

Role Mapping Administrator Installation and Configuration Guide Identity Manager 4.0.2

June 2012

Novell.

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 \(http://www.novell.com/info/exports/\)](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.

Copyright © 2007-2012 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	5
1 Overview	7
1.1 How Role Mapping Works	7
1.2 Role Mapping Administrator	9
1.3 Identity Vault Access	9
1.4 System Access	10
1.5 Authentication	10
1.6 Authorization	10
1.7 Database	11
1.8 Role Management	11
2 Meeting Prerequisites and System Requirements	13
2.1 Prerequisites	13
2.2 System Requirements	13
2.3 Installing the iManager Plug-Ins for Identity Manager 4.0.2	14
2.4 Granting Rights to the Role Mapping Administrator	15
2.4.1 Identity Vault Rights for Administration	15
2.4.2 Roles Based Provisioning Module Assignments for Administration	16
2.4.3 Required Rights for the Role Mapping Administrator	16
3 Installing the Role Mapping Administrator	17
3.1 Installing the Role Mapping Administrator	17
3.2 Installing the Role Mapping Administrator in Silent Mode	18
3.3 Reconfiguring the Role Mapping Administrator	18
3.3.1 Changing the Port Number	19
3.3.2 Changing the Password	19
4 Configuring the Application	21
4.1 Providing Identity Vault Connection Information	21
4.2 Configuring the Drivers	23
4.3 Loading Authorizations into the Database	24
4.4 Enabling SSL	24
4.4.1 Enabling an SSL Connection from the Role Mapping Administrator to the Identity Vault	25
4.4.2 Enabling SSL for a Browser to Access the Role Mapping Administrator	26
4.5 Configuring the Role Mapping Administrator for Automatic Startup	26
4.5.1 Linux	26
4.5.2 Windows	26
4.6 Changing the Java Heap Size	27

5	Changing the Configuration	29
6	Configuring Authentication	31
6.1	Configuring Single Sign-On Through the Roles Based Provisioning Module	31
6.1.1	Enabling the Roles Based Provisioning Module for Single Sign-On	31
6.1.2	Creating a Shared Page	32
6.1.3	Assigning Permissions.	32
6.1.4	Selecting Content	32
6.2	Configuring Single Sign-On Through Access Manager	33
6.2.1	Prerequisites	34
6.2.2	Configuring Active Directory to Assign Kerberos Tickets	34
6.2.3	Configuring the Access Manager Identity Server to Consume the Kerberos Tickets	36
6.2.4	Configuring the User's Web Browser.	41
7	Enabling Auditing	43
7.1	Configuring the Role Mapping Administrator Auditing	43
7.1.1	Default Values of Role Mapping Administrator Auditing Configuration	43
7.1.2	Examples of Role Mapping Administrator Auditing Configuration	44
8	Security Best Practices	45
8.1	Tuning Session Timeouts.	45
A	Role Mapping Administrator Audit Events	47
A.1	Event ID 00031550	47
A.2	Event ID 00031551	48
A.3	Event ID 00031630	49
A.4	Event ID 00031631	49
A.5	Event ID 00031632	50
A.6	Event ID 00031633	51
A.7	Event ID 00031634	52
A.8	Event ID 000361635	52
A.9	Event ID 00031670	53
A.10	Event ID 00031671	54
A.11	Event ID 00031674	55
A.12	Event ID 00031675	55
A.13	Event ID 00031676	56
A.14	Event ID 00031677	57
A.15	Event ID 0003167A	57
A.16	Event ID 0003167B	58

About This Guide

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

Installation Information:

- ♦ [Chapter 1, “Overview,” on page 7](#)
- ♦ [Chapter 2, “Meeting Prerequisites and System Requirements,” on page 13](#)
- ♦ [Chapter 3, “Installing the Role Mapping Administrator,” on page 17](#)

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 45](#)

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 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 [Identity Manager 4.0.2 Documentation Web site \(http://www.novell.com/documentation/idm402\)](http://www.novell.com/documentation/idm402).

Additional Documentation

For documentation on the Novell Compliance Management Platform, see the [Novell Compliance Management Platform Documentation Web site \(http://www.novell.com/documentation/ncmp10/index.html\)](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 4.0.2 Documentation Web site \(http://www.novell.com/documentation/idmrbpm402/index.html\)](http://www.novell.com/documentation/idmrbpm402/index.html).

