www.novell.com/documentation

Identity Reporting Module Guide

Identity Manager 4.0.2

January 2014

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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.netiq.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This book describes the Identity Reporting Module for Identity Manager 4.0 and how you can use the features it offers, including:

- A high-level introduction to the product
- Installation instructions
- How to get started
- Using the Overview page
- Using the Repository page
- Using the Import page
- Using the Calendar page
- Using the Completed and Running Reports page
- Using the Settings and Data Collection pages
- How to download predefined report definitions
- How to create custom report definitions
- REST interfaces for reporting

Audience

This guide is intended for all users of the Identity Reporting Module.

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 *Identity Manager Reporting Guide*, visit the Identity Manager Web site (http://www.netiq.com/documentation/idm402/index.html).

Additional Documentation

For documentation on other Identity Manager components, see the Identity Manager Documentation Web site (http://www.netiq.com/documentation/idm40/index.html).

1 Welcome to the Identity Reporting Module

This section provides an overview of the Identity Reporting Module.

1.1 About the Identity Reporting Module

The Identity Reporting Module generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from Identity Vaults and managed systems such as Active Directory or SAP. The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives you the option to import custom reports defined in a third-party tool. The user interface for the reporting module makes it easy to schedule reports to run at off-peak times to optimize performance.

NOTE: For details on the predefined reports, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm402/idm_reports/data/bookinfo.html).

The core of the reporting module is the *Identity Information Warehouse*. The warehouse is an intelligent repository of information about the actual state and the desired state of the Identity Vault and the managed systems within an organization. By querying the warehouse, you can retrieve all of the information you need to ensure that your organization is in full compliance with relevant business laws and regulations. The warehouse gives you a 360-degree view of your business entitlements, providing the knowledge you need to see the past and present state of authorizations and permissions granted to identities in your organization. With this knowledge, you can answer even the most sophisticated Governance Risk and Compliance (GRC) queries.

The Identity Information Warehouse uses two new drivers to collect data about an organization:

- Data Collection Service Driver
- Managed System Gateway Driver

The Data Collection Service Driver uses a push model to collect data about changes made to user accounts, roles, resources, group memberships, and other objects in the vault. The Managed System Gateway Driver can pull information from any managed system that has been enabled for data collection in Identity Manager 4.0.2, as long as it supports entitlements. In addition to maintaining data about identities that are under the full control of the Identity Manager engine, the Identity Information Warehouse collects data about identities that are not managed by the engine.

The reporting module provides several open integration points. For example, if you want to collect data about third-party applications that are not connected to Identity Manager, you can implement a custom REST endpoint to collect data from these applications. In addition, you can customize the data that is pushed to the Identity Vault. To do this, you add a filter to the Data Collection Service Driver to add custom objects or attributes, causing these additional pieces of information to be stored in the warehouse. When this data is available, you can write custom reports to see this information.

The Identity Reporting Module is tightly integrated with *Event Auditing Service (EAS)*. EAS is a software component that captures log events associated with actions performed in several Novell products, including the reporting module, the Roles Based Provisioning Module (RBPM), the Role Mapping Administrator (RMA), NMAS, Identity Manager, and the Identity Vault. These events are stored in a separate schema within the warehouse. You have the option to forward these events to *Sentinel*. If you choose to forward events, you can then use Sentinel to create a holistic view of all of the activity within your enterprise. Sentinel lets you assimilate logs and other security information from heterogeneous input sources, giving you visibility and accountability into the various activities within the enterprise.

You can access the user interface for the reporting module directly or launch it from the Work Dashboard within the User Application.

NOTE: If you want to be able to launch it from the Work Dashboard, you need to have your Configuration Administration specify the URL for the reporting module on the *Administration* tab. The Configuration Administrator needs to specify the URL in the *Novell Identity Manager Reporting Module URL* field within the Provisioning UI Display Settings page. In addition, you need to have the *Access Reporting Module* navigation permission. The Report Administrator is given this permission by default.

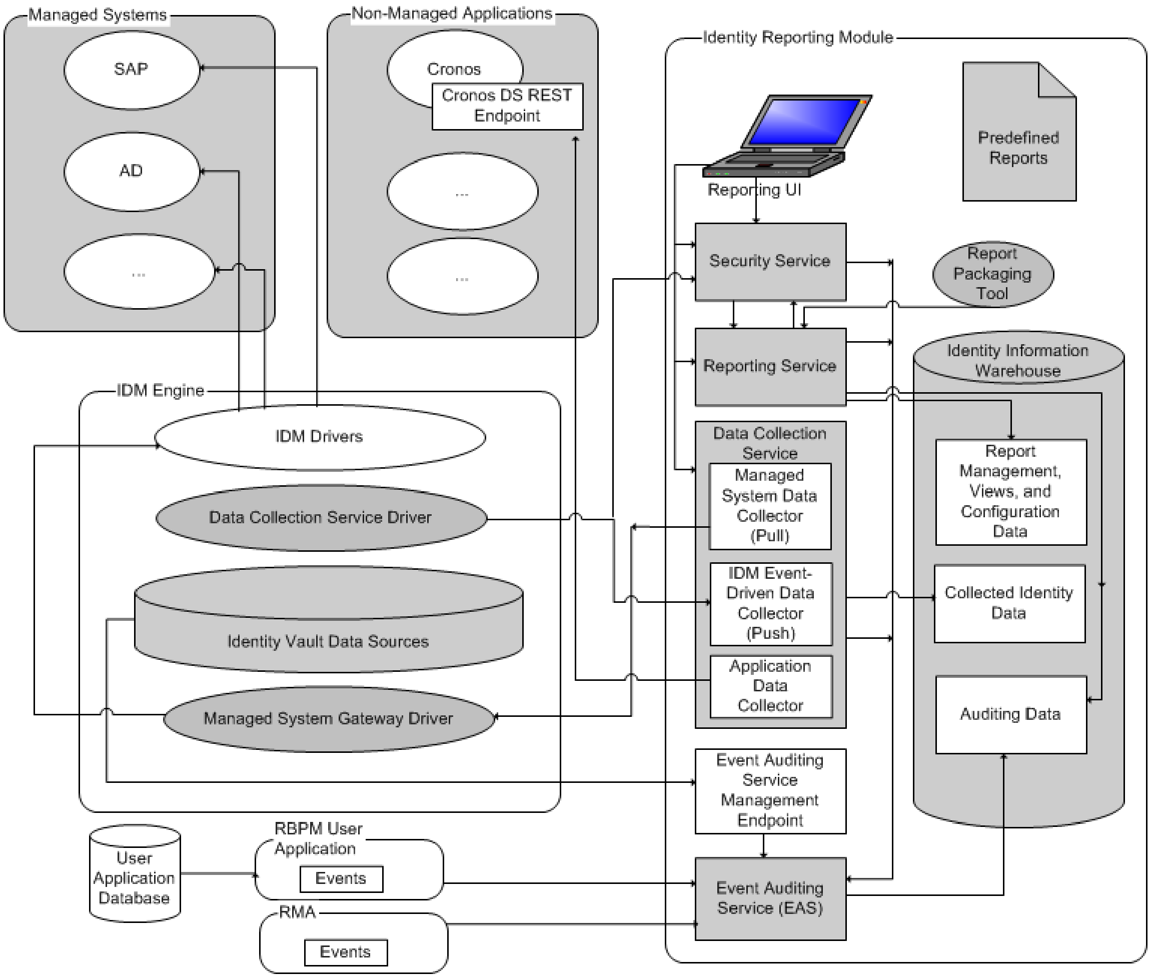
Standard Edition Identity Manager 4.0.2 Standard Edition provides a subset of the reporting features available with Advanced Edition. The restrictions that apply to Standard Edition are listed below:

- The Managed System Gateway Driver is disabled in Standard Edition.
- Reports generated with Standard Edition show Identity Vault data only, and do not show data about managed (connected) systems.
- Standard Edition does not provide the ability to collect historical state data for reporting. With Standard Edition, you can only see current state data.
- Some of the reports provided with the product are only meaningful if you have purchased the Advanced Edition. The reason for this is that some of the reports report on data that is not available in Standard Edition, such as roles, resources, and workflow processes. For more information, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm402/idm_reports/data/bookinfo.html).

1.2 Identity Manager Reporting Architecture

The following diagram shows the components of the Identity Manager reporting architecture:

Figure 1-1 *Reporting Architecture*


Managed Systems
SAP
AD
...
Non-Managed Applications
Cronos
Cronos DS REST Endpoint
...
...
Identity Reporting Module
Reporting UI
Predefined Reports
Security Service
Report Packaging Tool
Reporting Service
Identity Information Warehouse
Data Collection Service
Managed System Data Collector (Pull)
IDM Event-Driven Data Collector (Push)
Application Data Collector
Report Management, Views, and Configuration Data
Collected Identity Data
Auditing Data
Event Auditing Service Management Endpoint
Event Auditing Service (EAS)
IDM Engine
IDM Drivers
Data Collection Service Driver
Identity Vault Data Sources
Managed System Gateway Driver
User Application Database
RBPM User Application
Events
RMA
Events

Each of the major components is described below:

Table 1-1 *Major Components of the IDM Reporting Architecture*

Component	**Description**
Identity Reporting Module	Browser-based application that generates reports by making calls to the Reporting Service.
Predefined Reports	The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives you the option to import custom reports defined in a third-party tool. For details on the predefined reports, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm402/idm_reports/data/bookinfo.html).
Report Packaging Tool	To facilitate the process of creating new reports, Novell provides the Novell Identity Manager Report Packaging Tool. You can customize reports in iReport and use the Reporting Packaging Tool to package them for use within the reporting module.

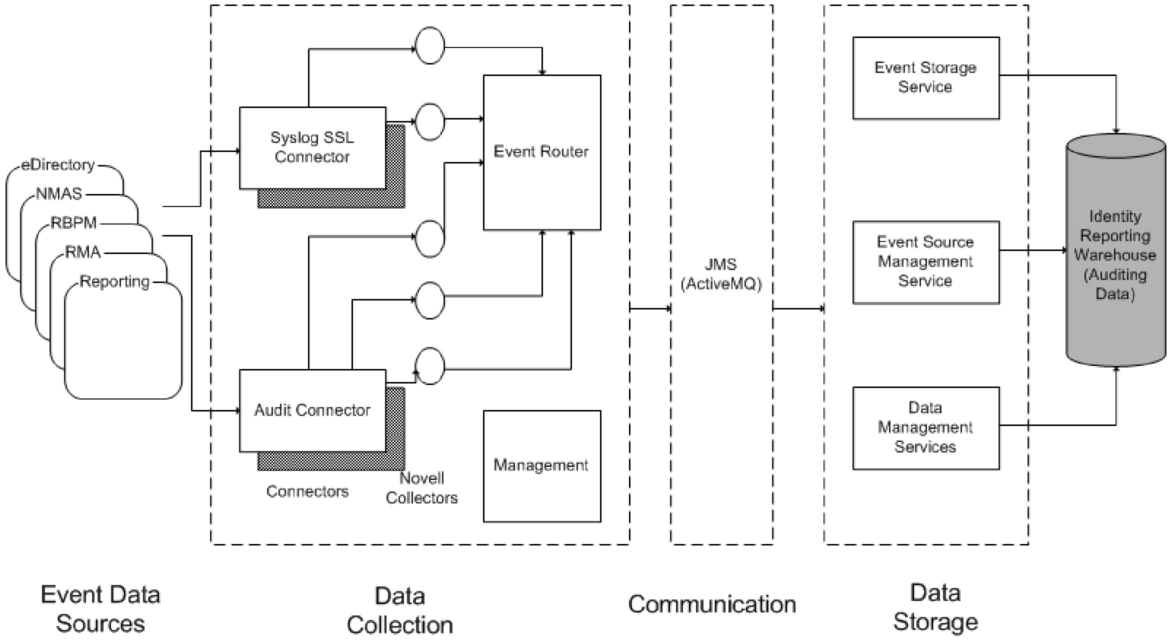
Component	Description
Reporting Service	Service that retrieves the data needed for report generation from the Identity Information Warehouse, which contains all report management information (such as report definitions and schedules), database views, and configuration information required for reporting. To produce reports, the Reporting Service invokes the JasperReports engine, which compiles and executes report definitions according to schedules defined by the Report Administrator.
Identity Information Warehouse	Repository for the following kinds of information: ◆ Report management information (such as report definitions, report schedules, and completed reports), database views used for reporting, and configuration information. This information is stored in tables within the idm_rpt_cfg schema. ◆ Identity data collected by the Managed System Data Collector, IDM Event-Driven Data Collector, and Application Collector. This data is stored in tables within the idm_rpt_data schema. ◆ Auditing data, which includes events collected by the Event Auditing Service (EAS). This data is stored in tables within the public schema. The Identity Information Warehouse stores its data in the Security Information and Event Management (SIEM) database.
Data Collection Service	Service that collects information from various sources within an organization. The Data Collection Service includes three subservices: ◆ The *Managed System Data Collector* uses a pull design model to retrieve data from one or more Identity Vault data sources. The collection runs on a periodic basis, as determined by a set of configuration parameters. To retrieve the data, the collector calls the Managed System Gateway Driver. ◆ The *IDM Event-Driven Data Collector* uses a push design model to gather event data captured by the Data Collection Service Driver. ◆ The *Application Data Collector* retrieves data from one or more non-managed applications by calling a REST endpoint written specifically for each application. Non-managed applications are applications within your enterprise that are not connected to the Identity Vault.

Component	Description
Data Collection Service Driver	Driver that captures changes to objects stored in an Identity Vault, such as accounts, roles, resources, groups, and team memberships. The Data Collection Service Driver registers itself with the Data Collection Service and pushes change events (such as data synchronization, add, modify, and delete events) to the Data Collection Service. The information captured records changes to these objects: ◆ User accounts and identities ◆ Roles and role levels (hierarchical relationships between roles) ◆ Groups **NOTE:** The reporting module does not support dynamic groups and only generates reports on static group data. ◆ Group memberships ◆ Provisioning Request Definitions (PRDs) ◆ Separation of Duties (SoDs) definitions and violations ◆ User entitlement associations ◆ Resource definitions and resource parameters ◆ Role and resource assignments ◆ Identity Vault entitlements, entitlement types, and drivers
Managed System Gateway Driver	Driver that collects information from managed systems. To retrieve the managed system data, the driver queries the Identity Vault. The data retrieved includes the following: ◆ List of all managed systems ◆ List of all accounts for the managed systems ◆ Entitlement types, values, and assignments (groupings), and user account profiles for the managed systems
Security Service	Service that controls access to all other services within the reporting module. The Security Service includes these key components: ◆ A *stand-alone authentication service* that provides several functions through REST, including programmable authentication, token validation, token expiration notification, and attribute retrieval for an identity. ◆ An *authentication module within the core service* that performs internal functions such as performing authentication within the scope of the core service and retrieving additional identity attributes. ◆ An *authorization module within the core service* that controls what an authenticated user can do with reporting resources. This module defines access control policies for resources and determines the permissions based on attributes of the authenticated user, access control policy, and the resource being accessed.

Component	Description
Event Auditing Service (EAS)	Captures log events associated with actions performed in several Novell products, including the reporting module, the Roles Based Provisioning Module (RBPM), the Role Mapping Administrator (RMA), and eDirectory. These events are stored in the public schema within the warehouse. You have the option to forward these events to Sentinel. If you choose to forward events, you can then use Sentinel to create a more holistic view of all of the activity within your enterprise. Sentinel lets you assimilate logs and other security information from various heterogeneous input sources, giving you visibility and accountability into the various activities within the enterprise.
Identity Vault Data Sources	Repositories for identity information. The Identity Reporting Module allows you to report on state information in the Identity Vault, such as which users have been provisioned with particular resources, or which users have been assigned to particular roles. You can report on current and past data from the Identity Vault. The Identity Vault Data Sources page allows you to specify which Identity Vaults you want to report on, and provide information about where the reporting module can find these vaults. You can include data sources for one or more Identity Vaults on the Identity Vault Data Sources page.
Managed Systems	A system in an enterprise that is connected to the Identity Vault with an Identity Manager driver. The Identity Reporting Module allows you to report on state information about the managed systems. For example, the reports allow you to determine that a particular user known to the Identity Vault exists in Active Directory. The Identity Reporting Module allows you to report on current and past data from managed systems.
Applications	Any non-managed application running in an enterprise. A non-managed application is an application that is not connected to the Identity Vault. To include information from a non-managed application, you need to implement a REST endpoint, as outlined in Section 13.2, "Non-Managed Application REST API," on page 207. You also need to configure a custom data source for the application on the Non-Managed Application Data Sources page within the reporting module, as described in Section 9.3, "Defining the Settings for Non-Managed Applications," on page 153.

The following diagram shows the components of the EAS architecture:

Figure 1-2 *EAS Architecture*



EAS provides these connectors for capturing events from various Novell data sources:

- Syslog SSL Connector
- Syslog UDP Connector
- Audit Connector

Different Novell applications use different connectors:

- The Role Mapping Administrator (RMA) can be configured to use the Audit Connector or the Syslog SSL Connector.
- Identity Manager and eDirectory can be configured to use the Audit Connector or the Syslog SSL Connector.
- RBPM uses the Audit Connector.

When you configure EAS to work with the reporting module, you need to provide ports for these connectors on the *Auditing* page within the user interface for the reporting module.

1.3 Basic Setup and Configuration

Before you begin using the Identity Reporting Module, you need to install the module, as described in Chapter 2, “Installation and Driver Configuration,” on page 19.

1.4 Working in the Identity Reporting Module

The user interface for the Identity Reporting Module runs within a Web browser. It uses familiar components and controls to present information and allow the user to perform actions quickly and easily.

How styles are rendered: The reporting module uses a set of default styles to control the appearance of the reporting user interface. However, you can provide your own styles to customize the user interface. The reporting client WAR supports customization through a file called `custom.css`. It looks for this file in a directory called `novl_rpt_custom` in the user's home directory. This is is the home directory of the user that started the Application Server on the server where the Application Server is running. For example, with a SLES install, this would be root so the home directory is `/root`. If that file exists, the reporting client uses it to override any styles for the reporting user interface.

You can determine whether the file can be found by entering the following URL:

```
http://[report.server]:8180/IDMRPT/custom/custom.css
```

How the Back button functions: In the Identity Reporting module, the *Back* button takes you to your previous application or to the last Web site you loaded, not to the last page you visited within the reporting module. All navigation within the reporting module takes place within the initially loaded page.

1.5 Security Considerations

This section describes security considerations you should be aware of when working with the reporting module.

1.5.1 Authentication Token Exposure

On Windows, the authentication token used for login operations is exposed as a URL parameter in Internet Explorer’s address bar when the user opens a PDF file for a report. This happens because a link to a PDF file is handled by the browser, not by JavaScript.

Although you might want to copy and paste the link to a report PDF, you should not do this. If the token has not yet expired and the user has not logged out, the receiver of the link, who might not be a legitimate user, is able to access the reporting module by using the token given to the legitimate user.

IMPORTANT: Do not try to copy and send links within the reporting module, because this action might potentially expose your login information.

2 Installation and Driver Configuration

This section provides instructions for installing the Identity Reporting Module by using the stand-alone installers.

- Section 2.1, "About the Identity Reporting Installation Process," on page 19
- Section 2.2, "Running the EAS Install Program," on page 25
- Section 2.3, "Running the Identity Reporting Module Install Program," on page 35
- Section 2.4, "Configuring the Drivers," on page 58

2.1 About the Identity Reporting Installation Process

The process of installing the Identity Reporting Module requires that you run two separate install programs:

- Event Auditing Service (EAS) install program
- Identity Reporting Module install program

You need to run the EAS install program before running the Identity Reporting Module.

NOTE: You must have the Roles Based Provisioning Module (RBPM) installed and configured before beginning the installation of the reporting module. You must also install the User Application driver and assign the Report Administrator role to any users you want to be able to access the reporting module.

The remaining topics in this section provide instructions for running the stand-alone versions of each of these install programs. You can also use the Integrated Installer for Identity Manager, which runs these install programs for you. For more information, see the *Identity Manager 4.0.2 Integrated Installation Guide* (http://www.netiq.com/documentation/idm402/idm_integrated_install/index.html?page=/documentation/idm402/idm_integrated_install/data/front.html)

The Identity Reporting Module relies on the following drivers:

- Identity Manager Driver for Data Collection Service
- Identity Manager Managed System Gateway Driver

These drivers are installed automatically by the Integrated Installer for Identity Manager, so the steps provided in this section are only necessary if you are running the stand-alone versions of the install programs.

- Section 2.1.1, "System Requirements," on page 20
- Section 2.1.2, "About the EAS Installer," on page 22
- Section 2.1.3, "About the Identity Reporting Installer," on page 24
- Section 2.1.4, "Users Created During the Installation Process," on page 24

2.1.1 System Requirements

The Event Auditing Service (EAS) runs on SUSE Linux Enterprise Server 11 (32-bit and 64-bit), as well as Red Hat Enterprise Linux 5.7 and 6.0 (32-bit and 64-bit). You need to launch the installer for EAS on a SUSE Linux Enterprise Server or Red Hat Enterprise Linux machine.

NOTE: EAS requires that ksh be installed on the SLES machine. A standard installation of SLES includes ksh. If you remove it, the init.d script will not execute properly.

The reporting module can be installed and run in a variety of environments.

IMPORTANT: The reporting module must have an exclusive EAS running on a separate Linux machine. You cannot have multiple reporting instances communicating with a single EAS environment.

To use the reporting module, you must meet the system requirements listed in Table 2-1 on page 21. Certified platforms have been fully tested. Supported platforms are expected to be functional, but have not been fully tested.

Table 2-1 *System Requirements for the Identity Reporting Module*

Required System Component	System Requirements
Application Server	The reporting module runs on JBoss, WebSphere, and WebLogic. The reporting module with JBoss Enterprise Application Platform 5.1.2 (or JBoss Community Edition 5.1.0) requires JRE 1.6.0_31 from Sun and is certified on: ◆ Windows Server 2003 SP2 (32-bit) ◆ Windows Server 2008 R2 SP1 (64-bit only) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Open Enterprise Server 11 (64-bit only) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.0 (32-bit and 64-bit) The reporting module on WebSphere 7.0 requires the IBM J9 VM (build 2.4, J2RE 1.6.0). It is certified on these platforms: ◆ Windows Server 2003 SP2 (32-bit only) ◆ Windows Server 2008 R2 SP1 (64-bit only) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Open Enterprise Server 11 (64-bit only) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.0 (32-bit and 64-bit) The reporting module on WebLogic 10.3.5 (11gR1 requires JRockit JVM 1.6.0_05 and is certified on these platforms. ◆ Windows Server 2003 SP2 (32-bit) ◆ Windows Server 2008 R2 SP1 (64-bit) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Open Enterprise Server 11 (64-bit only) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit and 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit and 64-bit) ◆ Red Hat Linux 5.7 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux 6.0 (32-bit and 64-bit)

Required System Component	System Requirements
Virtualization	The reporting module supports virtualization on the following platforms as long as the guest operating system is one that is certified by the User Application: ◆ Red Hat Enterprise Linux Virtualization ◆ Xen ◆ VMWare ESX/ESXi ◆ Windows Server 2008 R2 Virtualization with Hyper-V
Database Server	PostgreSQL 8.4.3. (This is the only database certified with the reporting module.)
Metadirectory	eDirectory 8.8.7 with Identity Manager 4.0.2 For the list of certified operating systems, see the Identity Manager and eDirectory documentation.
Browser	The User Application is certified with both Firefox and Internet Explorer, as described below. FireFox 9 is certified on: ◆ Windows XP with SP3 ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSUSE 11.2 ◆ Apple Mac Internet Explorer 8 is certified on: ◆ Windows XP with SP3 Internet Explorer 9 is certified on: ◆ Windows 7

Uninstalling EAS or the Identity Reporting Module In order to conserve disk space, the installation programs for EAS and the Identity Reporting Module do not install a Java virtual machine (JVM). Therefore, if you need to uninstall one or more components, you need to be sure you have a JVM available and also make sure that the JVM is in the PATH. If you encounter an error during an uninstall, add the location of a JVM to the local PATH environment variable and run the uninstall program again.

2.1.2 About the EAS Installer

The installer for the Event Auditing Service (EAS) performs these functions:

- Installs and optionally configures the service
- Configures the user who is able to perform administration tasks for the service
- Configures the DBA used by the service to interact with the database
- Allows you to define the port on which the PostgreSQL database runs

EAS runs on SUSE Linux Enterprise Server 11, as well as Red Hat Enterprise Linux 6.0 (32-bit and 64-bit). You need to launch the installer for EAS on one of these certified platforms.

Check the clocks before running the EAS installer If the times of your machines are not in synchronization when you install the Event Auditing Service (EAS), there may be problems with your configuration. You cannot install EAS on Windows. It must be installed on Linux. Therefore, the Linux server where EAS is installed must be synchronized with the machine where you are installing the rest of your components.

Prerequisites for Red Hat Enterprise Linux or SUSE Linux

This section outlines several prerequisites for installing EAS on Red Hat Enterprise Linux or SUSE Linux. Before installing EAS on RHEL or SLES, ensure that these prerequisites are met.

These prerequisites apply to RHEL 5.7 and 6.0.

Verify that the hostname returns properly In order for the installer to work properly, the Linux system must be able to properly return the hostname. To do this, add the hostname to the `/etc/hosts` file to the line containing the IP address (for example, 127.0.0.1), then enter `hostname -f` to make sure that the hostname is displayed properly.

Change the Kernel SHMMAX Parameter to Enable PostgreSQL You must change the kernel SHMMAX parameter to enable the database to run on the Linux server. To change the kernel SHMMAX parameter on RHEL 6.x, append the following information to the `/etc/sysctl.conf` file.

```
# for Sentinel Postgresql
kernel.shmmax=1073741824
```

NOTE: The value shown above for the kernel SHMMAX parameter is a minimum value. Your system may require more memory.

To set the SHMMAX parameter on RHEL 6.0, execute these commands:

```
cd /proc/sys/kernel
echo new_val_to_set > shmmax
```

For more information, see "Managing Kernel Resources" in the PostgreSQL documentation (http://www.postgresql.org/docs/8.2/static/kernel-resources.html).

Configure the Firewall for Syslog Port Forwarding If you want to forward the syslog file, you must configure the server for port forwarding. The installers give you the option to configure the server. However, if your are not able to configure the server during the installation process, execute the following command:

```
iptables -t nat -A PREROUTING -p udp --destination-port 514 -j REDIRECT –toports
1514
```

Check for Openssl libraries version changes EAS requires Openssl libraries, usually `libssl.so.0.9.8` and `libcrypto.so.0.9.8`. Before installing EAS, see if the version of the .so files matches. Otherwise, create a soft-link.

In Red Hat Enterprise Linux 6.x, these libraries are found under `/usr/lib` and `/usr/lib64` for 32-bit and 64-bit operating systems, respectively. RHEL 6.x may also use a bundled upgrade version such as: `libssl.so.1.0.0`.

```
ln -s libssl.so.1.0.0 libssl.so.0.9.8
ln -s libcrypto.so.1.0.0 libcrypto.so.0.9.8
```

In Red Hat Enterprise Linux 5.x, these libraries are found under `/lib` and `/lib64` for 32-bit and 64-bit OS respectively.

```
ln -s libssl.so.0.9.8e libssl.so.0.9.8
ln -s libcrypto.so.0.9.8e libcrypto.so.0.9.8
```

Check KornShell availability KornShell is usually bundled with all of the Linux operating system environments. However, you should make sure it is installed, since some of the installation scripts use KornShell (found at `/bin/ksh`).

