NetIQ Directory and Resource Administrator

Installation Guide

April 2022

Legal Notice

Contents

About this Guide

The *Installation Guide* provides planning, installation, licensing, and configuration information for the NetIQ Directory and Resource Administrator (DRA) and its integrated components.

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

Intended Audience

This book provides information for anyone installing DRA.

Additional Documentation

This guide is part of the NetIQ Directory and Resource Administrator documentation set. For the most recent version of this guide and other DRA documentation resources, visit the DRA Documentation website (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at https://www.microfocus.com/support-and-services/.

Getting Started

Before you install and configure all of the components of Net IQ 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 architecture.

1 What is Directory and Resource Administrator

NetIQ Directory and Resource Administrator (DRA) 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.

DRA also extends the powerful features of Microsoft Exchange to provide seamless management of Exchange objects. Through a single, common user interface, DRA delivers policy-based administration for the management of mailboxes, public folders and distribution lists across your Microsoft Exchange environment.

DRA provides the solutions you need to control and manage your Microsoft Active Directory, Windows, Exchange, and Azure Active Directory environments.

- **Support for Azure and on-premises Active Directory, Exchange, and Skype for Business:**

  Delivers administrative management of Azure and on-premises Active Directory, on-premises Exchange Server, on-premises 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.

2 Understanding Directory and Administrator Components

The components of DRA that you will consistently use to manage privileged access include primary and secondary servers, administrator consoles, reporting components, and the Workflow Automation 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
Advanced Administrator	DRA Reporting Center Setup (NRC) PowerShell *(optional)* CLI *(optional)* DRA ADSI Provider *(optional)*	Any DRA server
Help Desk Occasional Administrator	Web Console	Any DRA server

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, Azure Active Directory, etc.).
- **Account and Resource Management:** Enables DRA assistant administrators to view and manage delegated objects of connected domains and services from the Delegation and Configuration Console.

Web Console

The Web Console is a web-based user interface that provides quick and easy access to 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.

