User Guide

NetIQ Identity Manager Home and Provisioning Dashboard

July 2014

Legal Notice

Contents

About this Book and the Library

The *User Guide* provides information about installing, configuring, and using the NetIQ Identity Manager Home and NetIQ Identity Manager Provisioning Dashboard add-on user interfaces for the Identity Manager Roles Based Provisioning Module.

Intended Audience

This book provides information for individuals responsible for using the Identity Manager Roles Based Provisioning Module to make and approve process requests of various types. The primary audience for this book is an end user of the User Application interface who needs simple, easy-to-understand access to user-facing RBPM functions.

Other Information in the Library

The library provides the following information resources:

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

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.

User Application: Installation Guide

Describes how to install the Identity Manager Roles Based Provisioning Module 4.0.2.

User Application: Localization Toolkit Guide

Describes how to use the Identity Manager User Application Localization Toolkit to add languages not typically supported by the Identity Manager User Application.

RBPM and Reporting Migration Guide

Describes how to migrate to the Roles Based Provisioning Module 4.0.2 from an earlier version of the User Application or Roles Based Provisioning Module. This guide also describes how to migrate to the Identity Reporting Module 4.0.2.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager 4.0 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.

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.

Help

Provides context-sensitive information and step-by-step guidance for common tasks.

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
Web Site:	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
Web Site:	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 Web site in HTML and PDF formats on a page that does not require you to log on. 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 Overview

NetIQ Identity Manager Home and the NetIQ Identity Manager Provisioning Dashboard are end user-focused interfaces that allows you to access an easily-customized view of your Identity Manager User Application functionality. These add-on interfaces provides a targeted view of Identity Manager data and roles-based provisioning functions.

Identity Manager Home and the Provisioning Dashboard provide a single access point for all Identity Manager users and administrators and allows access to all existing Roles-Based Provisioning Module (RBPM) and User Application functionality. In addition, Identity Manager Home and the Provisioning Dashboard include new user-oriented features. Users can access the new user interfaces using any supported Web browser, from either a desktop computer or a tablet.

Identity Manager Home and the Provisioning Dashboard target end users, not administrators. Administrators need to access the existing User Application user interface to perform most administrative functions and tasks. Identity Manager Home links directly to some of these areas and can be configured to link to other User Application areas as necessary.

Identity Manager users who log into Identity Manager Home or the Provisioning Dashboard can then access the User Application without logging in again, and vice versa.

This document provides information about installing, configuring, and using Identity Manager Home. For information about configuring and using the existing User Application, see the *User Application: Administration Guide* and the *User Application: User Guide*.

For a general overview of the Identity Manager Home and Provisioning Dashboard user interfaces for Identity Manager, see the following sections:

1.1 Identity Manager Home

Identity Manager Home provides a single access point for all Identity Manager users and administrators and allows access to all existing Roles-Based Provisioning Module and User Application functionality, as well as new user-oriented features.

Administrators can customize Identity Manager Home to show only the items and links their users need to see, organized into categories that make sense, and add their own links or REST endpoints.

Administrators can configure items on Identity Manager Home to include badges. Badges can, for example, display how many items of a certain type a user has access to. For information about configuring Identity Manager Home items, see “Configuring Identity Manager Home Items” on page 29.

Identity Manager Home and the Identity Manager Provisioning Dashboard are separate user interfaces, with Identity Manager Home linking to different areas of the Dashboard. Identity Manager Home includes the following default set of links:

- **Make a Request**
- **My Tasks**
- **My History**
- **My Permissions**
- **My Profile**
- **Password**
- **Search**
- **Org Chart**
- **Roles**
- **Resources**
- **Create Users and Groups**
- **Provisioning and Security**
- **Reporting Module**
- **Compliance**

Additionally, as an administrator, you can configure what features you want your users to be able to access. Identity Manager Home can be easily localized in multiple languages.

1.2 Provisioning Dashboard

While Identity Manager Home provides a single point of entry to the Identity Manager Roles Based Provisioning Module functionality, the Identity Manager Provisioning Dashboard is a personalized view of each user's permissions, tasks, and requests. Identity Manager Home links to the appropriate location on each user's Dashboard.

The Provisioning Dashboard focuses on the following basic areas of functionality:

I want something. If a user needs an item, whether the item is a piece of equipment like a laptop or something intangible like access to a particular server or application, the user can use the *Make a Request* functionality to request that item. The user can search for an item by entering all or part of a search term in the *Permissions* field. For information about making requests, see "Requesting Permissions" on page 38.

I need to do something. If a user wants to know what tasks they need to manage, *My Tasks* shows all of a user's pending tasks in the Identity Manager system. For information about managing and addressing pending tasks, see "Managing Your Tasks" on page 38.

What do I have? If a user wants to see everything they can currently access, *My Permissions* shows a user all of the roles and resources to which they have access and organizes those items into a list. For information about viewing your current permissions, see "Viewing Your Permissions" on page 38.

How did I get it? If a user wants to see a list of past requests, *History* shows a user everything they have requested recently, as well as the status of all their pending requests. For information about viewing a user's request history, see "Viewing Your History" on page 40.

2 Installing Identity Manager Home

To install Identity Manager Home and the Provisioning Dashboard, you must install the NetIQ Identity Manager Home and Provisioning Dashboard Enhancement Pack, which includes an updated version of the Roles Based Provisioning Module and additional new functionality.

For information about installing Identity Manager Home, see the following sections:

2.1 Product Requirements

Ensure that your Identity Manager environment meets the following prerequisites before installing NetIQ Identity Manager Home.

2.1.1 Platform Requirements

Identity Manager Home requires one of the following operating systems:

- SUSE Linux Enterprise Server 11 SP2 or SP3 (64-bit)
- Red Hat Enterprise Linux 5 or 6 (64-bit)

2.1.2 NetIQ Software Requirements

Identity Manager Home requires Identity Manager 4.0.2 Advanced Edition with the following components:

- eDirectory 8.8.7 (32-bit or 64-bit) or eDirectory 8.8.8 (64-bit)

  NOTE: Identity Manager Home requires one of the versions of eDirectory supported for Identity Manager 4.0.2. For more detailed information about overall Identity Manager requirements, see "System Requirements" (https://www.netiq.com/documentation/idm402/idm_framework_install/data/be1mcjd.html#be1mcjd), in the *Identity Manager 4.0.2 Framework Installation Guide* (https://www.netiq.com/documentation/idm402/idm_framework_install/data/front.html)

- Identity Manager 4.0.2 Engine & Remote Loader Patch 3 or later
- Identity Manager Roles Based Provisioning Module 4.0.2 Field Patch D or later

  NOTE: After you install Roles Based Provisioning Module 4.0.2 Field Patch D, ensure you follow the included steps for upgrading to Java 2 version 1.7.

- Designer for Identity Manager 4.0.2 Auto Update 4A or later
- (Conditional) Event Auditing Service for Identity Manager
- (Conditional) Identity Manager 4.0.2 Data Collection Service (DCS) Driver version 4.0.0.3 or later, with minimum Package version 2.2.1.20130828112545
- (Conditional) Identity Manager 4.0.2 Managed System Gateway (MSGW) Driver version 4.0.0.5 or later

  NOTE: You only need to install the Event Auditing Service, Data Collection Service Driver, and Managed System Gateway Driver if you use the Identity Reporting Module in your environment.

- All other Identity Manager 4.0.2 drivers with latest patches

NOTE: Identity Manager 4.0.2 Standard Edition does not support Identity Manager Home or the Identity Manager Provisioning Dashboard.

2.1.3 Application Server Requirements

Identity Manager Home requires JBoss AS 5.1 or later.

NOTE: Identity Manager currently only supports installing Identity Manager Home on a server running JBoss.

2.1.4 Database Requirements

Identity Manager Home requires one of the following databases:

- Microsoft SQL Server 2008 or 2008 R2
- MySQL 5.1
- Oracle Database 11gR2
- PostgreSQL 8.4.3 or 9.0

2.1.5 Additional Software Requirements

- Java 2 Platform Standard Edition Development version 1.7 or later (JDK or JRE) from Sun (Oracle)
- (Optional) SSL

  NOTE: If you want to use Identity Manager Home with HTTPS, you must enable SSL on your application server.

2.1.6 Supported Browsers

Users can access Identity Manager Home and the Provisioning Dashboard using any of the following supported browsers:

- **Desktop Computers:**
  - Apple Safari 7.0.1
  - Google Chrome 31 or later
  - Microsoft Internet Explorer 9 or 10

    NOTE: If you use Internet Explorer 9 to access Identity Manager Home and the Provisioning Dashboard and set the Document Mode to Quirks Mode, the browser may not display the user interfaces correctly. For more information on this issue, see the *NetIQ Identity Manager Home and Provisioning Dashboard Release Notes* (https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html).
  - Mozilla Firefox 21 or later
- **iPads:**
  - Apple Safari
  - Google Chrome 31 or later

NOTE: All browsers must have cookies enabled to access Identity Manager Home and the Provisioning Dashboard. If cookies are disabled, the product does not work.

2.2 Preparing for Installation

Before you begin the installation process, ensure that you have installed all system requirements specified in "Product Requirements" on page 11.

