Directory and Resource Administrator

Installation Guide

July 2018

Legal Notice

Contents

About this Guide

The *Administrator Guide* provides conceptual information about the Directory and Resource Administrator (DRA) and Exchange Administrator (ExA) products. This book defines terminology and includes implementation scenarios.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Additional Documentation

This guide is part of the Directory and Resource Administrator documentation set. For a complete list of publications supporting this release, visit the Documentation website (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

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 documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the 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

NetIQ Communities, 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, NetIQ Communities 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 Getting Started

Before you install and configure all of the components of Directory and Resource Administrator™ (DRA) you should understand the basic tenants of what DRA will do for your enterprise and the role of DRA components in the product architechure.

What is Directory and Resource Administrator

Directory and Resource Administrator delivers secure and efficient privileged-identity administration of Microsoft Active Directory (AD). DRA performs granular delegation of “least privilege” so that administrators and users receive just the permissions needed to complete their specific responsibilities. DRA also enforces adherence to policy, provides detailed-activity auditing and reporting, and simplifies repetitive task completion with IT process automation. Each of these capabilities contributes to protecting your customers’ AD and Exchange environments from the risk of privilege escalation, errors, malicious activity, and regulatory non-compliance, while reducing administrator burden by granting self-service capabilities to users, business managers and Help Desk personnel.

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 mailboxes, public folders 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, Microsoft Exchange and Microsoft Office 365 environments.

- **Support for Active Directory, Office 365, Exchange, and Skype for Business:** Delivers administrative management of Active Directory, on-premise Exchange Server, on-premise Skype for Business, Exchange Online, and Skype for Business Online.
- **Granular user and administrative privilege-access controls:** Patented ActiveView technology delegates just the privileges needed to complete specific responsibilities and protect against privilege escalation.
- **Customizable web console:** Intuitive approach enables non-technical personnel to easily and safely perform administrative tasks via limited (and assigned) capabilities and access.
- **In-depth activity auditing and reporting:** Provides a comprehensive audit record of all activity performed with the product. Securely stores long-term data and demonstrates to auditors (e.g. PCI DSS, FISMA, HIPAA and NERC CIP) that processes are in place for controlling access to AD.
- **IT Process Automation:** Automates workflows for a variety of tasks, like provisioning and deprovisioning, user and mailbox actions, policy enforcement, and controlled self-service tasks; increases business efficiencies, and reduces manual and repetitive administrative efforts.
- **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.
- **Integration with Change Guardian:** Enhances auditing for events generated in Active Directory outside of DRA and workflow automation.

Understanding Directory and Administrator Components

The components of DRA that you will consistenly use to manage priviliged access include primary and secondary servers, administrator consoles, reporting components, and the Aegis workflow engine to automate workflow processes.

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

Type of DRA User	User Interfaces	Administration Server
DRA Administrator (The person who will maintain the product configuration)	Delegation and Configuration Console	Primary server
	DRA Reporting Center Setup (NRC) CLI *(optional)* DRA ADSI Provider *(optional)*	Secondary server
Help Desk Occasional Administrator	Account and Resource Management Console	Secondary server
Help Desk Occasional Administrator	Web Console	Any DRA server with DRA REST installed

DRA Administration Server

The DRA Administration server stores configuration data (environmental, delegated access, and policy), executes operator and automation tasks, and audits system wide activity. While supporting several console and API level clients, the server is designed to provide high availability for both redundancy and geographic isolation through a Multi-Master Set (MMS) scale-out model. In this model, every DRA environment will require one primary DRA Administration server that will synchronize with a number of additional secondary DRA Administration servers.

We strongly recommend that you do not install Administration servers on Active Directory domain controllers. For each domain that DRA manages, ensure there is at least one domain controller in the same site as the Administration server. By default, the Administration server accesses the closest domain controller for all read and write operations; when performing site-specific tasks, such as password resets, you can specify a site specific domain controller to process the operation. As a best practice, consider dedicating a secondary Administration server for your reporting, batch processing, and automated workloads.

Delegation and Configuration Console

The Delegation and Configuration console is an installable user interface that provides system administrators access to DRA configuration and administration functions.

- **Delegation Management:** Enables you to granularly specify and assign access to managed resources and tasks to Assistant Administrators.
- **Policy and Automation Management:** Enables you to define and enforce policy to ensure compliance to the standards and conventions of the environment.
- **Configuration Management:** Enables you to update DRA system settings and options, add customizations, and configure managed services (Active Directory, Exchange, Office 365, etc.).

Account and Resource Management Console

The Account and Resource Management Console is an installable user interface for DRA Assistant Administrators to view and manage delegated objects of connected domains and services.

