

NetIQ Identity Manager Standard Edition Quick Start Guide

February 2017



This document provides guidelines to install, configure, and upgrade Identity Manager 4.6 Standard Edition.

1 Overview

Identity Manager 4.6 Standard Edition provides the following features:

- ♦ Rule-based automated provisioning
- ♦ Password management (Self Service Password Reset)
- ♦ Identity Reporting
- ♦ Content packaging framework
- ♦ Single sign-on (One SSO)
- ♦ Analyzer
- ♦ Designer

For more information, see the [NetIQ Identity Manager Setup Guide](#).

IMPORTANT: Although Identity Manager 4.6 Advanced and Standard Editions are bundled in the same ISO file, there is no change to the existing licensing model. Also, the integration modules continue to remain the same for both editions.

For information about new features, enhancements, and features that have changed or are no longer supported in this version, see the

2 Components

Identity Manager 4.6 Standard Edition includes the following components:

- ♦ Identity Vault
- ♦ iManager
- ♦ Identity Manager Engine
- ♦ Designer
- ♦ Analyzer
- ♦ Remote Loader
- ♦ Sentinel Log Management for Identity Governance and Administration (IGA)
- ♦ Tomcat (supported application server)
- ♦ Single Sign-on (One SSO)
- ♦ Self Service Password Reset (SSPR)
- ♦ Identity Reporting

To learn about the interaction among Identity Manager components, see [Introduction](#) in the *NetIQ Identity Manager Setup Guide*.

3 Installing Identity Manager 4.6 Standard Edition

Download the software from the [Product Web site](#). The following .iso files contain the DVD image for installing the Identity Manager components:

- ♦ Identity_Manager_4.6_Linux.iso
- ♦ Identity_Manager_4.6_Windows.iso

The installation files are located in the products directory in the Identity Manager installation package. For information about the default installation locations, see [NetIQ Identity Manager 4.6 Release Notes](#).

NetIQ recommends that you review the [Installation Prerequisites](#) in the [NetIQ Identity Manager 4.6 Release Notes](#) and then run the below checklist in the given sequence. Each task provides brief information and a reference to where you can find complete details. For specific details about installing each Identity Manager component, see the component installation sections.

Task	Notes
1. Prerequisites	♦ Review the system requirements for each component to ensure that your computer or virtual images meet the installation prerequisites. For specific information about which component can be installed on which operating system, see Selecting an Operating System Platform for Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i>. ♦ For information about prerequisites, computer requirements, installation, upgrade, or migration, see Considerations and Prerequisites for Installation in the <i>NetIQ Identity Manager Setup Guide</i>.
2. Plan your installation	See Planning to Install Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i> .
3. Order of installation	Ensure that you install the components in the following order because the installation programs for some components require information about previously installed components. 1. eDirectory 2. Sentinel Log Management for Identity Governance and Administration (IGA) 3. Identity Manager Engine 4. iManager 5. Apache Tomcat and PostgreSQL Identity Manager provides a convenience installer to install these components. 6. Single Sign-on 7. Password Management 8. Designer 9. Identity Reporting 10. Analyzer

