing, and configuration information for the following products:

- Directory and Resource Administrator (DRA)
- Exchange Administrator (ExA)

This book guides you through the installation process and helps you make the correct decisions to install and configure DRA and ExA.

Intended Audience

This book provides information for anyone installing DRA or ExA.

Other Information in the Library

The library provides the following information resources:

Administrator Guide

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

User Guide

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

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

Provides comprehensive concepts, 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 measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

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

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

Contacting Documentation Support

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

Contacting the Online User Community

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

Chapter 1
Introduction

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

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

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

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

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

Key benefits of DRA include:

Policy and regulation compliance

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

Operational integrity

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

Process enforcement

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

What are DRA and ExA?

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

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

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

What DRA and EXA Provide

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

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

- Microsoft Windows Server 2003 Active Directory, Microsoft Windows Server 2008 Active Directory, and Microsoft Windows Server 2008 R2 Active Directory
- Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, and Microsoft Exchange Server 2010

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

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

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

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

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

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

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

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

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

How DRA and ExA Help You

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

Provide Regulatory Compliance

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

Recycle Bin

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

Dual-Key Tasks

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

Policy Enforcement and Automation

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

Naming Convention Enforcement

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

Transform User Tasks

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

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

Maintain Control of Active Directory

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

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

Increase Administration Efficiency

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

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

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

Reduce Administration Costs

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

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

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

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

Ensure Data Integrity

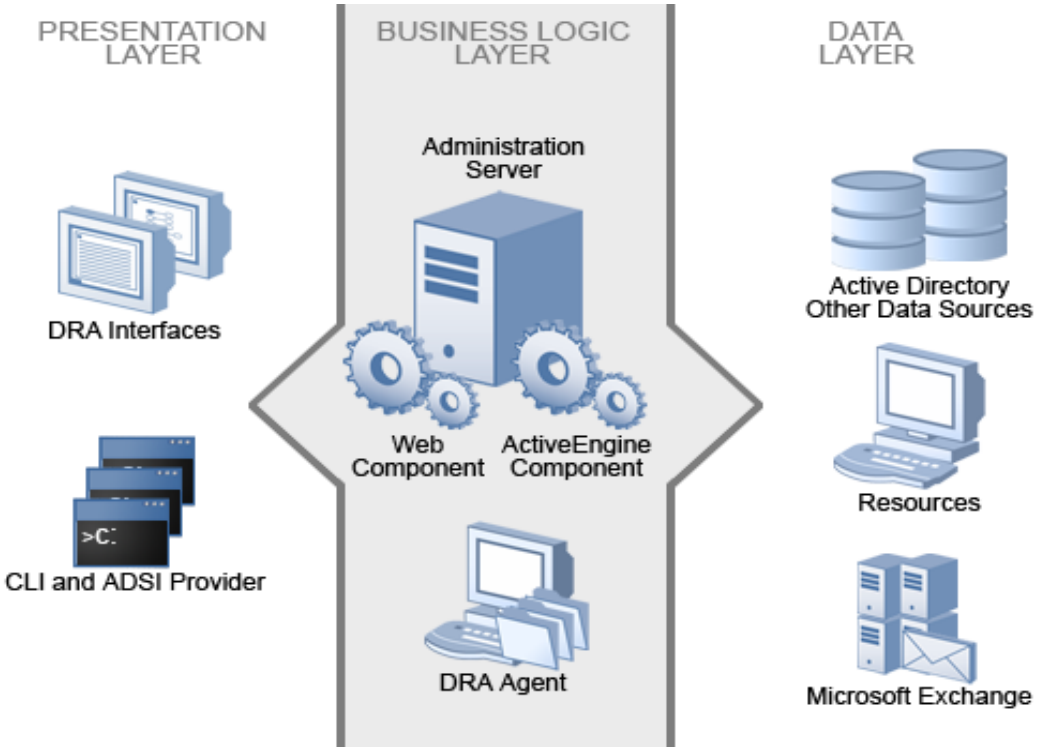
Managing any data set that contains inconsistencies creates security risks and may interfere with efficient operations. You can publish naming policies and permission guidelines for different accounts, but users may not remember to follow the guidelines. DRA can automatically enforce your policies, ensuring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

How DRA and ExA Work

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

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

These products use the same native interfaces as the native Active Directory and Microsoft Exchange administration consoles. Therefore, DRA and ExA are as secure and reliable as Active Directory and Exchange. DRA and ExA support a three-tiered architecture that efficiently distributes workload into three functional layers, namely the presentation layer, business logic layer, and data layer. Each layer addresses different processes and functions and enables fast performance and reduced network load.



Presentation Layer

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

Delegation and Configuration Console

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

Account and Resource Management Console

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

Web Console

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

NetIQ Reporting Center Console

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

Command-Line Interface

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

DRA ADSI Provider

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

Business Logic Layer

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

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

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

This layer includes the following components:

ActiveEngine component

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

NetIQ DRA Core

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

DRA Agents (optional)

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

Log Archive Service

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

Web component

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

Data Layer

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

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

Chapter 2
Understanding Requirements

This chapter outlines the recommended hardware, software, and permissions requirements for DRA and ExA. This chapter also provides licensing requirements.

Administration Server Requirements

The Administration server computer should be a server in the domain you plan to manage.

Notes

- To connect to the Administration server, your user account must be from a managed or trusted domain. When you first start the user interfaces, DRA initially connects to the domain of your logon account. If you attempt to log on to a domain or computer that is not managed by an Administration server, or if DRA cannot connect to the Administration server for your managed domain or computer, DRA may display an error message. Ensure your logon account is from the managed domain or establish a trust relationship and try again.
- To use DRA to manage open files located on a dedicated file server running NetApp Filer, ensure you install DataOntap on the Administration server computer. For the most recent information about third party software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.

The following table describes the recommended hardware and software requirements for the Administration server computer.

Component	Requirement
CPU	Minimum: 1 GHz Intel Core processor Recommended: 2 GHz or faster Intel Core processor
RAM	Minimum: 4 GB Recommended: varies by environment The amount of memory recommended depends on the number of objects in the managed domain. On Windows Server 2003, enable the /3GB switch.
Disk Space	Minimum: 500 MB temporary disk space on C drive and 4 GB on drive where Installation folder resides Recommended: 10 GB or greater The amount of disk space required depends on the number of objects in the managed domain, the number of administrative actions performed in the environment, and the number of days to retain the data. For more information about estimating disk space requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.
Operating System	One of the following versions of Microsoft Windows: • Microsoft Windows Server 2003 Service pack 2 or greater • Microsoft Windows Server 2003 R2 Service pack 2 or greater • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2 The server also must be a member of a Microsoft Windows Server 2003, Microsoft Windows Server 2008, or Microsoft Windows Server 2008 R2 native domain. For more information about domain levels, see the Microsoft article available at http://support.microsoft.com/kb/322692. For the most recent information about software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.
DRA Reporting Server (optional Management reports)	SQL Server 2005, 2008, or 2008 R2 SQL Server Reporting Services Microsoft Internet Information Services (IIS) 6.0, 7.0, or 7.5

Component	Requirement
Enabled Support	DCOM Microsoft Windows and Microsoft Exchange in English or Japanese Microsoft Data Access Component (MDAC) 2.6, 2.7, or 2.8 on Windows Server 2003 computers Microsoft .NET Framework 3.5 Service Pack 1 Microsoft Message Queuing (MSMQ) Microsoft Core XML Services (MSXML) For Windows Server 2008, enable the following roles and features: **Roles** • ADLDS • AD DS (to raise domain functional level) • Web Server IIS • File Services **Features** • .NET Framework features • · Message queuing server and services • · Remote server admin tools • · AD LDS tools • · IIS tools • · .Net environment • · Configuration APIs
Web Component	Microsoft Internet Information Services 6.0, 7.0 or 7.5 Microsoft Internet Explorer 6.0, 7.0, 8.0, or 9.0 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 (needed only for Exchange Administrator)	Microsoft Exchange management tools that match the software version of your Microsoft Exchange Server for Exchange Server 2003 and Exchange Server 2007. To manage Exchange Server 2010 objects: • Windows Remote Management (WinRM) 2.0 • Windows PowerShell 2.0 For the most recent information about software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.

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 Service Pack 2
- Microsoft Exchange Server 2007 Service Pack 2
- Microsoft Exchange Server 2010 with Update Rollup 4

Client Requirements

The following table describes the recommended hardware and software requirements for computers running the DRA and ExA user interfaces. To deploy the Web Console, ensure your client computers are running Internet Explorer 6 or greater and have active scripting enabled. For the most recent information about third party software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra. For more information, see "Deploying the Web Console" on page 26.

Component	Requirement
CPU	1 GHz Intel Core processor
RAM	Minimum: 1 GB Recommended: 2 GB
Disk Space	500 MB temporary disk space on the C Drive and 2 GB on the drive where the Installation folder resides
Operating System	Ensure the client computer runs one of the following Microsoft Windows operating systems: • Microsoft Windows XP Service Pack 3 • Microsoft Microsoft Windows Server 2003 Service Pack 2 • Microsoft Windows Server 2003 R2 • Microsoft Windows Server 2003 R2 Service Pack 2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 R2 • Microsoft Windows Vista Service Pack 1 • Microsoft Windows 7 For the most recent information about software requirements, see the NetIQ Knowledge Base available at http://support.netiq.com/dra.
Enabled Support	Microsoft .NET Framework 3.5 Service Pack 1 (By default, the setup program installs.NET Framework version 3.5 Service Pack 1.) Active scripting enabled in Internet Explorer to run the setup program.