Web Console

The Web Console is a web-based user interface that provides quick and easy access to DRA Assistant Administrators to view and manage delegated objects of connected domains and services.

Administrators can customize the look and use of the Web Console to include customized enterprise branding and customized object properties, as well as configure integration with Change Guardian servers to enable change auditing that occurs outside of DRA.

The DRA Administrator can also create and modify automated workflow forms to run routine automated tasks when triggered.

Unified Change History is another feature of the Web Console that enables integration with Change History servers to audit changes made to AD objects outside of DRA. Change History report options include the following:

- Changes made to...
- Changes made by...
- Mailbox created by...
- User, group, and contact email address created by...
- User, group, and contact email address deleted by...
- Virtual attribute created by...
- Objects moved by...

Reporting Components

DRA Reporting provides built-in, customizable templates for DRA management and details of DRA managed domains and systems:

- Resources reports for AD objects
- AD object data reports
- AD summary reports
- DRA configuration reports
- Exchange configuration reports
- Office 365 Exchange Online reports
- Detailed activity trends reports (By month, domain, and peak)
- Summarized DRA activity reports

DRA reports can be scheduled and published through SQL Server Reporting Services for convenient distribution to stakeholders.

Workflow Engine

DRA integrates with the Aegis workflow engine to automate workflow tasks via the Web Console where Assistant Administrators can configure the Workflow Server and execute customized workflow automation forms, and then view the status of those workflows. For more information about the workflow engine, see the DRA Documentation site (https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

Product Architecture

2 Product Installation and Upgrade

This chapter outlines the recommended hardware, software, and account requirements required by Directory and Resource Administrator. It then guides you through the installation process with a checklist for each component of the installation.

Planning Your Deployment

As you plan your Directory and Resource Administrator deployment, use this section to assess your hardware and software environment for compatibility and to note the required ports and protocols you will need to configure for the deployment.

Tested Resource Recommendations

This section provides sizing information for our base resource recommendation. Your results may vary based on the hardware available, the specific environment, the specific type of data processed, and other factors. It is likely that larger, more powerful hardware configurations exist that can handle a greater load. If you have questions, please consult with NetIQ Consulting Services.

Executed in an environment with approximately one million Active Directory objects:

Component	CPU	Memory	Storage
DRA Administration Server	4 CPU (x64)/cores 2.0 GHz	16 GB	100 GB
DRA Web Console	2 CPU (x64)/cores 2.0 GHz	8 GB	100 GB
DRA Reporting	4 CPU (x64)/cores 2.0 GHz	16 GB	100 GB
DRA Workflow Server	4 CPU (x64)/cores 2.0 GHz	16 GB	100 GB

Virtual Environment Resource Provisioning

DRA keeps large memory segments active for extended periods of time. When provisioning resources for a virtural environment, the following recommendations should be considered:

- Allocate the storage as “Thick Provisioned”
- Set memory reservation to Reserve All Guest Memory(All Locked)
- Make sure that the paging file is large enough to cover the potential ballooned memory reallocation at the virtual layer

Required Ports and Protocols

The ports and protocols for DRA communication are provided in this section.

- Configurable ports are indicated with one asterisik *
- Ports requiring a certificate are indicated with two asterisks **

DRA Administration Servers

Protocol and Port	Direction	Destination	Usage
TCP 135	Bi-directional	DRA Administration Servers	End-point mapper, a basic requirement for DRA communication; enables Administration servers to locate each other in MMS
TCP 445	Bi-directional	DRA Administration Servers	Delegation model replication; file replication during MMS synchronization (SMB)
Dynamic TCP port range *	Bi-directional	Microsoft Active Directory domain controllers, DRA Clients	By default, DRA assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 50000 *	Bi-directional	DRA Administration Servers	Attribute replication and DRA server-ADAM communication. (LDAP)
TCP 50001 *	Bi-directional	DRA Administration Servers	SSL attribute replication (ADAM)
TCP/UDP 389	Outbound	Microsoft Active Directory domain controllers	Active Directory object management (LDAP)
	Outbound	Microsoft Exchange Server	Mailbox management (LDAP)
TCP/UDP 53	Outbound	Microsoft Active Directory domain controllers	Name resolution
TCP/UDP 88	Outbound	Microsoft Active Directory domain controllers	Allows authentication from the DRA Server to the domain controllers (Kerberos)
TCP 80	Outbound	Microsoft Exchange Server	Needed for all on-premises Exchange servers 2010 through 2013 (HTTP)
	Outbound	Microsoft Office 365	Remote PowerShell access (HTTP)
TCP 443	Outbound	Microsoft Office 365, Change Guardian	Graph API access and Change Guardian Integration (HTTPS)
TCP 443, 5986, 5985	Outbound	Microsoft PowerShell	Native PowerShell cmdlets (HTTPS) and PowerShell Remoting