Task	Notes
4. Install and configure eDirectory	Install eDirectory 8.8.8 Patch 9 Hotfix 2 or eDirectory 9.0.2 Hotfix 2. For installation instructions, see Installing the Identity Vault in the <i>NetIQ Identity Manager Setup Guide</i>. ◆ After installing and configuring eDirectory, stop eDirectory services. ◆ Apply the latest released eDirectory patch. ◆ Start the eDirectory services.
5. Install Sentinel Log Management for IGA	For installation instructions, see Installing and Managing Sentinel Log Management for Identity Governance and Administration in the <i>NetIQ Identity Manager Setup Guide</i>.
6. Install Identity Manager Engine, Drivers, and Plug-ins	For installation instructions, see Installing the Identity Manager Engine, Drivers, and Plug-ins in the <i>NetIQ Identity Manager Setup Guide</i>. NOTE: The installation program does not create the DirMXL-PasswordPolicy object in the Identity Vault. After installing the Identity Manager engine, launch Designer and create the driver set. Install the Identity Manager Default Universal Password Policy package that contains DirMXL-PasswordPolicy. Add this policy to the driver set. Do this for each Identity Manager driver set in the Identity Vault.
7. Install and configure iManager	Install iManager 2.7.7.8.1 or iManager 3.0.2.1 version that is compatible with your installed eDirectory version. For installation instructions, see Installing iManager in the <i>NetIQ Identity Manager Setup Guide</i>.
8. Install Tomcat and PostgreSQL	Select Tomcat for deploying Identity Reporting. identity Reporting will use the PostgreSQL database for storing the reporting data. For audit-based reports, configure Sentinel Log Management for IGA to forward events to the reporting database. For installation instructions, see Installing PostgreSQL and Tomcat for Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i>. NOTE: If you are installing Tomcat on a computer that has iManager installed, do not use port 8080 for Tomcat. If other ports are already in use, change them during installation.
9. Install the Single Sign-on Component	For installation instructions, see Installing Single Sign-on for Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i>.

Task	Notes
10. Install the Password Management Component	For installation instructions, see Installing the Password Management Component in the <i>NetIQ Identity Manager Setup Guide</i>. After installing the Password Management component, do the following actions: ♦ Extend the eDirectory schema. This task allows you to extend your eDirectory schema with the object class and attribute definitions. - Copy the following content to a file and save it as a .ldif file. <pre>dn: o="Your Organization" changetype: modify add: ACL ACL: 7#subtree#[This]#pwmResponseSet</pre> - In iManager, go to Roles and Task > Schema > Extend Schema > Import data from file on disk and click Next. - Click File to Import and browse to the .ldif file. Verify that this file contains Organization container name as o="Your Organization"; otherwise add the existing Organization container name and click Next. - Specify values for the following fields, then click Next and Finish. ♦ Server DNS Name/ IP Address ♦ Authentication login ♦ User DN ♦ Password NOTE: The LDAP server does not accept a non-secure connection by default. You can either use SSL authentication or change the server settings to allow clear text connections. After the file import is complete, the window displays a message about the success of the import. ♦ Set up SSL auditing. If you enabled auditing during SSPR installation, SSPR requires SSL certificate to audit the events. For instructions about importing the SSL certificate and auditing the events, see Setting Up SSL Auditing in the <i>NetIQ Self Service Password Reset Administration Guide</i>.
11. Install and configure Identity Reporting	- For general information about the components and framework required for Identity Reporting, see Installing the Identity Reporting Components in the <i>NetIQ Identity Manager Setup Guide</i>. - For installing Identity Reporting using an installation wizard, either in GUI format or from the console, see Section 3.1, "Installing Identity Reporting," on page 5. - For performing a silent installation, see Section 3.1.2, "Installing Identity Reporting Silently," on page 10. - For configuring the drivers, see Managing the Drivers for Reporting in the <i>NetIQ Identity Manager Setup Guide</i>. - For deploying REST APIs for Identity Reporting, see Deploying REST APIs for Identity Reporting in the <i>NetIQ Identity Manager Setup Guide</i>. NOTE: You must import the report definitions into Identity Reporting. To download them, use the Download page within the Reporting application.

Task	Notes
12. (Conditional) Configure Data Synchronization Policy in Sentinel Log Management for IGA	If you need audit-based reports, configure the Data Synchronization Policy in Sentinel Log Management for IGA to forward events to the reporting database.
13. Activating Identity Manager	Activate your Identity Manager components. For more information, see Activating Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i> .

3.1 Installing Identity Reporting

The Identity Manager installation package includes the installation files in the products/Sentinel and products/Reporting directories within the .iso image file. By default, the installation program installs the components in the following locations:

- ♦ **Linux:** /opt/netiq/idm/apps/IDMReporting
- ♦ **Windows:** C:\netiq\idm\apps\IDMReporting

3.1.1 Using the Guided Process to Install Identity Reporting

The following procedure describes how to install Identity Reporting by using an installation wizard, either in GUI format or from the console.