For documentation on the SAP drivers, see the [Identity Manager 4.0.2 Drivers Documentation Web site \(http://www.novell.com/documentation/idm402drivers/index.html\)](http://www.novell.com/documentation/idm402drivers/index.html).

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

For documentation on Sentinel, see the [Sentinel 6.1 Documentation Web site \(http://www.novell.com/documentation/sentinel61/index.html\)](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 \(http://support.novell.com/products/sentinel/secure/sentinel61.html\)](http://support.novell.com/products/sentinel/secure/sentinel61.html).

1 Overview

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.

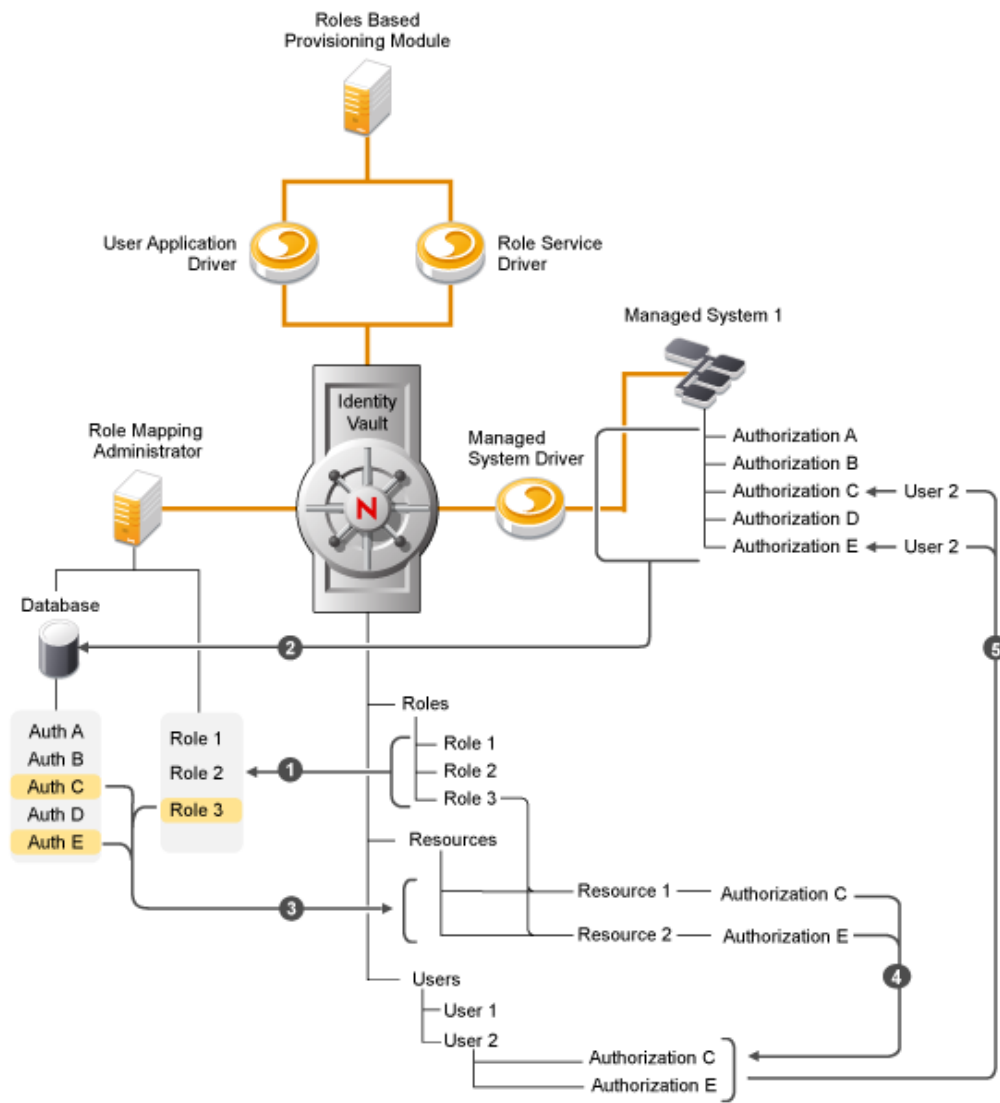
The following sections provide information you should understand before installing and configuring the Role Mapping Administrator:

- ♦ [Section 1.1, “How Role Mapping Works,” on page 7](#)
- ♦ [Section 1.2, “Role Mapping Administrator,” on page 9](#)
- ♦ [Section 1.3, “Identity Vault Access,” on page 9](#)
- ♦ [Section 1.4, “System Access,” on page 10](#)
- ♦ [Section 1.5, “Authentication,” on page 10](#)
- ♦ [Section 1.6, “Authorization,” on page 10](#)
- ♦ [Section 1.7, “Database,” on page 11](#)
- ♦ [Section 1.8, “Role Management,” on page 11](#)

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 role mapping process is explained in [Figure 1-1](#).

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 managed system authorizations by using the managed system driver to query the managed systems. The retrieved managed system 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, a resource is created and updated to reflect the authorization mapping. The role is updated in the Identity Vault to map to the newly created resource.

IMPORTANT: In earlier version of Role Mapping Administrator, roles were mapped directly to the authorizations. With this release onwards, resources are introduced. Roles are mapped to resources that are in turn are mapped to authorizations. When you create a mapping between a role and an entitlement/authorization, resources are automatically created in the Role Mapping Administrator.

Resources provide the ability for end users to request provisioning of authorizations for themselves or for users that they have a relationship with. With Role Mapping Administrator 1.0, users could not understand what they requested or the status of what they had requested. Providing an interface that conveys this information is critical to the success of the product. Resources provide the ability for administrators to gain better control over the management of user access to entitlements/authorizations, ensuring that the right people have the right access to the right resources.

4. A user is assigned the role in the Roles Based Provisioning Module, at which point the Role Service driver grants the user an authorization to all managed system authorizations that are mapped to the role.
5. The managed system driver responds to the entitlement grant by initiating the authorization assignment in the managed 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 13](#) 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. The users should have both Resource Administrator and Role Administrator roles.
- ♦ Retrieving roles information to display if the authenticated user is a Role Module Administrator. If the authenticated user is a Role Manager, the Role Mapping Administrator uses the user’s credentials to display roles.
- ♦ Creating resources with the selected authorization/entitlement and mapping them with the Identity Vault role.
- ♦ Accessing information stored on the Identity Manager driver object to build the queries required to retrieve authorizations from managed systems.
- ♦ Sending the queries to the Identity Manager drivers.
- ♦ Creating, editing, and deleting roles.

For more information, see [Section 2.4, “Granting Rights to the Role Mapping Administrator,” on page 15](#).

IMPORTANT: Because no warnings are displayed in the user interface, you must not perform any modifications on the mappings unless you are sure about what you are doing.

1.4 System Access

The Role Mapping Administrator does not require direct access to the managed 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 13.

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 both Resource Administrators and Role Administrators 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 Administrators, Role Managers, Resource Administrators, and Resource 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:

Table 1-1 Allowed Operations for Various Roles in RMA

Role	Allowed Operation in RMA
roleAdministrator, resourceAdministrator	Unrestricted access. <ul style="list-style-type: none">◆ Create mappings◆ Edit mappings◆ Delete mappings
roleAdministrator, resourceManager	Restricted access
roleManager, resourceAdministrator	Restricted access
roleManager, resourceManager	Restricted access

NOTE: Restricted access means read-only access to roles and mappings in Role Mapping Administrator.

For information, see [Section 2.4, “Granting Rights to the Role Mapping Administrator,”](#) on page 15.

1.7 Database

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

The managed system authorizations must be manually loaded into the database. You can select which authorizations 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 managed 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 you create a new role, you can add the role to the correct category, give it a level location, and assign owners.

2 Meeting Prerequisites and System Requirements

- ♦ Section 2.1, “Prerequisites,” on page 13
- ♦ Section 2.2, “System Requirements,” on page 13
- ♦ Section 2.3, “Installing the iManager Plug-Ins for Identity Manager 4.0.2,” on page 14
- ♦ Section 2.4, “Granting Rights to the Role Mapping Administrator,” on page 15

2.1 Prerequisites

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

- Install and configure Identity Manager 4.0.2. For more information, see the *Identity Manager 4.0.2 Installation Guide* (http://www.novell.com/documentation/idm402/idm_install/index.html?page=/documentation/idm402/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/idmrbpm402/install/data/bcy2k2j.html>).
- You must have updated iManager plug-ins and an updated Designer in order to manage these new drivers.
 - ♦ Install Designer 4.0.2
 - ♦ Install the iManager plug-ins for Identity Manager 4.0.2
- Install and configure the supported Identity Manager drivers. You can have one or more of each supported driver.