2.1.3 About the Identity Reporting Installer

The installer for the reporting module performs these functions:

- Allows you to choose an application server platform
- Deploys the client WAR file to the application server

  This WAR file contains the user interface components for reporting.
- Deploys the core WAR file

  This WAR file contains the core REST services needed for reporting.
- Deploys the authentication services WAR file

  This WAR file contains the authentication services, which control authentication to the reporting module.
- Defines the location of the server for the Event Auditing Service (installed separately)
- Creates the reporting schema in the Security Information and Event Management (SIEM) database
- Configures the PostgreSQL JDBC driver that connects to the SIEM database
- Configures the authentication services for the reporting module
- Configures the e-mail delivery system for the reporting module
- Configures the core reporting services for the reporting module

Check the clocks before running the reporting installer Before running the installer, be sure that all servers have the same time. If the times of your machines are not in synchronization when you install the Identity Reporting Module, some reports might be empty when executed. This might occur if the Metadirectory and reporting servers are running on different machines, and the time stamp value of the Metadirectory server is ahead compared to the reporting server. This happens only for new users when the time between the servers is out of synchronization. If a user is created and then modified, the reports are populated with data.

Changing from Standard Edition to Advanced Edition If you change from the Standard Version to the Advanced Edition, the version change for the reporting module might not show immediately. The version change occurs after the next batch of events is processed.

2.1.4 Users Created During the Installation Process

The EAS installation process creates a *novell* group and *novell* user. The novell user is created without a password. If you want to log in as the novell user later (for example, to install patches), create a password for this user after the installation is completed.

In addition, when you install EAS and the Identity Reporting Module, the following database users are created automatically:

Table 2-2 *Database Users Created By the Install Process*

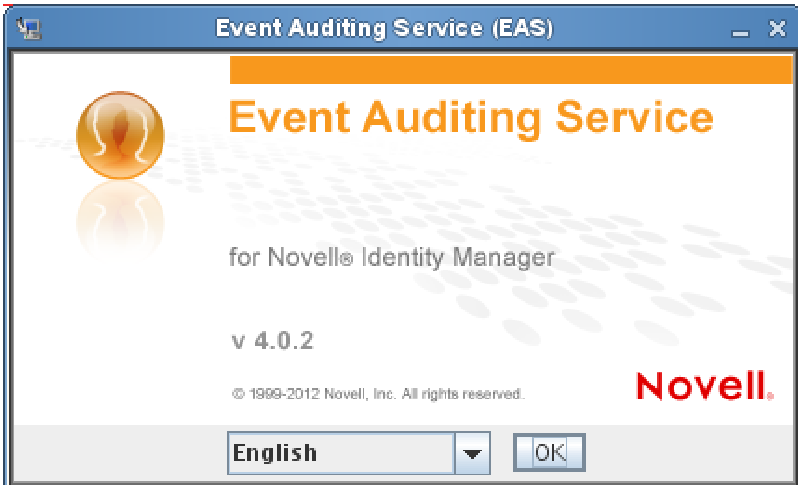
User name	Description
dbauser	Administrator of the PostgreSQL server and owner of the EAS schema and views.
admin	User identity for use with EAS administrative utilities.
idmrptsrv and idmrptuser	Owner of the Identity Reporting schema and views, as well as credentials used for Identity Reporting database connectivity.
rptuser and appuser	Reserved for compatibility with Sentinel.

2.2 Running the EAS Install Program

1 Launch the installer for SUSE Linux Enterprise Server 11 or Red Hat Enterprise Linux 6.0:

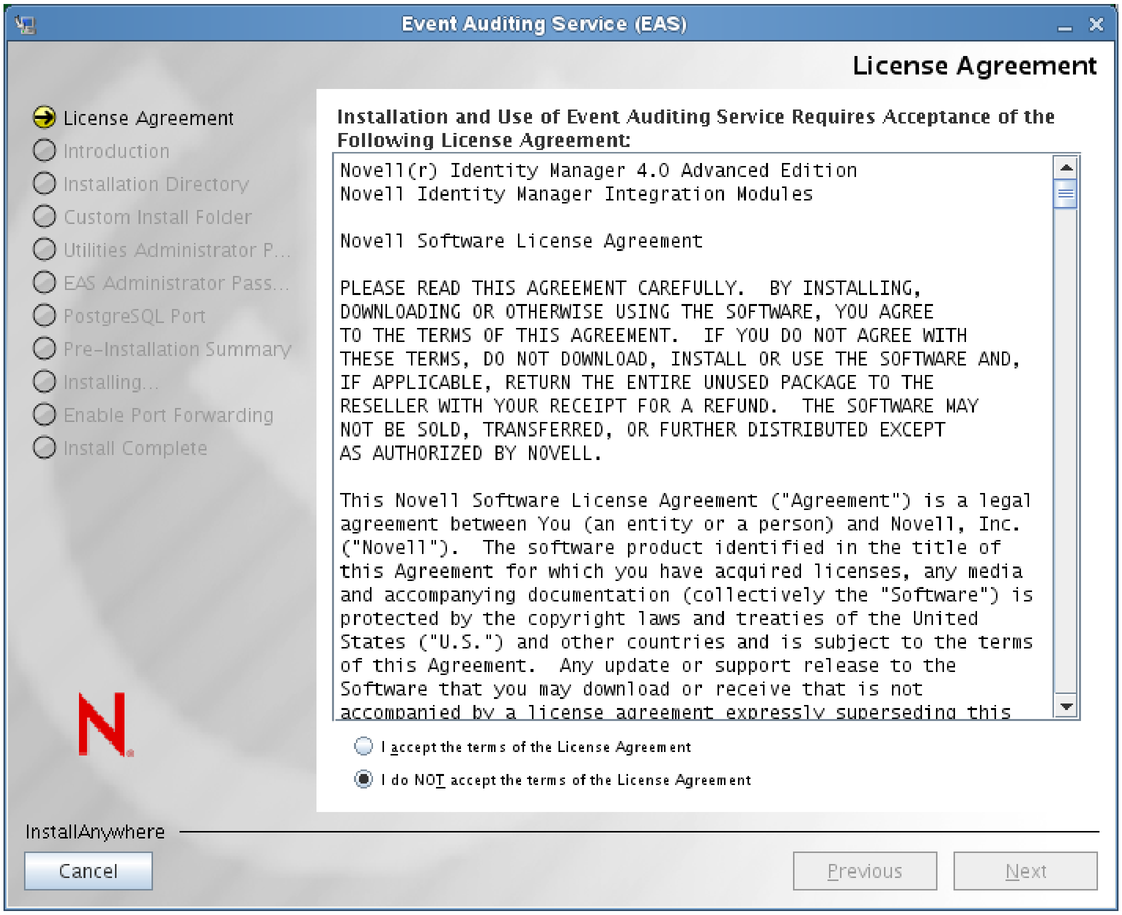
```
./EASInstall.bin
```

When the installer launches, you are prompted for the language:


Event Auditing Service (EAS)
Event Auditing Service
for Novell® Identity Manager
v 4.0.2
© 1999-2012 Novell, Inc. All rights reserved.
Novell.
English
OK

2 Choose the language for your installation and click *OK*.

The installer displays the License Agreement screen:



Installation and Use of Event Auditing Service Requires Acceptance of the Following License Agreement:

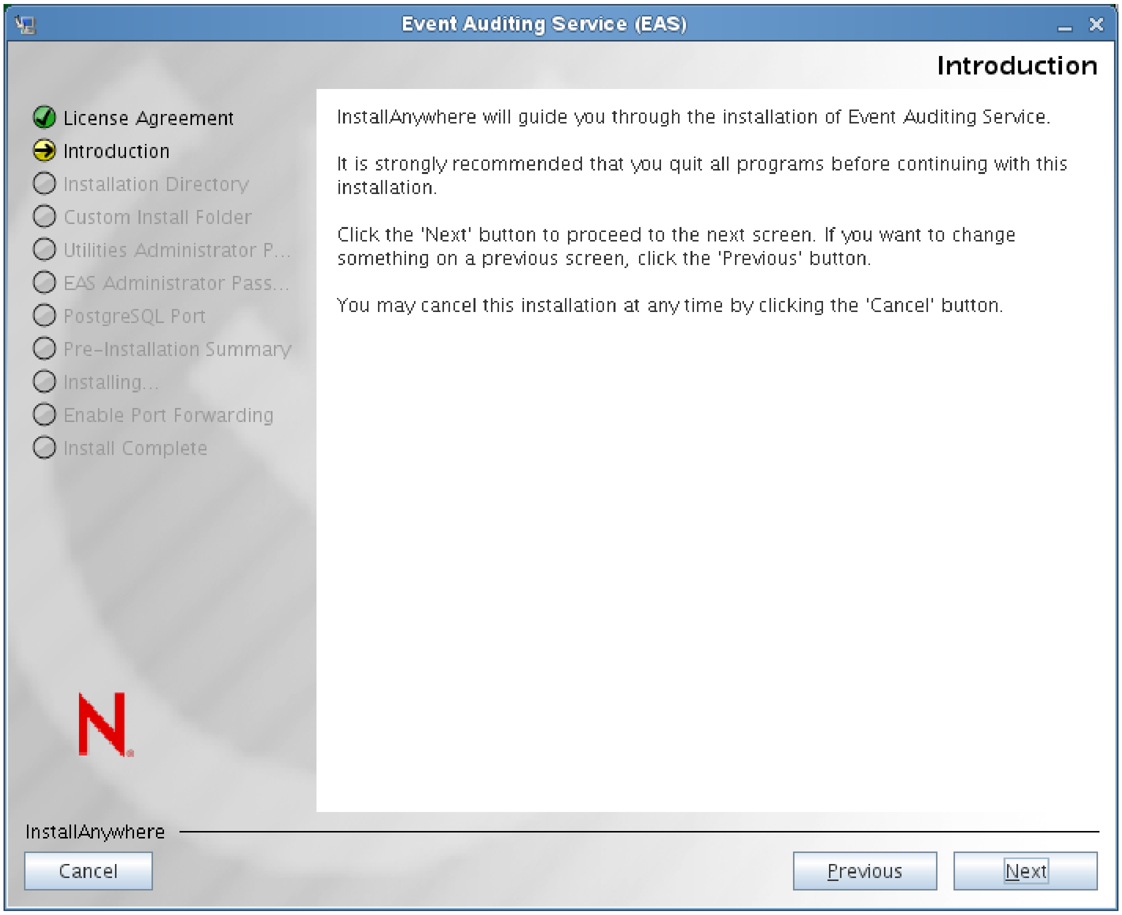
```
Novell(r) Identity Manager 4.0 Advanced Edition
Novell Identity Manager Integration Modules

Novell Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY.  BY INSTALLING,
DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU AGREE
TO THE TERMS OF THIS AGREEMENT.  IF YOU DO NOT AGREE WITH
THESE TERMS, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE AND,
IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE
RESELLER WITH YOUR RECEIPT FOR A REFUND.  THE SOFTWARE MAY
NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED EXCEPT
AS AUTHORIZED BY NOVELL.

This Novell Software License Agreement ("Agreement") is a legal
agreement between You (an entity or a person) and Novell, Inc.
("Novell").  The software product identified in the title of
this Agreement for which you have acquired licenses, any media
and accompanying documentation (collectively the "Software") is
protected by the copyright laws and treaties of the United
States ("U.S.") and other countries and is subject to the terms
of this Agreement.  Any update or support release to the
Software that you may download or receive that is not
accompanied by a license agreement expressly superseding this
```

○ I accept the terms of the License Agreement

● I do NOT accept the terms of the License Agreement

3 Confirm the license agreement and click *Next*.

The installer displays the Introduction screen:



InstallAnywhere will guide you through the installation of Event Auditing Service.

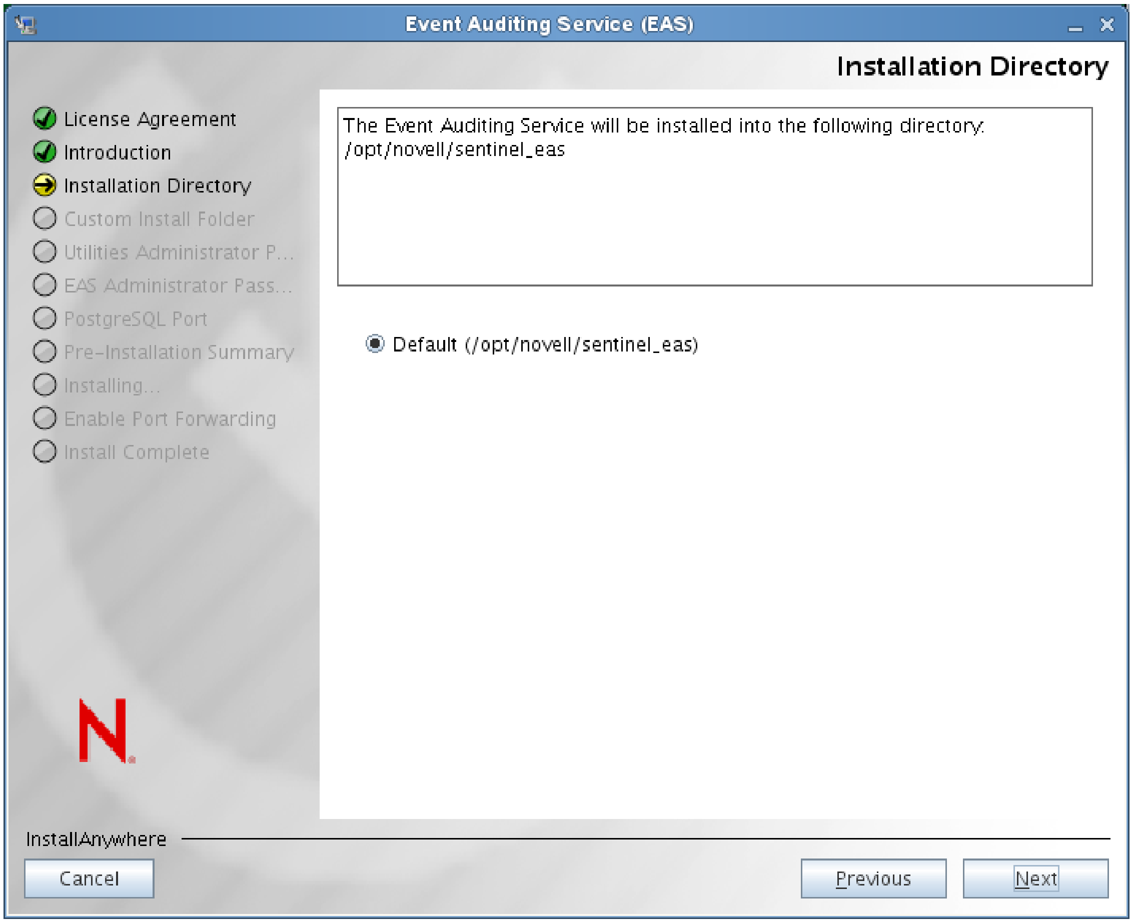
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

4 Click *Next*.

The installer displays the Installation Directory screen:



Event Auditing Service (EAS)

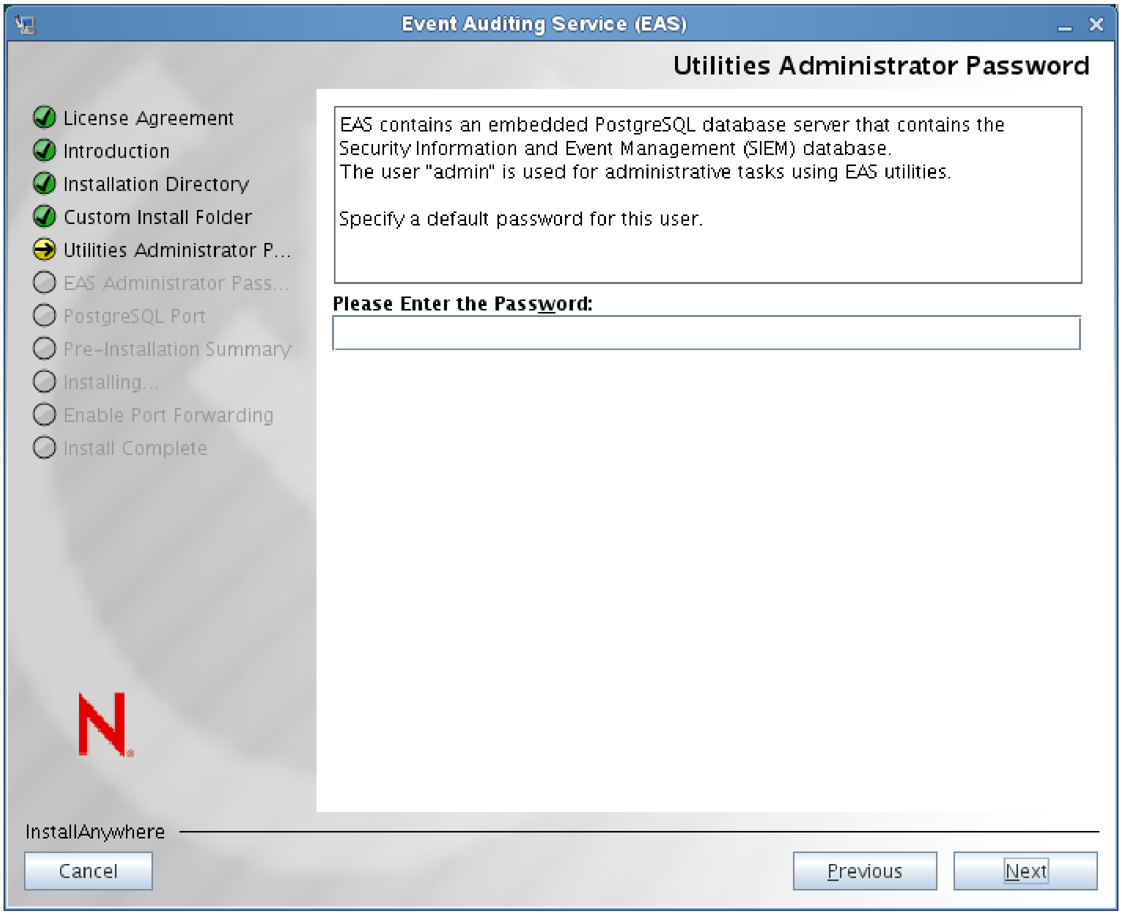
Installation Directory

The Event Auditing Service will be installed into the following directory:
/opt/novell/sentinel_eas

● Default (/opt/novell/sentinel_eas)

5 Choose *Default* to install the EAS packages in the default directory location, then click *Next*.

The installer displays the Utilities Administrator Password screen:



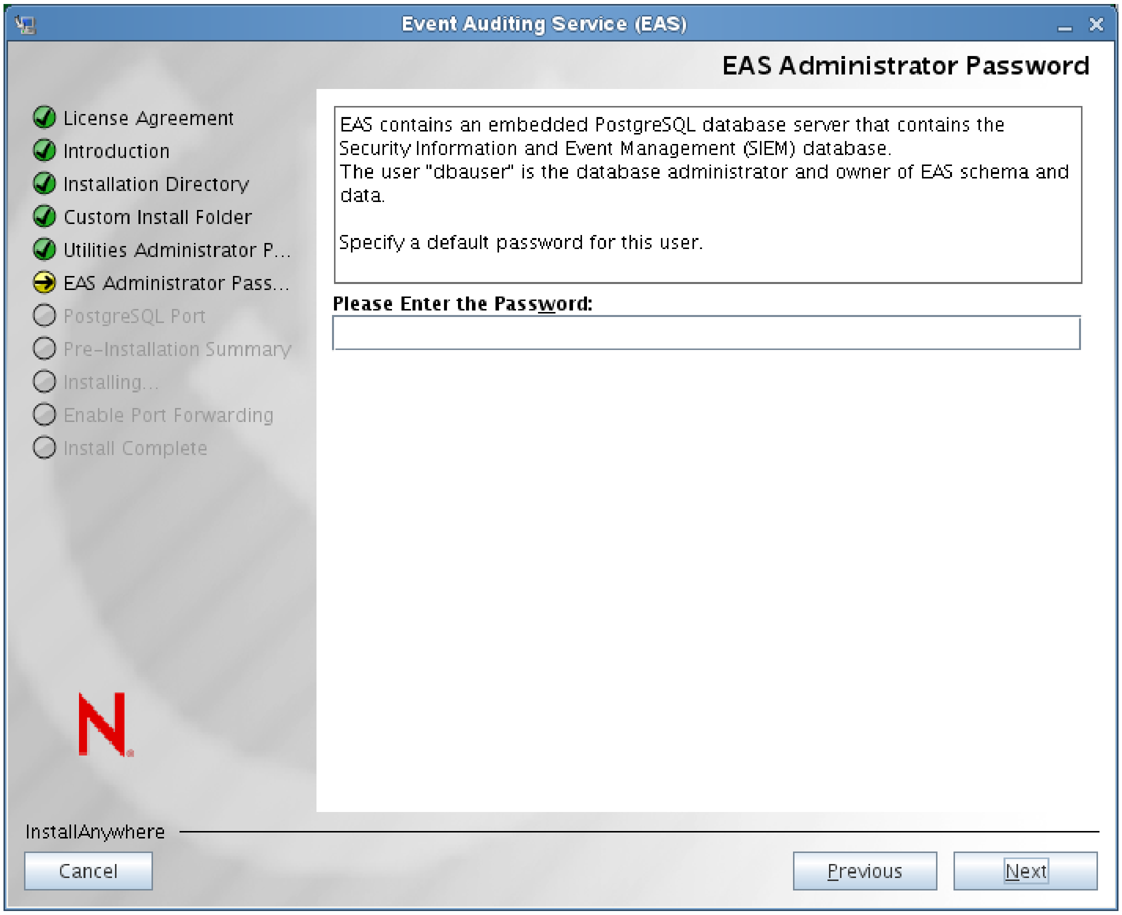
EAS contains an embedded PostgreSQL database server that contains the Security Information and Event Management (SIEM) database.
The user "admin" is used for administrative tasks using EAS utilities.

Specify a default password for this user.

Please Enter the Password:

6 Type the administrator's password and click *Next*.

The installer displays the EAS Administrator Password screen:



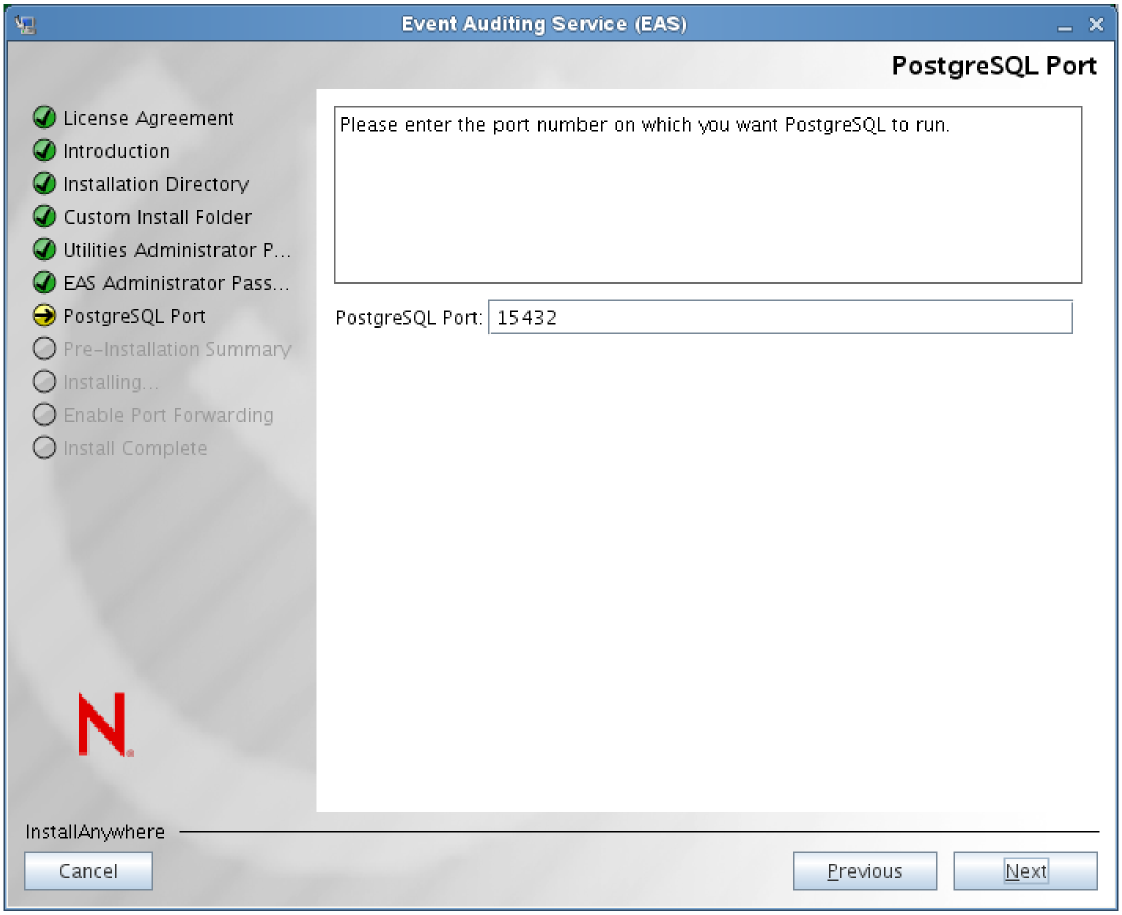
EAS contains an embedded PostgreSQL database server that contains the Security Information and Event Management (SIEM) database.
The user "dbauser" is the database administrator and owner of EAS schema and data.

Specify a default password for this user.

Please Enter the Password:

7 Type the EAS Administrator's password and click *Next*.

The installer displays the PostgreSQL Port screen:

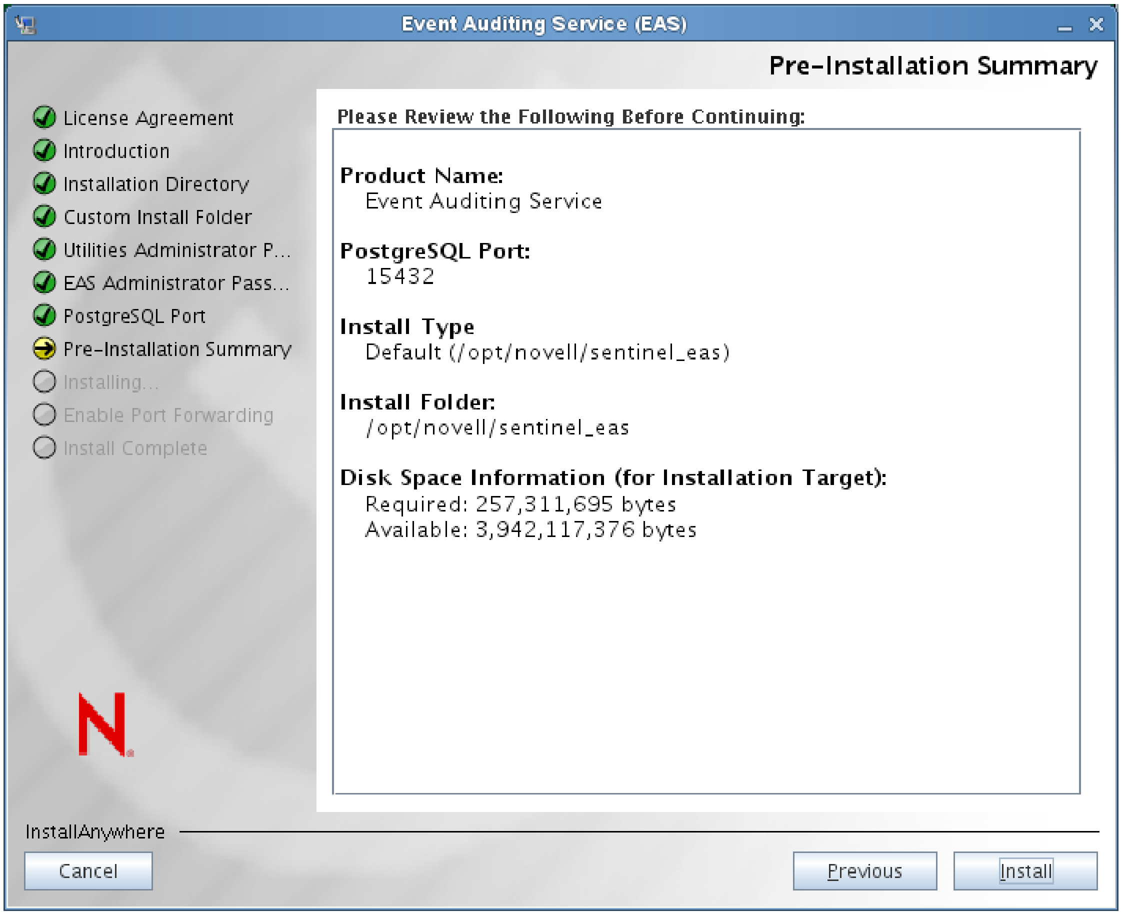


Please enter the port number on which you want PostgreSQL to run.

