Quick Start Guide for Installing and Upgrading NetIQ Identity Manager 4.7 Standard Edition

February 2018

Introduction

This document provides guidelines to install and configure Identity Manager 4.7 Standard Edition, and upgrade to this version.

Overview

Identity Manager 4.7 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 installing Identity Manager Standard Edition, see the setup guide for your platform:

- *NetIQ Identity Manager Setup Guide for Linux*
- *NetIQ Identity Manager Setup Guide for Windows*

IMPORTANT: Identity Manager 4.7 Advanced and Standard Editions are bundled in the same ISO file. 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 NetIQ Identity Manager 4.7 Release Notes.

Prerequisites

For general prerequisites, see Considerations for Installing Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Linux* or “Prerequisites for Installing the Identity Reporting Components” in the *NetIQ Identity Manager Setup Guide for Windows*.

The Report Admin role must exist in the Identity Vault and assigned to any users that you want to access the reporting functionality. Ensure that the container where the this role resides does not include any object with the same name. This role is automatically created by the Identity Manager installer for Windows. On Linux, manually create the role and then assign it to a user that you want to access the reporting functionality. For more information, see “Creating and Assigning rptadmin Role to a User on Linux” on page 6. If you completed the installation without creating this role, run the Configuration Update utility (configupdate.sh) to create the role after completing the Identity Reporting installation.

Installing Identity Manager 4.7 Standard Edition on Linux

Download the software from the Product Web site. The `Identity_Manager_4.7_Linux.iso` file contains the DVD image for installing the Identity Manager components on Linux:

The installation files are located in the `mnt` directory in the Identity Manager installation package. For information about the default installation locations, see NetIQ Identity Manager 4.7 Release Notes.

NetIQ recommends that you review the installation prerequisites in the installation guide for your platform and then run the installation 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 in the *NetIQ Identity Manager Setup Guide for Linux*.

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 Identity Manager 4.7 Technical Information page. ◆ For information about prerequisites, computer requirements, installation, upgrade, or migration, see Planning to Install Identity Manager and planning information for each component in the *NetIQ Identity Manager Setup Guide for Linux*.
2. Plan your installation	See Planning to Install Identity Manager in the *NetIQ Identity Manager Setup Guide for Linux*.
3. Order of installation and/or configuration	Ensure that you install the components in the following order because the installation programs for some components require information about previously installed components. 1. Sentinel Log Management for Identity Governance and Administration (IGA) 2. Identity Manager Engine components 3. Self-Service Password Reset 4. Identity Reporting components (also installs single sign-on component) 5. Designer for Identity Manager 6. Analyzer for Identity Manager
4. (Conditional) Install Sentinel Log Management for IGA	If you need audit-based reports, configure the Data Synchronization Policy in the Identity Manager Data Collection Services page to forward events to the reporting database. (This web page has been added in this version.) For installation instructions, see Installing Sentinel Log Management for Identity Governance and Administration in the *NetIQ Identity Manager Setup Guide for Linux*.

Task	Notes
5. Install Identity Manager Server, Password Management Component, and Identity Reporting Components	From the root directory of the `.iso` file, run the following command to install Identity Manager server and Identity Reporting components: `./install.sh` When prompted, specify a value to install the required components. For more information, see one of the following resources in the *NetIQ Identity Manager Setup Guide for Linux*. ◆ Performing an Interactive Installation ◆ Performing a Silent Installation Identity Manager provides a separate installation program for installing SSPR. For installation instructions, see Installing SSPR or see Performing a Silent Installation of SSPR in the *NetIQ Identity Manager Setup Guide for Linux*. **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. The Identity Reporting installation process installs the authentication service for reporting. It also deploys a special API WAR file, `rptdoc.war`, which contains the documentation of REST services needed for reporting. The `rptdoc.war` is automatically deployed on your application sever when Identity Reporting is installed. After completing the reporting installation, assign the Report Administrator role to a user that you want to access reporting functionality. For more information, see "Creating and Assigning rptadmin Role to a User on Linux" on page 6. **NOTE:** You must import the report definitions into Identity Reporting. To download them, use the Download page within the Reporting application.

