NetIQ® Identity Manager Driver for NetIQ Access Review

Installation and Configuration Guide

March 2016

Legal Notice

Contents

About this Book and the Library

This guide explains how to install and configure the Identity Manager Driver for NetIQ Access Review.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts for roles and resource management across the enterprise, and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Access Review User Guide

Provides conceptual information about NetIQ Access Review, including installation information, and step-by-step guidance for many administrative and user-oriented tasks.

Identity Manager Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provide implementation information specific to an Identity Manager driver.

Identity Manager Setup Guide

Provides an overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

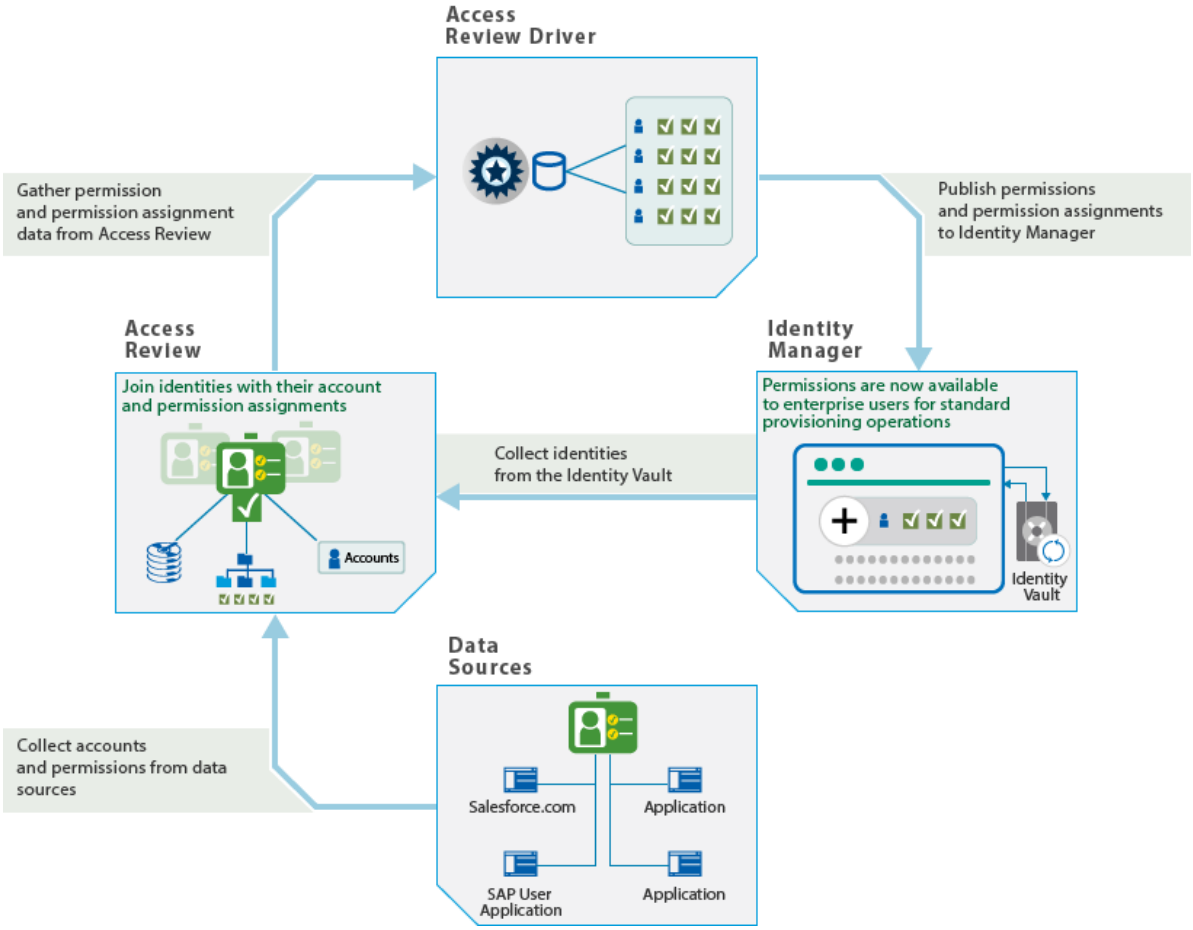
NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the Access Review Driver

The **Identity Manager Driver for NetIQ Access Review** (Access Review driver) allows you to provision application-specific permission catalog data from Access Review to Identity Manager. This gives you the ability to review and certify permission assignments using Access Review, as well as to request and provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager as needed for the customer's use-case.