Permissions Requirements

Before you start installation, create an access account with the appropriate permissions for your environment. The Administration server uses this access account to log on to a Windows domain and process valid requests. The following sections identify access account permissions requirements. When you install the Administration server, you must specify the following user and group accounts:

Administration Server Service Account

Account the Administration server uses to access trusted domains and other Administration servers by default. You can configure the Administration server to use this account as the access account for your managed domain. This account must be part of an ActiveView with the View All Objects power.

ADAM Admin Account

Account the Administration server uses to access the ADAM instance. This account can be a user account or a group account. For best practices, this account should be a domain local security group. You need to consider the following requirements:

- On the primary Administration server, all Administration server service accounts in an MMS need to be members of the ADAM admin group account.
- For secondary Administration servers, either use the same ADAM admin account you used on the primary Administration server or create a new domain local security group in the domain of the secondary server. To use the same ADAM admin account for a secondary Administration server, the secondary Administration server must be a member of the same forest as the primary Administration server. If you create a new group, the secondary Administration server service account needs to be a member of the group.
- Before you promote a secondary Administration server to a primary Administration server, add all Administration server service accounts in the MMS to the ADAM Admin account.
- Each ADAM instance runs as an independent and separately administered service on the computer. During the DRA installation process, you need to provide an LDAP port number, a Secure Sockets Layer (SSL) port number, an ADAM instance name, and an Active Directory domain local security group to use as an ADAM admin account. When you install DRA on other servers in the same MMS, use the same ADAM admin account you used during the first installation.
- When you install the DRA server on a domain controller, the ADAM instance runs under the Network Service account. In this scenario, run ADAM under an Active Directory account that does not have administrative privileges. For more information about the best practices in such a scenario, see the Microsoft Technet article at http://technet2.microsoft.com/windowsserver/en/library/db9893df-3209-4b66-8a68-a17d9bbbd56d1033.mspx?mfr=true.
- If DRA is running in a Microsoft Windows 2000 Mixed Mode domain, the NetIQ Administration service cannot connect to the ADAM partition. To avoid this issue, promote the domain functional level to Microsoft Windows 2000 Native Mode or higher. Microsoft Windows 2000 Mixed Mode is a requirement only if you have pre-Windows 2000 domain controllers and DRA does not support pre-Windows 2000 domain controllers.

Access Account

Account the Administration server uses to access a specific managed domain or subtree. By default, this account also accesses file servers and Microsoft Exchange servers in the specified domain or subtree. This account is also called the **domain override account**.

You can specify a different access account for each managed or trusted domain, and each managed subtree. Using multiple access accounts to manage multiple domains or subtrees removes the concern that one account has enterprise-wide access. For more information about configuring access accounts for different environments, see "Managing Multiple Domains and Subtrees" on page 37.

Note

To ensure the Web Console initializes quickly, you should go to the `C:\windows\temp\Mission Critical Software` folder. On the File menu, click **Properties**. On the Security tab, grant Full Control permissions to Everyone.

Access Account and Service Account Permissions

By default, the Administration server uses the Administration server service account to access trusted domains and other Administration servers. If you choose to limit the access of the Administration server service account in a fully managed domain, consider the following requirements:

- The Administration server service account must be a local Windows administrator account. This account must have Administrator permissions on the domain controller. In addition, the service accounts need full administrator authority on all managed computers.
- The service account used in a managed domain must have administrator permissions, such as being a member of the local Administrators group, in the managed domain.
- With Windows 2000, a member of the Users group cannot enumerate account information. Therefore, you need to grant the service accounts created for the Administration server, managed domains, and managed computers the right to enumerate account information.

You can specify another access account. Ensure the account you specify meets the following permissions requirements on the Administration server computer:

- Backup and restore permissions
- Logon as a service user right
- Be part of an ActiveView with power to View All Objects

To access objects in trusted domains, ensure the specified account is a known account in each trusted domain. The domain of the Administration server computer should also trust the domains trusted by your managed domain. For more information about installing the Administration server with other configurations, see "Installing DRA in Complex Environments" on page 35.

The Administration server can also use this account to access managed domains and subtrees, Microsoft Exchange servers, and file servers. To access a domain, subtree, or Microsoft Exchange server, the Administration server requires additional permissions.

If you want to:	Also assign:
Access managed domains Support Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, or Microsoft Exchange Server 2010	For more information, see "Managed Domain Permissions" on page 15
Access managed subtrees Support Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, or Microsoft Exchange Server 2010	For more information, see "Managed Subtree Permissions" on page 15

Managed Domain Permissions

To administer accounts, resources, and Microsoft Exchange mailboxes in a managed domain, you must specify which account the Administration server should use to access the managed domain. You can specify either the Administration server service account or an access account (also called domain override account).

Notes

- If your Microsoft Exchange server uses the Recipient Update Service (RUS) to administer mailboxes for user accounts in another managed domain, install Microsoft Exchange tools on a domain controller in the managed domain. Through Microsoft Exchange server, assign Exchange Full Administrator permissions to the Administrator of that domain.
- You can use Exchange View Only Administrator permissions to enable Microsoft Exchange 2003 support for certain Microsoft Exchange environments. For more information, see Microsoft Knowledge Base Article 330475.
- To manage hidden groups, ensure the specified account is a member of the Account Operators group in all managed domains with Microsoft Exchange Server support. If the account is not an Account Operators group member, DRA cannot manage hidden groups and may return unexpected results. For example, to delegate administration through group memberships, ensure the specified account belongs to the Account Operators group in the managed domain.

The following table lists the permissions required for managed domains:

If you want to:	Assign:
Manage accounts and resources in a specific domain Manage accounts and resources on a specific workstation or server	Domain Admins permissions in the managed domain Administrator access to all objects on the managed computer Read access to all objects in trusted domains
Manage Microsoft Exchange mailboxes	Exchange Full Administrator permissions at the Administrative Group level or Organization level 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

Managed Subtree Permissions

To administer accounts, resources, and Microsoft Exchange mailboxes in a managed subtree, you must specify which account the Administration server should use to access the managed subtree. You can specify either the Administration server service account or the access account. By using access accounts, you can achieve the following flexibility:

- Fully manage one domain but manage only a subtree of another domain
- Manage multiple subtrees in multiple domains

- Manage a subtree without assigning administrative permissions for the entire domain

Notes

- If your Microsoft Exchange server uses the Recipient Update Service (RUS) to administer mailboxes for user accounts in another managed domain, install Microsoft Exchange tools on a domain controller in the managed domain. Through Microsoft Exchange server, assign Exchange Full Administrator permissions to the Administrator of that domain.
- To manage hidden groups, ensure the specified account is a member of the Account Operators group in all managed domains with Microsoft Exchange 2000 support. If the account is not an Account Operators group member, DRA cannot manage hidden groups and may return unexpected results. For example, to delegate administration through group memberships, ensure the specified account belongs to the Account Operators group in the domain of the managed subtree.

The following table lists the permissions required for managed subtrees.

If you want to:	Assign:
Manage accounts in a subtree of a Microsoft Windows domain	Full Control permissions for all objects in the managed subtree Read access to all objects in the domain of the managed subtree
Manage resources and home directories	Local administrator rights on the appropriate computers
Access objects in domains trusted by the domain of a managed subtree	Member of the Account Operators group in the trusted domain
Clone accounts	Write permissions to modify the primary group of the account you want to clone By default, user accounts have Domain Users set as their primary group. This primary group does not require additional write permissions
Manage Microsoft Exchange mailboxes	Exchange View Only Administrator permissions on the Microsoft Exchange server for the managed subtree. If you want to move mailboxes or modify mailbox rights, then the access account must also have Exchange Administrator permissions.

Reporting Account Requirements

The following table lists the Reporting Center account requirements.

Permissions	Requirement
Database installation	• System Administrator privileges on the SQL server where you install the Configuration Database. • Local administrative permissions on the computer where you run the Setup program.
Web Service installation	• System Administrator privileges on the SQL server where you install the Web Service. • Local administrative permissions on the computer where you run the Setup program.

Licensing Requirements

Your license determines the products and features you can use. DRA and ExA require a license key file. This file contains your license information and is installed with the Administration server. When you install the Administration server, use the customized license key file (`License1.lic`) you receive from NetIQ Corporation.

The license key file defines an expiration date, a grace number of user accounts, and the number of user accounts you can manage with DRA and ExA. When you start using the grace number of user accounts, the Administration server provides warning messages in the event log and through the user interfaces. If you exceed the number of licensed user accounts, DRA will no longer allow you to create user accounts. You can continue to perform other administrative tasks, such as modifying existing user accounts. If you exceed the expiration date, you may no longer be able to use the product. DRA also recognizes InetOrgPerson objects as normal users and includes the InetOrgPerson object types in the license count.

If you purchase additional licenses, you can add these new user licenses by running the NetIQ Administration Products installer. You can also add the new user licenses through the Installed Licenses window during the setup process. For more information, see "Upgrading Licenses" on page 33.