Reporting Components

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

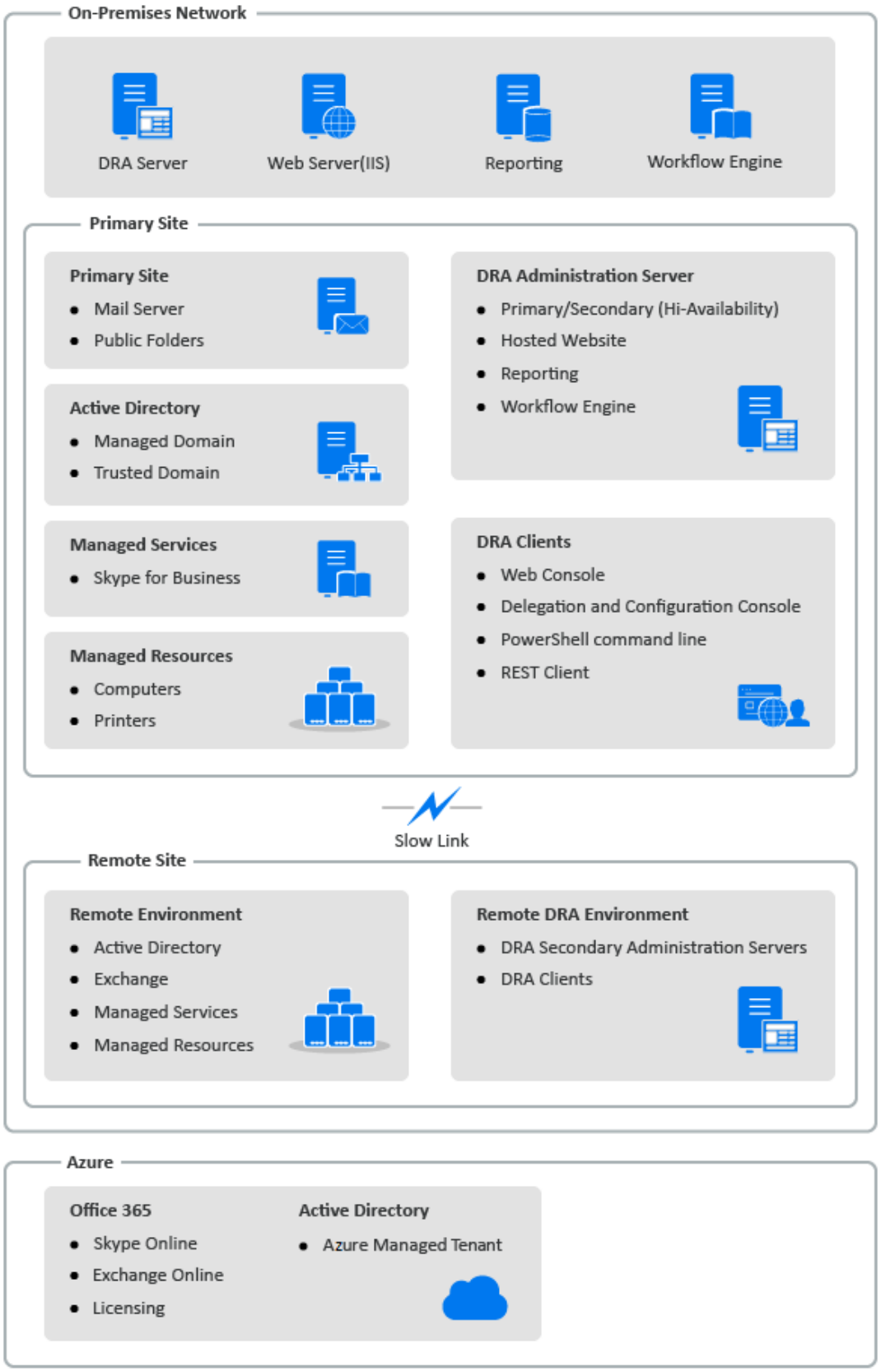
- Resources reports for Active Directory objects
- Active Directory object data reports
- Active Directory summary reports
- DRA configuration reports
- Exchange configuration reports
- Office 365 Exchange Online reports
- Detailed activity trends reports (By month, domain, and peak)
- Summarized DRA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

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

Workflow Automation Engine

DRA integrates with the Workflow Automation 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 Automation Engine, see the DRA Documentation site.

Product Architecture



II 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.

3 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	8 CPU/cores 2.0 GHz	16 GB	120 GB
DRA Web Console	2 CPU/cores 2.0 GHz	8 GB	100 GB
DRA Reporting	4 CPU/cores 2.0 GHz	16 GB	100 GB
DRA Workflow Server	4 CPU/cores 2.0 GHz	16 GB	120 GB

Virtual Environment Resource Provisioning

DRA keeps large memory segments active for extended periods of time. When provisioning resources for a virtual 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 asterisk *
- Ports requiring a certificate are indicated with two asterisks **

Component tables:

- "DRA Administration Servers" on page 18
- "DRA REST Server" on page 20
- "Web Console (IIS)" on page 20
- "DRA Delegation and Administration Console" on page 20
- "Workflow Server" on page 21

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	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*.
TCP 50000 *	Bi-directional	DRA Administration Servers	Attribute replication and DRA server-AD LDS communication. (LDAP)
TCP 50001 *	Bi-directional	DRA Administration Servers	SSL attribute replication (AD LDS)
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

Protocol and Port	Direction	Destination	Usage
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 2013 and later (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
TCP 5984	Localhost	DRA Administration Servers	IIS access to the Replication Service to support temporary group assignments
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
TCP 8898	Bi-directional	DRA Administration Servers	DRA Replication Service communication between DRA servers for temporary group assignments
TCP 636	Outbound	Microsoft Active Directory domain controllers	Active Directory object management (LDAP SSL).

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 135	Outbound	Microsoft Active Directory domain controllers	Autodiscovery using Service Connection Point (SCP)
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, and DRA PowerShell
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* (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* (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) and (HTTPS)
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 Automation 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 product page.