PostgreSQL Port: 15432

8 Type the port number for PostgreSQL to run on and click *Next*.

The installer displays the Pre-Installation Summary screen:



Please Review the Following Before Continuing:

Product Name:
Event Auditing Service

PostgreSQL Port:
15432

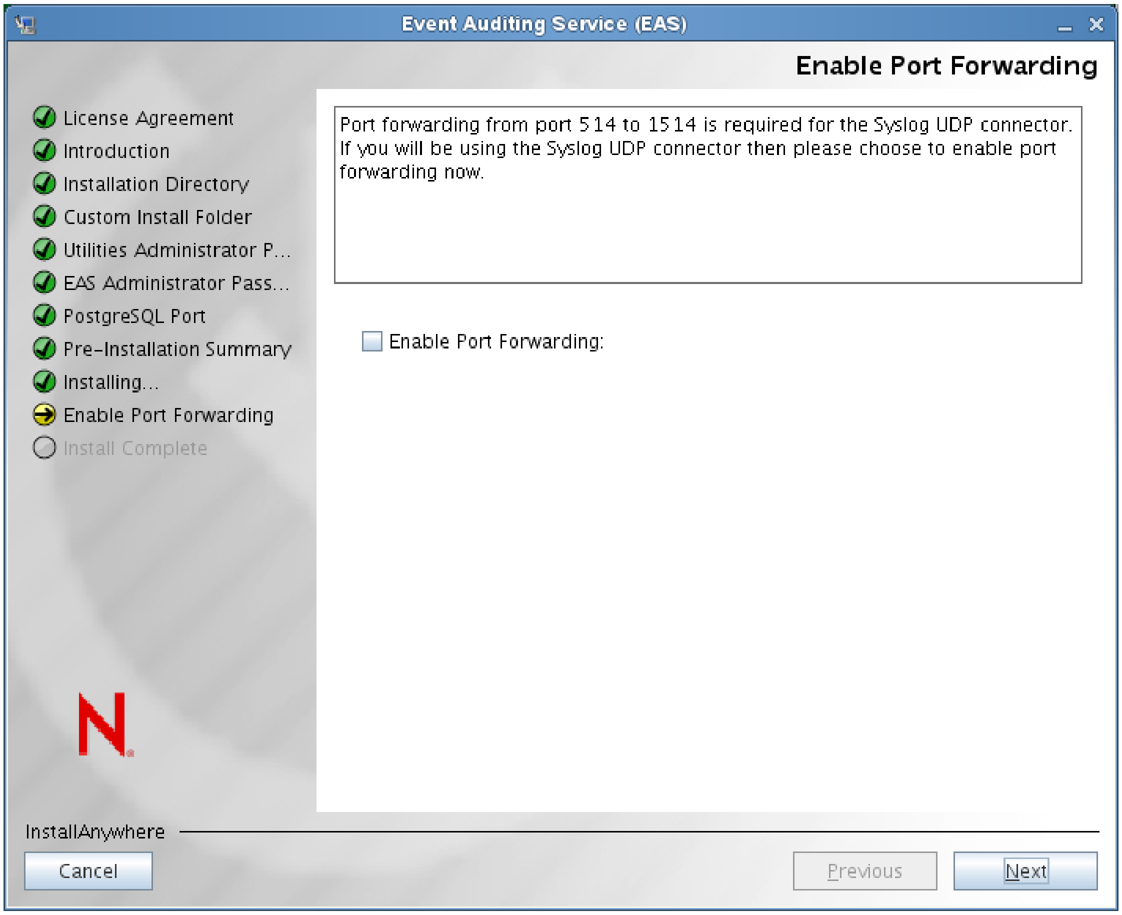
Install Type
Default (/opt/novell/sentinel_eas)

Install Folder:
/opt/novell/sentinel_eas

Disk Space Information (for Installation Target):
Required: 257,311,695 bytes
Available: 3,942,117,376 bytes

9 Click *Install* to begin copying files. If you need to change any of your installation settings, click *Previous*.

The installer displays the Enable Port Forwarding screen:

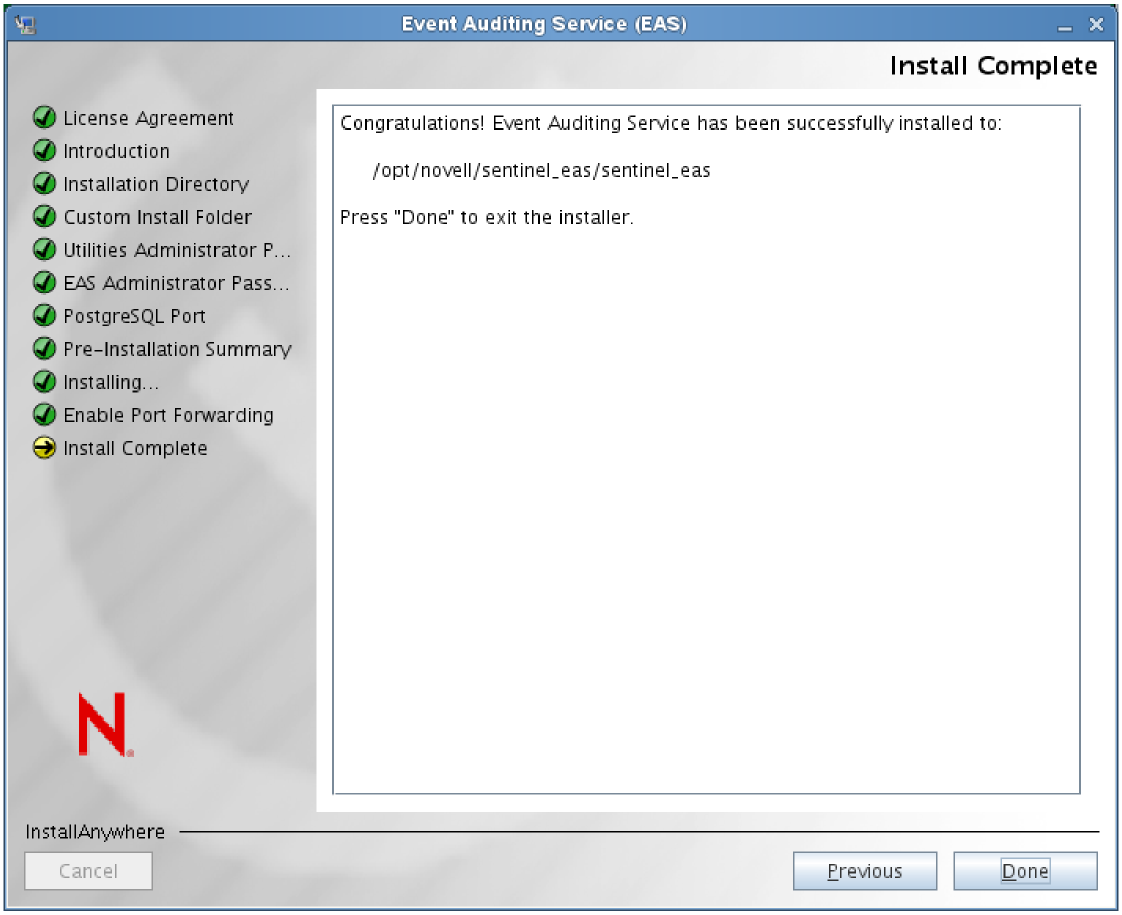


Port forwarding from port 514 to 1514 is required for the Syslog UDP connector. If you will be using the Syslog UDP connector then please choose to enable port forwarding now.

□ Enable Port Forwarding:

10 Select *Enable Port Forwarding* if you plan to use the Syslog UDP connector, then click *Next*.

The installer displays the Install Complete screen:



Congratulations! Event Auditing Service has been successfully installed to:

/opt/novell/sentinel_eas/sentinel_eas

Press "Done" to exit the installer.

11 Click *Done* to finish the installation process.

2.2.1 Running the Installer in Silent Mode

You can run the EAS installer in silent mode. Before running the installer, you need to edit the properties file for the installer. Once you've edited the properties file, launch it with this command:

```
./EASInstall.bin -i silent -f <path to the properties file>
```

For example:

```
./EASInstall.bin -i silent -f /root/Software/eas_configure.properties
```

2.2.2 Setting Passwords in the Environment for a Silent Install

If you do not want to specify the passwords in the properties file, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the properties file. This can provide some additional security.

The following passwords need to be set for the EAS installer:

- ADMIN_PWD
- DBA_PWD

To set a password on Linux, use the `export` command, as shown in the following example:

```
export ADMIN_PWD=myPassWord
```

2.2.3 Upgrading from Novell Audit

If you are upgrading from Novell Audit, you need to be sure that the `logevent.conf` file points to EAS and uses the correct ports. This is necessary to make sure that events are routed to EAS rather than to the Novell Auditing server.

2.3 Running the Identity Reporting Module Install Program

To run the installation program for the reporting module:

1. Launch the installer for your platform:

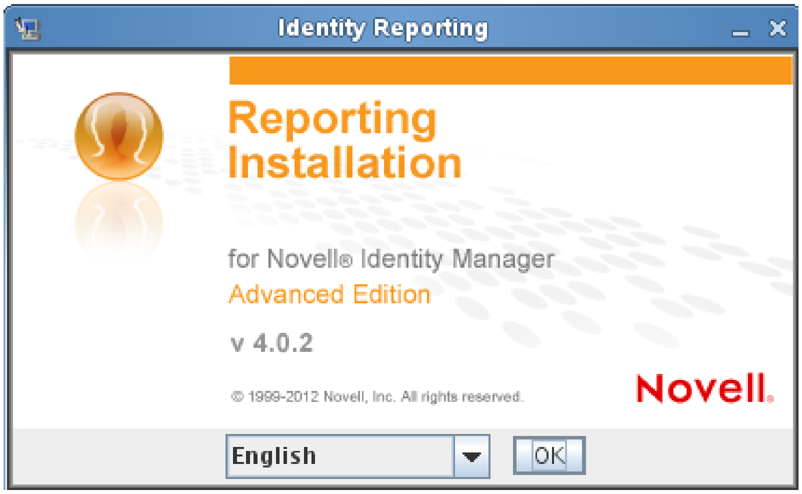
   Linux

   ```
   ./IDMReport.bin
   ```

   Windows

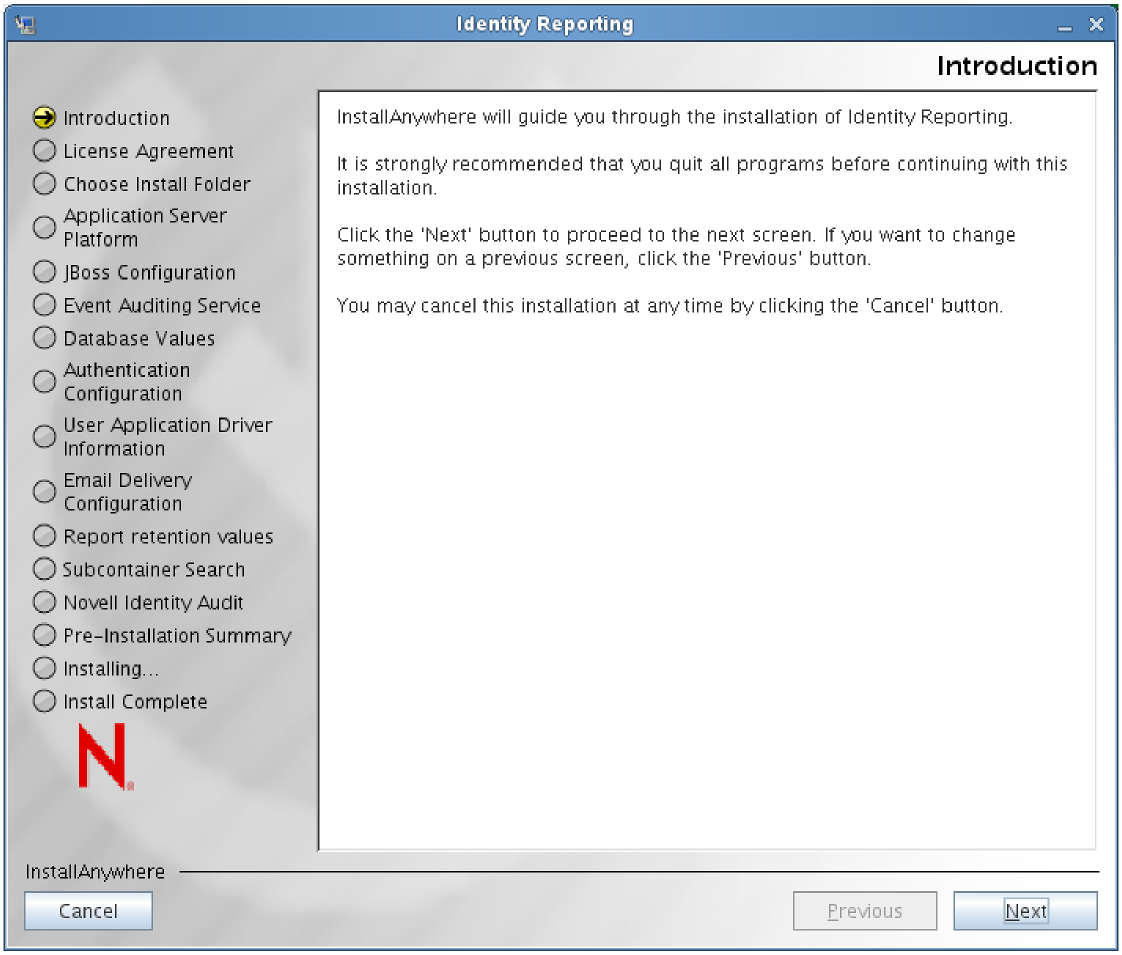
   ```
   IDMReport.exe
   ```

   When the installation program launches, you are prompted for the language:

2. Choose the language for your installation and click *OK*.

   The installer displays the Introduction screen:



InstallAnywhere will guide you through the installation of Identity Reporting.

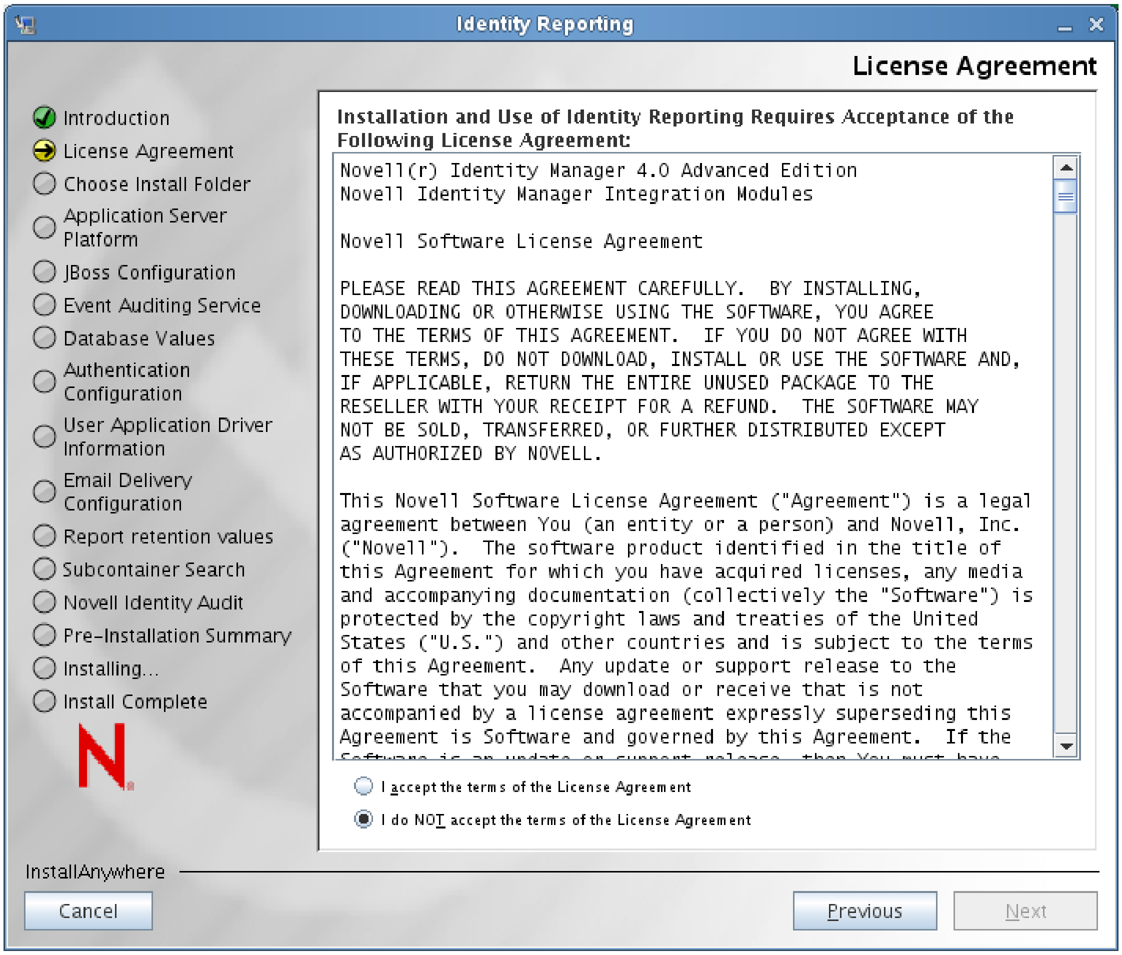
It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

3 Click *Next*.

The installer displays the License Agreement screen:



License Agreement

Installation and Use of Identity Reporting Requires Acceptance of the Following License Agreement:

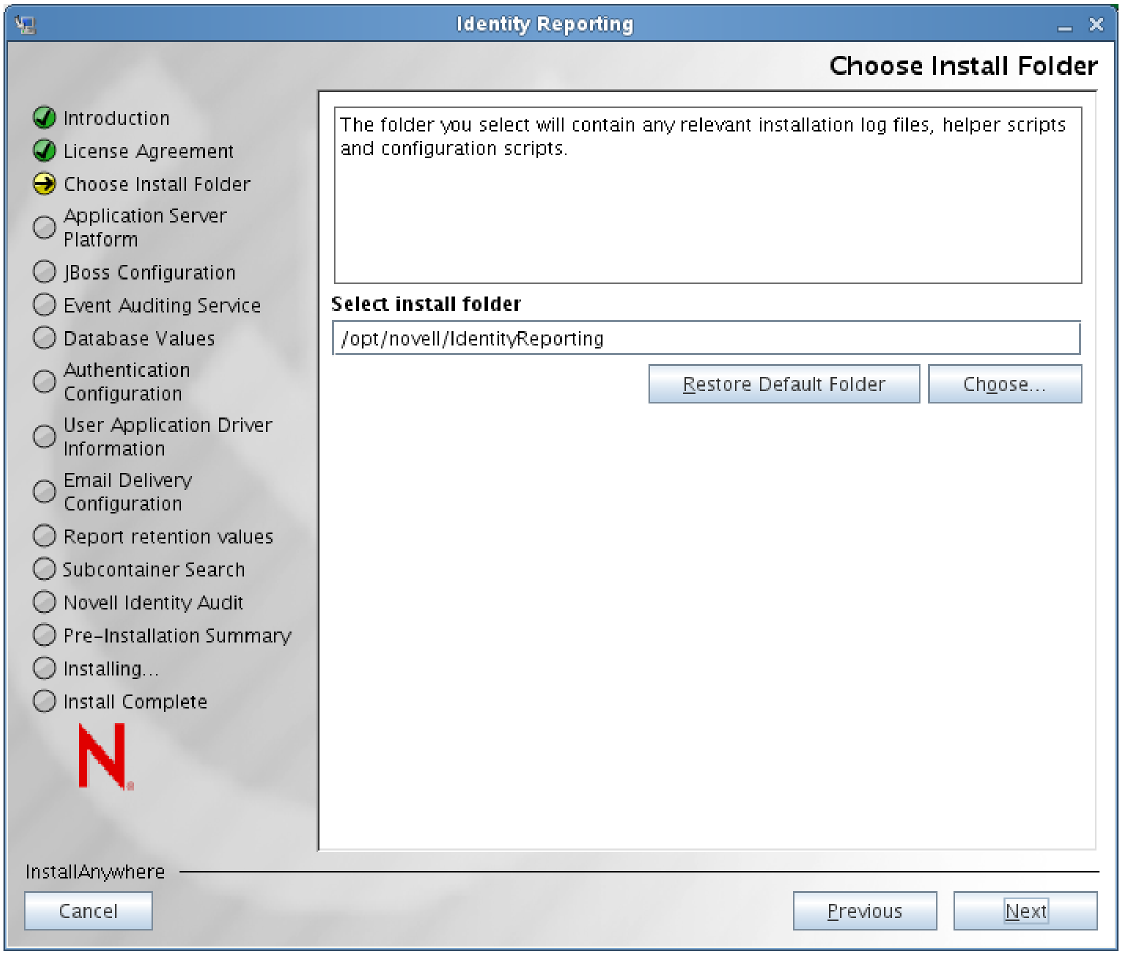
```
Novell(r) Identity Manager 4.0 Advanced Edition
Novell Identity Manager Integration Modules

Novell Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY.  BY INSTALLING,
DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU AGREE
TO THE TERMS OF THIS AGREEMENT.  IF YOU DO NOT AGREE WITH
THESE TERMS, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE AND,
IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE
RESELLER WITH YOUR RECEIPT FOR A REFUND.  THE SOFTWARE MAY
NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED EXCEPT
AS AUTHORIZED BY NOVELL.

This Novell Software License Agreement ("Agreement") is a legal
agreement between You (an entity or a person) and Novell, Inc.
("Novell").  The software product identified in the title of
this Agreement for which you have acquired licenses, any media
and accompanying documentation (collectively the "Software") is
protected by the copyright laws and treaties of the United
States ("U.S.") and other countries and is subject to the terms
of this Agreement.  Any update or support release to the
Software that you may download or receive that is not
accompanied by a license agreement expressly superseding this
Agreement is Software and governed by this Agreement.  If the
```

○ I accept the terms of the License Agreement

● I do NOT accept the terms of the License Agreement

4 Confirm the license agreement and click *Next*.

The installer displays the Choose Install Folder screen:



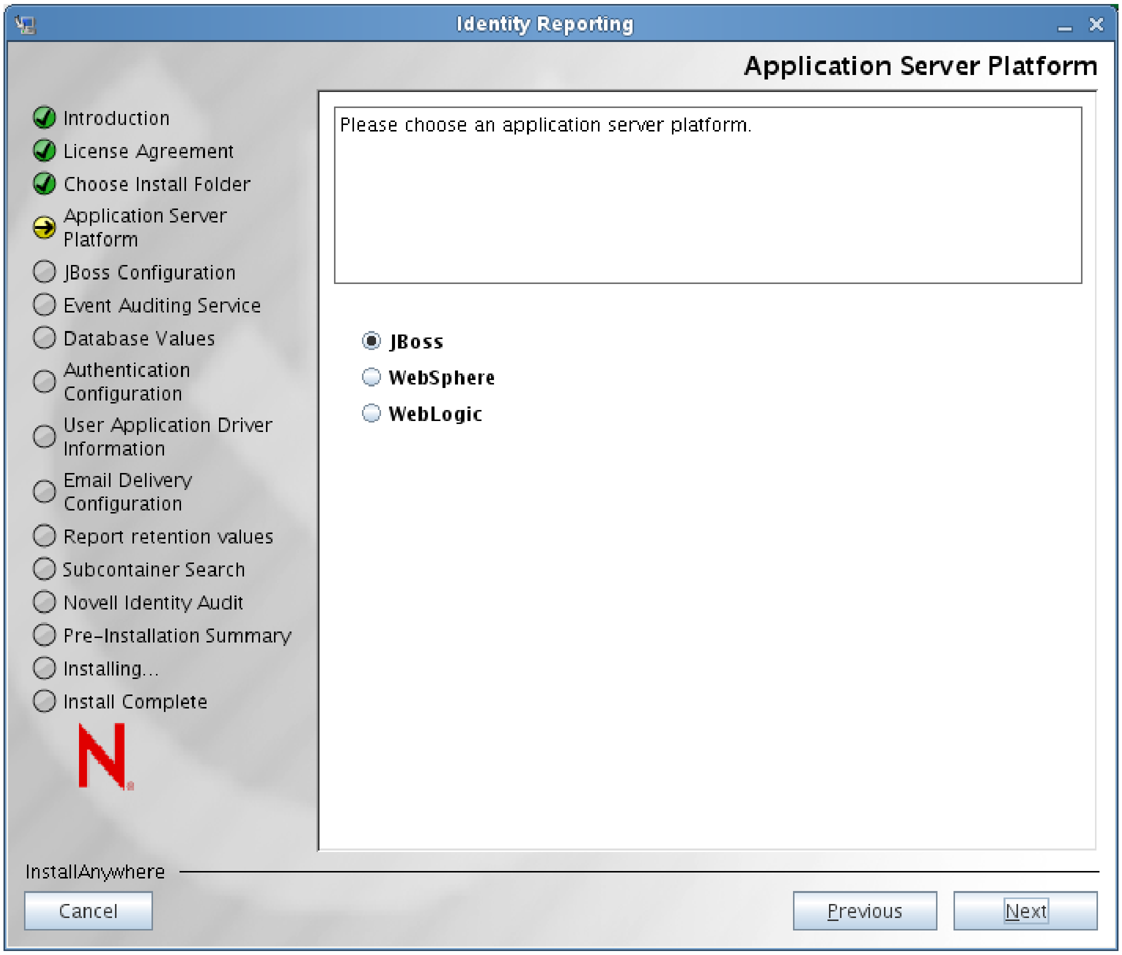
Choose Install Folder

The folder you select will contain any relevant installation log files, helper scripts and configuration scripts.

Select install folder: /opt/novell/IdentityReporting

5 Specify the target location on disk where you want the installation files to be stored and click *Next*.

The installer displays the Application Server Platform screen:



Please choose an application server platform.

