NetIQ Identity Manager Standard Edition Quick Start Guide

February 2015

This document provides guidelines to install, configure, and upgrade Identity Manager 4.5 Standard Edition.

1 Overview

Identity Manager 4.5 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 *NetIQ Identity Manager Setup Guide*.

IMPORTANT: Integration modules continue to remain the same for both Identity Manager Advanced and Standard Editions.

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

2 Components

Identity Manager 4.5 Standard Edition includes the following components:

- Identity Vault
- iManager
- Identity Manager Engine
- Designer
- Analyzer
- Remote Loader
- Event Auditing Service (EAS)
- 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 4.5 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_4.5_Linux_Standard.iso`
- `Identity_Manager_4.5_Windows_Standard.iso`

The installation files are located in the `products` directory in the Identity Manager installation package. For information about the default installation locations, see Locating the Installation Paths in the Release Notes.

NetIQ recommends that you review the Installation Prerequisites in the 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 *NetIQ Identity Manager Setup Guide*.

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 *NetIQ Identity Manager Setup Guide*. ◆ For information about prerequisites, computer requirements, installation, upgrade, or migration, see Considerations and Prerequisites for Installation in the *NetIQ Identity Manager Setup Guide*.
2. Plan your installation	See “Planning to Install Identity Manager” in the *NetIQ Identity Manager Setup Guide*.
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. iManager 3. Identity Manager Engine 4. Designer 5. Analyzer 6. Event Auditing Service (EAS) 7. Tomcat (supported application server) 8. Single Sign-on and Password Management Components 9. Identity Reporting **IMPORTANT:** The installation programs install the Identity manager components in

Task	Notes
4. Install and configure eDirectory	Install eDirectory 8.8.8 Patch 3 or later. For installation instructions, see "Installing the Identity Vault" in the *NetIQ Identity Manager Setup Guide*. ◆ After installing and configuring eDirectory, stop eDirectory services. ◆ Apply the latest released eDirectory patch. ◆ Start the eDirectory services.
5. Install and configure iManager	Install iManager 2.7.7 Patch 2 or later. For the auditing to work, install iManager 2.7.7 Patch 3 or later. For installation instructions, see "Installing iManager" in the *NetIQ Identity Manager Setup Guide*.
6. Install Identity Manager Engine, Drivers, and Plug-ins	For installation instructions, see "Installing the Identity Manager Engine, Drivers, and Plug-ins" in the *NetIQ Identity Manager Setup Guide*. **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 Event Auditing Service	For installation instructions, see "Installing the Event Auditing Service" in the *NetIQ Identity Manager Setup Guide*.
8. Install Tomcat	Select only Tomcat for deploying Identity Reporting. You do not need to install PostgreSQL because you are not installing RBPM. For installation instructions, see "Installing PostgreSQL and Tomcat" in the *NetIQ Identity Manager Setup Guide*. **NOTE:** If you are installing Tomcat on a computer that has iManager installed, do not use port 8080 for Tomcat. If the other ports are already in use, change them during installation.

Task	Notes

9. Install the Single Sign-on and Password Management Components	For installation instructions, see "Installing the Single Sign-on and Password Management Components" in the *NetIQ Identity Manager Setup Guide*.
	
	After installing the Single Sign-on and Password Management components, 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 Setting Up SSL Auditing (https://www.netiq.com/documentation/sspr3/adminguide/data/b14knaes.html) in the *NetIQ Self Service Password Reset 3.2 Administration Guide*.

10. Install and configure Identity Reporting	1. For general information about the components and framework required for Identity Reporting, see "Installing the Identity Reporting Components" in the *NetIQ Identity Manager Setup Guide*. 2. 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. 3. For performing a silent installation, see Section 3.1.2, "Installing Identity Reporting Silently," on page 10. 4. For configuring the drivers, see "Configuring Drivers for Identity Reporting" in the *NetIQ Identity Manager Setup Guide*. 5. For deploying REST APIs for Identity Reporting, see "Deploying REST APIs for Identity Reporting " in the *NetIQ Identity Manager Setup Guide*. **NOTE:** You must import the report definitions into Identity Reporting. To download them, use the Download page within the Reporting application.

Task	Notes
11. Activating Identity Manager	Activate your Identity Manager components. For more information, see "Activating Identity Manager" in the *NetIQ Identity Manager Setup Guide*.