Warning

If you install a replacement license, DRA will remove all existing licenses and replace these with the replacement licenses. To view the current license, on the File menu, select **DRA Properties > License**.

Chapter 3
Installing or Upgrading the Product

This chapter guides you through installing or upgrading DRA and ExA. For more information, see "Installing DRA in Complex Environments" on page 35 or "Upgrading Large Environments" on page 45.

Installation Checklist

Use the following checklist to guide you through the installation process. You should install the Administration server on a Microsoft Windows server. You can deploy the appropriate user interfaces on the Administration server computer and on multiple client computers.

By default, the setup program installs the Web Component on the Administration server computer. For more information about other configurations, such as installing the Web component on a server other than the Administration server, see "Installing DRA in Complex Environments" on page 35.

Before you install DRA and ExA, be sure you understand how the Administration server works with these products. For more information about the Administration server and products, see "How DRA and ExA Work" on page 5.

	Checklist Items
☐	1. Ensure your server and client computers meet the product hardware and software requirements. For more information, see "Understanding Requirements" on page 9.
☐	2. Identify the domains or subtrees you want to manage. For more information, see "How DRA and ExA Work" on page 5.
☐	3. Identify the user account or group you want DRA to assign the built-in DRA Admin role. Ensure the user account or group you specify meets the following requirements: • Is a security group or user account. • Is a member of the managed domain, managed subtree, or a trusted domain. If you specify a local Administrator group, ensure the local computer is a managed object. If you specify an account from a trusted domain, ensure the Administration server computer can authenticate this account.
☐	4. Create the local domain admin group you want DRA to use as the ADAM admin account.
☐	5. Identify the user accounts you want DRA to use as access accounts for your managed domains, subtrees, and servers. Ensure these accounts meet the appropriate permissions requirements. For more information, see "Access Account and Service Account Permissions" on page 14.

	Checklist Items
☐	6. Install reporting components on a SQL Server computer to enable DRA Management reports. For more information, see “Installing and Upgrading DRA Reporting Components” on page 26.
☐	7. Install DRA and ExA. For more information, see “Installing or Upgrading the Administration Server” on page 22 and “Installing or Upgrading the User Interfaces” on page 23.
☐	8. Customize DRA and ExA to meet your specific needs. Customizations you can perform include the following tasks: • Delegate secure administration of accounts, resources, and mailboxes • Enforce corporate policy for consistent account management across domains and departments • Add other managed domains or subtrees as your administration needs change • Encrypt all communications between the Administration server and the user interfaces • Schedule cache refreshes for optimal frequencies and times • Schedule data collection to enable DRA Management reports For more information about customizing DRA and ExA, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator* or the Help for the product.
☐	9. Complete the following tasks: • Ensure the computer where the IIS Admin service runs has the Trusted for delegation flag set in the computer account properties. For more information, refer to the NetIQ Knowledge Base article NETIQKB14935, available at www.netiq.com/support/dra/knowledgebase.asp. • Ensure the IIS server running the Directory and Resource Administrator Web Component is configured as a local intranet site and not as a trusted site. For more information, see Installing the Web Component on a Dedicated Web Server. • Select the **Integrated Windows Authentication** check box on the Internet Options Advanced tab of Internet Explorer. For more information, refer to the NetIQ Knowledge Base article NETIQKB14935, available at www.netiq.com/support/dra/knowledgebase.asp. After installing DRA, you should configure DCOM settings on that computer. For more information, see Configuring DCOM Settings.

Upgrade Requirements

The following checklist guides you through the entire upgrade process. Use this process to upgrade each server set in your environment.

You can spread your upgrade process over several phases, upgrading one Multi-Master Set (MMS) at a time. The upgrade process allows you to temporarily include secondary servers running a previous DRA version and secondary servers running the current DRA version in the same MMS. DRA supports synchronization between Administration servers running a previous DRA version and servers running the current DRA version. However, be aware that DRA does not support running a previous DRA version with the current DRA version on the same Administration server or client computer.

Warning

Do not upgrade your secondary Administration servers until you upgrade the primary Administration server for that MMS.

	Checklist Items
☐	1. Perform a test upgrade in your lab environment to identify potential issues and minimize production down time.
☐	2. Determine the order in which you want to upgrade your server sets.
☐	3. Prepare each MMS for upgrade. For more information, see "Preparing to Upgrade" on page 22.
☐	4. Upgrade the primary Administration server in the appropriate MMS. For more information, see "Upgrading the Primary Administration Server" on page 49.
☐	5. To minimize down time at remote sites, install a local secondary Administration server running the current version of DRA. For more information, see "Installing a Local Secondary Administration Server for the Current DRA Version" on page 49. This step is optional.
☐	6. Upgrade the secondary Administration servers in the MMS. For more information, see "Deploying the DRA User Interfaces" on page 50.
☐	7. Deploy the DRA user interfaces to your Assistant Admins (AAs).

Preparing to Upgrade

Prepare each server set for upgrade by completing the following steps:

	Checklist Items
☐	1. Make a deployment plan for upgrading the Administration servers and user interfaces (AA client computers). Redirect older DRA user interfaces to the same version Administration server to maintain workflow during the upgrade process.
☐	2. Dedicate a secondary Administration server to run the current version of DRA as you upgrade a site. This step is optional.
☐	3. Make any necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings.
☐	4. Synchronize the MMS.
☐	5. Back up the registry from the primary Administration server.
☐	6. Upgrade the primary Administrator server first, then the secondary servers immediately afterwards.

Note:
After you upgrade, do not perform an MMS synchronization immediately after you complete the upgrade.

Installing or Upgrading the Administration Server

You can install the Administration server on a Microsoft Windows server or domain controller. You can also install more than one Administration server. The requirements for primary and secondary Administration servers are the same. If you install a single Administration server, that server must be a primary Administration server.

By default, the setup program installs the ActiveEngine component and Web component on the Administration server computer. You can install the Web component on any Web server in a managed or trusted domain. When you install the Web component, you also enable Web Console functionality by installing the Web Console virtual directory.

Note
For more information about installing multiple Administration servers or installing the Web component on a different Web server, see "Installing DRA in Complex Environments" on page 35.

To install or upgrade the Administration server:

1. Log on the Microsoft Windows server or domain controller with an administrator account.

   Ensure this account also meets the following requirements:

   - Is a User in the domain of the Administration server service account.

- Has full permissions to the `Inetpub\wwwroot` folder on the computer where you plan to install the Web component. By default, the setup program installs the Web component on the Administration server computer.

2. Run `Setup.exe` in the root folder of the installation kit.

Note
To install the Administration server through a Windows Terminal Services session, run the setup program through the Add/Remove Programs application in Control Panel.

3. Click the Production Setup tab.
4. Click **Begin Production Setup**.
5. Select the appropriate installation option, and then click **Next**.
   - To install the Administration server with the user interfaces, select **Full**.
   - To install the Administration server without the user interfaces, select **Server only**.
   - To install the Administration server without the Web component, select **Custom**.
6. Select the product you want to install, and then click **Next**.
7. Follow the instructions until you have finished installing the Administration server, and then click **Finish**.
8. ***If you chose to install the Reporting components,*** the NetIQ Reporting Center setup program begins. For more information, see "Installing and Upgrading DRA Reporting Components" on page 26.

Installing or Upgrading the User Interfaces

You can install or upgrade the following user interfaces on any Administration server or client computer:

Product	Supported User Interfaces
DRA and ExA	Account and Resource Management Console Delegation and Configuration Console Reporting Center Console Command-line Interface (CLI) ADSI Provider

Through the flexible user interfaces install option, you can install the user interfaces separately. This option lets you tailor your deployment to your specific administration needs.

Notes
- You can use group policy to easily install or upgrade user interfaces on multiple client computers across your enterprise. For more information, see "Deploying User Interfaces through Group Policy" on page 24.
- Directory and Resource Reporting has been replaced with DRA Reporting, which uses the NetIQ Reporting Center product to display DRA Management Reports. For more information about installing Reporting Center, see "Installing and Upgrading DRA Reporting Components" on page 26.

Deploying User Interfaces through the Setup Program

You can deploy the user interfaces for DRA and ExA through the setup program. Use the setup program to install or upgrade the user interfaces on one or more client computers.

To deploy user interfaces through the setup program:

1. Log on with an administrator account to the client computer. For more information, see "Client Requirements" on page 12.
2. Run `Setup.exe` in the root folder of the installation kit.

   Notes

   - You can also run `SetupClients.exe` to install the user interfaces.
   - To install the Administration server through a Windows Terminal Services session, run the setup program through the Add/Remove Programs application in Control Panel.

3. Click the Production Setup tab.
4. Click **Begin Production Setup**.
5. Select **User interfaces**, and then click **Next**.
6. Select the specific DRA or ExA user interface you want to install, and then click **Next**.
7. Follow the instructions until you have finished installing the user interfaces, and then click **Finish**.
8. ***If you chose to install the Reporting components,*** the NetIQ Reporting Center setup program begins. For more information, see "Installing and Upgrading DRA Reporting Components" on page 26.

Deploying User Interfaces through Group Policy

You can deploy the user interfaces for DRA and ExA by distributing the appropriate files through group policy. This flexibility lets you easily install or upgrade user interfaces on multiple client computers across your enterprise. Group policy ensures the appropriate personnel can install these user interfaces.

