AUTHORIZED DOCUMENTATION

Role Mapping Administrator
Installation and Configuration Guide

Novell®
Identity Manager

1.0

August 28, 2009

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide provides installation and configuration instructions for the Novel® Identity Manager Role Mapping Administrator. The guide is organized as follows:

Installation Information:

- Chapter 1, “Overview,” on page 9
- Chapter 2, “Meeting Prerequisites and System Requirements,” on page 15
- Chapter 3, “Installing the Role Mapping Administrator,” on page 19

Configuration Information:

- Chapter 4, “Configuring the Application,” on page 21
- Chapter 6, “Configuring Authentication,” on page 31
- Chapter 7, “Enabling Auditing,” on page 43
- Chapter 8, “Security Best Practices,” on page 49
- Chapter 9, “Troubleshooting,” on page 51

Audience

This guide is intended for partners, consultants, and customers who are very familiar with the products in the Novell Compliance Management Platform extension for SAP environments.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell Identity Manager Role Mapping Administrator Installation and Configuration Guide*, visit the Novell Compliance Management Platform extension for SAP environments Documentation Web site (http://www.novell.com/documentation/ncmp_sap10).

Additional Documentation

For documentation on the Novell Compliance Management Platform, see the Novell Compliance Management Platform Documentation Web site (http://www.novell.com/documentation/ncmp10/index.html).

For documentation on the Identity Manager Roles Based Provisioning Module, see the Identity Manager Roles Based Provisioning Module 3.6.1 Documentation Web site (http://www.novell.com/documentation/idmrbpm361/index.html).

For documentation on the SAP* drivers, see the Identity Manager 3.6 Drivers Documentation Web site (http://www.novell.com/documentation/idm36drivers/index.html).

For documentation on Access Manager, see the Access Manager 3.1 Documentation Web site (http://www.novell.com/documentation/novellaccessmanager31/index.html).

For documentation on Sentinel™, see the Sentinel 6.1 Documentation Web site (http://www.novell.com/documentation/sentinel61/index.html).

For documentation on the SAP Connector, SAP Collector, and the SAP Solution Pack, see the Sentinel 6.1 download Web site (http://support.novell.com/products/sentinel/secure/sentinel61.html).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

Overview

1

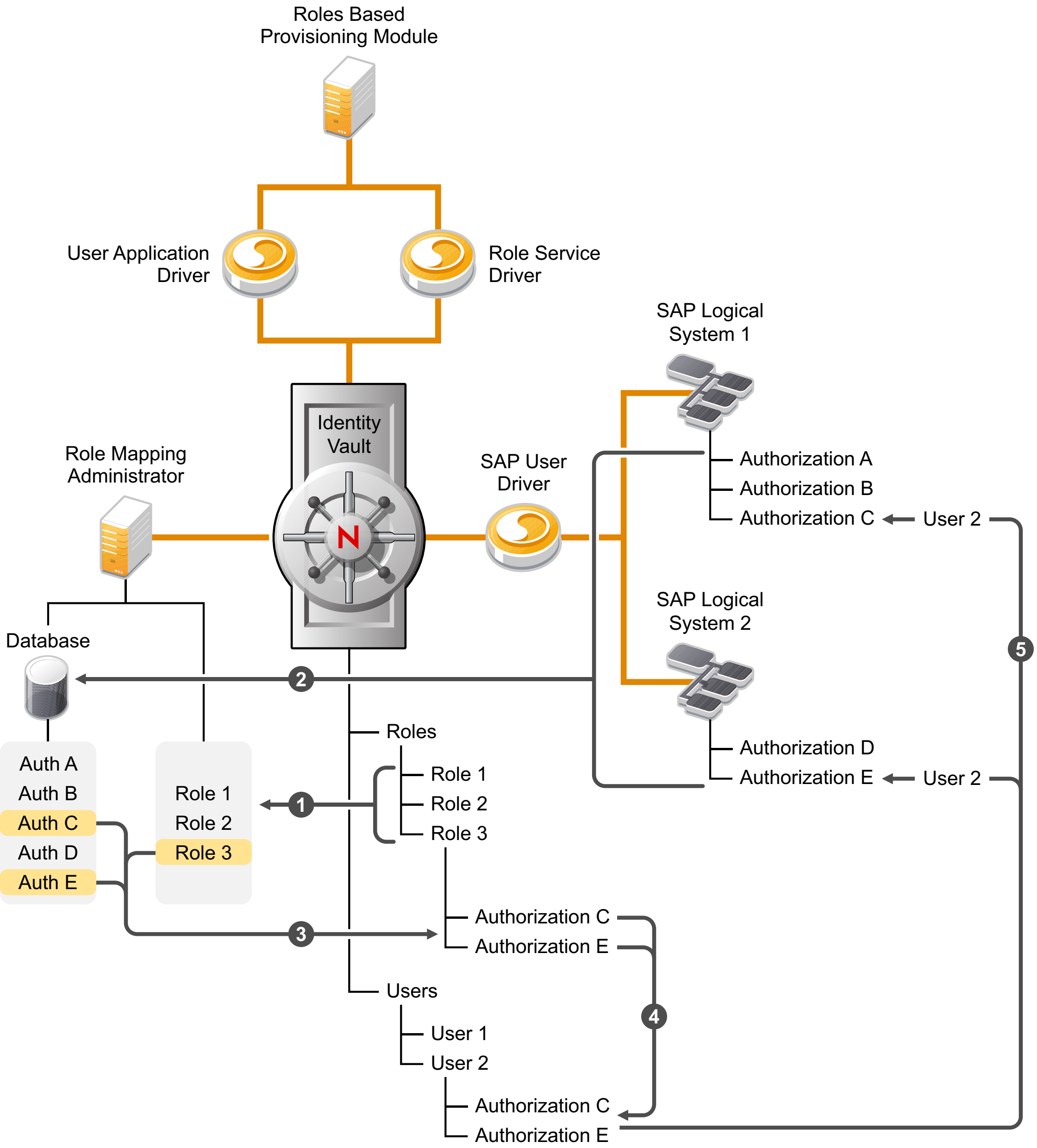
The Novell Identity Manager Role Mapping Administrator lets you map roles, composite roles, and profiles (collectively referred to as *authorizations*) to Identity Manager roles. When a user is assigned an Identity Manager role in the Roles Based Provisioning Module, he or she receives all authorizations mapped to that role.

The following sections provide information you should understand before installing and configuring the Role Mapping Administrator:

1.1 How Role Mapping Works

The Role Mapping Administrator is one part of the Novell role mapping solution. It is dependent on the proper installation and configuration of all role mapping components. The following diagram shows the components involved in the role mapping. Following the diagram, the role mapping process is explained, using SAP as the connected system to Identity Manager.

Figure 1-1 How the Role Mapping Administrator Works



1. The Role Mapping Administrator connects to the Identity Vault and reads the Identity Manager roles stored in the vault.
2. The Role Mapping Administrator retrieves the SAP systems authorizations by using the SAP User Management driver to query the connected SAP systems. The retrieved SAP authorizations are added to the Role Mapping Administrator database.
3. A user of the Role Mapping Administrator maps authorizations to one or more Identity Manager roles. When an authorization is mapped to a role, the role is updated in the Identity Vault to reflect the authorization mapping.

4. A user is assigned the role in the Roles Based Provisioning Module, at which point the Role Service driver grants the user an entitlement to all SAP authorizations that are mapped to the role.
5. The SAP User Management driver responds to the entitlement grant by initiating the authorization assignment in the SAP system.

1.2 Role Mapping Administrator

The Role Mapping Administrator is a Web application. All components required for the application are included in the installation file, including a Tomcat application server and an HSQL database. See Chapter 2, “Meeting Prerequisites and System Requirements,” on page 15 for the application’s system requirements.

1.3 Identity Vault Access

The Role Mapping Administrator requires access to the Identity Vault. This enables the Role Mapping Administrator to perform the required Identity Vault operations, including:

- Authenticating users who log in to the Role Mapping Administrator and establishing their authorization level (Role Module Administrator or Role Manager).
- Retrieving roles information to display if the authenticated user is a Role Module Administrator. If the authenticated user is a a Role Manager, the Role Mapping Administrator uses the user’s credentials to display roles.
- Adding authorization information to the Role objects when an authorization is mapped to an Identity Vault role.
- Accessing information stored on the Identity Manager driver object to build the queries required to retrieve authorizations from connected systems.
- Sending the queries to the Identity Manager drivers.
- Creating, editing, and deleting roles.

For more information, see Section 2.5, “Granting Rights to the Use Role Mapping Administrator,” on page 17.

1.4 System Access

The Role Mapping Administrator does not require direct access to the connected systems. All authorizations are retrieved through the Identity Manager drivers, that support the Role Mapping Administrator.

When the Role Mapping Administrator connects to the Identity Vault, it automatically detects the Identity Manager drivers configured in the vault. The Role Mapping Administrator displays each system connected via a driver and allows you to retrieve authentications from any of those systems.

For a list of the supported Identity Manager drivers, see Chapter 2, “Meeting Prerequisites and System Requirements,” on page 15.

1.5 Authentication

The Role Mapping Administrator uses the Identity Vault to authenticate users. Access is restricted to Identity Vault users who are defined as Role Module Administrators or Role Managers in the Roles Based Provisioning Module application.

You can set up Role Mapping Administrator authentication through the following methods:

- **Direct login:** The user provides credentials (username and password) on the Role Mapping Administrator login page.
- **Single sign-on through the Roles Based Provisioning Module:** A Role Mapping Administrator link is added to the Roles Based Provisioning Module. When a user clicks the link, the Roles Based Provisioning Module passes the user's credentials to the Role Mapping Administrator.
- **Single sign-on through Access Manager:** Access Manager provides the user's credentials (username and password or SAML token) to the Role Mapping Administrator through Access Manager Identity Injection. The user is not prompted for any credential information.