After installing all system requirements, complete the following steps to prepare your environment:

1. Back up your User Application database. Refer to the documentation specific to your database for instructions.
2. Back up your eDirectory Identity Vault. For information about backing up eDirectory, see "Backing Up and Restoring eDirectory" in the *eDirectory Administration Guide*.
3. In Designer, back up and export your Designer project. For information about exporting Designer projects, see "Exporting a Project," in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
4. If using virtual machines to host Identity Manager components, create snapshots of all the virtual machines you use. Refer to the documentation specific to your virtualization software for instructions.

2.3 Enabling SSL

We recommend that you enable SSL when configuring Identity Manager Home. However, Identity Manager Home does not require SSL be enabled unless you want to use HTTPS. If you want to use Identity Manager Home with HTTPS, you must first enable SSL on your JBoss server.

For information about enabling SSL, see "Enabling SSL in a Production Environment," in the *User Application: Administration Guide*.

2.4 Installing Identity Manager Home Using the Updater Utility

When installing Identity Manager Home and the Provisioning Dashboard, we recommend you use the included Updater utility (`IdmHPD.bin`) to automatically install and configure the application in your Identity Manager environment.

The Updater utility includes the following files:

- `IdmHPD.bin`
- `hpd-conf-runtime-4.0.2A.zip`

WARNING: The installation process assumes that you used the default Roles Based Provisioning Module path and context for JBoss, as follows:

`/opt/novell/idm/jboss/server/IDMProv/`

If you specified a different path for the Roles Based Provisioning Module, use that path in the installation steps. If you specified a context other than `IDMProv`, see "Installing Identity Manager Home Using a Non-Default Context" on page 47 before continuing with the installation process.

---

1. Download the Identity Manager Home Updater files to your User Application server.
2. Stop the JBoss application server.
3. At a command prompt, navigate to the directory where you downloaded the Updater files and enter the following command:

```
./IdmHPD.bin
```

NOTE: You may need to modify the `IdmHPD.bin` file to allow you to execute the file as a program.

4. Click *Next*.
5. Review the license agreement, select *I accept the terms of the License Agreement*, and click *Next*.
6. Specify the location of the `hpd-conf-runtime-4.0.2A-Version.zip` file and click *Next*.
7. Specify whether the User Application, Identity Reporting Module, or both are installed in your environment and click *Next*.
8. Specify the location of the `install.properties` file on your User Application server and click *Next*.
9. (Conditional) If you do not have your User Application `install.properties` file, clear *Load Properties*, click *Next*, and specify the configuration information for your installation on the subsequent windows.
10. Confirm the default backup directory or specify a different backup directory to use, then click *Next*.
11. Click *Install*, then click *Done* when finished.
12. At a command prompt, navigate to the `IDMProv/tmp` directory and enter the following command:

    ```
    rm -rf *
    ```

13. Navigate to the `IDMProv/work/jboss.web` directory and enter the following command:

    ```
    rm -rf *
    ```

2.5 Updating and Configuring the Identity Vault

After you install the Identity Manager Home files, you must also update your existing Identity Vault.

1. Download the `hpd-conf-vault-4.0.2A.zip` file to your Identity Vault server.
2. Extract the contents of the ZIP file to a directory on the server.
3. (Conditional) If you have not previously installed the SAML schema and NMAS methods, complete the following steps:
   - **3a** In a terminal, navigate to the *`ExtractedDirectory`*`/saml` directory, where *`ExtractedDirectory`* is the location of the extracted `hpd-conf-vault-4.0.2A.zip` files.
   - **3b** Enter the following command:

     ```
     unzip nmassaml.zip
     ```

   - **3c** Navigate to the extracted `SAML` directory.
   - **3d** Enter the following command to install the SAML schema:

     ```
     ndssch -h eDirectoryHostIP eDirectoryAdmin authsaml.sch
     ```

     Where *`eDirectoryHostIP`* is the IP address of your eDirectory installation and *`eDirectoryAdmin`* is the administrative user account for eDirectory. For example:

     ```
     ndssch -h 164.99.99.99 admin.sa.system authsaml.sch
     ```

   - **3e** Enter your administrative user account password.
   - **3f** Enter the following command to install the NMAS methods:

```
nmasinst -addmethod eDirectoryAdmin TreeName ./config.txt
```

3g Enter your administrative user account password.

4 In a terminal, navigate to the *ExtractedDirectory*/schema directory.

5 Enter the following commands:

```
unzip osp-sch.zip
```

```
ndssch -h eDirectoryHostIP eDirectoryAdmin osp.sch
```

6 Enter your administrative user account password.

7 On the server command line, enter the following command to stop eDirectory:

```
/etc/init.d/ndsd stop
```

8 Move the following files from the eDirectory `classes` directory, which is `/opt/novell/eDirectory/lib/dirxml/classes` by default, to the `/tmp` directory:

- `nrfdriver.jar`
- `srvprvUAD.jar`

NOTE: The location of the `classes` directory may vary depending on your installation.

9 Copy the following files from the `classes` subdirectory of the extracted `hpd-conf-vault-4.0.2A.zip` directory to the eDirectory `classes` directory:

- `nrfdriver.jar`
- `srvprvUAD.jar`

10 At a command prompt, use the following command to restart eDirectory:

```
/etc/init.d/ndsd start
```

2.6 Configuring the Event Auditing Service

If you have Reporting configured in your Identity Manager environment, you must configure the Event Auditing Service (EAS) to function properly with Identity Manager Home and the Provisioning Dashboard.

1 Download the `hpd-conf-eas-4.0.2A.zip` file to the server where EAS is installed.

2 Extract the contents of the ZIP file to a directory on the server.

3 In a terminal, enter the following command to stop the EAS service:

```
/etc/init.d/sentinel_eas stop
```

4 In the terminal, navigate to the *ExtractedDirectory*/eas directory.

5 Enter the following command:

```
./update_selfextract.sh
```

6 Restart the EAS service.

2.7 Updating the User Application Driver Package

After you install the NetIQ Identity Manager Home files on your User Application server, you must use Designer for Identity Manager to update the existing User Application package in your environment.

For more information about managing packages in Designer, see "Managing Packages," in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

1. Download the `hpd-conf-designer-4.0.2A.zip` file to the server where Designer is installed.
2. Extract the contents of the ZIP file to a directory on the server.
3. Start Designer.
4. (Conditional) If you have not yet updated Designer 4.0.2 to AU4a, select *Help* > *Check for Designer Updates*, select *Yes* to update Designer, then select *OK*.
5. (Conditional) If your project does not already include a User Application driver, import the driver into your project.
6. In the Outline view, right-click *Package Catalog* and select *Import Package*.
7. Click *Browse*.
8. Navigate to the directory where you extracted the `hpd-conf-designer-4.0.2A.zip` file.
9. Open the `designer` directory and select `NOVLUABASE_3.0.0.20131213110230.jar`, then click *OK*.
10. In the Select Package window, select version 3.0.0.20131213110230 of the User Application Base package (`NOVLUABASE`) and click *OK*.
11. After Designer imports the package, click *OK*.
12. Right-click *Package Catalog* and select *Import Package*.
13. Clear *Show Base Packages Only*.
14. In the Select Package window, find and select version 2.0.0.20130322140144 of the *Provisioning Notification Templates* package.

    NOTE: If the window does not display version 2.0.0.20130322140144 of the *Provisioning Notification Templates* package, click *Cancel* and skip to Step 16.
15. Click *OK*, then click *OK* again.
16. In the Outline view, right-click the User Application driver and select *Properties*.
17. Click *Packages*.
18. Click *Select Operation* for the User Application Base package and select *Upgrade*.
19. Select version *3.0.0.20131213110230* and click *OK*.
20. (Conditional) If prompted to upgrade Provisioning Notification Templates, click *OK*.
21. Click *Apply*.
22. Verify the information in the Package Installation Wizard window and click *Next*.
23. Click *Finish*, then click *OK*.
24. In the Modeler, right-click the User Application driver and select *Driver* > *Deploy*.
25. Click *Deploy*.
26. If prompted to restart the User Application driver, click *Yes*.
27. Click *OK*.

2.8 Configuring the Data Collection Service Driver to Support OAuth

For Identity Manager Home and the Provisioning Dashboard to function properly with the Identity Reporting Module, you must configure the Data Collection Service (DCS) driver to support the OAuth protocol.

NOTE

- You only need to install and configure the Data Collection Service Driver if you use the Identity Reporting Module in your environment.
- If you have multiple Data Collection Service Drivers configured in your environment, you must complete the following steps for each driver.

---

1. (Conditional) If your project does not already include a Data Collection Service driver, import the driver into your project.
2. (Conditional) If you have not already upgraded your DCS driver to patch 4.0.0.3 or a later version of the patch, complete the following steps:
   - **2a** Download the latest DCS driver patch file.
   - **2b** Extract the patch file to a location on your server.
   - **2c** In a terminal, navigate to the location of the extracted patch RPM for your environment and run the following command:

     ```
     rpm -Uvh novell-DXMLdcs.rpm
     ```

   - **2d** Restart eDirectory.
   - **2e** In Designer, ensure that you have version 2.2.1.20130828112545 or later of the Data Collection Service Base package installed. If you do not have at least that version of the package installed, install the latest version of the package before continuing.
   - **2f** Redeploy and restart the DCS driver in Designer.
3. In the Outline view in Designer, right-click the DCS driver and select *Properties*.
4. Click *Driver Configuration*.
5. Click the *Driver Parameters* tab.
6. Click *Show connection parameters* and select *show*.
7. Click *SSO Service Support* and select *Yes*.
8. Specify the IP address and port for the Reporting Module.
9. Specify a password for the SSO Service Client. The default password is `driver`.
10. Click *Apply*, then click *OK*.
11. In the Modeler, right-click the DCS driver and select *Driver* > *Deploy*.
12. Click *Deploy*.
13. If prompted to restart the DCS driver, click *Yes*.
14. Click *OK*.