To prepare for the installation, review the prerequisites and system requirements listed in “[System Requirements for Identity Reporting](#)” in the *NetIQ Identity Manager Setup Guide* and the [Release Notes](#).

- 1 In case of a fresh installation, the installation program creates tables in the database and verifies connectivity. The program also installs a JAR file for the PostgreSQL JDBC driver, and automatically uses this file for database connectivity.
If you have migrated your data, for example, SIEM, from EAS to PostgreSQL database, then the installation program will connect to the existing database.
- 2 Log in to the computer where you want to install Identity Reporting.
- 3 Stop the application server. In this case, it is Tomcat.
- 4 (Conditional) If you have the .iso file for the Identity Manager installation package, navigate to the directory containing the installation files for Identity Reporting, located by default in the products/Reporting/ directory.
- 5 (Conditional) If you downloaded Identity Reporting installation files from the [NetIQ Downloads website](#), complete the following steps:
 - 5a Navigate to the .tgz file for the downloaded image.
 - 5b Extract the contents of the file to a folder on the local computer.
- 6 From the directory that contains the installation files, complete one of the following actions:
 - ♦ **Linux (console):** Enter `./rpt-install.bin -i console`
 - ♦ **Linux (GUI):** Enter `./rpt-install.bin`
 - ♦ **Windows:** Run `rpt-install.exe`
- 7 In the installation program, specify the language that you want to use for installation, and then click OK.
- 8 Review the Introduction text, and then click Next.

- 9 Accept the License Agreement, and then click Next.
- 10 To complete the guided process, specify values for the following parameters:
- ♦ **Installation folder**
Specifies the location for the installation files.
 - ♦ **Reporting Setup**
Select Identity Manager and specify the hostname and port to establish an LDAP connection to the eDirectory server over SSL. The default port is 636. To modify these settings after installation, use the Reporting Configuration utility (`configupdate.sh`) located in the `/opt/netiq/idm/apps/IdentityReporting/bin/lib` directory.
Identity Vault server
Specifies the DNS name or IP address of the Identity Vault server.
Secure LDAP port
Specifies the LDAP port that you want Identity Reporting to use for communication with the Identity Vault.
 - ♦ Specify the URL for the landing page.
 - ♦ **Application Server Details**
Represents the application server that you want to run Identity Reporting. The application server must already be installed.
For your convenience, NetIQ provides Tomcat.
Secondary
Specifies if you want to set the local application server instance as the secondary node in a cluster.
Tomcat root folder
Specifies a path to the deployment or webapps directory of the Tomcat instance. For example, `/opt/netiq/idm/apps/tomcat/webapps`.
Java JRE Base folder
Specifies the path a path to the JRE folder. The path contains the ConfigUpdate utility file and is used to launch this utility after Identity Reporting is installed.
 - ♦ **Application Address**
Represents the settings of the URL that users need to connect to Identity Reporting on the application server. For example, `https:myserver.mycompany.com:8443`.

NOTE: If OSP runs on a different instance of the application server, you must also select **Connect to an external authentication server** and specify the values for the OSP server.

Protocol

Specifies whether you want to use *http* or *https*. To use SSL for communication, specify *https*.

Host name

Specifies the DNS name or IP address of the application server. Do not use `localhost`.

Port

Specifies the port that you want the application server to use for communication with Identity Manager.

Connect to an external authentication server

Specifies whether a different instance of the application server hosts the authentication server (OSP). The authentication server contains the list of users who can log in to Identity Reporting.

If you select this setting, also specify values for the authentication server's Protocol, Host name, and Port.

♦ **Authentication Server Details**

Specifies the password that you want to create for the Identity Reporting service to use when connecting to the OSP client on the authentication server.

To modify this password after installation, use the Reporting Configuration utility.

♦ **Database details**

Represents the settings for connecting to your database.

Database name

Specifies the name of the database. The default value is 15432.