For information on how to configure single sign-on, see Chapter 6, "Configuring Authentication," on page 31.

1.6 Authorization

Only users who are defined as Role Module Administrators or Role Managers in the Roles Based Provisioning Module can log in to the Role Mapping Administrator. After a user is logged in, the user can perform only the tasks associated with his or her assigned role:

- **Role Module Administrator:** Authorizes a user to:
  - Map connected systems authorizations to all Identity Manager roles
  - Create, modify, and remove Identity Manager roles
- **Role Manager:** Authorizes a user to:
  - Map connected systems authorizations to select Identity Manager roles
  - Create, modify, and remove select Identity Manager roles

  A Role Manager can only map and manage Identity Manager roles to which he or she has been granted access in the Roles Based Provisioning Module. Roles to which the user doesn't have access are not displayed in the Role Mapping Administrator.

For information, see Section 2.5, "Granting Rights to the Use Role Mapping Administrator," on page 17.

1.7 Database

The Role Mapping Administrator uses HSQLDB, a lightweight 100% Java* SQL database, to store authorizations that it retrieves from the connected systems. This allows the Role Mapping Administrator to quickly display authorizations for mapping.

The connected systems authorizations must be manually loaded into the database. You can select which authorizations (Group, Roles, or Profiles) you want loaded for each system connected through a supported Identity Manager driver. After the authorizations have been loaded into the database, authorizations must be manually refreshed to reflect any new authorizations in the connected systems.

Identity Manager roles are not stored in the Role Mapping Administrator database. The Role Mapping Administrator reads and displays the roles directly from the Identity Vault.

1.8 Role Management

In addition to mapping roles, the Role Mapping Administrator can create new Identity Manager roles, edit existing roles, and remove existing roles. When creating a new role, you can add the role to the correct category, give it a level location, and assign owners.

Meeting Prerequisites and System Requirements 2

- Section 2.1, "Prerequisites," on page 15
- Section 2.2, "System Requirements," on page 16
- Section 2.3, "Installing the 3.0.1 Designer Auto Update," on page 16
- Section 2.4, "Installing the iManager plug-ins for Identity Manager 3.6.1," on page 16
- Section 2.5, "Granting Rights to the Use Role Mapping Administrator," on page 17

2.1 Prerequisites

Verify that the following prerequisites have been met before installing the Role Mapping Administrator:

- ❑ Install and configure Identity Manager 3.6. For more information, see the *Identity Manager 3.6 Installation Guide* (http://www.novell.com/documentation/idm36/idm_install/index.html?page=/documentation/idm36/idm_install/data/front.html).
- ❑ Install and configure the Roles Based Provisioning Module. For more information, see the *Roles Base Provisioning Module Installation Guide* (http://www.novell.com/documentation/idmrbpm361/install/data/bcy2k2j.html).
- ❑ The Identity Manager drivers that support the Role Mapping Administrator use structured GCVs. You must have updated iManager plug-ins and an updated Designer in order to manage these new drivers.
    - Install the 3.01 Designer AU
    - Install the iManager plug-ins for Identity Manager 3.6.1
- ❑ Install and configure the supported Identity Manager drivers. You can have one or more of each supported driver. The following Identity Manager 3.6.1 drivers are supported with the Role Mapping Administrator.
    - Driver for SAP User Management
    - Driver for SAP Portal
    - Driver for SAP GRC Access Control

  Only the Identity Manager 3.6.1 drivers are supported. They can run on Identity Manager 3.6 or 3.6.1. For installation instructions, see the following driver guides:
    - *Identity Manager 3.6.1 Driver for SAP GRC Access Control Implementation Guide*
    - *Identity Manager 3.6.1 Driver for SAP Portal Implementation Guide*
    - *Identity Manager 3.6.1 Driver for SAP User Management Implementation Guide*
- ❑ Grant users sufficient rights to use the Role Mapping Administrator, so they can log in and use the application. For instructions, see Section 2.5, "Granting Rights to the Use Role Mapping Administrator," on page 17.

2.2 System Requirements

The following is the list of system requirements for the Role Mapping Administrator. Only one instance of the Role Mapping Administrator can be installed per server.

System Component	Requirement
Role Mapping Administrator	SUSE® Linux Enterprise Server 10 SP2
Web Browser	Microsoft* Internet Explorer* 7
	Mozilla* Firefox* 3
Java	Java 5

2.3 Installing the 3.0.1 Designer Auto Update

In order to manage drivers with structured GCVs, you must install the 3.0.1 Designer Auto Update.

1 From the Designer 3.0.1 toolbar, select *Help > Check for Designer Updates*.

2 Follow the prompts to complete the installation.

3 Click *Yes* to restart Designer.

   Designer must be restarted for the changes to take effect.

2.4 Installing the iManager plug-ins for Identity Manager 3.6.1

In order to manage drivers with structured GCVs, you must install the iManager plug-ins for Identity Manager 3.6.1.

1 Launch iManager and log in as an administrative user.

2 From the toolbar, click the *Configure* icon.

3 Click *Plug-in Installation > Available Novell Plug-in Modules*.

4 Select *Novell Identity Manager Plug-ins for 3.6.1*, then click *Install*.

5 Select *I Agree* in the license agreement, then click *OK*.

6 After the installation completes, click *Close* twice.

7 Log out of iManager and restart Tomcat to have the changes take effect.

or

1 If the Novell Identity Manager Plug-ins for 3.6.1 are not in the list, download the Identity Manager 3.6.1 plug-ins for iManager 2.7 from the Novell product download Web site (http://download.novell.com) to your iManager server.

2 Launch iManager and log in as an administrative user.

3 From the toolbar, click the *Configure* icon.

4 Click *Plug-in Installation > Available Novell Plug-in Modules*.

5 Click *Add*.

6 Browse to and select the Identity Manager `.npm` file, then click *OK*.

7. After the installation completes, click *Close* twice.
8. Log out of iManager and restart Tomcat to have the changes take effect.

2.5 Granting Rights to the Use Role Mapping Administrator

Users must have a specific set of rights in the Identity Vault and specific role assignments in the Roles Based Provisioning Module to use the Role Mapping Administrator.

The best practice is to create a user that is used for administration of the Role Mapping Administrator. All other users that use the Role Mapping Administrator should have their rights limited to match their job duties.

- Section 2.5.1, "Identity Vault Rights for Administration," on page 17
- Section 2.5.2, "Roles Based Provisioning Module Assignments for Administration," on page 18
- Section 2.5.3, "Rights Required to Use Role Mapping Administrator," on page 18

2.5.1 Identity Vault Rights for Administration

An administrative user needs the following minimal rights to use the Role Mapping Administrator:

- Browse entry rights so they can select objects in the configuration panel of the Role Mapping Administrator. For example the Root User Container, Driver Discover DN, and the User Application driver DN.
- Browse entry and read rights on the users contained within the Root User container defined in the configuration panel of the Role Mapping Administrator. The list of potential role owners is derived by these rights.
- Browse entry rights on the active Driver Set object that is located under the Driver Discovery DN as defined in the Role Mapping Administrator configuration panel.
- Inherited browse rights and read attribute rights on the drivers that participate in role mapping. The Role Mapping Administrator needs access to the entitlements and entitlement configuration objects that are contained within the drivers that participate in role mapping.
- Inherited browse entry and read attribute rights on the User Application driver. The Role Mapping Administrator needs access to DAL category definitions, role configuration objects, and role definition containers.
- Inheritable supervisor rights to the roleDefs.RoleConfig.AppConfig container within the UAD. All role adds, modifies, and deletes are done with these rights. Rights can be pared down as needed.

You can make these assignments to specific users or you can make the assignments to a group or a container, then assign users to the group or add users to the container.

1. Log in to iManager as an administrative user for your Identity Vault.
2. Select *View Objects* in the toolbar, then browse to and select the user, group, or container you want to assign rights to.
3. Select the object, then click *Actions* > *Modify Trustees*.
4. Add the rights as defined above, then click *OK* to save the changes.

2.5.2 Roles Based Provisioning Module Assignments for Administration

The administration or configuration users must be members of the Role Manager role or the Role Module Administrator role in the Roles Based Provisioning Module. You can make these role assignments to specific users or you can make the assignments to a group or a container, then assign users to the group or add users to the container.

1. Log in to the Roles Based Provisioning Module as an administration user.
2. Click *Roles* > *Roles Assignments*.
3. Select *User*, *Group*, or *Container* to make the role assignment.
4. Search for the user, group, or container, then select the desired object.
5. Click *New Assignment*.
6. Fill in the following fields:

   Initial Request Description: Specify a reason for requesting the role.

   Select Roles: Search for the *Role Manager* role and the *Role Module Administrator* role, select the roles, then click *Select*.

   Effective Date: (Optional) Specify a date this assignment is effective.

   Expiration Date: (Optional) Select whether there is an expiration date for this assignment.
7. Click *Submit* to make the assignments.

2.5.3 Rights Required to Use Role Mapping Administrator

A user should be only granted the minimal rights required to fulfill their job duties. You can restrict rights by restricting the rights to the roles the user is assigned to and restricting their rights in the Identity Vault as well. The extension for SAP environments solutions guide contains a solution specific to this scenario. For more information, see “Managing Roles” in the *Novell Compliance Management Platform Extension for SAP Environments 1.0 SP1 Solutions Guide*.

Installing the Role Mapping Administrator

3

You should not install the Role Mapping Administrator as `root`.

To install the Role Mapping Administrator:

1. Download the application from the Novell Compliance Management Platform extension for SAP environments product download Web site (http://download.novell.com/Download?buildid=8o_N7mVgOVo~).
2. From a command line, enter `java -jar path_to_IDMRMAP.jar`.
3. Enter `yes` to accept the license agreement.
4. Specify the installation location for the application.