Managed System	Prerequisites
Azure Active Directory	To enable Azure administration, you must install the following PowerShell modules: ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 version or later ◆ AzureRM.Profile 5.8.2 version or later ◆ Exchange Online PowerShell V2 1.0.1 or later PowerShell 5.1 or the latest module is required to install the new Azure PowerShell modules.

Managed System	Prerequisites
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype for Business	◆ Microsoft Skype for Business 2015
Change History	◆ Change Guardian 5.1 or later
Databases	◆ Microsoft SQL Server 2016
Web Browsers	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019

DRA Administration Server and Web Console Requirements

DRA components require the following software and accounts:

- "Software Requirements" on page 23
- "Server Domain" on page 24
- "Account Requirements" on page 24
- "Least Privilege DRA Access Accounts" on page 26

Software Requirements

Component	Prerequisites
Installation Target	**NetIQ Administration Server Operating System:**
Operating System	◆ Microsoft Windows Server 2012 R2, 2016, 2019 **NOTE:** The server must also be a member of a supported Microsoft on-premises Active Directory domain. **DRA Interfaces:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019
Installer	◆ Microsoft .Net Framework 4.8 and above
Administration Server	**Directory and Resource Administrator:** ◆ Microsoft .Net Framework 4.8 and above ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages (x64 and x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory Lightweight Directory Services roles ◆ Remote Registry Service Started ◆ Microsoft Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services application request routing **NOTE:** DRA REST Endpoint and Service is installed with the Administration Server. **Microsoft Office 365/Exchange Online Administration:** ◆ Windows Azure Active Directory Module for Windows PowerShell ◆ Windows PowerShell Module ◆ Exchange Online PowerShell V2 module ◆ Enable WinRM for Basic authentication on the client-side for Exchange Online tasks. For more information, see Supported Platforms.
User Interface	**DRA Interfaces:** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages (x64 and x86)
PowerShell Extensions	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 or later

Component	Prerequisites
DRA Web Console	**Web Server:** ◆ Microsoft .Net Framework 4.x > WCF Services > HTTP Activation ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services application request routing

Server Domain

Component	Operating Systems
DRA Server	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

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

Account	Description	Permissions

DRA Service Account	The permissions required to run the NetIQ Administration Service	◆ For “Distributed COM Users” Permissions
		◆ Member of the AD LDS Admin Group
		◆ Account Operator Group
		◆ Log Archive groups (OnePointOp ConfgAdms & OnePointOp)
		◆ One of the following Account tab > **Account options** must be selected for the DRA service account user if installing DRA on a server using STIG methodology:
		  ◆ Kerberos AES 128 bits encryption
		  ◆ Kerberos AES 256 bits encryption
		NOTE
		◆ For more information on setting up least privilege domain access accounts see: Least Privilege DRA Access Accounts.
		◆ For more information on setting up a group Managed Service Account for DRA see: “Configuring DRA Services for a Group Managed Service Account” in the *DRA Administrator Guide*.

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 through 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. It is required only when you are using thick client or the Delegation and Configuration console. **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: Using ADSI Edit grant the Domain Access account the following Active Directory Permissions at the top domain level for the following descendant object types:

- FULL control over builtInDomain objects
- FULL control over Computer objects
- FULL control over Connection Point objects
- FULL control over Contact objects
- FULL control over Container objects
- FULL control over Group objects
- FULL control over InetOrgPerson objects
- FULL control over MsExchDynamicDistributionList objects
- FULL control over MsExchSystemObjectsContainer objects
- FULL control over msDS-GroupManagedServiceAccount objects
- FULL control over Organizational Unit objects
- FULL control over Printer objects
- FULL control over publicFolder objects
- FULL Control over Shared Folder objects
- FULL control over User objects

Grant the Domain Access account the following Active Directory Permissions at the top domain level to this object and all descendant objects:

- Allow create Computer objects
- Allow create Contact objects
- Allow create Container objects
- Allow create Group objects
- Allow create MsExchDynamicDistributionList objects
- Allow create msDS-GroupManagedServiceAccount objects
- Allow create Organizational Unit objects
- Allow create publicFolders objects
- Allow create Shared Folder objects
- Allow create User objects
- Allow delete Computer objects
- Allow delete Contact objects
- Allow delete Container
- Allow delete Group objects
- Allow delete InetOrgPerson objects

- Allow delete MsExchDynamicDistributionList objects
- Allow delete msDS-GroupManagedServiceAccount objects
- Allow delete Organizational Unit objects
- Allow delete publicFolders objects
- Allow delete Shared Folder objects
- Allow delete User objects

NOTE

- By default, some Builtin container objects within Active Directory do not inherit permissions from the top level of the domain. For this reason those objects will require inheritance to be enabled, or explicit permissions to be set.
- If you use the least privilege account as the access account, ensure that the account is assigned the “Reset Password” permission for itself in Active Directory for the password reset to be successful in DRA.

Exchange Access Account: To manage on-premises Microsoft Exchange objects, assign the Organizational Management role to the Exchange Access Account and the Exchange Access Account to the Account Operators group.

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

Azure Tenant Access Account: Assign the following Azure Active Directory permissions to the Azure Tenant Access Account:

- Distribution Groups
- Mail Recipients
- Mail Recipient Creation
- Security Group Creation and Membership
- (Optional) Skype for Business Administrator

  If you want to manage Skype for Business Online, assign the Skype for Business Administrator power to the Azure tenant access account.
- User Administrator

NetIQ Administration Service Account Permissions:

- Local Administrators

- Grant the least privilege override account “Full Permission” on share folders or DFS folders where Home directories are provisioned.
- **Resource Management**: To manage published resources within a managed Active Directory domain, the Domain Access account must be granted local administration permissions on those resources.

Post DRA installation: You must run the following commands before you manage the required domains:

- 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>`

- To delegate permission to the “NetIQReceyleBin OU” from the DRA Installation folder:

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

Remote Access to SAM: Assign Domain Controllers or member servers managed by DRA to enable the accounts listed in the GPO setting below, so they can make remote queries to the Security Account Manager's (SAM) database. The configuration needs to include the DRA service account.

Network access: Restrict clients allowed to make remote calls to SAM

To access this setting, do the following:

1. Open the Group Policy Management console on the domain controller.
2. Expand **Domains** > **[domain controller]** > **Group Policy Objects** in the node tree.
3. Right-click **Default Domain Controllers Policy** and select **Edit** to open the GPO editor for this policy.
4. Expand **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** in the node tree of the GPO editor.
5. Double-click **Network access: Restrict clients allowed to make remote calls to SAM** in the policies pane, and select **Define this policy setting**.
6. Click **Edit Security** and enable **Allow** for Remote Access. Add the DRA service account if it is not already included as a user or part of the administrators group.
7. Apply the changes. This will add the security descriptor, `O:BAG:BAD:(A;;RC;;;BA)` to the policy settings.

For more information, see Knowledge Base article 7023292.

Reporting Requirements

Requirements for the DRA Reporting include the following:

Software Requirements

Component	Prerequisites
Installation Target	**Operating System:** ◆ Microsoft Windows Server 2012 R2, 2016, 2019
NetIQ Reporting Center (v3.3)	**Database:** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ The Domain administrator who manages SQL Agent jobs requires security permissions for Microsoft SQL Server Integration Services or some NRC reports may not be processed. **Web Server:** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft IIS Components: ◆◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ Required to run the NRC installer ◆ Also required on the DRA Primary Server for the DRA Reporting Services configuration **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. **Communication Security Protocol:** ◆ SQL Server must support TLS 1.2. For more information, see TLS 1.2 support for Microsoft SQL Server. ◆ SQL Server must have an updated TLS supported driver installed on the DRA server. The suggested driver is the latest Microsoft® SQL Server® 2012 Native Client - QFE ◆ The same TLS protocol version must be supported in the operating system of both SQL Server and the DRA Administration Server. For example, only TLS 1.2 has been enabled.
DRA Reporting	**Database:** ◆ Microsoft SQL Server Integration Services ◆ Microsoft 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 can use the Health Check Utility to install your purchased license. A trial license key (TrialLicense.lic) is also included in the installation package that enables 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.