DBA host

Specifies the DNS name or IP address of the database.

DBA type

Specifies the type of the database. For example, PostgreSQL or Oracle. You need to specify the JDBC jar file if you are using a database type other than PostgreSQL.

Share password

Specifies the password to connect to the database.

Specify password for each user

Specifies the password for each database account. You can use same the same password for all database accounts or different passwords for each account.

Configure database now or at startup

Specify whether you want to create and configure the database now or later. To configure the database now, specify the name and password of the administrative account for the SIEM database server.

For example, postgres

Generate SQL for later

Specifies whether you want to generate SQL later.

Target locale

Specifies the language that you want to use for Identity Reporting. The application uses the specified locale in searches.

♦ **Identity Vault Credentials**

Represents the Identity Vault credentials for the Identity Vault server.

Identity Vault Administrator

Specifies the DN of the admin user who has the authority to grant and revoke roles from other users.

Identity Vault Administrator Password

Specifies the password of the admin user.

Keystore Path

Specifies the path of a keystore file that contains the certificates to trust in SSL connections. By default, it is the same path that is created by the OSP and SSPR installer.

Keystore Password

Specifies the password for opening the keystore file. The default password is *changeit*.

Report Admin Role Container DN

Specifies the DN of the container where the installer will create the reportAdmin role.

Report Admin User DN

Specifies the DN of the user that the installer will assign the reportAdmin role.

NOTE: Ensure that the container where the reportAdmin role resides does not include any object with the same name.

Default email address

Specifies the email address that you want Identity Reporting to use for sending email notifications.

SMTP server

Specifies the IP address or DNS name of the SMTP email host that Identity Reporting uses for notifications. Do not use `localhost`.

SMTP server port

Specifies the port number for the SMTP server. The default value is 465.

Use SSL for SMTP

Specifies whether you want to use SSL protocol for communication with the SMTP server.

Require server authentication

Specifies whether you want to use authentication for communication with the SMTP server.

If you select this setting, also specify the credentials for the email server.

♦ Email Delivery

Represents the settings for the SMTP server that sends report notifications. To modify these settings after installation, use the Reporting Configuration utility.

Default email address

Specifies the email address that you want Identity Reporting to use as the origination for email notifications.

SMTP server

Specifies the IP address or DNS name of the SMTP email host that Identity Reporting uses for notifications. Do not use `localhost`.

SMTP server port

Specifies the port number for the SMTP server. The default port is 465.

Use SSL for SMTP

Specifies whether you want to use SSL protocol for communication with the SMTP server.

Require server authentication

Specifies whether you want to use authentication for communication with the SMTP server.

If you select this setting, specify the following credentials for the email server.

- ♦ ***SMTP user name***

Specify the name of an login account for the SMTP server.

- ♦ ***SMTP password***

Specify the password of a login account for the SMTP server.

- ♦ **Report Details**

Represents the duration for keeping the reports in the database.

Keep finished reports for

Specifies the amount of time that Identity Reporting will retain completed reports before deleting them. For example, to specify six months, enter 6 and then select Month.

Location of report definitions

Specifies the path where you want to store the report definitions. For example, /opt/netiq/IDMReporting.

- ♦ **Novell Identity Audit**

Represents the settings for auditing activity in Identity Reporting.

Enable auditing for Identity Reporting

Specifies whether you want to send log events to an auditing server.

If you select this setting, also specify the location for the audit log cache.

Audit server

Specifies the host name of the auditing server, that is, the IP where Sentinel is hosted.

Audit log cache folder

Applies only when you enable auditing for Identity Reporting.

Specifies the location of the cache directory that you want to use for auditing. For example, /opt/novell/Identity Reporting.

NOTE: If you enable auditing, ensure that the logevent file has valid paths for the cache directory and the nauditpa.jar file. If these settings are not defined correctly, Identity Reporting will not start.

- ♦ **NAudit Certificates**

Represents the settings for enabling auditing for Identity Reporting.