1.1 Understanding the Workflow Process

The following workflow shows how you can streamline the process for maintaining user identities.



Access Review

Access Review collects data from a wide variety of identity and application sources. **Identity sources**, such as SAP User Management and the Identity Vault in Identity Manager, provide the attributes of a user's identity. **Application sources**, such as Salesforce.com, provide account and permission information. Some of the account and permission information might be gathered from systems that are not already connected to identities in Identity Manager.

Access Review helps you join the imported account, permission, and attribute data into a **unified identity**. Then you review and certify whether each unified identity should have the assigned resources. If permission assignments change, Access Review helps you fulfill the changes by creating manual tasks or initiating provisioning workflows in Identity Manager.

Access Review driver

Using an account in Identity Manager, the Access Review driver transfers a snapshot of the permissions and permission assignments from the Access Review database to Identity Manager. This process creates assignment actions for Identity Manager to set the actual state of the affected permissions without the need for user intervention.

You can also configure the driver to create new user accounts in Identity Manager based on identities published from Access Review. After adding the accounts, the driver reports the DN and tree name of the newly created users to Identity Manager.

NetIQ recommends that you create a dedicated system account in the identity applications for the driver. A system account provides the following advantages:

- Allows you to track any actions that the driver takes in Identity Manager
- Allows the driver to set resource assignments in Identity Manager
- Reduces the number of approval workflows required to assign and revoke resources to identities in Identity Manager

Identity Manager

When receiving the data from the Access Review driver, Identity Manager populates the Identity Vault with the user identities and adds account and permission information to the identity applications catalog. Because Access Review collects data from more sources than might be connected to Identity Manager, the catalog now has identities, permissions, and accounts that represent a larger picture of your identity and access environment.

In the catalog, Identity Manager administrators can create roles and permissions associated with the application sources that Access Review collected. Then users can manage their unified identity and request access to other resources in the catalog even if those applications are not directly connected to Identity Manager. To process user requests, administrators can configure workflows. You can also use workflows to fulfill the change requests generated by a review in Access Review.

For more information about using Access Review, see the *NetIQ Access Review User Guide*. For more information about Identity Manager, see the NetIQ Identity Manager documentation site.

1.2 Understanding Synchronization and Reflection

Access Review can collect data from identity and application sources that are not connected to Identity Manager. The Access Review driver allows you to **synchronize** changes to identities and applications with user and resource objects in Identity Manager. You can also **reflect** collected user identities and application data as resources in the Identity Vault. The driver provides Global Configuration Values (GCVs) that allow you to delete or disable user objects or delete these resource

objects in the Identity Vault. Alternatively, you can remove the association between the user object and the identity in Access Review. For more information, see “Understanding Synchronization and Reflection” in the *NetIQ Access Review User Guide*.

1.3 Planning to Install and Configure the Driver

This section provides useful information for planning the installation and configuration process.

1.3.1 Installation Requirements

The Access Review driver requires the following applications and files, at a minimum. When you installed Identity Manager, you might also have chosen to install the files for the Access Review driver.

- Access Review 1.1
- Identity Manager 4.5 Service Pack 1, particularly the following components:
  - Identity applications
  - Designer
  - Remote Loader
  - Role and Resource Service driver

    `NOVLRSERVB` - Role and Resource Service Driver Base, package version 4.5.0.20140925170245, at a minimum
  - User Application driver

    `NOVLUABASE` - User Application Base, version 4.5.1.20150602213315, at a minimum

    `NOVLPROVNOTF` - Provisioning Notification Templates, version 2.0.1.20150528174045, at a minimum
  - Drive Set packages

    `NOVLACOMSET` - Driver Set package for Common Settings Advanced Edition

    `NOVLCOMSET` - Driver Set package for Common Settings
- Database JDBC file
  - Third-party JDBC driver for connecting to the Access Review database
- Access Review driver file
  - `arshim.jar` - Access Review driver shim
- Access Review driver packages
  - `NOVLARBASE` - Access Review Base
  - `NOVLARDCFG` - Access Review Default Configuration
  - `NOVLARMSINFO` - Access Review Managed System Information
  - `NOVLARWDSYN` - Access Review Password Sync

1.3.2 Information Needed for Installation and Configuration

Ensure that you have the information that you need to install and configure the Access Review driver. For more information about the process, see Section 2.1, “Checklist for Installing and Configuring the Driver,” on page 13.

