

Driver for SAP* GRC Access Control Implementation Guide

Novell® Identity Manager

3.6.1

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 \(http://www.novell.com/info/exports/\)](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 © 2009 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., 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 \(http://www.novell.com/company/legal/patents/\)](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 \(http://www.novell.com/documentation\)](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	7
1 Overview	9
1.1 Terminology	9
1.2 How It Works	9
1.2.1 Subscriber Channel	10
1.2.2 Publisher Channel	11
1.3 Driver Components	12
1.4 Support for Standard Driver Features	12
1.4.1 Local Platforms	12
1.4.2 Remote Platforms	13
1.4.3 Entitlements	13
1.4.4 Password Synchronization	13
1.4.5 Account Tracking	13
1.4.6 Identity Manager Role Mapping Administrator	13
2 Installing the SAP GRC Access Control Driver	15
2.1 Downloading the Installation Program	15
2.2 Installing the Driver Files on the Metadirectory Engine	15
2.3 Installing the Driver Files on the Remote Loader	16
2.4 Installing the Designer and iManager Updates	16
2.4.1 Installing the 3.0.1 Designer Auto Update	17
2.4.2 Installing the Updated iManager Plug-Ins for Identity Manager	17
3 Creating a New Driver	19
3.1 Using Designer to Create and Configure the Driver	19
3.1.1 Using Designer to Import the Driver Configuration File	19
3.1.2 Using Designer to Adjust the Driver Settings	20
3.1.3 Using Designer to Deploy the Driver	20
3.1.4 Using Designer to Start the Driver	21
3.2 Using iManager to Create and Configure the Driver	21
3.2.1 Using iManager to Import the Driver Configuration File	22
3.2.2 Using iManager to Configure the Driver Settings	24
3.2.3 Using iManager to Start the Driver	24
3.3 Activating the Driver	24
4 Configuring the SAP GRC Access Control System	27
4.1 Configuring Request Types	27
4.2 Configuring a Workflow	28
4.2.1 Creating an Initiator	28
4.2.2 Creating a Stage	29
4.2.3 Creating a Path	30
5 Configuring the SAP GRC to Work with the Publisher Channel	31
5.1 Creating a Connector in the SAP GRC Access Control System	31

5.2	Adding Auto Provisioning for the Connector	32
5.3	Configuring Field Mapping	33
5.4	Creating a Request in the SAP GRC Access Control System	34
6	Managing the Driver	35
7	Troubleshooting the Driver	37
7.1	Troubleshooting the SAP GRC Access Control Driver	37
7.2	Error Occurs when Uninstalling the Driver	37
8	Role Export Utility	39
A	Driver Properties	41
A.1	Driver Configuration	41
A.1.1	Driver Module	41
A.1.2	Authentication	42
A.1.3	Startup Option	43
A.1.4	Driver Parameters	44
A.2	Global Configuration Values	45

About This Guide

This guide explains how to install, configure, and manage the Novell® Identity Manager driver for SAP GRC Access Control.

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Installing the SAP GRC Access Control Driver,” on page 15
- ♦ Chapter 3, “Creating a New Driver,” on page 19
- ♦ Chapter 4, “Configuring the SAP GRC Access Control System,” on page 27
- ♦ Chapter 5, “Configuring the SAP GRC to Work with the Publisher Channel,” on page 31
- ♦ Chapter 6, “Managing the Driver,” on page 35
- ♦ Chapter 7, “Troubleshooting the Driver,” on page 37
- ♦ Chapter 8, “Role Export Utility,” on page 39
- ♦ Appendix A, “Driver Properties,” on page 41

Audience

This guide is intended for Novell Identity Manager administrators and SAP developers and administrators.

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 Driver for SAP GRC Access Control Implementation Guide*, visit the [Novell Compliance Management Platform Extension for SAP Environment Documentation Web site \(http://www.novell.com/documentation/ncmp_sap10\)](http://www.novell.com/documentation/ncmp_sap10).

Additional Documentation

For documentation on Identity Manager, see the [Identity Manager Documentation Web site \(http://www.novell.com/documentation/idm36/index.html\)](http://www.novell.com/documentation/idm36/index.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 SAP GRC Access Control driver provisions users from the GRC Access Control into the Identity Vault.

- ♦ [Section 1.1, “Terminology,” on page 9](#)
- ♦ [Section 1.2, “How It Works,” on page 9](#)
- ♦ [Section 1.3, “Driver Components,” on page 12](#)
- ♦ [Section 1.4, “Support for Standard Driver Features,” on page 12](#)

1.1 Terminology

This section gives you essential information about terminology used with SAP. If you need further help with SAP terminology, see the [Glossary for the SAP Library \(http://help.sap.com/saphelp_46c/helpdata/En/35/2cd77bd7705394e10000009b387c12/frameset.htm\)](http://help.sap.com/saphelp_46c/helpdata/En/35/2cd77bd7705394e10000009b387c12/frameset.htm).

ABAP: Advanced Business Application Programming. A programming language designed for creating large-scale business applications.

BAPI: Business Application Programming Interface. SAP business APIs for the SAP business object types.

CCMS: Computer Center Management System. A set of tools to monitor, control, and configure an SAP system.

CUA: Central User Administration. The SAP tool used to centrally maintain user master records.

ERP: Enterprise resource planning. A software system for planning and automating enterprise-wide business processes.

GRC: Governance, risk, and compliance. Software or business processes that facilitate conformity to legal requirements.

IDocs: Intermediate document. A data exchange format used between SAP systems and between SAP systems and external applications.

SPML: Service Provisioning Markup Language. An XML-based framework for managing the provisioning and allocation of identity information and system resources within and between organizations.

UME: User Management Engine. Provides central user administration for Java applications.

1.2 How It Works

The SAP GRC Access Control driver works in two different scenarios. Use the scenario that works best for your environment.

- ♦ [Section 1.2.1, “Subscriber Channel,” on page 10](#)
- ♦ [Section 1.2.2, “Publisher Channel,” on page 11](#)