Task	Notes
6. Configure the installed components (Identity Manager Engine, Password Management Component, and Identity Reporting Components)	Configure Identity Manager server and Identity Reporting components by running `configure.sh`, located in the root of the `.iso` image file of the Identity Manager installation package. Before beginning the configuration process for all components, review the configuration options from Understanding the Configuration Parameters in the *NetIQ Identity Manager Setup Guide for Linux*. **NOTE:** If Identity Manager engine is already configured, the configuration script prompts you to specify Identity Vault information for the following parameters while configuring Identity Reporting: `Identity Vault hostname/IP address`, `Identity Vault Administrator name`, and `Identity Vault Administrator password`. For configuring SSPR, see Configuring SSPR in the *NetIQ Identity Manager Setup Guide for Linux*.
7. Install Designer	From the root directory of the `Identity_Manager_Linux_LDAP_Designer.tar.gz` file, run one of the following commands: ◆ **Console:** `./install` ◆ **GUI:** `./install -i console` Follow the prompts and complete the installation. For more information, see Installing Designer in the *NetIQ Identity Manager Setup Guide for Linux*.
8. Install Analyzer	From the root directory of the `Identity_Manager_Linux_Analyzer.tar.gz` file, run one of the following commands: ◆ **Console:** `./install` ◆ **GUI:** `./install -i console` Follow the prompts and complete the installation. For more information, see Installing Analyzer in the *NetIQ Identity Manager Setup Guide for Linux*.
9. Activating Identity Manager	Activate your Identity Manager components. For more information, see Activating Identity Manager in the *NetIQ Identity Manager Setup Guide for Linux*.

Installing Identity Manager 4.7 Standard Edition on Windows

Download the software from the Product Web site. The `Identity_Manager_4.7_Windows.iso` file contains the DVD image for installing the Identity Manager components.

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 4.7 Release Notes.

NetIQ recommends that you review the installation prerequisites in the installation guide for your platform 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 in the *NetIQ Identity Manager Setup Guide for Windows*.

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 Identity Manager 4.7 Technical Information (https://www.netiq.com/Support/identity-manager/SP_IDM_Components.asp) page. ◆ For information about prerequisites, computer requirements, installation, upgrade, or migration, see Considerations for Installing Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Windows*.
2. Plan your installation	See Planning to Install Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*.
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
4. Install and configure eDirectory	Install eDirectory 9.1. For installation instructions, see Installing the Identity Vault in the *NetIQ Identity Manager Setup Guide for Windows*.

Task	Notes
5. Install Identity Manager Engine, Drivers, and Plug-ins	For installation instructions, see Installing the Engine, Drivers, and iManager Plug-ins in the *NetIQ Identity Manager Setup Guide for Windows*. **NOTE:** The installation program does not create the DirMXL-PasswordPolicy object in the Identity Vault. After installing 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.
6. Install and configure iManager	Install iManager 3.1. For installation instructions, see Installing iManager in the *NetIQ Identity Manager Setup Guide for Windows*.
7. 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 in the *NetIQ Identity Manager Setup Guide for Windows*. **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.
8. Install the Single Sign-on Component	For installation instructions, see Installing Single Sign-on for Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*.

