Oracle® Fusion Middleware

Administrator's Guide for Oracle Identity Navigator

11g Release 2 (11.1.2.2)

E27135-05

December 2013

Oracle Identity Navigator is an administrative portal designed to act as a launch pad for Oracle Identity Management products. This book describes how to configure and use Oracle Identity Navigator.

ORACLE®

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator 11g Release 2 (11.1.2.2)

E27135-05

Contents

3   Using the Oracle Identity Navigator Dashboard

Preface

Oracle Identity Navigator is an administrative portal designed to act as a launch pad for Oracle Identity Management products. This book describes how to configure and use Oracle Identity Navigator.

Audience

This document is intended for Oracle Identity Navigator administrators and Oracle Identity Management component administrators.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11*g* documentation set.

- *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introduction to Oracle Identity Navigator

Oracle Identity Navigator is an administrative portal designed to act as a single launch pad for accessing the administration consoles for other Oracle Identity Management components. It does not replace the individual component consoles. Rather, it allows you to access the Oracle Identity Management consoles centrally from one location. This chapter contains the following topics:

- Section 1.1, "Relationships with Other Components"
- Section 1.2, "Single Sign-On Integration"
- Section 1.3, "Common Admin Roles"
- Section 1.4, "Administrative Role Types"
- Section 1.5, "Reports"
- Section 1.6, "News and Announcements"
- Section 1.7, "System Requirements and Certification"

1.1 Relationships with Other Components

Oracle Identity Navigator is installed with other Oracle Identity Management components and centralizes access to product administration consoles, as well as other identity services. Oracle Identity Navigator can be installed with other Oracle Identity Management components in the same domain or in different domains. It is a web-based application that you access through a browser.

Starting with 11*g* Release 2 (11.1.2.2), Oracle Identity Navigator is deployed in a managed server after installation. The default server name is `opam_server1`. However, Oracle Privileged Account Manager will not be configured unless selected in the configuration wizard.

You can use Oracle Identity Navigator to access the following product administration consoles and identity services:

- Oracle Access Management Access Manager
- Oracle Adaptive Access Manager
- Oracle Authorization Policy Manager
- Oracle Directory Services Manager
- Oracle Directory Integration Platform
- Oracle Enterprise Manager
- Oracle Entitlements Server

- Oracle Identity Analytics

- Oracle Access Management Identity Federation

- Oracle Identity Manager

- Oracle Privileged Account Manager

- Oracle Role Manager

- Oracle WebLogic Server

- Oracle Web Services Manager

Figure 1–1 shows the following relationships between Oracle Identity Navigator and the Oracle Identity Management components:

- Each administration console launches in its own separate browser window. You configure Oracle Identity Navigator to connect to these consoles either by specifying the URLs directly, or by employing the product discovery feature.

- Like Oracle Enterprise Manager Fusion Middleware Control, Oracle Identity Navigator is a Java EE application deployed on an Oracle WebLogic Server. It uses Oracle Metadata Service.

- The Oracle Identity Navigator report feature relies on Oracle Business Intelligence Publisher and requires configuration to communicate with an Oracle Business Intelligence Publisher server.

- You can access Oracle RSS feeds and view them in the Dashboard. You might need to configure a proxy to connect through your company's firewall.

Figure 1–1   Relationships Between Oracle Identity Navigator and Other Components
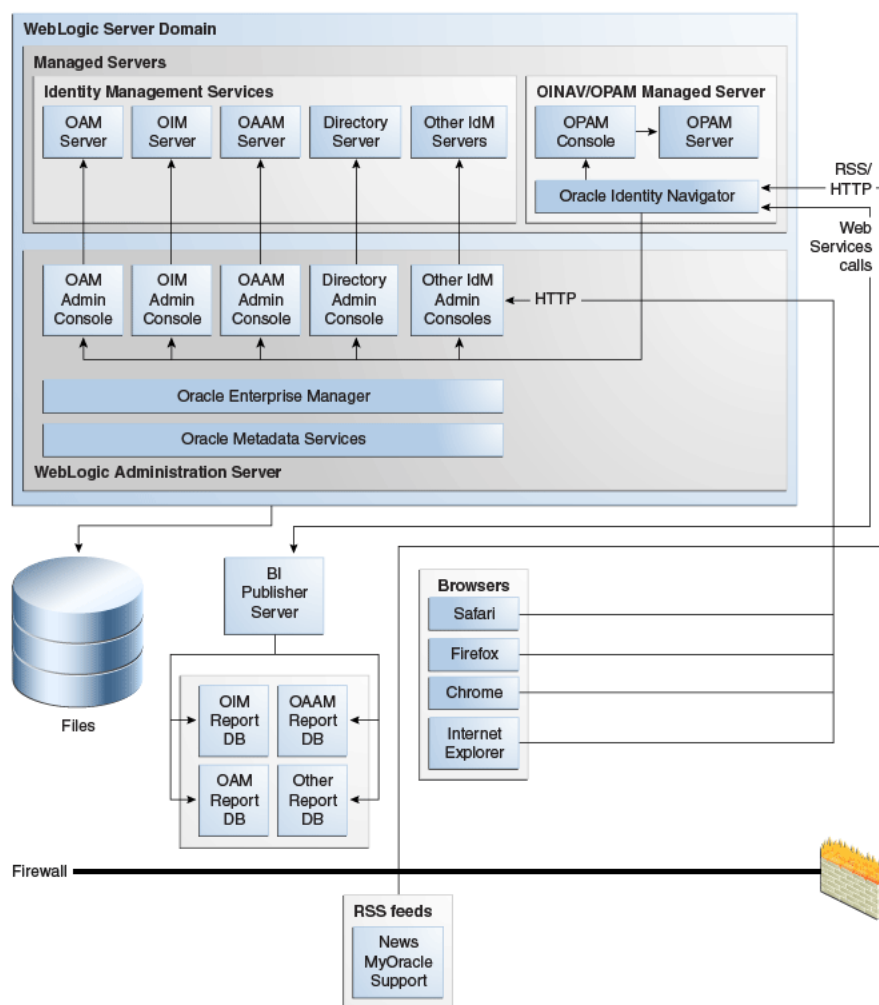
1.2 Single Sign-On Integration