Protocol and Port	Direction	Destination	Usage
TCP 8092 * **	Outbound	Workflow Server	Workflow status and triggering (HTTPS)
TCP 50101 *	Inbound	DRA Client	Right-Click Change History report to UI Audit Report. Can be configured during installation.
TCP 8989	Localhost	Log Archive Service	Log archive communication (does not need to be opened through the firewall)
TCP 50102	Bi-directional	DRA Core Service	Log Archive Service
TCP 50103	Localhost	DRA Cache Service	Cache service communication on the DRA server (does not need to be opened through the firewall)
TCP 1433	Outbound	Microsoft SQL Server	Reporting data collection
UDP 1434	Outbound	Microsoft SQL Server	SQL Server browser service uses this port to identify the port for the named instance.
TCP 8443	Bi-directional	Change Guardian Server	Unified Change History

DRA REST Server

Protocol and Port	Direction	Destination	Usage
TCP 8755 * **	Inbound	IIS Server, DRA PowerShell cmdlets	Execute DRA REST-based workflow activities (ActivityBroker)
TCP 11192 * **	Outbound	DRA Host Service	For communication between DRA REST Service and DRA Administration Service
TCP 443	Outbound	Microsoft AD Domain Controllers	Autodiscovery using Service Connection Point (SCP)

Web Console (IIS)

Protocol and Port	Direction	Destination	Usage
TCP 8755 * **	Outbound	DRA REST Service	For communication betweeen DRA Web Console, DRA PowerShell, and DRA Host Service
TCP 135	Outbound	Microsoft Active Directory domain controllers	Autodiscovery using Service Connection Point (SCP)
TCP 443	Inbound	Client Browser	Opening a DRA web site
TCP 443 **	Outbound	Advanced Authentication Server	Advanced Authentication

DRA Delegation and Administration Console

Protocol and Port	Direction	Destination	Usage
TCP 135	Outbound	Microsoft Active Directory domain controllers	Autodiscovery using SCP
Dynamic TCP port range *	Outbound	DRA Administration Servers	DRA Adapter workflow activities. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 50102	Outbound	DRA Core Service	Change History report generation

Workflow Server

Protocol and Port	Direction	Destination	Usage
TCP 8755	Outbound	DRA Administration Servers	Execute DRA REST-based workflow activities (ActivityBroker)
Dynamic TCP port range *	Outbound	DRA Administration Servers	DRA Adapter workflow activities. By default, DCOM assigns ports dynamically from the TCP port range of 1024 through 65535. You can, however, configure this range by using Component Services. For more information, see Using Distributed COM with Firewalls (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 1433	Outbound	Microsoft SQL Server	Workflow data storage
TCP 8091	Inbound	Operations Console and Configuration Console	Workflow BSL API (TCP)
TCP 8092 **	Inbound	DRA Administration Servers	Workflow BSL API (HTTP)
TCP 2219	Localhost	Namespace Provider	Used by the Namespace Provider to run adapters
TCP 9900	Localhost	Correlation Engine	Used by the Correlation Engine to communicate with the Workflow Engine and Namespace Provider
TCP 10117	Localhost	Resource Management Namespace Provider	Used by the Resource Management Namespace Provider

Supported Platforms

For the most recent information about supported software platforms, refer to the Directory and Resource Administrator page on the NetIQ website: https://www.netiq.com/support

Managed System	Prerequisites
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (Except for Public Folders) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Windows Azure Active Directory Module for Windows PowerShell https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype for Business Online, Windows PowerShell Module https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype for Business	◆ Microsoft Skype for Business 2015
Change History	◆ Change Guardian 5.0, 5.1
Web Browsers	◆ Microsoft Internet Explorer 11, Edge ◆ Google Chrome ◆ Mozilla Firefox

DRA Administration Server Requirements

DRA requires the following server requirements for software and accounts:

Software Requirements:

Component	Prerequisites
Installation Target	**NetIQ Administration Server Operating System:**
Operating System	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 is supported for upgrade only. **NOTE:** The server must also be a member of a supported Microsoft Windows Server native domain. **Windows DRA Interfaces:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 & x64), 10 (x86 & x64)
Installer	◆ Microsoft .Net Framework 4.5.2 and above

Administration Server	**Directory and Resource Administrator:**
	◆ Microsoft .Net Framework 4.5.2 and above
	◆ One of the following:
	  ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages (x64 and x86)
	  ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 and x86)
	◆ Microsoft Message Queuing
	◆ Microsoft Active Directory Lightweight Directory Services roles
	◆ Remote Registry Service Started
	Microsoft Office 365/Exchange Online Administration:
	◆ Windows Azure Active Directory Module for Windows PowerShell
	◆ Microsoft Online Services Sign-In Assistant for IT Professionals
	◆ Skype for Business Online, Windows PowerShell Module
	For more information, see Supported Platforms.