Task	Notes

9. Install the Password Management Component	For installation instructions, see Installing Password Management for Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*.
	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.
	1. Copy the following content to a file and save it as a `.ldif` file.
	`dn: o="Your Organization"`
	
	`changetype: modify`
	`add: ACL`
	`ACL: 7#subtree#[This]#pwmResponseSet`
	2. In iManager, go to **Roles and Task > Schema > Extend Schema** > **Import data from file on disk** and click **Next**.
	3. 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**.
	4. 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 the *NetIQ Self Service*

10. Install and configure Identity Reporting	1. For general information about the components and framework required for Identity Reporting, see Installing Identity Reporting in the *NetIQ Identity Manager Setup Guide for Windows*. **IMPORTANT:** You must install ActiveMQ by using the Tomcat and PostgreSQL convenience installer. Otherwise, the Reporting page does not load after you log in to Identity Reporting. Alternatively, copy the `activemq jar` file in `<tomcat>/libs` after completing the PostgreSQL installation and restart Tomcat. 2. For installing Identity Reporting, see one of the following sections in the *NetIQ Identity Manager Setup Guide for Windows*: - Using the Guided Process to Install Identity Reporting - Installing Identity Reporting Silently 3. For configuring Identity Reporting, see Configuring Identity Reporting in the *NetIQ Identity Manager Setup Guide for Windows*. **NOTE:** You must import the report definitions into Identity Reporting. To download them, use the Download page within the Reporting application.
11. Activating Identity Manager	Activate your Identity Manager components. For more information, see Activating Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*.

Creating and Assigning rptadmin Role to a User on Linux

You create an Organizational Role object in the Identity Vault and then assign this role to a new user or an existing user by using iManager.

1 Create an Organizational Role object.

1a In NetIQ iManager, click **View Objects**.

1b Click the Organizational Unit in which you want to create a new Report Administrator (`reportAdmin`) role.

1c Click **New** > **Create Object**.

1d From **Available object classes**, select Organizational Role and click **OK**.

1e Type the name and context of the object or use the Object Selector to find it, then click **OK**.

1f When the confirmation message appears, click **OK**.

2 Assign `reportAdmin` role to a user object.

2a In NetIQ iManager, click **Roles and Tasks**.

2b Click **Directory Administration > Modify Object**.

2c Specify the name and context of the user object or use the Object Selector to locate it, then click **OK**.

The Content frame displays the user object’s property book.

2d On the **General** tab, click the **Other** page.

2e On the screen that appears, select **Object Class** from **Valued Attributes**.

2f Click **Edit** to add a new attribute to the user object.

2g Click **+**, then specify a name, nrfIdentity, for the attribute, and click **OK**.

2h Click **OK** to save your changes.

2i Select **Object Class** from **Valued Attributes**.

2j From **Unvalued Attributes**, select nfrmemberof attribute, then click **Right Arrow** graphic to add this attribute to **Valued Attributes**.

2k To specify a value for the attribute, browse to the `reportAdmin` role that you created in Step 1 on page 6.

If you are using Firefox, click the **+** symbol to add information instead of typing directly in the field.

2l Click **Apply** or **OK** to save the changes.

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/configupdate`.
  - **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 Tomcat application server for the changes to take effect. However, you do not need to restart the application 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: `https://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.

Upgrading Identity Manager

NetIQ supports the following upgrade paths for upgrading to Identity Manager 4.7 Standard Edition:

- Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Standard Edition
- Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Advanced Edition

You cannot perform a direct upgrade from Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Advanced Edition. However, you can choose one of the following approaches to complete the upgrade:

- Upgrade Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Standard Edition and then upgrade to Identity Manager 4.7 Advanced Edition.
- Upgrade Identity Manager 4.6 Standard Edition to Identity Manager 4.6 Advanced Edition and then upgrade to Identity Manager 4.7 Advanced Edition.

Upgrading Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Standard Edition

To perform the upgrade, NetIQ recommends that you review Upgrading to Standard Edition in the NetIQ Identity Manager 4.7 Release Notes and then complete the following tasks in the same sequence:

Task	Linux	Windows
1. Review the differences between an upgrade and a migration	See Understanding Upgrade Process in the *NetIQ Identity Manager Setup Guide for Linux*.	See Understanding Upgrade and Migration in the *NetIQ Identity Manager Setup Guide for Windows*.
2. Upgrade from Identity Manager 4.0.2	You cannot directly upgrade or migrate to version 4.7 from versions before 4.5. For more information, see the *NetIQ Identity Manager Setup Guide 4.5*.	You cannot directly upgrade or migrate to version 4.7 from versions before 4.5. For more information, see the *NetIQ Identity Manager Setup Guide 4.5*.