2.9 Creating a Keystore for One SSO Provider

Identity Manager Home and the Provisioning Dashboard use One SSO Provider (OSP) to enable single sign-on from multiple Identity Manager user interfaces. To enable single sign-on, you must create a Java KeyStore (JKS) file for OSP.

At a command prompt, enter the following command to create the `osp` keystore:

```
/JDKPath/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore
JBossInstallPath/server/IDMProv/conf/osp.jks -storepass KeystorePassword -keypass
KeyPassword -alias osp -dname 'cn=PublicServerName'
```

For example:

```
/opt/novell/idm/jdk1.7.0_21/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -
keystore /opt/novell/idm/jboss/server/IDMProv/conf/osp.jks -storepass n0v3ll -
keypass n0v3ll -alias osp -dname 'cn=test.yourcompany.com'
```

NOTE: For the *PublicServerName* value of the `-dname` keytool option, you must specify a "public" URL or IP address that users can use to access your environment. You cannot use an internal host name or IP address.

2.10 Configuring the PostgreSQL User Application Database

To install Identity Manager Home, you must modify the existing User Application database schema. To update the PostgreSQL database schema, we recommend you start your JBoss application server, which automatically updates the schema.

NOTE

- You can also update the PostgreSQL schema manually using a SQL script. However, you should only use the SQL script to update the schema if your organization requires users make all database updates using scripts or if the User Application tables were originally created or updated using the SQL script option during the Identity Manager Roles Based Provisioning Module 4.0.2 installation process. For information about updating the PostgreSQL schema using a SQL script, see "Using a SQL Script to Update the PostgreSQL Schema" on page 49.
- If you use a database other than PostgreSQL, see "Configuring Non-PostgreSQL User Application Databases" on page 20.

To update the PostgreSQL database schema by starting your JBoss application server, complete the following steps:

1. Navigate to the User Application deploy directory within the JBoss installation. For example: `/opt/novell/idm/jboss/server/IDMProv/deploy`
2. In the `deploy` directory, use a text editor to open the `IDMProv-ds.xml` file.
3. In the `<connection-url>` element, append `?compatible=true` to the existing text. For example:

   ```
   <connection-url>jdbc:postgresql://localhost:5432/
   idmuserappdb?compatible=true</connection-url>
   ```

4. Save and close the `IDMProv-ds.xml` file.
5. In a command prompt, enter the following command:

   ```
   /etc/init.d/jboss_init start
   ```

6. Use the JBoss log to verify that the server started completely and address any issues or errors.

NOTE: JBoss may log an error regarding the OSP keystore. This error occurs because you have not yet configured SSO in your Identity Manager Home environment. You can ignore the error.

2.11 Configuring Non-PostgreSQL User Application Databases

To modify the existing User Application database schema for non-PostgreSQL databases, complete the following steps:

1. In a command prompt, navigate to the Identity Manager deploy directory and enter the following command:

   ```
   unzip IDMProv.war WEB-INF/classes/hibernate.cfg.xml
   ```

2. Use a text editor to open the `WEB-INF/classes/hibernate.cfg.xml` file.
3. In the `hibernate.cfg.xml` file, find the `dialect` property.
4. Update the value of the dialect property for your database, as follows:
   - **Microsoft SQL Server 2008** `com.netiq.persist.SQLServerDialect`
   - **MySQL 5.1** `com.netiq.persist.MySQL5InnoDBDialect`
   - **Oracle 11g** `com.netiq.persist.Oracle10gDialect`
5. Save and close the file.
6. In the command prompt, enter the following command:

   ```
   zip -u0 IDMProv.war WEB-INF/classes/hibernate.cfg.xml
   ```

7. Delete the `WEB-INF` directory and all its contents.

2.12 Configuring Single Sign-On

Identity Manager uses single sign-on to provide authentication between the User Application, Identity Manager Home, and the Identity Manager Provisioning Dashboard.

NOTE

- You must configure single sign-on to use Identity Manager Home and the Provisioning Dashboard.
- After you configure and enable single sign-on in your environment, users can no longer access the User Application as a guest or anonymous user. Users are instead prompted to log into the user interface.

1. Start your JBoss server.
2. Create the certificates and keys necessary for single sign-on. For information about creating certificates and keys for single sign-on, see "Creating the Certificates," in the *User Application: Administration Guide*.

   NOTE: This procedure assumes your environment will utilize one certificate for eDirectory, the SSO controller, and the OAuth Provider. If your company requires additional layers of separation, create a separate certificate for the OAuth Provider.

3. Configure your eDirectory installation for single sign-on. For information about configuring eDirectory for single sign-on, see "Configuring eDirectory," in the *User Application: Administration Guide*.

NOTE: If you previously extended the eDirectory schema to include the SAML schema and installed the required NMAS methods, as described in "Updating and Configuring the Identity Vault" on page 15, you do not need to perform those steps a second time. Instead, skip to the subsection about creating the Trusted Root Container.

4 Use a Web browser to access your User Application server, logging in as the User Application administrator.

5 Configure the SSO controller. For information about configuring the SSO controller, see "Configuring the SSO Controller," in the *User Application: Administration Guide*.

IMPORTANT: Do not restart the application server as instructed in the *User Application: Administration Guide*.

6 To verify you have configured the SSL Controller correctly, look for the following entry in the `server.log` file:

```
INFO [AuthTokenGenerator] [RBPM] SSO Framework is enabled
```

7 On the User Application Single Sign On (SSO) page, verify that the SSO Providers list includes the OAuth provider.

8 Confirm *Enable Single Sign On (SSO) To User Application* is selected, then select *OAuth*.

9 In the *Expiration Interval* field, specify the number of seconds Identity Manager keeps the OAuth SSO header alive. For example, you could specify 300 seconds as the expiration interval.

10 Select *Distinguished Name*.

11 (Conditional) If not already configured, specify the signing certificate and signing key and provide the signing key password.

NOTE: The signing key should be a PKCS8 format key.

12 Select *Save*.

13 Select the checkbox for the OAuth provider and select *Enable*, then click *Enable* to confirm.

14 Verify that the SSO Providers list displays a green check in the Status column for the OAuth provider.

15 Close your browser without logging out of the User Application.

16 Stop your JBoss server.

2.13 Configuring the Roles Based Provisioning Module and Application Server

Before using Identity Manager Home and the Provisioning Dashboard, you must run the Roles Based Provisioning Module Configuration utility (`configupdate.sh`) and configure the Roles Based Provisioning Module and JBoss application server.

The Roles Based Provisioning Module Configuration utility allows you to configure the following "realms" within Identity Manager:

- User Application
- Authentication
- Reporting
- SSO Clients

NOTE

- You should not need to modify any settings in the User Application or Reporting tabs of the utility.
- The utility only displays the Reporting tab if you have the Reporting Module installed in your environment.

To run the utility, complete the following steps:

1. Using a text editor, open the `configupdate.sh` file, located in the User Application installation directory. For example: `/opt/novell/idm/configupdate.sh`
2. In `configupdate.sh`, ensure the following options are configured correctly:

   ```
   -edit_admin true
   ```

   ```
   -use_console false
   ```

   NOTE: You should only configure the value of `-use_console` to be `true` if you want to run the utility in console mode.
3. Save and close `configupdate.sh`.
4. Start the User Application Configuration utility by running `./configupdate.sh` from the command prompt.

   NOTE: You may need to wait a few minutes for the utility to finish starting up.
5. Click the *Authentication* tab.
6. (Conditional) Change all instances of `localhost` to specify the actual server DNS name or IP address. You should only use `localhost` if all access to Identity Manager Home and the Provisioning Dashboard will be local, including access through a browser. The address must be resolvable from all clients.

   NOTE: This "public" host name or IP address should be the same as the value of the `-dname` option specified in "Creating a Keystore for One SSO Provider" on page 19.
7. For the *LDAP DN of Admins Container* setting, click the *Browse* button and select the container within the Identity Vault that contains your User Application administrator.
8. Specify the OAuth keystore file you created in "Creating a Keystore for One SSO Provider" on page 19, including the keystore file path, keystore file password, key alias, and key password. The default keystore file is `osp.jks`, and the default key alias is `osp`.
9. Click the *SSO Clients* tab.
10. (Conditional) Change all instances of `localhost` to specify the actual server DNS name or IP address. You should only use `localhost` if all access to Identity Manager Home and the Provisioning Dashboard will be local, including access through a browser. The address must be resolvable from all clients.

    NOTE: This "public" host name or IP address should be the same as the value of the `-dname` option specified in "Creating a Keystore for One SSO Provider" on page 19.
11. (Conditional) If you configured specific ports in your environment for use with the User Application, Identity Manager Home, the Provisioning Dashboard, the Reporting Module, or the Catalog Administrator, modify the port numbers as necessary.
12. Click *OK* to save your changes.

2.14 Updating the Event Auditing Service WAR File

If you have the Identity Reporting Module installed, you must manually update the `easwebstart.war` file used by the Event Auditing Service (EAS).