Legacy Web Components	**Web Server:** ◆ Microsoft Internet Information Services (IIS) Versions 8.0, 8.5, 10 **Microsoft IIS Components:** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Microsoft IIS security Role Service **Windows DRA Interfaces:** ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

Account Requirements:

Account	Description	Permissions
AD LDS Group	The DRA service account needs to be added to this group for access to AD LDS	◆ Domain Local Security Group
DRA Service Account	The permissions required to run the NetIQ Administration Service	◆ “Distributed COM Users” Permissions ◆ Member of the AD LDS Admin Group ◆ Account Operator Group ◆ Log Archive groups (OnePointOp ConfgAdms & OnePointOp) **NOTE:** For more information on setting up least privilege domain access accounts see: Least Privilege DRA Access Accounts.
DRA Administrator	User account or Group provisioned to the built in DRA Admins role	◆ Domain Local Security Group or domain user account ◆ Member of the managed domain or a trusted domain ◆ If you specify an account from a trusted domain, ensure the Administration server computer can authenticate this account.
DRA Assistant Admin Accounts	Accounts that will be delegated powers though DRA	◆ Add all DRA Assistant Admin accounts to the “Distributed COM Users” group so that they can connect to the DRA Server from remote clients. **NOTE:** DRA can be configured to manage this for you during the installation.

Least Privilege DRA Access Accounts

Below are the permissions and privileges needed for the accounts specified and the configuration commands you need to run.

Domain Access Account: Assign the following Active Directory permissions to the Domain Access Account:

- FULL control over User objects
- FULL control over Computer objects
- FULL control over Group objects
- FULL control over Contact objects
- FULL control over Organization Unit objects
- FULL control over Inetorgperson objects
- FULL control over Printer objects
- FULL control over BuiltIn Domain objects

- FULL control over Container objects
- FULL control over MsExchSystemObjectContainer objects
- FULL control over Dynamic Distribution Groups
- FULL control over Public Folders

Specify the following privileges with a scope of “This object and all child objects” to the Domain Service Account:

- Allow create computer objects
- Allow delete computer objects
- Allow create contact objects
- Allow delete contact objects
- Allow create Group Objects
- Allow delete Group Objects
- Allow delete InetOrgPerson Objects
- Allow create Organization Unit Objects
- Allow delete Organizational Unit Objects
- Allow create User Objects
- Allow delete User Objects
- Allow create Dynamic Distribution Groups
- Allow delete Dynamic Distribution Groups
- Allow create Service Connection Point
- Allow delete Service Connection Point
- Allow create Container
- Allow delete Container
- Allow create Public Folders
- Allow delete Public Folders

Office 365 Tentant Access Account: Assign the following Active Directory permissions to the Office 365 Tenant Access Account:

- User Management Administrator in Office 365
- Recipient Management in Exchange Online

Exchange Access Account: Assign the **Organizational Management** role to the Exchange Access Account to manage Exchange 2010.

Skype Access Account: Ensure that this account is a Skype-enabled user and that is a member of at least one of the following:

- CSAdministrator role
- Both the CSUserAdministrator and CSArchiving roles

Public Folder Access Account: Assign the following Active Directory permissions to the Public Folder Access Account:

- Public Folder Management
- Mail Enabled Public Folders

Post DRA installation:

- Run the following command to delegate permission to the “Deleted Objects Container” from the DRA Installation folder (Note: the command must be executed by a domain administrator):

  `DraDelObjsUtil.exe /domain:<NetbiosDomainName> /delegate:<Account Name>`

- Run the following command to delegate permission to the “NetIQReceyleBin OU” from the DRA Installation folder (Note: this can be done only after adding the respective domains to be managed by DRA):

  `DraRecycleBinUtil.exe /domain:<NetbiosDomainName> /delegate:<AccountName>`

- Add the least privilege override account to the “Local Administrators” group on each computer that DRA will manage resources such as Printers, Services, Event Log, Devices and so forth.
- Grant the least privilege override account “Full Permission” on share folders or DFS folders where Home directories are provisioned.
- Add the least privilege override account to the “Organization Management” role to manage Exchange objects.

