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

June 2017

Legal Notice

Contents

About this Book and the Library **5**
About NetIQ Corporation **7**

1 Understanding Requirements **9**

Administration Server Requirements . . . 9
Microsoft Exchange Server Requirements . . . 10
Client Requirements . . . 11
Reporting Requirements . . . 11
Licensing Requirements . . . 11

2 Installing DRA **13**

Planning Your Environment . . . 13
Supported Environments . . . 13
Identifying Installation Scenarios . . . 14
Basic Environment Considerations . . . 15
Enterprise Environment Considerations . . . 20
Installation Checklist . . . 26
Installing the REST Services Extensions . . . 28
Requirements . . . 28
Installation Checklist . . . 28

3 Initial Configuration **29**

Configuration Checklist . . . 29
Adding Managed Domains . . . 30
Adding Managed Subtrees . . . 30
Configuring DCOM Settings . . . 30
Configuring the Distributed COM Users Group . . . 30
Configuring the Domain Controller and Administration Server . . . 31
Installing or Upgrading Licenses . . . 32

4 Upgrading DRA **33**

Upgrade Checklist . . . 33
Preparing to Upgrade . . . 34
Planning Deployment . . . 34
Dedicating a Local Administration Server to Run a Previous DRA Version . . . 35
Setting Up a New Secondary Server . . . 35
Using an Existing Secondary Server . . . 36
Synchronizing Your Previous DRA Version Server Set . . . 36
Backing Up the Administration Server Registry . . . 36
Upgrading the Primary Administration Server . . . 37
Installing a Local Secondary Administration Server for the Current DRA Version . . . 37
Deploying the DRA User Interfaces . . . 38
Upgrading Secondary Administration Servers . . . 39
Upgrading DRA Reporting Components . . . 39

A Ports and Protocols Used in DRA Communications 41

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:

Administration Guide

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

Reporting Guide

Provides conceptual information about the NetIQ Reporting Center (Reporting Center) product. This book defines terminology and includes implementation scenarios.

Help

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

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

1 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 following table describes the recommended hardware requirements for the Administration server computer of the following two types of environment:

- **Regular Environments** include 100 thousand to one million Active Directory objects and may get up to 1000 events per hour.
- **Enterprise Environments** include more than one million Active Directory objects and may get up to 10 thousand events per hour.

Component	Regular Environment	Enterprise Environment
CPU	2GHz or greater Intel octa-core processor	2GHz or greater Intel octa-core processor
RAM	8 GB	16 GB
Disk space	80 GB	100 GB

The following table describes the recommended software requirements for the Administration server computer of an environment of any size.

Component	Requirement
Operating System	One of the following 64-bit versions of Microsoft Windows: ◆ Microsoft Windows Server 2012 64-bit ◆ Microsoft Windows Server 2012 R2 64-bit ◆ Microsoft Windows Server 2016 64-bit **NOTE:** The server also must be a member of a supported Microsoft Windows Server 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.

Component	Requirement

Enabled Software and Support
 	
NOTE: As part of its installation process, DRA will install any of the components listed here that are missing from the targeted system.
	◆ Microsoft .Net Framework 4.5.2
	◆ Microsoft Visual C++ 2008 Redistributable Package (x86)
	◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)
	◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x64)
	◆ Microsoft Message Queueing (MSMQ)
	◆ Microsoft Internet Information Services (IIS)
	  ◆ Windows Server 2012 and 2012 R2 require IIS 7.5, 8.0, or 8.5
	  ◆ Windows Server 2016 requires IIS 10.0
	◆ AD LDS
	◆ ASP .NET
	◆ ASP

Microsoft Office 365/ Skype for Business/ Exchange Online	◆ Windows Azure Active Directory Module for Windows PowerShell ◆ Skype for Business Online, Windows PowerShell Module ◆ Microsoft Online Services Sign-In Assistant for IT Professionals
Microsoft Exchange Tools (needed only for Exchange Administrator)	Microsoft Exchange management tools that match the software version of your Microsoft Exchange Server 2010, 2013, or 2016. To manage Exchange Server 2010, 2013, or 2016 objects: ◆ Windows Remote Management (WinRM) 2.0 ◆ Windows PowerShell 2.0
DRA Reporting Server (optional Management reports)	◆ SQL Server 2012 SP2 ◆ SQL Server 2014 ◆ SQL Server Reporting Services ◆ NRC 2.1 **NOTE:** If NRC 2.1 is not installed you will be given the option of installing it over your current version of NRC. NRC 2.1 requires Microsoft .NET 4.0 and ASP .NET 4.0 to function. Your existing database will not be affected. ◆ Microsoft Internet Information Services (IIS) 6.0, 7.0, or 7.5

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 2013 CU16
- Microsoft Exchange Server 2016 CU5

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 a supported web browser 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 18.