4 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.

The DRA server package has the following features:

- **Administration Server:** Stores configuration data (environmental, delegated access, and policy), executes operator and automation tasks, and audits system-wide activity. It has the following features:
  - **Log Archive Resource Kit:** Enables you to view audit information.
  - **DRA SDK:** Provides the ADSI sample scripts and helps you to create your own scripts.
  - **Temporary Group Assignments:** Provides the components to enable synchronization of Temporary Group Assignments.
- **User Interfaces:** The web client interface that is primarily used by assistant administrators, but also includes customization options.
  - **ADSI Provider:** Enables you to create your own policy scripts.
  - **Command-line Interface:** Enables you to perform DRA operations.
  - **Delegation and Configuration:** Enable system administrators access to DRA configuration and administration functions. Also, enables you to granularly specify and assign access to managed resources and tasks to assistant administrators.
  - **PowerShell Extensions:** Provides a PowerShell module that allows non-DRA clients to request DRA operations using PowerShell cmdlets.
  - **Web Console:** The web client interface that is primarily used by assistant administrators, but also includes customization options.

For information about installing specific DRA consoles and command line clients on multiple computers, see Install the DRA Clients.

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 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.
Install DRA	Click **Install DRA** and **Next** to see the installation options. **NOTE:** To run the install later, navigate to the location where the installation media was extracted (View Installation Kit), and execute `Setup.exe`.
Default Installation	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 installation. Component options: **Administration Server** ◆ Log Archive Resource Kit (Optional) ◆ DRA SDK ◆ Temporary Group Assignments **User Interfaces** ◆ ADSI Provider (Optional) ◆ Command-line Interface (Optional) ◆ Delegation and Configuration ◆ PowerShell Extensions ◆ Web Console
Verify prerequisites	The **Prerequisites List** dialog will display the list of required software based on the components selected for the installation. The installer will guide you through 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.
Specify log location	Specify a location for DRA to store all the log files. **NOTE:** The Delegation and Configuration Console logs and ADSI logs are stored in the user-profile folder.
Select the Server Operation Mode	Select **Primary Administration Server** to install the first DRA Administration Server in a multi-master set (there will be only one primary in a deployment) or **Secondary Administration Server** to join a new DRA Administration Server to an existing multi-master set. For information about multi-master set, see “Configuring the Multi-Master Set” in the *DRA Administrator Guide*.

Step	Details
Specify installation accounts and credentials	◆ DRA Service Account ◆ AD LDS Group ◆ DRA Administrator Account For more information see: DRA Administration Server and Web Console Requirements.
Configure DCOM permissions	Enable DRA to configure “Distributed COM” access to authenticated users.
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.
Specify DRA replication database location	◆ Specify the file location for the DRA replication database and the replication service port. ◆ Specify the SSL certificate that you want to use for secure communications with the database through IIS, and specify the IIS replication port.
Specify REST Service SSL Certificate	Select the SSL certificate you will use for the REST service, and specify the REST service port.
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.
Post Install Verification	After the install has completed, the Health Checker will run to verify the install and update the product license. For more information, see “Health Check Utility” in the *DRA Administrator Guide*.

Install 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:

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, 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*.

Install Workflow Automation and Configure Settings

To manage Workflow Automation requests in DRA you need to do the following:

- Install and configure Workflow Automation and the DRA Adapter.

  For information see, the *Workflow Automation Administrator Guide* and the *Workflow Automation Adapter Reference for DRA*.

- Configure Workflow Automation integration with DRA.

  For information, see “Configuring the Workflow Automation Server” in the *DRA Administrator Guide*.

- Delegate Workflow Automation powers in DRA.