● JBoss
○ WebSphere
○ WebLogic

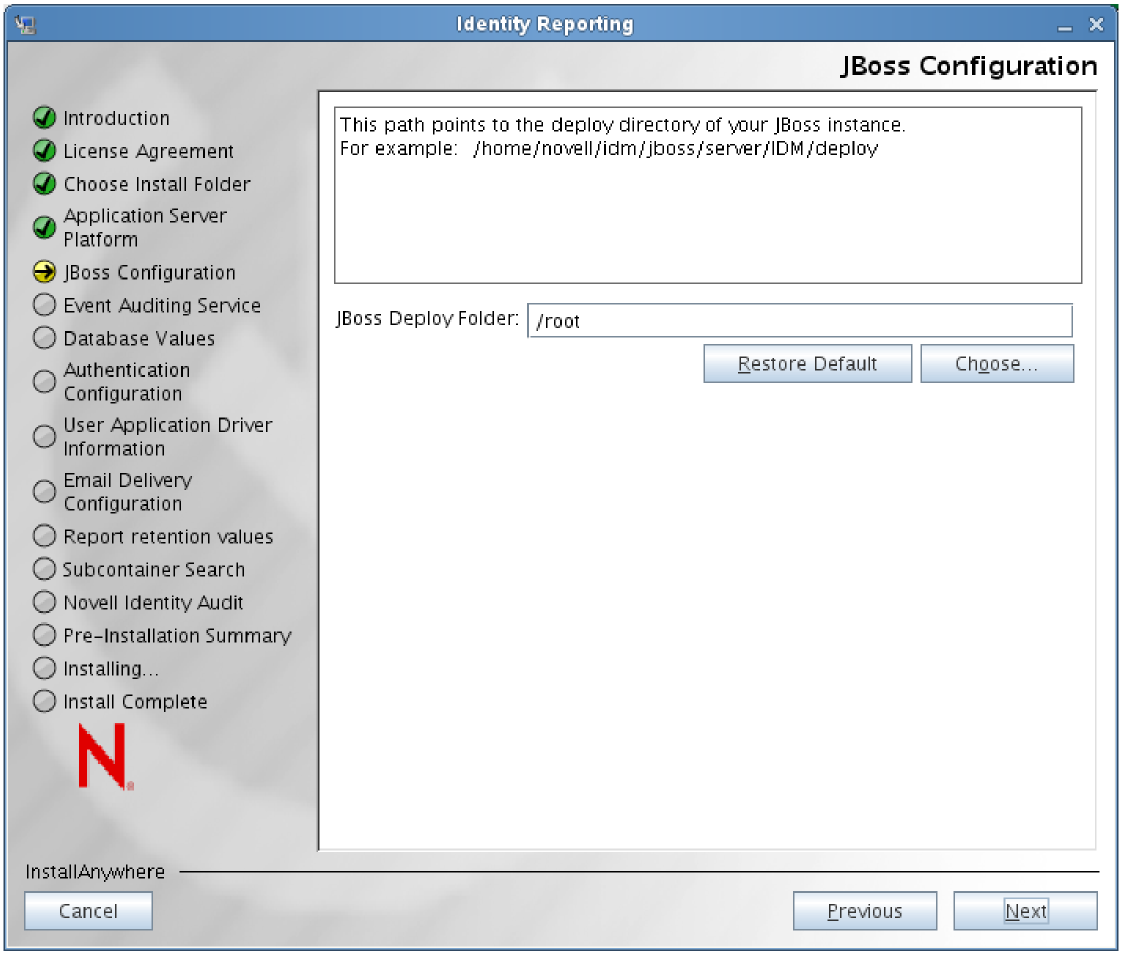
6 Select the application server platform where you will be running the core WAR (IDMRPT-Core.war) and the authentication WAR (IDMRPT-Auth.war) for the reporting module. Click *Next*.

IMPORTANT: The names of these WAR files must not be changed. If you change either of the WAR file names, the deployment process fails.

The installer displays the configuration screen that applies to your application server platform.

WebLogic and WebLogic Configuration: If you are deploying the reporting module on WebSphere or WebLogic, be sure to read Section 2.3.6, “Configuration Notes for WebLogic and WebSphere,” on page 56.

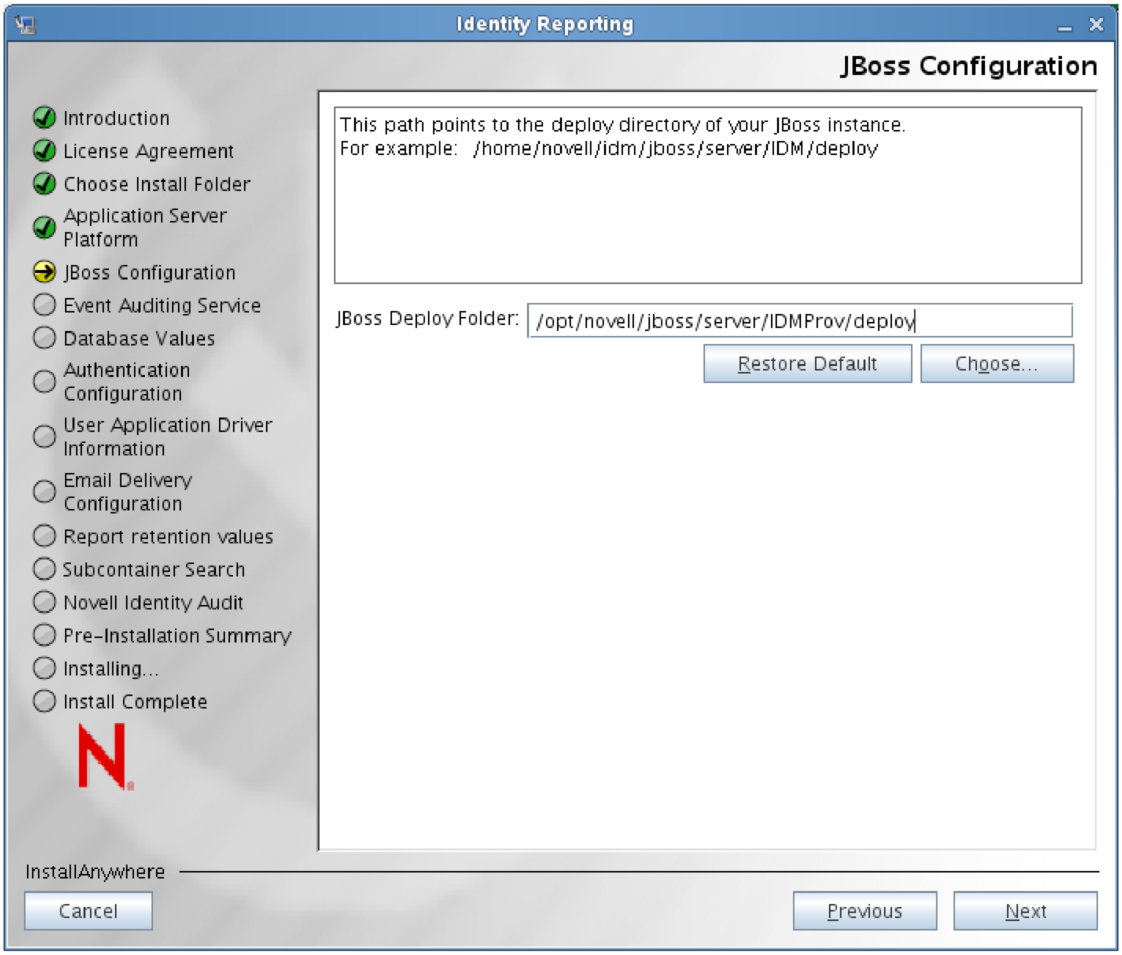
JBoss Configuration: For JBoss, the install program displays this screen:



This path points to the deploy directory of your JBoss instance.
For example: /home/novell/idm/jboss/server/IDM/deploy

JBoss Deploy Folder: /root

7 Specify the target location on disk of the deploy directory for your JBoss server:

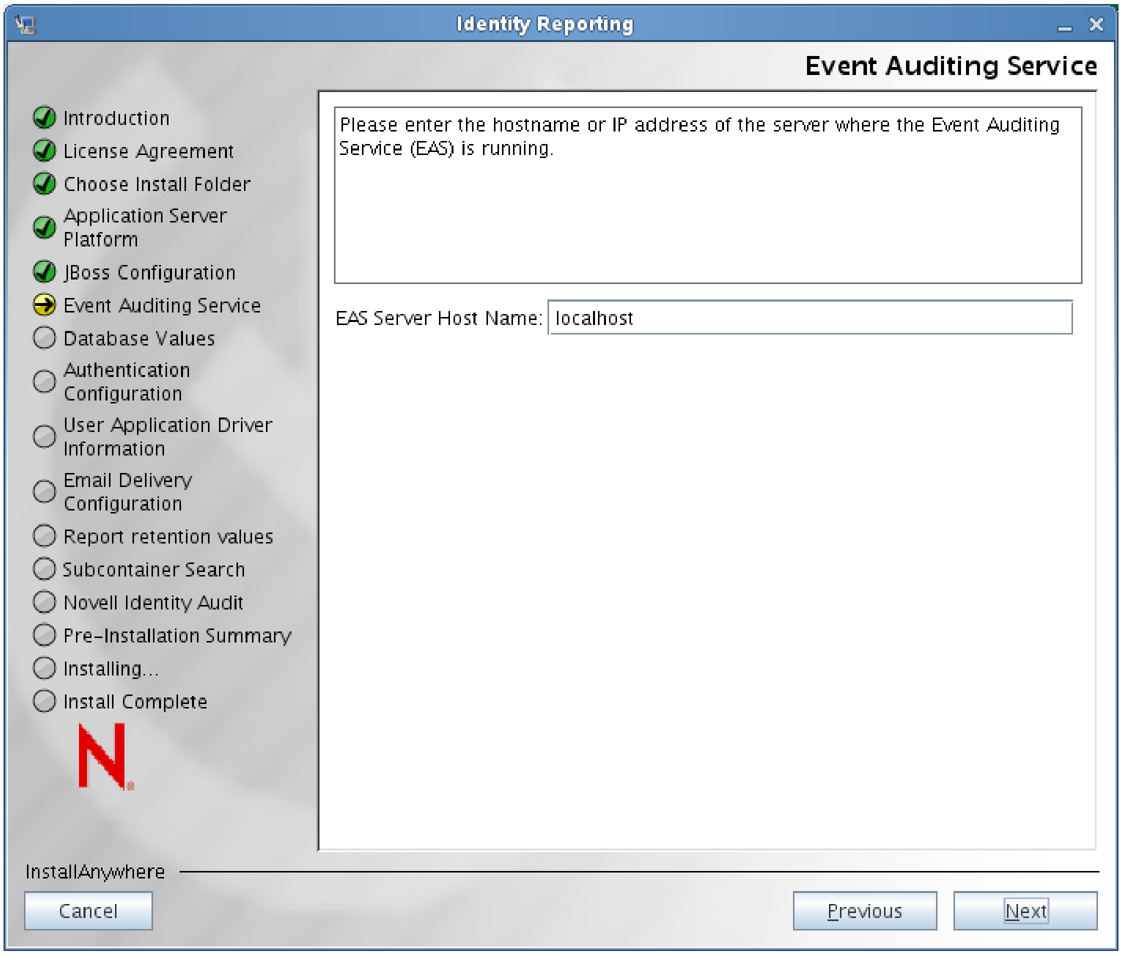


This path points to the deploy directory of your JBoss instance.
For example: /home/novell/idm/jboss/server/IDM/deploy

JBoss Deploy Folder: /opt/novell/jboss/server/IDMProv/deploy

8 Click *Next*.

The installer displays the Event Auditing Service (EAS) screen:



Please enter the hostname or IP address of the server where the Event Auditing Service (EAS) is running.

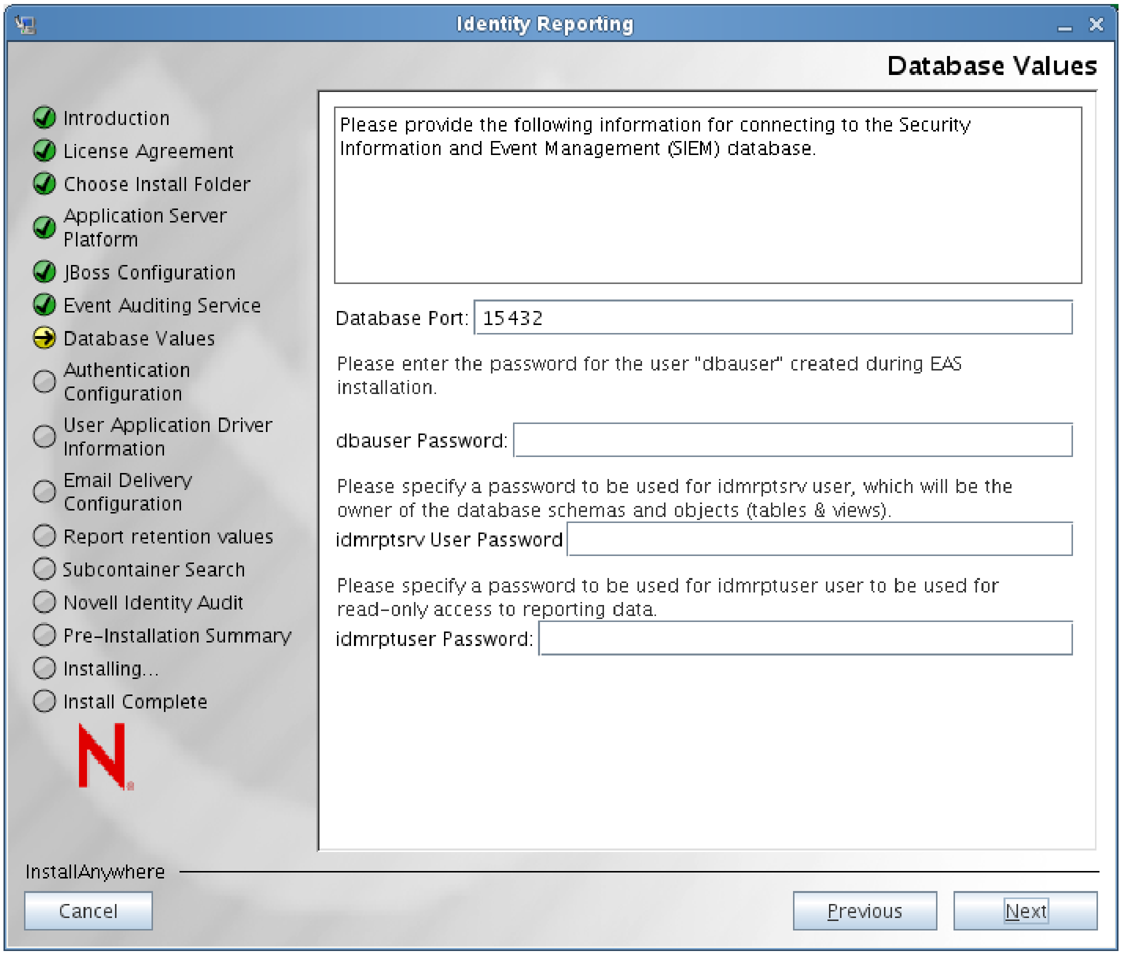
EAS Server Host Name: localhost

9 Specify the server name or IP address of the EAS server in the *EAS Server Host Name* field.

If your EAS server is installed on a remote machine, the installer displays an additional screen for EAS configuration that allows you to specify a password for the server. Copy the system password from the `system` property in the `activemqusers.properties` file on the machine where EAS is installed, and paste it into the *EAS System password* field.

10 Click *Next*.

The installer displays the Database Values screen:



Database Values

Please provide the following information for connecting to the Security Information and Event Management (SIEM) database.

Database Port: 15432

Please enter the password for the user "dbauser" created during EAS installation.

dbauser Password:

Please specify a password to be used for idmrptsrv user, which will be the owner of the database schemas and objects (tables & views).

idmrptsrv User Password

Please specify a password to be used for idmrptuser user to be used for read-only access to reporting data.

idmrptuser Password:

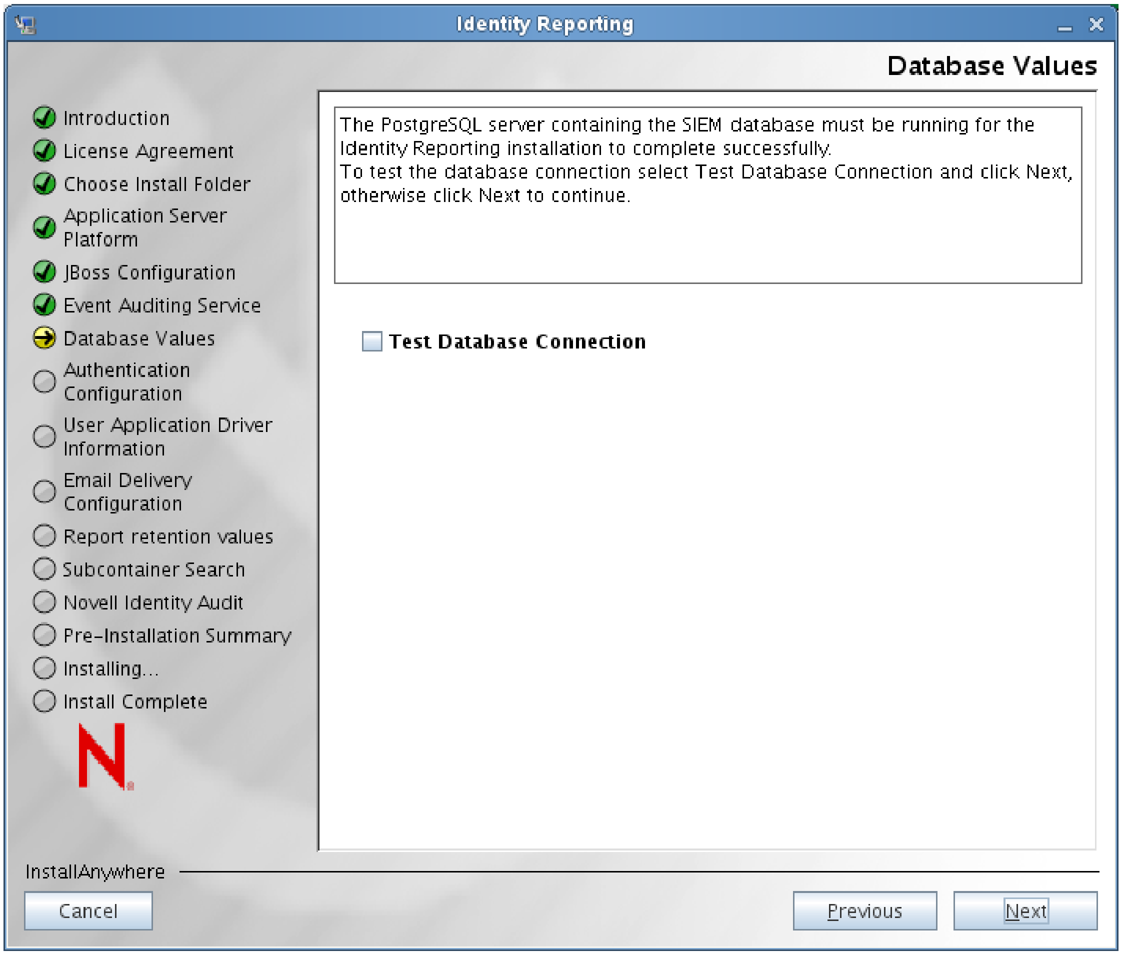
11 Specify the port number for the database server where the Security Information and Event Management (SIEM) database is stored. Also specify passwords for the following users:

- Database administrator (user named `dbauser`)
- Owner of the database schemas and objects for reporting (user named `idmrptsrv`)
- User with read-only access to the reporting data (user named `idmrptuser`)

12 Click *Next*.

The reporting module installs a JAR file for the PostgreSQL JDBC driver, and automatically uses this file for database connectivity. Therefore, you do not need to select the JAR file for the JDBC driver.

The installer updates the Database Values screen to include a check box that allows you to test the connection to the database:



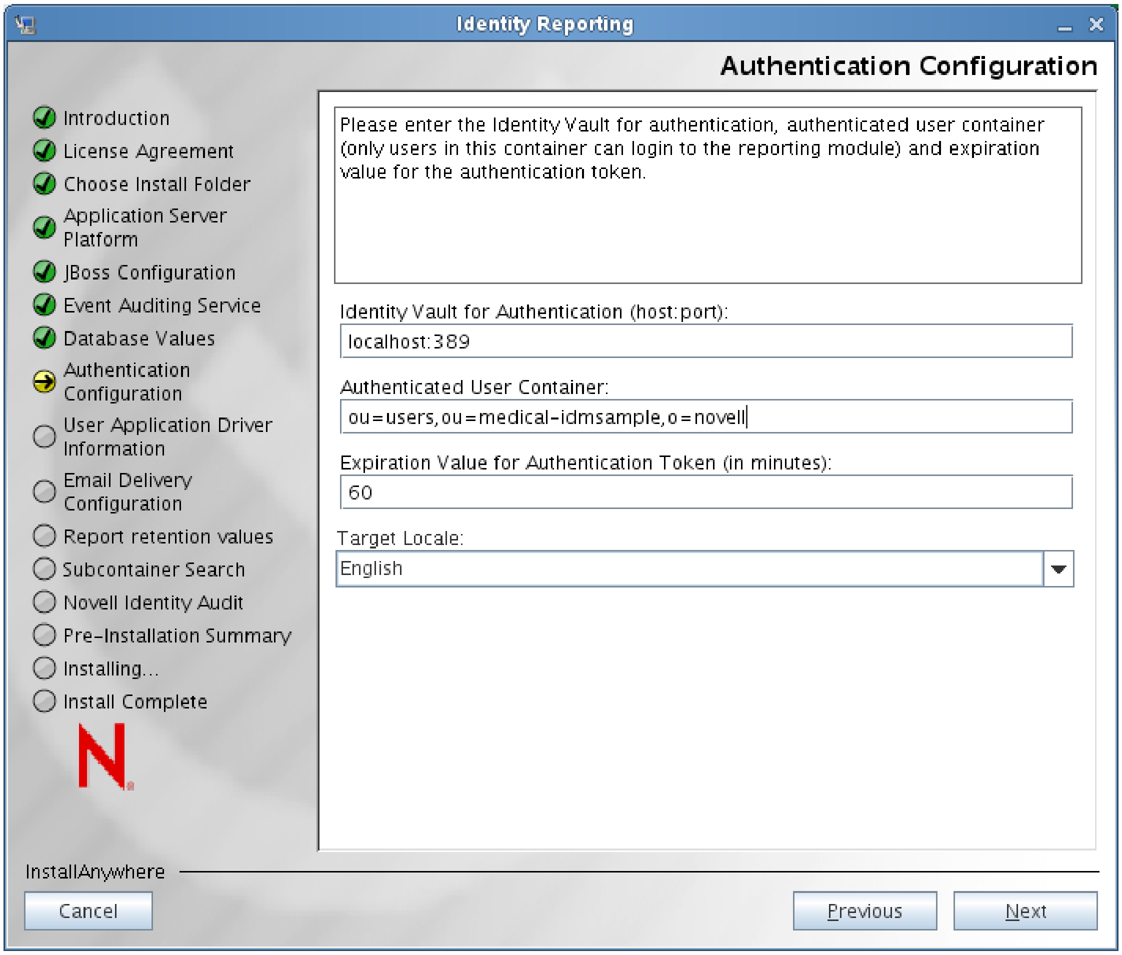
The PostgreSQL server containing the SIEM database must be running for the Identity Reporting installation to complete successfully.
To test the database connection select Test Database Connection and click Next, otherwise click Next to continue.

□ Test Database Connection

NOTE: The installer requires that the database be running. If it is not running, the installation process does not finish successfully.

13 Select *Test Database Connection* and click *Next*.

The installer displays the Authentication Configuration screen:



Please enter the Identity Vault for authentication, authenticated user container (only users in this container can login to the reporting module) and expiration value for the authentication token.

Identity Vault for Authentication (host:port): localhost:389

Authenticated User Container: ou=users,ou=medical-idmsample,o=novell

Expiration Value for Authentication Token (in minutes): 60

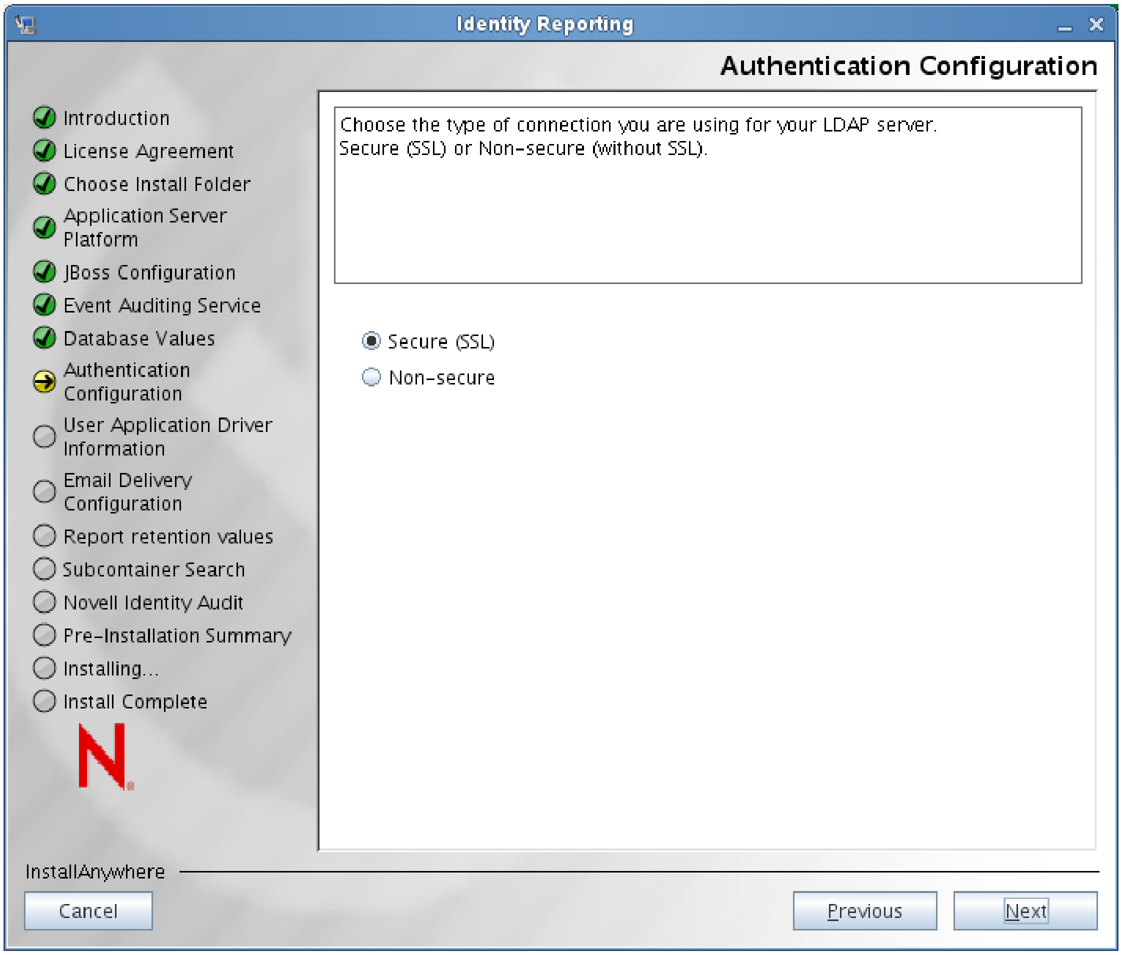
Target Locale: English

14 Provide the following information about the configuration:

Configuration Value	Description
Identity Vault for Authentication	Specifies the name and port number for the Identity Vault that will be used for authentication.
Authenticated User Container	Specifies the LDAP distinguished name (DN) of the container for users that authenticate. Only users in this container can log in to the reporting module. **NOTE:** If the DN contains any special characters as defined in RFC 2253/4514 section 2.4, those characters have to be provided as already escaped according to RFC 2253/4514.
Expiration Value for Authentication Token	Specifies the number of minutes to retain the token for authentication.
Target Locale	Lets you select a language for the configuration.

15 Click *Next*.

The installer updates the Authentication Configuration screen to show radio buttons that allow you to specify the type of connection you are using:



Authentication Configuration

Choose the type of connection you are using for your LDAP server.
Secure (SSL) or Non-secure (without SSL).