Specify existing certificate / Generate a certificate

Specifies whether to use an existing certificate for the NAudit server or create a new certificate.

Enter Public key

Applies only when you want to use an existing certificate.

Specifies the custom public key certificate that the NAudit service will use to authenticate audit messages.

Enter RSA Key

Applies only when you want to use an existing certificate.

Specifies the path to the custom private key file that the NAudit service will use to authenticate audit messages.

NOTE: Ensure that the logevent file has valid paths for the cache directory and nauditpa.jar file. If these settings are not defined correctly, Identity Reporting will not start.

- 11 Review the information in the Pre-Installation Summary window, and then click Install.

3.1.2 Installing Identity Reporting Silently

A silent (non-interactive) installation does not display a user interface or prompts any questions to the user. Instead, the system uses information from a `.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

To prepare for the installation, review the prerequisites and system requirements listed in [System Requirements for Identity Reporting](#) in the *NetIQ Identity Manager Setup Guide* and the *NetIQ Identity Manager 4.6 Release Notes*.

- 1 (Conditional) To avoid specifying the administrator passwords for the installation in the `.properties` file for a silent installation, use the `export` or `set` command. For example:

- ♦ **Linux:** `export NOVL_ADMIN_PWD=myPassword`
- ♦ **Windows:** `set NOVL_ADMIN_PWD=myPassword`

The silent installation process reads the passwords from the environment, rather than from the `.properties` file.

Specify the following passwords:

NETIQ_DB_RPT_USER_PASSWORD

Specifies the password for the administrator for the SIEM database.

NETIQ_IDM_SRV_PWD

Specifies the password for the owner of the database schemas and objects for reporting.

NETIQ_IDM_USER_PWD

Specifies the password for the `idmrptuser` that has read-only access to reporting data.

NETIQ_ADMIN_PWD

(Conditional) To enable subcontainer searches at login time, specifies the password of an LDAP administrator.

NETIQ_SMTP_PASSWORD

(Conditional) To use authentication for email communications, specifies the password for the default SMTP email user.

- 2 To specify the installation parameters, complete the following steps:
 - 2a Ensure that the `.properties` file is located in the same directory as the execution file for installation.

For your convenience, NetIQ provides two `.properties` files, located by default in the `products/Reporting` directory of the `.iso` image:

 - ♦ `rpt_installonly.properties` to use the default installation settings
 - ♦ `rpt_configonly.properties` to customize the installation settings
 - 2b In a text editor, open the `.properties` file.

- 2c Specify the parameter values. For a description of the parameters, see [Step 10 on page 6](#).
- 2d Save and close the file.
- 3 To launch the installation process, enter one of the following commands:
 - ♦ **Linux:** `./rpt-install.bin -i silent -f path_to_properties_file`
 - ♦ **Windows:** `./rpt-install.exe -i silent -f path_to_properties_file`

NOTE: If the `.properties` file resides in a different directory from the installation script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

3.1.3 Post-Installation Tasks

- ♦ To modify installation properties after installation, run the configuration update utility depending on your platform.
 - ♦ **Linux:** Run `configupdate.sh` from `/opt/netiq/idm/apps/IDMReporting/bin/lib`.
 - ♦ **Windows:** Run `configupdate.bat` from `C:\netiq\idm\apps\IDMReporting\bin`.

If you change any setting for Identity Reporting with the configuration tool, you must restart the application server for the changes to take effect. However, you do not need to restart the server after making changes in the web user interface for Identity Reporting.

- ♦ Access the Reporting URL as a Report Administrator. The URL will follow this pattern: `http://server:port/IDMRPT/`. Ensure that authentication and authorization is successful. NetIQ recommends that you do not attempt logging in without sufficient administrative rights.

IMPORTANT: If you logged in to the Reporting application with a user with no rights, the logout option and Home link are not displayed.