NOTE: You only need to update the EAS WAR file if you use the Identity Reporting Module in your environment.

---

1. In a command prompt, navigate to the User Application deploy directory within the JBoss installation. For example: `/opt/novell/idm/jboss/server/IDMProv/deploy`
2. Enter the following command:

   ```
   unzip easwebstart.war WEB-INF/web.xml
   ```

3. Use a text editor to open the `web.xml` file and set the value of the `EAS_SERVER_IP` parameter to either `localhost` or the IP address of the server where you installed EAS.
4. Save and close the `web.xml` file.
5. In the command prompt, enter the following commands:

   ```
   zip -u0 easwebstart.war WEB-INF/web.xml
   ```

   ```
   rm -rf WEB-INF/
   ```

2.15 Reconfiguring Forgotten Password Self-Service

When you run the Updater utility (`IdmHPD.bin`), the utility replaces your existing forgotten-password management WAR file, `IDMPwdMgt.war`, with a new version of the file that works with the User Application, Identity Manager Home, and the Provisioning Dashboard.

If you deployed and configured `IDMPwdMgt.war` in your environment before installing Identity Manager Home, you must update the new version of the file for your environment. For information about configuring the forgotten-password management WAR, see "Configuring Forgotten Password Self-Service ", in the *User Application: Administration Guide*.

NOTE

- You only need to update and reconfigure `IDMPwdMgrt.war` if you had previously deployed the file in your environment.
- If you deployed the `IDMPwdMgt.war` file on a separate server, copy the new file to that server and update as described in the *Administration Guide*.

2.16 Configuring Auditing and Logging

When you run the Updater utility (`IdmHPD.bin`), the utility replaces your existing logging configuration files for the User Application and Reporting Module (if installed). The utility sets all logging settings back to the default configuration when the User Application or Reporting Module were first installed. In addition, the utility disables Auditing by default.

If you previously configured and enabled Auditing and logging in your environment, you must reconfigure Auditing and logging before starting the application server.

NOTE: You only need to reconfigure and enable Auditing if you had previously enabled Auditing in your environment.

Do not enable Auditing unless you have configured your environment as outlined in "Setting Up Logging," in the *User Application: Administration Guide*.

1. (Conditional) If you have the Reporting Module installed and Auditing enabled, complete the following steps:
   - **1a** Navigate to the location of the logging configuration files within the JBoss installation. For example: `/opt/novell/idm/jboss/server/IDMProv/conf/`
   - **1b** Using a text editor, open the first `idmrpt`*`NAME`*`_logging.xml` file.
   - **1c** Under `<appender-ref ref="NAUDIT"/>`, uncomment the following entries:

     ```
     <logger additivity="true" name="com.novell" level="INFO">
     <logger additivity="true" name="com.netiq" level="INFO">
     ```

   - **1d** Save and close the file.
   - **1e** Repeat the substeps above for each `idmrpt`*`NAME`*`_logging.xml` file.
2. In a command prompt, enter the following command:

   ```
   /etc/init.d/jboss_init start
   ```

3. Use the JBoss log to verify that the server started completely and address any issues or errors.
4. To verify you have configured the SSL Controller correctly, look for the following entry in the `server.log` file:

   ```
   INFO [com.novell.common.auth.saml.AuthTokenGenerator] (main) [RBPM] SSO
   Framework is enabled
   ```

5. Use a Web browser to access your User Application server, logging in as the User Application administrator.
6. Click the *Administration* tab, then click the *Application Configuration* tab.
7. Click *Logging*.
8. Select *Enable audit service*, then click *Submit*.
9. Log out of the User Application.

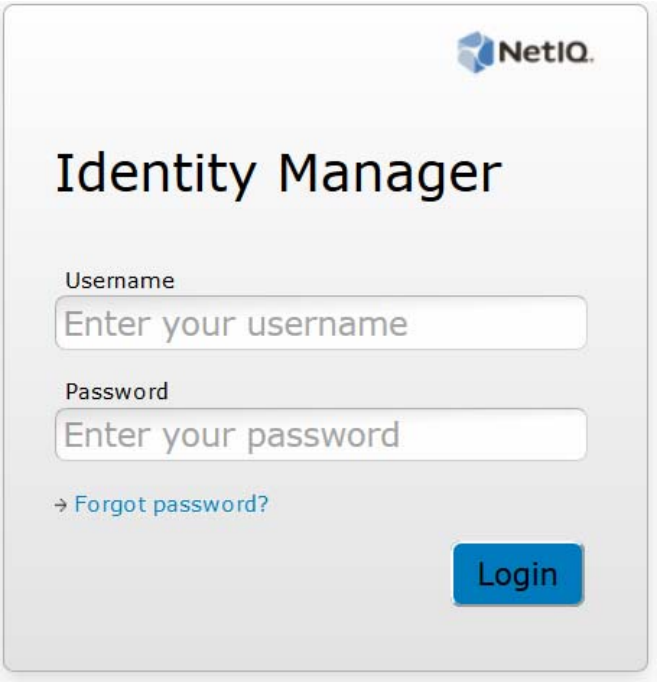
2.17 Verifying Identity Manager Home Installation

After you finish installing and configuring Identity Manager Home, verify that you can log into both Identity Manager Home and the User Application.

1. In a new browser window, navigate to Identity Manager Home on your User Application server:

   `http://`*`server`*`:8180/landing`

   Ensure that the login screen displayed looks like the image below, but do not log into Identity Manager Home.



2 In your browser, navigate to the User Application:

`http://server:8180/IDM-context`

3 Verify that the User Application displays the same login screen as the login screen in Step 1.

4 Log in to the User Application.

5 In the top right corner, click the *Home* icon and verify that you can access Identity Manager Home and the Provisioning Dashboard without logging in again.

NOTE: If you must log in separately for the User Application and Identity Manager Home, verify that your single sign-on settings are correctly configured. For more information about configuring single sign-on settings, see "Configuring Single Sign-On" on page 20.

---

3 Accessing Identity Manager Home

To access Identity Manager Home and the Provisioning Dashboard:

1. Open a Web browser and navigate to one of the following URLs, depending on whether SSL is configured in your environment:

   `http://IDMServer:8180/landing`

   `https://IDMServer:8180/landing`

   Where *IDMServer* is the fully-qualified name or IP address of your Identity Manager Roles Based Provisioning Module server. If you do not know the address you need to use, contact your Identity Manager administrator.

   For a list of browsers you can use to access Identity Manager Home and the Provisioning Dashboard, see "Supported Browsers" on page 13.

2. Provide your Identity Manager user name and password.

   NOTE

   - If you have previously accessed the Identity Manager User Application, you may be able to use the same user name and password to access Identity Manager Home.
   - You cannot access Identity Manager Home using an account that includes any of the following characters in the name:

     `\ /, * ? . $ # +`

3. Select *Login*.

4 Configuring Identity Manager Home

After you install Identity Manager Home components in your User Application environment, you must configure Identity Manager Home to allow your users to perform their necessary tasks.

For information about configuring and administering your environment using Identity Manager Home, see the following sections:

4.1 Configuring Identity Manager Home Items

As an administrator, you can customize the default Identity Manager Home items your users can access. You can add or remove Home items as needed or add your own new custom items.

NOTE

- If you want to add the available iManager item to Identity Manager Home, you must configure the link to point to your iManager installation. If you add the item to Identity Manager Home without configuring the link, the link returns an error.
- Users can only see the items to which they have access. If you want to restrict users' access to specific Home items, use the User Application Administration module.

To customize the default Identity Manager Home items displayed:

1. Log in to Identity Manager Home using a Role, Resource, Provisioning, and Security domain administrator account.
2. On Identity Manager Home, select *Edit*, located in the top right-hand corner of the page.
3. (Optional) If you want to add the provided iManager item to Identity Manager Home, complete the following steps:
   - **3a** In the *New and available items* column, mouse over *iManager* and select the *Edit* icon.
   - **3b** In the *Link* field, specify the URL for your iManager installation.
   - **3c** Select *Save*.
   - **3d** Select and drag *iManager* from the *New and available items* list to one of the categories displayed on the right side of the page.

4 (Optional) If you want to add a new category to Identity Manager Home, complete the following steps:

4a Select *New Category*. The user interface adds a new untitled category at the bottom of your current set of categories.

4b Select the title `Untitled Category` and specify the name you want to use for the category.

4c Select on the page outside of the category title to save the new name.

5 (Optional) If you want to delete a category, select the *Delete this category* icon  under *Categories*.

NOTE: If you delete a category, Identity Manager Home automatically moves any items in that category back to the *New and available items* list.

---

6 (Optional) If you want to add or remove an Identity Manager Home item, select and drag the item to and from the *New and available items* list and one of the categories displayed on the right side of the page. You can also drag and drop items from one category to another category.

7 (Optional) If you want to add a new Identity Manager Home item to the *New and available items* list, complete the following steps:

7a Select *New item*.

7b Specify a name and description for the new item.

7c To specify an image to use for the item, select *Browse*, navigate to the image, and select *Open*.

7d (Optional) If you want the new item to link to a specific URL, either within the User Application or outside of Identity Manager, specify the URL in the *Link* field.

7e (Optional) If you want to add additional functionality to the Identity Manager Home item, like a badge that displays the number of pending tasks, you can specify a REST endpoint with JSON data in the *API URL* field. For more information about REST endpoints, see "REST Services," in the *User Application: Administration Guide*.