Access Review settings

- Host and port of the Access Review server
- URL for the Access Review application
- (Conditional) For https connectivity, security certificate for the Access Review application
- Account and password for a global or data administrator in Access Review
- Account and password for the administrator of the Access Review databases
- Name of the Operations table in the Access Review database, by default `arops`
- OSP client name and password for Access Review in the Roles Based Provisioning Module configuration utility

Identity Manager settings

- Host and port for the Remote Loader running on the Access Review server
- DN for the User Application driver
- URL for the User Application where an administrator creates user accounts

  By default, the URL contains `IDMProv`.
- (Conditional) For https connectivity, security certificate for the User Application
- Account and password for an administrator of the User Application

2 Installing and Configuring the Access Review Driver

The installation and configuration process for the Access Review driver requires access to the Access Review server, Identity Manager Remote Loader, and Designer for Identity Manager. This guide makes the following assumptions:

- Access Review is not installed on the same server as the Identity Manager engine or the identity applications.
- The Access Review driver is installed with the Identity Manager Remote Loader on the same server as Access Review.

Ensure that you have activated Identity Manager. You do not need to activate the Access Review driver.

2.1 Checklist for Installing and Configuring the Driver

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

	Checklist Items
❑	1. Review the considerations for installing and configuring the Access Review driver. For more information, see Section 1.3.2, “Information Needed for Installation and Configuration,” on page 12.
❑	2. Ensure that your environment meets the requirements for installing and configuring the Access Review driver. For more information, see Section 1.3, “Planning to Install and Configure the Driver,” on page 11.
❑	3. Install the Remote Loader and the driver files on the Access Review server. For more information, see Section 2.2, “Installing the Remote Loader and Driver Files,” on page 14.
❑	4. Ensure that the Access Review driver can perform provisioning tasks in the identity applications. For more information, see Section 2.3, “Creating an Identity Manager Provisioning Service Account for the Driver,” on page 16.
❑	5. Ensure that you have the appropriate packages installed and imported for the Access Review driver, User Application driver, and notifications object in Designer. For more information, see Section 2.4.1, “Updating the Base Package for the Access Review Driver,” on page 16.
❑	6. Configure the basic settings for the Access Review driver. For more information, see Section 2.4.2, “Configuring the Access Review Driver,” on page 17.
❑	7. Apply the system account that you created in the identity application for the driver. For more information, see Section 2.4.3, “Adding the Driver Account to the Access Review Driver,” on page 18.
❑	8. Deploy the updated Access Review driver, User Application driver, and notifications object. For more information, see Section 2.4.4, “Deploying the Access Review Driver and Supporting Objects,” on page 18.

	Checklist Items
❑	9. Ensure that Access Review can integrate collected permissions and permission assignment tasks with the role and resource catalog in Identity Manager. For more information, see Section 2.5, “Configuring Access Review,” on page 19.

2.2 Installing the Remote Loader and Driver Files

The files for the Access Review driver need to be on the same server where you install the Remote Loader.

2.2.1 Installing the Remote Loader

The Remote Loader loads drivers and communicates with the Identity Manager engine on behalf of drivers installed on remote servers. To ensure appropriate communication between the Access Review driver and Identity Manager, NetIQ recommends that you install the Remote Loader on the Access Review server.

For more information about installation, see “Installing and Managing the Remote Loader” in the *NetIQ Identity Manager Setup Guide*.

2.2.2 Adding the Access Review Driver File to the Identity Vault

This section provides information for downloading and adding the latest `arshim.jar` file for the Access Review driver to the Identity Vault server. Ensure that you have the most recent `NIdM_Driver_4.5_AR1-1.zip` file from the Identity Manager 4.5 Downloads page.

Adding the Driver File to the Identity Vault on a Linux Server

By default, NetIQ installs the Identity Vault in the `/opt/novell/eDirectory/` folder.