You can run `NetIQAdmin.msi` from the Intel folder of the installation kit. The `NetIQAdmin.msi` file installs most DRA and ExA components, including the Administration server, user interfaces, documentation, and utilities. It does not install the optional DRA Reporting components. However, you can configure a group policy object to install specific user interfaces by specifying one of the following `.mst` or `.msi` files:

NetIQDRAAdminConsole.mst	Installs the Delegation and Configuration console
NetIQDRAUserConsole.mst	Installs the Account and Resource Management console
DRAReporting.msi	Installs the Reporting Center interface for DRA Reporting
NetIQDRACLI.mst	Installs the command-line interface
NetIQDRAADSI.mst	Installs the DRA ADSI provider
NetIQDRABase.mst	Installs documentation and utilities
NetIQDRAClients.mst	Installs all DRA and ExA user interfaces
netiqreportingcentersetup_x32.exe	Installs Reporting Center components on 32-bit operating systems
netiqreportingcentersetup_x64.exe	Installs Reporting Center components on 64-bit operating systems

Notes

- If you use a group policy to deploy these user interfaces to client computers running Microsoft Windows XP, the client computers may require two logons to apply the upgrade. For more information, see Microsoft Knowledge Base Article Q305293.
- For more information about giving user accounts special permissions or enabling group policy settings, see the Microsoft Knowledge Base Article Q259377.
- For more information about group policy, see the Microsoft Windows Help. To easily and securely test and deploy group policy across your enterprise, use NetIQ Group Policy Administrator.

To deploy user interfaces through group policy:

1. To upgrade the user interfaces, start Active Directory Users and Computers and edit the existing group policy object.
2. To install the user interfaces, start Active Directory Users and Computers and create a new group policy object.
3. Add the `NetIQAdmin.msi` package to this group policy object.
4. Ensure this group policy object has one of the following properties:
   - Each user account in the group has at least Power User permissions for the appropriate computer.
   - The **Always Install with Elevated Privileges** policy setting is enabled.
5. Add the following files to this group policy object:
   - The `NetIQDRABase.mst` file
   - The user interface `.mst` file, such as `NetIQDRAUserConsole.mst`
6. Distribute your group policy.

Deploying the Web Console

You can run the Web Console from any computer with Internet Explorer 6 or Internet Explorer 7, the link provided in the Account and Resource Management console, or from the Start menu. You do not need to install additional software. The setup program automatically backs up the previous version of Web Console files to the `DRAWebConsole\VersionUpgradeBackups` folder under Program Files. This task describes how to deploy the Web Console.

To deploy the Web Console:

1. Install the Web component.

   By default, the setup program installs the Web component on the Administration server computer. You can install the Web component on any Web server computer running IIS that supports ASP. For more information, see "Installing the Web Component on a Dedicated Web Server" on page 40.

2. Ensure the appropriate client computers support Internet access and your IIS security settings. Ensure active scripting is enabled in the client browser.

3. Set the client browser to check for newer versions of cached pages so the Web Console displays the most current account and Exchange information.

4. Distribute the appropriate URL. For example, if you installed the Web component on the `HOUserver` computer, distribute the following URL: `http://HOUserver/dra`.

Installing and Upgrading DRA Reporting Components

The following sections list considerations to help you plan your installation.

The Order of Your Installation

You can install the Reporting Center components individually or in any combination. If you install the components on separate computers, install the components in the following order:

1. Configuration Database
2. Web Service
3. Reporting Services Data Extension
4. Console

Configuration Database Considerations

Before you install the Configuration Database, consider the following information:

- After installing Reporting Center, if you run the setup program to modify your installation, there is no option to install the Configuration Database. This is a safeguard that prevents you from having multiple Configuration Databases installed in a single Reporting Center environment.
- After installing Reporting Center, set up regular SQL server backups for the Configuration Database.
- When you uninstall Reporting Center, the setup program removes all components except the Configuration Database.

Web Service Considerations

If you install the Web Service on a non-default Web site, do not customize the corresponding Host Header value. For information about removing the Host Header, see the Troubleshooting chapter in the *Reporting Center Reporting Guide*.

Reporting Services Data Extension Considerations

Before you install the Reporting Services Data Extension, consider the following information:

- You usually install the Reporting Services Data Extension on the computer hosting SSRS, your report server. However, if you are planning on using the Report Designer component of SSRS to customize reports, install the Reporting Services Data Extension on the computer hosting Report Designer.
- If you configured SSRS with SSL, during installation you can specify the URL for the SSL-configured report server. You can also change the default SSRS URL after installation in the Console. Go to **Tools > Options > Enterprise Options > Reporting Services > Default Report Server Location**, and enter the URL for the SSL-configured report server.

Console Considerations

Because the Web Service is the communication layer between the Console and the database, install the Web Service before installing the Console.

Installing Reporting Center on Windows Server 2008

Install IIS on Windows Server 2008 (IIS 7.0) or Windows Server 2008 R2 (IIS 7.5) with the following Role Services selected:

- Application Development: ASP.NET
- Security: Windows Authentication

Installing DRA Reporting

When you install DRA Reporting components, you install Reporting Center along with the DRA Management reports that ship with DRA. You can install the Reporting components on a primary or secondary Administration server.

The following table lists the prerequisites you need to install each component of Reporting Center. .

Component	Installation Prerequisites
Configuration Database	• Credentials for the Database Installer Account. • The name of the SQL Server instance where you will install the Configuration Database, in this format: *`ServerName\Instance`*
Web Service	• Credentials for the Web Service Installer Account. • The location of the Configuration Database, in this format: *`ServerName\Instance`* • Credentials for the Web Service User Account.

Component	Installation Prerequisites
Console	• The location of the Configuration Database, in this format: *`ServerName\Instance`* • The name of the Web Service server, in this format: `http://` *`ServerName`*`/ACWebService`
Reporting Services Data Extension	• The location of SQL Server Reporting Services (SSRS), in this format: *`ServerName\Instance`*

To install DRA Reporting:

1. Log on the Microsoft Windows server or domain controller with an administrator account.

   Ensure this account also meets the reporting requirements. For more information, see "Reporting Account Requirements" on page 16.

2. Run `Setup.exe` in the root folder of the installation kit.

   Note
   To install the Administration server through a Windows Terminal Services session, run the setup program through the Add/Remove Programs application in Control Panel.

3. Click the Production Setup tab.
4. Click **Begin Reporting Setup**.
5. Follow the instructions until you have supplied all the necessary information about your reporting server.
6. When the DRA Reporting installation completes, click **Finish** to begin the NetIQ Reporting Center installation.
7. On the Component Selection dialog, select **Configuration Database**, **Web Service**, and **Console**, and click **Next**.
8. Follow the instructions until the installation completes, and click **Finish**.

You can also install the Reporting Center console on other computers.

To install Reporting Center console:

1. Log on the Microsoft Windows server with an administrator account.

   Ensure this account also meets the reporting requirements. For more information, see "Reporting Account Requirements" on page 16.

2. ***If you are installing the console on a 32-bit operating system***, run `netiqreportingcentersetup_x86.exe` in the Intel folder of the installation kit.
3. ***If you are installing the console on a 64-bit operating system,*** run `netiqreportingcentersetup_x64.exe` in the Intel folder of the installation kit.
4. On the Component Selection dialog, select the appropriate component and click **Next**.
5. Follow the instructions until the installation completes, and click **Finish**.

After installing DRA Reporting, you must enable and configure reporting in DRA. For more information, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Upgrading DRA Reporting

When you upgrade to Reporting Center 1.5, you can use SQL Server 2008 or 2008 R2 to produce DRA Management Reports.

Before upgrading to SQL Server 2008, you should uninstall the previous version of the Reporting Center Data Extension component so that it will work correctly after you upgrade to Reporting Center 1.5.

If you already upgraded to SQL Server 2008, and then upgraded to Reporting Center 1.5, the Reporting Center setup program displays an error at the end of installation and will not install the Data Extension component. Acknowledge the error message by clicking **OK**, and click **Finish** to complete the installation of the other components. Then use the following instructions to uninstall and reinstall the Data Extension component.

Uninstalling and reinstalling the Data Extension component does not affect deployed reports.

To uninstall and reinstall the Data Extension component on SQL Server 2008:

1. From the Control Panel, click **Add or Remove Programs** or **Programs and Features**, according to your operating system.
2. Click **Reporting Center** and click **Change/Remove**.
3. In the Welcome box, click **Modify** and then click **Next**.
4. In the Feature Selection box, clear the Data Extension check box and click **Next**.
5. In the Requirement check box, click **Next**, and in the Installation Summary box, click **Install** to uninstall the Data Extension component.
6. Click **Finish** when prompted.
7. To reinstall the Data Extension component, repeat steps 1 through 3 and select **Data Extension**.
8. In the Data Extension Step 1 box, enter the local reporting server.
9. Follow the prompts and click **Install** to begin reinstalling the Data Extension component. Click **Finish** when prompted.

If you are moving your Configuration Database to a different server or database instance, follow these steps:

1. Back up the Configuration Database.
2. Restore the backup to the new server or instance.
3. Modify the Web Service connection information using one of these methods:
   - If the Web Service uses SQL authentication to connect with the Configuration Database, uninstall the Web Service component, and then install the Web Service component using the new SQL Server instance details.
   - If the Web Service uses Windows authentication to connect with the Configuration Database, edit the `Web.config` file in the Web Service installation folder, typically `C:\Program files\NetIQ\Reporting Center\Webservice`, and change the server name value in the Connection tag to the new Configuration Database SQL Server instance name.