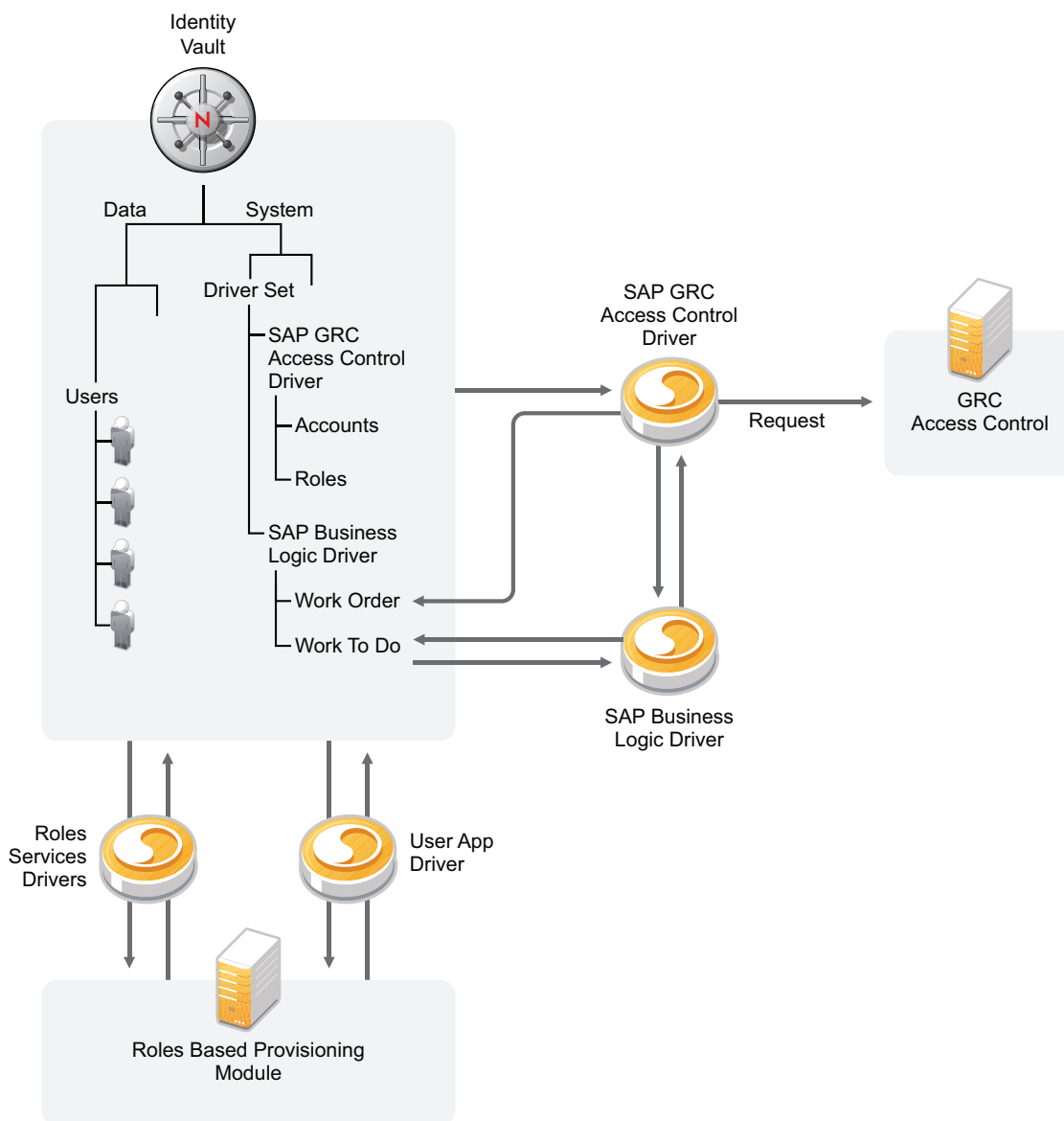
1.2.1 Subscriber Channel

The GRC Access Control system is an asynchronous system, and Identity Manager is a synchronous system. This means when a request is sent to the GRC Access Control system from the SAP GRC Access Control driver, that request can be processed immediately or it can be processed at some time in the future.

For Identity Manager to work correctly, it must know what the status of the request is. The SAP Business Logic driver is used with the SAP GRC Access Control driver to provide a way to track the status of each request. The SAP Business Logic driver acts like a timer.

Following the diagram is an explanation of how the SAP GRC Access Control driver works with the SAP Business Logic driver.

Figure 1-1 Subscriber Channel



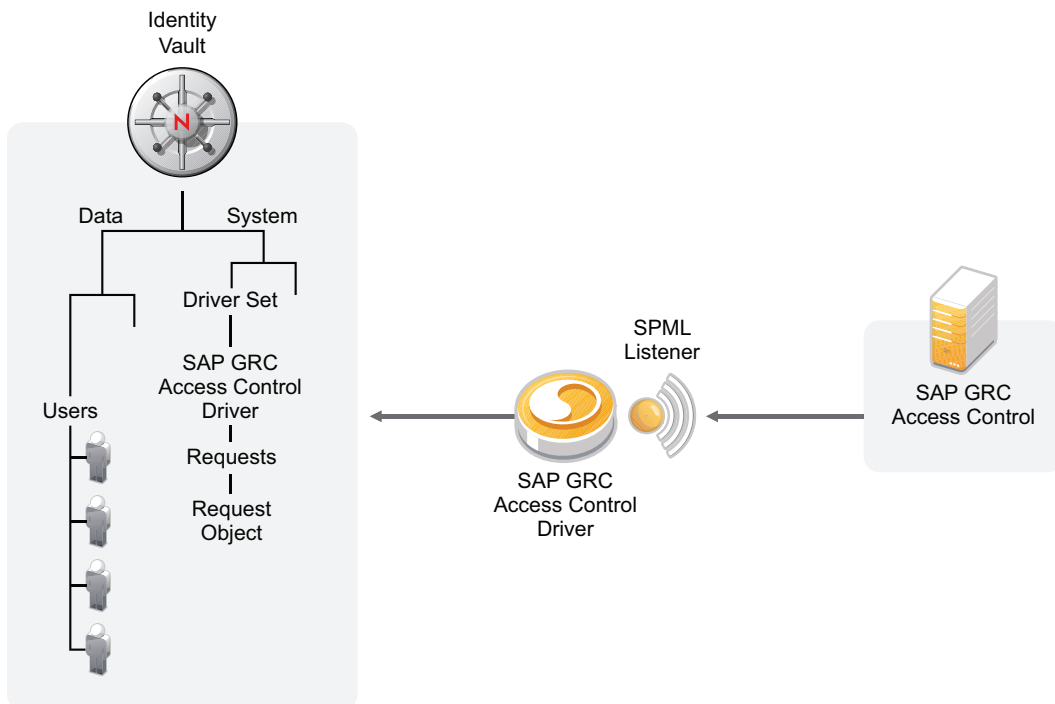
1. A role is assigned to a user in the Identity Vault through the Roles Based Provisioning Module.

2. Because the role that is assigned is associated with a GRC Access Control entitlement, the GRC Access Control entitlement is granted.
3. The GRC Access Control entitlement causes the SAP GRC Access Control driver to submit a request to the GRC Access Control system.
4. When a request is successful submitted to the GRC Access Control by the SAP GRC Access Control driver, the SAP Access Control driver creates a Work Order object.
5. The SAP Business Logic detects that the Work Order object is created, then the SAP Business Logic driver creates a Work To Do object. The Work To Do object contains the request number and the status of the request. The Work To Do object exist until the request to the GRC Access Control system is completed.
6. The SAP Business Logic driver checks the status of the request. One of three things can occur, depending upon the status of the request:
 - ♦ If the status is closed, the Work Order object remains and the GRC Access Control entitlement is updated with the results of the request.
 - ♦ If the status is rejected, the Work Order object remains and the GRC Access Control entitlement is updated with the results of the request.
 - ♦ If the status is something either than closed or rejected, the Work Order object is rescheduled.

1.2.2 Publisher Channel

The Publisher channel receives on the SAP GRC Access Control driver receives SPML requests from the GRC Access Control system.

Figure 1-2 *Publisher Channel*



The driver has an SPML listener and waits to receive the SPML requests from the GRC Access Control system. When the driver receives the SPML requests, it acts on that request in the Identity Vault. The driver can create, modify, or delete a user object in the Identity Vault.

Every time a request comes through the driver, a request object is created under the SAP GRC Access Control driver in the Identity Vault. These objects store the status of the request from the GRC Access Control system. At anytime, the GRC Access Control system can query Identity Manager to find out the status of the request it sent the SAP GRC Access Control driver.

These request objects are persistent. When you configure the driver for this scenario, you must also plan on managing these objects. These objects are stored under the driver object.

1.3 Driver Components

The driver is made up of several different components:

- ♦ **Driver Configuration File:** Used to create the driver object in the Identity Vault. It contains the policies that make the driver work, and the policies contain the business logic.