1. Log in to the Identity Vault server as `root` or Administrator.
2. Copy and extract the `NIdM_Driver_4.5_AR1-1.zip` file to a temporary location on the server.
3. Stop eDirectory.
4. To remove the old `.rpm` file, enter the following command:

   ```
   rpm -ev novell-DXMLarshim
   ```

5. In a terminal, navigate to the *`extracted_location`*`/NIdM_Driver_4.5_AR1-1/Linux` folder.
6. Enter the following command:

   ```
   rpm -ivh ./netiq-DXMLarshim.rpm
   ```

7 (Optional) To verify the `.rpm` version that is currently installed, enter one of the following commands:

- `rpm -qa |grep -i "netiq"`
- `rpm -qi netiq-DXMLarshim`

8 Start eDirectory.

Adding the Driver File to the Identity Vault on a Windows Server

By default, NetIQ installs the Identity Vault in the `C:\NetIQ\IdentityManager\NDS` directory.

1 Log in to the Identity Vault server as Administrator.

2 Copy and extract the `NIdM_Driver_4.5_AR1-1.zip` file to a temporary location on the server.

3 Stop eDirectory.

4 Delete the old `arshim.jar` file from the `eDirectory\lib` folder.

5 Copy the `arshim.jar` file from the *`extracted_location`*`/Windows/lib` folder to the `eDirectory\lib` folder.

6 Start eDirectory.

2.2.3 Adding the Access Review Driver Files to the Remote Loader Server

This section provides information for adding the files for the Access Review driver to the Remote Loader server.

1 Log in to the server where you installed the Remote Loader.

NetIQ recommends that you install the Remote Loader on the Access Review server.

2 Copy the `arshim.jar` file from the Identity Vault server to the `lib` directory for the Remote Loader, located by default in the `opt/novell/eDirectory/lib/dirxml/classes` directory.

3 In the `lib` directory, install the third-party JDBC driver that supports the Access Review database, either Oracle or Postgres.

4 In the `/etc/opt/novell/dirxml/rdxml` directory, create a text file that defines the classpath for the Access Review driver. For example:

```
-description "AR Driver"
-commandport 8000
-connection "port=8090"
-trace 3
-tracefile "/opt/netiq/ar.log"
-tracefilemax 100M
-class "com.novell.nds.dirxml.driver.arshim.AccessReviewDriverShim"
```

For more information about classpaths, see “Installing and Managing the Remote Loader” in the *NetIQ Identity Manager Setup Guide*.

5 Note the port number associated with the Remote Loader instance. You need this value when configuring the driver in Designer.

2.3 Creating an Identity Manager Provisioning Service Account for the Driver

The Access Review driver needs a user account in Identity Manager to grant and revoke permissions. The account must have **Resource Administrator** permissions in the identity applications.

1. Log in to Identity Manager Home as an administrator.
2. To create the new system account, complete the following steps:
   - **2a** Select **Create Users and Groups**.
   - **2b** Create a new User object for a system account. For example, in the `OU=sa,O=data` container, create an object called `driverProvServiceAcct`.
   - **2c** Specify values for the required fields for the new user, and then select **Continue**.
   - **2d** Specify a password for the new user object.
3. To assign resource administrator permissions to the account, complete the following steps:
   - **3a** Select **Administration > RBPM Provisioning and Security**.
   - **3b** Select **Administrator Assignments > Assign**.
   - **3c** Specify a description for this assignment request. For example, `Resource Provisioning Account`.
   - **3d** For **Domain**, specify **Resource**.
   - **3e** For **User(s)**, specify the name that you assigned to the new User object.
   - **3f** Select **All Permissions**.
   - **3g** Select **Assign**.
4. Log out of Identity Manager Home.

2.4 Preparing the Access Review Driver

This section helps you create, configure, and deploy the Access Review driver. You perform these tasks in your project in Designer.

2.4.1 Updating the Base Package for the Access Review Driver

NetIQ regularly provides updates to the Identity Manager drivers. You must have the latest content for the Access Review driver, User Application driver, and notifications object. For more information about the packages, see Section 1.3.1, “Installation Requirements,” on page 11.