Oracle Identity Navigator is integrated with 11*g* Oracle Platform Security Services for single sign-on (SSO) support. Some of the component consoles accessible from Oracle Identity Navigator are single sign-on enabled and can be configured to authenticate against the same authentication service in the Oracle Identity Navigator operation environment. Single sign-on enabled consoles include Oracle Access Management, Oracle Identity Manager, Oracle Adaptive Access Manager, Oracle Authorization Policy Manager, and Oracle Privileged Account Manager. Double sign-on occurs for other components, such as Oracle Directory Services Manager and Oracle Enterprise Manager Fusion Middleware Control. For more information, see Section 2.3, "Configuring Single Sign-On (SSO)".

1.3 Common Admin Roles

Common Admin Roles are a set of predefined standardized application roles for securing administrative access to Oracle Identity Management applications. These roles encapsulate the common administrative tasks across the Oracle Identity Management Suite.

> **Note:** You must configure enterprise roles to support the Common Admin Roles before you can begin using them. For more information, see Section 2.2, "Configuring the Enterprise Roles".

Common Admin Roles can be assigned to users from the Oracle Identity Navigator Administration page. Each administrative role enables a corresponding set of rights that are common across the Identity Management Suite components.

Table 1–1 describes the responsibilities each role type supports and the skills and expertise required in order to perform typical duties associated with that role. You can assign any of the roles described in Table 1–1 to a user as a component role. Once a role assignment is made, the user is granted the corresponding administrative capabilities for that component.

Table 1–1   Summary of the Common Admin Roles

Common Admin Role Name	Responsibility	Skills and Expertise Required
Application Configurator	■ Use Identity Management applications to support business requirements within an assigned business scope.	■ Strong knowledge of product features. ■ Good knowledge of business requirements.
Application Auditor	■ Use Identity Management application to support business requirements within an assigned business scope.	■ Strong knowledge of product features. ■ Good knowledge of business requirements related to transactional pattern analysis.
Application Troubleshooter	■ Use Identity Management application to support business-specific troubleshooting or investigation.	■ Strong knowledge of analysis features.
Security Auditor	■ Provide audit reports to upper management. ■ Verify permissions and generate access reports. ■ Verify proper configuration of Identity Management applications.	■ Strong knowledge of access management processes. ■ Strong knowledge of the risks associated with unauthorized access. ■ Good understanding of information security and system architecture.
Security Admin	■ Configure Identity Management application roles and approve role grants. ■ Configure Identity Management applications to work with corporate infrastructure and applications. ■ Maintain system credentials for identity stores, key stores, databases, and other repositories. ■ Grant administrative roles and permissions.	■ Strong knowledge of corporate infrastructure. ■ Strong technical knowledge to troubleshooting infrastructure access rights. ■ Strong knowledge of Identity Management security architecture.
User Manager	■ Create, modify, and delete users and groups. ■ Reset passwords and unlock accounts.	■ Strong knowledge of corporate identity infrastructure.
Helpdesk Admin	■ Reset passwords and unlock accounts. ■ Troubleshoot access problems.	■ Strong knowledge of corporate applications. ■ Strong knowledge of troubleshooting infrastructure access rights.

1.4 Administrative Role Types

Actions that an authenticated user can perform are based on the roles assigned. Oracle Identity Navigator supports two types of administrative roles:

- Administrators with Common Admin Roles

  Administrators with Common Admin Roles specific to Oracle Identity Navigator can administer Oracle Identity Navigator as summarized in Table 1–2.

- Component administrators

  A component administrator manages a specific Identity Management component. These role types can be finer grained than the Common Admin Role. For more information, see Section 2.9, "Advanced: Configuring Component Administrative Role-Based Access".

Table 1–2 describes the Common Admin Roles that are specific to Oracle Identity Navigator and the access rights each conveys. All authenticated users can access My Profile and News and Announcements.

Table 1–2   Summary of Oracle Identity Navigator Common Admin Roles

Common Admin Role Name	Access Rights
Security Admin	- Access to all the product links in the Product Launcher. - Access to the Access Privileges page for User/Role search and assignment.
Security Auditor	- Access to all the product links in the Product Launcher. - Access to the My Reports page with full privileges for reports.
Application Configurator	- Access to all the product links in the Product Launcher. - Access to BI Publisher, including configuration, report folder mapping, and assignment to product components. - Access to Product Registration, including Discover Products and Product Links setup.

After installation, all users who are members of the Oracle WebLogic Server Administrators group are granted all superuser privileges required to administer Oracle Identity Navigator. The default administrator is the weblogic user (also known as the *bootstrap* user) who is a member of the Administrators group.

The weblogic user, as the bootstrap user, can be used to map the users from the domain identity store to the Oracle Identity Navigator Common Admin Roles detailed in Table 1–2. Users mapped to the Security Admin role can assign the Common Admin Roles to other users, and can later replace the weblogic user in your environment. After the initial user mapping is completed, replace the default weblogic user by mapping the Security Admin role to at least one administrator user defined in your domain identity store.

> **Note:** Administration roles specific to Oracle Privileged Account Manager are managed in Oracle Identity Navigator. For information about managing Oracle Privileged Account Manager roles, see *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

1.5 Reports

Oracle Identity Navigator supports a set of default reports. These reports provide meaningful information to auditors for examining the security practices of the component as deployed, as well as enabling a check of the component health status.