The driver configuration file name is `SAPGRCAC-CMP-IDM3_6_0-V1.xml`. For more information, see [Chapter 3, “Creating a New Driver,”](#) on page 19.

- ♦ **Driver Shim:** Handles the communication between the SAP GRC Access Control and the Metadirectory engine.

The driver shim file name is `SAPGRCACShim.jar`. For more information, see [Chapter 2, “Installing the SAP GRC Access Control Driver,”](#) on page 15.

- ♦ **Role Export Utility:** A Java* console application that exports your Identity Manager Roles Based Provisioning Module roles to an Excel* spreadsheet, delimited text file, or both. For more information, see [Chapter 8, “Role Export Utility,”](#) on page 39.

1.4 Support for Standard Driver Features

The following sections provide information about how the SAP GRC Access Control driver supports standard driver features:

- ♦ [Section 1.4.1, “Local Platforms,”](#) on page 12
- ♦ [Section 1.4.2, “Remote Platforms,”](#) on page 13
- ♦ [Section 1.4.3, “Entitlements,”](#) on page 13
- ♦ [Section 1.4.4, “Password Synchronization,”](#) on page 13
- ♦ [Section 1.4.5, “Account Tracking,”](#) on page 13
- ♦ [Section 1.4.6, “Identity Manager Role Mapping Administrator,”](#) on page 13

1.4.1 Local Platforms

The SAP GRC Access Control driver can be installed on the same operating systems supported by the Metadirectory server. For information, see “[Metadirectory Server](#)” in “[System Requirements](#)” in the *Identity Manager 3.6.1 Installation Guide*.

1.4.2 Remote Platforms

If you don't want to install the Metadirectory engine and Identity Vault (eDirectory™) on the SAP server, you can use the Remote Loader service to run the driver on the SAP server, and have the Metadirectory engine and Identity Vault on another server.

The SAP GRC Access Control driver can be installed on the same operating systems supported by the Remote Loader. For information, see “[Remote Loader](#)” in “[System Requirements](#)” in the *Identity Manager 3.6.1 Installation Guide*.

1.4.3 Entitlements

Entitlements are a way to set up a list of criteria to grant or revoke access to resources. The SAP GRC Access Control driver contains two preconfigured entitlements: user account and role. There is no configuration required to enable these entitlements. The SAP GRC Access Control driver must use these entitlements to provision accounts.

1.4.4 Password Synchronization

The SAP GRC Access Control driver does not support password synchronization.

1.4.5 Account Tracking

The Account Tracking feature is not supported with the SAP GRC Access Control driver.

1.4.6 Identity Manager Role Mapping Administrator

The SAP GRC Access Control driver can be configured to work with the Identity Manager Role Mapping Administrator, which is a tool that allows you to map business roles to IT roles. The Role Mapping Administrator is included with the Novell® Compliance Management Platform Extension for SAP Environments. For more information, see the *Identity Manager Role Mapping Administrator 1.0 Installation and Configuration Guide*.

Installing the SAP GRC Access Control Driver

2

The SAP GRC Access Control driver is installed when you install the SAP Integration module. The installation program extends the Identity Vault schema and installs the driver shim. This driver requires the latest updated driver configuration file. You must update Designer and iManager to get the updated configuration file.

- [Section 2.1, “Downloading the Installation Program,” on page 15](#)
- [Section 2.2, “Installing the Driver Files on the Metadirectory Engine,” on page 15](#)
- [Section 2.3, “Installing the Driver Files on the Remote Loader,” on page 16](#)
- [Section 2.4, “Installing the Designer and iManager Updates,” on page 16](#)

2.1 Downloading the Installation Program

The SAP GRC Access Control driver installation program is available on the [Novell® Identity Manager 3.6.1 Integration Module for Enterprise download site \(http://download.novell.com/Download?buildid=XAwwFo5tM8A~\)](http://download.novell.com/Download?buildid=XAwwFo5tM8A~).

- 1 Click *Novell Identity Manager 3.6.1 Integration Module for Enterprise*, then click *Download*.
- 2 Click *proceed to download*, then download the `NIIdM_Drivers_for_SAP.iso` file.

2.2 Installing the Driver Files on the Metadirectory Engine

The installer checks for the installed version of Identity Manager. You must have Identity Manager 3.6.1 installed for the installer to work.

- 1 Use the correct installation program for your platform on the `NIIdM_Driver_for_SAP.iso` file.

Platform	File
Windows*	<code>sap_drivers_install.exe</code>
Linux	<code>./sap_drivers_install_linux.bin</code>
Solaris*	<code>./sap_drivers_install_solaris.bin</code>
AIX*	<code>./sap_drivers_install_aix.bin</code>

- 2 Read and accept the license agreement, then click *Next*.
- 3 Select *Drivers* and *Schema Extensions*, then click *Next*.
- 4 Specify the LDAP DN of an administrative user that has rights to extend schema.
- 5 Specify the password of the administrative user.

- 6 Review the pre-installation summary, then click *Install*.
- 7 Review installation complete message, then click *Done*.

2.3 Installing the Driver Files on the Remote Loader

- 1 Use the correct installation program for your platform on the `NIIdM_Driver_for_SAP.iso` file.

Platform	File
Windows	<code>sap_drivers_install.exe</code>
Linux	<code>./sap_drivers_install_linux.bin</code>
Solaris	<code>./sap_drivers_install_solaris.bin</code>
AIX	<code>./sap_drivers_install_aix.bin</code>

- 2 Read and accept the license agreement, then click *Next*.
- 3 Select *Drivers* and *Utilities*, then click *Next*.
- 4 Specify the path to install the driver. The default location is:

Platform	Location
Windows	<code>c:\Novell\RemoteLoader\lib</code>
Linux/UNIX	<code>/opt/novell/eDirectory/lib/dirxml</code>

- 5 Click *Next*.
- 6 Specify the path to install the utilities. The default location is:

Platform	Location
Windows	<code>c:\Novell\NDS\DirXML\Utilities</code>
Linux/UNIX	<code>/opt/novell/</code>

- 7 Review the pre-installation summary, then click *Install*.
- 8 Review the installation complete message, then click *Done*.

2.4 Installing the Designer and iManager Updates

There is a new driver configuration file for the SAP GRC Access Control driver that must be installed to use the driver.

- ♦ [Section 2.4.1, “Installing the 3.0.1 Designer Auto Update,” on page 17](#)
- ♦ [Section 2.4.2, “Installing the Updated iManager Plug-Ins for Identity Manager,” on page 17](#)

2.4.1 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.

2.4.2 Installing the Updated iManager Plug-Ins for Identity Manager

In order to manage drivers with structured GCVs, you must install the updated iManager plug-ins.

- 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 the *Identity Manager 3.6.1 FPI Plug-in for iManager 2.7*, 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.

Creating a New Driver

3

After the SAP GRC Access Control driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the SAP GRC Access Control Driver,” on page 15](#)), you can create the driver in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- ♦ [Section 3.1, “Using Designer to Create and Configure the Driver,” on page 19](#)
- ♦ [Section 3.2, “Using iManager to Create and Configure the Driver,” on page 21](#)
- ♦ [Section 3.3, “Activating the Driver,” on page 24](#)

3.1 Using Designer to Create and Configure the Driver

The following sections provide steps for using Designer to create and configure a new SAP GRC Access Control driver. For information about using iManager to accomplish these tasks, see [Section 3.2, “Using iManager to Create and Configure the Driver,” on page 21](#).