  For information, see “Delegating Workflow Automation Server Configuration Powers” in the *DRA Administrator Guide*.

The documents referenced above are available on the DRA Documentation site.

Install DRA Reporting

DRA Reporting requires you to install the DRAReportingSetup.exe file from the NetIQ DRA Installation Kit.

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 meet the requirements of the DRA product installer pre-requisite.
Execute the DRA Reporting install	Navigate to the location were the installation media was extracted and execute DRA`ReportingSetup.exe` to install the management component for DRA reporting integration.

Steps	Details
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. For information about NetIQ Reporting Center, see *Reporting Center Guide* on the documentation web site.
Accept the EULA license agreement	Accept the terms of the End User License Agreement to finishing running the installation.

5 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 “Configuring the Multi-Master Set” in the *DRA 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 assistant administrators rely on each MMS. If the majority of your assistant administrators rely on specific servers or server sets, upgrade those servers first during off-peak hours.
- Determine which assistant administrators need the Delegation and Configuration console. You can obtain this information in one of the following ways:
  - Review which assistant administrators are associated with the built-in assistant administrator groups.
  - Review which assistant administrators 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 assistant administrators about your upgrade plans for the user interfaces.
- Determine which assistant administrators need to connect to the primary Administration server. These assistant administrators should upgrade their client computers once you upgrade the primary Administration server.

Notify these assistant administrators 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.

IMPORTANT

- If your previous DRA version has the Account and Resource Management (ARM) console installed, the ARM console will be removed during the upgrade.
- When you upgrade the DRA Server from a DRA 9.x version, it removes any managed tenants from DRA. To continue using these tenants using Azure, you need to add the tenants after upgrade. For information about adding tenants, see "Creating an Azure Application and Adding an Azure Tenant" in the *DRA Administrator Guide*.
- Because Exchange 2010 it is not supported in DRA 10.1, Exchange gets disabled when upgrading from DRA 9.x. To continue to perform Exchange operations after upgrade, disable and re-enable the **Enable Exchange Policy** option in the Delegation and Configuration Console. Both changes need to be "applied" to reset the policy.

  For information on this policy configuration, see "Enabling Microsoft Exchange" in the *DRA Administrator Guide*.

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 (assistant administrator 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.
Synchronize the MMS	Synchronize the server sets so each Administration server contains the latest configuration and security settings.

Steps	Details
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.
Convert gMSA to DRA user accounts	*Optional:* If you are using a group Managed Service Account (gMSA) for the DRA Service account, change the gMSA account to a DRA user account prior to upgrade. Post upgrade, you will need to change the account back to a gMSA.

NOTE: If you need to restore the AD LDS Instance, 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.

Pre-upgrade topics:

- "Dedicating a Local Administration Server to Run a Previous DRA Version" on page 39
- "Synchronizing Your Previous DRA Version Server Set" on page 40
- "Backing Up the Administration Server Registry" on page 41

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 assistant administrators 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 assistant administrators, 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 assistant administrators 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 assistant administrators 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 assistant administrators 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. Open the Delegation and Configuration Console and expand **Configuration Management**.
3. Click **Administration servers**.
4. In the right pane, select the appropriate primary Administration server for this server set.
5. Click **Properties**.
6. On the Synchronization schedule tab, click **Refresh Now**.
7. 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**.

Upgrading 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.

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

You can spread the 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.

IMPORTANT: The DRA upgrade installation makes the following changes when you upgrade the DRA Server from a DRA 9.x version to a DRA 10.x version:

- Moves the UCH and Workflow Automation server user configurations from the Web Console to the Delegation and Configuration Console
- Removes the old Web component from the server.
- Removes any managed tenants.

For information about adding tenants, see "Configuring Azure Tenants" in the *DRA Administrator Guide*.