● Secure (SSL)

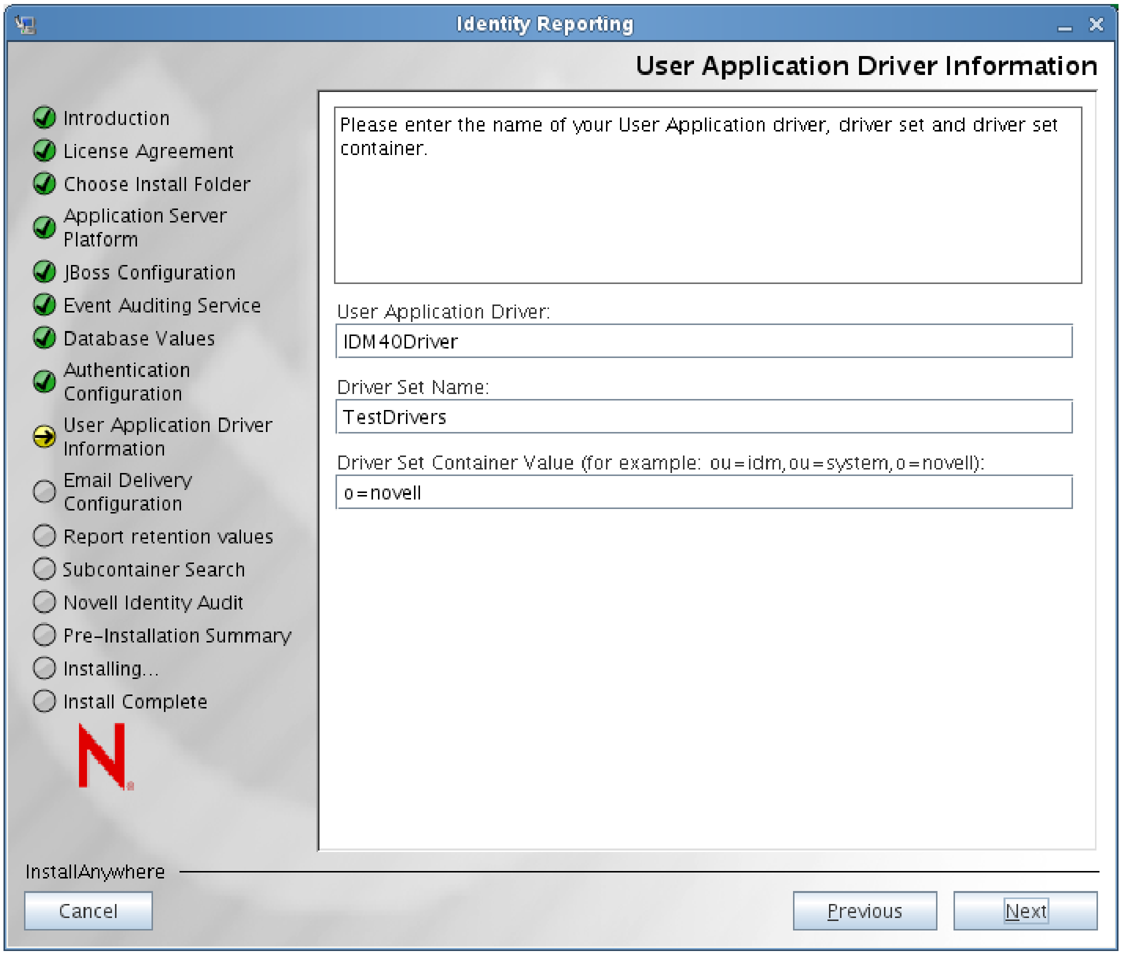
○ Non-secure

16 Select one of these options to specify the type of connection you want to use with your LDAP Server:

Option	Description
Secure (SSL)	Select this option to require that all communication be done using a secure socket. (This option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.
Non-secure	Select this option to allow communication without SSL.

17 Click *Next*.

The installer displays the User Application Driver Information screen:



Please enter the name of your User Application driver, driver set and driver set container.

User Application Driver: IDM40Driver

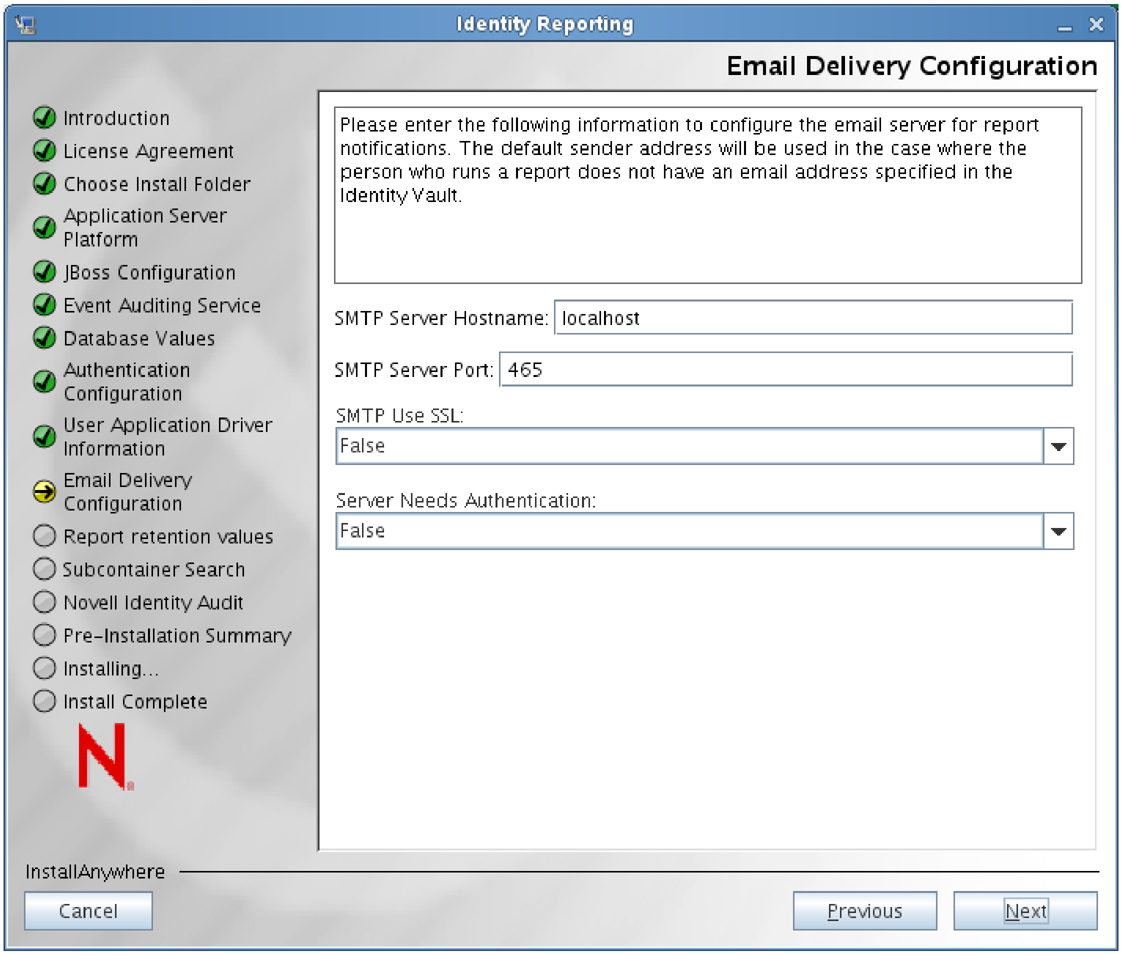
Driver Set Name: TestDrivers

Driver Set Container Value (for example: ou=idm,ou=system,o=novell): o=novell

18 Specify the name of the User Application Driver, driver set, and driver set container you plan to use for the reporting module, then click *Next*.

NOTE: The values for all three fields on this screen must be escaped according to the rules defined in RFC 2253/4514.

The installer displays the Email Delivery Configuration screen:



Please enter the following information to configure the email server for report notifications. The default sender address will be used in the case where the person who runs a report does not have an email address specified in the Identity Vault.

SMTP Server Hostname: localhost

SMTP Server Port: 465

SMTP Use SSL: False

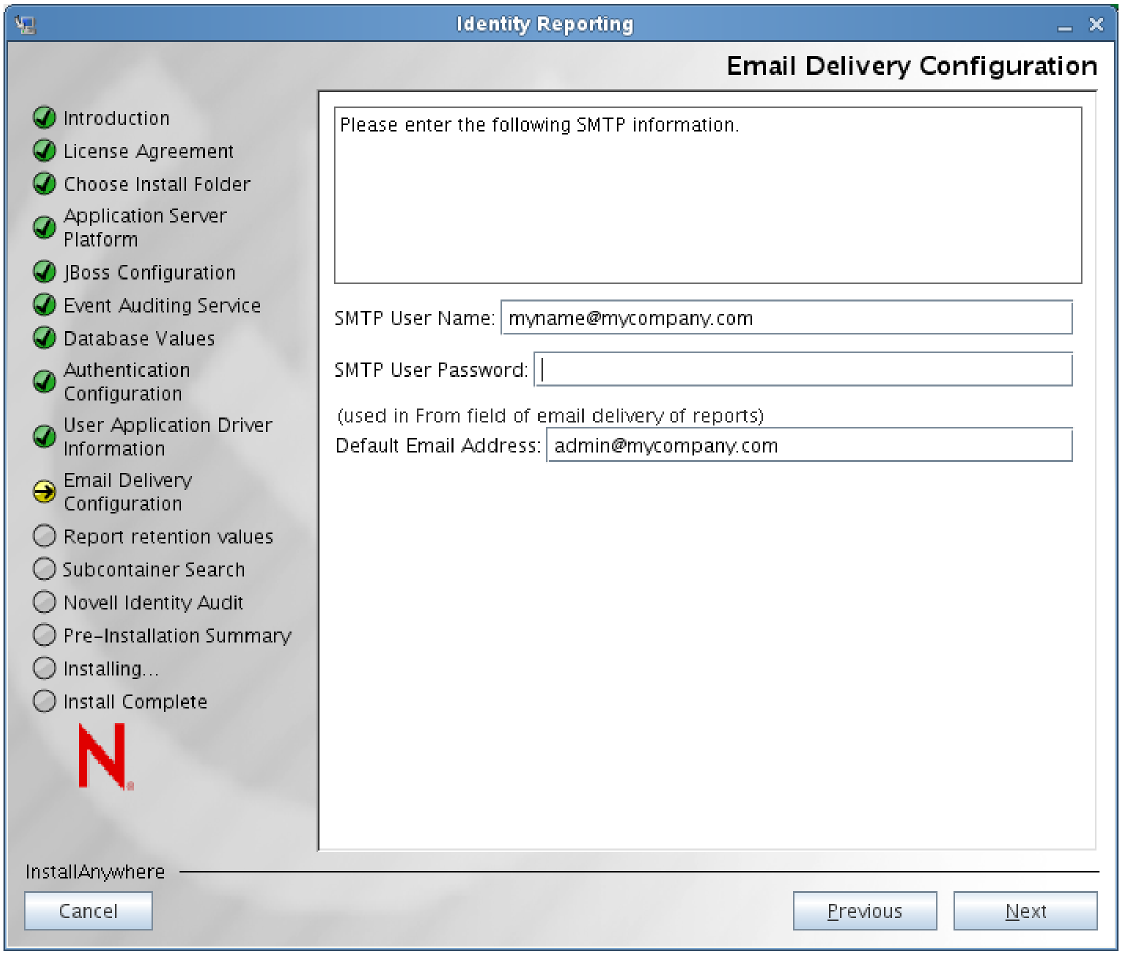
Server Needs Authentication: False

19 Provide the following information about your Simple Mail Transfer Protocol (SMTP) server configuration:

Setting	Description
SMTP Server Hostname	Specifies the host address for the e-mail server that will be used for e-mail notifications sent by the reporting module
SMTP Server Port	Specifies the port number for the e-mail server.
SMTP Use SSL	Enables or disables SSL for communications with the e-mail server. Select *True* to enable SSL, or *False* to disable SSL.
Server Need Authentication	Enables or disables authentication for communications with the e-mail server. Select *True* to enable SSL, or *False* to disable authentication.

20 Click *Next*.

The Email Delivery Configuration screen is updated to include several additional fields required for the e-mail configuration:



Please enter the following SMTP information.

SMTP User Name: myname@mycompany.com

SMTP User Password:

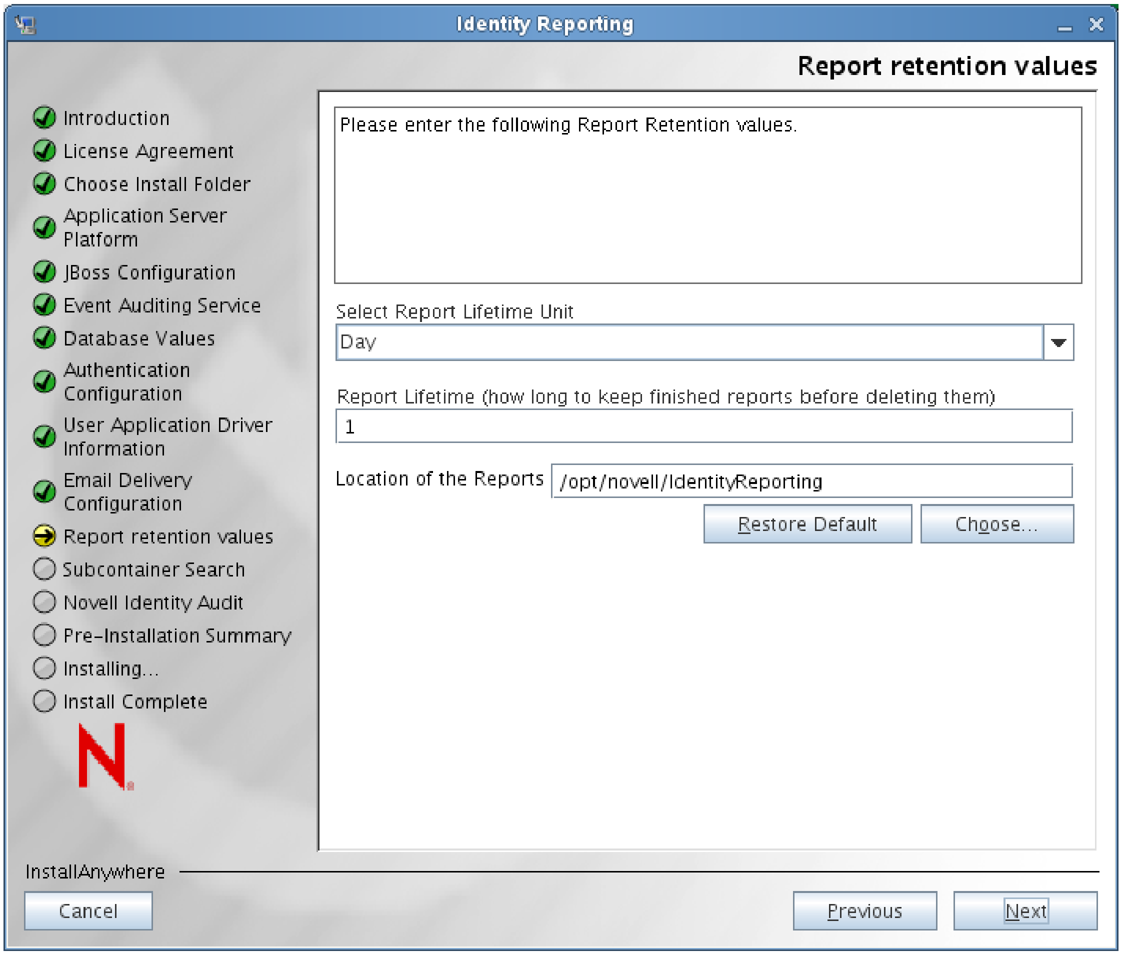
(used in From field of email delivery of reports)
Default Email Address: admin@mycompany.com

21 Provide these additional SMTP settings:

SMTP Setting	Description
SMTP User Name	Specifies the e-mail address to use for authentication, when authentication is enabled.
SMTP User Password	Specifies the password associated with the e-mail address used for authentication.
Default Email Address	Provides the default e-mail address to use in the From field for e-mail notifications from the reporting module.

22 Click *Next*.

The installer displays the Report Retention Values screen:



Report retention values

Please enter the following Report Retention values.

Select Report Lifetime Unit: Day

Report Lifetime (how long to keep finished reports before deleting them): 1

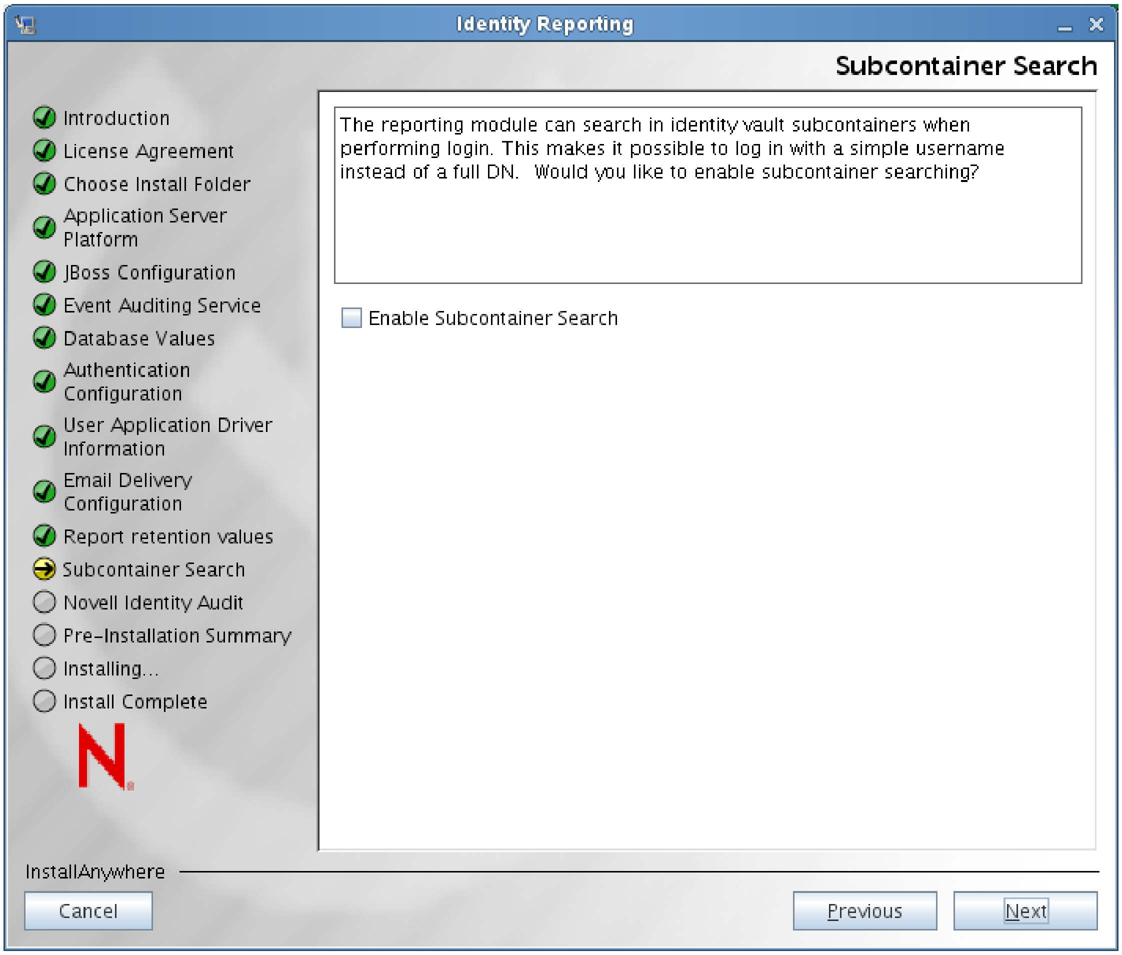
Location of the Reports: /opt/novell/IdentityReporting

23 Provide these additional report settings:

SMTP Setting	Description
Select the Report Unit	Before specifying a report lifetime value, you need to specify the unit for the report lifetime value. Select one of the following units: ◆ Day ◆ Week ◆ Month
Report Lifetime	Specifies how long the reporting module should retain completed reports before deleting them.
Location of the Reports	Specifies the disk location where report definitions will be stored.

24 Click *Next*.

The installer displays the Subcontainer Search screen:

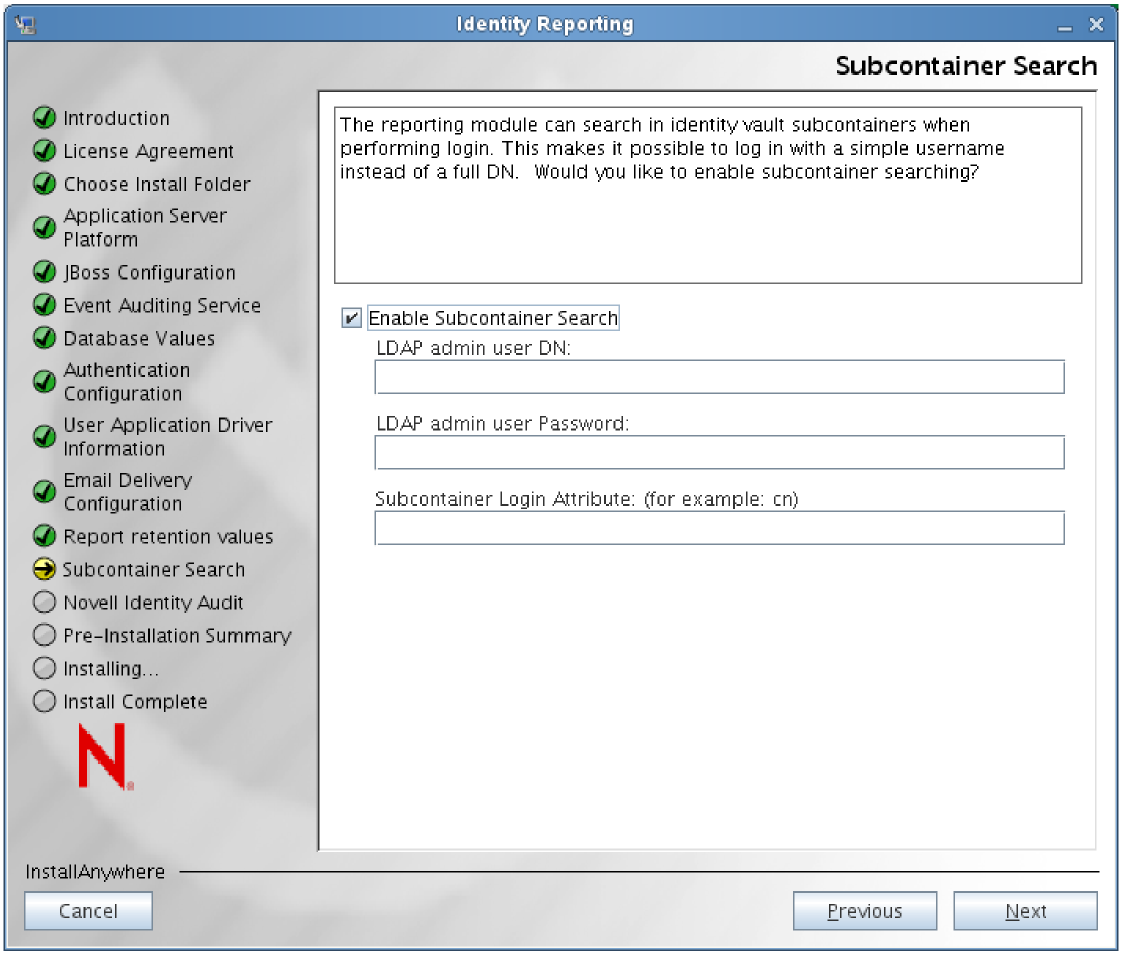


The reporting module can search in identity vault subcontainers when performing login. This makes it possible to log in with a simple username instead of a full DN. Would you like to enable subcontainer searching?

□ Enable Subcontainer Search

25 Indicate whether you want to enable subcontainer searches at login time by selecting or deselecting the *Enable Subcontainer Search* check box on the Subcontainer Search screen.

If you enable subcontainer searches, you need to provide an LDAP administrator username and password and also specify which login attribute will be used for searching the subtree of the user container. If there are any special characters in the LDAP administrator username, you need to escape these characters:



The reporting module can search in identity vault subcontainers when performing login. This makes it possible to log in with a simple username instead of a full DN. Would you like to enable subcontainer searching?

☑ Enable Subcontainer Search

LDAP admin user DN:

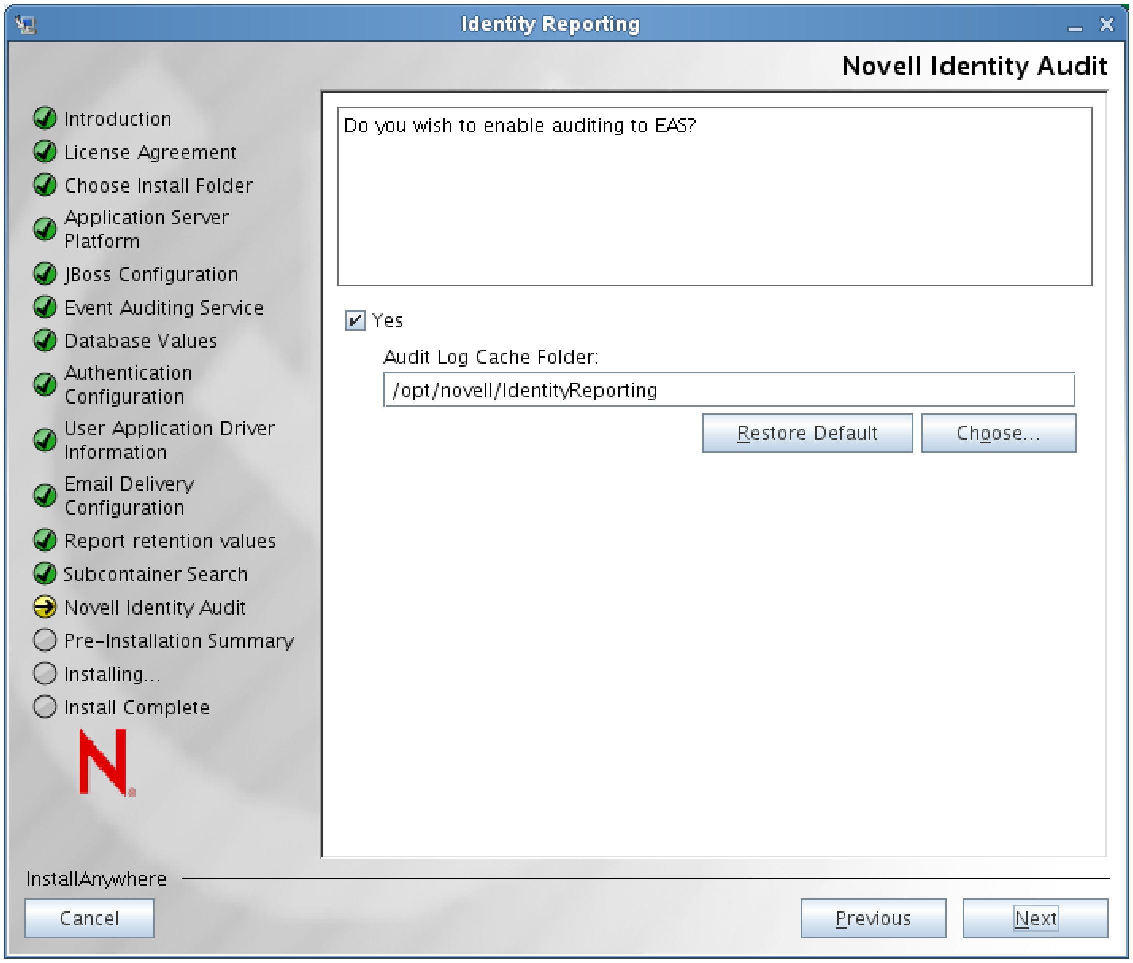
LDAP admin user Password:

Subcontainer Login Attribute: (for example: cn)

If you disable subcontainer searches, no searches are performed within the subtree of the user container, and the simple name that the user types during login is always treated as a CN.

26 Click *Next*.

The installer displays the Novell Identity Audit screen:



Do you wish to enable auditing to EAS?