3.1 Installing Identity Reporting

The Identity Manager installation package includes the installation files in the `products/EAS` 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. Ensure that the SIEM database is running in your event auditing service.

   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.
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.
    - **Identity Vault Connection Details**

Represents the connection settings for the Identity Vault. 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.

- **Application server platform**

  Specifies the application server that will run the core (`IDMRPT-Core.war`), EASREST REST API (`easrestapi.war`), EAS Webstart (`easwebstart.war`), and Reporting REST API Reference WAR (`rptdoc.war`) files. NetIQ supports only Tomcat for Identity Reporting.

NOTE: Do not change the names of these WAR files. If you change the file names, the deployment process fails.

- **Application server details**

  Specifies a path to the deployment or webapps directory of the Tomcat instance. For example, `/opt/netiq/idm/apps/tomcat/webapps`.

- **Application server connection**

  Represents the settings of the URL that users need to connect to Identity Reporting on the application server. For example, `https:myserver.mycompany.com:8080`.

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

- **Event auditing service**

Specifies whether you want to use NetIQ Event Auditing Service (EAS) to track events in Identity Reporting.

If you select this setting, also specify the DNS name or IP address of the server that hosts EAS.

- **Database details**

  Represents the settings for your SIEM database.

  Database port

  Specifies the port for the SIEM database. The default value is 15432.

  DBA password

  Specifies the password for the administrative account for the database.

  If you are using EAS, the installation program creates this password for the `dbauser` account.

  idmrptsrv user password

  Specifies the password for the account that owns the Identity Reporting schema and view in the database.

  The installation program creates this password for the `idmrptsrv` account.

  idmrptuser user password

  Specifies the password for the account that can access the database to run reports.

  The installation program creates this password for the `idmrptuser` account.

  Test database connection

  Indicates whether you want the installation program to test the values specified for the database.

  The installation program attempts the connection when you click **Next** or press **Enter**.

  NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database.

- **Authentication details**

  Represents the settings for the authentication server. To modify these settings after installation, use the Reporting Configuration utility.

  Base container

  Specifies the DN of the container that lists the users that can log in to Identity Reporting. For example, `o=data`.

  NOTE: If the DN contains special characters, you might need to escape those characters. For more information, see RFC 2253/4514 Section 2.4.

  Login attribute

  Specifies the attribute that you want to use for searching the subtree of the user container. For example, `cn`.

  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 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.

- **Choose Java JRE Base folder path**

  Represents the location of the JRE used by the application server.

  Java JRE Base folder

  Specifies the path for JRE used by the application server. For example, `/opt/netiq/idm/apps/jre`

- **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 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.

- **Report details**

  Represents the settings for maintaining completed reports.

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 a path where you want to store the report definitions. For example, `/opt/netiq/IdentityReporting`.

- **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 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**

Applies only when you enable auditing for Identity Reporting.

Represents the settings for the NAudit service which sends events from Identity Reporting to EAS.

Specify existing certificate / Generate a certificate

Indicates whether you want to use an existing certificate for the NAudit server or create a new one.

Enter Public key

Applies only when you want to use an existing certificate.

Lists the custom public key certificate that you want the NAudit service to use to authenticate audit messages sent to EAS.

Enter RSA Key

Applies only when you want to use an existing certificate.

Specifies the path to the custom private key file that you want the NAudit service to use to authenticate audit messages sent to EAS.

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*. Also see the Release Notes accompanying the release.

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_EAS_SYSTEM_PASSWORD

Specifies the password for the EAS server.

You can copy the system password from the system property in the `activemqusers.properties` file on the computer where EAS is installed.

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 5.

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/IdentityReporting/bin/lib`.
  - **Windows:** Run `configupdate.bat` from `C:\netiq\idm\apps\IdentityReporting\bin\lib.`

  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 Identity Manager 4.0.2 Standard Edition:

- Identity Manager 4.0.2 Standard Edition to Identity Manager 4.5 Standard Edition
- Identity Manager 4.5 Standard Edition to Identity Manager 4.5 Advanced Edition

You cannot perform a direct upgrade from Identity Manager 4.0.2 Standard Edition to Identity Manager 4.5 Advanced Edition. However, you can choose one of the following approaches to complete the upgrade:

- Upgrade Identity Manager 4.0.2 Standard Edition to Identity Manager 4.5 Standard Edition and then upgrade to Identity Manager 4.5 Advanced Edition.
- Upgrade Identity Manager 4.0.2 Standard Edition to Identity Manager 4.0.2 Advanced Edition and then upgrade to Identity Manager 4.5 Advanced Edition.