- ♦ [Section 3.1.1, “Using Designer to Import the Driver Configuration File,” on page 19](#)
- ♦ [Section 3.1.2, “Using Designer to Adjust the Driver Settings,” on page 20](#)
- ♦ [Section 3.1.3, “Using Designer to Deploy the Driver,” on page 20](#)
- ♦ [Section 3.1.4, “Using Designer to Start the Driver,” on page 21](#)

3.1.1 Using Designer to Import the Driver Configuration File

Importing the SAP GRC Access Control driver configuration file creates the driver in the Identity Vault and adds the policies needed to make the driver work properly.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver set where you want to create the driver, then select *New > Driver* to display the Driver Configuration Wizard.
- 3 In the *Driver Configuration* list, select *SAP GRC Access Control*, then click *Run*.
- 4 On the Import Information Requested page, fill in the following fields:

Driver Name: Specify a name that is unique within the driver set.

SAP GRC Web Service URL: Specify the GRC Web Service URL on the SAP NetWeaver* server. Leave this field blank when the Subscriber channel is not active.

Authentication ID: Specify the authentication ID for the SAP GRC Web service.

Authentication Password: Specify the password of the authentication ID.

Requestor: Specify the ID of the GRC user that is defined as the *requestor id* for all requests in GRC.

First name: Specify the first name of the GRC user that is defined as the *requestor first name* for all requests in GRC.

Last name: Specify the last name of the GRC user that is defined as the *requestor last name* for all requests in GRC.

Email address: Specify the e-mail address of the GRC user that is defined as the *requestor email address* for all requests in GRC.

Driver is Local/Remote: Select whether the driver is running locally or is using the Remote Loader. For more information, see the *Identity Manager 3.6.1 Remote Loader Guide*.

- 5 Click *Next* to import the driver configuration.

At this point, the driver is created from the basic configuration file. To ensure that the driver works the way you want it to for your environment, you must review and modify (if necessary) the driver's default configuration settings.

- 6 To modify the default configuration settings, click *Configure*, then continue with the next section, *Using Designer to Adjust the Driver Settings*.

or


To skip the configuration settings at this time, click *Close*. When you are ready to configure the settings, continue with the next section, *Using Designer to Adjust the Driver Settings*.

3.1.2 Using Designer to Adjust the Driver Settings

The information specified on the Import Information Requested page is the minimum information required to import the driver. However, the base configuration might not meet your needs, or you might need to change the configuration you created when you imported the driver.


- ♦ You might need to change whether the driver is running locally or remotely.
- ♦ You might need to change whether the driver can work with the Role Mapping Administrator or not.

If you need to do additional configuration for the driver, you must access the properties page of the driver. If you do not have the Driver Properties page displayed:

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Properties*.
This opens the properties page for the driver. Use the information in *Appendix A, "Driver Properties," on page 41* to adjust the configuration.
- 3 Continue with *Section 3.1.3, "Using Designer to Deploy the Driver," on page 20*, to deploy the driver into the Identity Vault.

3.1.3 Using Designer to Deploy the Driver

After a driver is created in Designer, it must be deployed into the Identity Vault because Designer is an offline tool.

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Deploy*.
- 3 If you are authenticated to the Identity Vault, skip to *Step 5*; otherwise, specify the following information to authenticate:

Host: Specify the IP address or DNS name of the server hosting the Identity Vault.

Username: Specify the DN of the user object used to authenticate to the Identity Vault.

Password: Specify the user's password.

4 Click *OK*.

5 Read through the deployment summary, then click *Deploy*.

6 Read the successful message, then click *OK*.

7 Click *Define Security Equivalence* to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

7a Click *Add*, then browse to and select the object with the correct rights.

7b Click *OK* twice.

8 Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

8a Click *Add*, then browse to and select the user object you want to exclude.

8b Click *OK*.

8c Repeat **Step 8a** and **Step 8b** for each object you want to exclude.

8d Click *OK*.

9 Click *OK*.

3.1.4 Using Designer to Start the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver after the driver is deployed:

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon  or the driver line, then select *Live > Start Driver*.

For information about management tasks with the driver, see [Chapter 6, "Managing the Driver,"](#) on [page 35](#).


3.2 Using iManager to Create and Configure the Driver

The following sections provide steps for using iManager to create and configure a new SAP GRC Access Control driver. For information about using Designer to accomplish these tasks, see [Section 3.1, "Using Designer to Create and Configure the Driver,"](#) on [page 19](#).

- ♦ [Section 3.2.1, "Using iManager to Import the Driver Configuration File,"](#) on [page 22](#)
- ♦ [Section 3.2.2, "Using iManager to Configure the Driver Settings,"](#) on [page 24](#)
- ♦ [Section 3.2.3, "Using iManager to Start the Driver,"](#) on [page 24](#)

3.2.1 Using iManager to Import the Driver Configuration File

Importing the SAP GRC Access Control driver configuration file creates the driver in the Identity Vault and adds the policies needed to make the driver work properly.

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 In the Administration list, click *Utilities > Import Configuration* to launch the Import Configuration Wizard.
- 3 Use the following information to complete the wizard and create the driver.

Prompt	Description
Where do you want to place the imported configuration?	You can add the driver to an existing driver set, or you can create a new driver set and add the driver to the new set. If you choose to create a new driver set, you are prompted to specify the name, context, and server for the driver set.
Import a configuration into this driver set	Use the default option, <i>Import a configuration from the server (.XML file)</i> . In the <i>Show</i> field, select <i>Identity Manager 3.6 configurations</i> . In the <i>Configurations</i> field, select the <code>SAPGRCAC-CMP-IDM3_6_0-V1.xml</code> file.
Driver name	Specify a name that is unique within the driver set.
SAP GRC Web Service URL	Specify the GRC Web Service URL on SAP NetWeaver. Leave this field blank when the Subscriber channel is not active.
Authentication ID	Specify an authentication ID for the SAP GRC Web service.
Authentication Password	Specify the password for the authentication ID.
Requestor	Specify the ID of the GRC user that is defined as the <i>requestor id</i> for all requests in GRC.
First name	Specify the first name of the GRC user that is defined as the <i>requestor first name</i> for all requests in GRC.
Last name	Specify the last name of the GRC user that is defined as the <i>requestor last name</i> for all requests in GRC.
Email address	Specify the e-mail address of the GRC user that is defined as the <i>requestor email address</i> for all requests in GRC.
Driver is Local/Remote	Select whether the driver is running locally or is using the Remote Loader. For more information, see the <i>Identity Manager 3.6.1 Remote Loader Guide</i> .
Define Security Equivalences	The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.
Exclude Administrative Roles	You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

When you finish providing the information required by the wizard, a Summary page similar to the following is displayed.

Import Configuration

Summary - Current Configuration

Warning: Drivers May Require Configuration

Drivers imported from a configuration file may require additional configuration settings to be fully functional. Select the driver's link to edit its configuration settings.

The following summarizes the state of the driver as it currently exists.

- [metaserver1](#) (NCP Server)
- [driverset1](#) (Driver Set)
- SAP GRC Access Control CMP 2** (Drivers May Require Configuration) (Driver)
 - [smp](#) (Schema Mapping Policy)
 - [itp-ManufactureAssociation](#) (Input Transformation Policy)
 - [otp-SpecialAttributeHandling](#) (Output Transformation Policy)
 - [Publisher](#) (Publisher)
 - [none](#) (Command Transformation Policy)
 - [pub-etp-RequestStatusQuery](#) (Event Transformation Policy)
 - [none](#) (Matching Policy)
 - [pub-cp](#) (Creation Policy)
 - [pub-pp](#) (Placement Policy)

<< Back Next >> Cancel Finish

At this point, the driver is created from the basic configuration file. To ensure that the driver works the way you want it to for your environment, you must review and modify (if necessary) the driver's default configuration settings.