4 Upgrading Identity Manager

NetIQ supports the following upgrade paths for upgrading to Identity Manager 4.6 Standard Edition:

- ♦ Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Standard Edition
- ♦ Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Advanced Edition

You cannot perform a direct upgrade from Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Advanced Edition. However, you can choose one of the following approaches to complete the upgrade:

- ♦ Upgrade Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Standard Edition and then upgrade to Identity Manager 4.6 Advanced Edition.
- ♦ Upgrade Identity Manager 4.5 Standard Edition to Identity Manager 4.5 Advanced Edition and then upgrade to Identity Manager 4.6 Advanced Edition.

4.1 Upgrading Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Standard Edition

To perform the upgrade, NetIQ recommends that you review the [Upgrade Prerequisites](#) in the Release Notes and then complete the following tasks in the same sequence:

Task	Notes
1. Review the differences between an upgrade and a migration	For more information, See Understanding Upgrade and Migration in the <i>NetIQ Identity Manager Setup Guide</i> .
2. Upgrade from Identity Manager 4.0.2	You cannot directly upgrade or migrate to version 4.6 from versions before 4.5. For more information, see the <i>NetIQ Identity Manager Setup Guide 4.5</i> .
3. Get the files needed for upgrade/migrate	Ensure that you have the latest installation kit to upgrade/migrate Identity Manager to 4.6 Standard Edition.
4. Interaction among Identity Manager components	For more information, see Introduction in the <i>NetIQ Identity Manager Setup Guide</i> .
5. System requirements	Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Considerations and Prerequisites for Installation in the <i>NetIQ Identity Manager Setup Guide</i> and the accompanying Release Notes.
6. Back up the current project, driver configuration, and databases	For more information, see Backing Up the Current Configuration in the <i>NetIQ Identity Manager Setup Guide</i> .
7. Upgrade Analyzer	Upgrade Designer to the latest version. For more information, see Upgrading Analyzer in the <i>NetIQ Identity Manager Setup Guide</i> .
8. Upgrade Designer	Upgrade Designer to the latest version. For more information, see Upgrading Designer in the <i>NetIQ Identity Manager Setup Guide</i> .
9. Upgrade eDirectory	On the server running Identity Manager, upgrade eDirectory to the latest version and patch. For more information, see the <i>NetIQ eDirectory Installation Guide</i> and <i>NetIQ Identity Manager 4.6 Release Notes</i> .
10. Upgrade iManager	Upgrade iManager to the latest version and patch. For upgrade instructions, see Upgrading iManager in the <i>NetIQ Identity Manager Setup Guide</i> .
11. Stop the drivers	Stop the drivers that are associated with the server where you installed the Identity Manager engine. For more information, see Stopping and Starting Identity Manager Drivers during Migration in the <i>NetIQ Identity Manager Setup Guide</i> .
12. Upgrade the Identity Manager engine	For more information, see Upgrading the Identity Manager Engine in the <i>NetIQ Identity Manager Setup Guide</i> . NOTE: If you are migrating the Identity Manager engine to a new server, you can use the same eDirectory replicas that are on the current Identity Manager server. For more information, see Migrating Identity Manager to a New Server in the <i>NetIQ Identity Manager Setup Guide</i> .
13. (Conditional) Upgrade Remote Loader	If any of the drivers in the driver set for the Identity Manager Engine are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see Upgrading the Remote Loader in the <i>NetIQ Identity Manager Setup Guide</i> .