Component	Requirement
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 Server 2016 64-bit ◆ Microsoft Windows Server 2012 R2 64-bit ◆ Microsoft Windows Server 2012 64-bit ◆ Microsoft Windows 8.1 ◆ Microsoft Windows 10

Reporting Requirements

Requirements for the DRA Reporting include the following:

Component	Requirement
Operating System	Ensure the Reporting Center computer runs one of the following Microsoft Windows operating systems: ◆ Microsoft Windows Server 2012 R2 ◆ Microsoft Windows Server 2012

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. After you install the Administration server, use the Health Check Utility to install the customized license key file (`License1.lic`) you receive from NetIQ Corporation.

The license key file provides access to an unlimited amount of user accounts that you can manage with DRA and ExA. 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. For more information about licenses, see “Installing or Upgrading Licenses” on page 32.

2 Installing DRA

This chapter guides you through installing DRA and ExA in environments of different sizes and complexities.

Planning Your Environment

This section guides you through the process of planning your DRA and ExA installation in your environment.

Supported Environments

DRA supports several different types of environments, including the following installations:

- Managed and trusted domains
- Microsoft Exchange support
- Departmental support through managed subtrees
- Multiple Administration servers

Managed and Trusted Domains

DRA lets you securely administer account and resource objects and Microsoft Exchange mailboxes from multiple managed domains. You can manage Microsoft Windows domains as well as multiple subtrees from specific Microsoft Windows domains. You can also perform the following administration tasks on objects in trusted domains:

- View objects in trusted domains
- Add accounts from trusted domains to groups in your managed domains

For more information about configuring managed and trusted domains, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Microsoft Exchange Support

DRA lets you manage Microsoft Exchange Server mailboxes as you manage the associated user accounts, contacts, and groups. You can implement many integrated Microsoft Exchange management features across your enterprise, including the following functions:

- Automatically create, move, and delete mailbox stores when managing accounts
- Automatically generate email addresses based on account naming conventions
- Delegate administration of specific mailbox properties, such as mailbox security settings

DRA supports and extends your security model. By integrating Microsoft Exchange management into your DRA workflow, you save time and money with streamlined administrative processes. For more information about securely managing Microsoft Exchange mailboxes and implementing Microsoft Exchange policy, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Departmental Support through Managed Subtrees

Departmental support lets you manage multiple subtrees of specific Microsoft Windows domains. By managing a subtree, you can use DRA to secure a department or division within a larger corporate domain. Departmental support also limits your licensing requirements to only those objects you manage in the subtree.

For more information about implementing departmental support, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Multiple Administration Servers

You can install multiple Administration servers across your managed domain. Called a Multi-Master Set (MMS), these servers help distribute administration loads and provide fault tolerance within a site. Each MMS consists of one primary Administration server and multiple secondary Administration servers.

For more information about Administration servers, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*. For more information about implementing an MMS, see “Enterprise Environment Considerations” on page 20.

Identifying Installation Scenarios

A **basic** environment consists of the following:

- ❑ Up to four DRA servers;
- ❑ A common service account used across all DRA servers;
- ❑ No firewall between DRA servers;
- ❑ Up to four trusted domains;
- ❑ No non-trusted domains;
- ❑ No multiple managed domains;
- ❑ No access to the Deleted Objects Container in Active Directory.

An **enterprise** environment can consist of any or all of the following:

- ❑ Any number of DRA servers;
- ❑ A firewall between DRA servers might or might not be present;
- ❑ One common service account used across all DRA servers or multiple common service accounts;
- ❑ Any number of trusted domains;
- ❑ Any number of non-trusted domains;
- ❑ Multiple managed domains;
- ❑ At least 25,000 objects;
- ❑ Limited access to the Deleted Objects Container in Active Directory.

Basic Environment Considerations

Installing the Administration Server

Always install the Administration server on a Microsoft Windows server. 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 NetIQ Administration server 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.

Installing the User Interfaces

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

Product	Filename	Supported User Interfaces
DRA	NetIQAdminInstallationKit.msi	Account and Resource Management Console Delegation and Configuration Console NetIQ Reporting Center features (console, server, and database) Command-line Interface (CLI) ADSI Provider
REST Services	RESTServicesInstaller.exe	DRA Host Service DRA REST Service PowerShell extensions Web Console

IMPORTANT: The PowerShell extensions require PowerShell 2.0.