Task	Linux	Windows
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.	Ensure that you have the latest installation kit to upgrade/migrate Identity Manager to 4.6 Standard Edition.
4. Interaction among Identity Manager components	See “Considerations for Installing Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Linux*.	See “Considerations for Installing Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Windows*.
5. System requirements	See “Planning to Install Identity Manager” in the *NetIQ Identity Manager Setup Guide for Linux*.	Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Considerations for Installing Identity Manager Components in the NetIQ Identity Manager Setup Guide for Windows and the accompanying Release Notes.
6. Back up the current project, driver configuration, and databases	See “Backing Up the Current Configuration” in the *NetIQ Identity Manager Setup Guide for Linux*.	See Backing Up the Current Configuration in the *NetIQ Identity Manager Setup Guide for Windows*.
7. Upgrade Analyzer	See “Upgrading Analyzer” in the *NetIQ Identity Manager Setup Guide for Linux*.	See Upgrading Analyzer in the *NetIQ Identity Manager Setup Guide for Windows*.
8. Upgrade Designer	See “Upgrading Designer” in the *NetIQ Identity Manager Setup Guide for Linux*.	See Upgrading Designer in the *NetIQ Identity Manager Setup Guide for Windows*.
9. Upgrade eDirectory	See Upgrading the Identity Vault in the *NetIQ Identity Manager Setup Guide for Linux*.	On the server running Identity Manager, upgrade eDirectory to the latest version. For more information, see the *NetIQ eDirectory Installation Guide* and NetIQ Identity Manager 4.7 Release Notes.
10. Upgrade iManager	Upgrade iManager to the latest version. For upgrade instructions, see Upgrading iManager in the *NetIQ Identity Manager Setup Guide for Linux*.	Upgrade iManager to the latest version. For upgrade instructions, see Upgrading iManager in the *NetIQ Identity Manager Setup Guide for Windows*.
11. Stop the drivers	See Stopping the Drivers in the *NetIQ Identity Manager Setup Guide for Linux*.	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 in the *NetIQ Identity Manager Setup Guide for Windows*.
12. Upgrade the Identity Manager engine	See Upgrading Identity Manager Engine in the *NetIQ Identity Manager Setup Guide for Linux*.	For more information, see Upgrading the Identity Manager Engine in the *NetIQ Identity Manager Setup Guide for Windows*. **NOTE:** If you are migrating 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 *NetIQ Identity Manager Setup Guide for Windows*.
13. (Conditional) Upgrade Remote Loader	See Upgrading Identity Manager Engine in the *NetIQ Identity Manager Setup Guide for Linux*.	If any of the drivers in the driver set are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see Upgrading the Remote Loader in the *NetIQ Identity Manager Setup Guide for Windows*.

Task	Linux	Windows
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 *NetIQ Identity Manager Setup Guide for Linux*. 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.	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 *NetIQ Identity Manager Setup Guide for Windows*. 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 4.7 Standard Edition activation key	In iManager, make sure that you apply the Identity Manager 4.7 Standard Edition activation. If you do not apply the activation, Identity Manager engine and drivers run in the evaluation mode.	In iManager, make sure that you apply the Identity Manager 4.7 Standard Edition activation. If you do not apply the activation, Identity Manager engine and drivers run in the evaluation mode.