DRA Web Console and Extensions Requirements

Requirements for the Web Console and REST extensions include the following:

Software Requirements:

Component	Prerequisites
Installation Target	**Operating System:** ◆ Microsoft Windows Server 2016, Microsoft Windows 10, with Microsoft IIS 10 ◆ Microsoft Windows Server 2012, 2012 R2 with Microsoft IIS 8.0, 8.5
DRA Host Service	◆ Microsoft .Net Framework 4.5.2 ◆ DRA Administration Server
DRA REST Endpoint and Service	◆ Microsoft .Net Framework 4.5.2
PowerShell Extensions	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

Component	Prerequisites
DRA Web Console	**Web Server:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Services WCF (Activation) **Microsoft IIS Components:** ◆ Web Server ◆ Common HTTP Features ◆ Static Content ◆ Default Document ◆ Directory Browser ◆ HTTP Errors ◆ Application Development ◆ ASP ◆ Health and Diagnostics ◆ HTTP Logging ◆ Request Monitor ◆ Security ◆ Basic Authentication ◆ Performance ◆ Static Content Compression ◆ Web Server Management Tools

Reporting Requirements

Requirements for the DRA Reporting include the following:

Software Requirements:

Component	Prerequisites
Installation Target	**Operating System:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016

Component	Prerequisites
NetIQ Reporting Center (v3.2)	**Database:** ◆ Microsoft SQL Server 2012, 2014, 2016 ◆ Microsoft SQL Server Reporting Services **Web Server:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft IIS Components: ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** Every DRA Administration server that connects to DRA Reporting, also requires .NET Framework 3.5. **NOTE:** When installing the NetIQ Reporting Center (NRC) on a SQL Server computer, .NET Framework 3.5 may require a manual installation prior to installing NRC.
DRA Reporting	**Database:** ◆ Microsoft SQL Server Integration Services ◆ Microsofte SQL Server Agent

Licensing Requirements

Your license determines the products and features you can use. DRA requires a license key installed with the Administration Server.

After you install the Administration server, you may use the Health Check Utility to install a trial license key (License1.lic) that allows you to manage an unlimited number of user accounts and mailboxes for 30 days.

Refer to the product End User License Agreement (EULA) for additional information regarding license definition and restrictions.

Product Installation

This chapter guides you through installing the Directory and Resource Administrator. For more information on planning your install or upgrade, see Planning Your Deployment.

Install the DRA Administration Server

You can install the DRA Administration Server as either a primary or secondary node in your environment. The requirements for a primary and secondary administration server are the same, however, every DRA deployment must include one primary administration server.

Interactive Installation Checklist:

Step	Details
Log on to the target server	Log on to the target Microsoft Windows server for the install with an account that has local administrative privileges.
Copy and run the NetIQ Admin Installation Kit	Execute the DRA installation kit (NetIQAdminInstallationKit.msi) to extract the DRA installation media to the local file system. **NOTE:** The installation kit will install the .Net framework on the target server if needed.
Execute the DRA install	Launch the DRA install. **NOTE:** To run the install later, navigate to the location were the installation media was extracted and execute `Setup.exe`.
Select NetIQ Administratrion Server Component and the installation target	Choose the components to install and either accept the default installation location `C:\Program Files (x86)\NetIQ\DRA` or specify an alternate location for the install. Component options: **NetIQ Administration Server** ◆ Log Archive Resource Kit ◆ NetIQ DRA SDK **Legacy Web Component** **User Interfaces** ◆ Account and Resource Management ◆ DRA ADSI Provider ◆ Command-line Inerface ◆ Delegation and Configuration
Verify prerequisites	The **Prerequisites** dialog will display the list of required software based on the components selected for the installation. The installer will guide you though installing any missing prerequisites that are required for the install to complete successfully.
Accept the EULA license agreement	Accept the terms of the End User License Agreement.
Select the Server Operation Mode	Select **Primary** to install the first DRA Administration Server in a multi-master set (there will be only one primary in a deployment) or **Secondary** to join a new DRA Administration Server to an existing multi-master set. For information about multi-master set, see “What Is a Multi-Master Set?” in the *Directory and Resource Administrator Administrator Guide*.
Specify installation accounts and credentials	◆ DRA Service Account ◆ AD LDS Group ◆ DRA Administrator For more information see: DRA Administration Server Requirements.
Configure DCOM permissions	Enable DRA to configure “Distributed COM” access to authenticated users.