1.5.1 Oracle Business Intelligence Publisher

All reports are generated using Oracle Business Intelligence Publisher. Oracle BI Publisher 11.1.1.5.0, or higher, must be installed separately. See Section 2.5.2, "Configuring Oracle Business Intelligence Publisher" for more information on installing and configuring Oracle BI Publisher.

1.5.2 My Reports

My Reports is a portlet used to view Oracle Identity Management BI Publisher Reports. In addition, the My Reports portlet allows you to save a report query so you can run the report again. Every administrative user has their own My Reports portlet in the Dashboard page. You can add report categories to My Reports and save different reports under different categories. Reports are categorized by the component name.

The following tasks can be performed in My Report:

- Show a list of Oracle Identity Management BI Publisher Reports in a portlet configuration page.

- Select, add configuration parameters to query the data, and add the report to My Reports list from a portlet configuration page.

- View and run any report that the you have access to.

For more information about using My Reports, see Section 3.4, "Managing Your Reports".

1.6 News and Announcements

Oracle Identity Navigator supports the following three Oracle RSS feeds:

- Identity Management Discussion Forum

- Oracle New Downloads

- Oracle Security Alerts

The RSS feeds can not be changed.

1.7 System Requirements and Certification

Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other

information. Both of these documents are available on Oracle Technology Network (OTN).

The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

The certification document covers supported installation types, platforms, operating systems, databases, JDKs, and third-party products:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

2

Managing Oracle Identity Navigator

This chapter describes the common configuration and management tasks an enterprise administrator can perform while using Oracle Identity Navigator. This chapter contains the following topics:

2.1 Configuring the Identity Store

> **Note:** This section provides information about configuring the domain identity store using Oracle Internet Directory or Oracle Virtual Directory with a supported LDAP-based directory server. For information about other supported identity stores, see Section 1.7, "System Requirements and Certification".
>
> Consult the vendor product documentation for information about configuring the identity store in your environment.

A domain identity store must be configured before you can view users when searching from the Access Privileges pane. To configure the identity store as the main authentication source, you must configure the Oracle WebLogic Server domain where Oracle Identity Navigator is installed. Configuration is done in the WebLogic Server Administration Console.

The Control Flag attribute for the authenticator provider must be set to determine the ordered execution of the Authentication providers. The possible values for the Control Flag attribute are:

- REQUIRED - This LoginModule must succeed. Even if it fails, authentication proceeds down the list of LoginModules for the configured Authentication providers. This setting is the default.

- REQUISITE - This LoginModule must succeed. If other Authentication providers are configured and this LoginModule succeeds, authentication proceeds down the list of LoginModules. Otherwise, control is returned to the application.

- SUFFICIENT - This LoginModule need not succeed. If it does succeed, return control to the application. If it fails and other Authentication providers are configured, authentication proceeds down the LoginModule list.

- OPTIONAL - This LoginModule can succeed or fail. However, if all Authentication providers configured in a security realm have the JAAS Control Flag set to OPTIONAL, the user must pass the authentication test of one of the configured providers.

For more information about creating a new default authenticator in Oracle WebLogic Server, see *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* and *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

To configure the OID authenticator in Oracle WebLogic Server:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, myrealm.

3. Select the **Providers** tab, then select the **Authentication** sub-tab.

4. Click **New** to launch the Create a New Authentication Provider page. Complete the fields as follows:

    - **Name**: Enter a name for the authentication provider. For example, MyOIDDirectory.

    - **Type**: Select **OracleInternetDirectoryAuthenticator** from the list.

    - Click **OK**. The authentication providers table is updated.

5. In the authentication providers table, click the newly added authenticator.

6. In Settings, select the **Configuration** tab, then select the **Common** tab.

    - Set the Control Flag to **SUFFICIENT**.

    - Click **Save**.

7. Select the **Provider Specific** tab and enter the following required settings using values for your environment:

    - **Host**: The host name of the Oracle Internet Directory server.

    - **Port**: The port number on which the Oracle Internet Directory server is listening.

    - **Principal**: The distinguished name (DN) of the Oracle Internet Directory user to be used to connect to the Oracle Internet Directory server. For example: cn=OIDUser,cn=users,dc=us,dc=mycompany,dc=com.

    - **Credential**: Password for the Oracle Internet Directory user entered as the Principal.

    - **Group Base DN**: The base distinguished name (DN) of the Oracle Internet Directory server tree that contains groups.

- **User Base DN**: The base distinguished name (DN) of the Oracle Internet Directory server tree that contains users.

- **All Users Filter**: LDAP search filter. Click **More Info...** for details.

- **User From Name Filter**: LDAP search filter. Click **More Info...** for details.

- **User Name Attribute**: The attribute that you want to use to authenticate (for example, `cn`, `uid`, or `mail`). For example, to authenticate using a user's email address you set this value to `mail`.

8. Click **Save**.

9. From the Settings for myrealm page, select the **Providers** tab, then select the **Authentication** tab.

10. Click **Reorder**.

11. Select the new authenticator and use the arrow buttons to move it into the first position in the list.

12. Click **OK**.

13. Click **DefaultAuthenticator** in the Authentication Providers table to display the Settings for DefaultAuthenticator page.

14. Select the **Configuration** tab, then the **Common** tab, and select **SUFFICIENT** from the Control Flag list.

15. In the Change Center, click **Activate Changes**.

16. Restart Oracle WebLogic Server.

To use Oracle Virtual Directory as the domain identity store, you must do the following:

- Configure Oracle Virtual Directory with the LDAP-based server. For more information, see "Creating LDAP Adaptors" in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

- Configure the OVD authenticator in Oracle WebLogic Server. For more information, see *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

2.2 Configuring the Enterprise Roles

Enterprise roles must be created in the domain identity store to support the Common Admin Roles. Templates are provided for both Oracle Internet Directory and Oracle Virtual Directory configured with an LDAP-based directory server. The template is used with the `ldifmigrator` tool.