   The default path is your current location.

   You must have the appropriate rights to the directory where you are installing.
5. Specify the portion of the URL representing the application.

   The default value is IDMRMAP.
6. Specify the HTTP port number.

   The default value is 8081.
7. Specify a password for the configuration administrator.

   This is the password used to access the configuration page of the application.

The Role Mapping Administrator is now installed. The application is not automatically started after the installation completes. Use the `start.sh` and stop `stop.sh` scripts in the installation directory to stop and start the application.

After the application is installed and started, you must configure it. Proceed to Chapter 4, “Configuring the Application,” on page 21.

If you need to change any of the information specified during the installation, see Chapter 5, “Changing the Configuration,” on page 29.

Configuring the Application

4

After you install the Role Mapping Administrator, you need to configure the application with the information required for it to connect to the Identity Vault. You also need to configure the Identity Manager drivers and load the SAP authorizations into the Role Mapping Administrator database so that the application is ready to use.

4.1 Providing Identity Vault Connection Information

1 In a supported Web browser, enter the Role Mapping Administrator address. For example:

```
http://server:port
```

where *server:port* is the DNS (or IP address) and port of the server that is hosting the application. By default, the port is 8081.

The Role Mapping Administrator configuration login page is displayed.

2 Specify the configuration administration password set during the installation, then click *Login*.

The Role Mapping Administrator Configuration page is displayed.

3 Fill in the following fields:

Vault Display Name: Specify a display name for the Identity Vault in the Role Mapping Administrator.

Role Vault Address: Specify the DNS address of the Identity Vault. IP addresses are accepted but not recommended.

Role Vault Port: Specify the Identity Vault port. The default port is 389 or 636 for SSL.

Use SSL: Select this option to connect to the Identity Vault through SSL. For additional configuration steps, see Section 4.4.2, “Enabling SSL for a Browser to Access the Role Mapping Administrator,” on page 25.

Admin DN: Specify the LDAP distinguished name (LDAP DN) of an Identity Vault administrator user. The administrator user provides a proxy through which the Role Mapping Administrator can perform LDAP operations in the Identity Vault.

Admin Password: Specify the password for the administrator user.

Root User Container: Browse to the root container for the user objects in the Identity Vault.

The container must be specified by the fully qualified LDAP DN. For example:

```
ou=users,ou=data,o=novell
```

User App Driver DN: Browse to the User Application driver located in the Identity Vault.

The driver must be specified by the fully qualified LDAP DN. For example:

```
cn=UserApp1,cn=IDMDrivers,o=novell
```

Driver Discovery DN: Specify the root location to search for drivers. For example, if you only have one driver set, specify the driver set. If you have multiple driver sets, specify the container that holds the driver sets.

If this field is left blank, an LDAP search is performed of the entire Identity Vault. If you change this value after you have loaded the authorizations, the authorizations can change.

Access Manager Logout URL: (Optional) Specify the URL for the Access Manager Identity Server. This is allows for simultaneous logout from the Role Mapping Administrator and Access Manager. Having a value in this filed does not enable this behavior. For more information, see Chapter 6, "Configuring Authentication," on page 31.

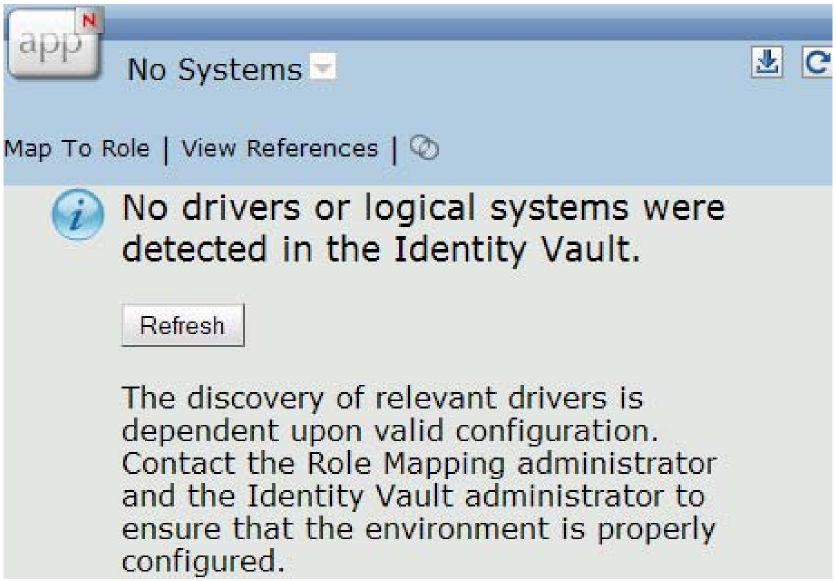
4 Click *Save*.

5 Click *Login To Role Mapping Administrator* to launch the Role Mapping Administrator.

4.2 Configuring the Drivers

After you log in to the Role Mapping Administrator, you might or might not have the supported Identity Manager configured to populate the authorizations. If the drivers are not configure, the message *No drivers or logical systems were detected in the Identity Vault* is displayed in the Authorizations panel.

Figure 4-1 *No Identity Manager Drivers Configured*



No drivers or logical systems were detected in the Identity Vault.

The discovery of relevant drivers is dependent upon valid configuration. Contact the Role Mapping administrator and the Identity Vault administrator to ensure that the environment is properly configured.

The following criteria must be met, for each Identity Manager driver, used to add authorizations to the Role Mapping Administrator.

❑ The Identity Manager driver is supported with the Role Mapping Administrator. The following are the supported drivers:

- *Identity Manager 3.6.1 Driver for SAP GRC Access Control Implementation Guide*

  - *Identity Manager 3.6.1 Driver for SAP Portal Implementation Guide*
  - *Identity Manager 3.6.1 Driver for SAP User Management Implementation Guide*

□ The Role Mapping GCVs are configured for each driver.

□ The Identity Manager drivers are running. For more information, see “Starting, Stopping, or Restarting the Driver” in the *Identity Manager 3.6.1 Common Driver Administration Guide*.

To configure the GCVs:

1. In Designer or iManager access the properties of the driver.
2. Click GCVs.
3. Select *show* for the *Role Mapping > Show role mapping configuration*.
4. Select *Yes* to enable role mapping.

   The options for each driver are different. Refer to each implementation guide for the specific parameters.
5. Click *OK* to save the changes.

4.3 Loading Authorizations into the Database

The Role Mapping Administrator stores the authorizations for the connected systems in its local database. This database must be loaded before users can map authorizations to roles. Any user who is authorized to log in to the Role Mapping Administrator can load and reload the database. Load the database the first time you log in so that it is ready for immediate use.

You can control from which connected systems authorizations are loaded, and you can control which types of authorizations (Groups, Roles, Profiles, or all) are loaded.

1. In the Authorizations panel, click the *Load Authorizations* icon ⬇ to display the authorizations to load.
2. Select the types of authorizations (Groups, Roles, and Profiles) you want loaded for each system displayed.

   If you select Roles, both single roles and composite roles are loaded.
3. Click *OK*.

   The Role Mapping Administrator begins retrieving the authorizations from the selected connected systems. The time required to retrieve and load the authorizations depends on the number of connected systems you selected and the number or authorizations contained in each system.

4.4 Enabling SSL

To enable SSL there are two different components that must be configured to completely secure the communication channel.

- Section 4.4.1, “Enabling an SSL Connection from the Role Mapping Administrator to the Identity Vault,” on page 24
- Section 4.4.2, “Enabling SSL for a Browser to Access the Role Mapping Administrator,” on page 25

4.4.1 Enabling an SSL Connection from the Role Mapping Administrator to the Identity Vault

You can configure the Role Mapping Administrator to have an SSL connection to the Identity Vault. The following explains how to configure the Role Mapping Administrator to use SSL.

1 Select *Use SSL* during the configuration of the Role Mapping Administrator.

2 Specify the LDAP port for SSL on the Identity Vault during the configuration of the Role Mapping Administrator.

3 If you have a self-signed certificate, proceed to Step 5. Otherwise, continue with Step 4 to create a self-signed certificate in iManager.

4 Export a self-signed certificate from the certificate authority in the Identity Vault:

   4a From iManager, in the *Roles and Tasks* view, click *Directory Administration* > *Modify Object*.

   4b Select the certificate authority object for the Identity Vault, then click *OK*.

   It is usually found in the Security container and is named something like *TREENAME CA.Security*.

   4c Click *Certificate* > *Self Signed Certificate*.

   4d Click *Export*.

   4e When you are asked if you want to export the private key with the certificate, click *No*, then click *Next*.

   4f Select either *File in binary DER format* or *File in Base64 format* for the certificate, then click *Next*.

   The Role Mapping Administrator uses a Java-based keystore or trust store, so you can choose either format.

   4g Click *Save the exported certificate*.

   4h Browse to a location on your computer where you want to save the file, then click *Save*.

   or

   Click *Save* to save the file to the default location.

   Different browsers act differently.

   4i Click *Close*.

5 Import the self-signed certificate into the Role Mapping Administrator's trust store.

   5a Use the keytool executable that is included with any Java JDK*.

   For more information on keytool, see "Keytool - Key and Certificate Management Tool" (http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html).

   5b Import the certificate into the Role Mapping Administrator's trust store or by entering the following command at a command prompt:

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt
-keystore filename -storepass password
```

   For example:

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -
keystore cacerts -storepass changeit
```

The trusted certificate must be imported into the trust store of the JRE* that launches the Role Mapping Administrator.

4.4.2 Enabling SSL for a Browser to Access the Role Mapping Administrator

To finish enabling SSL, you need to configuring Tomcat for an SSL connection. For more information, see the Apache* Tomcat Documentation Web site (http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html).