1. Open Designer.
2. Select **Help > Check for Package Updates**.

3 Select the updated packages that you want to update, including packages for the User Application driver and notification templates.

4 Click **Yes**.

5 When the update completes, restart Designer.

2.4.2 Configuring the Access Review Driver

This section helps you configure the Access Review driver and establish its basic settings.

The driver interacts with Access Review through database views. It uses the Access Review administrator account as well as an account in the Identity Manager identity applications. When configuring the driver, you need information about Access Review and Identity Manager settings. For more information about required settings, see Section 1.3.2, “Information Needed for Installation and Configuration,” on page 12.

NOTE: The Access Review driver requires the driver set packages for common settings: `NOVLACOMSET` and `NOVLCOMSET`. Ensure that you import these packages before configuring the driver. For more information about the packages, see Section 1.3.1, “Installation Requirements,” on page 11.

---

1 In the **Modeler** view of Designer, select **Developer**.

2 (Conditional) If you have more than one driver set in the Identity Vault, select the driver set in the **Modeler** view to which you want to add the driver.

3 In the **Palette** view, expand **Service**.

4 Drag **Access Review** to the **Modeler** view.

This action opens the Driver Configuration Wizard.

5 For **Select Driver Base Configuration,** select **Access Review Base**, then click **Next**.

6 For **Optional Features**, select the following items:

- `Default Configuration`
- `Managed System Information`
- `Password Synchronization`

7 Click **Next**.

8 For **Driver Name**, specify a value. For example, `Access Review Driver`.

9 Click **Next**.

10 For **Application Authentication**, specify the settings for connecting to the Access Review database: user account and account password.

11 For **Driver Parameters**, specify the settings that allow the Access Review driver to communicate with the Access Review server and the User Application.

The following sections provide guidance for configuring some of the settings.

Publisher Options

Represents the settings that Identity Manager needs to manage application permissions received from Access Review. Identity Manager uses the User Application administrator account to dynamically create `nrfResourceDefs` permission folders and `nrfResource` objects. The folders and objects are stored in a base container within the `ResourceDefs` folder of the User Application driver.

The default container name is `ACCESS_REVIEW_RESOURCES`.

Allow IDM Account creation?

Represents the settings that allow Identity Manager to create new users based on the identities published from the Access Review repository. To add user accounts, the driver uses an account in Access Review that has the Data Administrator or Global Administrator role. The Access Review connection parameters grouped with this option enable the driver to update the Access Review Identities with critical IDM naming attributes after they are successfully added to Identity Manager. This option also controls the behavior of user object migration since this also requires the ability to update the Access Review Identities with IDM naming attributes.

Publisher User Object Placement

Specifies the folder in the Identity Vault that stores the users created by the driver. The default value is `data/users/arusers`. For more information, see the following sections:

- Section 2.5.2, "Integrating Access Review Data with Identity Manager," on page 19
- "Integrating Collected Data with Identity Manager" in the *NetIQ Access Review User Guide*

12 Click **Finish**.

2.4.3 Adding the Driver Account to the Access Review Driver

This section helps you apply the system account that you created for the driver in the identity applications to the driver. For more information about the account, see Section 2.3, "Creating an Identity Manager Provisioning Service Account for the Driver," on page 16.

NOTE: Identity Manager shares Global Configuration Values (GCVs) with the entire driver set, the Role and Resource driver, and Access Review driver. NetIQ recommends that you periodically review the GCVs to ensure that it does not get reset by installations of other drivers or changes to the Access Review driver.

---

1. In the **Outline** view of Designer, right-click the Access Review driver.
2. Select **Properties**.
3. In the navigation pane, select **Driver Configuration** and select **Publisher Options** tab.
4. Specify the DN and password of the service account created for `User Application Provisioning Service Account DN`.

   The **Properties** window displays the name of the service account based on the descriptive name that you created when you added the account to the GCVs for the driver set. For example, `User Application Provisioning Service Account DN`. For more information, see Section 2.3, "Creating an Identity Manager Provisioning Service Account for the Driver," on page 16.
5. Click **OK**.

2.4.4 Deploying the Access Review Driver and Supporting Objects

After you create, configure, or modify the driver, you must deploy the Access Review driver, User Application driver, and notifications object.