Pre-requisites to configuring enterprise roles for the Common Admin Roles:

1. The domain identity store must be configured. For more information, see Section 2.1, "Configuring the Identity Store".

2. The domain policy store must be configured. For more information, see *Oracle Fusion Middleware Application Security Guide*.

For more information about supported identity and policy store configurations for Oracle Identity Navigator, see Section 1.7, "System Requirements and Certification".

To configure enterprise roles in the domain identity store:

1. Select the template for your environment from ORACLE_ HOME/common/templates.

   - Oracle Internet Directory: use oinav_template_oid.ldif

   - Oracle Virtual Directory: use oinav_template_ovd.ldif

2. To use the `ldifmigrator` tool, set $JAVA_HOME and include JAVA_ HOME/bin in PATH.

3. Use the `ldifmigrator` tool to create the enterprise roles in the identity store under *<GroupBase>* as follows, where *<ldif template>* is the template name:

```
Run
java -cp $MIDDLEWARE_HOME/oracle_common/modules/oracle.ldap_
11.1.1/ldapjclnt11.jar -DORACLE_HOME=$ORACLE_HOME/oracle_common
oracle.ldap.util.LDIFMigration   input_file=<ldif template>  output_
file=<outputfile>  namespace=<GroupBase>  -load dn=<bindDn> password=<>
host=<hostName> port=<portNumber>
```

When using Oracle Virtual Directory with an LDAP-based directory server, the `host`, `port`, `dn`, and `groupbase` refer to Oracle Virtual Directory and not the LDAP server.

2.3 Configuring Single Sign-On (SSO)

By default, the Oracle Access Manager 11*g* agent provides single sign-on functionality for Oracle Identity Navigator and the following Identity Management consoles:

- Oracle Identity Manager

- Oracle Access Management

- Oracle Adaptive Access Manager

- Oracle Authorization Policy Manager

- Oracle Privileged Account Manager

The Access Manager agent can only protect consoles in a single domain. If your environment spans multiple domains, you can use Access Manager 11*g* Webgate for Oracle HTTP Server 11*g*. To configure Oracle Identity Navigator for Webgate-based single sign-on, see the chapter "Integrating with Oracle Identity Navigator" in *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

2.4 Configuring Secure Socket Layer (SSL)

The web.xml file provides configuration and deployment information for a Web application, such as Oracle Identity Navigator. The Oracle Identity Navigator web.xml file is located in oinav.ear. The optional `<user-data-constraint>` element in web.xml can be used to specify a transport guarantee that prevents content from being transmitted insecurely. Within the `<user-data-constraint>` tag, the `<transport-guarantee>` tag defines how communication should be handled. There are three possible values for that tag:

- NONE – the application does not require any transport guarantees.

- INTEGRAL – the application requires that data sent between the client and server be sent in a manner that it cannot be changed in transit.

- CONFIDENTIAL – the application requires that data be transmitted in a manner that prevents other entities from observing the contents of the transmission.

Because Oracle Identity Navigator supports both SSL and non-SSL connections to component consoles, the web.xml attribute `<user-data-constraint>` is set to a default value of `NONE`. That is, Oracle Identity Navigator does not, by default, support a constraint for a transport guarantee. If you want such a guarantee, you can change the `<transport-guarantee>` tag within the `<user-data-constraint>` tag to either `INTEGRAL` or `CONFIDENTIAL`.

2.5 Getting Started with Oracle Identity Navigator

Log in as an administrator as follows:

1. Start the WebLogic Server.

2. Enter the following URL in a browser:

   `http://host:port/oinav`

   where *port* is the Managed Server port.

3. Supply the Administrator **Username** and **Password**. The Administrator account must exist in the identity store and have the Oracle Identity Navigator Administrator role.

4. Click **Log In**.

2.5.1 Initial Configuration Tasks

You must have appropriate privileges to perform the following tasks.

1. Configure component categories. See Section 2.6, "Managing the Product Launcher". Next add components manually or by using discovery. See Section 2.6.1, "Adding a Component Link to the Product Launcher by Using Product Discovery".

   You must be the Oracle Identity Navigator administrator or have the Application Configurator Common Admin Role to perform this task.

2. Configure BI Publisher. See Section 2.5.2, "Configuring Oracle Business Intelligence Publisher".

   You must be the Oracle Identity Navigator administrator or have the Application Configurator Common Admin Role to perform this task.

3. If your RSS feed is outside a firewall, configure a proxy. See Section 2.5.3, "Configuring a Proxy to Access News Feeds".

   You must be an administrator to perform this task.

4. If needed, configure Oracle Privilege Account Manager. See Section 2.5.4, "Configuring Oracle Privileged Account Manager".

2.5.2 Configuring Oracle Business Intelligence Publisher

Oracle Identity Navigator has been integrated with Oracle BI Publisher. The integrated interface supports stronger customization than when using BI Publisher alone. Using the integrated interface enables each administrator to customize their Dashboard page. The report tree has fewer levels when viewed in Oracle Identity Navigator than when using BI Publisher alone, which reduces the number of clicks to access reports.

> **Note:** Only one Oracle Business Intelligence Publisher instance can be connected to an Oracle Identity Navigator instance.

2.5.2.1 Before You Create a Connection to BI Publisher

Before you attempt to create a connection between Oracle Identity Navigator and an instance of BI Publisher, you must install BI Publisher 11.1.1.5.0, or higher, and configure the report templates. For information about installing BI Publisher, see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*.