- 4 To modify the default configuration settings, click the linked driver name, then continue with the next section, **Using iManager to Configure the Driver Settings**.

or

To skip the configuration settings at this time, click *Finish*. When you are ready to configure the settings, continue with the next section, **Using iManager to Configure the Driver Settings**.


WARNING: Do not click *Cancel* on the Summary page. This removes the driver from the Identity Vault and results in the loss of your work.

3.2.2 Using iManager to Configure the Driver Settings

The information specified during the creation of the driver is the minimum information required to import the driver. However, the base configuration might not meet your needs.

- ♦ You might need to change whether the driver is running locally or remotely.
- ♦ You might need to change whether the driver is using the Role Mapping Administrator or not.


To configure the settings:

- 1** Make sure the Modify Object page for the SAP GRC Access Control driver is displayed in iManager. If it is not:
 - 1a** In iManager, click  to display the Identity Manager Administration page.
 - 1b** Click *Identity Manager Overview*.
 - 1c** Browse to and select the driver set object that contains the new SAP GRC Access Control driver.
 - 1d** Click the driver set name to access the Driver Set Overview page.
 - 1e** Click the upper right corner of the driver, then click *Edit properties*.
This displays the properties page of the driver.
- 2** Review the settings for the driver parameters, global configuration values, or engine control values. The configuration settings are explained in [Appendix A, “Driver Properties,” on page 41](#).
- 3** After modifying the settings, click *OK* to save the settings and close the Modify Object page.

3.2.3 Using iManager to Start the Driver

When a driver is created, you must start the driver. Identity Manager is an event-driven system, so after the driver is started, it processes events as they occur.

To start the driver after the additional configuration is completed:

- 1** In iManager, click  to display the Identity Manager Administration page.
- 2** Click *Identity Manager Overview*.
- 3** Browse to and select the driver object that contains the SAP GRC Access Control driver you want to start.
- 4** Click the driver set name to access the Driver Set Overview page.
- 5** Click the upper right corner of the driver, then click *Start driver*.

For information about management tasks with the driver, see [Chapter 6, “Managing the Driver,” on page 35](#).

3.3 Activating the Driver

The extension for SAP environments contains its own activation that you receive from the customer center. The drivers that are part of the extension for SAP environments require this new activation within 90 days of creating the driver. Otherwise, the driver stops working.

For more information on activation, refer to “[Activating Novell Identity Manager Products](#)” in the *Identity Manager 3.6.1 Installation Guide*.

Configuring the SAP GRC Access Control System

4

The GRC Access Control system needs to be installed and configured in order to work with the SAP GRC Access Control driver. You can set up and configure the GRC Access Control system many different ways, however there are two main GRC Access Control components that need to be configured:

- [Section 4.1, “Configuring Request Types,” on page 27](#)
- [Section 4.2, “Configuring a Workflow,” on page 28](#)

4.1 Configuring Request Types

A request type defines the actions that are performed when a request is processed. The SAP GRC Access Control driver is requestor. The driver works with the default request types. You must create a new request type that contains only the action of `CHANGE_USER`. If you create other request types, the driver does not recognize them. However, you can change the actions assigned to the default request types and the driver performs the assigned actions.

[Table 4-1](#) contains the default request types, the required assigned actions, and the GCV that contains this request type. The request types can have more actions assigned to them, but the actions listed are what the driver is expecting to be there. For more information about the GCVs, see [Section A.2, “Global Configuration Values,” on page 45](#).

Table 4-1 Request Types and GCVs

Request Type	Action	GCV
NEW	CREATE_USER	New account request type
CHANGE	ASSIGN_ROLE	Role assignment request type
DELETE	DELETE_USER	Delete account request type
LOCK	LOCK_USER	Lock account request type
UNLOCK	UNLOCK_USER	Unlock account request type
CHANGE_USER*	CHANGE_USER only	Modify user information request type

The last request type is the new request type that must be created for the driver to work. This request type must contain only the `CHANGE_USER` action. There is a default request type of `CHANGE` in the GRC Access Control, but it also contains `ASSIGN_ROLE`, and this request type does not work for the driver.

To create the new request type:

- 1 Log in to the SAP GRC Access Control as an administrative user.
- 2 Click the *Configuration* tab.

- 3 Click *Request Type*, then click *Create*.
- 4 Use the following information to create the request type:
 - Type:** Specify a unique name for the request type. It must be in uppercase.
 - Short Description:** Specify a short description for the request type.
 - Description:** Specify a description for the request type.
 - Sequence:** Specify a value for the sequence. The sequence defines the order in which request types appear on the Request Access screen. If you assign 0, the request type does not appear on the Request Access screen. However, if the request type is active, it appears on the Request Type drop-down list throughout Compliant User Provisioning.
 - Workflow Type:** Select *CUP* as the workflow type.
 - Active:** Select the check box to make the request type active.
 - End User Description:** Specify a description that is displayed to the users.
- 5 Click *Go* under *Available Actions* to see the actions.
- 6 Select *CHANGE_USER*, then click the left-arrow to assign the action.
- 7 Click *Save* to save the request type.

4.2 Configuring a Workflow

You must have a workflow defined in the GRC Access Control in order to act upon the request types. A workflow consists of an initiator, a stage, and a path. Each request type must be assigned to an initiator. You can set up one workflow that contains all of the request types, or you can create a separate workflow for each request type.

The following is an example of how to configure one workflow with all of the request types.

- ♦ [Section 4.2.1, “Creating an Initiator,” on page 28](#)
- ♦ [Section 4.2.2, “Creating a Stage,” on page 29](#)
- ♦ [Section 4.2.3, “Creating a Path,” on page 30](#)

4.2.1 Creating an Initiator

An initiator is an object that defines a precise request condition, and identifies the single, unique workflow designed to handle that type of request. Initiators and workflows function as matched pairs. Each initiator can call only one workflow, and each workflow can be called by one initiator.

- 1 Log in to the SAP GRC Access Control as an administrative user.
- 2 Click the *Configuration* tab.
- 3 Click *Workflow > Initiator*, then click *Create*.
- 4 Use the following information to create the initiator:
 - Name:** Specify a name for the initiator. It must be uppercase and it cannot contain spaces. For example, *WF_INIT_ONE*.
 - Short Description:** Specify a short description for the workflow.
 - Description:** Specify a description for the workflow.
 - Workflow Type:** Select *CUP* as the workflow type.

- 5 Select attributes for the initiator with the following information:
 - Condition:** Select the condition of *AND*, *NOT*, or *Or*. For this example the condition is *Or*.
 - Attribute:** Select *Request Type* for the attribute.
 - Value:** Select one of the request types listed in [Table 4-1 on page 27](#).
- 6 Click *Add Attribute*, then repeat [Step 5](#) for each request type listed in [Table 4-1 on page 27](#).
- 7 Click *Save* to create the initiator.
- 8 Continue with [Section 4.2.2, “Creating a Stage,” on page 29](#).

4.2.2 Creating a Stage

A stage is a decision point in a workflow. At each stage, one or more approvers must approve or deny the request. The stage defines who must approve the request. It also determines what happens next, based on the decision of the approver. At each stage of the request process, the system sends an e-mail message to the user designated to approve or deny the request. The request process cannot continue until the approver responds by approving or rejecting the request.