☑ Yes

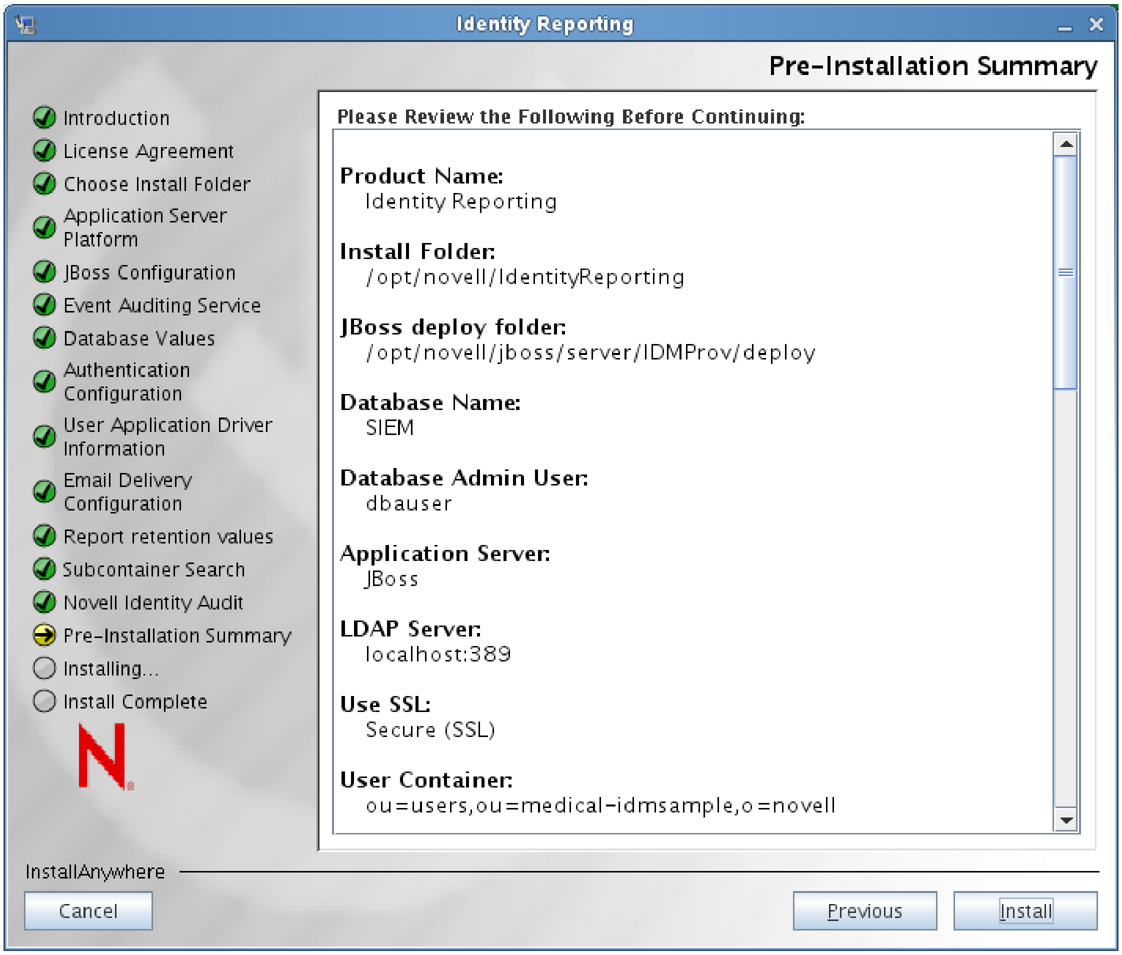
Audit Log Cache Folder:

/opt/novell/IdentityReporting

27 If you want to enable auditing to EAS, select *Yes*, specify the location of the cache folder for auditing, then click *Next*.

If you do not want to enable auditing, simply click *Next*.

The installer displays the Pre-Installation Summary screen:



Please Review the Following Before Continuing:

Product Name:
Identity Reporting

Install Folder:
/opt/novell/IdentityReporting

JBoss deploy folder:
/opt/novell/jboss/server/IDMProv/deploy

Database Name:
SIEM

Database Admin User:
dbauser

Application Server:
JBoss

LDAP Server:
localhost:389

Use SSL:
Secure (SSL)

User Container:
ou=users,ou=medical-idmsample,o=novell

28 Click *Install* to begin copying files.

If you need to change any of your installation settings, click *Previous*.

2.3.1 Running the Installer in Silent Mode

You can run the reporting installer in silent mode. Before running the installer, you need to edit the properties file for the installer. Once you've edited the properties file, launch it with this command:

```
./IDMReport.bin -i silent -f <path to the properties file>
```

For example:

```
./IDMReport.bin -i silent -f /root/Software/silent.properties
```

2.3.2 Setting Passwords in the Environment for a Silent Install

If you do not want to specify the passwords in the properties file, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the properties file. This can provide some additional security.

The following passwords need to be set for the reporting installer:

- NOVL_ADMIN_PWD
- NOVL_DB_RPT_USER_PASSWORD

- NOVL_SMTP_PASSWORD
- NOVL_EAS_SYSTEM_PASSWORD
- NOVL_IDM_SRV_PWD
- NOVL_IDM_USER_PWD

To set a password on Linux, use the `export` command, as shown in the following example:

```
export NOVL_ADMIN_PWD=myPassWord
```

To set a password on Windows, use the `set` command, as shown in the following example:

```
set NOVL_ADMIN_PWD=myPassWord
```

2.3.3 Making Configuration Changes After the Installation

After the installation process is complete, you can still make changes to many of the installation properties for the Identity Reporting Module by running the post-install configuration tool. To launch this tool, execute this file:

```
./ReportConfig.bin
```

The user interface for this tool is very similar to the interface for the Identity Reporting Module installer, so you can simply make changes within this tool just as you would within the installer.

If you change any setting for the reporting module by using the post-install configuration tool, you need to restart the application server for the changes to take effect. Any changes made in the Web user interface for the Identity Reporting Module don't require restarting the server.

2.3.4 Defining User Preferences After the Installation

The preferences defined with the post-install configuration tool (`ReportConfig.bin`) apply to the user that started the tool. Suppose the “root” user installed the reporting module and configured the settings for reporting during the installation. In this case, the configuration applies to the system preferences, which define the default settings for the application. When another user such as Allison Blake later launches the reporting module, the module runtime uses the system preferences by default. However, Allison can run the post-install configuration tool to modify the configuration. In this case, the new configuration does not overwrite the system preferences, but instead saves these preferences separately for Allison. This behavior applies to all users. In addition, the REST API can be used to configure user preferences for reporting module users. Whenever a particular user launches the reporting module, the application uses the preferences for the logged in user.

Now suppose that the “root” user decides to uninstall the reporting module. This user runs the uninstaller, which removes the binaries as well as the system preferences and user preferences for the “root” user. However it doesn't remove the user preferences for any other users. Later, if the “root” user installs the reporting module again, and Allison tries to launch the reporting module, Allison will still be using the user preferences configured for her during the previous installation. Therefore, in some situations, you might to suggest that the individual users of the reporting module clean up their user preferences before an uninstall and reinstall of the product.

2.3.5 Setting the System Properties for Reporting on 64-Bit Windows

If you installed the reporting module using 32-bit Java on a 64-bit Windows operating system, you need to export and import the configuration settings (stored in Java Preferences) between the 32-bit and 64-bit Java environments. The reporting module provides the PreferencesUtil.jar utility to help you do this.

To set the System Properties on a 64-bit Windows operating system:

1 Execute this command to export the system-level configuration into a file:

   ```
   <path_to_32bit_java>/java -jar PreferencesUtil.jar export_system
   <path_to_dump_file>
   ```

   For example:

   ```
   c:\Program Files (x86)\Java\jdk1.6.0_31\bin\java.exe" -jar
   PreferencesUtil.jar export_system c:\reporting32bitprops.xml
   ```

2 Execute this command to import the configuration from the file to the 64-bit Java environment:

   ```
   <path_to_64bit_java>/java -jar PreferencesUtil.jar import <path_to_dump_file>
   ```

   For example:

   ```
   c:\Program Files\Java\jdk1.6.0_31\bin\java.exe" -jar PreferencesUtil.jar
   import c:\reporting32bitprops.xml
   ```

After importing the configuration, you should see the configuration properties under:

```
HKEY_LOCAL_MACHINE
  SOFTWARE
     JavaSoft
       Prefs
```

At this point, you should be able to start the reporting module using 64-bit Java and use all components of the application.

2.3.6 Configuration Notes for WebLogic and WebSphere

The install program for the reporting module creates the users idmrptsrv and idmrptuser in the PostgreSQL database. These users are needed in order to test the data sources required by the reporting module. Furthermore, the data sources need to exist before you deploy the application.

- "Preparing a WebLogic or WebSphere Environment to Run the Reporting Module" on page 56
- "Additional Configuration Notes For WebLogic" on page 57
- "Additional Configuration Notes for WebSphere" on page 57

Preparing a WebLogic or WebSphere Environment to Run the Reporting Module

To ensure that your environment is set up correctly, you must perform these steps in the order shown below.

1 Install the reporting module, as described under Section 2.3, "Running the Identity Reporting Module Install Program," on page 35.

   This step creates the idmrptsrv and idmrptuser users in the PostgreSQL database, as well as writes the WARs to /opt/novell/IdentityReporting.

2 Create two data sources for PostgreSQL that connect to the SIEM database. These data sources are bound to the users idmrptsrv and idmrptuser.

   For WebSphere, you need to create data sources with the names IDMRPTCfgDataSource and IDMRPTDataSource.

   On WebLogic, the names for the datasources must be jdbc/IDMRPTCfgDataSource and jdbc/IDMRPTDataSource.

IDMRPTCfgDataSource is bound to the user called idmrptuser and IDMRPTDataSource is bound to the user called idmrptsrv.

The installation for JBoss creates both data sources automatically, so you do not need to create the data sources for JBoss.

3 Deploy the reporting module using the application server deployment tools.

Additional Configuration Notes For WebLogic

This section provides additional configuration notes for WebLogic.

- "Disabling the enforce-valid-basic-auth-credentials Flag" on page 57
- "SSL Configuration" on page 57
- "Adding JAR Files to the PRE_CLASSPATH" on page 57

Disabling the enforce-valid-basic-auth-credentials Flag

On WebLogic, the reporting module does not find your Identity Vaults unless you disable the enforce-valid-basic-auth-credentials flag.

1. Open the `config.xml` file in the `<WLHome>\user_projects\domains\idm\config\` folder.
2. Add the following line in the `<security-configuration>` section right before the closing of this section:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
   credentials>
   </security-configuration>
   ```

3. Save the file and restart the server.

After making this change, you should see your Identity Vaults in the reporting module.

SSL Configuration

If you are using SSL connections, you need to persist the eDirectory certificate. This is not necessary for JBoss, because the User Application installer (via configupdate) should have persisted the certificate already.

For WebLogic, you can use keytool:

```
keytool -importcert -trustcacerts -file MyCACert.der -keystore cacerts
```

Adding JAR Files to the PRE_CLASSPATH

If you have installed the Roles Based Provisioning Module and the reporting module on separate servers, you need to add the `antlr-2.7.6.jar` to the EXT_PRE_CLASSPATH environment variable for the reporting module configuration on WebLogic.

Additional Configuration Notes for WebSphere

This section outlines additional configuration steps required for WebSphere.

- "Configuring the Spring Framework" on page 58
- "Configuring the Reporting Module to Run Within a Windows Service" on page 58
- "SSL Configuration" on page 58

Configuring the Spring Framework

WebSphere 7 has the Spring framework 2.5.5 in its system classpath, whereas the EAS REST API war contains (and uses) the Spring framework 3.0.1. Therefore, you need to remove the Spring framework 2.5.5 jars from the WebSphere system classpath. The WebSphere server should be dedicated to Novell applications because other applications deployed on the same server that rely on WebSphere's bundled Spring framework do not work. The location for the Spring framework jar files is `<websphere>/AppServer/lib`. This applies to all supported operating systems. On Windows, the path should use backslashes instead of forward slashes.

The files that need to be removed are as follows:

```
spring-beans-2.5.5.jar
spring-core-2.5.5.jar
```

Configuring the Reporting Module to Run Within a Windows Service

When the Identity Reporting Module is deployed to a Web container that runs as a Windows Service, the *Log on as* property of that service needs to be configured properly so that it can read or write the same configuration data that is set by the installer or post-install configuration tool.

If you do not make this change, you might see problems when WebSphere 7.0 is installed as a Windows service. In this case, the *Log on as* property is set by default to "local system," which doesn't map to any user defined in the users and groups for the system. The reporting module uses Java Preferences to store application configuration data, which are associated with the OS user who executes the process (in other words, the application server).

The solution is to set the *Log on as* property to the user account that you expect the application server to run as. For example, if you want it to run as "administrator," then set *Log on as* to administrator. The post-install configuration tool must run as the same user. For more information, see Section 2.3.4, "Defining User Preferences After the Installation," on page 55.

SSL Configuration

If you are using SSL connections, you need to persist the eDirectory certificate. This is not necessary for JBoss, because the User Application installer (via configupdate) should have persisted the certificate already.

For WebSphere, you can uploaded the CA to the Trusted Store via the console utility.

2.4 Configuring the Drivers

The following drivers are required by the reporting module:

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

These drivers are installed automatically by the Integrated Installer for Identity Manager, so the steps provided below are only necessary if you are running the stand-alone versions of the install programs.

If you are running the stand-alone versions of the install programs, you can use the new package management tools provided with Designer for Identity Manager to install and configure the drivers.

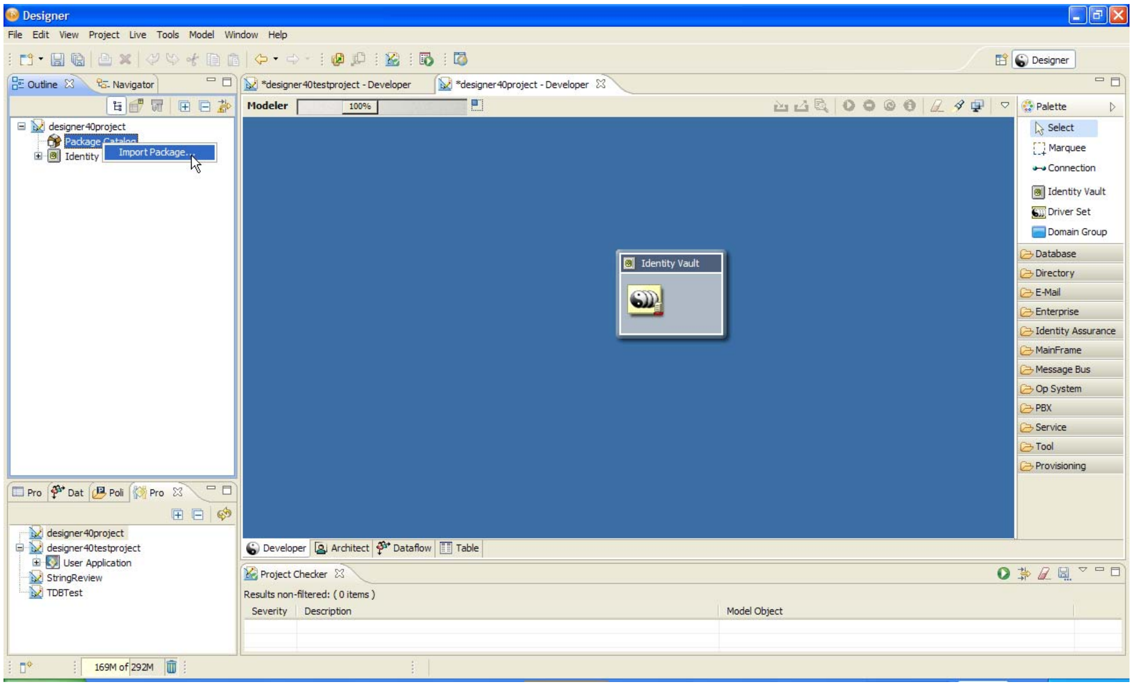
- Section 2.4.1, "Installing the Packages," on page 59
- Section 2.4.2, "Configuring the Managed System Gateway Driver," on page 60

- Section 2.4.3, “Configuring the Identity Manager Driver for Data Collection Service,” on page 67
- Section 2.4.4, “Deploying the Drivers,” on page 72
- Section 2.4.5, “Backing Up and Restoring the Reporting Module,” on page 72
- Section 2.4.6, “Runtime Configuration and Troubleshooting,” on page 73
- Section 2.4.7, “Recommended Auditing Flags for the Drivers,” on page 96

2.4.1 Installing the Packages

Before you attempt to configure the drivers, you need to be sure you have all of the necessary packages in the Package Catalog. When you create a new Identity Manager project, the user interface automatically prompts you to import several packages into the new project. If you choose not to import the packages at the time you create your project, you need to install them later, as described below.

1 After you create a new Identity Manager project in Designer, select the *Package Catalog* and click *Import Package*.



Designer displays the Select Package dialog box.

2 Click *Select All*, then click *OK*.

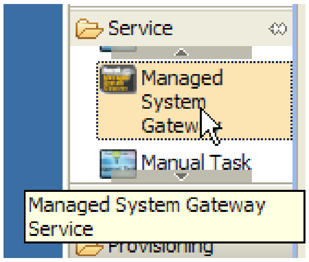
Designer adds several new package folders under the *Package Catalog*. These package folders correspond to the objects in the palette on the right side of the Modeler view in Designer.

3 Click *Save* to save your project.

Configuring Drivers for the Roles Based Provisioning Module: At this point, you would typically want to configure the User Application Driver and the Roles and Resources Driver in Designer, which are required for the Roles Based Provisioning Module. The procedure for configuring these drivers is described in the *Roles Based Provisioning Module Installation Guide*. The sections that follow describe the steps you would take to configure the Managed System Gateway Driver and the Data Collection Service Driver.

2.4.2 Configuring the Managed System Gateway Driver

1 In the Modeler view, select *Service* > *Managed System Gateway* in the palette.



2 Drag the icon for the *Managed System Gateway* application onto the Modeler view.

Designer displays the Driver Configuration Wizard.

3 Select *Managed System Gateway Base* and click *Next*.

NOTE: For the 4.0.2 release, you need to have version 2.0.0.20120509205929 of the Managed System Gateway Base package.

The Driver Configuration Wizard now shows the Select Mandatory Features screen.

4 Make sure the mandatory features listed are selected and click *Next*.

The interface displays a dialog box to inform you that need an additional package called *Advanced Java Class*.

5 Click *OK* to install the required package.

The wizard displays a screen that allows you to specify a name for the driver.

6 Specify the name you want to use for the driver, then click *Next*.

The wizard now displays a screen that allows you to specify the connection parameters for the driver.

7 Specify the IP address and port the driver should listen on, as well as the protocol you want to use.

The reporting module requests data from the Managed System Gateway Driver. Therefore, it needs to know which IP address, port, and protocol to use (http or https).

NOTE: Do not assign an address of “localhost” for the Managed System Gateway Driver if you want to be able to use the REST end points. You cannot connect remotely to “localhost” through REST testing tools.

8 (Optional) If you specify `https` as the protocol you want to use, you must also specify the KMO name stored in the Identity Vault.

9 (Optional) If you want to enable end-point tracing, select *true* from the dropdown menu for *Enable end-point tracing*, then specify the location you want to use for storing trace files.

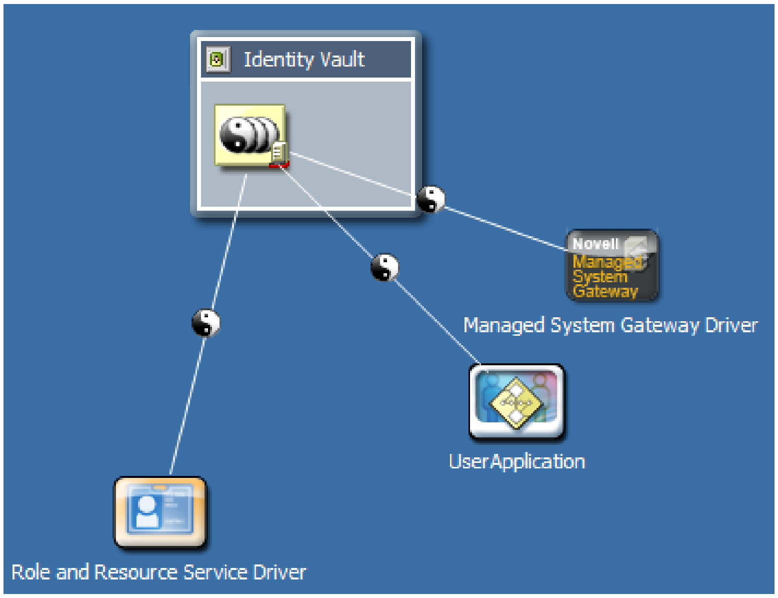
10 Click *Next*.

The wizard now displays a screen that asks whether you plan to connect to a remote loader.

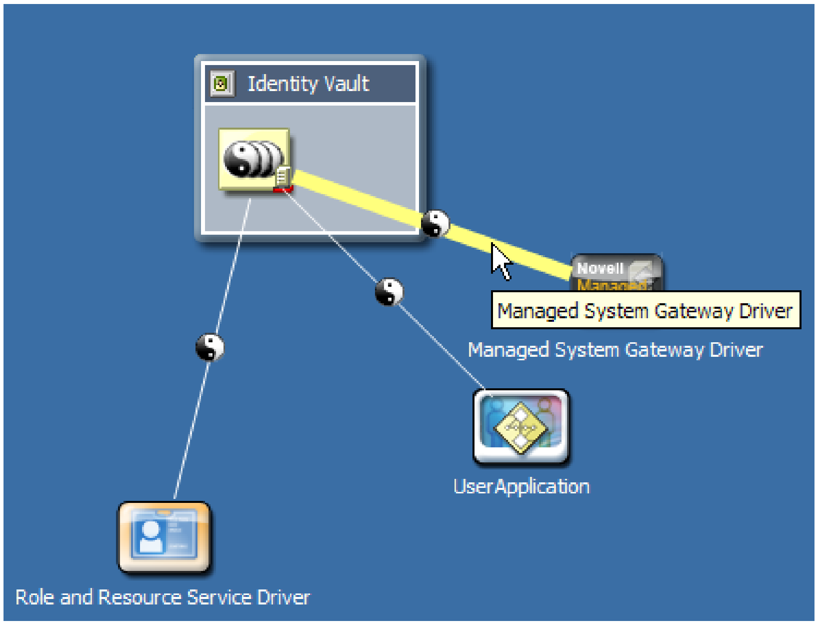
11 Select *yes* or *no* to indicate whether you will using a remote loader, then click *Next*.

12 If everything looks correct on the Confirm Installation Tasks screen, click *Finish*.

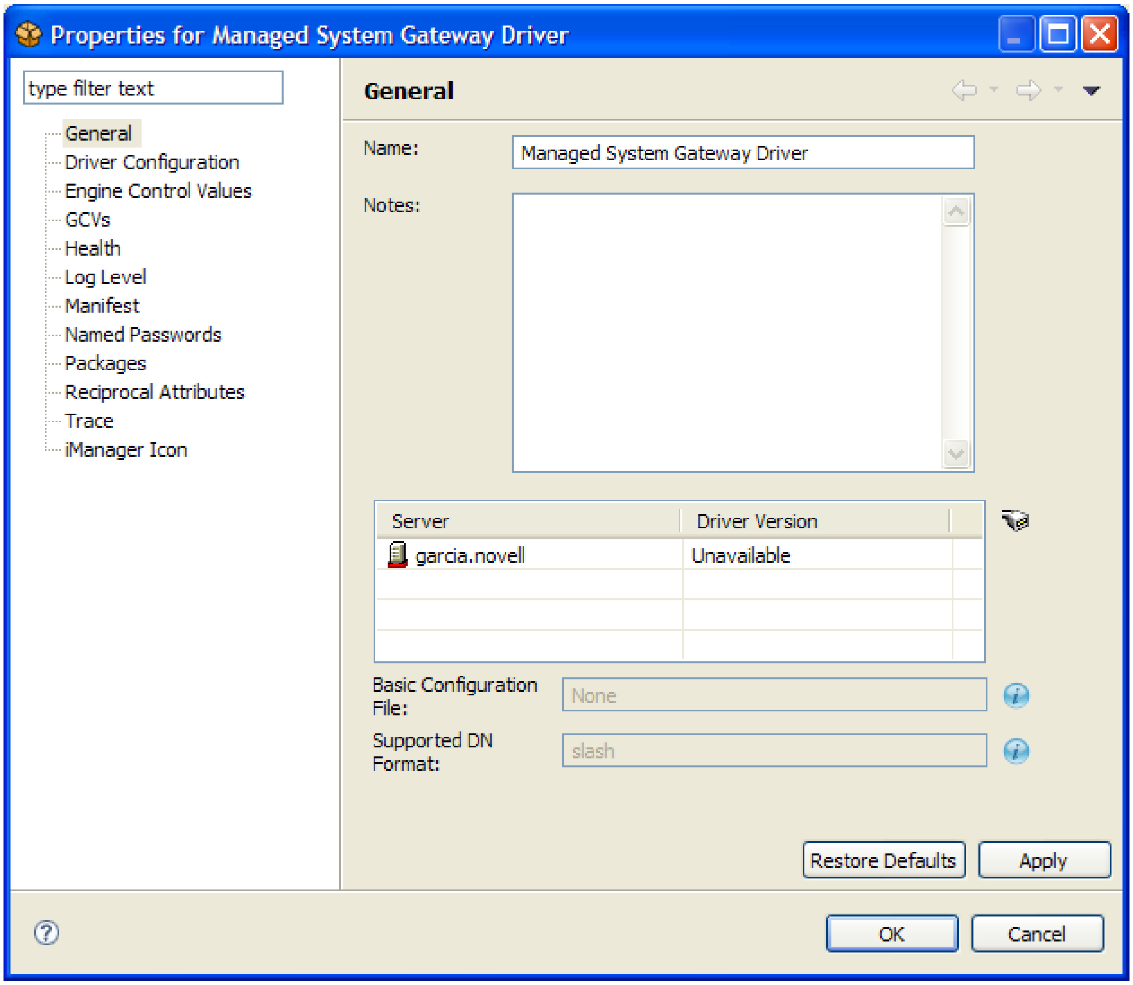
Designer adds the Managed System Gateway Driver to the Modeler view:


Identity Vault
Novell Managed System Gateway
Managed System Gateway Driver
UserApplication
Role and Resource Service Driver

13 To configure additional settings for the driver, right-click the line connecting the Managed System Gateway Driver to the driver set and select *Properties*.


Identity Vault
Novell Managed
Managed System Gateway Driver
Managed System Gateway Driver
UserApplication
Role and Resource Service Driver

14 Designer displays the Properties for Managed System Gateway Driver dialog box:



General

Name: Managed System Gateway Driver

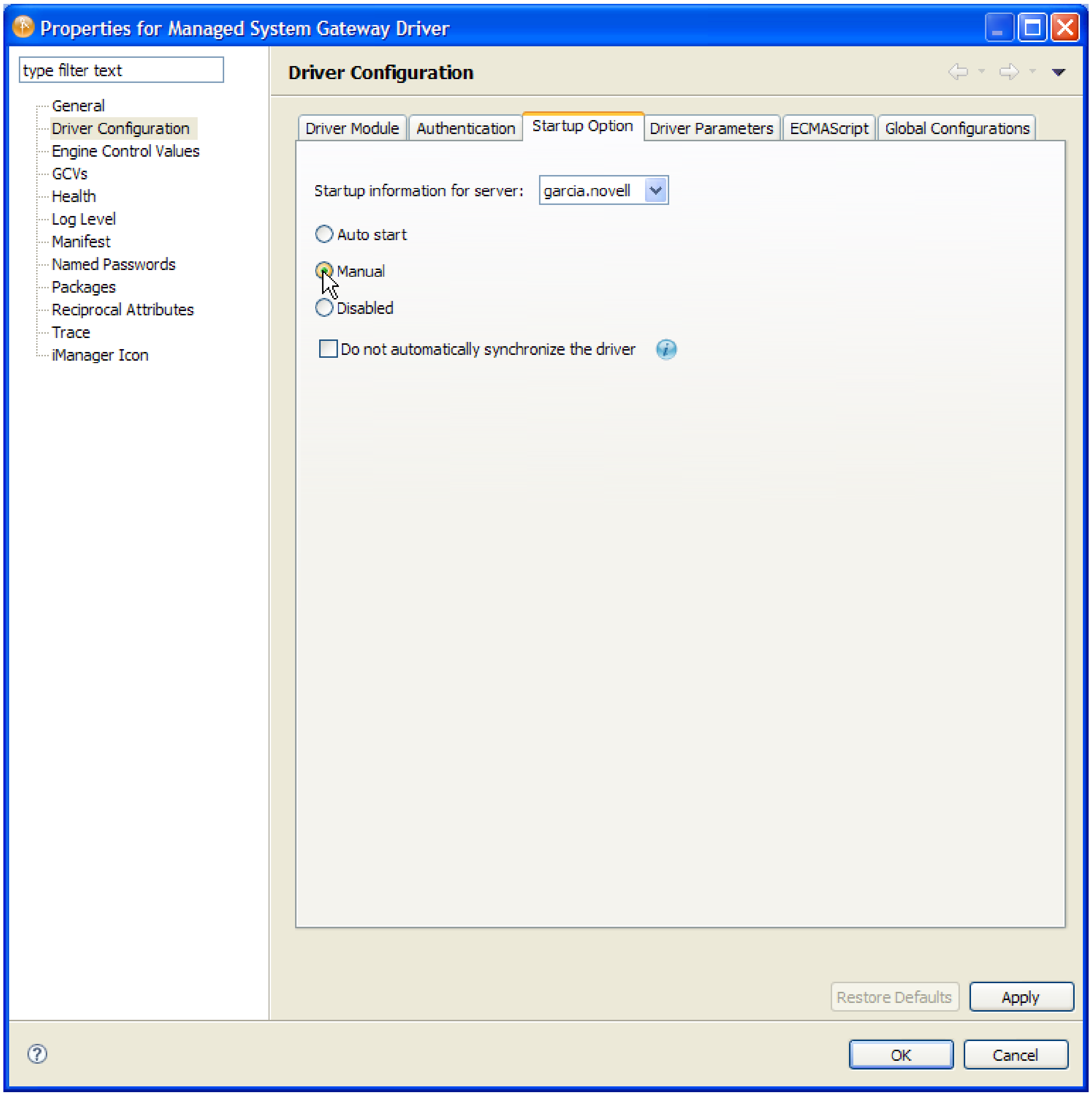
Notes:

Server	Driver Version
garcia.novell	Unavailable

Basic Configuration File: None

Supported DN Format: slash

15 Select *Driver Configuration* in the left menu and click the *Startup Option* tab. Select *Manual* for the startup setting:



Properties for Managed System Gateway Driver

Driver Configuration

Startup information for server: garcia.novell

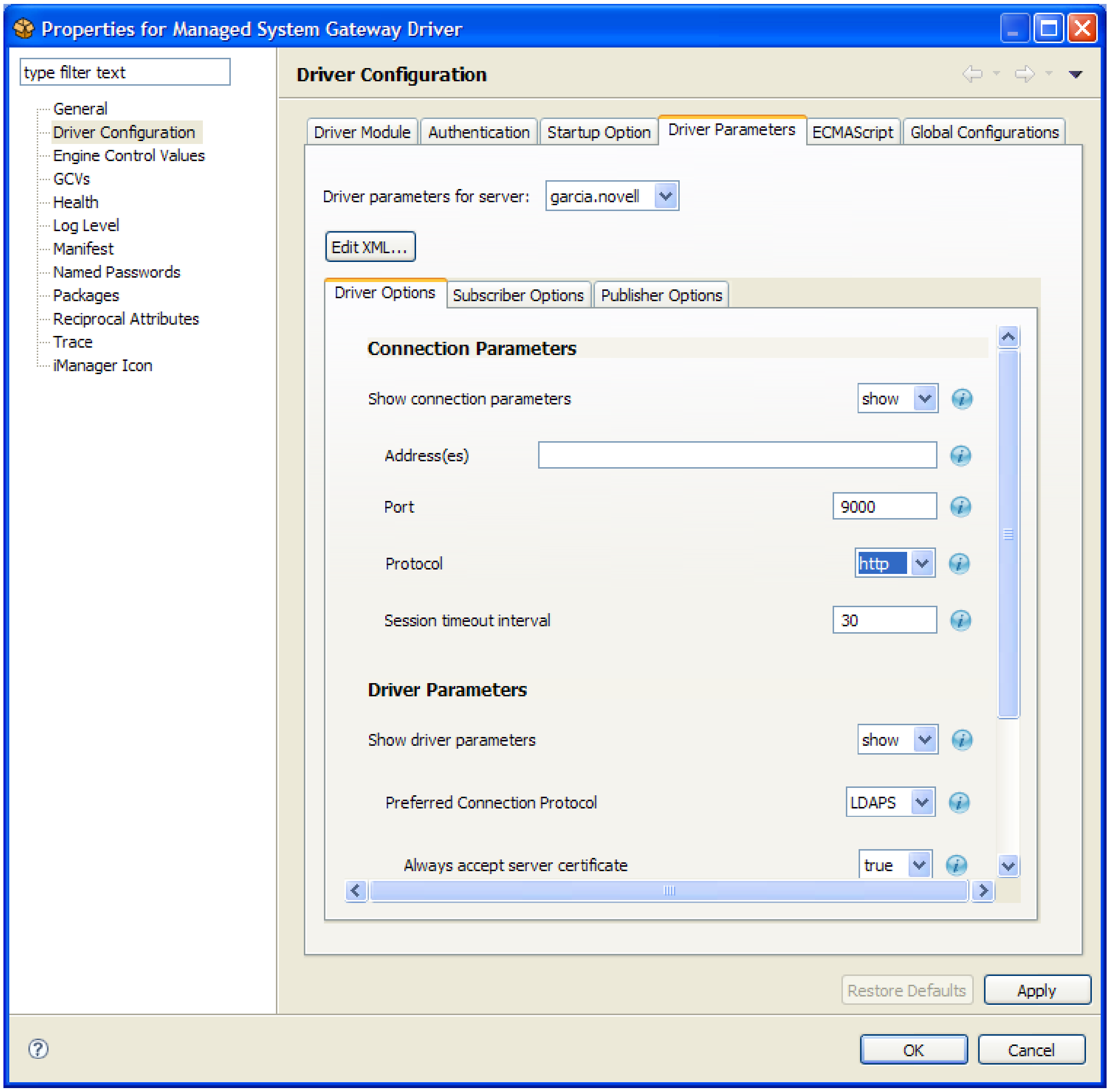
○ Auto start

● Manual

○ Disabled

□ Do not automatically synchronize the driver

16 Click the *Driver Parameters* tab and select *show* under *Connection Parameters* to show the settings you provided to the wizard:



Driver parameters for server: garcia.novell

Connection Parameters

Show connection parameters: show

Address(es):

Port: 9000

Protocol: http

Session timeout interval: 30

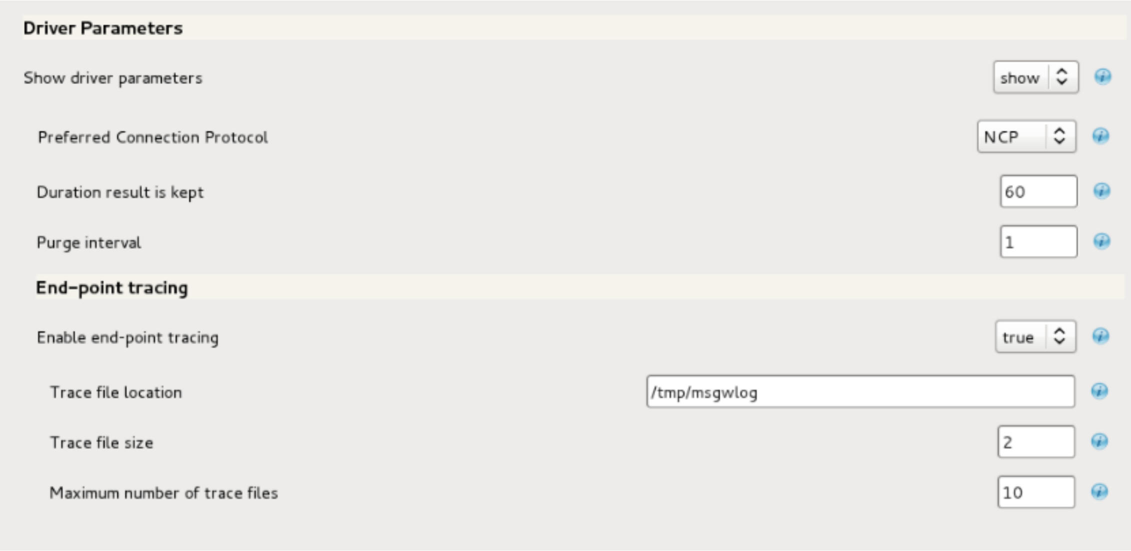
Driver Parameters

Show driver parameters: show

Preferred Connection Protocol: LDAPS

Always accept server certificate: true

17 Select *show* under *Driver Parameters.*



Driver Parameters

Show driver parameters: show

Preferred Connection Protocol: NCP

Duration result is kept: 60

Purge interval: 1

End-point tracing

Enable end-point tracing: true

Trace file location: /tmp/msgwlog

Trace file size: 2

Maximum number of trace files: 10

You can optionally make changes to the Connection Parameters, Driver Parameters, and Publisher Options settings. The settings that you might want to modify are described below:

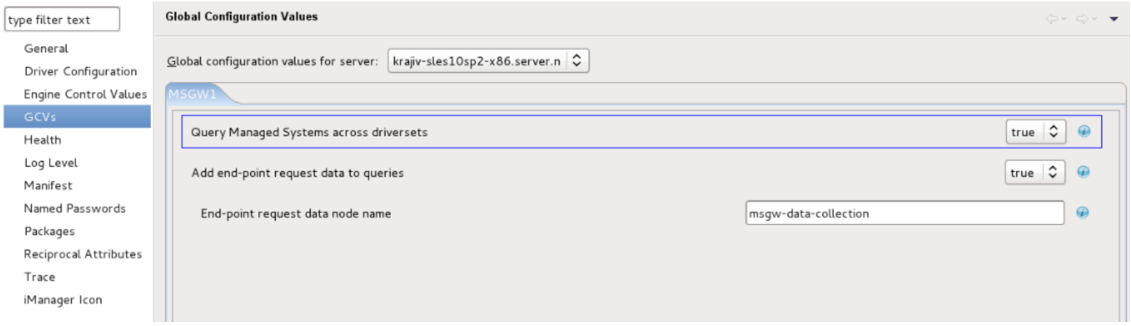
Parameter Type	Parameter	Description
Connection Parameters	Address(es)	IP address on which the driver should listen. If you want the driver to listen on more than one interface, you can provide a comma-separated list of addresses. **NOTE:** If you use the loopback address of 127.0.0.1 as the IP address for the Managed System Gateway driver when configuring with the integrated installer, that is valid and will work correctly. However, when you use the endpoints, having the IP address be the loopback (127.0.0.1) does not work. In this case, you need to specify the correct IP address.

	Port	The port on which the driver accepts requests. If multiple addresses are specified, the same port number is used to listen on all the interfaces. For example, if the address is set to 164.99.88.30,127.0.0.1, and the port is set to 9000, then the driver listens on the following:
		`164.99.88.30:9000`
		`127.0.0.1:9000`

	Protocol	Protocol for accessing the driver. The choices are HTTP and HTTPS. If you select HTTPS, you need to provide the KMO name.
	Session timeout interval	Defines a timer for the session that controls how long (in minutes) the session can be inactive before it is terminated.
Driver Parameters	Duration result is kept	Specifies the duration (in minutes) for which query results are available before they are marked for purging. All results that exceed this duration are purged in the next purge cycle.
	Purge interval	Specifies the duration (in hours) between purge cycles. A new purge cycle is executed when this interval is reached. The purge cycle cleans up all results that have been marked for purging.

Parameter Type	Parameter	Description
	End-point tracing	For release 4.0.2, the following options have been added to give you control over end-point tracing for the driver. The end-point logs are useful for debugging connection issues: ◆ *Enable end-point tracing*: If set to true, all end-point invocations will be logged to a file. ◆ *Trace file location*: Specifies the directory where the trace files will be created. A trace file named `MsGateway.log` will be written to this location. ◆ *Trace file size*: Specifies the maximum size for a trace file in MB. Once the maximum size is reached or the driver is restarted, the trace file is backed up. ◆ *Maximum number of trace files*: Specifies the maximum number of trace files that should be preserved. Older trace files are deleted when the maximum count is reached.
Publisher Options	Publisher heartbeat interval	Specifies the duration (in minutes) between heartbeats. Whenever this interval is reached and there has been no traffic on the Publisher channel, a new heartbeat is sent.

18 Optionally, open the *GCVs* tab to set the Global Configuration Values for the server.



Global Configuration Values

Global configuration values for server: krajiv-sles10sp2-x86.server.n

Query Managed Systems across driversets: true

Add end-point request data to queries: true

End-point request data node name: msgw-data-collection

In release 4.0.2, you can set the following values for the Managed System Gateway Driver:

- *Query Managed Systems across driversets*: Defines the scope of operation for the Managed System Gateway Driver. If set to true, the driver returns information about managed systems across driversets. Otherwise, the scope is restricted to the local driverset.
- *Add end-point request data to queries*: Specifies whether end-point request data be added to the queries sent by the driver. This will be added as an `operation-data` node.
- *End-point request data node name*: Specifies a node-name that will be added to the `operation-data` of the queries. The node attributes will contain the details about the request.

19 Open the other tabs associated with Driver Configuration to review the settings.

You can make changes to the settings, if you like, but you do not need to in order to get the driver up and running.

20 Select the *Packages* option in the left menu to see which packages have been installed.

You do not need to change the *Operation* settings unless you want to uninstall a particular package.

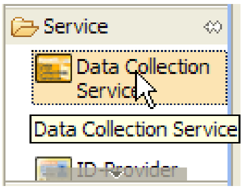
21 Click *Apply* when you are satisfied with all of the settings.

22 After configuring the driver packages and parameters, you must enable the Subscriber channel for the Reporting Module to function correctly.

2.4.3 Configuring the Identity Manager Driver for Data Collection Service

NOTE: After you configure the Data Collection Service driver, ensure that you install all available entitlement packages for the other drivers in your environment. The Data Collection Service driver requires these entitlement packages, even if you do not use entitlements to manage objects.

1 In the Modeler view, select *Service* > *Data Collection Service* in the palette.



2 Drag the icon for the *Data Collection Service* application onto the Modeler view.

Designer displays the Driver Configuration Wizard.

3 Select *Data Collection Service Base* and click *Next*.

NOTE: For the 4.0.2 release, you need to have version 2.0.0.20120509205909 of the Data Collection Service Base package.

4 Make sure any mandatory features listed are selected and click *Next*.

5 Make sure the optional features listed are selected and click *Next*.

6 The interface displays a dialog box to inform you that need an additional package called LDAP Library. Click *OK* to install the required package.

7 (Optional) On the Install LDAP Library page, if you want to configure a global connection profile for all drivers, click the dropdown menu and select *Yes*.

8 Click *Next*.

9 Specify the Data Collection Service driver name you want to use, then click *Next*.

10 Specify the IP address and port of the reporting module, as well as the protocol you want to use. Also, specify the user and password of the Reporting Administrator for authentication.

11 Click *Next*.

The wizard now displays a screen that allows you to specify settings for the Identity Vault Registration and Managed System Gateway Registration.

12 For the Identity Vault Registration, provide a name and description, as well as the IP address for the Identity Vault.

13 Select *Yes* for *Register Managed System Gateway*. For the *Managed System Gateway Registration*, provide the DN for the driver, as well as the user and password for the LDAP administrator.