BI Publisher 10*g* reports are not supported. For information about how to remove any 10*g* reports, see Section 2.5.2.1.1, "Removing BI Publisher 10g Reports."

Optionally, you can configure BI Publisher for SSL. For more information, see Section 2.5.2.1.3, "Configuring BI Publisher for SSL (Optional)."

2.5.2.1.1 Removing BI Publisher 10g Reports BI Publisher 10g reports are not supported and cannot be viewed in this release. If you have upgraded from an earlier version of Oracle Identity Navigator, you can remove both the connection to the BI Publisher 10*g* instance and any 10*g* reports.

To remove the BI Publisher 10*g* reports, proceed as follows:

1. Go to the following location:

   ```
   cd DOMAIN_HOME/servers/AdminServer/tmp/_WL_user/oinav_11.1.1.3.0
   ```

   Two randomized directories are found. For example, `542tm8` and `8mz05i`.

2. Change to the directory that contains the `adf/mds/oracle-part/oracle/adf/rc/metadata/IdmNavigator` directory. For example:

   ```
   cd 542tm8/adf/mds/oracle-part/oracle/adf/rc/metadata/IdmNavigator
   ```

3. Make a back up of the `IdmNavigator` directory.

4. Remove the `BIConn.xml` file and the `mdssys` folder from the `idmNavigator` directory.

5. Restart WebLogic Server.

   You can now create a connection to BI Publisher 11.1.1.5.0 or higher. For more information, see Section 2.5.2.2, "Creating a Connection to BI Publisher."

2.5.2.1.2 Configuring BI Publisher Report Templates Oracle Identity Management BI Publisher report templates are installed as zip files under Oracle home directories. For each component, all the templates are in a single zip file. All templates are the Audit Report type.

The template zip files are located in specific directories under the component Oracle homes. For example:

Component	Directory Under Oracle Home
Oracle Adaptive Access Manager	`oaam/reports`
Oracle Access Management	`oam/server/reports`
Oracle Identity Manager	`server/reports`

Component	Directory Under Oracle Home
Oracle Privileged Account Manager	`opam/reports`

To configure the report templates, copy then unzip each zip file to the Audit Report folder located under the BI Publisher Report root folder. Copy and unzip other report-type zip files to the BI Publisher Report root folder. Use the BI Publisher web interface to configure data sources with report databases.

> **See Also:**
>
> ■ *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*.
>
> ■ "Using Audit Analysis and Reporting" in *Oracle Fusion Middleware Application Security Guide*.

2.5.2.1.3 Configuring BI Publisher for SSL (Optional) If you plan to use an SSL connection between Oracle Identity Navigator and BI Publisher, you must configure BI Publisher for SSL, as described in "Configuring BI Publisher for Secure Socket Layer (SSL) Communication" in *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*. In addition to configuring BI Publisher for SSL, you must provision a CA certificate to Oracle Identity Navigator so it can connect to BI Publisher through SSL.

To provision the CA certificate, proceed as follows:

1. Import the BI Publisher CA certificate into the Oracle WebLogic Server trust store, using the `keytool` command.

```
keytool -keystore trust_store -export -alias alias -file certificate_file
```

For example:

```
keytool -keystore truststore.jks -export -alias cacert -file cacert.cer
```

If you get a hostname verification error when you issue the `keystore` command, disable hostname verification by adding the following flag to `EXTRA_JAVA_PROPERTIES` in the file `setDomainEnv.sh`:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

Then issue the `keystore` command again.

2. Restart the WebLogic Server.

> **See Also:** *Oracle Fusion Middleware Securing Oracle WebLogic Server* for additional information about configuring SSL on the Oracle WebLogic Server.

2.5.2.2 Creating a Connection to BI Publisher

To create a connection, proceed as follows:

1. Click the **Administration** tab.

2. Expand **BI Publisher.**

3. In the right pane, enter values for **Host**, **Port**, **User**, and **Password**.

4. If you have configured Oracle Identity Navigator and BI Publisher to use an SSL connection, select **SSL**.

5. Under Specify BI Publisher report components, click **Create**.

6. Select a component and supply a name and path.

   To limit the connection entry to a subset of the reports available for the component, click the **Finder** icon and navigate to the desired path. You can have more than one path for a component. Using paths in this manner can reduce the amount of text associated with a report name on the Dashboard.

   Repeat for each component you want to add.

7. Click **Test** to verify the connection information you have supplied. A dialog will verify that the connection has succeeded or tell you why it failed.

8. If the test succeeds, click **Apply** to finish the configuration. If the test fails, consult the appropriate administrator at your site.

9. To delete a component, select it and click **Delete**, then click **Apply**.

After BI Publisher has been configured, the My Reports section of the Dashboard page will contain the link **Click here to create reports**.

> **Note:** If you change the name or path of a component, the new name or path will apply to new reports. The reports that are already saved are not modified.

2.5.3 Configuring a Proxy to Access News Feeds

You may need to specify a proxy so that Oracle Identity Navigator can access Oracle news feeds from inside your firewall. You do this by adding lines to the `setDomainEnv.sh` script, which is in the `bin` directory of your WebLogic domain. For example:

```
$MIDDLEWARE_HOME/user_projects/domains/base_domain/bin/setDomainEnv.sh
```

The file name is `setDomainEnv.sh` on Linux and UNIX systems and `setDomainEnv.cmd` on Windows systems. The script sets the domain-wide environment variables for starting and running a WebLogic Server instance. It is invoked by the `startWebLogic` and `stopWebLogic` commands.