1 Create a certificate with the following command.

```
JDK_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA
```

The default file name is *$HOME*/.keystore, which is the default keystore for Tomcat.

2 Edit the server.xml file to enable Tomcat for TLS communication. The file is located in /*installation_directory*/tomcat/conf/serrver.xml.

3 Locate the following section of the server.xml and unremark the section to enable SSL for Tomcat.

```
<Connector port="8444" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" keystoreFile="/path_to_keystore" keystorePass="password"
/>
```

Add the correct path to the keystore file and the correct password for your environment.

4 Restart Tomcat.

4.5 Configuring the Role Mapping Administrator for Automatic Startup

As first installed, the Role Mapping Administrator does not start automatically. You can configure the Role Mapping Administrator to automatically start when the server is started.

1 From the *Computer* menu, select *Gnome Terminal*.

2 Log in as root by entering su, then enter the root password.

3 Copy the start.sh file from the /*installation_directory*/idmrmap directory to the /etc/init.d directory.

4 Rename the file from start.sh to idmrmap.sh, for example.

You can name the file anything you want that does not already exist in the /etc/init.d directory.

5 Use a text editor to add the full path to the startup.sh file and to set the correct path for the Java installation. For example:

```
#!/bin/sh
export JAVA_HOME=/opt/novell/jdk1.5.0_11
export JRE_HOME=$JAVA_HOME/jre
export PATH=$JAVA_HOME/bin:$PATH
/home/admin/idmrmap/tomcat/bin/startup.sh
```

The default location of the `startup. sh` file is in the /*installation_directory*/idmrmap/tomcat/bin/startup.sh.

6. Enter `ls -l /etc/init.d/idmrmap` to verify the file copied.
7. Enter `chown root:sys /etc/init.d/idmrmap` to change the owner of the file.
8. Enter `chmod 700 /etc/init.d/idmrmap` to change access to the file.
9. Enter `chkconfig -add idmrmap` to add the script as a system service.
10. Use the following two commands to verify whether idmrmap runs before or after ndsd and userapp in run-level 3 during the system start procedure.

    Ultimately, you must ensure that idmrmap starts after ndsd and userapp.

    NOTE: The first command uses a lowercase letter l twice. It is not the number 11.

    ```
    metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep idmrmap
    lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12idmrmap -> ../idmrmap
    lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10idmrmap -> ../idmrmap
    ```

    ```
    metaserver1:/home/admin # ll /etc/init.d/rc3.d/ |grep ndsd
    lrwxrwxrwx 1 root root  7 2008-05-16 13:23 K11ndsd -> ../ndsd
    lrwxrwxrwx 1 root root  7 2008-05-16 13:23 S11ndsd -> ../ndsd
    ```

    Watch the SXX numbers (S10idmrmap and S11ndsd) that are prefixed to the script name. They indicate the start order. A higher number means the service is started after a lower number. If the numbers are the same, both services are started at the same time.

    In this case, idmrmap runs before ndsd, which is the opposite of what you want. Enter the following commands as a corrective action if the idmrmap number is the same or lower than the ndsd number:

    ```
    metaserver1:/home/admin # mv /etc/init.d/rc3.d/S10idmrmap /etc/init.d/
    rc3.d/S12idmrmap
    ```

11. Repeat Step 10 using userapp instead of ndsd.
12. Verify the startup order for run-level 5 (the same commands as Step 10, but instead of rc3.d, you now use rc5.d):

    ```
    metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep idmrmap
    lrwxrwxrwx 1 root root 10 2008-05-16 16:26 K12idmrmap -> ../idmrmap
    lrwxrwxrwx 1 root root 10 2008-05-16 16:26 S10idmrmap -> ../idmrmap
    ```

    ```
    metaserver1:/home/admin # ll /etc/init.d/rc5.d/ |grep ndsd
    lrwxrwxrwx 1 root root  7 2008-05-16 13:23 K11ndsd -> ../ndsd
    lrwxrwxrwx 1 root root  7 2008-05-16 13:23 S11ndsd -> ../ndsd
    ```

    Enter the following commands as a corrective action if the idmrmap number is the same or lower than the ndsd number:

    ```
    metaserver1:/home/admin # mv /etc/init.d/rc5.d/S10idmrmap /etc/init.d/
    rc5.d/S12idmrmap
    ```

13. Repeat Step 12 using userapp instead of ndsd.
14. Start the Role Mapping Administrator by entering `/etc/init.d/idmrmap start`
15. You must use the /*installation_directory*/idmrmap/stop.sh script to stop the Role Mapping Administrator.

    Entering `/etc/init.d/idmrmap stop` does not stop the Role Mapping Administrator.

16. Enter `exit` twice to log out as `root` and close the Gnome Terminal.

4.6 Chaning the Java Heap Size

By default, the minimum Java heap size is 64 MB and the maximum heap size is 256 MB for the Role Mapping Administrator. If you have a large set of roles or authorizations, increasing the Java heap size helps the performance of the Role Mapping Administrator.

To change the Java heap size:

1. Open the `/`*`installation_directory`*`/idmrmap/tomcat/bin/catalina.sh` file in a text editor.
2. Search for the lines:

   ```
   # Setup var for IDMRMAP configuration file
   JAVA_OPTS="$Java_OPTS -Xms64m -Xmx256m -
   Didmuserapp.logging.config.dir=$CATALINA_HOME/config -
   Dlog.init.file=idmrmap_logging.xml"
   ```

3. Increase the amount of memory allocated to the Role Mapping Administrator by changing the `-Xms64m` and `-Xmx256m` options.

   The amount of memory to add depends upon your environment.

4. Save your changes and exit out of the file.
5. Restart the Role Mapping Administrator using stop and start scripts.

5 Changing the Configuration

Changing the following information within the Role Mapping Administrator requires you to uninstall and reinstall the Role Mapping Administrator:

- Installation location
- Application context
- The HTTP port number
- The configuration administrator's password

The Role Mapping Administrator stores mappings and authorizations in the Identity Vault. When you uninstall and reinstall the Role Mapping Administrator, this information is not affected.

To uninstall the Role Mapping Administrator:

1. Stop the Role Mapping Administrator by executing the `stop.sh` script. The default location is:

   /*installation_directory*/idmrmap/stop.sh

2. Delete the installation directory. The default location is:

   /*installation_directory*/idmrmap

3. Delete the installation log that contains the parameters specified during the installation. The default location is:

   /*installation_directory*/install.log

4. Reinstall the Role Mapping Administrator with new values. For installation instructions, see Chapter 3, "Installing the Role Mapping Administrator," on page 19.

Configuring Authentication

6

There are three different ways to authenticate to the Role Mapping Administrator:

- **Direct login:** The user provides credentials (username and password) on the Role Mapping Administrator login page.
- **Single sign-on through the Roles Based Provisioning Module:** A Role Mapping Administrator link is added to the Roles Based Provisioning Module. When a user clicks the link, the Roles Based Provisioning Module passes the user's credentials to the Role Mapping Administrator.
- **Single sign-on through Access Manager:** Access Manager provides the user's credentials (username and password or SAML token) to the Role Mapping Administrator through Access Manager Identity Injection. The user is not prompted for any credential information.

Direct login is available as soon as the Role Mapping Administrator is installed. Authentication through the Roles Based Provisioning Module and Access Manager requires additional configuration.

- Section 6.1, "Configuring Single Sign-On Through the Roles Based Provisioning Module," on page 31
- Section 6.2, "Configuring Single Sign-On Through Access Manager," on page 33

6.1 Configuring Single Sign-On Through the Roles Based Provisioning Module

This solution uses the iFrame portlet of the Roles Based Provisioning Module. The iFrame portlet invokes a URL inside an iFrame control within the portlet. This allows the portlet to pass the authentication parameters from the Roles Based Provisioning Module to the Role Mapping Administrator.

- Section 6.1.1, "Enabling the Roles Based Provisioning Module for Single Sign-On," on page 31
- Section 6.1.2, "Creating a Shared Page," on page 32
- Section 6.1.3, "Assigning Permissions," on page 32
- Section 6.1.4, "Selecting Content," on page 32

6.1.1 Enabling the Roles Based Provisioning Module for Single Sign-On

1. Log in to the Roles Based Provisioning Module as the administrator user.
2. Select the *Administration* tab.
3. In the *Application Configuration* tab, select *Password Module Setup* > *Login*.
4. In the *Enable SSO* setting, select *true*.
5. Click *Save*, then log out to enable single sign-on.

6.1.2 Creating a Shared Page

1. Log in to the Roles Based Provisioning Module as the administrator user.
2. Select the *Administration* tab.
3. In the *Page Admin* tab, select *Maintain Shared Pages*.
4. Select *New* under *Page Actions* at the bottom of this page.
5. Fill in the following fields:

   Page Link Name: Specify the URL of the shared page that contains the iFrame in the Roles Based Provisioning Module.

   Page Name: This field is populated when you enter a value in the *Page Link Name* field. You can keep the prepopulated name or you can change it.

   Assign Categories: Select the categories where the shared page link is displayed in the Roles Based Provisioning Module. You can select one or more of the following options:

   - Administration
   - General
   - Information Management
   - Directory Management
   - Guest Pages
   - Password Management

   Description: (Optional) Specify a description for the new page.
6. Click *Save Page* to save the new page.

6.1.3 Assigning Permissions

By default, only the administrator user can see the new page. You must assign permissions to the users before they can see the page.

1. At the bottom of the *Page Admin* tab, click *Assign Permissions*.
2. Search for users, groups, or containers you want to assign rights to view this page.
3. Select the users, groups, or containers, then click the right-arrow to add them to the *Current Assignments* list.
4. Click *Save* to save the assignments, then close the window.