- 1 Click *Workflow > Stage*, then click *Create*.
- 2 Use the following information to create the stage:
 - Name:** Specify a name for the stage. It must be uppercase and it cannot contain spaces.
 - Short Description:** Specify a short description for the stage.
 - Description:** Specify a description for the stage.
 - Workflow Type:** Select the workflow type as *CUP*.
 - Approver Determinator:** From the drop-down list, select who receives the request types from the driver.
 - Request Wait Time (Days):** Specify amount of time, in days, for the Compliance User Provisioning to wait for an approver to respond to a request before escalating the request. In this example it is 0, because there is no escalation configured.
 - Request Wait Time (Hours):** Specify amount of time, in hours, for the Compliance User Provisioning to wait for an approver to respond to a request before escalating the request. In this example it is 0, because there is no escalation configured.
 - Escalation Configuration:** From the drop-down list, select *No Escalation*.
 - Notification Configuration:** Configure whether and to whom the system notifies about actions taken at this point in the stage.
 - Additional Configuration:** Define any additional functionality required at this stage.
 - Additional Security Configuration:** Define whether the approver needs to configure his or her identity to take an action at this stage.
- 3 Click *Save* to create the stage.
- 4 Continue with [Section 4.2.3, “Creating a Path,” on page 30](#).

4.2.3 Creating a Path

A path defines the sequence of stages in a workflow. When you create a workflow, you begin by creating each of its stages. By themselves, the stages serve no purpose. Each stage is an independent entity, unrelated to any other stage. When you create a path, you define the order in which the workflow calls its stages.

1 Click *Workflow > Path*, then click *Create*.

2 Use the following information to create the path:

Name: Specify a name for the path. It must be uppercase and it cannot contain spaces.

Short Description: Specify a short description of the path.

Description: Specify a description of the path.

Workflow Type: Select the workflow type as *CUP*.

Number of Stages: Specify the number of stages you want to include in the path.

Initiator: From the drop-down list, select the initiator that you created in [Section 4.2.1, “Creating an Initiator,”](#) on page 28.

Active: Select *Active* to make the path active when it is created.

3 Click *Save* to create the path.

Configuring the SAP GRC to Work with the Publisher Channel

5

In order to use the Publisher channel functionality of the SAP GRC Access Control driver, you must configure the GRC Access Control system to submit data from approved requests into the Identity Vault. These steps are required only if the Publisher channel functionality is needed. For more information about how the Publisher channel for the SAP GRC Access Control driver works, see [Section 1.2.2, “Publisher Channel,” on page 11](#).

- [Section 5.1, “Creating a Connector in the SAP GRC Access Control System,” on page 31](#)
- [Section 5.2, “Adding Auto Provisioning for the Connector,” on page 32](#)
- [Section 5.3, “Configuring Field Mapping,” on page 33](#)
- [Section 5.4, “Creating a Request in the SAP GRC Access Control System,” on page 34](#)

5.1 Creating a Connector in the SAP GRC Access Control System

You must create a connector in the SAP GRC Access Control Compliant User Provisioning system to communicate with the Identity Vault:

- 1 Log in to the SAP GRC Access Control system as an administrative user.
- 2 Click the *Configuration* tab, then click *Connectors > Create Connectors*.
- 3 Select *IDM* as the connector type.
- 4 Use the following information to create the connector:

Short Description: Specify a short description for the connector.

Web Service URI: Specify a URI in the form `http://host.port` where the host and port values match the values in the *Listening IP address and port* driver parameter for the Publisher channel.

User ID: Specify the value for the *Authentication ID* driver parameter for the Publisher channel. This value does not need to correspond with a real identity in either the Identity Vault or the GRC Access Control system.

Password: Specify the value for the *Authentication Password* driver parameter for the Publisher channel.

- 5 Use the following name-value pairs to populate the Parameter Names and Parameter Values section:

Parameter Name	Parameter Value
ASSIGN_ROLES:OC	SubmitRequest
AUDIT_SEARCH_ATTRIBUTE	requestid
AUDIT_SEARCH_OPERATION	operation=auditlog
AUDIT_TYPE	auditlogs
CHANGE_USER:OC	SubmitRequest
CREATE_USER:OC	SubmitRequest
DATE	time
DELETE_USER:OC	SubmitRequest
LOCK_USER>Login Disabled	true
LOCK_USER:OC	SubmitRequest
OPERATION	operation
PROV_CALL	Sync
REQUEST_ID	id
REQUEST_STATUS	result
RESET_PASSWORD:OC	SubmitRequest
REST_PASSWORD:resetPassword	true
ROLE	Group Membership
SCHEMA_ID	SubmitRequest
SEARCH_CRITERIA	searchBase
UNLOCK_USER>Login Disabled	false
UNLOCK_USER:OC	SubmitRequest
USER_ID	object-id

6 Test the connection, the save the connector.

5.2 Adding Auto Provisioning for the Connector

You must configure the connector for auto provisioning, or the events are not sent to the SAP GRC Access Control driver automatically.

- 1 Log in to the SAP GRC Access Control system as an administrative user.
- 2 Click the *Configuration* tab, then click *Workflow > Auto Provisioning*.
- 3 Click the *By System* tab.
- 4 Click the *Create* icon.
- 5 In the *System* drop-down menu, select the connector you created in [Section 5.1, “Creating a Connector in the SAP GRC Access Control System,”](#) on page 31.

- 6 Select *Direct* for the default provisioning type.
- 7 Select *Auto-Provision* at the end of request for the auto-provisioning type.
- 8 Select *No* for the value of the *Create If User Does Not Exist* parameter.
- 9 Accept the default values for the other parameters, then click *Save*.

5.3 Configuring Field Mapping

You must configure field mapping between SAP GRC Access Control Compliant User Provisioning and the Identity Vault.

- 1 Log in to the SAP GRC Access Control system as an administrative user.
- 2 Click the *Configuration* tab, then click *Field Mapping > Provisioning*.
- 3 Click the *Create* icon.
- 4 Use the following information to configure the field mapping:
 - Group Name:** Specify a group name for this field mapping.
 - Short Description:** Specify a short description for the field mapping.
 - Connector Type:** Select *IDM* for the connector type.
- 5 In the Application table, click the plus icon to add the connector you created in [Section 5.1, “Creating a Connector in the SAP GRC Access Control System,”](#) on page 31, then select *Default System*.
- 6 Click *Continue*.
- 7 Use the following table to map the AC fields (GRC Access Control) with the application fields (Identity Vault).

These mappings are used to map GRC Access Control fields to attributes names commonly used with SPML. The schema mapping in the driver configuration file is then used to map the SPML attribute names to the names used in the Identity Vault.

AC Field	Application Field
Email Address - STANDARD	emailAddress
Employee Type - STANDARD	employeeType
Location - STANDARD	location
Org. Unit - STANDARD	department
Position - STANDARD	Title
Requestor ID - STANDARD	displayName
Telephone Number - STANDARD	telephone
User FName - STANDARD	firstName
User ID - STANDARD	CN
User LName - STANDARD	lastName

- 8 Click *Save* after you have defined the mappings.

5.4 Creating a Request in the SAP GRC Access Control System

When you create requests in the GRC Access Control system, select the connector that you created in [Section 5.1, “Creating a Connector in the SAP GRC Access Control System,” on page 31](#) as one of the applications to be provisioned if the request is approved. You must select this connector if you want the data from the request to be provisioned to the Identity Vault when the request is approved.