Only the Identity Manager 3.6.1, 4.0, or later drivers are supported. They can run on Identity Manager 3.6, 3.6.1, or 4.0 or later. For installation instructions, see these guides at *Identity Manager 3.6.1 Drivers* (<http://www.novell.com/documentation/idm361drivers/>) and *Identity Manager 4.0.2 Drivers* (<http://www.novell.com/documentation/idm402drivers/>).
- Grant users sufficient rights to use the Role Mapping Administrator, so they can log in and use the application. For instructions, see Section 2.4, “Granting Rights to the Role Mapping Administrator,” on page 15.
- Resources will be created with the selected authorization/entitlement and mapped to the role


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 SP3 32 and 64-bit, SUSE Linux Enterprise Server 11 32 and 64-bit, Windows Server 2003 SP2 32-bit, or Windows 2008 R2 64-bit, Red Hat Enterprise Linux 5.4 32 and 64-bit
Web Browser	Microsoft Internet Explorer 7, 8, and 9 Mozilla Firefox 3.5, Firefox 3.6.x, and Firefox 5.x
Java	Sun JRE 1.6

2.3 Installing the iManager Plug-Ins for Identity Manager 4.0.2

In order to manage drivers with structured GCVs, you must install the iManager plug-ins for Identity Manager 4.0.2.

- 1 Launch iManager and log in as an administrative user.
- 2 On the toolbar, click the *Configure* icon .
- 3 Click *Plug-in Installation > Available Novell Plug-in Modules*.
- 4 Select *Novell Identity Manager Plug-ins for 4.0*, then click *Install*.
- 5 Select *I Agree* in the license agreement, then click *OK*.
- 6 After the installation finishes, 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 4.0.2 are not in the list, download the Identity Manager 4.0 plug-ins for iManager 2.7 from the [Novell product download Web site \(http://download.novell.com\)](http://download.novell.com) to your iManager server.
- 2 Launch iManager and log in as an administrative user.
- 3 On 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 finishes, click *Close* twice.
- 8 Log out of iManager and restart Tomcat to have the changes take effect.

2.4 Granting Rights to the 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 2.4.1, “Identity Vault Rights for Administration,” on page 15](#)
- ♦ [Section 2.4.2, “Roles Based Provisioning Module Assignments for Administration,” on page 16](#)
- ♦ [Section 2.4.3, “Required Rights for the Role Mapping Administrator,” on page 16](#)

2.4.1 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 Discovery 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, ResourceDefs.RoleConfig.AppConfig and ResourceAssociations.RoleConfig.AppConfig containers within the UAD. All role and resource 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* on 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.

2.4.2 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, *Role Administrator* role, *Resource Manager* role, and the *Resource 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.

2.4.3 Required Rights for the Role Mapping Administrator

Users 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 his or her rights in the Identity Vault as well.

3 Installing the Role Mapping Administrator

The Role Mapping Administrator can be installed as root or through a silent installation.

- ♦ [Section 3.1, “Installing the Role Mapping Administrator,” on page 17](#)
- ♦ [Section 3.2, “Installing the Role Mapping Administrator in Silent Mode,” on page 18](#)
- ♦ [Section 3.3, “Reconfiguring the Role Mapping Administrator,” on page 18](#)

3.1 Installing the Role Mapping Administrator

To install the Role Mapping Administrator:

- 1 Locate the Role Mapping Administrator installation file on the Identity Manager media located here:
 - ♦ **Windows:** `IDM4.0.2_Win:\products\RMA\IDMRMAP.jar`
 - ♦ **Linux:** `IDM4.0.2_Lin/products/RMA/IDMRMAP.jar`
- 2 From a command line access Role Mapping Administrator installation directory, then enter `java -jar IDMRMAP.jar`.

NOTE: For security reasons, it is recommended to install the Role Mapping Administrator as a nonroot user, on Linux.