Task	Linux	Windows
16. Install Identity Reporting components	Install Identity Reporting components. The installation process also installs the Single Sign-On component. For more information, see Considerations for Installing Identity Reporting Components in the *NetIQ Identity Manager Setup Guide for Linux*. If you are installing the Single Sign-On component on a different server, copy the existing Single Sign-On settings to the new server and then run the merge_jars method on this server to restore your settings. For more information, see One SSO Provider in the *NetIQ Identity Manager Setup Guide for Linux*.	Install Identity Reporting components. This requires you to perform the following actions: 1. Install Sentinel. Sentinel installation is supported only on a Linux server. For more information, see Installing Sentinel Log Management for Identity Governance and Administration in the *NetIQ Identity Manager Setup Guide for Linux*. 2. Install Tomcat and PostgreSQL. For more information, see Installing PostgreSQL and Tomcat for Identity Manager in the *NetIQ Identity Manager Setup Guide for Windows*. 3. Install and configure NetIQ One SSO Provider (OSP). For more information, see Installing the Single Sign-on Component in the *NetIQ Identity Manager Setup Guide for Windows*. 4. Install and configure Self Service Password Reset (SSPR). For more information, see Installing the Password Management Component in the *NetIQ Identity Manager Setup Guide for Windows*. 5. Install Identity Reporting. During installation, specify the DNS name or IP address of the Sentinel Log
17. Start the drivers	Start the drivers associated with the Identity Reporting and Identity Manager engine. For more information, see Starting the Drivers in the *NetIQ Identity Manager Setup Guide for Linux*.	Start the drivers associated with the Identity Reporting and Identity Manager engine. For more information, see Starting the Drivers in the *NetIQ Identity Manager Setup Guide for Windows*.
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 *NetIQ Identity Manager Setup Guide for Linux*.	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 *NetIQ Identity Manager Setup Guide for Windows*.
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 *NetIQ Sentinel Installation and Configuration Guide*.	Sentinel installation is not supported on Windows.

Upgrading Identity Manager 4.6 Standard Edition to Identity Manager 4.7 Advanced Edition

Upgrading Identity Manager 4.6 Standard Edition to Identity Manager 4.7 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 4.7 Advanced Edition includes all the features included in the Standard Edition along with additional features such as identity applications. The NetIQ Identity Manager 4.7 Release Notes includes brief summaries of the new features in Identity Manager 4.7. You might want to take a few minutes to look at the new features.

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

Task	Linux	Windows
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 Process in the *NetIQ Identity Manager Setup Guide for Linux*.	Review the differences between an upgrade and a migration. For more information, see Understanding Upgrade and Migration in the *NetIQ Identity Manager Setup Guide for Windows*.
2. Upgrade to Identity Manager 4.7 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*.	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.	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 “Planning Overview” in the *NetIQ Identity Manager Setup Guide for Linux*.	For more information, see “Planning Overview” in the *NetIQ Identity Manager Setup Guide for Windows*.
5. System requirements	Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Planning Overview in the *NetIQ Identity Manager Setup Guide for Linux* and the Release Notes for the version to which you want to upgrade.	Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, sFor more information, see Considerations for Installing Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Windows* 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.	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 Identity Reporting in the *NetIQ Identity Manager Setup Guide for Linux*.	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 Identity Reporting in the *NetIQ Identity Manager Setup Guide for Windows*.