The Identity Management Discussion Forums uses SSL. To access this feed, you must minimally add the following lines to `EXTRA_JAVA_PROPERTIES` in the `setDomainEnv.sh` file.

```
-Dhttp.proxyHost=proxy_server_host
-Dhttp.proxyPort=proxy_server_port
-Dhttp.nonProxyHosts=non_proxy_hosts
-Dhttps.proxyHost=ssl_proxy_server_host
-Dhttps.proxyPort=ssl_proxy_server_port
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.SSL.allowSmallRSAExponent=true
```

Consider this example:

- Oracle Identity Management components, including Oracle Identity Navigator are deployed in the Oracle WebLogic Server domain `mycompany.com`. The domain also contains the machines `server1.mycompany.com` and `server2.mycompany.com`.

- A firewall exists between the domain in `mycompany.com` and the Oracle news feed server. You must route news feed requests from Oracle Identity Navigator through the proxy server to the Oracle news feed site outside the firewall.

- HTTP requests sent to servers `server1.mycompany.com` and `server2.mycompany.com` need not be routed to the proxy server.

You would add the following lines to the `setDomainEnv.sh` file on the WebLogic Server.

```
EXTRA_JAVA_PROPERTIES="-Dhttp.proxyHost=www-proxy.mycompany.com
-Dhttp.proxyPort=80
-Dhttp.nonProxyHosts=server1.mycompany.com|server2.mycompany.com ${EXTRA_JAVA_
PROPERTIES}"
export EXTRA_JAVA_PROPERTIES
```

For completeness, you can also add the following additional lines:

```
-DftpProxyHost=ftp_host
-DftpProxyPort=FTP_proxy_server_port
-DsocksProxyHost=SOCKS_proxy_server_host
-DsocksProxyPort=SOCKS_proxy_server_port
```

You must restart WebLogic Server for the changes to take effect.

2.5.4 Configuring Oracle Privileged Account Manager

Oracle Privileged Account Manager manages privileged accounts that are not being managed by any other Oracle Identity Management components. After Oracle Privileged Account Manager is installed you must select a user and grant that person the Application Configurator role using the Access Privileges page. The Application Configurator user must configure Oracle Privileged Account Manager to enable communication with the Oracle Privileged Account Manager server. When this communication is successful, the Oracle Privileged Account Manager GUI will be populated with content.

For more information about this requirement, see the chapter "Getting Started with Administering Oracle Privileged Account Manager" in *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

For information about granting a role assignment to a user, see Section 2.7, "Managing Access Privileges".

2.6 Managing the Product Launcher

As an Administrator, you can modify the list of categories and components that appear on the Product Launcher.

You can add components within a category using either of two methods:

- Specify component console information.

- Specify host information and use product discovery to determine which component consoles are available.

2.6.1 Adding a Component Link to the Product Launcher by Using Product Discovery

From the Administration tab, you can use product discovery to discover all active Java EE components in the domain, including the Oracle WebLogic Server console and Oracle Enterprise Manager Fusion Middleware Control.

1. Click the **Administration** tab.

2. Under Product Registration, select **Discover Product(s)**. The Domain Selection page of the product discovery wizard appears in the right pane.

3. Specify the **Host**, **Port**, **User**, and **Password** for the server from which you want to discover components. If you are using the SSL port, select **SSL**.

    Click **Next**.

4. On the Available Products page, select the component consoles you want to add to Oracle Identity Navigator. For each console you select, specify a **Display Name**. If a category has not been selected automatically, select a category from the **Category** list.

    Click **Next**.

5. On the Product Removed page, you can optionally select previously discovered components to be removed.

    Click **Next**.

6. Review the status of the links on the Confirmation page. If necessary, click **Back** and correct any errors. When the Confirmation page is correct, click **Finish**.

2.6.2 Adding a Link to the Product Launcher Without Product Discovery

Add a link as follows:

1. Click the **Administration** tab.

2. Under Product Registration, click the **Create Product Link** icon or select **Create Product Link** from the **Actions** list.

3. In the New Product Registration dialog, select the type of component you want to add.

4. Provide values for Category, Display Name, Type, Version, Host, Port, and URL.

5. Click **OK** to add the link or **Cancel** to abandon adding the link.

2.6.3 Editing a Link

Edit a link as follows:

1. Click the **Administration** tab.

2. Under Product Registration, click the product you want to edit.

3. On the Product Registration screen, make desired changes

4. Click **Apply** to apply the changes or **Revert** to remove the changes you have made.

2.6.4 Removing a Link

Remove a link as follows:

1. Click the **Administration** tab.

2. Under Product Registration, highlight the item you want to remove.

3. Click the **Delete Product Link** icon or select **Delete Product Link** from the Actions list.

4. In the Confirmation dialog, click **OK** to proceed or click **Cancel** to cancel the deletion.

You can also use the product discovery interface to delete several links at once.

2.6.5 Adding a Category

Add a component category as follows:

1. Click the **Administration** tab.

2. Under Product Registration, select **Create Category** from the **Actions** list.

3. In the right pane, enter the component category name.

4. Click **Save**.

5. Verify that the new category has been added to the left pane.

2.6.6 Editing a Category

Edit a category as follows:

1. Click the **Administration** tab.

2. Under Product Registration, select a product category. The product category information appears tin the right pane.

3. Make the desired changes.

4. Click **Apply**.

2.6.7 Removing a Product Category

Remove a category as follows:

1. Click the **Administration** tab.

2. Under Product Registration, select a product category. The product category information appears in the right pane.

3. Select **Delete Category** from the **Actions** list.

4. Click **OK** in the confirmation dialog.

2.7 Managing Access Privileges

Use the Access Privileges page to assign Common Admin Roles to users or to view the role assignments granted to users, by component name. You can search for a user or a Common Admin Role using the Access Privileges page Search pane. If the search is successful, select from the results list and data for the user or role appears in the right pane.

When working with users, the Common Admin Roles display in a table on the right side. The different components are shown in separate table columns.