- 3 Enter `Yes` to accept the license agreement.
- 4 Specify the installation directory for the Role Mapping Administrator. The default path is your current location.
- 5 Specify the portion of the URL representing the Role Impinging Administrator name. The default value is `IDMRMAP`.
- 6 Specify the HTTP port. The default value is `8081`.
- 7 Specify a password for the configuration administrator.

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

- ♦ **Windows:** The start script is `start.bat` and the stop script is `stop.bat`.
- ♦ **Linux:** The start script is `start.sh` and the stop script is `stop.sh`.

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](#).

NOTE: You should not install the Role Mapping Administrator as `root` for security considerations.

3.2 Installing the Role Mapping Administrator in Silent Mode

The Role Mapping Administrator can be installed silently without human intervention. Use the following command to configure the unattended installation, including the install location, port configuration, Role Mapping Administrator administration configuration password, and so on.

```
java -jar IDMRMAP.jar [-h] [-s] [-i <install path>] [-p <port>] [-w <password>] [-n <name>] [-l <log path>]
```

where `[-s]` specifies silent installation.

Table 3-1 Silent Installation CLI Arguments

Argument	Description
<code>-h</code>	Displays help.
<code>-i</code>	Specifies the installation location.
<code>-l <log directory></code>	Specifies the Role Mapping Administrator installation log file location, <code>rma-install.log</code> . By default, the log file is located in the installation directory.
<code>-n <name></code>	Specifies the Role Mapping Administrator application name. The default name is <code>IDMRMAP</code> .
<code>-p <port></code>	Specifies the Role Mapping Administrator HTTP port number. The default port is <code>8081</code> .
<code>-s</code>	<code>-i</code> is a mandatory argument for silent installation. It performs the silent installation.
<code>-w <password> <env:VAR></code>	Specifies the Role Mapping Administrator administration configuration password. The password can be passed in clear text or through a user defined environment variable. The installer reads the password from the environment variable. Example 1: <code>-w mypassword</code> , The user password is <code>mypassword</code> . Example 2: <code>-w env:RMA_PASSWD</code> The installer reads the password from the <code>RMA_PASSWD</code> environment variable. <ul style="list-style-type: none">◆ On Windows, run the <code>set RMA_PASSWD=novell</code> command.◆ On Linux, run the <code>export RMA_PASSWD=novell</code> command.

If the silent installation arguments are not passed, default values are assumed.

3.3 Reconfiguring the Role Mapping Administrator

- ◆ [Section 3.3.1, “Changing the Port Number,” on page 19](#)
- ◆ [Section 3.3.2, “Changing the Password,” on page 19](#)

3.3.1 Changing the Port Number

You can change the Role Mapping Administrator port numbers by editing the following entries in the `<rma_install_path>/rma/tomcat/conf/server.xml` file.

- ◆ Replace 8081 and 8443 port numbers with the new port numbers in the following entries for the HTTP service.

```
<Connector port="8081" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

- ◆ Replace the 8006 port number with the new port number used to shut down the Tomcat service.