6.1.4 Selecting Content

1. At the bottom of the *Page Admin* tab, click *Select Content*.
2. Select *iFrame* in the *Available Content* pane, then click *Add*.
3. Click *Content Preferences* under the *Selected Content* pane.
4. Click *OK* in the message stating something has changed on the page.
5. Fill in the following fields:

   URL: Specify the URL to the login page for the Role Mapping Administrator.

   For example: http://dns_name:8081/IDMRMAP

URL / Form Parameters: Specify the following three parameters in the same order as listed below:

- `login_panel_user=$PORTLET_AUTH_ID$`
- `login_panel_pwd=$PORTLET_AUTH_PWD$`
- `url=./com.novell.rolemap.client.ui.UI/UI.html`

Encode URL parameters: Set this parameter to *True*.

Form Post?: Set this parameter to *True*.

Authentication Required?: Set this parameter to *True*.

Username: Specify the format of the username. This is the format that is used when a user logs into the Roles Based Provisioning Module. The three options are:

- **$(Application/login-user):** Passes the exact ID that is entered in the Roles Based Provisioning Module.
- **$(User/simpleid):** Only provides the CN of the user.
- **$(User/canonical):** Provides the dot notation of the logged-in user.

Password: Click *Use scope path*, then enter the following parameter in the *Password* field:

```
$(Application/login-pass)
```

Height and Width: Set the height and width options as required.

6 Click *Save Preferences* to save these parameters.

7 Click *Save Contents* to save the iFrame configuration.

6.2 Configuring Single Sign-On Through Access Manager

Access Manager allows users to log in to Active Directory* and launch a Web browser to automatically access the Role Mapping Administrator. The user does not need to enter a username or password.

The single sign-on process is as follows:

1. A user logs in to an Active Directory workstation and is issued a Kerberos* ticket.
2. Access Manager accepts the Kerberos ticket issued by Active Directory and extracts the userPrincpalName of the Active Directory user from the ticket.
3. Access Manager maps the userPrincpalName (from the Kerberos ticket) to user object attribute in the Identity Vault as defined by the Access Manager Kerberos class. For example, use the mail attribute.

   This attribute can be any attribute in the Identity Vault, including a custom attribute, as long as the value in the attribute matches the userPrincipalName attribute value in Active Directory.
4. When the user launches a Web browser and navigates to the Role Mapping Administrator URL, the configured Access Manager Proxy Service forwards the username and password, via a SAML assertion, to the Role Mapping Administrator. If the username and password match a user in the Identity Vault, the user is automatically authenticated without needing any additional credentials.

The following sections contain the steps required to configure Access Manager to allow the single sign-on to occur for the users.

- Section 6.2.1, “Prerequisites,” on page 34
- Section 6.2.2, “Configuring Active Directory to Assign Kerberos Tickets,” on page 34
- Section 6.2.3, “Configuring the Access Manager Identity Server to Consume the Kerberos Tickets,” on page 36
- Section 6.2.4, “Configuring the User’s Web Browser,” on page 42

6.2.1 Prerequisites

- ❑ Install and configure Access Manager 3.1. For more information, see the *Novell Access Manager 3.1 SP1 Installation Guide*.
- ❑ Make sure that time is synchronized among the Access Manager Identity server, the Role Mapping Administrator, and the Identity Vault.
- ❑ Add a DNS A record for the Role Mapping Administrator to your DNS server. Access Manager uses the DNS name to handle requests.

6.2.2 Configuring Active Directory to Assign Kerberos Tickets

Complete the following sections to enable Active Directory to assign Kerberos tickets. When users logs in to Active Directory they are automatically issued a Kerberos ticket.

- “Installing the spn and ktpass Utilities” on page 34
- “Creating a User Account in Active Directory for the Identity Server” on page 34
- “Creating a Keytab File” on page 35

Installing the spn and ktpass Utilities

The spn and ktpass utilities must be installed on the Active Directory domain controller. These utilities are not installed by default. You need both of these utilities to configure the Access Manager Identity Server for Kerberos authentication.

1. Insert the Windows* 2003 disk into the CD drive.
2. To install the utilities, run `\SUPPORT\TOOLS\SUPTOOLS.MSI` on the CD.

   The utilities are installed in `C:\Program Files\Support Tools`.

Creating a User Account in Active Directory for the Identity Server

Creating this account allows the Identity Server from Access Manager to run as a service.

1. In the user management tool, using the following information to create the user account:

   firstname: Specify a name for the Identity Server.

   lastname: Specify a name for the Identity Server.

   userPrincipalName: Specify the userPrincipalName. The format is HTTP/your.idp.fqdn@YOUR.DOMAIN.

   For example: HTTP/amser.provo.novell.com@AD.NOVELL.COM

samAccountName: Specify the samAccountName for the user. It consists of the firstname-lastname (required for the setspn utility).

password: Specify a password for this user account.

Deselect the option *User must change password at next logon* and select the option *Password never expires*. The user account needs a password, but it must never expire or be changed.

2 Set the servicePrinicpalNames on the user object.

This sends the Kerberos token to the Identity Server instead of directly to the SAP Portal, so the single sign-on can occur.

2a At a command line, enter:

```
setspn -a HTTP/amserv.provo.novell.com@AD.NOVELL.COM samAccountName
```

2b At a command line, enter:

```
setspn -a HTTP/amserv.provo.novell.com samAccountName
```

3 Export the keytab file by using the ktpass utility.

```
ktpass /out nidp.keytab /princ HTTP:///
amserv.provo.novell.com@AD.NOVELL.COM /mapuser
samAccountName@AD.NOVELL.COM /pass secret +DesOnly /crypto DES-CBC-MD5 /
ptype KRB5_NT_PRINCIPAL
```

4 Copy the keytab file to `jre` directory on the Identity Server. The default location is:

Linux: `/opt/novell/java/jre/lib/security`

Windows: `C:\Program Files\Novell\jre\lib\security`

Creating a Keytab File

The keytab file contains the secret encryption key that is used to decrypt the Kerberos ticket. You need to generate the keytab file and copy it to the Identity Server.

1 On the Active Directory server, open a command window and enter a `ktpass` command with the following parameters:

```
ktpass /out value /princ value /mapuser value /pass value
```

The command parameters require the following values:

Parameter	Value	Description
/out	<outputFilename>	Specify a name for the file, with `.keytab` as the extension. For example: `nidpkey.keytab`
/princ	<servicePrincipalName>@<KERBEROS_REALM>	Specify the service principal name for the Identity Server, then @, followed by the Kerberos realm. The default value for the Kerberos realm is the Active Directory domain name in all capitals. The Kerberos realm value is case sensitive.
/mapuser	<identityServerUser>@<AD_DOMAIN>	Specify the username of the Identity Server user and the Active Directory domain to which the user belongs.
/pass	<userPassword>	Specify the password for this user.

For this configuration example, you would enter the following command to create a keytab file named `nidkey`:

```
ktpass /out nidkey.keytab /princ HTTP/amser.provo.novell.com@AD.NOVELL.COM
/mapuser/ amser@AD.NOVELL /pass novell
```

2 Copy the keytab file to the Identity Server.

The default location for the keytab file on the Identity Server is:

- **Linux:** `/opt/novell/java/jre/lib/security`
- **Windows:** `C:\Program Files\Novell\jre\lib\security`

6.2.3 Configuring the Access Manager Identity Server to Consume the Kerberos Tickets

You must configure Access Manager to consume the Kerberos tickets from Active Directory. Access Manager can use the authentication information in the Kerberos tickets to enable single sign-on for the Role Mapping Administrator.

- "Enabling Logging for Kerberos Transactions" on page 36
- "Creating the bcsLogin.conf File" on page 37
- "Creating a User Store for the Active Directory Domain" on page 37
- "Creating a Kerberos Authentication Class for the Identity Server" on page 38
- "Creating a Kerberos Method for the Identity Server" on page 39
- "Creating a Kerberos Contract for the Identity Server" on page 39
- "Verifying the Kerberos Configuration" on page 39
- "Creating a SAML Identity Injection Policy" on page 40
- "Refreshing the Identity Server" on page 40
- "Creating a Protect Resource for the Role Mapping Administrator" on page 40
- "Refreshing the Access Gateway" on page 41

Enabling Logging for Kerberos Transactions

This helps with troubleshooting authentication issues.

1 In the Access Manager Administration Console, click *Devices* > *Identity Server* > *Edit* > *Logging*.

2 Select the *File Logging* and *Echo to Console* options to enable these options.

3 Under the *Component File Loggers Levels* heading, set the *Application* option to *debug*.

4 Enable *Trace Logging*, then select *Application*, *Configuration*, and *User Store* as *Component Content Filters*.

5 Click *OK*, then update the Identity Server.

Creating the bcsLogin.conf File

The `bcsLogin.conf` file is an authentication file for Java authentication and authorization service (JAAS).

1 In an text editor, type the following lines:

```
com.sun.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
debug="true"
useTicketCache="true"
ticketCache="/opt/novell/java/jre/lib/security/spnegoTicket.cache"
doNotPrompt="true"
principal="HTTP/amser.provo.novell.com@AD.NOVELL.COM"
useKeyTab="true"
keyTab="/opt/novell/java/jre/lib/security/nidpkey.keytab"
storeKey="true";
};
```

The file cannot contain any white space, only end-of-line characters.

ticketCache: The location of the cache file where the Kerberos ticket is stored. In the example, this is the default location on SLES 10. If you are using Windows, the default location is:

```
C:\\Program Files\\Novell\\jre\\lib\\security\\spnegoTicket.cache
```

The path must contain double slashes.

principal: Specify the service principal name for the Access Manager Identity Server. This value is unique to your configuration.

keyTab: Specify the location of the keytab you created in "Creating a Keytab File" on page 35. This value is unique to your configuration. In the example, this is the default location on SLES 10. If you are using Windows, the default location is:

```
C:\\Program Files\\Novell\\jre\\lib\\security\\nidpkey.keytab
```

The path must contain double slashes.