Step	Details
Configure ports	For more information on the default ports, see Required Ports and Protocols.
Specify storage location	Specify the local file location for DRA to use for storing audit and cache data.
Verify install configuration	You can verify the configuration on the installation summary page before clicking **Install** to proceed with the installation.
Post Install Verification	After the install has completed, the Health Checker will run to verify the install and update the product license.

Installing DRA Clients

You can install specific DRA consoles and command line clients by executing the DRAInstaller.msi with the corresponding .mst package on the installation target:

NetIQDRAUserConsole.mst	Installs the Account and Resource Management console
NetIQDRACLI.mst	Installs the command-line interface
NetIQDRAADSI.mst	Installs the DRA ADSI provider
NetIQDRAClients.mst	Installs all DRA user interfaces

To deploy specific DRA clients to multiple computers across your enterprise, configure a group policy object to install the specific .MST package.

1. Start Active Directory Users and Computers and create a group policy object.
2. Add the DRAInstaller.msi package to this group policy object.
3. Ensure this group policy object has one of the following properties:
   - Each user account in the group has Power User permissions for the appropriate computer.
   - Enable the Always Install with Elevated Privileges policy setting.
4. Add the user interface .mst file, such as NetIQDRAUserConsole.mst, to this group policy object.
5. Distribute your group policy.

NOTE: For more information about group policy, see Microsoft Windows Help. To easily and securely test and deploy group policy across your enterprise, use *Group Policy Administrator*.

Installing the DRA REST Extensions

The DRA REST Extensions package has four features:

- **NetIQ DRA Host Service:** Gateway used to communicate with the DRA Administration Service. This service must run on a computer with the DRA Administration Service installed.
- **DRA REST Service and Endpoints:** Provides the RESTful interfaces that enable the DRA Web Console and non-DRA clients to request DRA operations. This service must run on a computer with either a DRA console or the DRA Administration Service installed.
- **PowerShell Extensions:** Provides a PowerShell module that allows non-DRA clients to request DRA operations using PowerShell cmdlets.
- **DRA Web Console:** The web client interface that is primarily used by Assistant Administrators, but also includes customization options.

Step	Details
Log on to the target server	Log on to the target Microsoft Windows server for the install with an account that has local administrative privileges.
Install the SSL Certificate	If not already installed on the Windows server, you will need to have an SSL certificate installed before you run the installation.
Copy and run the NetIQ Admin Installation Kit	Copy the DRA installation kit `NetIQAdminINstallationKit.msi` to the target server and execute it by double-clicking the file or calling it from the command line. The installation kit will extract the DRA installation media to the local file system to a customizable location.
Execute the DRA REST Extensions Installer	After the DRA installation kit finishes extracting the installation media, it will prompt you to launch the DRA install. Navigate to the location were the installation media was extracted, right-click the `DRARESTExtensionsInstaller.exe` file, and select **Run as administrator**.
Accept the EULA license agreement	Accept the terms of the End User License Agreement.
Select Components and Specify the target location for the installation	From the Installation **Select Components** dialog, install all options: DRA Host Service, DRA REST Endpoints and service, PowerShell Extensions, and DRA Web Console. Either accept the default installation location `C:\Program Files (x86)\NetIQ\DRA Extensions` or specify an alternate location for the install.
Verify prerequisites	The **Prerequisites** dialog will display the list of required software based on the components selected for the installation. The installer will guide you though installing any missing prerequisites that are required for the install to complete successfully.
Specify the Service Account to Run As	By default the existing service account from DRA server is displayed. Specify the service account password. For more information on setting up a service account for the DRA Administration Server, see DRA Administration Server Requirements.
Specify REST Service SSL Certificate	Select the SSL certificate you will use for the REST service, and specify the REST and Host service ports.
Specify Web Console SSL Certificate	Specify the SSL certificate you will use for the HTTPS binding.
Verify install configuration	You can verify the configuration on the installation summary page before clicking **Install** to proceed with the installation.

Install the Workflow Server

For information about installing the Workflow Server, refer to the Aegis Administrator Guide.

Install DRA Reporting

DRA Reporting requires you to install two executable files from the NetIQ DRA Installation Kit: `NRCSetup.exe` and `DRAReportingSetup.exe`.