- If you have installed the Account and Resource Management Console in earlier release and when you upgrade to a DRA 10.x version, the Account and Resource Management console will be removed.
- During an MMS upgrade, the primary server is upgraded first, followed by the secondary servers. For the successful replication of temporary group assignments in the secondary server, run the **Multi-master synchronization schedule** manually or wait for its scheduled run.
- Because Exchange 2010 it is not supported in DRA 10, Exchange gets disabled when upgrading from DRA 9.x. To continue to perform Exchange operations after upgrade, disable and re-enable the **Enable Exchange Policy** option in the Delegation and Configuration Console. Both changes need to be "applied" to reset the policy.

  For information on this policy configuration, see "Enabling Microsoft Exchange" in the *DRA Administrator Guide*.

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.
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. For information, see Upgrading the Primary Administration Server.
Install new secondary server	*(Optional)* To minimize downtime at remote sites, install a local secondary Administration server running the newest version of DRA. For information, see Installing a Local Secondary Administration Server for the Current DRA Version.
Deploy user interfaces	Deploy the user interfaces to your assistant administrators. For information, see Deploying the DRA User Interfaces
Upgrade secondary servers	Upgrade the secondary Administration servers in the MMS. For information, see Upgrading Secondary Administration Servers.
Upgrade DRA Reporting	Upgrade DRA Reporting. For information, see Upgrading Reporting.
Run Health Check utility	Run the Health Check Utility that was installed as part of the upgrade. Fix any issues.
Add Azure tenants *(post upgrade)*	(*Optional, post upgrade)* If you were managing any Azure tenants pre-upgrade, the tenants get removed during upgrade. You will need add those tenants again and run a full accounts cache refresh from the Delegation and Configuration Console. For more information, see "Configuring Azure Tenants" in the *DRA Administrator Guide*.

Steps	Details
Update Web Console configuration *(post upgrade)*	*(Conditional, post upgrade)* If you have either of the Web Console configurations below before upgrade, they will need to be updated after the upgrade installation completes: ◆ Default server connections enabled ◆ Modified configuration files For more information, see Updating the Web Console Configuration - Post Installation.

Server upgrade topics:

Upgrading the Primary Administration Server

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

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

Before you upgrade, notify your assistant administrators 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 assistant administrators 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 assistant administrators 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 assistant administrators, 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 assistant administrators from either site to use a previous DRA version as well as the current DRA version until the upgrade is complete. Additionally, your assistant administrators 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 assistant administrators 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, the ADSI provider, PowerShell, 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 assistant administrators install the DRA user interfaces or deploy these interfaces through group policy. You can also easily and quickly deploy the Web Console to multiple assistant administrators.

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 assistant administrator 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 assistant administrators who use this server to install the appropriate user interfaces, such as the Web Console.
3. Repeat steps 1 and 2 above until you completely upgrade the MMS.

Before you upgrade, notify your assistant administrators 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 assistant administrators can continue using the previous DRA version during the upgrade. When you complete the upgrade process for this MMS, and all assistant administrator client computers are running upgraded user interfaces, take any remaining previous DRA version servers offline.

Updating the Web Console Configuration - Post Installation

Perform either or both of the actions below, post upgrade installation, if they are applicable to your DRA environment:

Default DRA Server Connection

The DRA REST Service component is consolidated with the DRA Server beginning in DRA 10.1. If you have the default DRA Server connection configured prior to upgrade from a DRA 10.0.x or earlier version, you need to review those settings post upgrade as there is now only one connection configuration, the DRA Server Connection. You can access this configuration in the Web Console at **Administration** > **Configuration** > **DRA Server Connection**.

You can also update these settings post upgrade in the `web.config` file at `C:\inetpub\wwwroot\DRAClient\rest` on the DRA Web Console server, as follows:

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Web Console Login Configuration

When upgrading from DRA 10.0.x or earlier versions, if the DRA REST Service is installed without the DRA Server, uninstalling the DRA REST Service is a prerequisite for upgrade. A copy of files that were modified before the upgrade are made to `C:\ProgramData\NetIQ\DRA\Backup\` on the server. You can use these files for reference to update any relevant ones after the upgrade.