2 Save this file with the name `bcsLogin.conf`.

3 Copy this file to the directory where the keytab file is stored.

4 Make sure that the permissions are set to 644.

5 Restart Tomcat.

Linux: `/etc/init.d/novell-tomcat5 restart`

Windows: Stop and start the Tomcat service from the control panel.

When a change is made to the `bcsLogin.conf` file, Tomcat must be restarted.

Creating a User Store for the Active Directory Domain

You need to either configure your Identity Server to use Active Directory as a user store or verify your existing configuration for your Active Directory user store.

1 In the Administration Console, click *Devices* > *Identity Servers* > *Edit*.

2 Click *Local* to view your user stores.

If you have already configured your Identity Server to use the Active Directory server, click its name.

If you haven't configured a user store for the Active Directory server, click *New*.

3 For a new user store, fill in the following fields. For an existing Active Directory user store, verify the values.

Name: Specify a name for the user store for reference.

Admin name: Specify the name of the administrator of the Active Directory server. Administrator-level rights are required for setting up a user store. This ensures read/write access to all objects used by Access Manager.

Directory Type: Select *Active Directory*.

Server replica: (Conditional) For a new Active Directory user store, click *New* to add a replica. Fill in the following fields:

- **Name:** Specify a name of the replica for reference. This can be the name of the Active Directory server.
- **IP Address:** Specify the IP address of the Active Directory server and the port you want the Identity Server to use when communicating with the Active Directory server.
- **Port:** Specify the port that the Active Directory server uses to communicate to the Identity Server. This communication occurs over LDAP. The default non-secure port is 389. The default secure port is 636.

Search Context: For a new user store, click *New* and specify the context of the administrator of the Active Directory server. For an existing user store, verify that you have an entry for the context of the administrator. Add a context if it is missing.

4 Click *OK* to save the changes.

Creating a Kerberos Authentication Class for the Identity Server

1 In the *Local* tab of the Identity Server, click *Classes* > *New*.

2 Fill in the following fields:

Display name: Specify a name to identify this class.

Java Class: Select *KerberosClass*.

3 Click *Next*.

4 Fill in the following fields:

Service Principal Name: Specify the value of the servicePrincipalName attribute of the Identity Server user. This is the user created in "Creating a User Account in Active Directory for the Identity Server" on page 34.

Kerberos Realm: Specify the name of the Kerberos realm. The default value for this realm is the domain name of the Active Directory server, entered in all uppercase. The value in this field is case sensitive.

JAAS config file for Kerberos: Specify the path to the `bcsLogin.conf` file. This is the created in "Creating the bcsLogin.conf File" on page 37.

Kerberos KDC: Specify the IP address of the Active Directory server.

User Attribute: Specify the attribute in the Identity Vault that contains the userPrincipalName from Active Directory. For example, the mail attribute in the Identity Vault can store the userPrincipalName from Active Directory.

If this attribute does not contain the userPrincipalName from Active Directory, the authentication to the Role Mapping Administrator fails.

5 Click *Finish* to save the authentication class.

Creating a Kerberos Method for the Identity Server

1. In the *Local* tab of the Identity Server, click *Method* > *New*.
2. Fill in the following fields:

   Display name: Specify a name to identify this method.

   Class: Select the Kerberos class created in "Creating a Kerberos Authentication Class for the Identity Server" on page 38.

   User stores: Move the user store for the Identity Vault to the list of *User stores*. This must be the Identity Vault user store, not the Active Directory user store.
3. Click *Finish* to save the method.

Creating a Kerberos Contract for the Identity Server

1. In the *Local* tab of the Identity Server, click *Contract* > *New*.
2. Fill in the following fields:

   Display name: Specify a name to identify this contract.

   URI: Specify a value that uniquely identifies the contract from all other contracts.

   The URI cannot begin with a slash, and it must uniquely identify the contract. For example: `kerberos/contract`

   Methods: From the list of available methods, move the Kerberos method, you created in "Creating a Kerberos Method for the Identity Server" on page 39 to the *Methods* list.
3. Click *Finish* to save the contract.

Verifying the Kerberos Configuration

To view the `catalina.out` (Linux) or the `stdout.log` (Windows) file of the Identity Server:

1. In the Administration Console, click *Auditing* > *General Logging*.
2. In the Identity Servers section, select the `catalina.out` or `stdout.log` file.
3. Download the file and open it in a text editor.
4. Search for Kerberos and verify that a subsequent line contains a `Commit Succeeded` phrase. For the configuration example, the lines look similar to the following:

   ```
   principal's key obtained from the keytab
   principal is HTTP/amser.provo.novell.com@AD.NOVELL.COM
   Added server's keyKerberos Principal HTTP/
   amser.provo.novell.com@AD.NOVELL.COMKey Version 3key EncryptionKey:
   keyType=3 keyBytes (hex dump)=0000: CB 0E 91 FB 7A 4C 64 FE

   [Krb5LoginModule] added Krb5Principal HTTP/
   amser.provo.novell.com@AD.NOVELL.COM to Subject
   Commit Succeeded
   ```
5. If the file does not contain any lines similar to these, verify that you have enabled logging. See "Enabling Logging for Kerberos Transactions" on page 36.
6. If the commit did not succeed, search backward in the file and verify the following values:
   - Service Principal Name
   - Name of the keytab file

For the example configuration, the file contains lines with text similar to the following:

```
Principal is HTTP/amser.provo.novell.com

KeyTab is /usr/lib/java/jre/lib/security/nidpkey.keytab
```

7 (Conditional) If you make any modifications to the configuration, either in the Administration Console or to the `bcsLogin file`, restart Tomcat on the Identity Server.

Creating a SAML Identity Injection Policy

You must create a SAML identity injection policy for Access Manager to use. This allows the authentication information in the Kerberos tickets to be passed to the Role Mapping Application.

1 In the Administration Console, click *Policies* > *Policies* > *Master_Container*.

The policy must reside in the master container.

2 Click *New* to create a new policy.

3 Specify a name to identify the policy.

4 For the policy type, select *Access Gateway: Identity Injection*.

5 Click *OK*.

6 Fill in the following fields to define the policy:

Description: Specify a description for the policy.

Priority: Leave the priority to the default level of 1.

Actions: Click *New* > *Inject into Authentication Header*.

- **User Name:** Select *Credential Profile*, then select *LDAP Credentials:LDAP User Name* for the user name.
- **Password:** Select Credential Profile, then select SAML Credentials:SAML Assertion.
- **Multi-Value Separator:** Leave the default separator as a comma.
- **DN Format:** Leave the default DN format as LDAP.

7 Click *OK* twice to save the policy.

Refreshing the Identity Server

In order for the changes to the Identity Server to take effect, you must refresh the Identity Server.

1 In the Administration Console, select *Devices* > *Identity Servers*.

2 Select your Identity Server, then click *Refresh*.

3 Click *Close*.

Creating a Protect Resource for the Role Mapping Administrator

You must configure the Role Mapping Administrator as a protected resource in the Access Gateway.

1 In the Administration Console, click *Devices* > *Access Gateways*, then click the name of your Access Gateway.

2 (Conditional) If you have a Proxy Service defined for the Role Mapping Administrator, skip to Step 3. Otherwise, complete the following steps to create the Proxy Service for the Role Mapping Administrator:

 2a Click *New* in the Proxy Service List.

 2b Fill in the following fields:

 Proxy Service Name: Specify a name to identify the Role Mapping Administrator as a Proxy Service.

 Multi-Homing Type: Select *Domain-Based*.

 Published DNS Name: Specify the DNS name for the Role Mapping Administrator server.

 Path: Specify the Role Mapping Administrator's application context. The default context is IDMRMAP. There should be two entries For example:

```
/*
```

```
/IDMRMAP/*
```

 Web Server IP Address: Specify the IP address of the Web server.

 Host Header: Select *Web Server Host Name* to publish the DNS name that the user sent in the request to be replaced by the DNS name of the Web server.

 Web Server Host Name: Specify the DNS name of the Web server.

 2c Click *OK* to create the Proxy Service for the Role Mapping Administrator.

3 Click the display name of the Role Mapping Administrator Proxy Service.

4 Click the *Protected Resources* tab, then click *New*.

5 Specify the name of the protected resource, then click *OK*.

6 Fill in the following fields on the *Overview* tab:

 Description: Specify a description for the protected resource.

 Contract: Select the Kerberos contract created in "Creating a Kerberos Contract for the Identity Server" on page 39.

 URL Path: Click the /* path, then define the application context for the Role Mapping Administrator. For example:

```
/* /IDMRMAP/*
```

7 Click the *Identity Injection* tab, then click *Manage Policies*.

8 Select the policy created in "Creating a SAML Identity Injection Policy" on page 40, then click *Apply Changes*.

9 Click *Close* to close the policies window.

10 Click *OK* twice to save the changes to the protected resource.

Refreshing the Access Gateway

In order for the changes for the protected resource to take affect, you must refresh the Access Gateway.

1 In the Administration Console, select *Devices* > *Access Gateways*.

2 Select your Access Gateway, then click *Refresh*.

3 Click *Close*.

6.2.4 Configuring the User's Web Browser

Each user's Web browser must be configured to trust the Access Manager Identity Server.

1 Add the computers of the users to the Active Directory domain.

For instructions, see your Active Directory documentation.

2 Log in to the Active Directory domain, rather than the machine.

3 Configure the Web browser to trust the Identity Server:

For Internet Explorer version 7: Click *Tools* > *Internet Options* > *Security* > *Local intranet* > *Sites* > *Advanced*. (For Internet Explorer version 6, click *Tools* > *Internet Options* > *Security* > *Trusted sites* > *Sites*.)