NOTE

- When you specify a REST endpoint for an Identity Manager Home item, you must configure the endpoint itself on your Identity Manager Home server.
- If you specify a REST endpoint, you can include REST parameters in the item *Description* field. For example, the description for the default Tasks item includes the following text:

```
View my {0} Identity Manager approval tasks
```

7f Select *Save*.

8 When finished configuring Identity Manager Home items, select *I'm done*.

4.2 Configuring Featured Items

When configuring your Identity Manager Home environment, you can create and configure any Featured Items you want all users to be able to access in their personal Provisioning Dashboards.

NOTE: If you do not add any items to a Featured Items category, the Dashboard does not display the category.

1. Log in to Identity Manager Home using a Role, Resource and Provisioning domain administrator account.
2. Select *Make a Request*.
3. Select *Edit Featured Items*.
4. Select *Add an item*.
5. In the *Add an uncategorized item* field, specify the role, resource, or process request you want to include as a Featured Item. The Dashboard automatically displays any existing roles, resources, or PRDs matching the specified text.
6. Select the item you want to include.
7. (Optional) If you want to specify a particular image to use for the Featured Item, select *Browse*, select the image, and select *Open*.

   NOTE: You can specify an image with a maximum file size of 512 KB, in JPG, GIF, PNG, or SVG format.
8. Select *Save*.
9. (Optional) If you want to create a specific Featured Item category, select *New category*, then specify a name for the category and press *Enter*.
10. Select the new item in the *New and available items* list and drag the item to the category where you want to display the item. You can also drag and drop items from one category to another category.
11. Repeat Step 4 through Step 10 for each Featured Item you want to add.
12. (Optional) If you want to modify an existing item, mouse over the item and select the *Edit* icon. You can then modify the image for the item or select *Delete* to delete the item completely.
13. (Optional) If you want to delete a category, select the *Delete this category* icon  under *Categories*.

    NOTE: If you delete a category, Identity Manager Home automatically moves any items in that category back to the *New and available items* list.
14. When finished configuring your Featured Items, select *I'm done*. The Dashboard lists your new items under *Featured Items*.
15. Select the *Home* icon  .

4.3 Localizing Identity Manager Home and the Provisioning Dashboard

You can localize or customize the text displayed on Identity Manager Home and Provisioning Dashboard by modifying a set of language-specific properties files provided by Identity Manager. Localization properties files use the `.properties` extension.

Identity Manager Home includes the following properties files by default:

Language	Locale Designation
Chinese (China)	zh_CN
Chinese (Taiwan)	zh_TW
Danish	da
Dutch	nl
English	en
French	fr
German	de
Italian	it
Japanese	ja
Portuguese	pt
Russian	ru
Spanish	es
Swedish	sv

To customize Identity Manager Home strings for your environment, complete the following steps:

1. Log in to Identity Manager Home using an domain administrator account that is assigned the Role Administrator, Resource Administrator, Provisioning Administrator, and Security Administrator roles.
2. On Identity Manager Home, select *Edit*.
3. Select *Localize*.
4. Select the locale for which you want to localize and save the properties file to your local computer.
5. Open the properties file in a text editor and specify text for each property listed. For example, if you download the `sv.properties` file to localize Identity Manager Home and the Provisioning Dashboard in Swedish, modify the properties file as follows:

   ```
   # English value: My Category
   category-featured-47-name = Min kategori
   ```

   NOTE: If you want to use double-byte or extended characters in the properties file, ensure that you save the file using the correct encoding.

6. Save and close the properties file.
7. On Identity Manager Home, select the *File Upload* icon  for the locale.
8. Navigate to the properties file on your local computer and select *Open*.
9. Repeat Step 4 through Step 8 for each locale you want to enable.
10. Select *Back to edit*, then select *I'm done*.

4.4 Configuring Forgot Password Functionality

If you want to set up the Identity Manager Home login page to display the *Forgot password?* link, you must configure the Login Settings in the Administration tab of the User Application and then restart the JBoss application server.

To enable the *Forgot password?* link for Identity Manager Home:

1. Log in to Identity Manager Home using an administrator account.
2. In your browser, navigate to the User Application:

   `http://server:8180/IDM-context`
3. Click the Administration tab.
4. Under `Password Module Setup`, click *Login*.
5. Select *true* for the *Enable Forgot Password Link* setting.
6. Click *Save*.
7. Click *Logout*.
8. In a command prompt, enter the following command:

   ```
   /etc/init.d/jboss_init restart
   ```
9. After JBoss finishes restarting, go to the Identity Manager Home login page and verify the page displays the *Forgot password?* link.

4.5 Configuring Localized User Names

Identity Manager Home, the Provisioning Dashboard, and the User Application allow you to configure the format of displayed user names in your environment based on the user's current locale.

You can then use localized user names in Approval forms in the User Application, using the literal `%LocaleFormattedFullName%` for forms with the `User` entity definition key. For more information about creating or configuring User Application forms in Designer, see "Creating Forms for a Provisioning Request Definition," in the *User Application: Design Guide*.

To configure localized name formatting, use Designer to edit the `Full Name` entity in the Directory Abstraction Layer (DAL):

1. Start Designer.
2. Open your current project and click the project name in the Outline view.
3. In the Provisioning view, right-click *Full Name* and select *Edit*.
4. In the Directory Abstraction Layer editor, expand *Entities* > *Full Name*.
5. Select the locale name pattern you want to modify.
6. Modify the *Calculated Attribute* expression to specify the format you want to use for the locale. For example, if you want to display the user's surname first and given name second, modify the expression as follows:

   ```
   attr.getValue("Surname") + " " + attr.getValue("Given Name")
   ```

   You can either modify the expression manually in the Expression field or click the *Build ECMAScript Expression* icon and use the ECMA Expression Builder to modify the expression. For more information about modifying ECMAScript expressions, see "Working with ECMA Expressions," in the *User Application: Design Guide*.

7 Save your changes to the locale name pattern.

8 Repeat Step 5 through Step 7 for each name pattern you want to configure.

9 When finished, close the Directory Abstraction Layer editor.

10 In the Modeler, right-click the User Application driver and select *Driver* > *Deploy*.

11 Click *Deploy*, then click *Yes* to restart the driver.

12 Click *OK*.

4.6 Configuring Email Notification Templates

By default, email notification templates in Identity Manager direct recipients to the User Application user interface. If you want email notification templates to direct recipients to Identity Manager Home and the Provisioning Dashboard, you must modify the default templates in Designer.

NOTE

- Only some default notification templates include links to the User Application.
- Modifying an existing notification template marks that template as customized in Designer.
- For more information about modifying notification templates, see "Editing a Notification Template," in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

To configure email notification templates for Identity Manager Home, complete the following steps:

1 Start Designer.

2 Make sure you have imported email notification templates into your Designer project.

3 In the Outline view, right-click the notification template you want to modify and select *Copy*.

NOTE: We recommend you create and modify a copy of the original notification template you want to configure, rather than modifying the original. You can then specify the "Identity Manager Home" version of the template in any workflows where you want users to use Home and the Provisioning Dashboard, and not modify the workflows where you want users to use the User Application.

4 Specify a name for the copied template and click *OK*.

5 Right-click the copied template and select *Edit*, then click *Yes* to confirm.

6 (Optional) If you want to remove all links to the User Application, modify the message text as follows:

6a Find and remove any instances of `$PROTOCOL$://$HOST$:$PORT$/$TASK_DETAILS$`. In the Provisioning Dashboard, users can no longer directly access the details of a task.

6b Change any instances of the following:

```
$PROTOCOL$://$HOST$:$PORT$/$TASKLIST_CONTEXT$
```

to:

```
$PROTOCOL$://$HOST$:$PORT$/dash/#myTasks
```

7 (Optional) If you want to retain the existing User Application links, add text similar to the following line to the notification template message:

```
You can review your tasks list using the new Provisioning Dashboard at
$PROTOCOL$://$HOST$:$PORT$/dash/#myTasks.
```

8. When finished, save and close the notification template.
9. Repeat Step 3 through Step 8 for each notification template you want to modify, including any localized templates.
10. Deploy the new templates to the Identity Vault.
11. Modify any workflows where the approver should use Identity Manager Home and the Provisioning Dashboard so the workflow uses the new notification templates.

5 Making and Managing Requests

Most users access Identity Manager Home because they need to request an item or approve someone else's request. In Identity Manager Home and the Provisioning Dashboard, items users can request are generically called **permissions**.

Using Identity Manager Home and the Provisioning Dashboard, a user can request hardware, access to a particular server, or permission to use a particular application in their environment. The user's manager then logs into Identity Manager Home, sees a pending task displayed in the My Tasks badge, and looks at that request in their My Tasks list and either approves or denies the request.

Users can also view their existing permissions in the My Permissions list on the Provisioning Dashboard, and see the status of their past requests in the History list on the Dashboard.

Identity Manager Home and the Provisioning Dashboard streamline the provisioning process for both end users and managers, allowing users and managers to make and approve requests quickly and easily.

NOTE: If you have previously used the User Application and Roles Based Provisioning Module, permissions are either **roles** or **resources**.

You cannot configure roles, resources, PRDs, or categories using Identity Manager Home. For more information about configuring roles in Identity Manager, see "Configuring Roles," in the *User Application: Design Guide*.