Managing the Driver

6

As you work with the SAP GRC Access Control driver, there are a variety of management tasks you might need to perform, including the following:

- ◆ Starting, stopping, and restarting the driver
- ◆ Viewing driver version information
- ◆ Using Named Passwords to securely store passwords associated with the driver
- ◆ Monitoring the driver's health status
- ◆ Backing up the driver
- ◆ Inspecting the driver's cache files
- ◆ Viewing the driver's statistics
- ◆ Using the DirXML[®] Command Line utility to perform management tasks through scripts
- ◆ Securing the driver and its information
- ◆ Synchronizing objects
- ◆ Migrating and resynchronizing data

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 3.6.1 Common Driver Administration Guide*.

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

Troubleshooting the Driver

7

- [Section 7.1, “Troubleshooting the SAP GRC Access Control Driver,” on page 37](#)
- [Section 7.2, “Error Occurs when Uninstalling the Driver,” on page 37](#)

7.1 Troubleshooting the SAP GRC Access Control Driver

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DTrace. You should only use it during testing and troubleshooting the driver. Running DTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see “[Viewing Identity Manager Processes](#)” in the *Identity Manager 3.6.1 Common Driver Administration Guide*.

7.2 Error Occurs when Uninstalling the Driver

If you have installed the SAP GRC Access Control driver on a server that does not have a Java Virtual Machine (JVM) installed on it, you receive the following error when trying to uninstall the driver.

```
No Java virtual machine could be found from your PATH
environment variable. You must install a VM prior to
running this program.
```

The problem only occurs if you install the SAP GRC Access Control driver on a server that does not have Identity Manager or the Remote Loader installed on it.

The work around is to install the driver on a server with Identity Manager or the Remote Loader, or install the JVM and add the installation location to the PATH variable.

Linux/UNIX: To add the JVM to the PATH variable:

- 1 From a command line, enter `export PATH=<JAVA-HOME-PATH>/bin/:$PATH`.
- 2 Run the uninstall script for the Identity Manager drivers for SAP, where the JAVA-HOME-PATH is the Java or JRE installation location.

Windows: To add the JVM to the PATH variable, use the following command:

```
"Uninstall Novell Identity Manager Drivers for SAP.exe" LAX_VM "<JAVA-HOME-
PATH>\bin\java.exe"
```


Role Export Utility

8

The SAP GRC Access Control driver contains a role export utility. The utility is a Java console application that exports the Identity Manager Roles Based Provisioning Modules roles to an Excel spreadsheet, a delimited text file, or both.

The Excel spreadsheet format can be imported into the Compliant User Provisioning (CUP) product in the SAP GRC Access Control suite. The delimited text format can be imported into the Risk Analysis and Remediation (RAR) product in the SAP GRC Access Control suite.

The CUP and RAR maintain separate databases that contain the role information for the SAP GRC Access Control suite. If you are using both products, you must import the Identity Manager Roles Based Provisioning Module roles into each product.

The role export utility supports Java 1.42 or above.

The role export utility is installed in the following default locations when the drivers for the extension for SAP environments is installed.

- ♦ **Windows:** C:\Novell\NDS\DirXMLUtilities\SAP\SAPUsers
- ♦ **Linux/UNIX:** /opt/novell/eDirectory/lib/dirxml/util/sapgrcac

This is a different directory than the standard Identity Manager directory for utilities which is /opt/novell/eDirectory/lib/dirxml/rules/<driverID>.

To run the role export utility:

- 1 Verify that the `RoleExport.jar`, `jxl.jar`, and `ldap.jar` files are in the same directory.
- 2 From a command line, enter `java -jar RoleExport.jar`.
- 3 Specify the hostname or IP address of the server that contains the Roles Based Provisioning Module definitions.
- 4 Specify the LDAP port for a clear text connection. The default port is 389.
- 5 Specify the LDAP DN of a user that has rights to read the role definitions.
- 6 Specify the password for the user.
- 7 Specify the LDAP DN of the container that holds the role definitions.
The default location of the role definitions container is `cn=RoleDefs,cn=RoleConfig,cn=<User App driver>,cn=<driver set>,dc=<container>`
- 8 Specify an LDAP filter for the set of roles you want to export.
The default filter is: `(objectclass=nrfRole)`
- 9 Specify 1 to export to Excel, specify 2 to export to a delimited text file, or specify 3 to export to both formats.
- 10 (Conditional) If you selected 1 or 3, specify the path and filename where the exported Excel file will be created.
If a file with the specified name exists, the existing file is overwritten with the new file.
- 11 (Conditional) If you selected 1 or 3, specify a value for the `ConnectorType` in the exported Excel file.

12 (Conditional) If you selected 2 or 3, specify the path and filename where the delimited text file will be created.

If a file with the specified name exists, the existing file is overwritten with the new file.


The first time the utility runs, all answers except for the password are saved in the `RoleExport.cfg` file. The next time the utility runs, the answers in the `RoleExport.cfg` file are used and you are prompted for the password.

If you want to change an answer, edit the `RoleExport.cfg` file or delete the file. This is a text file that can be edited with any text editor.

Driver Properties

A


This section provides information about the Driver Configuration and Global Configuration Values properties for the SAP GRC Access Control driver. These are the only unique properties for this driver. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to “[Driver Properties](#)” in the *Identity Manager 3.6.1 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an  icon.


- ♦ [Section A.1, “Driver Configuration,” on page 41](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 45](#)

A.1 Driver Configuration

In Designer:

- 1 Open a project in the Modeler.
- 2 Right-click the driver icon  or line, then select click *Properties > Driver Configuration*.

In iManager:

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.
- 3 Locate the SAP GRC Access Control driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
- 4 Click *Edit Properties* to display the driver’s properties page.

By default, the properties page opens with the *Driver Configuration* tab displayed.



The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,” on page 41](#)
- ♦ [Section A.1.2, “Authentication,” on page 42](#)
- ♦ [Section A.1.3, “Startup Option,” on page 43](#)
- ♦ [Section A.1.4, “Driver Parameters,” on page 44](#)

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.


Table A-1 *Driver Modules*









Option	Description
<i>Java</i>	<p>Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the <code>classes</code> directory as a class file, or in the <code>lib</code> directory as a <code>.jar</code> file. If this option is selected, the driver is running locally.</p> <p>The name of the Java class is: <code>com.novell.nds.dirxml.driver.sap.grcas.SAPGRCACShim</code></p>
<i>Native</i>	This option is not used with the SAP GRC Access Control driver.
<i>Connect to Remote Loader</i>	<p>Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:</p> <ul style="list-style-type: none"> ◆  <i>Driver Object Password</i>: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim. ◆  <i>Remote Loader Client Configuration for Documentation</i>: Includes information on the Remote Loader client configuration when Designer generates documentation for the SAP GRC Access Control driver.

A.1.2 Authentication

The authentication section stores the information required to authenticate to the connected system.

Table A-2 *Authentication Options*


Option	Description
<i>Authentication ID</i>	<p>Specify an SAP account that the driver can use to authenticate to the SAP system.</p> <p>Example: <code>SAPUser</code></p>
<i>Authentication Context</i> or  <i>Connection Information</i>	Specify the IP address or name of the SAP server the driver should communicate with.