Adding Managed Domains through the Setup Program

You can add managed domains, servers, or workstations after you install the Administration server. If you did not specify all the domains and computers you want the server to manage during the initial installation, you can run setup again to add any missing domains, servers, or workstations. To add managed domains and computers after you install the Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

Notes

- After you finish adding managed domains, ensure that the accounts cache refresh schedules for these domains are correct. For more information about modifying the accounts cache refresh schedule, see the Help.
- You must stop and restart the NetIQ Administration service for your changes to take effect.

To add managed domains and computers through the setup program:

1. From the Start menu on the primary Administration server computer, run Add/Remove Programs.
2. Select **NetIQ Administration Products**, and then click **Change/Remove**.
3. Click **Advanced Configuration**.
4. Select **Add or remove managed domains**, and then click **Next**.
5. Click **Select**.
6. For each managed domain or computer you want to add, complete the following steps:
   a. Click **Add**.
   b. Specify the domain or computer you want to manage. To specify a server or workstation, type the name of the computer in the following format: `\\computername`.
   c. In the **Access account** field, specify the service account you want DRA to use to access this domain. By default, DRA uses the Administration server service account.
   d. Click **OK**.
7. Verify the list of managed domains or computers, and then click **OK**.
8. Click **Next**.
9. Click **Yes** to restart the NetIQ Administration service, and then click **Next**.
10. Click **Next**.
11. Click **Finish**.

Adding Managed Subtrees through the Setup Program

You can add managed subtrees from specific Microsoft Windows domains after you install the Administration server. You can add any missing subtrees you want to manage through the setup program. To add managed subtrees after you install the Administration server, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role. To ensure the specified access account has permissions to manage this subtree and perform incremental accounts cache refreshes, use the Deleted Objects utility to verify and delegate the appropriate permissions. For more information about using this utility, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*. For more information about setting up the access account, see "Permissions Requirements" on page 12.

Notes

- You must stop and restart the NetIQ Administration service for your changes to take effect.
- After you finish adding managed subtrees, ensure that the accounts cache refresh schedules for the corresponding domains are correct. For more information about modifying the accounts cache refresh schedule, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

To add managed subtrees through the setup program:

1. From the Start menu on the primary Administration server computer, run Add/Remove Programs.
2. Select **NetIQ Administration Products**, and then click **Change/Remove**.
3. Click **Advanced Configuration**.
4. Select **Add or remove managed domains**, and then click **Next**.
5. Click **Select**.
6. Click **Add**.
7. Specify the domain of the subtree you want to manage.
8. Under **Managed subtrees**, select **Manage a subtree of this domain**.
9. For each managed subtree you want to add, complete the following steps:
    a. Click **Add**.
    b. Select the OU of the subtree you want to manage.
    c. Click **OK**.
10. Under **Access account**, specify the account you want DRA to use to access this domain. By default, DRA uses the Administration server service account.
11. Click **OK**.
12. Verify the list of managed domains or computers, and then click **OK**.
13. Click **Next**.
14. Click **Yes** to restart the NetIQ Administration service, and then click **Next**.
15. Click **Next**.
16. Click **Finish**.

Configuring DCOM Settings

Configure DCOM settings on the domain controllers where you have installed a DRA agent and on the primary Administration server if you did not allow the setup program to configure DCOM for you.

Configuring the Distributed COM Users Group

After installing DRA, you should update the membership of the Distributed COM Users group to include all user accounts that use DRA. This membership should include the DRA Service Account and all Assistant Admins.

To configure the Distributed COM Users group:

1. Log on to a DRA client computer as a DRA administrator.
2. Start the Delegation and Configuration console. If the console does not automatically connect to the Administration server, manually establish the connection.

   Note
   You may not be able to connect to the Administration server if the Distributed COM Users group does not contain any Assistant Admin accounts. If this is the case, configure the Distributed COM Users group using the Active Directory Users and Computers snap-in. For more information about using the Active Directory Users and Computers snap-in, see the Microsoft Web site.

3. In the left pane, expand **Account and Resource Management**.
4. Expand **All My Managed Objects**.
5. Expand the domain node for each domain where you have a domain controller.
6. Click the **Builtin** container.
7. Search for the Distributed COM Users group.
8. In the search results list, click the **Distributed COM Users** group.
9. Click **Members** in the lower pane, then click **Add Members**.
10. Add users and groups that will use DRA. Ensure you add the DRA service account to this group.
11. Click **OK**.

Configuring the Domain Controller and Administration Server

After configuring the client computer running the Delegation and Configuration console, you should configure each domain controller and each Administration server.

To configure the domain controller and Administration server:

1. On the Start menu, click **Settings > Control Panel**.
2. Open Administrative Tools, then open Component Services.
3. Expand **Component Services > Computers > My Computer > DCOM Config**.
4. Select **OnePointAgent** on the domain controller or **MCS OnePoint Administration Service** on the Administration Server.
5. On the Action menu, click **Properties**.

6. On the General tab in the Authentication Level area, select **Packet**.
7. On the Security tab in the Access Permissions area, select **Customize**, and then click **Edit**.
8. Ensure the Distributed COM Users group is available. If it is not available, add it. If the Everyone group is available, remove it.
9. Ensure the Distributed COM Users group has Local and Remote Access permissions.
10. On the Security tab in the Launch and Activation Permissions area, select **Customize**, and then click **Edit**.
11. Ensure the Distributed COM Users group is available. If it is not available, add it. If the Everyone group is available, remove it.
12. Ensure the Distributed COM Users group has the following permissions:
    - Local Launch
    - Remote Launch
    - Local Activation
    - Remote Activation
13. Apply the changes.

Upgrading Licenses

DRA and ExA require a license key file. This file contains your license information and is installed on the Administration server. When you install the Administration server, the setup program prompts for a customized license key file (`License1.lic`) provided for you by NetIQ Corporation. When you upgrade your license, upgrade the license file on each Administration server.

You can also view your product license through either the Delegation and Configuration console or the Account and Resource Management console. To view your product license, click **DRA Properties** on the File menu.

To upgrade your license:

1. On the Administration server, run Add/Remove Programs in the Control Panel.
2. Select **NetIQ Administration Products (DRA/ExA)**.
3. Click **Change/Remove**.
4. Click **Advanced Configuration** on the Add/Remove Application window.
5. Select **Upgrade license**, and then click **Next**.
6. Specify the path of the new license key file.
7. Review the terms of the License Agreement. If you agree to the terms of the License Agreement, click **Accept**.
8. Compare the terms of your new license with those of your current license.
    - To use your new license, click **Next**.
    - To continue using your old license, click **Cancel**.
9. Click **Yes** on the Service Stop window to stop and restart the server, and then click **Next**.

10. Review the information on the Start Installation window, and then click **Next**.
11. Click **Finish** on the Installation Summary window.

Uninstalling the Administration Server and User Interfaces

You can easily uninstall the Administration server and the user interfaces from your computer.

To uninstall the Administration server and user interfaces:

1. On the Administration server, run Add/Remove Programs in the Control Panel.
2. Select **NetIQ Administration Products**, and then click **Change/Remove**.
3. Click **Continue**.
4. Click **Remove All** on the Add/Remove Application window.
5. Click **Yes** on the Remove Registry Entries window, and then click **Next**.
6. Follow the instructions until you have finished uninstalling the Administration server and the related products, and then click **Finish**.

Chapter 4
Installing DRA in Complex Environments

This chapter provides guidelines and best practices for installing and configuring Directory and Resource Administrator (DRA) in unique environments. This chapter also provides references to additional resources, such as specific NetIQ Knowledge Base articles.

Installing Multiple Administration Servers

A Multi-Master Set (MMS) contains a primary Administration server and one or more secondary Administration servers. You can install different server sets at different network sites, depending on your administration needs. For more information about basic Administration server requirements, see "Administration Server Requirements" on page 9. For more information about the benefits of an MMS and how an MMS works, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

If you install the primary Administration server on a domain controller, you may experience decreased performance on that server. To better balance network loads, install your Administration servers on server computers. Also ensure each Administration server is located in the same network site as the domain controller of the managed domain. By default, the Administration server accesses the closest domain controller for all read and write operations. When performing time-sensitive or site-specific tasks, such as password resets, you can specify a target domain controller. You can also configure the Administration server to send all write operations to a single domain controller. For more information, see "Configuring the Administration Server to Write All Changes to a Specific Domain Controller" on page 37.

When managing a larger enterprise, consider dedicating a secondary Administration server for your reporting, CLI or batch processing, or DRA ADSI scripting needs. In this configuration, Assistant Admins can easily connect to other secondary Administration servers to perform their daily tasks.

Notes

- If you install the Administration server on a computer that is not connected to the network, you must run `DCPROMO.exe` and make the computer a domain controller. You must also install the Microsoft Loopback Adapter. The Network Path Not Found Error 53 message can indicate the Loopback Adapter is not correctly installed.
- If you plan to install multiple Administration servers, start the Remote Registry Service on each Administration server computer.