For more information about configuring resources in Identity Manager, see "Configuring Resources," in the *User Application: Design Guide*.

For more information about configuring PRDs in Identity Manager, see "Configuring Provisioning Request Definitions," in the *User Application: Design Guide*.

For information about making, approving, and viewing requests in Identity Manager Home and the Provisioning Dashboard, see the following sections:

5.1 Viewing Your Permissions

To view the roles and resources to which you have access, select *My Permissions* on Identity Manager Home. On the Provisioning Dashboard, you can then select a specific permission in the My Permissions list for further details on that role or resource. The Dashboard displays any reasons provided for the permission assignment.

If you want to find a particular permission in a large list, enter all or part of the name of the permission in the *Search my permissions* field. The My Permissions list displays only those permissions matching the specified text.

5.2 Requesting Permissions

As with the existing User Application interface, you can use the new interface to request new permissions.

NOTE: A user can only request permissions for themselves. If an administrator needs to request permissions for another user, that administrator must use the User Application.

To make a process request:

1. Log in to Identity Manager Home.
2. Select *Make a Request*.
3. On the Provisioning Dashboard, use the *Permissions* field to search for the specific permission you want to request. You can sort the resulting permissions by the closest matching result or in alphabetical order.

   NOTE: You should not use punctuation when specifying a permission you want to request. If the name of the permission you want to request includes punctuation, omit the punctuation when searching.

   ---
4. Provide any required information, including the effective date, expiration date, or the reason for the request.

   Different permissions require different information, depending on how the administrator has configured the form. If the permission requires detailed information, the Dashboard redirects you to a separate form window when you select the permission.
5. Select *Request* or *Submit*, depending on the type of permission requested.

You can request multiple permissions at the same time.

NOTE: Items that require additional detailed information may not be available for selection with other items. To request multiple permissions at once, the request forms for the various requests cannot require detailed information.

5.3 Managing Your Tasks

If you are responsible for approving or denying requested permissions in Identity Manager, you can use the Provisioning Dashboard to manage your tasks as you would in the User Application.

You can approve or deny requests one at a time, or you can approve or deny multiple simple requests that do not require detailed information in bulk.

To manage your tasks in the Provisioning Dashboard:

1. Log in to Identity Manager Home.
2. Select *My Tasks*.
3. (Optional) If you want to approve or deny a specific request, complete the following steps:
   - **3a** In the My Tasks list, select the request.
   - **3b** Select *Complete Task*.
   - **3c** On the form, provide any required information and select *Approve*, *Reject*, or *Deny*, as appropriate.
4. (Optional) If you want to approve or deny multiple requests at the same time, complete the following steps:
   - **4a** In the My Tasks list, select the requests you want to approve or deny.

     NOTE

     - For a more complex request that requires detailed information, the Provisioning Dashboard does not display a checkbox. You must approve or deny those requests by selecting each request and following Step 3a through Step 3c above.
     - When you select a more complex request to approve or deny, the Dashboard may need to open the request form in a separate browser tab.

   - **4b** Provide a comment explaining why you want to approve or deny the selected tasks.
   - **4c** Select *Approve X items* or *Deny X items*, as appropriate.

5.4 Removing Permissions

If you no longer want access to a role or resource, you can remove the permission using the Provisioning Dashboard.

NOTE

- If you add, remove, or modify a permission using the Provisioning Dashboard, the My Permissions list may not immediately reflect the change. Press *F5* to refresh the My Permissions list.
- You cannot remove permissions granted because of membership in a particular group in your Identity Manager environment. If you want to remove access to a role or resource assigned because of membership in a group, use the User Application to remove your account from that group.

1. Log in to Identity Manager Home.
2. Select *My Permissions*.
3. Select the name of the permission you want to remove.
4. Select the displayed value under *Values*.
5. Select *Remove*.
6. Specify why you want to remove the assigned permission and select *Remove*.
7. (Optional) If you want to remove multiple permissions at one time, select the permissions you want to remove on the Provisioning Dashboard.
8. Specify why you want to remove the assigned permissions and select *Remove X permissions*, where *X* is the number of permissions selected.

5.5 Viewing Your History

To view the history of your previous requests, tasks, and assignments, select *My History* on Identity Manager Home.

You can also cancel a pending request from the History list, by selecting the request in the list and selecting *Cancel this request* on the subsequent window.

NOTE: After you make a request, you cannot select a request in the History list until Identity Manager finishes processing. If you access the Dashboard using a slow connection, you may need to wait for the Dashboard to allow you to click the request name in the list.

The History list on the Provisioning Dashboard uses the following icons to indicate the status of a request:

Icon	Status	Description
	Pending	The submitted request needs to be approved or denied.
	Approved	The request reviewer approved the request.
	Completed	The request has been completed and fulfilled, if necessary.
	Denied	The request reviewer denied the request.
	Canceled	The requester canceled the pending request.
	Error	Identity Manager encountered an error processing the request.

6 Using Identity Manager Home Links

In addition to making and managing requests in Identity Manager Home and the Provisioning Dashboard, you can use Identity Manager Home to access other User Application functionality. Identity Manager Home provides default links to several areas of the User Application, streamlining the basic tasks end users and administrators need to perform in Identity Manager.

NOTE: To return to Identity Manager Home from anywhere within the User Application, click the Home icon in the top right corner.

Identity Manager Home can also include links to other areas of the User Application or to other Identity Manager components, like the Identity Reporting Module or iManager.

For information about accessing Identity Manager functionality through Identity Manager Home, see the following sections:

6.1 Searching for Users, Groups, or Teams

To search for users, groups, or teams in your Identity Manager environment, you can go to Identity Manager Home and select *Search*. The Identity Manager Home link redirects you to the Directory Search area of the Identity Self-Service tab in the User Application.

For more information about searching for users in Identity Manager, see "Using Directory Search," in the *User Application: User Guide*.

6.2 Updating Your Profile

To view or modify your Identity Manager profile information, you can go to Identity Manager Home and select *My Profile*. The Identity Manager Home link redirects you to the My Profile area of the Identity Self-Service tab in the User Application.

For more information about updating your profile in Identity Manager, see "Using My Profile," in the *User Application: User Guide*.

6.3 Changing Your Password

To change your Identity Manager password, go to Identity Manager Home and select *Password*. The Identity Manager Home link redirects you to the Change Password area of the Identity Self-Service tab in the User Application.

For more information about changing your Identity Manager password, see "Change Password," in the *User Application: User Guide*.

6.4 Viewing Your Organization Chart

To view your organization chart in Identity Manager, go to Identity Manager Home and select *Org Chart*. The Identity Manager Home link redirects you to the Organization Chart area of the Identity Self-Service tab in the User Application.

For more information about using the Identity Manager organization chart, see "Using the Organization Chart," in the *User Application: User Guide*.

6.5 Managing Roles and Resources

If you are an administrator and you want to create or modify roles or resources in your Identity Manager environment, go to Identity Manager Home and select *Roles* or *Resources*, as applicable. The Identity Manager Home links redirect you to either the Roles Catalog or Resources Catalog in the User Application.

For more information about managing roles in Identity Manager, see "Managing Roles in the User Application" in the *User Application: User Guide*. For more information about managing resources in Identity Manager, see "Managing Resources in the User Application" in the *User Application: User Guide*.

6.6 Managing Users and Groups

If you are an administrator and you want to create or modify users or groups in your Identity Manager environment, go to Identity Manager Home and select *Create Users and Groups*. The Identity Manager Home link redirects you to the Identity Self-Service tab in the User Application.

For more information about creating users and groups in Identity Manager, see "Creating Users or Groups," in the *User Application: User Guide*.

6.7 Configuring User Application Access

If you are an administrator and you want to configure access to Identity Manager User Application components, go to Identity Manager Home and select *Provisioning and Security*. The Identity Manager Home link redirects you to the Navigation Access Permissions area of the RBPM Provisioning and Security Configuration tab in the User Application.

For more information about configuring access to the User Application, see "Navigation Access Permissions," in the *User Application: Administration Guide*.

6.8 Managing Compliance-Based Actions

If you are an administrator and you want to view or create attestation processes in Identity Manager for compliance purposes, go to Identity Manager Home and select *Compliance*. The Identity Manager Home link redirects you to the View Attestation Process Requests area of the Compliance tab in the User Application.

For more information about managing attestation processes in the User Application, see "Making Attestation Requests," in the *User Application: User Guide*.

7 Troubleshooting Identity Manager Home

The following sections include information for troubleshooting Identity Manager Home and the Provisioning Dashboard.

7.1 Incorrect Keystore Configuration Causes Browser to Display Flashing Web Page

If you configure the application server you use to run Identity Manager Home, the Identity Manager Provisioning Dashboard, and the Identity Manager User Application to use Transport Layer Security/Secure Sockets Layer (TLS/SSL), you must ensure the trusted root certificate of the web container running One SSO Provider (OSP) is installed in the truststore for the application server running Home, the Dashboard, and the User Application.

Typically, you should put the trusted root certificate from the keystore you used to configure the OSP container TLS/SSL into the `cacerts` keystore for the JRE used by the application server.

If you do not correctly configure the truststore when using TLS/SSL, if a user tries to log in to Identity Manager Home or the Provisioning Dashboard, the browser displays a flashing web page that never fully loads.