```
<Server port="8006" shutdown="SHUTDOWN">
```

These port numbers can be changed when port numbers are in use.

3.3.2 Changing the Password

The Role Mapping Administrator admin password can be set through the command line interface during the installation program either through the password prompt or by passing it with `-w password|env:ENV_VAR` command line argument. You can also set it through the Web portal.

If a password has not been set through the command line interface during installation, you can set it through the Web portal.

- 1 Start the Role Mapping Administrator by executing `<rma_install_path>/rma/start.sh` or `<rma_install_path>\rma\start.bat` command relevant to your platform.
- 2 When the Role Mapping Administrator Web portal is launched with `http://localhost:8081`, set the Role Mapping Administrator administrator password. If the password has not been set through the command line interface during the installation program, there is no change in the behavior and you can see the administrator login page.



Enter the admin password. The Role Mapping Administrator admin password is set when the text string in the *Administrator Password* and *Confirm Password* fields match.

- 3 Click OK. You are again prompted to enter the admin password.



4 Configuring the Application

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 managed system authorizations into the Role Mapping Administrator database so that the application is ready to use.

- ♦ [Section 4.1, “Providing Identity Vault Connection Information,” on page 21](#)
- ♦ [Section 4.2, “Configuring the Drivers,” on page 23](#)
- ♦ [Section 4.3, “Loading Authorizations into the Database,” on page 24](#)
- ♦ [Section 4.4, “Enabling SSL,” on page 24](#)
- ♦ [Section 4.5, “Configuring the Role Mapping Administrator for Automatic Startup,” on page 26](#)
- ♦ [Section 4.6, “Changing the Java Heap Size,” on page 27](#)

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.

Novell® Role Mapping Administrator
Administrator Configuration

Logout HELP

Login To Role Mapping Administrator * Required

Current Active Profile: None

System Configuration 199.99.90.199

Profile Name:*

Active Status

Role Vault Address:* 199.99.99.99

Role Vault Port:* 389

Use SSL

Admin. DN:* cn=admin,ou=sa,o=system

Admin. Password:*

Root User Container:* ou=sa,o=data

User App. Driver DN:* cn=User Application Driver,cn=driverset1,o=system

Driver Discovery DN:

Access Manager

Logout URL:

User Application REST API URL: http://localhost:8180/RIS

Roles and Authorizations Database

Reset database clears out previous authorizations that have been loaded from IDM connected system(s). After a database reset is performed, reloading of authorizations in the application is required.

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 4.4.1, “Enabling an SSL Connection from the Role Mapping Administrator to the Identity Vault,”](#) 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 allows for simultaneous logout from the Role Mapping Administrator and Access Manager. Having a value in this field does not enable this behavior. For more information, see [Chapter 6, “Configuring Authentication,” on page 31](#).

User Application REST API URL: (Optional) Specify the URL for the User Application REST API. The Role Mapping Administrator uses the REST API to trigger synchronization of authorizations between the RBPM and the managed system.

- 4 Click *Save*.

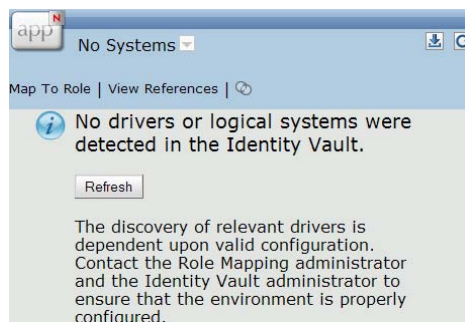
NOTE: To add multiple profiles, click the *Add a Configuration Profile*  button. To remove any profile, click the *Delete Configuration Profile*  button.

- 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 configuration to populate the authorizations. If the drivers are not configured, 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*



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

- The Identity Manager drivers are supported for the Role Mapping Administrator.

- ❑ 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 4.0.2 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 managed 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 managed systems authorizations are loaded, and you can control which types of authorizations are loaded.

- 1 In the Authorizations panel, click the *Load Authorizations*  icon to display the load authorizations dialog box.
- 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 managed systems. The time required to retrieve and load the authorizations depends on the number of managed systems you selected and the number of authorizations contained in each system.

You can change the load authorization timeout setting in the `web.xml` file. On Linux platforms, the `web.xml` file is located in the `/opt/novell/idm/rma/tomcat/webapps/IDMRMAP/WEB-INF` directory. On Windows, the file is in the

`<rma_install_path>\rma\tomcat\webapps\IDMRMAP\WEB-INF` directory.

4.4 Enabling SSL

There are two different components that must be configured to enable SSL and 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 25](#)
- ♦ [Section 4.4.2, “Enabling SSL for a Browser to Access the Role Mapping Administrator,” on page 26](#)

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.

- 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. Ensure that you set the `JAVA_HOME` environmental variable to the Java `install` directory and include `$JAVA_HOME/bin/` in the `PATH` environmental variable.

- 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)" (<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 \(http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html\)](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/server.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

- [Section 4.5.1, "Linux," on page 26](#)
- [Section 4.5.2, "Windows," on page 26](#)

4.5.1 Linux

The Role Mapping Administrator service automatically starts and stops during reboot through the `/etc/init.d/rma_init` script. This init script is only installed for the `root` user and is executed during the runlevels 3 and 5.