Implementing Centralized Administration

Centralized administration involves one or more Administration servers at a central location managing domains or OUs that contain objects at other locations. When considering a centralized administration model, ensure you install enough secondary Administration servers to provide adequate load balancing. If a large number of AAs will be connecting to a single Administration server, consider adding a secondary server to help balance this load.

The centralized administration model can cause performance or connection issues if your client computers must connect over a slow WAN link. In this case, consider installing additional secondary Administration servers at remote sites that require more reliable connections.

Implementing Distributed Administration

Distributed administration is one or more secondary Administration servers at each site or location, with a primary Administration server at a central location. Consider installing the primary Administration server at the site where the majority of administrators who create and maintain your security definitions are located.

Be aware that DRA does not synchronize security definitions and configuration settings from one primary Administration server to another primary Administration server. That is, you cannot synchronize your security model across server sets. To move your security model from one primary server to another, back up the registry files from the source Administration server and copy that registry on to the target Administration servers. By default, the Administration server stores security data under the `HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\OnePoint\Administration\Data\Modules\Security` registry key. For more information about how synchronization works, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Planning Administration Servers for Your Environment

Depending on the size of your environment, you may need to consider additional Administration server requirements. The following sections discuss these requirements.

Administration Server Location

When managing a Microsoft Windows domain, or a subtree of that domain, you can install the Administration server on a computer in the managed domain or in a different domain. However, some restrictions, such as available bandwidth, do apply.

When deciding on the Administration server location, consider the following restrictions:

- DRA does not require a direct trust between the domain of the Administration server and the managed domain. However, to include a user account in an Assistant Admin (AA) group, the selected account should exist in a domain trusted by the domain of the primary Administration server. Likewise, to ensure client computers in the managed domain can access an Administration server, the server must be a member of a domain that trusts the managed domain.

If the trust relationships between managed domains breaks, DRA discovers and identifies the broken trusts during the domain configuration refresh. You can schedule domain configuration refreshes to run on a routine basis, or you can perform an immediate domain configuration refresh to troubleshoot or resolve a current issue. You can also view the status of a managed domain through the Delegation and Configuration console. For more information, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

- In a Microsoft Windows environment, a reliable connection must exist between the Administration server and a domain controller for each managed domain. If these connections are lost, the Administration server cannot update objects or provide complete reporting. Bandwidth restrictions, such as the Remote Access Service (RAS), between the Administration server and the managed domains can cause the Administration server to require more time to start and to perform some operations.

Configuring the Administration Server to Write All Changes to a Specific Domain Controller

You can configure the Administration server to read information from and write changes to a specific domain controller.

To specify the domain controller:

1. Start the Delegation and Configuration console.
2. In the left pane, expand **Configuration Management**.
3. Click **Managed Domains**.
4. In the list pane, select the domain.
5. On the Tasks menu, click **Properties**.
6. On the General tab, click the **Browse** button next to the **Connect to domain controller** field.
7. Select the preferred domain controller from the list, and then click **OK**.
8. Click **Yes** when the warning message displays so that DRA initiates a full accounts cache refresh.

Managing Multiple Domains and Subtrees

When you manage multiple domains and subtrees, you can configure DRA to use different accounts to access and manage these domains and subtrees. By default, DRA uses the Administration server service account to access managed domains and subtrees. However, specifying access accounts allows you to better control security across your enterprise. Using multiple access accounts to manage multiple domains or subtrees, servers, and workstations removes the concern that one account has enterprise-wide privileges. For more information about access accounts, such as permissions requirements, see "Access Account and Service Account Permissions" on page 14.

Note
The Administration server stores access account information locally. If you change the name or password of an access account, you must also update the account specifications through the Delegation and Configuration console on each Administration server.

Access Accounts and Multiple Managed Domains

You can specify one or more access accounts to manage multiple domains. If you plan to use access accounts to manage multiple domains, consider the following guidelines:

- Configure and specify one access account for each managed domain.
- Do not use pass-through authentication when managing multiple domains in a native environment.

Access Accounts and Multiple Managed Subtrees

You can specify one or more access accounts to manage multiple subtrees. If you plan to manage multiple subtrees of the same domain, you can use the same access account to manage each subtree. However, if you are managing multiple subtrees from different domains, configure and specify one access account for each subtree.

To retrieve group and user account information from trusted domains, ensure the access account is a member of the Domain Users group in all trusted domains.

Access Accounts and Managed Computers

When specifying access accounts to manage specific member servers or workstations, consider the following guidelines:

- To manage servers or workstations that are members of a managed domain, the access account must be a domain account. The access account cannot be a local server or workstation account.
- To manage resources on a local computer, ensure the access account is a domain account from the managed domain.

Access Accounts from Trusted Domains

You can use an account from a trusted domain like the access account for a managed Microsoft Windows domain. This account requires the same permissions as an account from the managed domain.

Access Accounts and Active Directory Replication

Whether you install the Administration server on a server or domain controller, the access account definition must be replicated to all domain controllers before you can use the account to access another Administration server or a managed domain. You should force Active Directory replication in Microsoft Windows environments.

The Administration server updates information only on the domain controller in the managed domain. Therefore, if you want to access user accounts from trusted domains to manage group memberships, the access account must be a User (not a Guest) in each domain trusted by the managed domain.

Deciding When to Add Managed Domains and Subtrees

Depending on how many domains or subtrees you plan to manage, consider adding these domains and subtrees through the Delegation and Configuration console, instead of the DRA setup program, to minimize down time. The more domains and subtrees you manage, the longer the Administration server takes to initialize. The Administration server remains unavailable during initialization. For more information about adding managed domains and subtrees, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator.*

How DRA Uses Access Accounts in Different Environments

If your environment contains several domains, subtrees, servers and workstations, DRA supports multiple access account scenarios. Consider the following example environment:

- `NewYork` and `Houston` domains
- `Sales` subtree in `Houston` domain
- `SmithJ` server
- `ChildsJ` workstation

The following table illustrates how DRA uses the specified access account or default Administration server service account, depending on how you manage this environment:

If you specify these accounts...	And you manage...	DRA uses the following accounts...
Administration server service account	Any domain, server, or workstation	Administration server service account
Administration server service account	Any subtree of a Microsoft Windows 2000 domain	Administration server service account
Administration server service account Access account for the `Houston` domain	`NewYork` domain	Administration server service account
	`Houston` domain	Access account specified for the `Houston` domain
Administration server service account Access account for the `Houston` domain	`NewYork` domain	Administration server service account
	`Sales` subtree of the `Houston` domain	Access account specified for the `Houston` domain
Administration server service account Access account for the `Houston` domain	`NewYork` domain	Administration server service account
	`Sales` subtree of the `Houston` domain	Access account specified for the `Houston` domain
	server or workstation in the `Houston` domain	Access account specified for the `Houston` domain
Administration server service account Access account of the `Houston` domain Access account for the `SmithJ` workstation	`NewYork` domain	Administration server service account
	`Sales` subtree of the `Houston` domain	Access account specified for the `Houston` domain
	server `SmithJ`	Access account specified for this workstation
Administration server service account Access account for the `ChildJ` workstation	Any domain	Administration server service account
	Workstation `ChildsJ`	Access account specified for this workstation

Upgrading Multiple Secondary Servers

The sequence in which you upgrade DRA on multiple Administration servers is important. For example, if you deploy user interfaces before you upgrade the Administration server, the client computers may not be able to connect to that Administration server, and you may receive incorrect diagnostic data. To prevent compatibility issues, upgrade DRA components in the following order without interruption:

1. Primary Administration server
2. Secondary Administration servers, if any
3. Web component, if on a server other than your primary Administration server

Be aware that you should not synchronize secondary Administration servers until you upgrade all secondary servers to the same version of DRA running on the primary Administration server. However, you can update user interfaces on client computers any time after you finish upgrading the Administration servers and Web server (if any). For more information on installing the Web component, see "Deploying the Web Console" on page 26.

Caution

For more information about upgrading Multi-Master Sets, see "Upgrading Large Environments" on page 45. This chapter includes important upgrade steps and best-practice guidelines.

Installing the Web Component on a Dedicated Web Server

You can install the Web component on a dedicated Web server (IIS server) rather than the Administration server computer. This installation works best in a native mode environment that uses Kerberos-only authentication. The IIS server computer and the Administration server computer must belong to the same domain. For more information about Web component requirements, see "Deploying the Web Console" on page 26. For more information about configuring Kerberos authentication, see NETIQKB14935 and "Installing the Web Component on a Server not Running the Administration Server" on page 41.

If you install the Administration server and IIS server on separate computers, you should ensure the DRA ADSI provider on the IIS server uses Kerberos as the default authentication protocol. For more information about changing the default authentication protocol to Kerberos, see NETIQKB48582.

You should also check whether the NTFS permissions for the Local System account has been modified on the IIS server or the Administration server. For more information about checking NTFS permissions, see NETIQKB33414.

If you plan to manage a Microsoft Windows domain and you want to install the Administration server and Web component on different computers, ensure each domain controller in this managed domain is running the same version of the operating system as your Web server.

If you install the Web Component on a computer other than the Administration server, and you want to deploy the Web Console with Internet Explorer 6 or Internet Explorer 7, set your browser security to support integrated Windows authentication. To set your browser security, select **Enable Integrated Windows Authentication** under **Security** on the Advanced tab of the Internet Options window. You can access Internet Options through the Tools menu.