To view the Access Privileges page:

1. Click the **Administration** tab.

2. Click **Access Privileges** in the navigation panel.

2.7.1 Searching for Users

Search for users from the Search pane in the Access Privileges page.

> **Note:** You can only view users after the domain identity store has been configured as the authentication source. For more information, see Section 2.1, "Configuring the Identity Store".

To search for a user:

1. Select **User** from the Type list.

2. Provide a search string, which can be a user name, user ID, or email address, or a substring, of any of these.

3. Click the arrow. All users who match the criteria is displayed.

4. Select the desired user from the results list to view, set, or modify their access privileges. The information appears in the right pane.

2.7.2 Searching for Common Admin Roles

The Common Admin Roles must have enterprise roles configured before they will be visible in the Access Privileges page. For more information, see Section 2.2, "Configuring the Enterprise Roles".

To search for a Common Admin Role:

1. Select **Common Admin Role** from Type. The list of roles is displayed.

2. Select a role from the results list to view which users are assigned to that role. The information displays on the right.

2.7.3 Assigning a Common Admin Role

To assign a Common Admin Role to a user:

1. Search for the user by following the steps in Searching for Users.

2. Select the user name from the Search pane. The Access Privileges page displays.

3. Select the Role Name in the corresponding component column.

   For information about the access rights granted by Oracle Identity Navigator administrative role types, see Section 1.4, "Administrative Role Types".

   For information about the access rights granted by Oracle Privileged Account Manager administrative role types, see "Administration Role Types" and "Assigning the Application Configurator Role to a User" in *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

4. Click **Apply** to save the new settings or **Revert** to discard them.

2.8 Migrating Oracle Identity Navigator from Test to Production

For information about moving Oracle Fusion Middleware components, including Identity Management components, from a test environment to a production environment, see "Moving from a Test to a Production Environment" in *Oracle Fusion Middleware Administrator's Guide*.

2.9 Advanced: Configuring Component Administrative Role-Based Access

A component administrator has the privileges required to manage reports for a specific Identity Management application. Each component administrator can customize his or her own Dashboard page. Component administrators cannot access the Administration page of Oracle Identity Navigator.

Table 2–1 describes the Identity Management component specific Oracle Identity Navigator administrative roles and the access rights each conveys.

Table 2–1   Component Specific Administrative Roles

Component Specific Oracle Identity Navigator Admin Role Name	Access Right Granted
OIM_ADMIN	■ Access to all the product links in the Product Launcher. ■ Access to Oracle Identity Manager reports in My Reports page.
OAM_ADMIN	■ Access to all the product links in the Product Launcher. ■ Access to the Oracle Access Management reports in My Reports page.
OAAM_ADMIN	■ Access to all the product links in the Product Launcher. ■ Access to the Oracle Adaptive Access Manager reports in My Reports page.
OWSM_ADMIN	■ Access to all the product links in the Product Launcher. ■ Access to the Oracle Web Services Security reports in My Reports page.
OPAM_SECURITY_ AUDITOR	Access to the Oracle Privileged Account Manager reports in My Reports page.

These roles enable fine grained access control for all the reports. The following enterprise roles must be created in the domain identity store before you can begin using them:

■ OAM_ADMIN

■ OIM_ADMIN

■ OAAM_ADMIN

■ OWSM_ADMIN

■ OPAM_SECURITY_AUDITOR

After creation, users or groups that are members of the enterprise roles have the appropriate access privileges.

2.10 Troubleshooting

This section describes some problems that you could encounter while configuring or using Oracle Identity Navigator.

2.10.1 Cannot Access Oracle Identity Navigator in Browser

Problem

You enter the URL for Oracle Identity Navigator into a browser and attempt to access it. You receive an error message.

Solution

In a dual-stack, IPv4 and IPv6 environment, some URLs might be inaccessible from your browser. Consult your network administrator for more information.

2.10.2 Report Problems

Problem

You cannot create a connection to BI Publisher.

Solution

Make sure the Oracle WebLogic Server and BI Publisher server are running.

Problem

You cannot create or run a report.

Solution

Different login accounts might have different roles. If you log in as a user who does not have the Oracle Access Manager administrator role, for example, you will not be able to create Oracle Access Manager reports.

Make sure the Oracle WebLogic Server, BI Publisher server, and Oracle Database are running.

You can access BI Publisher reports from BI Publisher itself. Doing so can help you determine whether a configuration problem is due to Oracle Identity Navigator or BI Publisher.

Consult Oracle WebLogic Server logs.

Problem

You cannot view PDF reports with Adobe Reader in a browser.

Solution

Either upgrade to a newer version of Reader or configure Reader to run directly, not as an embedded function within the browser. See your Adobe Reader documentation for more information.

Problem

You cannot view a report in MHTML format.

Solution

Open the report in HTML format.

2.10.3 Cannot View the Common Admin Roles

Problem

You cannot view the Common Admin Roles in the Oracle Identity Navigator user interface.

Solution

Verify enterprise roles have been created to support the Common Admin Roles. For more information, see Section 2.2, "Configuring the Enterprise Roles".

3

Using the Oracle Identity Navigator Dashboard

This chapter describes how to access and use Oracle Identity Navigator as a component administrator. For information about managing Oracle Identity Navigator as an Oracle Identity Navigator administrator, see Chapter 2, "Managing Oracle Identity Navigator." It contains the following topics:

- Section 3.1, "Launching Oracle Identity Navigator"
- Section 3.2, "Logging in to Oracle Identity Navigator"
- Section 3.3, "Launching a Component Administrative Console"
- Section 3.4, "Managing Your Reports"
- Section 3.5, "Viewing Your Profile"
- Section 3.6, "Viewing Your Common Admin Roles"
- Section 3.7, "Reading News and Announcements"
- Section 3.8, "Personalizing Oracle Identity Navigator"

3.1 Launching Oracle Identity Navigator

Oracle Identity Navigator is installed as part of Oracle Identity and Access Management installation. To launch Oracle Identity Navigator, first start Oracle WebLogic Server, then enter the following URL in a browser:

```
http://host:port/oinav
```

where *port* is the Managed Server port.