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.

NOTE

- 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 17.
- 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 Reporting Center” on page 18.

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.

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 `DRAInstaller.msi` from the Intel folder of the installation kit. The `DRAInstaller.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:

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
NetIQDRAClients.mst	Installs all DRA user interfaces
NRCSetup.exe	Installs Reporting Center components on 32-bit or 64-bit operating systems

NOTE

- 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 `DRAInstaller.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 user interface `.mst` file, such as `NetIQDRAUserConsole.mst`, to this group policy object.
6. Distribute your group policy.

Deploying the Web Console

You can run the Web Console from any computer with a supported web browser by opening the link provided in the Account and Resource Management console, or by selecting the WebConsole shortcut 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.

Installing Reporting Center

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 Reporting Center with DRA Management Reports

You can install the Reporting Center components along with the DRA Management reports 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.
Console	◆ The location of the Configuration Database, in this format: *ServerName**Instance* ◆ The name of the Web Service server, in this format: `http://` *ServerName*`/NRCWebService`
Reporting Services Data Extension	◆ The location of SQL Server Reporting Services (SSRS), in this format: *ServerName**Instance*

To install Reporting Center with DRA Management Reports:

1. Log on the Microsoft Windows server where you have installed the SQL instance for the reporting databases with an administrator account. Ensure this account has local administrative privileges as well as System Administrator privileges on the SQL Server.
2. Run `DRAReporting.msi` in the Intel 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. Follow the instructions until the installation completes, and click **Finish**.

   When you click **Finish**, the setup utility launches the NRC Setup.
4. Follow the instructions until the installation completes, and click **Finish**.

You can also install the Reporting Center console on other computers. For more information about installing Reporting Center, see the *NetIQ Reporting Center Reporting Guide*.

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

Go to "Installation Checklist" on page 26.

Enterprise Environment Considerations

The information provided in the Basic Environment Considerations section applies to planning your enterprise environment as well.

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*.

NetIQ strongly recommends that you install the primary Administration server on a different computer than the domain controller. 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 22.

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.

NOTE

- 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 the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

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.
- To manage workgroups the access account must be a local server account.

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.

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

Installing the Web Application on a Dedicated Web Server

You can install the Web application 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 application requirements, see “Administration Server Requirements” on page 9. For more information about configuring Kerberos authentication, see NETIQKB14935 and “Installing the Web Application on a Server not Running the Administration Server” on page 25.

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 application 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 application on a computer other than the Administration server, and you want to deploy the Web Console with a supported web browser, 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.

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

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

To install the Web application 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:

   7a 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`.

   7b 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`.

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.

	Checklist Items
❑	Ensure your server and client computers meet the product hardware and software requirements. For more information, see Chapter 1, “Understanding Requirements,” on page 9.
❑	Identify the domains or subtrees you want to manage. For more information, see the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*
❑	Ensure that all your DRA servers are in a trusted domain.
❑	Determine the account information you want to use for the DRA Service Account.
❑	Create the local domain admin group you want DRA to use as the AD LDS admin account.
❑	Identify the user account or group you want DRA to assign the built-in DRA Admins 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.
❑	Decide if you want to allow the DRA installer to configure DCOM for you. If not, after installing DRA, configure DCOM settings on that computer. For more information, see “Configuring DCOM Settings” on page 30.
❑	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 the *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.
❑	Review “Installing the Administration Server” on page 15 and “Installing the User Interfaces” on page 16. Install DRA.
❑	(Optional) Install reporting components on a SQL Server computer to enable DRA Management reports. For more information, see “Installing Reporting Center” on page 18.
❑	Complete the following tasks: ◆ 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. ◆ 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 Application on a Dedicated Web Server” on page 24. ◆ (Optional) 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.

Installing the REST Services Extensions

During the installation of DRA you will also have the chance to install the following extensions that enhance DRA's capabilities:

- A RESTful web service that allows integration with DRA.
- A PowerShell module that allows non-DRA clients to request DRA operations using PowerShell cmdlets. This module can be installed on any machine that contains PowerShell 2.0.
- A Web Console, a Web-based user interface that provides quick and easy access to many DRA tasks. For more information, see "Installing the User Interfaces" on page 16 and the Web Console section of the *Directory and Resource Administrator User Guide*.