1. In the **Modeler** or **Outline** view of Designer, right-click **Driver Set** or the driver set where you installed the Access Review driver.
2. Select **Live > Deploy**.

3 Select **Deploy**, then select **OK**.

4 Right-click the Access Review driver, then repeat the two deployment steps.

5 Deploy the User Application driver.

6 Deploy the Default Notification Collection object.

7 (Conditional) If Identity Manager requests Security Equivalences values, set equivalence to the `admin.sa.system` user.

2.5 Configuring Access Review

Access Review uses the Access Review driver to integrate collected permissions and permission assignment tasks with the role and resource catalog in Identity Manager. To do so, you must modify the Access Review configuration settings.

- Section 2.5.1, “Integrating the Driver with Access Review,” on page 19
- Section 2.5.2, “Integrating Access Review Data with Identity Manager,” on page 19

2.5.1 Integrating the Driver with Access Review

You must configure Access Review to support integration with the Access Review driver. NetIQ provides the AR Configuration utility, which allows you to modify settings for Access Review. For more information about using the utility, see “Configuring Access Review Settings” in the *NetIQ Access Review User Guide*.

1 Log in to the server that hosts Access Review.

2 Navigate to the installation directory for Access Review. For example, `opt/netiq/idmapps/accessreview`.

3 To run the utility, enter the following command:

```
./bin/configutil.sh -password db_password
```

4 Select **Miscellaneous Settings**.

5 Select **Enable integration using Identity Manager Driver for Access Review**, then click **Save**.

6 To enable the new configuration, restart the application server that hosts Access Review.

2.5.2 Integrating Access Review Data with Identity Manager

The Access Review driver helps you integrate data that Access Review collects from application sources with role and resource data in Identity Manager. You might want to do this if your Access Review environment collects permissions from applications that are not also connected systems in Identity Manager. After you set up the integration, you can export the permissions and their assignments from the non-connected applications to Identity Manager.

For more information, see “Integrating Collected Data with Identity Manager” in the *NetIQ Access Review User Guide*.

3 Configuring Secure Communication

You can configure a secure connection for communication among the driver, Access Review, and Identity Manager.

3.1 Configuring TLS/SSL Communication with Identity Manager

To ensure that the Access Review driver communicates securely with the Access Review server and the User Application, you can configure a TLS/SSL connection. The driver supports the following types of certificates for secure communication:

- Self-signed public key certificate for the server
- Trusted root certificate of the certificate authority (CA) used to sign the server’s public key certificate

3.1.1 Using a Self-Signed Public Key Certificate

To use a self-signed public key certificate, you need the iac-certtool utility. You can download the utility from the Access Review customer portal.

1. Log in to the Access Review server as an administrator.
2. Run the iac-certtool utility.
3. Specify the URL for the Access Review application or the User Application.
4. Select **Get Certificate**.
5. If the content of the certificate is correct, select **Yes**.
6. Copy the certificate content to a text file.
7. In Designer, run the configuration wizard for the Access Review driver.
8. In the Publisher configuration section, paste the certificate content in the certificate input field.
9. Complete the configuration, and then deploy the updated driver.

3.1.2 Using a Trusted Root Certificate from a Certificate Authority

If your organization uses a public key certificate signed by a certificate authority, such as Verisign or Entrust, you must obtain the appropriate trusted root certificate that corresponds to the certificate authority. You can obtain the trusted root certificate from your organization or the certificate authority your organization used.

1. Acquire the trusted root certificate.
2. In Designer, run the configuration wizard for the Access Review driver.

3 In the Publisher configuration section, import the trusted root certificate.

4 Complete the configuration, and then deploy the updated driver.

3.2 Configuring TLS/SSL Communication with the Access Review Database

To ensure that the Access Review driver communicates securely with the Access Review database, you can configure a TLS/SSL connection. You must enable SSL for both the database and the driver.

3.2.1 Preparing the Database Platform for SSL Communication

This section provides information for creating an SSL server certificate that the PostgreSQL and Oracle database platforms can use for secure communication with the Access Review driver.