Task	Notes
14. (Conditional) Upgrade the packages	If you are using packages instead of driver configuration files, upgrade the packages on the existing drivers to get new policies. For more information, see Upgrading the Identity Manager Drivers in the <i>NetIQ Identity Manager Setup Guide</i>. This is only required if a newer version of a package is available and there is a new functionality included in the policies for a driver that you want to add to your existing driver.
15. Apply Identity Manager 4.6 Standard Edition activation key	In iManager, make sure that you apply the Identity Manager 4.6 Standard Edition activation. If you do not apply the activation, the Identity Manager engine and the drivers run in the evaluation mode.
16. Install Identity Reporting components	Install Identity Reporting components. This requires you to take the following actions: 1. Install Sentinel. For more information, see Installing and Managing Sentinel Log Management for Identity Governance and Administration in the <i>NetIQ Identity Manager Setup Guide</i>. 2. (Conditional) Migrate the existing data from EAS to Sentinel. For more information, see Migrating from Event Auditing Service to Sentinel Log Management for IGA in the <i>NetIQ Identity Manager Setup Guide</i>. 3. Install Tomcat and PostgreSQL. For more information, see Installing PostgreSQL and Tomcat for Identity Manager in the <i>NetIQ Identity Manager Setup Guide</i>. 4. Install and configure NetIQ One SSO Provider (OSP). For more information, see Installing the Single Sign-on Component in the <i>NetIQ Identity Manager Setup Guide</i>. 5. Install and configure Self Service Password Reset (SSPR). For more information, see Installing the Password Management Component in the <i>NetIQ Identity Manager Setup Guide</i>. 6. Install Identity Reporting. During installation, specify the DNS name or IP address of the Sentinel Log Management for IGA server if you choose to use it as your auditing server. For more information, see Installing Identity Reporting in the <i>NetIQ Identity Manager Setup Guide</i>. 7. (Conditional) Update the Data Collection Service driver configuration for your new application server (Tomcat).
17. Start the drivers	Start the drivers associated with the Identity Reporting and the Identity Manager engine. For more information, see Starting the Drivers in the <i>NetIQ Identity Manager Setup Guide</i> .
18. (Conditional) Restore your custom settings	If you have custom policies and rules, restore your custom settings. For more information, see Restoring Custom Policies and Rules to the Driver in the <i>NetIQ Identity Manager Setup Guide</i> .
19. (Conditional) Upgrade Sentinel	If you are using NetIQ Sentinel, ensure that you are running the latest service pack. For more information about upgrading Sentinel, see the <i>NetIQ Sentinel Installation and Configuration Guide</i> .

4.2 Upgrading Identity Manager 4.6 Standard Edition to Identity Manager 4.6 Advanced Edition

Upgrading Identity Manager 4.6 Standard Edition to Identity Manager 4.6 Advanced Edition involves configuration changes for the Identity Manager components. You do not need to run the Identity Manager installation program to perform this upgrade.

The Identity Manager 4.6 Advanced Edition includes all the features included in the Standard Edition along with additional features such as identity applications. The [NetIQ Identity Manager 4.6 Release Notes](#) includes brief summaries of the new features in Identity Manager 4.6. You might want to take a few minutes to look at the section.

To perform the upgrade, NetIQ recommends that you complete the steps in the below checklist in the given order:

Task	Description
1. Review the differences between an upgrade and a migration	Review the differences between an upgrade and a migration. For more information, see Understanding Upgrade and Migration in the <i>NetIQ Identity Manager Setup Guide</i> .
2. Upgrade to Identity Manager 4.6 Standard Edition	You cannot upgrade or migrate to version 4.6 from versions before 4.5. For more information, see the NetIQ Identity Manager Setup Guide 4.5 .
3. Get the files needed for upgrade/migrate	Ensure that you have the latest installation kit to upgrade Identity Manager to 4.6 Advanced Edition.
4. Learn about the interaction among Identity Manager components	For more information, see Introduction in the <i>NetIQ Identity Manager Setup Guide</i> .
5. System requirements	Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Considerations and Prerequisites for Installation in the <i>NetIQ Identity Manager Setup Guide</i> and the Release Notes for the version to which you want to upgrade.
6. Stop the application server where Identity Reporting is installed	Stop Tomcat.
7. Uninstall Identity Reporting	Uninstall the Identity Reporting WAR files from your application server. To do this, follow the instructions in the documentation specific to your application server. For more information, see Uninstalling the Identity Reporting in the <i>NetIQ Identity Manager Setup Guide</i> .
8. Apply the Identity Manager 4.6 Advanced Edition activation key	In iManager, ensure that you apply the Identity Manager 4.6 Advanced Edition activation key. Otherwise, the Identity Manager engine upgrade does not proceed.
9. Create and deploy the User Application, Roles and Resource Service, and the Managed System Gateway drivers	For more information, see Creating and Deploying the Drivers for the Identity Applications in the <i>NetIQ Identity Manager Setup Guide</i> .
10. (Conditional) Install the application server	Install Tomcat as your application server. You can reuse the existing instance of Tomcat.