Requirements

The following list describes the software requirements for computers running the REST Services extensions:

- Microsoft Internet Information Services 6.0, 7.0 or 7.5
- Internet Information Services World Wide Web Publishing Service (W3SVC)
- Supported browsers: Microsoft Internet Explorer 10.0 or newer, Google Chrome, Mozilla Firefox

To deploy the Web Console, ensure your client computers are running a supported web browser 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 18.

Installation Checklist

Use the following checklist to guide you through the installation process.

	Checklist Items
❑	Identify the machines onto which you want to install the REST Services extensions. Keep the following in mind: ◆ The DRA Host Service must share the same service account as the primary DRA Server and should be installed on the same machine. ◆ The REST Service can be installed on any machine that meets the software requirements listed previously. ◆ The Web Console should be installed on the IIS server. ◆ The PowerShell extensions can be installed on any machine running PowerShell 2.0.
❑	Run the RESTServicesInstaller.exe file on each targeted machine and select the appropriate extensions to install.

3 Initial Configuration

This chapter outlines the required configuration steps for the first time you install DRA.

Configuration Checklist

Use the following checklist to guide you in configuring DRA for first-time use.

	Checklist Items
❑	Use the Health Check Utility to apply a DRA license. For more information about DRA licenses, see "Installing or Upgrading Licenses" on page 32.
❑	Using the DRA service account, log on to a computer where the Delegation and Configuration Console is installed. Open the console.
❑	Add the first managed domain to DRA. **NOTE:** You can start delegating powers after the initial Full Account Refresh completes.
❑	*Optional:* Add additional managed domains and subtrees to DRA. For more information about managed domains, see "Adding Managed Domains" on page 30.
❑	*Optional:* Configure DCOM settings.
❑	*Optional:* Configure Office 365, Skype for Business, and Skype Online.
❑	Customize DRA 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 ◆ Seamlessly integrate the DRA console with other products by implementing custom tools, which allow you to run external applications, launch scripts, and open web pages quickly and easily from the DRA console. **NOTE:** When using custom tools or trigger files within a Multi-Master Set (MMS), the path used to store the custom tools or trigger files must be the same location on every DRA server within the MMS. By default this path is set to `{DRAInstallDir}\{MMS ID}\Download`. You can change this path on the **Configuration Management >> Custom Tools >> Application Settings** dialog.

Adding Managed Domains

You can add managed domains, servers, or workstations after you install the Administration server. When you add the first managed domain, you must log on using the DRA service account to a computer where the Delegation and Configuration Console is installed. You must also have Administrative Rights within the domain, such as the rights granted to the Domain Administrators group. To add managed domains and computers after you install the first managed domain, you must have the appropriate powers, such as those included in the built-in Configure Servers and Domains role.

NOTE: 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 *Administrator Guide for Directory Resource Administrator and Exchange Administrator*.

Adding Managed Subtrees

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 Advanced Configuration node in the Delegation and Configuration console. 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 Chapter 1, “Understanding Requirements,” on page 9.

NOTE: 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*.

Configuring DCOM Settings

Configure DCOM settings on the primary Administration server if you did not allow the setup program to configure DCOM for you.

Configuring the Distributed COM Users Group

If you selected to not configure Distributed COM during the DRA installation process, 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 **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.

Installing or Upgrading Licenses

DRA requires a license key file. This file contains your license information and is installed on the Administration server. After you install the Administration server, use the Health Check Utility to install the 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.

4 Upgrading DRA

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 *Directory and Resource Administrator and Exchange Administrator Administrator Guide.*

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 have upgraded the primary Administration server for that MMS.

	Checklist Items
❑	Install the standalone DRA Health Check utility and run it using a service account. Fix any issues.
❑	Perform a test upgrade in your lab environment to identify potential issues and minimize production downtime.
❑	Determine the order in which you want to upgrade your server sets.
❑	Prepare each MMS for upgrade. For more information, see “Preparing to Upgrade” on page 34.
❑	Upgrade the primary Administration server in the appropriate MMS. For more information, see “Upgrading the Primary Administration Server” on page 37.
❑	*(Optional)* To minimize downtime at remote sites, install a local secondary Administration server running the newest version of DRA. For more information, see “Installing a Local Secondary Administration Server for the Current DRA Version” on page 37.
❑	Deploy the user interfaces to your Assistant Admins. For more information, see “Deploying the DRA User Interfaces” on page 38.
❑	Upgrade the secondary Administration servers in the MMS.