4.1 Upgrading Identity Manager 4.0.2 Standard Edition to Identity Manager 4.5 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 *NetIQ Identity Manager Setup Guide*.

Task	Notes
2. Upgrade from Identity Manager 4.0.2	You cannot directly upgrade or migrate to version 4.5 from versions before 4.0.2. For more information, see the *NetIQ Identity Manager Setup Guide 4.0.2*.
3. Get the files needed for upgrade/migrate	Ensure that you have the latest installation kit to upgrade/migrate Identity Manager to 4.5 Standard Edition.
4. Interaction among Identity Manager components	For more information, see "Introduction" in the *NetIQ Identity Manager Setup Guide*.
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 *NetIQ Identity Manager Setup Guide* 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 *NetIQ Identity Manager Setup Guide*.
7. Upgrade Analyzer	Upgrade Designer to the latest version. For more information, see "Upgrading Analyzer" in the *NetIQ Identity Manager Setup Guide*.
8. Upgrade Designer	Upgrade Designer to the latest version. For more information, see "Upgrading Designer" in the *NetIQ Identity Manager Setup Guide*.
9. Upgrade eDirectory	On the server running Identity Manager, upgrade eDirectory to the latest version and patch. For more information, see the *NetIQ eDirectory 8.8 Installation Guide* and Identity Manager Release Notes.
10. Upgrade iManager	Upgrade iManager to the latest version and patch. For upgrade instructions, see "Upgrading iManager" in the *NetIQ Identity Manager Setup Guide*.
11. Stop the drivers	Stop the drivers that are associated with the server where you installed the Identity Manager engine (Metadirectory). For more information, see "Stopping the Drivers" in the *NetIQ Identity Manager Setup Guide*.
12. Upgrade the Identity Manager engine	For more information, see "Upgrading the Identity Manager Engine" in the *NetIQ Identity Manager Setup Guide*. **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 *NetIQ Identity Manager Setup Guide*.
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 *NetIQ Identity Manager Setup Guide*.
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*. 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.

Task	Notes
15. Apply Identity Manager 4.5 Standard Edition activation key	In iManager, make sure that you apply the Identity Manager 4.5 Standard Edition activation. If you do not apply the activation, the Identity Manager engine and the drivers run in the evaluation mode.
16. Remove RBPM and Identity Reporting files and folders	Remove RBPM and Identity Reporting files and folders from your current application server. This requires you to take the following actions: 1. (Conditional) Uninstall the RBPM and Identity Reporting WAR files from your application server. To do this, follow the instructions in the documentation specific to your application server. 2. Stop the application server where RBPM and Identity Reporting are installed. 3. Run the Identity Reporting uninstallation program to remove the installation files and folders. For more information, see "Uninstalling the Identity Reporting" in the *NetIQ Identity Manager Setup Guide*. 4. Run the RBPM uninstallation program to remove the installation files and folders. For more information, see "Uninstalling the Roles Based Provisioning Module" in the *NetIQ Identity Manager Setup Guide*.
17. Remove the User Application driver and the Roles and Resource Service driver	Remove the User Application driver and the Roles and Resource Service driver from the driver set of the upgraded setup and from the Designer project. For more information, see "Deleting the Drivers for the Roles Based Provisioning Module" in the *NetIQ Identity Manager Setup Guide*.

