Centralized Reporting for NetIQ Access Review 2.0 and NetIQ Identity Manager 4.5

Technical Reference

June 2016

When you use NetIQ Access Review in a NetIQ Identity Manager environment, you might want the reporting function to be able to run reports for both applications rather than having to manage separate reporting instances. With **NetIQ Identity Reporting 5.0**, you can have the updated reporting functionality for Access Review 2.0 reports while also running your existing Identity Manager 4.5 reports.

This Technical Reference provides information about installing and configuring Identity Reporting as a centralized reporting function for Access Review and Identity Manager. It also addresses the actions required for migrating custom reports from your previous version of Identity Reporting.

Contents

Overview

Identity Reporting 5.0 can provide centralized reporting for Access Review 2.0 and Identity Manager 4.5. If you previously installed reporting with Identity Manager 4.5, you must upgrade to the new version of reporting.

This Technical Reference assumes that you want to use the same reporting installation for both Access Review and Identity Manager. In this scenario, the Report Administrator accesses the reporting function from Identity Manager Home. The administrator must add Access Review as a data source and an application for data collection. Then the administrator can run reports against the catalogs for Access Review and Identity Manager.

To have separate reporting functions for Access Review and Identity Manager, see the following table:

	Identity Reporting	For more information, see...
Access Review 2.0	5.0	*NetIQ Access Review User Guide* v2.0
Identity Manager 4.5	4.5	*NetIQ Identity Manager Setup Guide* v4.5
Access Review 1.5	4.5	*NetIQ Access Review User Guide* v1.5

For more information about using Access Review with Identity Manager, see "Integrating Single Sign-on Access with Identity Manager" in the *NetIQ Access Review User Guide*.

Checklist for Enabling Centralized Reporting

Before beginning the process, NetIQ recommends that you review the following steps.

	Checklist Items
❑	1. Learn about the interaction among Identity Reporting components. For more information, see "Understanding Identity Reporting" in the *NetIQ Access Review User Guide*.
❑	2. Learn about the database required for reporting. You can use PostgreSQL or Oracle. The Access Review download kit includes a convenience installer for PostgreSQL. For more information, see "Understanding the Identity Reporting Database" in the *NetIQ Access Review User Guide*.
❑	3. Decide which server(s) you want to use for your Identity Reporting components. For more information, see "Recommended Installation Scenarios and Server Setup" in the *NetIQ Access Review User Guide*.
❑	4. Review the considerations for installing Identity Reporting. For more information, see "Prerequisites for Identity Reporting" in the *NetIQ Access Review User Guide*.
❑	5. Review the hardware and software requirements for the computer that will host Identity Reporting. For more information, see "System Requirements for Identity Reporting" in the *NetIQ Access Review User Guide*.

	Checklist Items
❑	6. (Conditional) If you have customized reports for your current version of Identity Reporting, you must export them. For more information, see .
❑	7. Ensure that the server where you want to install Identity Reporting has an application server, such as Tomcat. You can use IBM WebSphere or Apache Tomcat. The Access Review download kit includes a convenience installer for Tomcat For more information, see one of the following sections: ◆ "Installing PostgreSQL and Tomcat for Access Review" in the *NetIQ Access Review User Guide* ◆ INFO ABOUT WEBSPHERE -- reference IDM 4.5 Setup Guide?
❑	8. Ensure that you have a database to which the installation process can connect. For more information, see the following sections: ◆ "Understanding the Users that the Installation Process Creates" on page 3 ◆ "Creating a Database for Identity Reporting" in the *NetIQ Access Review User Guide*
❑	9. (Conditional) To use an Oracle database, ensure that the schema exists for the reporting user. For more information, see the following sections: ◆ "Understanding the Users that the Installation Process Creates" on page 3 ◆ "Preparing an Oracle Database for Access Review" in the *NetIQ Access Review User Guide*
❑	10. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on Events" in the *NetIQ Access Review User Guide*.
❑	11. Install Identity Reporting, For more information, see "Installing Identity Reporting" on page 4.
❑	12. Configure reporting identity sources. For more ifnormation, see .
❑	13. Import the customized reports that you exported from your previous version of Identity Reporting. For more information, see .

Understanding the Installation Process

Understanding the Installation Process for Identity Reporting

The installation program for Identity Reporting deploys the WAR files and configures the reporting settings. It can also create user accounts and schema. For more information, see "Understanding the Installation Process for Identity Reporting" in the *NetIQ Access Review User Guide*.

Understanding the Users that the Installation Process Creates

Identity Reporting requires a specific set of users/schema for each reporting database, which the installation program can create in most cases. The following table lists the default names of these users.