Preparing PostgreSQL for SSL Communication

1 On the server where you deployed Access Review, stop Tomcat.

2 Log in to the PostgreSQL server for Access Review.

3 Stop Postgres.

4 To generate a passphrase-protected certificate, enter the following command:

```
openssl req -new -text -out cert.req
```

5 To remove the passphrase so the server can start the postmaster automatically, enter the following command:

```
openssl rsa -in privkey.pem -out cert.pem
```

6 To convert the certificate into a self-signed certificate, enter the following command:

```
openssl req -x509 -in cert.req -text -key cert.pem -out cert.cert
```

7 Copy the following files to the `data` directory of the PostgreSQL installation:

- `cp cert.pem $PGDATA/server.key`
- `cp cert.cert $PGDATA/server.crt`

  where `$PGDATA` = `/opt/netiq/idm/apps/postgresql/data/`

8 To change the permission of the files, navigate to the /opt/netiq/idm/apps/postgresql/data/ directory and enter the following commands:

```
chown postgres:postgres server.key
chown postgres:postgres server.crt
chmod 600 server.key
```

9 In a text editor, change the SSL setting in the `$PGDATA/postgresql.conf` file to `on`. For example:

```
ssl=on
ssl_cert_file = '/opt/netiq/idm/apps/postgresql/data/server.crt' # (change
requires restart)
ssl_key_file = '/opt/netiq/idm/apps/postgresql/data/server.key'  # (change
requires restart)
```

10 Save and close the file.

11 Start Postgres.

12 (Optional) To verify that SSL communication is enabled for Postgres, complete the following steps:

12a Enter `$ ./opt/netiq/idm/apps/postgres/bin/psql -U postgres -h localhost`.

12b Verify that the output is similar to the following content:

```
psql (9.0.3)
SSL connection (cipher: DHE-RSA-AES256-SHA, bits: 256)
Type "help" for help.
```

13 Add the `server.crt` that you created in Step 7 on page 22 to the `cacert`. For example, enter the following command:

```
keytool -import -trustcacerts -alias ar -file server.crt -keystore /opt/netiq/
idm/apps/jre/lib/security/cacerts
```

14 Start Tomcat.

15 Ensure that you update the Access Review databases to recognize the secured connection.

For more information, see Section 3.2.2, “Enabling the Access Review Databases for SSL Communication,” on page 24.

Preparing Oracle for SSL Communication

To enable SSL in Oracle, you must have a certificate for the Oracle Server signed by a certificate authority (CA).

1 Download and unpack the SSL helper scripts named `ssl.ca-0.1.tar.gz`.

2 Create a certification request using Oracle Wallet Manager (`/opt/oracle/product/11gR1/db/owm`) using the following commands:

```
su –oracle
owm
```

3 Select **Wallet > New**.

4 Enter your password, then select **Yes** to create folders for the wallet.

5 Fill in the requested information, then select **OK**.

6 Highlight the certification request, then select **Operations > Export Certificate Request**.

7 Save the file with the extension `.csr` in the folder where you extracted `ssl.ca-0.1.tar.gz` then save the wallet.

8 Create a self-signed `root` certificate by running the `new-root-ca.sh` script in the `ssl.ca-0.1` folder that you extracted in the previous step to create a file called `ca.crt`.

9 To run the script that creates the self-signed server certificate, enter the following command:

```
./sign-server-cert.sh CerReq
```

10 Import the `ca.crt` into the Oracle wallet as a trusted certificate and import the *`certificate-request-filename.crt`* as a user certificate.

11 Enable auto-login and save the wallet so that it is now ready for use.

12 To configure Oracle advanced security and listener configuration on the database server, run the following commands:

```
su – oracle
netmgr
```

13 Select **Profile > Select Network Security > SSL**.

14 Ensure that the `sqlnet.ora` and `listener.ora` files mention the `WALLET`.

15 (Conditional) If the `SSL_CLIENT_AUTHENTICATION` parameter is not set, the default setting is `TRUE` and clients are required to present a certificate during the SSL handshake. If you do not need client authentication, disable it with the following parameter added to the end of the `$TNS_ADMIN/listener.ora` and `$TNS_ADMIN/sqlnet.ora` files:
`SSL_CLIENT_AUTHENTICATION=FALSE`

16 Restart the listener:

```
lsnrctl stop
lsnrctl start
```

17 Ensure that you update the Access Review databases to recognize the secured connection.

For more information, see Section 3.2.2, “Enabling the Access Review Databases for SSL Communication,” on page 24.