Task	Description
11. Install and configure the identity applications	NOTE: The upgrade process does not remove the existing roles assigned to users in eDirectory. If the Report Administrator user role still exists in the upgraded software, make sure you delete this role for security reasons. The installation program will install the following components: ♦ Catalog Administrator ♦ Home and Provisioning Dashboard ♦ Roles Based Provisioning Module (RBPM) For more information, see Installing the Identity Applications in the <i>NetIQ Identity Manager Setup Guide</i>.
12. Start the application server	Start Tomcat.
13. (Conditional) Update the Data Collection Service driver configuration	Update the Data Collection Service driver configuration for your new application server. Update the Data Collection Service driver configuration to register the Managed System Gateway driver. For more information, see Section 4.3, "Updating the Configuration Information of the Data Collection Service Driver," on page 16.
14. Upgrade Identity Reporting Components	Provide the existing auditing server details during the installation. For more information, see Upgrading Identity Reporting in the <i>NetIQ Identity Manager Setup Guide</i>. To log the Identity Reporting events in the auditing server, perform the following actions: 1. Stop the application server. For example, <code>/etc/init.d/idmapps_tomcat_init stop</code> 2. Stop the audit thread by running the following command: <pre>ps -eaf grep naudit</pre> 3. Enable Reporting to utilize auditing. a. (Optional) Update the ConfigUpdate utility to run in GUI mode. b. Launch the ConfigUpdate utility and select the Reporting tab. c. Select the Enable auditing checkbox. If it is already selected, de-select it, click OK. d. Launch the ConfigUpdate utility again and select the Reporting tab. e. Select the Enable auditing checkbox and click OK. 4. Start the application server. For example, <code>/etc/init.d/idmapps_tomcat_init start</code>
15. Start the drivers	Start the drivers associated with Identity Reporting and the Identity Manager engine. For more information, see Managing the Drivers for Reporting in the <i>NetIQ Identity Manager Setup Guide</i> .
16. (Conditional) Restore your custom settings	If you have custom policies and rules, restore your custom settings. For more information, see Restoring Custom Policies and Rules to the Driver in the <i>NetIQ Identity Manager Setup Guide</i> .

Task	Description
17. (Conditional) Upgrade Sentinel	(Conditional) If you are using NetIQ Sentinel, ensure that you are running the latest service pack. For more information about upgrading Sentinel, see the NetIQ Sentinel Installation and Configuration Guide .

4.3 Updating the Configuration Information of the Data Collection Service Driver

- 1 Launch Designer, then go to **DCS Driver Configuration > Driver Parameters > Driver Options**.
- 2 In the Managed System Gateway Registration section, change the settings as below:
 - ♦ Set **Register Manage System Gateway** to **Yes**.
 - ♦ Change the MSGW Driver DN. For example, CN=Managed System Gateway Driver,cn=driverset1,o=system.
 - ♦ Change the User DN. For example, cn=admin,ou=sa,o=system.
 - ♦ Specify the password for the User DN.
- 3 Save the settings, then deploy the DCS driver.
- 4 Restart the DCS driver.

Upgrading the Identity Reporting might not immediately show the Advanced Version. The version change occurs after the next batch of events is processed.

5 Uninstalling Identity Manager 4.6 Standard Edition

Some components of Identity Manager have prerequisites for uninstallation. Ensure that you review full section for each component before beginning the uninstallation process. For more information, see [Uninstalling Identity Manager Components](#) in the [NetIQ Identity Manager Setup Guide](#).

6 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <http://www.netiq.com/company/legal/> (<http://www.netiq.com/company/legal/>).

Copyright (C) 2017 NetIQ Corporation. All rights reserved.