User name	Description
arrptuser	Has the credentials to access the report views and run the reports for Access Review
idm_rpt_cfg	Owns the reporting configuration data and the reporting views for Identity Reporting
idm_rpt_data	Owns the data collected by Identity Reporting from Identity Manager
idmrptuser	Has the credentials to access the report views and run the reports for Identity Manager
appuser (optional)	Owns the data collected by Identity Reporting from NetIQ Sentinel (auditing service)
dbauser (optional)	Owns the data collected by Identity Reporting from NetIQ Event Auditing Service

For a PostgreSQL database, the installation process can create these users.

For an Oracle database, the installation process cannot create the database administrator or the schema for the views and reports. For more information about manually creating these users in Oracle, see “Preparing an Oracle Database for Access Review” in the *NetIQ Access Review User Guide*.

Preparing to Install Identity Reporting

INTRO PARAGRAPH THAT introduces the concepts in this section --

Saving Your Current Reporting Settings

The installation process creates a new instance of Identity Reporting for which you will need to add data sources and settings for data collection. If you are replacing an older version of Identity Reporting, you might want to take a snapshot of your existing settings for a quicker setup after installation.

1. Log in to Identity Reporting as the Report Administrator.
2. Select **Data Sources**.
3. Create a screen capture shot or make a note of the settings for each data source.
4. Perform the same action for the **Data Collection** settings for **Identity Vaults**, **Applications**, and **Auditing**.

Saving Your Customized Reports

You might have customized the reports that for use with Access Review 1.5 or Identity Manager 4.5. The installation process for Identity Reporting overwrites all of your customizations. This section helps you export the custom reports so you can use them after installing the latest version of Identity Reporting.

Installing Identity Reporting

This section describes the process for installing Identity Reporting.

- “Using the Guided Process to Install Identity Reporting” on page 5
- “Installing Identity Reporting Silently” on page 9

The installation files for Identity Reporting are available with the Access Review download package. By default, the installation program installs the components in the following location:

`opt/netiq/access-review/apps/Reporting`

To prepare for the installation, see “Checklist for Enabling Centralized Reporting” on page 2. Also see the Release Notes accompanying the Identity Reporting release.

Using the Guided Process to Install Identity Reporting

This procedure describes how to install Identity Reporting using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see “Installing Identity Reporting Silently” on page 9.

1. Log in to the computer where you want to install Identity Reporting.
2. Stop the application server, such as Tomcat.

   For example:

   ```
   /etc/init.d/idmapps_tomcat_init stop
   ```
3. Downloaded Identity Reporting installation files from the NetIQ Downloads website, the installation file is named `rpt-install-4.5.0-linux.bin`.
4. Launch the installer for console or GUI by enter the following:
   - **Linux (console)**: Enter `./rpt-install-4.5.0-linux.bin -i console`
   - **Linux (GUI)**: Enter `./rpt-install-4.5.0-linux.bin`
5. In the installation program, specify the language that you want to use for installation, and then select **OK**.
6. Review the Introduction text, and then select **Next**.
7. Accept the License Agreement, and then select **Next**.
8. For **NAME OF PAGE FOR AR vs IDM**, specify **Identity Manager**.

   NOTE: If you select **Access Review**, the installation program does not support the settings for centralized reporting with Identity Manager.

   ---
9. To complete the guided process, specify values for the following parameters:
   - **Installation folder**

     Specifies the location for the installation files.
   - **Reporting setup**

     Specifies connection information for Identity Manager, depending on how you want to set up your reporting environment.
   - **Application server platform**

     Specifies the application server that will run the core (`IDMRPT-Core.war`) and Reporting REST API Reference WAR (`rptdoc.war`) files.

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

   - **Application server details**

     Applies only for Tomcat application servers.

     Specifies whether this is a secondary node.

     Specifies a path to the deployment or webapps directory of the application server instance. For example, `/opt/netiq/access-review/apps/tomcat/webapps`.

- **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 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 Access Review.

  Connect to an external authentication server

  Specifies whether a different instance of the application server that 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 configuration utility for the identity application in Identity Manager.

- **Event auditing service**

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

- **Database details**

  Represents the settings for your reporting database.

  Database type

  Specifies whether your reporting database is an Oracle database. If you select this setting, also specify values for the JDBC driver.

  JDBC driver jar

  Applies only when your reporting database runs on an Oracle platform.

  Specifies the path to the jar file for the Oracle JDBC driver. For example, `opt/oracle/ojdbc7.jar`.

  For more information, see "Adding the Oracle JDBC File to the Application Server" in the *NetIQ Access Review User Guide*.

  JDBC driver classname

  Applies only when your reporting database runs on an Oracle platform.