If you select the **Use fully qualified domain names (FQDN)** option to specify the location of your Web server, DRA forces AAs to log in every time they access a property page. AAs can configure DRA to remember their logon name and password.

Configure the IIS server as a Local Intranet Site. To set your browser security, access the Security tab through Internet Options on the Tools menu. Under the Security tab, select **Local intranet** and click **Sites**. Type `http://IIS_server_name` in the **Add this Web site to the zone:** field.

If the DRA client is running on Microsoft Windows XP or Microsoft Windows Vista, select the **Trust computer for delegation** check box on the Microsoft Windows XP or Microsoft Windows Vista computer that is in the Active Directory domain. If you have installed Enhanced Internet Explorer Security settings on this computer, remove these settings. If you do not want to remove these settings, access the Security tab through Internet Options on the Tools menu. Under the Security tab, click **Custom Level** and enable ActiveX controls and plug-ins.

To install the Web component on a Web server:

1. Use the DRA setup program to custom install the Web component on the Web server computer.
2. Configure your IIS security settings to use basic authentication.
3. Set the IIS server computer as trusted for delegation.
4. Configure the appropriate Internet Explore security settings and resolve any IIS issues, such as failed authentication. For more information, see NetIQ Knowledge Base Article NETIQKB14935.
5. Deploy the Web Console. For more information, see "Deploying the Web Console" on page 26.

Installing the Web Component on a Server not Running the Administration Server

You can install the Web component on a server that is not running the Administration server component.

To install the Web component on a server not running the Administration server:

1. Run `Setup.exe` on the IIS server.
2. Click the Production Setup tab.
3. Click **Begin Production Setup**.
4. Select **Custom**, and click **Next**.
5. Select **Web Component**, and click **Next**.
6. Add the correct license information, and click **Next**.
7. Type the name of the server running the NetIQ Administration Service, and then click **OK**.

Deploying Multiple Web Console Applications

You can install more than one Web Console application on your Administration server or Web server computer. This flexibility allows you to deploy different, custom Web Consoles for each site or AA group. To install more than one Web Console application, set up a new virtual directory for each Web Console application you want to deploy.

Creating a Virtual Directory for the Web Console

For each Web Console application you want to deploy, create a virtual directory that references the correct files.

To create a virtual directory:

1. Log on with an administrator account to the computer where you want to install the virtual directory.
2. On the Start menu, click **Programs > Administrative Tools**.
3. Click **Internet Services Manager**.
4. Expand the server node.
5. Select **Default Web Site**.
6. On the Action menu, click **New > Virtual Directory**.
7. Follow the instructions until you have finished creating the virtual directory. Ensure you specify the following settings:
   a. Specify the path of the Web Console files in the **Directory** field on the Web Site Content Directory window. By default, the Web Console files are located under `C:\Inetpub\wwwroot\DRAWeb\WebConsole`.
   b. Select **Read** and **Run scripts** on the Access Permissions window.
8. Click **Finish**.

Configuring the Web Console Virtual Directory

For each Web Console application you want to deploy, ensure the virtual directory has the appropriate settings.

To configure a virtual directory:

1. In the left pane of the Internet Services Manager window, select the new virtual directory.
2. On the Action menu, click **Properties**.
3. On the Virtual Directory tab, click **Configuration**.
4. On the App Options tab, verify the following settings, and then click **OK**.
   - Select **Enable session state**.
   - Select **Enable buffering**.
   - Select **Enable parent paths**.
   - Type `VBScript` for the **Default ASP language**.
5. On the Documents tab, ensure `Default.asp` is one of the listed default documents.
6. On the Directory Security tab, click **Edit** under **Anonymous access and authentication control**.
7. Clear **Anonymous access**, and then click **OK**.
8. Click **OK**.

Testing the Web Console Virtual Directory

To test the new virtual directory before you deploy the Web Console application, type the URL of the new virtual directory in the **Address** field and press **Enter**.

For example, if you configured the `WCHouston` virtual directory on the server01 Administration server, type `http://server01/WCHouston`.

Chapter 5
Upgrading Large Environments

This chapter provides a migration path for large DRA customers currently running a previous supported version of DRA who want to upgrade to DRA 8.6. This chapter provides a process that helps you upgrade or migrate a distributed environment in controlled phases.

This chapter assumes your environment contains multiple Administration servers, with some servers located at remote sites. This configuration is called a Multi-Master Set (MMS). An MMS consists of one primary Administration server and one or more associated secondary Administration servers. For more information on how an MMS works, see the *Administrator Guide for Directory and Resource Administrator and Exchange Administrator.*

Upgrade Checklist

The following checklist guides you through the entire upgrade process. Use this process to upgrade each server set in your environment.

You can spread this upgrade process over several phases, upgrading one MMS at a time. This upgrade process also allows you to temporarily include secondary servers running a previous DRA version and secondary servers running the current DRA version in the same MMS. DRA supports synchronization between Administration servers running a previous DRA version and servers running the current DRA version. However, be aware that DRA does not support running a previous DRA version with the current DRA version on the same Administration server or client computer.

Warning
Do not upgrade your secondary Administration servers until you upgrade the primary Administration server for that MMS.

	Checklist Items
☐	1. Perform a test upgrade in your lab environment to identify potential issues and minimize production down time.
☐	2. Determine the order in which you want to upgrade your server sets.
☐	3. Prepare each MMS for upgrade. For more information, see "Preparing to Upgrade" on page 46.

	Checklist Items
☐	4. Upgrade the primary Administration server in the appropriate MMS. For more information, see "Upgrading the Primary Administration Server" on page 49.
☐	5. To minimize down time at remote sites, install a local secondary Administration server running DRA 8.6. For more information, see "Installing a Local Secondary Administration Server for the Current DRA Version" on page 49. This step is optional.
☐	6. Deploy the DRA 8.6 user interfaces to your Assistant Admins. For more information, see "Deploying the DRA User Interfaces" on page 50.
☐	7. Upgrade the secondary Administration servers in the MMS.

Preparing to Upgrade

Prepare each server set for upgrade by completing the following steps:

	Checklist Items
☐	1. Make a deployment plan for upgrading the Administration servers and user interfaces (AA client computers). For more information, see "Planning Deployment" on page 46.
☐	2. Dedicate a secondary Administration server to run a previous DRA version as you upgrade a site. For more information, see "Dedicating a Local Administration Server to Run a Previous DRA Version" on page 47. This step is optional.
☐	3. Make any necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings.
☐	4. Synchronize the MMS. For more information, see "Synchronizing Your Previous DRA Version Server Set" on page 48.
☐	5. Back up the registry from the primary Administration server. For more information, see "Backing Up the Administration Server Registry" on page 49.

Planning Deployment

Ensure you plan your deployment of DRA before you begin the upgrade process. As you plan your deployment, consider the following guidelines:

- Test the upgrade process in your lab environment before pushing the upgrade out to your production environment. Testing allows you to identify and resolve any unexpected issues without impacting daily administration responsibilities. For more information about installing DRA in uncommon or complex environments, see "Installing DRA in Complex Environments" on page 35.
- Determine how many AAs rely on each MMS. If the majority of your AAs rely on specific servers or server sets, upgrade those servers first during off-peak hours.

- Determine which AAs need the Delegation and Configuration console. You can obtain this information in one of the following ways:
  - Review which AAs are associated with the built-in AA groups.
  - Review which AAs are associated with the built-in ActiveViews.
  - Use Directory and Resource Administrator Reporting to generate security model reports, such as the ActiveView Assistant Admin Details and Assistant Admin Groups reports.

  Notify these AAs about your upgrade plans for the user interfaces. For more information, see "Deploying the DRA User Interfaces" on page 50.
- Determine which AAs need to connect to the primary Administration server. These AAs should upgrade their client computers once you upgrade the primary Administration server.

  Notify these AAs about your plans for upgrading the Administration servers and user interfaces. For more information, see "Deploying the DRA User Interfaces" on page 50.
- Determine whether you need to implement any delegation, configuration, or policy changes before beginning the upgrade process. Depending on your environment, this decision can be made on a site-by-site basis.
- Coordinate upgrading your client computers and your Administration servers to ensure minimal down time. Be aware that DRA does not support running previous DRA versions with the current DRA version on the same Administration server or client computer. Likewise, DRA does not support synchronization between Administration servers running previous DRA versions and servers running the current DRA version. Therefore, for each MMS, you should plan to upgrade the Administration servers and user interfaces in the same phase.

  If you plan to gradually upgrade your AA client computers, consider deploying the Web Console. For example, AAs can use the DRA 8.5 Service Pack 1 Web Console to access DRA 8.5 Service Pack 1 for time-sensitive tasks, such as resetting account passwords, and use the Account and Resource Management console to connect to an Administration server running DRA 8.6.

Dedicating a Local Administration Server to Run a Previous DRA Version

Dedicating one or more secondary Administration servers to run a previous DRA version locally at a site during upgrade can help minimize down time and costly connections to remote sites. This step is optional and allows AAs to use a previous DRA version throughout the upgrade process, until you are satisfied that your deployment is complete.

Consider this option if you have one or more of the following upgrade requirements:

- You require little or no down time.
- You must support a large number of AAs, and you are not able to upgrade all client computers immediately.
- You want to continue supporting access to a previous DRA version after you upgrade the primary Administration server.
- Your environment includes an MMS that spans across multiple sites.