In the *Add this website to the zone* text box, specify the Base URL for the Identity Server, then click *Add*.

In the configuration example, this is `http://amser.provo.novell.com`.

Click *Close*.

For Firefox: In the *URL* field, specify `about:config`. In the *Filter* field, specify *network.n*. Double click `network.negotiate-auth.trusted-uris`.

This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser. Specify a comma-delimited list of trusted domains or URLs.

For this example configuration, you would add `http://amser.provo.novell.com` to the list.

If the deployed SPNEGO solution is using the advanced Kerberos feature of Credential Delegation, double-click `network.negotiate-auth.delegation-uris`. This preference lists the sites for which the browser can delegate user authorization to the server. Specify a comma-delimited list of trusted domains or URLs.

For this example configuration, you would add `http://amser.provo.novell.com` to the list.

4 Click *OK*. The configuration appears as updated.

Restart your Firefox browser to activate this configuration.

5 In the URL field, enter the base URL of the Identity Server with port and application. For this example configuration:

```
http://amser.provo.novell.com:8080/nidp
```

The Identity Server authenticates the user without prompting the user for authentication information.

Enabling Auditing

7

The Role Mapping Administrator can be enabled to audit specific events. Enabling auditing allows you to maintain a record of what changes where made, who made the changes, and when the changes occurred. Auditing requires that Sentinel™ be installed and configured to capture the events.

There are specific events that are audited. For a list of these events, see Appendix A, "Role Mapping Administrator Audit Events," on page 55.

Use the following checklist to verify that all of the steps are completed to configure the Role Mapping Administrator with Sentinel.

- □ Install and configure Sentinel. Sentinel should be installed on a separate server from the Identity Manager and Roles Based Provisioning Module. For more information, see the *Novell Sentinel Installation Guide* (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_installation_guide.pdf).
- □ Install and configure the Novell® Sentinel Identity Manager Collector. For more information, see "Installing and Configuring the Identity Manager Collector" in the *Identity Manager 3.6.1 Reporting Guide for Novell Sentinel*.
- □ Install and configure the Novell Audit Connector. For more information, see "Installing and Configuring the Identity Manager Collector" in the *Identity Manager 3.6.1 Reporting Guide for Novell Sentinel*.
- □ Modify the logging file `idmrmap_logging.xml` file. For more information, see Section 7.1, "Modifying the Logging File," on page 43.
- □ Install and configure the Platform Agent. The Platform Agent is the client piece of the auditing architecture. For more information, see Section 7.2, "Installing and Configuring the Platform Agent," on page 44.

7.1 Modifying the Logging File

The `idmrmap_logging.xml` file must have an auditing line uncommented to allow events to be logged to the Novell Audit Connector. Use the following steps to verify that the auditing list uncommented:

1. Open the file `/installation_directory/tomcat/conf/idmrmap_logging.xml`.
2. Find the following lines:

```
    <category additivity="true" name="com.novell">
    <priority value="INFO"/>
    <appender-ref ref="CONSOLE_DEBUG"/>
    <--! remove this line to turn on audit logging
    <appender-ref ref="Naudit"/>
    remove this line to turn on audit logging -->
  </category>
```

3. Remove `<--! remote this line to turn on audit logging` and `remove this line to turn on audit logging -->` lines to turn on auditing.
4. Save the file.

5 Restart the Role Mapping Administrator by:

- Execute the stop.sh script to stop the Role Mapping Administrator. The default location is /*installation_directory*/idmrmap/stop.sh.
- Execute the start.sh script to start the Role Mapping Administrator. The default location is /*installation_directory*/idmrmap/start.sh.

7.2 Installing and Configuring the Platform Agent

The Platform Agent communicates with the Novell Audit Connector. The Platform Agent allows the events from the Role Mapping Administrator to be audited by Sentinel. You must install and configure the Platform Agent for auditing to work.

If either eDirectory™ or Identity Manager are installed on the same server as the Role Mapping Administrator, then the Platform Agent might already be installed. Check to see if the /etc/logevent.conf file exists. If it does exist, then you don't need to install the Platform Agent. If the Platform Agent is installed, you might need to change the configuration of the Platform Agent.

If you don't have the Platform Agent installed, proceed to Section 7.2.1, "Installing the Platform Agent," on page 44. If you have the Platform Agent installed, proceed to Section 7.2.2, "Configuring the Platform Agent," on page 44 to verify your configuration is correct.

7.2.1 Installing the Platform Agent

1 Download the Novell Audit 2.0.2 Starter Pack for Linux from the Novell Product Download Web site (http://download.novell.com/Download?buildid=DC7JtDaQB5M~).

The file name is Novell_Audit_202_Starter_Linux.tar.gz.

2 Extract the Novell_Audit_202_Starter_Linux.tar.gz file on the Role Mapping Administrator server.

3 Log in as root, then run the pinstall.lin file in the /download_directory/Linux directory.

4 Read through the license agreement by pressing the Spacebar, then enter Y to accept the licence agreement.

5 Enter P to install the Platform Agent.

6 Press Enter to finish the installation.

7 Proceed with Section 7.2.2, "Configuring the Platform Agent," on page 44.

7.2.2 Configuring the Platform Agent

After the Platform Agent is installed, you must configure the logevent.conf file. This file contains the configuration settings for the Platform Agent. The file is stored in the /etc directory.

There is a sample logevent.conf file included in the Role Mapping Administrator installation directory. This file can be copied to the /etc directory or merged with an existing file. The sample file contains the minimum parameters. Other parameters that are not included in this file might be required for your environment. Table 7-1 on page 45 contains a list of all of the settings that can be used in the file.

1 As root, modify the /etc/logevent.conf file with the following minimum parameters:

```
LogHost=myserver.novell.com
LogJavaClassPath=/installation_directory/tomcat/naudit/NAuditPA.jar
LogCachePort=2881
LogCacheDir=/var/opt/novell/audit/auditcache
LogMaxBigData=8192
```

2 As `root`, create the `/var/opt/novell/audit` directory.

This directory might already exist. By default, the Platform Agent creates the cache files in the `/var/opt/novell/naudit/cache` directory and the `nproduct.log` file in the `/var/opt/novell/naudit/`directory. The cache files directory can be changed with the LogCacheDir parameter.

3 As `root`, change ownership of the `/var/opt/novell/audit` directory to the user that runs the Role Mapping Administrator. For example:

```
chown userid /var/opt/novell/audit
```

4 Execute the `stop.sh` script to stop the Role Mapping Administrator. The default location is `/`*`installation_directory`*`/idmrmap/stop.sh`.

5 Execute the `start.sh` script to start the Role Mapping Administrator. The default location is `/`*`installation_directory`*`/idmrmap/start.sh`.

Table 7-1 *logevent Settings*

Setting	Description
LogHost=*dns_name*	The hostname or IP address of the Event Source Server where the Platform Agent sends events. In an environment where the Platform Agent connects to multiple hosts—for example, to provide system redundancy—separate the IP address of each server with commas in the LogHost entry. For example, `LogHost=192.168.0.1,192.168.0.3,192.168.0.4` The Platform Agent connects to the servers in the order specified. If the first logging server goes down, the Platform Agent tries to connect to the second logging server, and so on.
LogCacheDir=*path*	The directory where the Platform Agent stores the cached event information if the Event Source Server becomes unavailable.
LogEnginePort=*port*	The port where the Platform Agent can connect to the Event Source Server. By default, this is port 289.

Setting	Description
LogCachePort=*port*	The port where the Platform Agent connects to the Logging Cache Module. If the connection between the Platform Agent and the Event Source Server fails, Identity Manager continues to log events to the local Platform Agent. The Platform Agent simply switches into Disconnected Cache mode; that is, it begins sending events to the Logging Cache module (`lcache`). The Logging Cache module writes the events to the Disconnected Mode Cache until the connection is restored. When the connection to the Event Source Server is restored, the Logging Cache Module transmits the cache files to the Event Source Server. To protect the integrity of the data store, the Event Source Server validates the authentication credentials in each cache file before logging its events. When running as a non-root user, the value must be greater than 1024.
LogCacheUnload=Y|N	Set the parameter to `N` to prevent `lcache` from being unloaded.
LogCacheSecure=Y|N	Set the parameter to `Y` to encrypt the local cache file.
LogReconnectInterval=*seconds*	The interval, in seconds, where the Platform Agent and the Platform Agent Cache try to reconnect to the Event Source Server if the connection is lost.
LogDebug=Never|Always	The Platform Agent debug setting. ◆ Set to `Never` to never log debug events. ◆ Set to `Always` to always log debug events.
LogSigned=Never|Always	The signature setting for Platform Agent events. **IMPORTANT:** Sentinel can receive and map Audit signatures to a Novell Sentinel event field; however, Novell Sentinel does not currently verify event signatures. ◆ Set it to `Never` to never sign or chain events. ◆ Set it to `Always` to always log events with a digital signature and to sequentially chain events.
LogMaxBigData=*bytes*	The maximum size of the event data field. The default value is 3072 bytes. Set this value to the maximum number of bytes the client allows. Data that exceeds the maximum is truncated or not sent if the application doesn't allow truncated events to be logged.
LogMaxCacheSize=*bytes*	The maximum size, in bytes, of the Platform Agent cache file.
LogCacheLimitAction=stop logging|drop cache	The action that you want the cache module to take when it reaches the maximum cache size limit. ◆ Set to `stop logging` if you want to stop collecting new events. ◆ Set to `drop cache` if you want to delete the cache and start over with any new events that are generated.

Setting	Description
LogJavaClassPath	The location of the `NAuditPA.jar` lcache file. It must be the Platform Agent `.jar` file included with the Role Mapping Administrator. The default location is: `/`*`installation_directory`*`/tomcat/naudit/NAuditPA.jar`

Security Best Practices

8

This section contains a description of potential security issues with the Role Mapping Administrator.