> **Note:** In a dual-stack, IPv4 and IPv6 environment, some URLs might be inaccessible from your browser. Consult your network administrator for more information.

3.2 Logging in to Oracle Identity Navigator

Different login accounts might have different roles. If you log in as a user who does not have the Oracle Access Management administrator role, for example, you will not be able to create Oracle Access Management reports, and you won't have single sign-on access to the Oracle Access Management console.

To log in:

1. Supply the **User ID** and **Password** for the administrator account you want to log in to.

2. Click **Log In**.

3.3 Launching a Component Administrative Console

1. Click the **Dashboard** tab

2. Under Identity Management Product Launcher, click the entry.

If a product has been integrated with single sign-on, and you are logged in as an administrator with the appropriate role, you can access its console without logging in again.

3.4 Managing Your Reports

Adding a report to the My Reports portlet enables you to designate a filter, view, and name for a report. Running the report results in real time retrieval of data.

Note: Oracle BI Publisher 11.1.1.5.0, or higher, reports are supported. You cannot open reports in BI Publisher 10*g* format. For information about how to remove any 10*g* reports, see Section 2.5.2.1.1, "Removing BI Publisher 10g Reports."

3.4.1 Adding a New Report

1. Click the **Dashboard** tab.

2. If necessary, expand **My Reports**.

3. Under My Reports, click the **Create** icon.

4. In the Create Report dialog, select the desired report type in the left panel.

5. Expand the folder in the tree to locate the desired report.

6. Click the report.

7. In the Create Report dialog, supply the required information in the fields.

Note: In the Create Report dialog, Report Details, Report Name, Template, and Format labels are translated as specified by your browser `locale` setting. Other report details are localized based on the BI Publisher user interface language preference.

---

8. Click **Create Report** to create the report.

9. When you are finished adding reports, click **Close**.

The report icon for each report you have created is now available under My Reports.

3.4.2 Editing a Report

1. Click the **Dashboard** tab.

2. Under My Reports, highlight the report you want to edit.

3. Click the **Edit** icon.

4. In the Edit dialog, make desired changes.

5. Click **Save** to save the changes or **Cancel** to cancel the changes.

The report icon is now available under My Reports.

3.4.3 Cloning a Report

1. Click the **Dashboard** tab.

2. Under My Reports, highlight the report you want to clone.

3. Click the **Create Like** icon.

4. In the Clone Report dialog, make the desired changes to the report name, template and output format.

5. Click **Save** to save the new report or **Cancel** to abandon adding the report.

The report icon is now available under My Reports.

3.4.4 Removing a Report

1. Click the **Dashboard** tab.

2. Under My Reports, highlight the report you want to delete.

3. Click the **Remove** icon.

4. In the Confirmation dialog, click **OK** to continue with the removal or **Cancel** to abandon the removal.

3.4.5 Running a Report

1. Click the **Dashboard** tab.

2. Under My Reports, navigate to the desired report

3. Click the icon for the report you want to generate.

4. The report runs, then appears in a separate browser tab or window.

> **Note:** If you encounter problems viewing PDF reports with Adobe Acrobat Reader in a browser, either upgrade to a newer version of Reader or configure Reader to run directly, not as an embedded function within the browser. See your Adobe Reader documentation for more information.

3.5 Viewing Your Profile

1. Click the **Dashboard** tab.

2. Under **My Profile Information**, click the **Profile** tab. Your profile is listed.

3.6 Viewing Your Common Admin Roles

1. Click the **Dashboard** tab.

2. Under **My Profile Information**, click the **Common Admin Roles** tab.

All common admin role types are listed. Administration role assignments are indicated by a checkmark in the column corresponding to product name.

3.7 Reading News and Announcements

1. Go to the News and Announcements portal on the Dashboard.

2. Click the desired topic, Oracle Security Alerts, Oracle New Downloads, or Identity Management Discussion Forum.

3.8 Personalizing Oracle Identity Navigator

Oracle Identity Navigator uses Oracle Composer to enable runtime customization of the Dashboard page. Changes are stored in Metadata Services and are available only to the user who made them.

You can personalize the Dashboard in either View or Edit mode.

View mode is the normal state when you are running Oracle Identity Navigator in a browser. In View mode, you can rearrange page components by dragging and dropping them or by using the **Actions** menus. You can change the page layout by clicking the **Change Layout** icon and selecting a layout option.

You enter Edit mode by clicking **Customize** in the global navigation links. In Edit mode, you can add page resources by clicking **Add Content** and selecting which resource to add. You can remove content from a page section by clicking the **Remove** icon. You can edit a page section by clicking the **Edit** icon. A Component Properties Dialog with multiple tabs enables you to customize the page section.

For more information about using Oracle Composer to customize pages, see the "Enabling Runtime Editing of Pages Using Oracle Composer" chapter in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

> **Note:** In the Component Properties dialog, the display name and values of attributes shown on the Display Options tab are in English, even if your Locale is set to a non-English value.

3.8.1 Rearranging the Page Layout

You can change the layout of the Dashboard.

1. Click the **Customize** icon on the upper right.

2. To add content to a column, click **Add Content** at the top of the column.

3. Select the type of portal you want to add and click **Add**.

4. To change the layout, click **Change Layout**.

5. Select the layout you want. Click the triangle in the upper right to change the layout.

6. When you have finished customizing the page, click **Close** on the upper right.

7. To move a portal to a different position on the page, click the View Actions Menu icon next to the portal.