Steps	Details
Log on to the target server	Log on to the target Microsoft Windows server for the install with an account that has local administrative privileges. Ensure this account has local and domain administrative privileges as well as System Administrator privileges on the SQL Server.
Copy and run the NetIQ Admin Installation Kit	Copy the DRA installation kit `NetIQAdminINstallationKit.msi` to the target server and execute it by double-clicking the file or calling it from the command line. The installation kit will extract the DRA installation media to the local file system to a customizable location. In addition, the installation kit will install the .Net framework on the target server if needed to satisfy the DRA product installer pre-requisite.
Execute the NetIQ Reporting Center (NRC) Install	After the DRA installation kit finishes extracting the installation media, navigate to the location were the installation media was extracted and execute `NRCSetup.exe`.
Select NetIQ Reporting Center Component	From the Installation **Select Components** dialog, use the default “NetIQ Reporting Center” component to install the four NRC components.
Specify the target location for the installation	Either accept the default installation location `C:\Program Files (x86)\NetIQ\Reporting Center` or specify an alternate location for the install.
Verify and install prerequisites	The **Prerequisites** dialog will display the list of required software based on the components selected for the installation. The installer will guide you though installing any missing prerequisites that are required for the install to complete successfully. **IMPORTANT:** .NET Framework 3.5 must be manually installed on the Reporting server prior to installing NRC.
Accept the EULA license agreement	Accept the terms of the End User License Agreement.
Install the Configuration Database	Use the defaults in the **Configuration Database Installation - SQL Server Logon** dialog or provide the SQL authentication to complete the NRC installation. If you used the Default instance for the SQL Server installation, the Instance field should remain blank.
Execute the DRA Reporting install	Navigate to the location were the installation media was extracted and execute `DRAReportingSetup.exe` to install the managment component for DRA reporting integration.
Accept the EULA license agreement	Accept the terms of the End User License Agreement to finishing running the installation.

Product Upgrade

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 “Managing a Multi-Master Set” in the *Directory and Resource Administrator Administrator Guide*.

Planning a DRA Upgrade

Execute the `NetIQAdminInstallationKit.msi` to extract the DRA installation media and install and run the Health Check Utility.

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.
- Review Required Ports and Protocols.
- 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.
- 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.
- 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.

Pre-Upgrade Tasks

Before you start the upgrade installations, follow the pre-upgrade steps below to prepare each server set for upgrade.

Steps	Details
Backup the AD LDS instance	Open the Health Check Utility and run the **AD LDS Instance Backup** check to create a backup of your current AD LDS instance.
Make a deployment plan	Make a deployment plan for upgrading the Administration servers and user interfaces (AA client computers). For more information, see Planning a DRA Upgrade.
Dedicate a secondary server to run a previous DRA version	*Optional:* Dedicate a secondary Administration server to run a previous DRA version as you upgrade a site.
Make required changes for this MMS	Make any necessary changes to the delegation, configuration, or policy settings for this MMS. Use the primary Administration server to modify these settings.
Sychronize the MMS	Synchronize the server sets so each Administration server contains the latest configuration and security settings.
Back up the primary server registry	Back up the registry from the primary Administration server. Having a backup of your previous registry settings allows you to easily recover your previous configuration and security settings

NOTE: If you have cause to restore the AD LDS Instance backup, do the following:

1. Stop the current AD LDS Instance in Computer Management > Services. This will have a different title: `NetIQDRASecureStoragexxxxx`.
2. Replace the **current** `adamnts.dit` file with the **backup** `adamnts.dit` file as indicated below:
   - Current file location: `%ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/`
   - Backup file location: `%ProgramData%/NetIQ/ADLDS/`
3. Restart the AD LDS instance.

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. Right-click the `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` node, and select **Export**.
3. Specify the name and location of the file to save the registry key, and click **Save**.

Upgrade the DRA Administration Server

The following checklist guides you through the entire upgrade process. Use this process to upgrade each server set in your environment. If you have not done it yet, use the Health Check Utility to create a backup of your current AD LDS instance.

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.

Steps	Details
Run Health Check utility	Install the standalone DRA Health Check utility and run it using a service account. Fix any issues.
Perform a test upgrade	Perform a test upgrade in your lab environment to identify potential issues and minimize production downtime.
Determine order of upgrade	Determine the order in which you want to upgrade your server sets.

Steps	Details
Prepare each MMS for upgrade	Prepare each MMS for upgrade. For more information, see Pre-Upgrade Tasks.
Upgrade primary server	Upgrade the primary Administration server in the appropriate MMS.
Install new secondary server	*(Optional)* To minimize downtime at remote sites, install a local secondary Administration server running the newest version of DRA.
Deploy user interfaces	Deploy the user interfaces to your Assistant Administrators.
Upgrade secondary servers	Upgrade the secondary Administration servers in the MMS.
Upgrade DRA Reporting	Upgrade DRA Reporting.
Upgrade REST Extensions	Run the DRA REST Extensions installer.
Run Health Check utility	Run the Health Check Utility that was installed as part of the upgrade. Fix any issues.