```
# /etc/init.d/rma_init start
```

```
# /etc/init.d/rma_init stop
```

This script is also present in the `<rma_install_location>/rma_init` install location for both `root` and non `root` user installations.

4.5.2 Windows

To start the Role Mapping Administrator as an automated service, do these steps:

- 1 Follow the steps mentioned under [How To Create a User-Defined Service \(http://support.microsoft.com/kb/137890\)](http://support.microsoft.com/kb/137890).
- 2 The resource kit necessary for creating a user defined service is available at [Windows Server 2003 Resource Kit Tools \(http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd\)](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd).

4.6 Changing 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/idmrmmap/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=idmrmmap_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 the file.
- 5 Restart the Role Mapping Administrator by 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 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 `<rma-install-path>/rma/stop.sh` or `<rma-install-path>/rma/stop.bat` depending on your platform.
- 2 Delete the installation directory. The default location is `<rma-install-path>/rma/`.
 - ♦ **Linux:** Run `<rma_installed_path>/rma-uninstall.sh [-h] [-s]`
 - ♦ **Windows:** Run `<rma_installed_path>/rma-uninstall.bat [-h] [-s]`
 - ♦ `-h`: Specifies help.
 - ♦ `-s`: Specifies silent mode.

Uninstalling the Role Mapping Administrator deletes all the data from the Role Mapping Administrator installation location.

- 3 Delete the installation log that contains the parameters specified during the installation. The default location is:
`<rma-install-path>/rma-install.log`
- 4 Reinstall the Role Mapping Administrator with new values. For installation instructions, see [Chapter 3, “Installing the Role Mapping Administrator,”](#) on page 17.

6 Configuring Authentication

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/login`

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 `userPrincipalName` of the Active Directory user from the ticket.
3. Access Manager maps the `userPrincipalName` (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 41

6.2.1 Prerequisites

- Install and configure Access Manager 3.1 or later. For more information, see *Novell Access Manager 3.1 SP2 Installation Guide* (<http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html>).
- Make sure that time is synchronized among the Access Manager Identity server, the Role Mapping Administrator, and the Identity Vault.
- Add a DNS 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 log 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 servicePrincipalNames on the user object.

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

- 2a At a command line, enter:

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

- 2b At a command line, enter:

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

- 3 Export the keytab file by using the ktpass utility.

```
ktpass /out nidp.keytab /princ HTTP://amsvr.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 36](#)
- ♦ [“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 38](#)
- ♦ [“Creating a Kerberos Contract for the Identity Server” on page 38](#)
- ♦ [“Verifying the Kerberos Configuration” on page 39](#)
- ♦ [“Creating a SAML Identity Injection Policy” on page 39](#)
- ♦ [“Refreshing the Identity Server” on page 40](#)
- ♦ [“Creating a Protected 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 SUSE Linux Enterprise Server (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 created in [“Creating the bcsLogin.conf File” on page 36](#).

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 38](#) 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 Protected 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 38.
 - 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 39, 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 and later: 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.

7 Enabling Auditing

The Role Mapping Administrator can be enabled to audit specific events. Enabling auditing allows you to maintain a record of what changes were made, who made the changes, and when the changes occurred. Auditing requires that the Event Auditing System 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 47.

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

- Install and configure the Event Auditing System. For more information, see the [Identity Manager Reporting Guide](http://www.novell.com/documentation/idm40/pdfdoc/reporting.pdf) (<http://www.novell.com/documentation/idm40/pdfdoc/reporting.pdf>).
- Configure the Role Mapping Administrator auditing by using the `rmaConfig.jar` file. For more information, see [Section 7.1, “Configuring the Role Mapping Administrator Auditing,”](#) on page 43.

7.1 Configuring the Role Mapping Administrator Auditing

The `rmaConfig.jar` file is used to configure the Role Mapping Administrator. By default, the Role Mapping Administrator auditing is disabled if you install Role Mapping Administrator as a standalone component. The `rmaConfig.jar` file is located in the `<RMA Install Location>/rma/` directory. Use the `rmaConfig.jar` file as follows:

```
java -jar rmaConfig.jar [-h] [+N] [-N] [-S] [+S[,parameters]]
```

Table 7-1 The `rmaConfig.jar` File Options

Option	Description
-h	Displays help.
-N	Disables nAudit.
+N	Enables nAudit.
-S	Disables Syslog auditing.
+S,[@hostname[:port]],[protocol]	Enables Syslog auditing.

7.1.1 Default Values of Role Mapping Administrator Auditing Configuration

The following default values are used:

- ◆ hostname = localhost

- ♦ port = 1514
- ♦ protocol = udp

Other valid protocols are TCP and SSL.