7.2 Recreating Identity Manager Home Database Tables in PostgreSQL

If you encounter an error in your environment and need to delete and recreate your `idmuserappdb` database tables, you can run the following Java command to rebuild the database:

```
/JavaPath/jdk1.7.0_21/bin/java -Xms256m -Xmx256m -Dwar.context.name=Context -
Ddriver.dn="DriverDN" -jar /UserAppPath/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/PostgreSQLPath/postgresql/postgresql-
8.4-701.jdbc4.jar:/DeployPath/IDMProv.war --changeLogFile=DatabaseChangeLog.xml --
url="jdbc:postgresql://localhost:5432/idmuserappdb" --contexts="prov,newdb" --
logLevel=info --logFile=/LogPath/db.out --username=DBAdmin --
password=DBAdminPassword update
```

Where *`JavaPath`* is the path to your updated JDK or JRE, *`Context`* is the context you specified when you installed the User Application (`IDMProv`, by default), *`DriverDN`* is the full DN of the User Application driver, *`UserAppPath`* is the path to your main User Application installation directory, *`PostgreSQLPath`* is the path to your PostgreSQL installation directory, *`DeployPath`* is the path to your User Application and Identity Manager Home JBoss `deploy` directory, *`LogPath`* is the path to the directory where you want to save the database log, *`DBAdmin`* is the database administrator account, and *`DBAdminPassword`* is the database administrator password.

For example:

```
/usr/java/jdk1.7.0_21/bin/java -Xms256m -Xmx256m -Dwar.context.name=IDMProv -
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -jar /opt/novell/
idm/rbpm/UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/novell/idm/rbpm/postgresql/
postgresql-8.4-701.jdbc4.jar:/opt/novell/idm/rbpm/jboss/server/IDMProv/deploy/
IDMProv.war --changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://
localhost:5432/idmuserappdb" --contexts="prov,newdb" --logLevel=info --logFile=/
opt/novell/idm/rbpm/UserApplication/db.out --username=idmadmin --password=test
update
```

A Installing Identity Manager Home Using a Non-Default Context

If you specified a context other than the default IDMProv context when you installed the Roles Based Provisioning Module, the name of the main User Application .war file, which is IDMProv.war by default, matches the context. For example, if you specified the context IDMStartHere, the name of the file would be IDMStartHere.war.

When installing Identity Manager Home in an environment with a non-default context, you must perform the following additional steps:

1. At a command prompt, navigate to the JBoss deploy directory. For example: /opt/novell/idm/jboss/server/IDMProv/deploy
2. Rename the IDMProv.war file you copied from the Enhancement Pack to match the context name. For example, change the file name from IDMProv.war to IDMStartHere.war.
3. Enter the following command:

   ```
   unzip IDMContext.war WEB-INF/web.xml
   ```

   Where *IDMContext* is the modified name of the IDMProv.war file.
4. Use a text editor to open the WEB-INF/web.xml file.
5. In the web.xml file, find the following entry:

   ```
   <display-name>IDMProv</display-name>
   ```
6. Change the IDMProv value to match the context name, then save and close the file.
7. At the command prompt, enter the following command:

   ```
   zip -u0 IDMContext.war WEB-INF/web.xml
   ```
8. Enter the following command:

   ```
   unzip IDMContext.war WEB-INF/lib/IDMfw.jar
   ```
9. Navigate to the WEB-INF/lib directory, the enter the following command:

   ```
   unzip IDMfw.jar PortalService-conf/config.xml
   ```
10. Use a text editor to open the WEB-INF/lib/PortalService-conf/config.xml file.
11. In the config.xml file, find the following entry:

    ```
    <key>portal.context</key>
    <value>${portal.context:IDMProv}</value>
    ```
12. Change the IDMProv value to match the context name, then save and close the file.
13. In the command prompt window, go to the WEB-INF/lib directory and enter the following command:

    ```
    zip -u0 IDMfw.jar PortalService-conf/config.xml
    ```

14 In the command prompt window, navigate to the deploy directory and enter the following command:

```
zip -u0 IDMContext.war WEB-INF/lib/IDMfw.jar
```

15 Delete the `WEB-INF` directory.

16 Close the command prompt.

B Using a SQL Script to Update the PostgreSQL Schema

To update your PostgreSQL database schema using the included SQL script, complete the following steps.

NOTE: You should only use the SQL script to update the schema if your organization requires users make all database updates using scripts or if the User Application tables were originally created or updated using the SQL script option during the Identity Manager Roles Based Provisioning Module 4.0.2 installation process.

1. Navigate to the User Application deploy directory within the JBoss installation. For example: `/opt/novell/idm/jboss/server/IDMProv/deploy`
2. In the `deploy` directory, use a text editor to open the `IDMProv-ds.xml` file.
3. In the `<connection-url>` element, append "`?compatible=true`" to the existing text. For example:

   ```
   <connection-url>jdbc:postgresql://localhost:5432/rbpmprov?compatible=true</
   connection-url>
   ```

4. Save and close the `IDMProv-ds.xml` file.
5. In a command prompt, navigate to the deploy directory and enter the following command:

   ```
   unzip IDMProv.war WEB-INF/web.xml
   ```

6. Use a text editor to open the `WEB-INF/web.xml` file and set the value of the `create-db-on-startup` parameter to `false`.
7. Save and close the `web.xml` file.
8. In the command prompt, enter the following command:

   ```
   zip -u0 IDMProv.war WEB-INF/web.xml
   ```

9. Delete the `WEB-INF` directory and all its contents.
10. Navigate to the User Application installation directory. For example: `/opt/novell/idm`
11. In a text editor, open the `Novell-Custom-Install.log` file.
12. Search for the following text:

    ```
    ************************************************
    If a failure is encountered while creating the tables, verify that this string
    is correct
    If not , you can modify this string and copy/paste to a command line to run
    ************************************************
    ```

13. At a command prompt, navigate to the User Application directory.
14. Copy the command specified in the `Novell-Custom-Install.log` file and paste the command into the command prompt.

15 Replace the asterisks (*) within the command with the database username and password and changing `--contexts="prov,newdb"` to `--contexts="prov,updatedb"` if necessary. Ensure the name of the SQL file is unique.

16 Before running the command, add the following new property before the `-jar` option:

```
-Ddriver.dn="DriverDN"
```

Where *DriverDN* is the full DN of the User Application driver. For example:

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m -Dwar.context.name=IDMProv -
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -jar /opt/
novell/idm/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/novell/idm/Postgres/postgresql-
8.4-701.jdbc4.jar:/opt/novell/idm/jboss/server/IDMProv/deploy/IDMProv.war --
changeLogFile=DatabaseChangeLog.xml --url="jdbc:postgresql://localhost:5432/
idmuserappdb" --contexts="prov,updatedb" --logLevel=info --logFile=/opt/
novell/idm/db.out --username=idmadmin --password=password updateSQL > /opt/
novell/idm/UA-update.sql
```

17 Press *Enter*.

18 Provide the generated SQL file for your Identity Manager environment to your database administrator to import into the database server.

19 After the database administrator imports the SQL file, start the User Application server.

C Roles Based Provisioning Module Configuration Reference

This appendix describes all new Identity Manager Home, User Application, Reporting Module, and Catalog Administrator settings users can configure using the Roles Based Provisioning Module Configuration utility (`configupdate.sh`), after installing Identity Manager Home.

For information about running the Configuration utility, see "Configuring the Roles Based Provisioning Module and Application Server" on page 21. For information about existing Configuration utility settings, see "User Application Configuration Reference," in the *Identity Manager Roles Based Provisioning Module 4.0.2 User Application: Installation Guide*.

C.1 Authentication Parameters

This table includes the new configuration parameters available on the *Authentication* tab of the Configuration utility, including advanced parameters.

Table C-1 *Identity Manager Home and User Application Authentication Parameters*

Type of Setting	Option	Description
Authentication	*OAuth server's auth endpoint*	Required. Specify the URL of the OAuth server you want to authorize authentication.
	OAuth server's token endpoint	Required. Specify the URL of the OAuth server you want to validate the authentication token.
	OAuth server's logout endpoint	Required. Specify the URL of the OAuth server that ends the authentication session.
	LDAP DN of Admins Container	Required. Specify the distinguished name of the container in the Identity Vault that contains any administrator User objects used to authenticate via OAuth.
	OAuth keystore file	Required. Specify the path to the Java JKS keystore file you want to use for OAuth authentication. The keystore file must contain at least one public/private key pair.

Type of Setting	Option	Description
	OAuth keystore file password	Required. Specify the password used to load the OAuth keystore file.
	Key alias of key for use by OAuth	Required. Specify the name of the public/private key pair in the OAuth keystore file that you want to use to authenticate.
	Key password key for use by OAuth	Required. Specify the password for the private key used by OAuth.
	URL to custom CSS file for login screen	Specify the URL of a CSS stylesheet you want to use to customize the appearance of the Identity Manager Home and User Application login page. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Duplicate resolution naming attribute	Specify the name of the LDAP attribute used to differentiate between multiple eDirectory User objects with the same `cn` value. The default value of this parameter is `mail`. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Restrict authentication sources to contexts	Indicates whether searches in the user and administrator containers in the Identity Vault are restricted to only User objects in those containers or searches should also include subcontainers. Possible values for this parameter are `true` or `false`. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Validity duration for access token	Specify the number of seconds an OAuth access token remains valid. If unspecified, the default value for this parameter is 120 seconds. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.

Type of Setting	Option	Description
	Validity duration for refresh token	Specify the number of seconds an OAuth refresh token remains valid. The refresh token is only used internally by OAuth. If unspecified, the default value for this parameter is 2592000 seconds, or 30 days. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Maximum login duration	Specify the maximum number of seconds the authentication server keeps an OAuth refresh token revocation entry. The refresh token revocation entry is used to ensure OAuth refresh tokens are invalidated when a user's authentication session expires. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
TLS/SSL	*TLS/SSL keystore file*	If the authentication server uses TLS/SSL, and the trust certificate for the authentication server is not in the JRE trust store (`cacerts`), specify the path and filename of the Java JKS keystore file that contains the authentication server trust certificate. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	TLS/SSL keystore file password	Specify the password used to load the TLS/SSL authentication server keystore file. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.

Type of Setting	Option	Description
Novell Audit Digital Signature Certificate and Key	*Novell Audit Digital Signature Certificate*	Specify a custom public key certificate you want the OAuth server to use to authenticate audit messages send to the audit system. For information about configuring certificates for Novell Audit, see "Managing Certificates" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/b5f4vw6.html), in the *Novell Audit Administration Guide* (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html). **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Novell Audit Digital Signature Private Key	Specify the path to the custom private key file you want the OAuth server to use to authenticate audit messages sent to the audit system. For information about configuring certificates for Novell Audit, see "Managing Certificates" (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/b5f4vw6.html), in the *Novell Audit Administration Guide* (http://www.novell.com/documentation/novellaudit20/novellaudit20/data/bookinfo.html). **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.

C.2 Single Sign-On Parameters

This table includes the new configuration parameters available on the *SSO Clients* tab of the Configuration utility.

Table C-2 *Identity Manager Home and User Application Single Sign-On Parameters*

Type of Setting	Option	Description
Landing	*OAuth client ID*	Required. Specify the name you want to use to identify the Identity Manager Home single sign-on client to the authentication server. The default value for this parameter is `ualanding`.

Type of Setting	Option	Description
	OAuth client secret	Required. Specify the password for the Identity Manager Home single sign-on client.
	URL link to dash page	Required. Specify the relative URL to use to access the Provisioning Dashboard from Identity Manager Home. The default value for this parameter is `/dash`.
	OSP Oauth redirect url	Required. Specify the URL to which the authentication server redirects a browser client when authentication is complete.
Dashboard	*OAuth client ID*	Required. Specify the name you want to use to identify the Identity Manager Provisioning Dashboard single sign-on client to the authentication server. The default value for this parameter is `uadash`.
	OAuth client secret	Required. Specify the password for the Identity Manager Provisioning Dashboard single sign-on client.
	OSP Oauth redirect url	Required. Specify the URL to which the authentication server redirects a browser client when authentication is complete.
	User email	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's email attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `Email`.
	User phone	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's phone number attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `TelephoneNumber`.

Type of Setting	Option	Description
	User mobile	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's mobile phone number attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `MobileNumber`.
	User firstname	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's first name attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `FirstName`.
	User location	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's location attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `Location`.
	User department	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's department attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `Department`.
	User lastname	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's last name attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `LastName`.

Type of Setting	Option	Description
	User title	Required. Specify the value the Roles Based Provisioning Module uses to identity a user's job title attribute in the user information REST API results. The value must match the Entities configured using Designer. The default value for this parameter is `Title`.
RBPM	*OAuth client ID*	Required. Specify the name you want to use to identify the User Application single sign-on client to the authentication server. The default value for this parameter is `rbpm`.
	OAuth client secret	Required. Specify the password for the User Application single sign-on client.
	URL link to landing page	Required. Specify the relative URL to use to access Identity Manager Home from the User Application. The default value for this parameter is `/landing`.
	OSP Oauth redirect url	Required. Specify the URL to which the authentication server redirects a browser client when authentication is complete.
	Optional dedicated truststore	This parameter is not currently used. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Optional dedicated truststore password	This parameter is not currently used. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
Reporting	*OAuth client ID*	Required. Specify the name you want to use to identify the Reporting Module single sign-on client to the authentication server. The default value for this parameter is `rpt`.
	OAuth client secret	Required. Specify the password for the Reporting Module single sign-on client.

Type of Setting	Option	Description
	URL link to landing page	Required. Specify the relative URL to use to access Identity Manager Home from the Reporting Module. The default value for this parameter is `/landing`.
	OSP Oauth redirect url	Required. Specify the URL to which the authentication server redirects a browser client when authentication is complete.
	Optional dedicated truststore	This parameter is not currently used. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
	Optional dedicated truststore password	This parameter is not currently used. **NOTE:** The utility only displays this parameter if you click *Show Advanced Options*.
DCS Driver	*OAuth client ID*	Required. Specify the name you want to use to identify the Data Collection Service driver single sign-on client to the authentication server. The default value for this parameter is `dcsdrv`.
	OAuth client secret	Required. Specify the password for the Data Collection Service driver single sign-on client.
Catalog Administrator	*OAuth client ID*	Required. Specify the name you want to use to identify the Catalog Administrator single sign-on client to the authentication server. The default value for this parameter is `rra`.
	OAuth client secret	Required. Specify the password for the Catalog Administrator single sign-on client.
	OSP Oauth redirect url	Required. Specify the URL to which the authentication server redirects a browser client when authentication is complete.

D Identity Manager Home REST APIs

Identity Manager Home incorporates several REST APIs that enable different features within the user interface.

For information about the REST APIs Identity Manager Home uses, see the following sections:

IMPORTANT: When you invoke a REST call containing an incorrect payload for removing an object, it returns a success response even if the item required to be removed does not exist.

D.1 POST /api/util/permssort (sort a list of permissions by display name)

Sort the specified list of permissions by display name.

NOTE: This REST API does not require authentication.

Used In

Team compare view

URL Parameters

None

Data to Send

```
{
    "perms": [
        {
            "id": "cn=changepwd,cn=RequestDefs,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
            "name": "Change Password"
        },
        {
            "id":
"cn=billing,cn=Level10,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
            "name": "Billing Department Access"
        }
    ]
}
```

Response payload for status code: 200 OK

```
{
    "perms": [
        {
            "id":
"cn=billing,cn=Level10,cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
            "name": "Billing Department Access"
        },
        {
            "id": "cn=changepwd,cn=RequestDefs,cn=AppConfig,cn=User Application
Driver,cn=driverset1,o=system",
            "name": "Change Password"
        }

    ]
}
```

D.2 POST /api/util/usersort (sort a list of users by full name)

Sort the specified list of users by full name.

NOTE: This REST API does not require authentication.

Used In

Team compare view

URL Parameters

None

Data to Send

```
{
    "users": [
        {
            "id": "cn=bbender,ou=users,o=novell",
            "name": "Bill Bender"
        },
        {
            "id": "cn=cnano,ou=users,o=novell",
            "name": "Chip Nano"
        },
        {
            "id": "cn=ablake,ou=users,o=novell",
            "name": "Allison Blake"
        }
    ]
}
```

Response payload for status code: 200 OK

```
{
    "users": [
        {
            "id": "cn=ablake,ou=users,o=novell",
            "name": "Allison Blake"
        },
        {
            "id": "cn=bbender,ou=users,o=novell",
            "name": "Bill Bender"
        },
        {
            "id": "cn=cnano,ou=users,o=novell",
            "name": "Chip Nano"
        }

    ]
}
```

D.3 POST /api/util/tasksort (sort a list of tasks by the specified column)

Sort the specified tasks by the specified column.

NOTE: This REST API does not require authentication.

Used In

Dashboard task view

URL Parameters

None

Data to Send

```
{
    "sortBy":"recipientName",
    "sortOrder":"ASC",
    "tasks": [
        {
            "taskId":"85a180b8fad3425fb58a6d906075571a",
            "processName":"Anonymous Access - Create New User",
            "creationTime":"1337273009422",
            "expirationTime":"1338482609422",
            "recipient":  "cn=bmalley,ou=users,o=novell",
            "recipientName":  "Bill Malley",
            "simpleForm":  true
        },
        {
            "taskId":"85a180b8fad3425fb58a6d906075571a",
            "processName":"Anonymous Access -Delete User",
            "creationTime":"1337273009422",
            "expirationTime":"1338482609422",
            "recipient":  "cn=ablake,ou=users,o=novell",
            "recipientName":  "Allison Blake",
            "simpleForm":  true
        }
    ]
}
```

NOTE

- The `recipientName` value must be a value in the JSON data.
- For the `sortOrder` value, you can specify either `ASC` (ascending order) or `DESC` (descending order).

Response payload for status code: 200 OK

```
{
    "sortBy":"recipientName",
    "sortOrder":"ASC",
    "tasks": [
        {
            "taskId":"85a180b8fad3425fb58a6d906075571a",
            "processName":"Anonymous Access -Delete User",
            "creationTime":"1337273009422",
            "expirationTime":"1338482609422",
            "recipient":  "cn=ablake,ou=users,o=novell",
            "recipientName":  "Allison Blake",
            "simpleForm":  true
        },
        {
            "taskId":"85a180b8fad3425fb58a6d906075571a",
            "processName":"Anonymous Access - Create New User",
            "creationTime":"1337273009422",
            "expirationTime":"1338482609422",
            "recipient":  "cn=bmalley,ou=users,o=novell",
            "recipientName":  "Bill Malley",
            "simpleForm":  true
        }
    ]
}
```