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.

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.

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.

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 a DRA Upgrade.

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: You can not run multiple versions of DRA components side-by-side on the same DRA server. 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.

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 above 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 3.2. For more information on installation requirements and upgrade considerations, see the *NetIQ Reporting Center Reporting Guide*.

Steps	Details
Disable DRA Reporting Support	To ensure that the reporting collectors do not run during the upgrade process, disable DRA reporting support on the Reporting Service Configuration window in the Delegation and Configuration console.
Log on to the SQL instance server with applicable credentials	Log on to 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.
Run the DRA Reporting setup	Run `DRAReportingSetup.exe`. from the installation kit and follow the instructions in the installation wizard.
Run the NRC setup	*Conditional:* If your NRC web service is installed on a different computer, log on to the computer where the web service is installed, and run `NRCSetup.exe` to upgrade the NRC web service. **NOTE:** If the configuration database was installed on a separate server, it will need to be upgraded first
Run the NRC setup on client computers	Run `NRCSetup.exe` on all NRC client computers.
Enable DRA Reporting Support	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*.

Upgrade the DRA REST Extensions

In order to upgrade the Web Console and REST Extensions to Directory and Resource Administator 9.2, you must be using a DRA 9.0.1 or later version. For requirements information, see DRA Web Console and Extensions Requirements.

To upgrade the DRA Web Console and Extensions:

1. After downloading the DRA installation kit, navigate to the location were the installation media was extracted, right-click the `DRARESTExtensionsInstaller.exe` file, and select **Run as administrator**.
2. Follow the instructions in the install wizard until the installation completes, and click **Finish**.

For more detailed information about the steps in the the install wizard, refer to the steps for a new installation: Installing the DRA REST Extensions.

Upgrade Custom Content

When you upgrade to a newer version of DRA, you want to retain all of the customizations you have made for the Web Console on the web server. To make this easier, DRA has a Customization Upgrade utility that is built-in to the DRA REST Extensions installer. This utility runs automatically when you run `DRARESTExtensionsInstaller.exe` to upgrade REST Extensions on the web server. You can also re-run the utiltity manually from the DRA installation directory outside of the installation.

Part of the process of the Customization Upgrade utility is to back up your customizations before the upgrade starts. During the upgrade process, the utility creates a log file of all the changes made due to the upgrade and also includes a warning for any customization items that cannot be updated automatically.

As a best practice, we recommend that you review the log after the upgrade. If needed, you can roll back to the pre-upgrade customizations by copying them from the backup folder. You can define the folder path for the upgraded customizations when the Customization Upgrade utility opens, or you can use the default path, which auto-fills.

The default paths for upgraded customizations and the customizations backup are provided below:

- Default CustomFolderPath: `C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom`
- Default Backup Folder:

  `$CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup`

3 Product Configuration

This chapter outlines the required configuration steps and procedures if you are installing Directory and Resource Administrator for the first time.

Configuration Checklist

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

Steps	Details
Apply a DRA license	Use the Health Check Utility to apply a DRA license. For more information about DRA licenses, see Licensing Requirements.
Open Delegation and Configuration	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	Add the first managed domain to DRA. **NOTE:** You can start delegating powers after the initial Full Account Refresh completes.
Add managed domains and subtrees	*Optional:* Add additional managed domains and subtrees to DRA. For more information about managed domains, see Adding Managed Domains.
Configure DCOM Settings	*Optional:* Configure DCOM settings. For more information about DCOM settings, see Configuring DCOM Settings.
Configure Delegation and Configuration	Connect to servers, add managed domains, and customize the Delegation and Configuration Console.
Configure Office 365, Skype for Business, and Skype Online	*Optional:* Configure Office 365, Skype for Business, and Skype Online.

Steps	Details
Customize DRA	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.
Configure and customize the Web Console	Configure the Web Console for Smart Card and multi-factor authentication and customize console branding.
Configure Policies	Configure policies for Microsoft Exchange, Office 365, Home directory, password generation, and built-in policies for groups, user accounts, and computers.
Configure Audits and Reports	Enable Event Log auditing, reporting, and data collection, and learn how to access user Change History.

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 “Configuring Managed and Trusted Domains” in the *Directory and Resource Administrator Administrator Guide*.

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 “Deleted Objects Utility” in the *Directory and Resource Administrator Adminstrator Guide*.

For more information about setting up the access account, see “Specifying Domain Access Accounts” in the *Directory and Resource Administrator Adminstrator Guide*.

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 From the Start menu, go to **Settings > System and Security > Control Panel**.

2 Open Administrative Tools, and then 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 trial 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.