You can install a new secondary Administration server or designate an existing secondary server running a previous DRA version. If you intend to upgrade this server, this server should be the last server you upgrade. Otherwise, completely uninstall DRA from this server when you successfully finish your upgrade.

Setting Up a New Secondary Server

Installing a new secondary Administration server at a local site can help you avoid costly connections to remote sites, and ensures your AAs can continue using a previous DRA version without interruption. If your environment includes an MMS that spans across multiple sites, you should consider this option. For example, if your MMS consists of a primary Administration server at your London site and a secondary Administration server at your Tokyo site, consider installing a secondary server at the London site and adding it to the corresponding MMS. This additional server allows AAs from the London site to use a previous DRA version until the upgrade is complete.

Using an Existing Secondary Server

You can use an existing secondary Administration server as the dedicated server for a previous DRA version. If you do not plan to upgrade a secondary Administration server at a given site, you should consider this option. If you cannot dedicate an existing secondary server, consider installing a new Administration server for this purpose. Dedicating one or more secondary servers to run a previous DRA version allows your AAs to continue using a previous DRA version without interruption until the upgrade is complete. This option works best in larger environments that use a centralized administration model.

Synchronizing Your Previous DRA Version Server Set

Before you back up the previous DRA version registry or begin the upgrade process, ensure you synchronize the server sets so each Administration server contains the latest configuration and security settings.

Note

Ensure you made all necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings. Once you upgrade the primary Administration server, you cannot synchronize delegation, configuration, or policy settings to any Administration servers running previous DRA versions.

To synchronize your existing server set:

1. Log on to the primary Administration server as the Built-in Admin.
2. Start the MMC interface.
3. In the left pane, expand **Configuration**.
4. Click **Administration servers**.
5. In the right pane, select the appropriate primary Administration server for this server set.
6. Click **Properties**.
7. On the Schedule synch tab, click **Synchronize Now**.
8. Verify the successful completion of the synchronization, and that all secondary Administration servers are available.

Backing Up the Administration Server Registry

Backing up the Administration server registry ensures that you can return to your previous configurations. For example, if you must completely uninstall the current DRA version and use the previous DRA version, having a backup of your previous registry settings allow you to easily recover your previous configuration and security settings.

However, be careful when editing your registry. If there is an error in your registry, the Administration server may not function as expected. If an error occurs during the upgrade process, you can use the backup of your registry settings to restore the registry. For more information, see the *Registry Editor Help*.

To back up the Administration server registry:

1. Run `regedit.exe`.
2. Select the `HKEY_LOCAL_MACHINE\SOFTWARE\Mission Critical Software\OnePoint` key.
3. On the Registry menu, click **Export Registry File**.
4. Specify the name and location of the file to save the registry key.
5. Click **Selected branch**.
6. Click **Save**.

Upgrading the Primary Administration Server

After you successfully prepare your MMS, upgrade the primary Administration server. Do not upgrade user interfaces on the AA client computers until you complete upgrading the primary Administration server. For more information, see "Deploying the DRA User Interfaces" on page 50.

Before you upgrade, notify your AAs when you plan to start this process. If you dedicated a secondary Administration server to run a previous DRA version, also identify this server so AAs can continue using the previous DRA version during the upgrade.

Note
Once you upgrade the primary Administration server, you cannot synchronize delegation, configuration, or policy settings from this server to secondary Administration servers running a previous DRA version. Also, your AAs cannot connect to the primary server until you upgrade the user interfaces on their client computers.

Installing a Local Secondary Administration Server for the Current DRA Version

Installing a new secondary Administration server to run the current DRA version at a local site can help you minimize costly connections to remote sites while decreasing overall down time and allowing quicker deployment of the user interfaces. This step is optional and allows AAs to use both the current DRA version and a previous DRA version throughout the upgrade process, until you are satisfied that your deployment is complete.

Consider this option if you have one or more of the following upgrade requirements:

- You require little or no down time.
- You must support a large number of AAs, and you are not able to upgrade all client computers immediately.
- You want to continue supporting access to a previous DRA version after you upgrade the primary Administration server.
- Your environment includes an MMS that spans across multiple sites.

For example, if your MMS consists of a primary Administration server at your London site and a secondary Administration server at your Tokyo site, consider installing a secondary server at the Tokyo site and adding it to the corresponding MMS. This additional server better balances the daily administration load at the Tokyo site, and allows AAs from either site to use a previous DRA version as well as the current DRA version until the upgrade is complete. Additionally, your AAs experience no down time because you can immediately deploy the current DRA user interfaces. For more information about upgrading user interfaces, see "Deploying the DRA User Interfaces" on page 50.

Deploying the DRA User Interfaces

Typically, you should deploy the current DRA user interfaces after you upgrade the primary Administration server and one secondary Administration server. However, for AAs who must use the primary Administration server, ensure you upgrade their client computers first by installing the Delegation and Configuration console. For more information, see "Planning Deployment" on page 46.

The following table identifies the typical user interfaces and Administration servers used by the each type of DRA user:

Type of DRA User	User Interfaces	Administration Server
DRA Admin	Delegation and Configuration Console	Primary server
	DRA Reporting CLI DRA ADSI Provider	Secondary server
Help Desk Occasional Administrator	Account and Resource Management Console Web Console	Secondary server

If you often perform batch processing through the CLI or the ADSI provider, or frequently generate reports, consider installing these user interfaces on a dedicated secondary Administration server to maintain an appropriate load balance across the MMS.

You can let your AAs install the DRA user interfaces or deploy these interfaces through group policy. You can also easily and quickly deploy the Web Console to multiple AAs.

Note
DRA does not support running a previous version of DRA user interfaces with the current version of DRA user interfaces on the same Administration server or client computer. If you plan to gradually upgrade your AA client computers, consider deploying the Web Console to ensure immediate access to an Administration server running the current DRA version.

Upgrading Secondary Administration Servers

When upgrading secondary Administration servers, you can upgrade each server as needed, depending on your administration requirements. Also consider how you plan to upgrade and deploy the DRA 8.6 user interfaces. For more information, see "Deploying the DRA User Interfaces" on page 50.

For example, a typical upgrade path may include the following steps:

1. Upgrade one secondary Administration server.
2. Instruct the AAs who use this server to install the appropriate user interfaces, such as the Account and Resource Management console.
3. Repeat Steps 1 and 2 until you completely upgrade the MMS.

Before you upgrade, notify your AAs when you plan to start this process. If you dedicated a secondary Administration server to run a previous DRA version, also identify this server so AAs can continue using the previous DRA version during the upgrade. When you complete the upgrade process for this MMS, and all AA client computers are running upgraded user interfaces, take any remaining previous DRA version servers offline.

Appendix A
Ports and Protocols Used in DRA Communications

DRA and ExA use the following ports and protocols for communication.

Communication path	Protocol and port	Use
DRA primary Administration server to secondary servers	DCOM 135	End-point mapper, a basic requirement for DRA communication; allows Administration servers to locate each other in an MMS
	NetBIOS 139	Delegation model replication; file replication during MMS synchronization; export certain registry keys and copy them to secondary servers
	DCOM 445	Delegation model replication; file replication during MMS synchronization
	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.

Communication path	Protocol and port	Use
DRA secondary servers to primary Administration server	DCOM 135	End-point mapper, a basic requirement for DRA communication
	NetBIOS 139	Delegation model replication (disabled, but performed on service start); file replication during MMS synchronization
	DCOM 445	Delegation model replication (disabled, but performed on service start); file replication during MMS synchronization
	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.
	RPC all ports from 1024-65535 as served by the DCOM server	DCOM Service communication
between DRA secondary Administration servers	LDAP 50000	Attribute replication and DRA server-ADAM communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADAM) (if enabled). This port number can be configured during installation.
DRA to domain controllers	DCOM 135	End-point mapper, a basic requirement for DRA communication; allows Administration server to locate the DRA Agent
	NetBIOS 139	Agent deployment check (disabled, but performed on service start)
	DCOM 445	Agent deployment (disabled, but can be enabled from the user interface)
	LDAP 389	Active Directory object management
	RPC all ports from 1024-65535 as served by the DCOM server	DCOM Service communication
DRA to and from 32-bit clients	DCOM 135	End-point mapper, a basic requirement for DRA communication
DRA to and from DRA Web service	DCOM 135	End-point mapper, a basic requirement for DRA communication
	RPC all ports from 1024-65535 as served by the DCOM server	DCOM Service communication

Communication path	Protocol and port	Use
DRA Web service to and from DRA Web Console	HTTP SSL 443	Web client access
DRA clients to NetIQ DRA Core Service	TCP 50101	Communication between DRA Client and NetIQ DRA Core Service and also between NetIQ DRA Core Service components in an MMS. Used for generating a UI Report from DRA Client. This port number can be configured during installation.
DRA to Log Archive Server	TCP 1801	Log archive communication using Microsoft Message Queueing (MSMQ)
	TCP 8989	Log archive communication. You can configure this port using the Log Archive Configuration wizard.
DRA to SQL Server	TCP 1433	Database setup and configuration; XML check-in
	UDP 1434	If using a SQL Server instance, the browser service uses UDP 1434 to identify the port for the named instance.
DRA to the Exchange Server	LDAP 389 TCP 80	Mailbox management Only needed for Exchange Server 2010 communications