For additional information about securing your Identity Manager system, see the *Identity Manager 3.6 Security Guide*.

8.1 Tuning Session Timeouts

Web applications identify every user by a session. The session holds information about the user. An example is an Internet shopping cart. The content of the shopping cart is stored in a session. To prevent the number of sessions from increasing infinitely, they are destroyed after a certain time of inactivity from the user. This is a session timeout. When a session times out, all of the data stored in the session is gone.

If a session timeout is set too long, a user who forgets to log out leaves the session open for the next user who comes to the same computer. Reducing the session timeout reduces the chance of having two users use the same session.

To reduce a session timeout:

1 Locate the following section in the `tomcat_home/conf/web.xml` file:

```
<session-config>
   <session-timeout>30</session-timeout>
</session-config>
```

2 Specify the desired timeout value.

The timeout value is specified in minutes.

3 Save the file, then restart Tomcat to have the change take effect.

Troubleshooting

9

Refer to the following sections if you are having problems with the Role Mapping Administrator.

- Section 9.1, "Shutdown Port Conflict Error," on page 51
- Section 9.2, "Authentication Issues," on page 51
- Section 9.3, "Expected Roles Are Not Being Displayed," on page 52
- Section 9.4, "Expected Roles from the SAP Portal Are Not Being Displayed," on page 52
- Section 9.5, "Problems with Authorizations Being Displayed," on page 53

9.1 Shutdown Port Conflict Error

Problem

A Tomcat port conflict error occurs when you are starting the Role Mapping Administrator.

Solution

If you have the Role Mapping Administrator and the Roles Based Provisioning Module installed on the same server, the Tomcat shutdown ports conflict. To solve the problem:

1. Edit the `/installation_directory/idmrmap/tomcat/conf/server.xml` file.
2. Find the line `<Server port="8006" shutdown="SHUTDOWN">`.
3. Change the port to 8007 or another port that is not in uses.
4. Save the changes and restart the Role Mapping Administrator.

9.2 Authentication Issues

Problem

Failing to authenticate to the Role Mapping Administrator.

Solutions

Check the following items to correct the authentication problem. If the authentication issues continue, please contact your system administrator.

- The password is not correct.
- The username does not exist in the user store.
- There are multiple user accounts matching the specified username. Use the distinguished name (LDAP DN) instead of the common name (CN).
- There are network problems. The user's credentials are verified against the user store through an LDAP connection.
- The LDAP server is not communicating.

- If the eDirectory™ connection is using SSL, the certificate might have expired. Check with your system administrator to confirm whether the eDirectory certificate is valid.
- The user account you are using does not have sufficient rights in the Roles Based Provisioning Module. Check with your administrator to verify that you have sufficient rights to use the Role Mapping Administrator.

9.3 Expected Roles Are Not Being Displayed

Problem

Not all of the roles from the Roles Based Provisioning Module are being displayed, or too many roles are being displayed.

Solution

If a user belongs to the Role Module Administrator role in the Roles Based Provisioning Module, the Role Mapping Administrator uses the proxy admin credentials defined in the Role Mapping Administrator configuration. Verify the proxy admin user has the correct rights to the Identity Vault that contains the User Application driver.

9.4 Expected Roles from the SAP Portal Are Not Being Displayed

Problem

When loading authorizations from the SAP Portal system, groups that start with SAP_ are not being displayed.

Solution

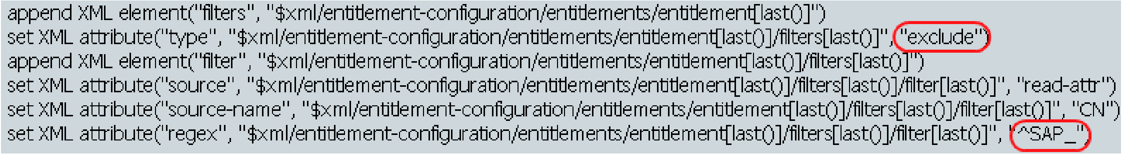
If the SAP Portal is using an ABAP server as the Authentication DataSource, then by default the UME cannot assign ABAP roles (which appear as groups in the SAP Portal) directly to ABAP users. Most of these ABAP roles begin with SAP_. The SAP Portal driver is configured to filter these roles when the Role Mapping Administrator queries for the available groups.

The filter is an XML filter element that is appended to the entitlement configuration object. By default, the filter element contains an attribute type that has a value of exclude. The filter element holds individual filters. Each filter contains the following attributes:

- **read-attr:** The source for the match.
- **source-name:** The attribute on which the regular expression is evaluated against.
- **regex:** The regular expression that is used.

You can modify the regular expression value or remove the value to change how the Role Mapping Administrator filters the results. By default, the regular expression is ^SAP_ which is evaluated as start with SAP underscore.

Figure 9-1 XML Filter Element



```
append XML element("filters", "$xml/entitlement-configuration/entitlements/entitlement[last()]")
set XML attribute("type", "$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()]", "exclude")
append XML element("filter", "$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()]")
set XML attribute("source", "$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()]/filter[last()]", "read-attr")
set XML attribute("source-name", "$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()]/filter[last()]", "CN")
set XML attribute("regex", "$xml/entitlement-configuration/entitlements/entitlement[last()]/filters[last()]/filter[last()]", "^SAP_")
```

To change the filter so you can see all groups:

1. Using Designer or iManager, edit the SAP Portal driver policy pub-its-InitEntitlementConfigurationResource on the Publisher channel.
2. In Policy Builder, select the Entitlements rule.
3. In the for each action, find the XML element of filter.
4. Change the type attribute value from exclude to include.
5. Remove the regular expression value of ^SAP_.
6. Save the changes, then restart the driver to have the changes take effect.

9.5 Problems with Authorizations Being Displayed

Problem

The authorizations were loaded, but they are not displayed in the Authorization panel.

Solution

Check the `idmrmap.log` file for more details. The `idmrmap.log` file is located in the `/installation_directory/idmrmap/tomcat/logs` directory. The driver might be reporting an error such as non-success query status. If this error occurs, the Role Mapping Administrator does not commit any authorizations that might have been queried. This indicates that the Remote Loader is not connecting to the host system.

Role Mapping Administrator Audit Events

A

The following sections contain the audit events logged for the Role Mapping Administrator, when you have auditing enabled for Identity Manager.

A.1 Event ID 00031550

Tracks when a some logs in to the application successfully.

Fields	Values
Event ID	00031550
Description	Login_Success
Originator (B) Title	Login ID
Target (U) Title	Target DN
Subtarget (V) Title	
Text1 (S) Title	Message
Text2 (T) Title	Client IP
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	

Fields	Values
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	
Data Type	
Display Schema	[[$rC] [$SO]: $SB successfully logged in from $ST. \n

A.2 Event ID 00031551

Tracks all log in failures.

Fields	Values
Event ID	00031551
Description	Login_Failure
Originator (B) Title	Login ID
Target (U) Title	Target DN
Subtarget (V) Title	
Text1 (S) Title	Message
Text2 (T) Title	Client IP
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	
Data Type	
Display Schema	[$rC] [$SO]: $SB failed to log in from $ST. \n

A.3 Event ID 00031630

Tracks when a role is created successfully.

Fields	Values
Event ID	00031630
Description	Create_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU\n

A.4 Event ID 00031631

Tracks when the creation of a role fails.

Fields	Values
Event ID	00031631
Description	Create_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	

Fields	Values
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU; Error Message: $SF\n

A.5 Event ID 00031632

Tracks when a role is successfully deleted.

Fields	Values
Event ID	00031632
Description	Delete_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	

Fields	Values
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU\n

A.6 Event ID 00031633

Tracks when a role deletion fails.

Fields	Values
Event ID	000316333
Description	Delete_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU; Error Message: $SF\n

A.7 Event ID 00031634

Tracks when a role is successfully modified.

Fields	Values
Event ID	000316334
Description	Modify_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU\n

A.8 Event ID 000361635

Tracks each modify event that fails.

Fields	Values
Event ID	000316335
Description	Modify_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message

Fields	Values
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] [$SO]: Initiated by $SB; Role DN: $SU; Error Message: $SF\n

A.9 Event ID 00031636

Tracks when a role is successfully mapped.

Fields	Values
Event ID	000316336
Description	Map_Authorization_Role_Add_Success
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	Entitlement DN
Text2 (T) Title	Entitlement Parameter
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object

Fields	Values
Data Type	S
Display Schema	[$rC] Authorization: Entitlement: $SS Parameter: [$ST} [$SO]: Initiated by $SB; Role DN: $SU\n

A.10 Event ID 00031637

Tracks when a role mapping fails.

Fields	Values
Event ID	000316337
Description	Map_Authorization_Role_Add_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	Entitlement DN
Text2 (T) Title	Entitlement Parameter
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] Authorization: Entitlement: $SS Parameter: [$ST} [$SO]: Initiated by $SB; Role DN: $SU; Error Message: $SF\n

A.11 Event ID 00031638

Tracks when a role mapping is successfully removed.

Fields	Values
Event ID	000316338

Fields	Values
Description	Map_Authorization_Role_Remove_Success
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	Entitlement DN
Text2 (T) Title	Entitlement Parameter
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] Authorization: Entitlement: $SS Parameter: [$ST} [$SO]: Initiated by $SB; Role DN: $SU\n

A.12 Event ID 00031639

Tracks when removal of a role mapping fails.

Fields	Values
Event ID	000316339
Description	Map_Authorization_Role_Add_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	Entitlement DN
Text2 (T) Title	Entitlement Parameter
Text3 (F) Title	
Value1 (1) Title	

Fields	Values
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[$rC] Authorization: Entitlement: $SS Parameter: [$ST} [$SO]: Initiated by $SB; Role DN: $SU; Error Message: $SF\n