For the SSL protocol, the Keystore file and the corresponding password must be passed in the below format:

```
ssl: [keyStoreFile] : [keyStorePasswd]
```

7.1.2 Examples of Role Mapping Administrator Auditing Configuration

To enable nAudit, run the following command:

```
java -jar rmaConfig.jar +N
```

To enable syslog auditing through 192.168.1.1 host address at 1520 port over SSL with the corresponding key file and password, run the following command:

```
java -jar rmaConfig.jar +S,@192.168.1.1:1520,/etc/ssl/mykey.cer,keypass
```

To disable syslog auditing, run the following command:

```
java -jar rmaConfig.jar -S
```

8 Security Best Practices

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 4.0.2 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.

A Role Mapping Administrator Audit Events

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

- ♦ [Section A.1, “Event ID 00031550,” on page 47](#)
- ♦ [Section A.2, “Event ID 00031551,” on page 48](#)
- ♦ [Section A.3, “Event ID 00031630,” on page 49](#)
- ♦ [Section A.4, “Event ID 00031631,” on page 49](#)
- ♦ [Section A.5, “Event ID 00031632,” on page 50](#)
- ♦ [Section A.6, “Event ID 00031633,” on page 51](#)
- ♦ [Section A.7, “Event ID 00031634,” on page 52](#)
- ♦ [Section A.8, “Event ID 000361635,” on page 52](#)
- ♦ [Section A.9, “Event ID 00031670,” on page 53](#)
- ♦ [Section A.10, “Event ID 00031671,” on page 54](#)
- ♦ [Section A.11, “Event ID 00031674,” on page 55](#)
- ♦ [Section A.12, “Event ID 00031675,” on page 55](#)
- ♦ [Section A.13, “Event ID 00031676,” on page 56](#)
- ♦ [Section A.14, “Event ID 00031677,” on page 57](#)
- ♦ [Section A.15, “Event ID 0003167A,” on page 57](#)
- ♦ [Section A.16, “Event ID 0003167B,” on page 58](#)

A.1 Event ID 00031550

Tracks when someone 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

Fields	Values
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} successfully logged in from \${ST}. \n

A.2 Event ID 00031551

Tracks all login 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	

Fields	Values
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 successfully created.

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	
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	

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] [\$SO]: Initiated by \$SB; Role DN: \$SU\n

A.6 Event ID 00031633

Tracks when a role deletion fails.

Fields	Values
Event ID	00031633
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

Fields	Values
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	00031634
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	000361635
Description	Modify_Role_Failure
Originator (B) Title	Initiator ID

Fields	Values
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.9 Event ID 00031670

Tracks each resource that is created.

Fields	Values
Event ID	00031670
Description	Create_Resource
Originator (B) Title	Initiator ID
Target (U) Title	Resource DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
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	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU

A.10 Event ID 00031671

Tracks each failure event during the creation of a resource.

Fields	Values
Event ID	00031671
Description	Create_Resource_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource 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	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU; Error Message: \$SF

A.11 Event ID 00031674

Tracks the event when a resource is modified.

Fields	Values
Event ID	00031674
Description	Modify_Resource
Originator (B) Title	Initiator ID
Target (U) Title	Resource 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	Resource Object
Data Type	S
Display Schema	\$\$SB; Resource DN: \$\$SU

A.12 Event ID 00031675

Tracks the failure detected during the modification of a resource.

Fields	Values
Event ID	00031675
Description	Modify_Resource_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource 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	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU; Error Message: \$SF

A.13 Event ID 00031676

Tracks when a resource association is created.

Fields	Values
Event ID	00031676
Description	Create_Resource_Association
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association 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	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU

A.14 Event ID 00031677

Tracks when a resource association fails.

Fields	Values
Event ID	00031677
Description	Create_Resource_Association_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association 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	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU; Error Message: \$SF

A.15 Event ID 0003167A

Tracks when a resource association is modified.

Fields	Values
Event ID	0003167A
Description	Modify_Resource_Association
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association 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	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU

A.16 Event ID 0003167B

Tracks failure detected during the modification of a resource association.

Fields	Values
Event ID	0003167B
Description	Modify_Resource_Association_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
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	Resource Association Object
Data Type	S
Display Schema	\$\$B; Resource Association DN: \$\$U; Error Message: \$\$F