Task	Linux	Windows
8. Apply the Identity Manager 4.7 Advanced Edition activation key	In iManager, ensure that you apply the Identity Manager 4.7 Advanced Edition activation key. Otherwise, Identity Manager engine upgrade does not proceed.	In iManager, ensure that you apply the Identity Manager 4.7 Advanced Edition activation key. Otherwise, Identity Manager engine upgrade does not proceed.
9. Create and deploy the User Application, Roles and Resource Service, and the Managed System Gateway drivers	The Identity Applications installation program automatically deploys User Application and Roles and Resource Service drivers required for Identity Applications to work. The Identity Reporting installation program automatically deploys Data Collection Service and Managed System Gateway drivers required for Identity Reporting to work.	For more information, see Creating and Deploying the Drivers for the Identity Applications in the *NetIQ Identity Manager Setup Guide for Windows*.
10. (Conditional) Install the application server	The Identity Applications installation program installs Tomcat. You cannot reuse the existing instance of Tomcat on Linux.	Install Tomcat as your application server. You can reuse the existing instance of Tomcat.
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. This installation option installs several components that provide the underlying framework for the identity applications.: ◆ Identity Manager Dashboard ◆ Identity Manager Administration Console ◆ User Application ◆ User Application driver ◆ Role and Resource Service driver The installer internally installs an authentication service to support single sign-on access to the identity applications and Identity Reporting. The installer also installs a password management service that helps you configure Identity Manager to allow users to reset their passwords. The installation process automatically deploys the User Application driver and the Role and Resource Service driver. For more information, see Upgrading Identity Applications in the *NetIQ Identity Manager Setup Guide for Linux*.	**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. This installation option installs several components that provide the underlying framework for the identity applications.: ◆ Identity Manager Dashboard ◆ Identity Manager Administration Console ◆ User Application ◆ User Application driver ◆ Role and Resource Service driver The installer internally installs an authentication service to support single sign-on access to the identity applications and Identity Reporting. The installer also installs a password management service that helps you configure Identity Manager to allow users to reset their passwords. The installation process automatically deploys the User Application driver and the Role and Resource Service driver. For more information, see Upgrading Identity Applications and Identity Reporting in the *NetIQ Identity Manager Setup Guide for Windows*.

Task	Linux	Windows
12. Start the application server	Start Tomcat.	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 “Updating the Configuration Information of the Data Collection Service Driver” on page 14.	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 “Updating the Configuration Information of the Data Collection Service Driver” on page 14.

Task	Linux	Windows
14. Upgrade Identity Reporting Components	Provide the existing auditing server details during the installation. For more information, see Upgrading Identity Reporting in the *NetIQ Identity Manager Setup Guide for Linux*. To log the Identity Reporting events in the auditing server, perform the following actions: 1. Stop the application server. For example, `/etc/init.d/idmapps_tomcat_init stop` 2. Stop the audit thread by running the following command: `ps -eaf | grep naudit` 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 **Enable auditing**. If it is already selected, de-select it and then click **OK**. d. Relaunch the ConfigUpdate utility and select the **Reporting** tab. e. Select **Enable auditing** and click **OK**. 4. Start the application server. For example, `systemctl start netiq-`	Provide the existing auditing server details during the installation. For more information, see Upgrading Identity Reporting in the *NetIQ Identity Manager Setup Guide for Windows*. To log the Identity Reporting events in the auditing server, perform the following actions: 1. Stop the application server. For example, add windows example 2. Stop the audit thread by running the following command: `ps -eaf | grep naudit ---- add windows info` 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 **Enable auditing**. If it is already selected, de-select it and then click **OK**. d. Relaunch the ConfigUpdate utility and select the **Reporting** tab. e. Select **Enable auditing** and click **OK**. 4. Start the application server. For example, add Windows example
15. Start the drivers	Start the drivers associated with Identity Reporting and Identity Manager engine. For more information, see Managing the Drivers for Reporting in the *NetIQ Identity Manager Setup Guide for Windows*. - is this required for Linux	Start the drivers associated with Identity Reporting and Identity Manager engine. For more information, see Managing the Drivers for Reporting in the *NetIQ Identity Manager Setup Guide for Windows*.
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 *NetIQ Identity Manager Setup Guide for Linux*.	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 *NetIQ Identity Manager Setup Guide for Windows*.
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*.	(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*.

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.

   For more information on configuring the driver, see Configuring the Driver for Data Collection Service in the *NetIQ Identity Manager Setup Guide for Windows*.
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.

Uninstalling Identity Manager 4.7 Standard Edition

Some components of Identity Manager have prerequisites for uninstallation. Ensure that you review all the information for each component before beginning the uninstallation process. For more information, see Uninstalling Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Linux* or Uninstalling Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Windows*.

Legal Notice: For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright (C) 2018 NetIQ Corporation. All rights reserved.