3.2.2 Enabling the Access Review Databases for SSL Communication

To use TLS/SSL connections, the three Access Review databases need the server certificate information. This section applies to both Oracle and PostgreSQL platforms.

1 Enable SSL functionality in the database platform.

For more information, see “Preparing PostgreSQL for SSL Communication” on page 22 or “Preparing Oracle for SSL Communication” on page 23.

2 Log in to the server where you deployed Access Review.

3 Stop Tomcat:

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

4 Add the SSL server certificate that you created for the database platform to the `cacert`. For example:

Postgres

```
keytool -import -trustcacerts -alias ar -file server.crt -keystore /opt/
netiq/idm/apps/jre/lib/security/cacerts
```

Oracle

```
keytool -import -trustcacerts -alias aroracle -file ca.crt -keystore /opt/
netiq/idm/apps/jre/lib/security/cacerts
```

5 In a text editor, open the `server.xml` file.

6 For the three Access Review databases listed in the file, specify the URL for the SSL server certificate. For example:

Postgres

```
url="jdbc:postgresql://hostname:5432/database_username?ssl=true"
```

Oracle

```
url="jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS = (PROTOCOL = TCPS)(HOST =
hostname)(PORT = 2484))(CONNECT_DATA =(SERVER = DEDICATED) (SERVICE_NAME =
name))(SECURITY=(SSL_SERVER_CERT_DN='CN=OracleDB,OU=IN,O=IN,L=IN,ST=IN,C=I
N')))"
```

By default, the databases have the usernames `arops`, `ardcs`, and `arwf`.

7 Start Tomcat:

```
/etc/ini.d/idmapps_tomcat_init start
```

8 Ensure that you update the Access Review driver to recognize the secured connection.

For more information, see Section 3.2.3, “Enabling the Access Review Driver for SSL Communication,” on page 25.

3.2.3 Enabling the Access Review Driver for SSL Communication

The Access Review driver can communicate securely with the Access Review databases. Ensure that you also enable SSL communication in the databases. For more information, see “Preparing PostgreSQL for SSL Communication” on page 22 or “Preparing Oracle for SSL Communication” on page 23.

1 Log in to the server where you installed the Access Review driver and Remote Loader.

2 Stop the Remote Loader. For example, enter the following command:

```
rdxml -config /home/ARShim.conf -u
```

3 In a text editor, open the Remote Loader `conf` file for the driver, by default `ARshim.conf`.

4 Add the content of the SSL server certificate to the file. For example:

Postgres

```
-description ARDriver
-commandport 8000
-connection "port=8090 rootfile=path/server.crt"
-trace 5
-tracefile "/opt/netiq/ar.log"
-tracefilemax 100M
-class "com.novell.nds.dirxml.driver.arshim.AccessReviewDriverShim"
```

Oracle

```
-description ARDriver
-commandport 8000
-connection "port=8090 rootfile=path/ca.crt"
-trace 5
-tracefile /tmp/remoteloader.log
-class com.novell.nds.dirxml.driver.arshim.AccessReviewDriverShim
```

5 Save and close the file.

6 Add the server certificate to the Remote Loader java certs. For example:

Postgres

```
keytool -import -trustcacerts -alias ar -file server.crt -keystore /opt/
novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts
```

Oracle

```
keytool -import -trustcacerts -alias aroracle -file ca.crt -keystore /opt/
novell/eDirectory/lib64/nds-modules/jre/lib/security/cacerts
```

7 Start the Remote Loader. For example, enter the following command:

```
rdxml -config /home/ARShim.conf
```

8 In the AR Driver configuration, verify that the setting for **Access Review Database Connection URL** resembles one of the following values:

Postgres

```
url="jdbc:postgresql://hostname:5432/database_username?ssl=true"
```

Oracle

```
jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS = (PROTOCOL = TCPS)(HOST =
hostname)(PORT = 2484))(CONNECT_DATA =(SERVER = DEDICATED) (SERVICE_NAME =
name))(SECURITY=(SSL_SERVER_CERT_DN='CN=OracleDB,OU=IN,O=IN,L=IN,ST=IN,C=I
N')))
```

By default, the databases have the usernames `arops`, `ardcs`, and `arwf`.

9 Restart the Access Review driver.