	Checklist Items
❑	Upgrade DRA Reporting. For more information, see “Upgrading DRA Reporting Components” on page 39.
❑	Run the Health Check Utility that was installed as part of the upgrade. Fix any issues.

Preparing to Upgrade

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

❑	Checklist Items
❑	Make a deployment plan for upgrading the Administration servers and user interfaces (AA client computers). For more information, see “Planning Deployment” on page 34.
❑	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 35. This step is optional.
❑	Make any necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings.
❑	Synchronize the MMS. For more information, see “Synchronizing Your Previous DRA Version Server Set” on page 36.
❑	Back up the registry from the primary Administration server. For more information, see “Backing Up the Administration Server Registry” on page 36.

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 “Enterprise Environment Considerations” on page 20.
- Review Appendix A, “Ports and Protocols Used in DRA Communications,” on page 41.
- 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 38.

- 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 38.
- 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 downtime. 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.

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 downtime 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 downtime.
- 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 Management**.
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 Synchronization schedule tab, click **Refresh 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 allows 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*.

IMPORTANT: The DRA server version, Windows OS name and managed domain configuration must be exactly the same when restoring the registry.

IMPORTANT: Before upgrading, back up the Windows OS of the machine that is hosting DRA or create a virtual machine snapshot image of the machine.

To back up the Administration server registry:

1. Run `regedit.exe`.
2. Select the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\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 38.

NOTE: For more detailed upgrade considerations and instructions, see the *Directory and Resource Administrator Release Notes*.

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 downtime 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 downtime.
- 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 downtime 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 38.

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 34.

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
(The person who will maintain the product configuration)	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 user interfaces. For more information, see “Deploying the DRA User Interfaces” on page 38.

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 “Upgrade one secondary Administration server.” on page 39 and Step 2 on page 39 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.

Upgrading DRA Reporting Components

Before you upgrade DRA Reporting, ensure that your environment meets the minimum requirements for NRC 2.1. For more information on installation requirements and upgrade considerations, see the *NetIQ Reporting Center Reporting Guide*.

To upgrade DRA Reporting:

1. To ensure that the reporting collectors do not run during the upgrade process, disable reporting support on the Reporting Service Configuration window in the Delegation and Configuration console.
2. Log on the Microsoft Windows server where you have installed the SQL instance for the reporting databases with an administrator account. Ensure this account has local administrative privileges as well as System Administrator privileges on the SQL Server.
3. Run `DRAReportingSetup.exe`. in Intel folder of the installation kit.
4. Follow the instructions until the installation completes, and click **Finish**.
5. *Conditional:* If your NRC web service is installed on a different computer, log on to the computer where the web service is installed.
   - **5a** Run `NRCSetup.exe` to upgrade the NRC web service.
6. Run `NRCSetup.exe` on all NRC client computers.
7. On your primary administration server, enable reporting in the Delegation and Configuration Console.

If your environment uses SSRS integration, you will need to re-deploy your reports. For more information about re-deploying reports, see the *NetIQ Reporting Center Reporting Guide*.

A Ports and Protocols Used in DRA Communications

DRA uses 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
	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.
DRA secondary servers to primary Administration server	DCOM 135	End-point mapper, a basic requirement for DRA communication
	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

Communication path	Protocol and port	Use
between DRA secondary Administration servers	LDAP 50000	Attribute replication and DRA server-ADLDS communication. This port number can be configured during installation.
	LDAP 50001	SSL attribute replication (ADLDS) (if enabled). This port number can be configured during installation.
DRA to domain controllers	LDAP 389	Active Directory object management
	Port 53	Name resolution
	Kerberos Port 88	Allows authentication from the DRA server to the domain controllers
Domain controller to DRA	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
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 50102	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.

Communication path	Protocol and port	Use
DRA to the Exchange Server	LDAP 389	Mailbox management
	TCP 80	Needed for all on-premise Exchange Servers 2010 through 2013.
DRA to Office 365	TCP 80	Remote PowerShell access
	HTTP SSL 443	Graph API access
DRA Cache Service	Any TCP port between 50000 and 66535. The default port is TCP 50103.	Cache service communication on the DRA server (does not need to be opened through the firewall)
REST Service	The default REST Service port is 8755. The default DRA Host Service port is 11192.	These ports can be changed by the user; however, the new ports must be open to allow clients to connect to them.
PowerShell to REST Service	HTTPS The default REST Service port is 8755.	This port can be changed by the user; however, the new ports must be open to allow clients to connect to them.