  Specifies the class of the JDBC driver.

JDBC driver type

Applies only when your reporting database runs on an Oracle platform.

Specifies the type of JDBC driver. Identity Reporting uses this value as a prefix in the JDBC URL.

Database host

Applies only when you do not use EAS.

Specifies the DNS name or IP address of the server that hosts your reporting database. Do not use `localhost`.

Database name

Specifies the name of your reporting database. For example, `reporting`.

Database port

Specifies the port for the reporting database. The default value is 15432 for Oracle and 5432 for PostgreSQL.

Configure database now or at startup

Specifies when you want to configure the database.

DBA userid

Specifies the name of the administrative account for the reporting database server and owner of the event auditing schema and views.

DBA password

Specifies the password for the administrative account for the database.

Test database connection

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

The installation program attempt the connection when you select **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. For more information, see "Manually Generating the Database Schema" in the *NetIQ Access Review User Guide*.

Generate SQL for later

Specifies to create the statements needed to create the database at some later time.

- **Authentication details**

Represents the settings for the authentication server. To modify these settings after installation, use the configuration utility for Access Review or the identity application in Identity Manager.

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.

- **User Application driver**

When installing Identity Reporting with Access Review only, leave the default values.

User Application driver

Specifies the name of the User Application driver.

Driver set name

Specifies the name of the driver set for the User Application driver.

Driver set container

Specifies the DN for the container that stores the driver set.

- **Email delivery**

Represents the settings for the SMTP server that sends report notifications. To modify these settings after installation, use the configuration utility for the identity applications in Identity Manager.

Default email address

Specifies the email address that you want Identity Reporting to use as the origin 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 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.

SMTP user name

Applies only when you select **Server requires authentication**.

Specifies the name of a login account for the SMTP server.

SMTP password

Applies only when you select **Server requires authentication**.

Specifies the password of a login account for the SMTP 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 sending auditing activity in Identity Reporting to NetIQ Sentinel or NetIQ Event Auditing Service (EAS). Auditing does not support xdas.

  Enable auditing for Identity Reporting

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

  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`.

- **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.

10. Review the information in the Pre-Installation Summary window, and then select **Install**.
11. When the installation process completes, continue to "Completing the Installation Process" on page 10.

Installing Identity Reporting Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a silent properties file. You can run the silent installation with the default file or edit the file to customize the installation process. To perform a guided installation, see "Using the Guided Process to Install Identity Reporting" on page 5.

1. Log in as `root` or an administrator to the computer where you want to install Identity Reporting.
2. (Conditional) To avoid specifying the administrator passwords for the installation in the silent properties file for a silent installation, use the `export` or `set` command. For example:

   ```
   export NOVL_ADMIN_PWD=myPassWord
   ```

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

   Specify the following passwords:

   NOVL_DB_RPT_USER_PASSWORD

   Specifies the password for the administrator for the reporting database.

NOVL_AR_SRV_PWD

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

NOVL_AR_USER_PWD

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

NOVL_ADMIN_PWD

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

NOVL_SMTP_PASSWORD

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

3 To specify the installation parameters, complete the following steps:

3a Locate the sample `rpt-install-4.5.0.silent.properties` silent properties file, by default in the same directory as the installation scripts for Access Review.

3b In a text editor, open the silent properties file.

3c Specify the parameter values. For a description of the parameters, see Step 9 on page 5.

3d Save and close the file.

4 Stop the application server, such as Tomcat.

For example:

```
/etc/init.d/idmapps_tomcat_init stop
```

5 To launch the installation process, enter the following command:

```
./rpt-install-4.5.0-linux.bin -i silent -f path_to_silent_properties_file
```

NOTE: If the silent 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.

6 When the installation process completes, continue to “Completing the Installation Process” on page 10.

Completing the Installation Process

- “Configuring the PostgreSQL Database for Identity Reporting” in the *NetIQ Access Review User Guide*
- “Configuring the Oracle Database for Identity Reporting” in the *NetIQ Access Review User Guide*
- (Conditional) To use WebSphere to host Identity Reporting, continue to “Configuring Identity Reporting for WebSphere ” in the *NetIQ Access Review User Guide* - .
- “Manually Generating the Database Schema” in the *NetIQ Access Review User Guide*
- “Preparing Identity Reporting for Use” in the *NetIQ Access Review User Guide*
- INSRUCTIONS FOR adding their customized reports, which they exported before starting this process
- ADDING AR as a data source
- ADD AR as a data collection source

- ADDING all their other data sources -- since the installation process wipes those out.
- DO WE need to update the Data Collection Services driver or the Managed Gateway System driver?