Option	Description
Remote Loader Connection Parameters or  <i>Host name</i>  <i>Port</i>  <i>KMO</i>  <i>Other parameters</i>	Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is <code>hostname=xxx.xxx.xxx.xxx port=xxxx</code> <code>kmo=certificatename</code> , when the host name is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090. The <code>kmo</code> entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: <code>hostname=10.0.0.1 port=8090</code> <code>kmo=IDMCertificate</code>
Driver Cache Limit (kilobytes) or  <i>Cache limit (KB)</i>	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.  Click <i>Unlimited</i> to set the file size to unlimited in Designer.
Application Password or  <i>Set Password</i>	Specify the password for the user object listed in the <i>Authentication ID</i> field.
Remote Loader Password or  <i>Set Password</i>	Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

A.1.3 Startup Option

The startup options allow you to set the driver state when the Identity Manager server is started.

Table A-3 *Startup Options*

Option	Description
<i>Auto start</i>	The driver starts every time the Identity Manager server is started.
<i>Manual</i>	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
<i>Disabled</i>	The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.
 <i>Do not automatically synchronize the driver</i>	This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.4 Driver Parameters

The driver parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment.

The parameters are presented by category:

- ◆ [Table A-4, “Driver Settings,” on page 44](#)
- ◆ [Table A-5, “Subscriber Settings,” on page 44](#)
- ◆ [Table A-6, “Publisher Settings,” on page 44](#)

Table A-4 *Driver Settings*

Parameter	Description
There are no driver parameters.	NA

Table A-5 *Subscriber Settings*

Parameter	Description
<i>SAP GRC Web Service URL</i>	Specify the GRC Web Service URL on the SAP NetWeaver server. Leave this field blank when the Subscriber channel is not active.
<i>Authentication ID</i>	Specify the ID of the GRC user that is defined as the <i>requestor id</i> for all request in GRC.
<i>Authentication Password</i>	Specify the password of the authentication ID.
<i>Show advanced connection options</i>	Select <i>show</i> to the advanced connection options.
<i>Show advanced connection options > Truststore file</i>	When the remote server is configured to provide server authentication, this is the path and the name of the keystore file which contains trusted certificates. For example: <code>C:\security\truststore</code> . Leave this field blank when server authentication is not used.
<i>Show advanced connection options > Proxy host and port</i>	When a proxy host and port are used, specify the host address and the host port. For example: <code>192.10.1.3:18180</code> . Choose an unused port number on your server.

Table A-6 *Publisher Settings*

Parameter	Description
<i>Listening IP address and port</i>	Specify the IP address of the server where this driver is installed and the port that this driver listens on for Web Service requests from GRC. You can specify <code>127.0.0.1</code> if there is only one network card installed in the server. Choose an unused port number on your server. For example, <code>127.0.0.1:18180</code> . The driver listens on this address for requests, processes the requests, and returns a result.
<i>Authentication ID</i>	Specify the authentication ID to validate incoming requests.


Parameter	Description
<i>Authentication Password</i>	Specify the password of the authentication ID.
<i>Publisher Heartbeat Interval</i>	Specify how many minutes of inactivity can elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.
<i>Show advanced connection options</i>	Select <i>show</i> to display the advanced connection options.
<i>Show advanced connection options > KMO name</i>	Specify the KMO name in the Identity Vault, when this server is configured to accept HTTPS connections. The KMO name is the name before - in the RDN. Leave this field blank when a keystore file is used or when HTTPS connections are not used.
<i>Show advanced connection options > keystore file</i>	Specify the path and name of the keystore file, when the server is configured to accept HTTPS connections. For example: C:\security\keystore. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
<i>Show advanced connection options > Keystore password</i>	Specify the keystore file password, when the server is configured to accept HTTPS connections. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
<i>Show advanced connection options > Server key alias</i>	Specify the key alias, when this server is configured to accept HTTPS connections. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
<i>Show advanced connection options > Server key password</i>	Specify the key alias password (not the keystore password), when the server is configured to accept HTTPS connections. Leave this field blank when a KMO name is used or when HTTPS connections are not used.
<i>Show advanced connection options > Require mutual authentication</i>	When using SSL, it is common to do only server authentication. However, if you want to force both client and server to present certificates during the handshake process, select <i>Required</i> .

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The SAP GRC Access Control driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:

- 1 Click  to display the Identity Manager Administration page.
- 2 Open the driver set that contains the driver whose properties you want to edit:
 - 2a In the *Administration* list, click *Identity Manager Overview*.
 - 2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
 - 2c Click the driver set to open the Driver Set Overview page.


3 Click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.

or


To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

Table A-7 *Global Configuration Values*

Option	Description
<i>Change incoming Group Membership values to association values</i>	If <i>True</i> , incoming values for Group Membership attributes are set as association-ref attributes values on the containing value elements.
<i>Request Information > Show requestor information</i>	Select <i>show</i> to display the information for the requestor.
<i>Requestor Information > Requestor ID</i>	Specify the ID of the GRC user that is supplied as the <i>requestor id</i> on all requests to GRC.
<i>Requestor Information > First name</i>	Specify the first name of a GRC user that is supplied as the <i>requestor first name</i> on all requests to GRC.
<i>Requestor Information > Last name</i>	Specify the last name of the GRC user that is supplied as the <i>requestor last name</i> on all requests to GRC.
<i>Requestor Information > Email address</i>	Specify the e-mail address of the GRC user that is supplied as the <i>requestor email address</i> on all requests to GRC.
<i>Request Mapping > Show request mapping information</i>	Select <i>show</i> to display the information for request mapping.
<i>Request Mapping > Priority</i>	Specify a value for the request priority. This value must correspond to a request priority value defined in GRC. It is the priority value specified with the request data.
<i>Request Mapping > Account entitlement remove means</i>	Select whether the account is disabled or deleted when the entitlement for a user account in the GRC system is revoked. delete account: A Delete Account request is submitted to GRC. disable account: A Lock Account request is submitted to GRC.
<i>Request Mapping > New account request type</i>	Specify the GRC request type that contains the CREATE_USER action. For more information, see Section 4.1, "Configuring Request Types," on page 27 .

Option	Description
<i>Request Mapping > New account request requires role assignment</i>	Select <i>true</i> if the GRC request type used for new user accounts also contains the action ASSIGN_ROLES, otherwise select <i>false</i> .
<i>Request Mapping > Role assignment request type</i>	Specify the value of the GRC request type that contains the ASSIGN_ROLES action.
<i>Request Mapping > Delete account request type</i>	Specify the value of the GRC request type that contains the DELETE_USER action.
<i>Request Mapping > Lock account request type</i>	Specify the value of the GRC request type that contains the LOCK_USER action.
<i>Request Mapping > Unlock account request type</i>	Specify the value of the GRC request type that contains the UNLOCK_USER action.
<i>Request Mapping > Modify user information request type</i>	Specify the GRC request type that contains the CHANGE_USER action, but not the ASSIGN_ROLES action.
<i>Request Status > Show request status retrieval parameters</i>	Select <i>show</i> to display the request status parameters.
<i>Request Status > Status check interval in minutes</i>	Specify a value for how often GRC is polled to get the current status of a previously submitted request.
<i>Request Status > Always perform GRC risk analysis</i>	Select <i>true</i> to always obtain the results of a GRC risk analysis after submitting a request to GRC. Select <i>false</i> to not obtain the GRC risk analysis results.
<i>Request Status > Get GRC audit trail on request completion</i>	Select <i>true</i> to always obtain the GRC audit trail when requests are approved or rejected. Select <i>false</i> to not obtain the GRC audit trail for requests.
Role Mapping > Show role mapping configuration.	Select <i>show</i> to display the GCVs for enabling the driver to work with the Role Mapping Administrator. For more information, see the <i>Identity Manager Role Mapping Administrator 1.0 Installation and Configuration Guide</i> .