Upgrading Workflow Automation

To perform an in-place upgrade on non-clustered 64-bit environments, simply run the Workflow Automation setup program on your existing Workflow Automation computers. It is not necessary to stop any Workflow Automation services that may be running.

Any Workflow Automation adapters that are not built-in to the Workflow Automation installer, must be uninstalled and reinstalled post upgrade.

For more detailed information about upgrading Workflow Automation, see “Upgrading from a Previous Version” in the *Workflow Automation Administrator Guide*.

Upgrading Reporting

Before you upgrade DRA Reporting, ensure that your environment meets the minimum requirements for NRC 3.3. 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 DRA`ReportingSetup.exe`. from the installation kit and follow the instructions in the installation wizard.
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 *Reporting Center Guide* on the documentation web site.

III Product Configuration

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

6 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 domain controllers and Administration servers	Configure the client computer running the Delegation and Configuration console for each domain controller and each Administration server. For more information, see Configuring the Domain Controller and Administration Server.
Configure DRA Services for a gMSA	*Optional:* Configure DRA services for a Group Managed Service Account (gMSA). For more information, see Configuring DRA Services for a Group Managed Service Account.

7 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 your purchased license. If needed, a trial license key file (`TrialLicense.lic`) is also provided with the installation package that enables you to manage an unlimited number of user accounts and mailboxes for 30 days.

To upgrade an existing or trial license, open the Delegation and Configuration console, and navigate to **Configuration Management** > **Update License**. When you upgrade your license, upgrade the license file on each Administration server.

8 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 Caching” in the *DRA Administrator Guide*.

---

9 Adding Managed Subtrees

You can add managed or missing subtrees from specific Microsoft Windows domains after you install the Administration server. These functions are executed in the Delegation and Configuration console from the **Configuration Management** > **Managed Domains** node. 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 *DRA Administrator Guide*.

For more information about setting up the access account, see “Specifying Domain Access Accounts” in the *DRA Administrator 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 “Configuring Caching” in the *DRA Administrator Guide*.

---

10 Configuring DCOM Settings

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

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, all Assistant Admins, and the account used to manage DRA REST, DRA Host, and DRA Admin services.

To configure the Distributed COM Users group:

1. Log on to a DRA Administration 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**.

11 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 **Control Panel** > **System and Security**.
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.

12 Configuring DRA Services for a Group Managed Service Account

If required, you can use a group Managed Service Account (gMSA) for DRA services. For more information about using a gMSA, see the Microsoft reference *Group Managed Service Accounts Overview*. This section explains how to configure DRA for a gMSA after adding the account to Active Directory.

IMPORTANT: Do not use the gMSA as a service account while installing DRA.

To configure the DRA Primary Administration server for a gMSA:

1. Add the gMSA as a member of the following groups:
   - Local Administrators group on the DRA server
   - AD LDS group in the DRA managed domain
2. Change the logon account in service Properties for each of the services below to the gMSA:
   - NetIQ Administration Service
   - NetIQ DRA Audit Service
   - NetIQ DRA Cache DB Service

     NetIQ DRA Cache Service
   - NetIQ DRA Core Service
   - NetIQ DRA Log Archive
   - NetIQ DRA Replication Service
   - NetIQ DRA Rest Service
   - NetIQ DRA Skype Service
3. Restart all the services.
4. Delegate the "Audit all objects" role to the gMSA by running the following command:

   ```
   Add-DRAAssignments -Identifier "All Objects" -Users "CN=<gMSA_name>
   ,CN=Managed Service Accounts,DC=MyDomain,DC=corp"  -Roles "Audit All
   Objects"
   ```

To configure a DRA secondary administration server for a gMSA:

1. Install the secondary server.
2. On the primary server, assign the **Configure Servers and Domains** role to the **Administration Servers and Managed Domains** ActiveView for the secondary server's service account.
3. On the primary server, add a new secondary server and specify the secondary server service account.

4. Add the gMSA to the local administrators group on the DRA Secondary Administration server.
5. On the secondary server, change the logon account of all the DRA services to the gMSA and then re-start the DRA services.