Task	Notes
18. Install Identity Reporting components	Install Identity Reporting components. This requires you to take the following actions: 1. Create a backup of the EAS data. For more information, see "Backing Up the Schema for the Drivers" in the *NetIQ Identity Manager Setup Guide*. 2. Upgrade the Event Auditing Service (EAS). To upgrade EAS, install the new version on top of the older version. For more information, see "Upgrading the Event Auditing Service" in the *NetIQ Identity Manager Setup Guide*. 3. The installation program provides options for installing Tomcat and PostgreSQL.Choose to install Tomcat only. For more information, see "Installing PostgreSQL and Tomcat for Identity Manager" in the *NetIQ Identity Manager Setup Guide*. 4. Install and configure NetIQ One SSO Provider (OSP) and Self Service Password Reset (SSPR). For more information, see "Installing the Single Sign-on and Password Management Components" in the *NetIQ Identity Manager Setup Guide*. 5. Install Identity Reporting. During installation, specify the DNS name or IP address of the server that hosts the upgraded EAS. For more information, see "Installing Identity Reporting" in the *NetIQ Identity Manager Setup Guide*. 6. (Conditional) Update the Data Collection Service driver configuration for your new application server (Tomcat). 7. Delete the references to `reportRunner` from the PostgreSQL database before starting the application server after the Reporting installation. a. (Conditional) Stop Tomcat. b. In the Identity Reporting root folder, rename the `reportContent` folder. For Example: `/opt/netiq/idm/apps/IdentityReporting` c. In the Tomcat root folder, clean the `temp` and `work` directories. d. In EAS, log in to the PostgreSQL database and issue the following statements to delete the references to `reportRunner`: ◆ `DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE rpt_def_id='com.novell.content.reportRunner';` ◆ `DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE def_id='com.novell.content.reportRunner';` e. Start Tomcat.
19. 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 *NetIQ Identity Manager Setup Guide*.
20. (Conditional) Restore your custom settings	(Conditional) 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*.

Task	Notes
21. (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*.

4.2 Upgrading Identity Manager 4.5 Standard Edition to Identity Manager 4.5 Advanced Edition

Upgrading Identity Manager 4.5 Standard Edition to Identity Manager 4.5 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 4.5 Advanced Edition includes all the features included in the Standard Edition along with additional features such as identity applications. The New Features section in the Identity Manager 4.5 Advanced Edition Release Notes includes brief summaries of the new features in Identity Manager 4.5 Advanced Edition. 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 *NetIQ Identity Manager Setup Guide*.
2. Upgrade to Identity Manager 4.5 Standard Edition	You cannot upgrade or migrate to version 4.5 from versions before 4.0.2. For more information, see the NetIQ Identity Manager Setup Guide 4.0.2.
3. Get the files needed for upgrade/migrate	Ensure that you have the latest installation kit to upgrade Identity Manager to 4.5 Advanced Edition.
4. Learn about the interaction among Identity Manager components	For more information, see "Introduction" in the *NetIQ Identity Manager Setup Guide*.
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 *NetIQ Identity Manager Setup Guide* and the Release Notes for the version to which you want to upgrade.
6. Stop the application server where Identity Reporting is installed	In this case, the application server is 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 *NetIQ Identity Manager Setup Guide*.

Task	Description
8. Apply the Identity Manager 4.5 Advanced Edition activation key	In iManager, ensure that you apply the Identity Manager 4.5 Advanced Edition activation key. Otherwise, the Identity Manager engine upgrade does not proceed. **IMPORTANT:** To ensure that Identity Manager displays correct version and brand name after upgrade, apply the Identity Manager 4.5 Patch 2 from the NetIQ Downloads website (http://download.novell.com/Download?buildid=vNsTfMo9g-4~). For detailed information on downloading and applying the patch, see "Applying a Hotfix to Identity Manager Components" in the *NetIQ Identity Manager Setup Guide*.
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 *NetIQ Identity Manager Setup Guide*.
10. (Conditional) Install the application server	Install WebSphere or JBoss as your application server. If you want to use 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. 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 *NetIQ Identity Manager Setup Guide*.
12. Start the application server	If your application server is not Tomcat, start your application server (WebSphere or JBoss) and Tomcat. You need to run Tomcat because NetIQ supports OSP installation only on Tomcat.
13. Update the Data Collection Service driver configuration	(Conditional) 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 17.

Task	Description
14. Install and configure Identity Reporting	Provide the existing EAS server details during the installation. For more information, see "Installing the Identity Reporting Components" in the *NetIQ Identity Manager Setup Guide*. To log the Identity Reporting events in the EAS 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 the **Enable auditing to EAS** 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 to EAS** checkbox and click **OK**. 4. Start the application server. For example, `/etc/init.d/idmapps_tomcat_init start`
15. 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 *NetIQ Identity Manager Setup Guide*.
16. (Conditional) Restore your custom settings	(Conditional) 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*.
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.

     For more information on configuring the driver, see "Configuring the Driver for Data Collection Service" in the *NetIQ Identity Manager Setup Guide*.
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 4.5 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