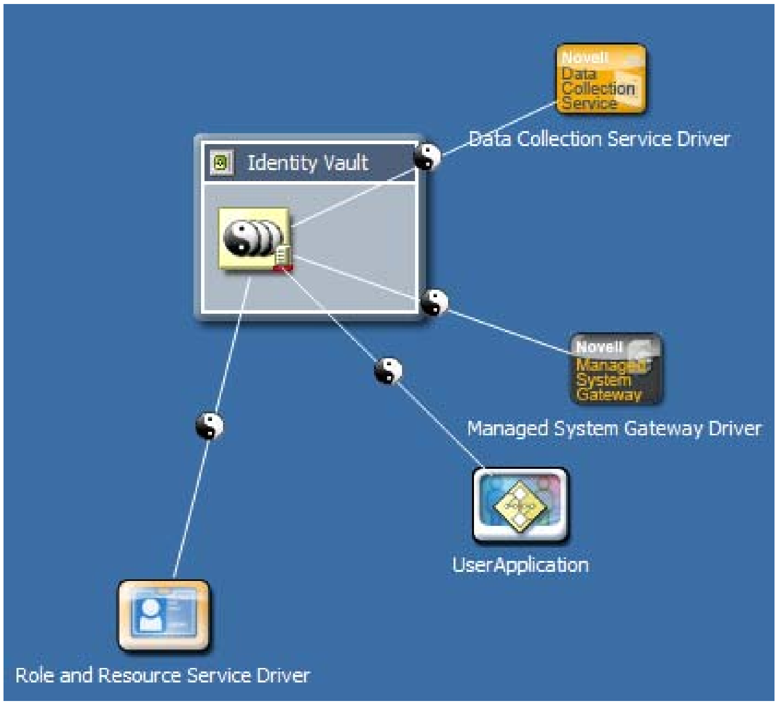
NOTE: Because the driver has not yet been deployed, the browse function does not show the Managed System Gateway driver you just configured, so you might need to type the DN for the driver.

14 Click *Next*.

The wizard now displays the Confirm Installation Tasks screen.

15 If everything looks correct, click *Finish*.

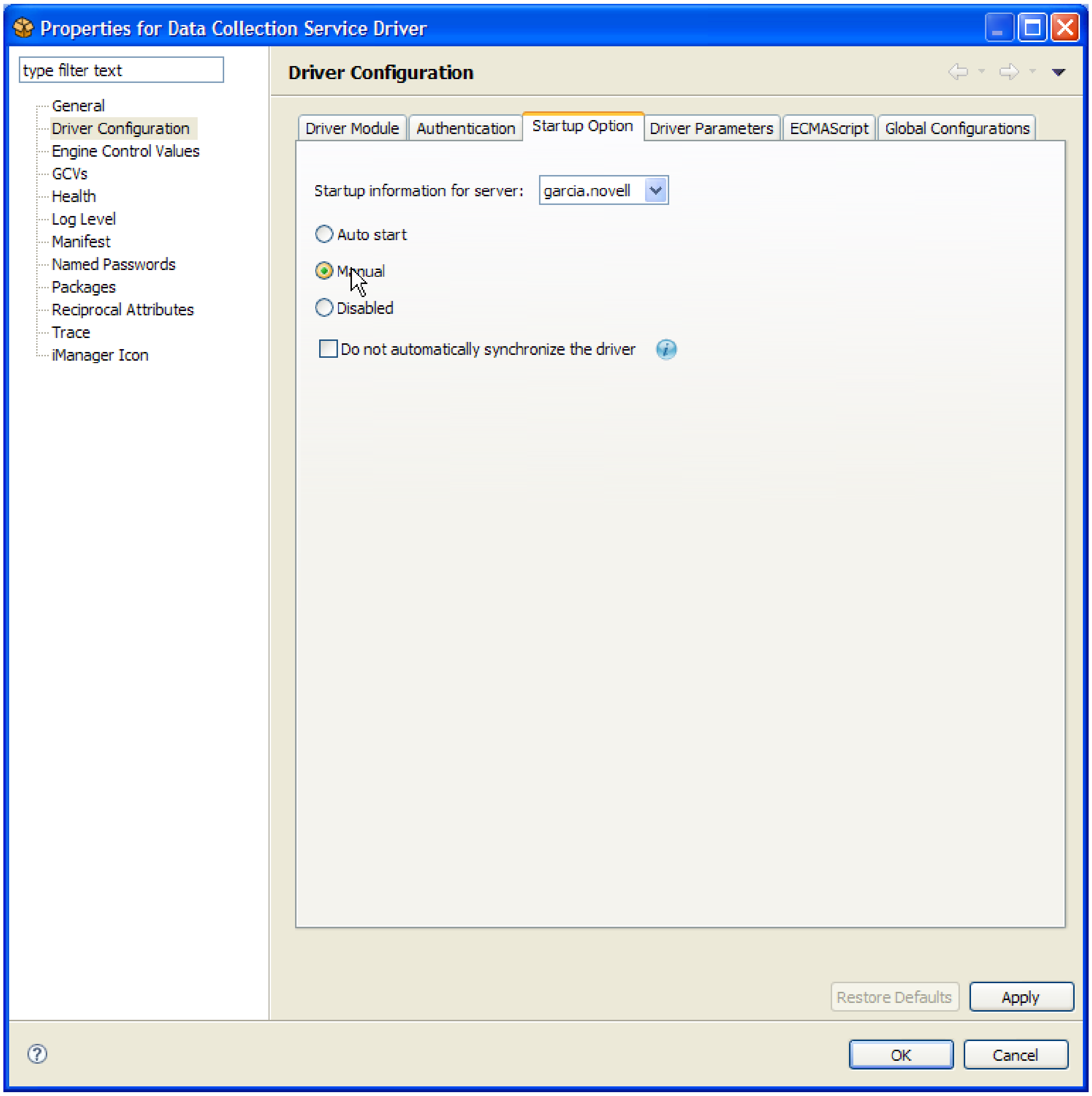
Designer adds the Data Collection Service Driver to the Modeler view:


Novell Data Collection Service
Data Collection Service Driver
Identity Vault
Novell Managed System Gateway
Managed System Gateway Driver
UserApplication
Role and Resource Service Driver

16 To configure additional settings for the driver, right-click the line connecting the Data Collection Service Driver to the driver set and select *Properties*.

Designer now displays the *Properties for Data Collection Service Driver* dialog.

17 Select *Driver Configuration* in the left menu and click the *Startup Option* tab. Select *Manual* for the startup setting:



Startup information for server: garcia.novell

○ Auto start

● Manual

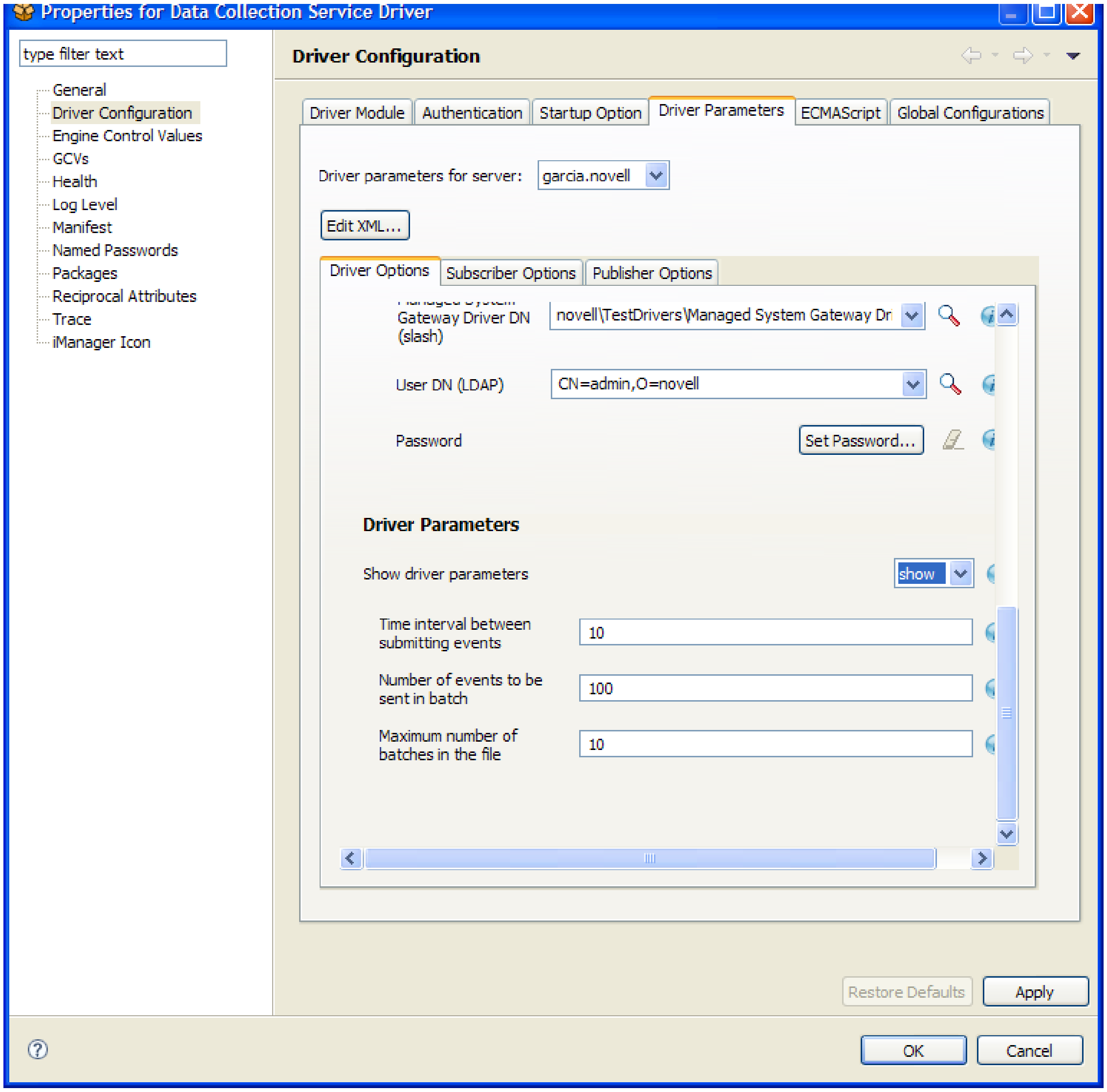
○ Disabled

□ Do not automatically synchronize the driver

18 Select *Driver Configuration* in the left menu and click the *Driver Parameters* tab. Select *show* under *Connection Parameters*. Also, select *show* under *Driver Parameters*.

19 Scroll down to the settings shown in the *Driver Parameters* section.

You might want to change the values for some of these settings. In a test environment, you might want to use low numbers to be sure your events are being processed correctly. However, in a production environment, you probably want to use higher numbers so that the system does not process events unnecessarily:



Driver parameters for server: garcia.novell

Managed System Gateway Driver DN (slash): novell\TestDrivers\Managed System Gateway Dr

User DN (LDAP): CN=admin,O=novell

Password

Driver Parameters

Show driver parameters: show

Time interval between submitting events: 10

Number of events to be sent in batch: 100

Maximum number of batches in the file: 10

You can optionally make changes to the Connection Parameter, Identity Vault Registration, Managed System Gateway Registration, and Driver Parameters settings. The settings that you might want to modify are described below:

Parameter Type	Parameter	Description
Connection Parameters	IP Address	IP address where the reporting module is installed and running.
	Port	Port number for the reporting module (for REST connections).
	Protocol	Protocol for accessing the reporting module. The choices are HTTP and HTTPS. If you select HTTPS, you need to indicate whether you always trust the server’s certificate.

Parameter Type	Parameter	Description
Identity Vault Registration	Name	Provides the name you want to use to refer to your Identity Vault within the reporting module.
	Description	A short description of the Identity Vault.
	Address	IP address of the Identity Vault. `164.99.130.127` **NOTE:** You must specify an IP address. Do not specify an address of “localhost” for the Identity Vault Registration.
Managed System Gateway Registration	Register Managed System Gateway	Indicates whether you want to register the Managed System Gateway Driver.
	Managed System Gateway Driver DN (slash)	Specifies the DN of the Managed System Gateway Driver in slash format.
	User DN (LDAP)	Specifies the LDAP DN of the user that the driver should use to authenticate to the Managed System Gateway Driver. This DN must exist in the Identity Vault.
	Password	Specifies the password for the user.
Driver Parameters	Time interval between submitting events	The maximum amount of time, in minutes, that an event can remain in the persistence layer before being submitted to the DCS (and to the database for the reporting module).
	Number of events to be sent in batch	Specifies the number of events that can be gathered by the persistence layer before it sends them over to the DCS (without waiting for the timeout to occur). **NOTE:** In environments where the driver receives large numbers of events, we recommend setting the number of events per batch to 500. This batch size helps to increase the speed at which the driver processes events.
	Maximum number of batches in the file	Defines an upper limit for the storage capacity of the persistence layer. **NOTE:** In environments where the driver receives large numbers of events, we recommend setting the number of batches per file to no more than 10. If you set this parameter to a value greater than 10, the driver cannot process events as efficiently.

20 Select *Engine Control Values* in the left menu.

For the *Qualified form for DN-syntax attribute values* setting, be sure that *True* is selected so that DNs are configured properly.

21. Open the other tabs associated with Driver Configuration to review the settings.

    You can make changes to the settings, if you like, but you do not need to in order to get the driver up and running.

22. Select *GCVs* in the left menu, then select *Show* for *Show override options*.
23. (Optional) Provide new values that override the global configuration values.
24. Click *OK*.

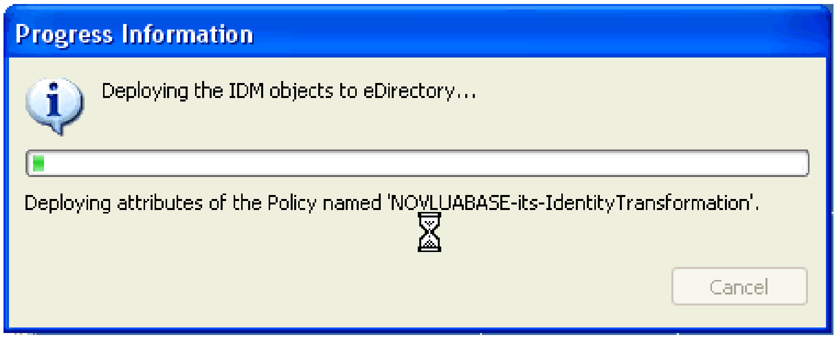
    Designer returns you to the Modeler view.

2.4.4 Deploying the Drivers

To deploy the drivers you just configured:

1. Select the driver set (either in the Modeler view or in the Outline view).
2. Choose *Live > Deploy*.

   Designer displays a progress window that shows which objects are being deployed:



Deploying the IDM objects to eDirectory...

Deploying attributes of the Policy named 'NOVLUABASE-its-IdentityTransformation'.

For each driver deployed, you see a dialog box prompting you for the security equivalent. You need to provide the LDAP Administrator for each driver.

2.4.5 Backing Up and Restoring the Reporting Module

If necessary, you can back up the EAS PostgreSQL database the Identity Reporting Module uses to store audit data, event data, and configuration information. The database contains three separate schemas:

- **public:** Stores audit data, event source configuration information, and other administrative information.
- **idm_rpt_data:** Stores data collected by the Managed System Gateway Driver and the Data Collection Service Driver, as well as data collection configuration information.
- **idm_rpt_cfg:** Stores reporting configuration information, reports, and report scheduling information.

Backing Up and Restoring the idm_rpt_data and idm_rpt_cfg Schemas

We recommend you use the standard PostgreSQL backup and restore procedures to back up or restore the `idm_rpt_data` and `idm_rpt_cfg` schemas. For detailed information on backing up and restoring PostgreSQL databases, see "Backup and Restore" in the PostgreSQL documentation (http://www.postgresql.org/docs/8.4/static/backup.html)

Backing Up and Restoring the public Schema

However, for the public schema, you should use the `backup_util.sh` utility provided with Identity Manager. The utility is located in the `/opt/novell/sentinel/bin` directory on the Identity Manager server.

For detailed information on using the backup_util.sh script, see "Backing Up and Restoring Data" (https://www.netiq.com/documentation/sentinel70/s701_admin/data/bn1fcap.html), in the *NetIQ Sentinel Administration Guide* (https://www.netiq.com/documentation/sentinel70/s701_admin/data/bookinfo.html).

2.4.6 Runtime Configuration and Troubleshooting

This section provides some additional configuration steps you should take to ensure that the runtime environment is operating correctly. It also provides troubleshooting techniques, as well as some information about database tables that are of particular interest.

- "Verifying That the Managed Systems Are Working" on page 73
- "Starting the Drivers" on page 79
- "Migrating the Data Collection Service Driver" on page 86
- "Starting the Collection Process for the Managed System Gateway Driver" on page 88
- "Adding Support for Custom Attributes and Objects" on page 92
- "Adding Support for Multiple Driversets" on page 94
- "Configuring the Drivers to Run in Remote Mode with SSL" on page 95
- "Troubleshooting the Drivers" on page 96

Verifying That the Managed Systems Are Working

Before you start the Managed System Gateway Driver and the Data Collection Service Driver, you should confirm that the underlying managed systems are properly configured. By doing this, you can isolate problems with your environment that do not relate to the configuration of the reporting drivers.

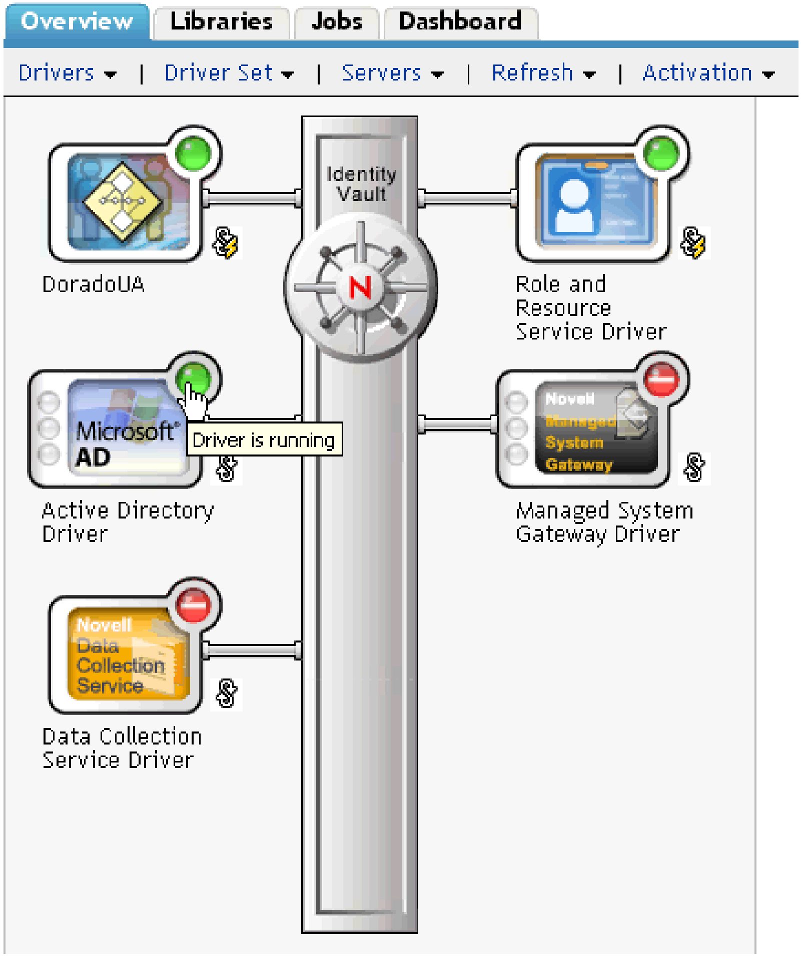
To troubleshoot your Active Directory environment, for example, you might want to test an Active Directory entitlement by assigning a resource in the User Application.

NOTE: Details on configuring the Active Directory driver are provided in the *Driver for Active Directory Implementation Guide* (http://www.netiq.com/documentation/idm40drivers/index.html).

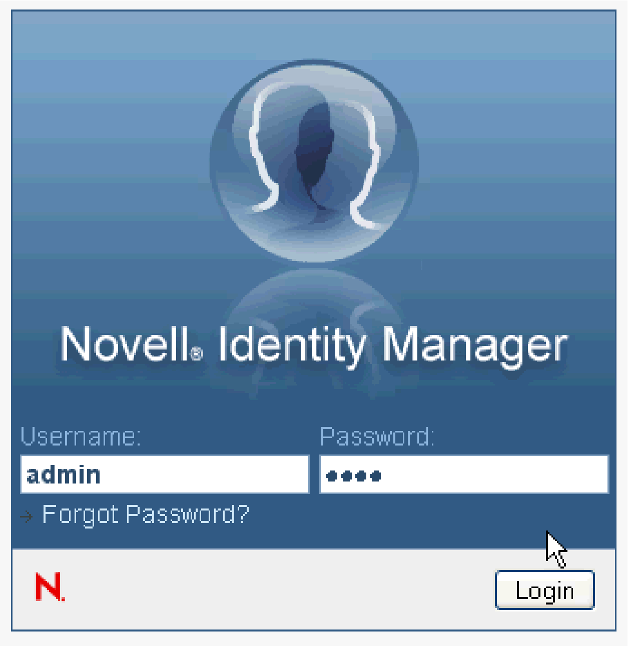
The following steps demonstrate one way to confirm that Active Directory is properly configured:

1 Make sure that the User Application and the Identity Reporting Module are both running on the same server.

2 In iManager, verify that the User Application Driver and the Role and Resource Service Driver are running, and make sure that the driver for the managed system is running:


Overview
Libraries
Jobs
Dashboard
Drivers
Driver Set
Servers
Refresh
Activation
Identity Vault
DoradoUA
Role and Resource Service Driver
Microsoft AD
Driver is running
Active Directory Driver
Novell Managed System Gateway
Managed System Gateway Driver
Novell Data Collection Service
Data Collection Service Driver

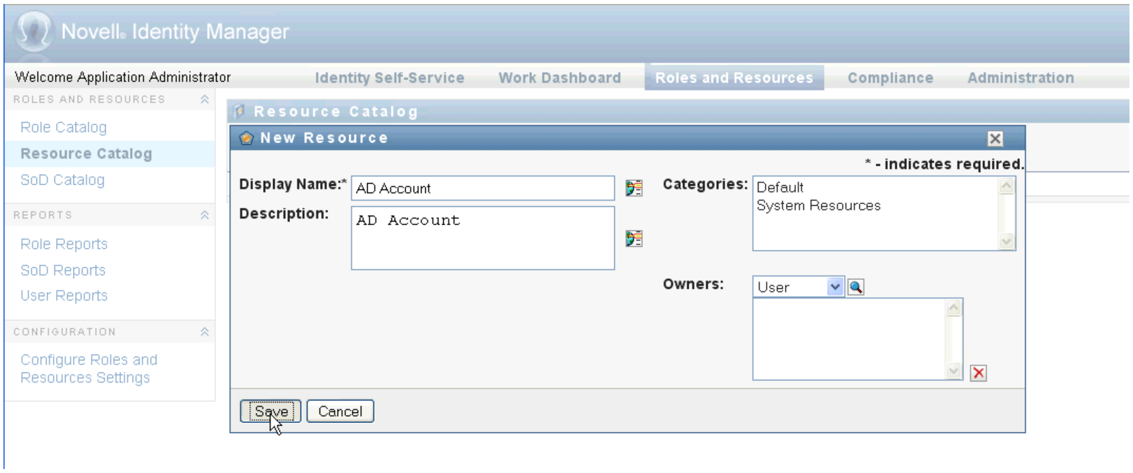
3 To verify that the User Application can retrieve information from Active Directory, first log into the User Application as a User Application Administrator:



Username: admin

Password: ●●●●

4 In the Resource Catalog, create a new resource for Active Directory accounts:



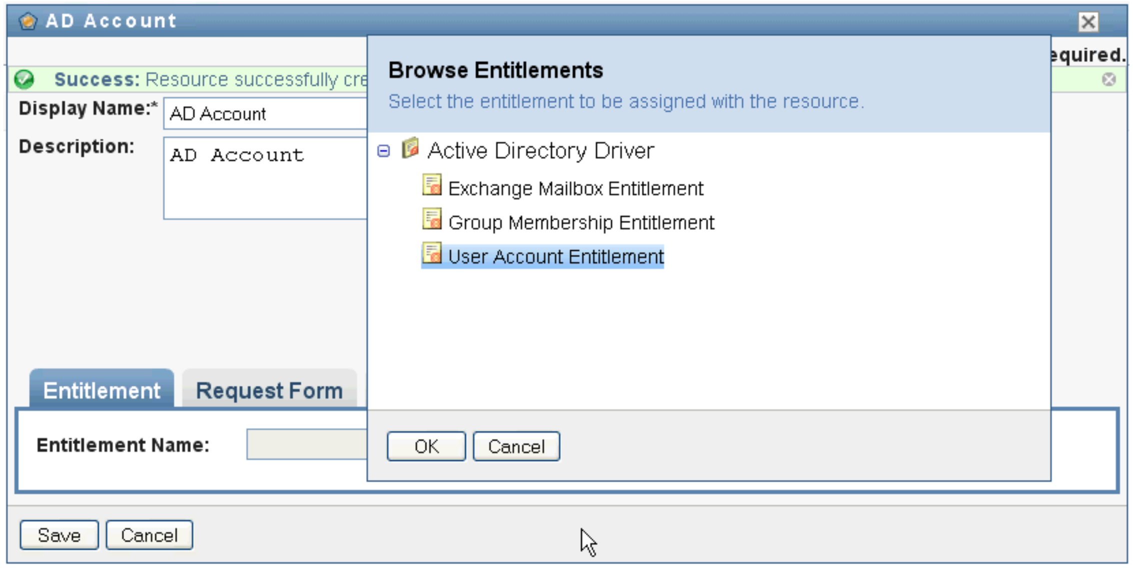
Display Name:* AD Account

Description: AD Account

Categories: Default
System Resources

Owners: User

5 Bind the resource to an entitlement within the Active Directory Driver, such as *User Account Entitlement*:



AD Account

Success: Resource successfully cre

Display Name:* AD Account

Description: AD Account

...equired.

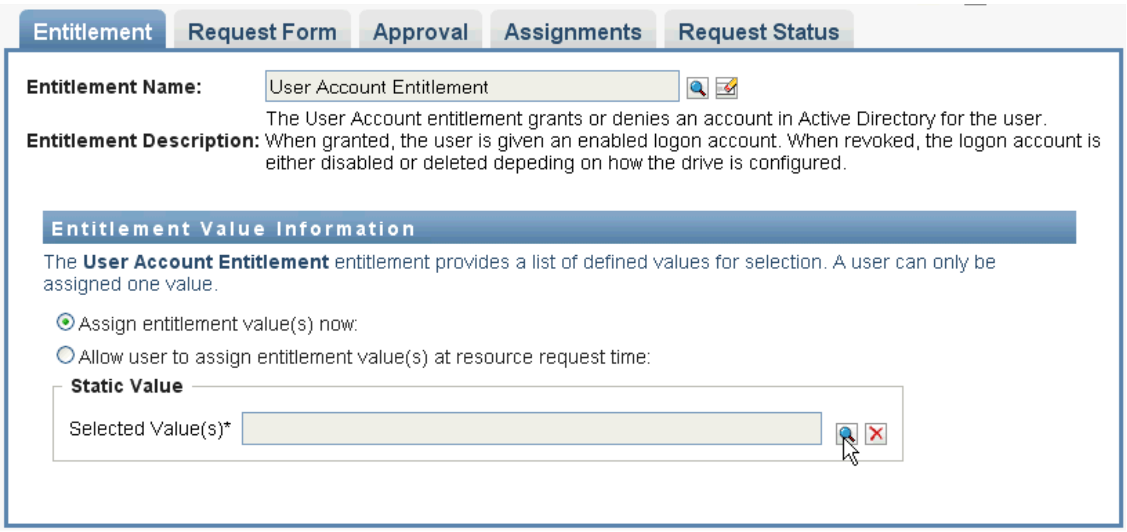
Browse Entitlements

Select the entitlement to be assigned with the resource.

- Active Directory Driver
  - Exchange Mailbox Entitlement
  - Group Membership Entitlement
  - User Account Entitlement

Notice that the User Application is able to retrieve the entitlement from the driver.

6 Because this particular resource pertains to accounts, configure the resource to assign an account value:



Entitlement Name: User Account Entitlement

Entitlement Description: The User Account entitlement grants or denies an account in Active Directory for the user. When granted, the user is given an enabled logon account. When revoked, the logon account is either disabled or deleted depeding on how the drive is configured.

Entitlement Value Information

The **User Account Entitlement** entitlement provides a list of defined values for selection. A user can only be assigned one value.

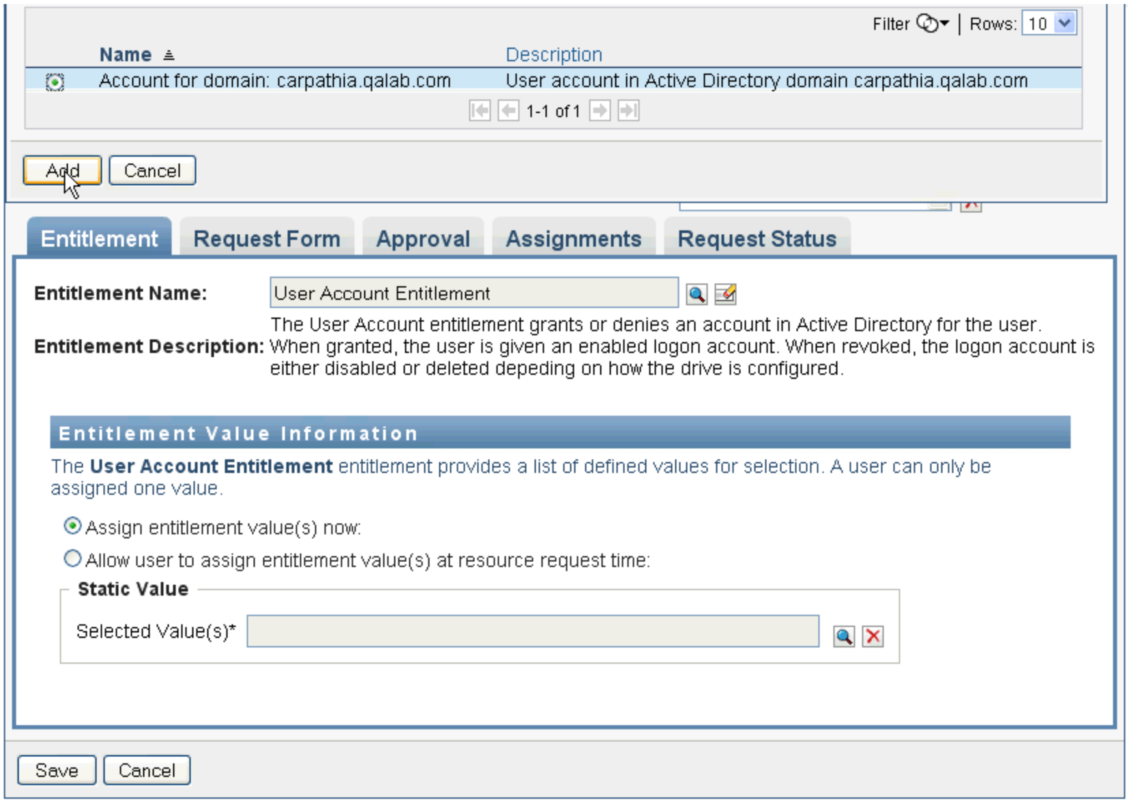
● Assign entitlement value(s) now:

○ Allow user to assign entitlement value(s) at resource request time:

Static Value

Selected Value(s)*

7 Select the account value and click *Add*:



Filter | Rows: 10

Name	Description
Account for domain: carpathia.qalab.com	User account in Active Directory domain carpathia.qalab.com

1-1 of 1

Entitlement Name: User Account Entitlement

Entitlement Description: The User Account entitlement grants or denies an account in Active Directory for the user. When granted, the user is given an enabled logon account. When revoked, the logon account is either disabled or deleted depeding on how the drive is configured.

Entitlement Value Information

The **User Account Entitlement** entitlement provides a list of defined values for selection. A user can only be assigned one value.

● Assign entitlement value(s) now:

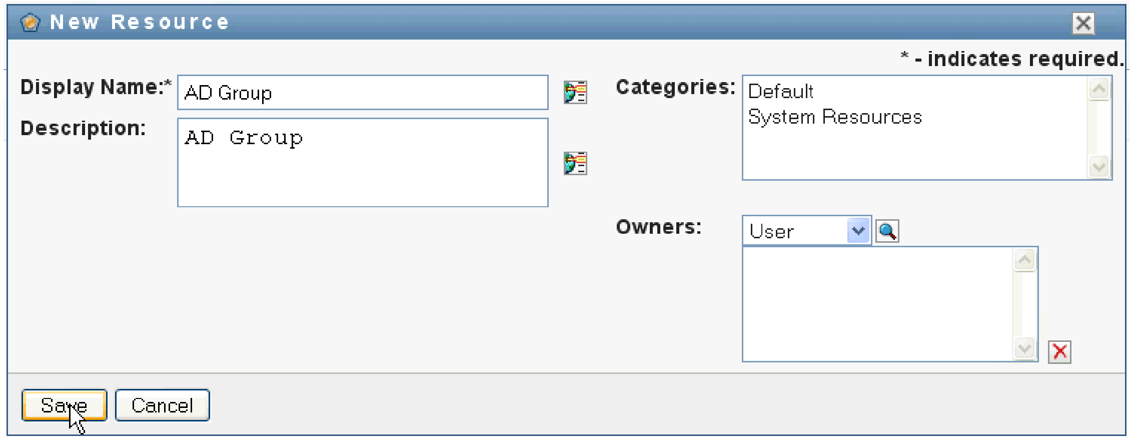
○ Allow user to assign entitlement value(s) at resource request time:

Static Value

Selected Value(s)*

This release supports two entitlement parameter formats, one for legacy values, and one for Identity Manager 4.0.2. When you create a new driver, the policy format used is the new format for Identity Manager 4.0.2.

8 Now create another resource that assigns groups:



New Resource

* - indicates required.

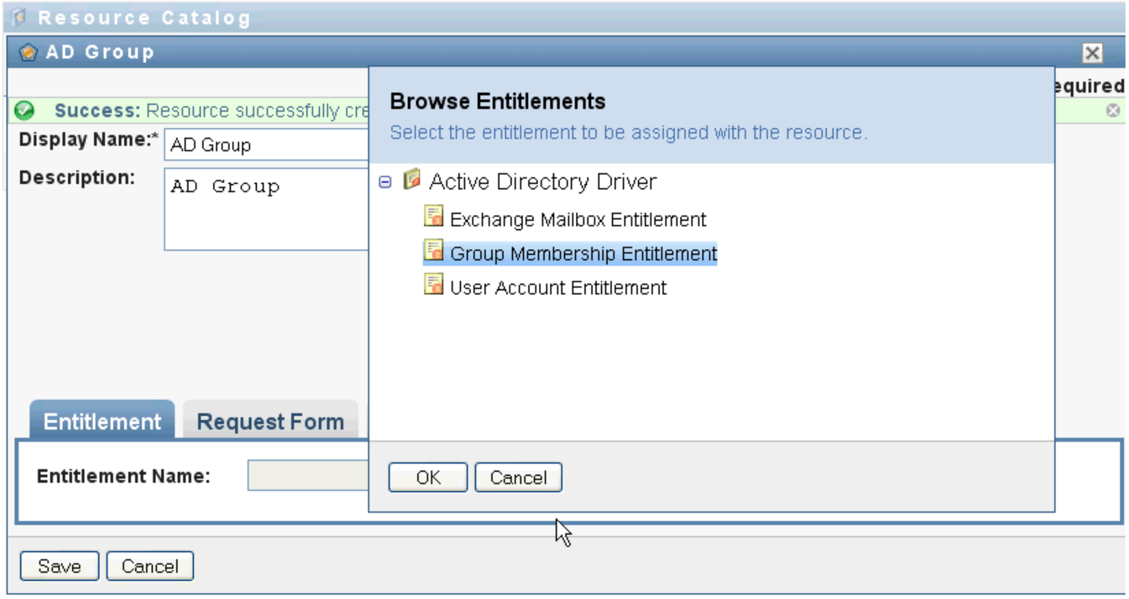
Display Name:* AD Group

Description: AD Group

Categories: Default
System Resources

Owners: User

9 Bind the resource to an entitlement that is suitable for groups. For this particular resource, map to the *Group Membership Entitlement*:



Success: Resource successfully cre

Display Name:* AD Group

Description: AD Group

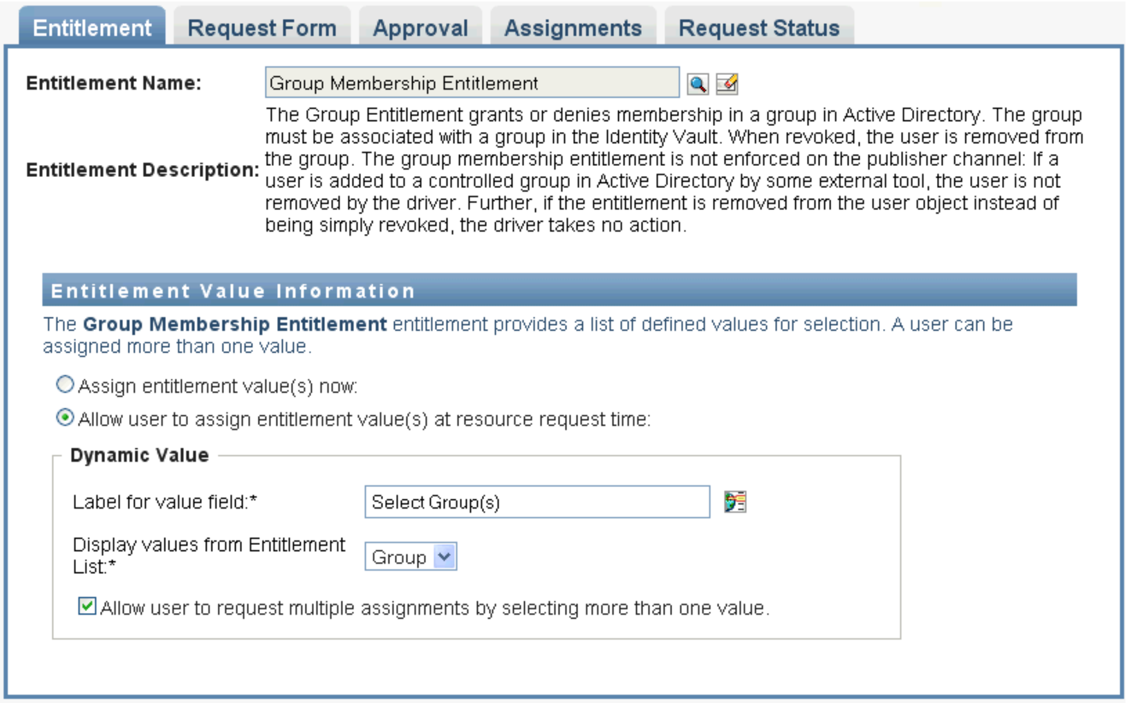
Browse Entitlements

Select the entitlement to be assigned with the resource.

- Active Directory Driver
  - Exchange Mailbox Entitlement
  - Group Membership Entitlement
  - User Account Entitlement

Entitlement Name:

10 Configure this resource so that the entitlement value is assigned by the user at request time, and allow the user to select multiple values for a single assignment request:



Entitlement Name: Group Membership Entitlement

Entitlement Description: The Group Entitlement grants or denies membership in a group in Active Directory. The group must be associated with a group in the Identity Vault. When revoked, the user is removed from the group. The group membership entitlement is not enforced on the publisher channel: If a user is added to a controlled group in Active Directory by some external tool, the user is not removed by the driver. Further, if the entitlement is removed from the user object instead of being simply revoked, the driver takes no action.

Entitlement Value Information

The **Group Membership Entitlement** entitlement provides a list of defined values for selection. A user can be assigned more than one value.

○ Assign entitlement value(s) now:

● Allow user to assign entitlement value(s) at resource request time:

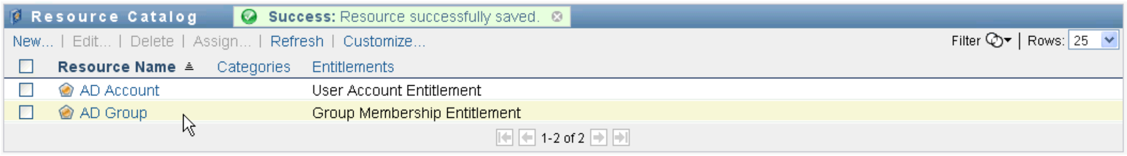
Dynamic Value

Label for value field:* Select Group(s)

Display values from Entitlement List:* Group

☑ Allow user to request multiple assignments by selecting more than one value.

11 Verify that the entitlements were created successfully:



Resource Catalog — **Success:** Resource successfully saved.

New... | Edit... | Delete | Assign... | Refresh | Customize... Filter | Rows: 25

□	Resource Name ▲	Categories	Entitlements
□	AD Account		User Account Entitlement
□	AD Group		Group Membership Entitlement

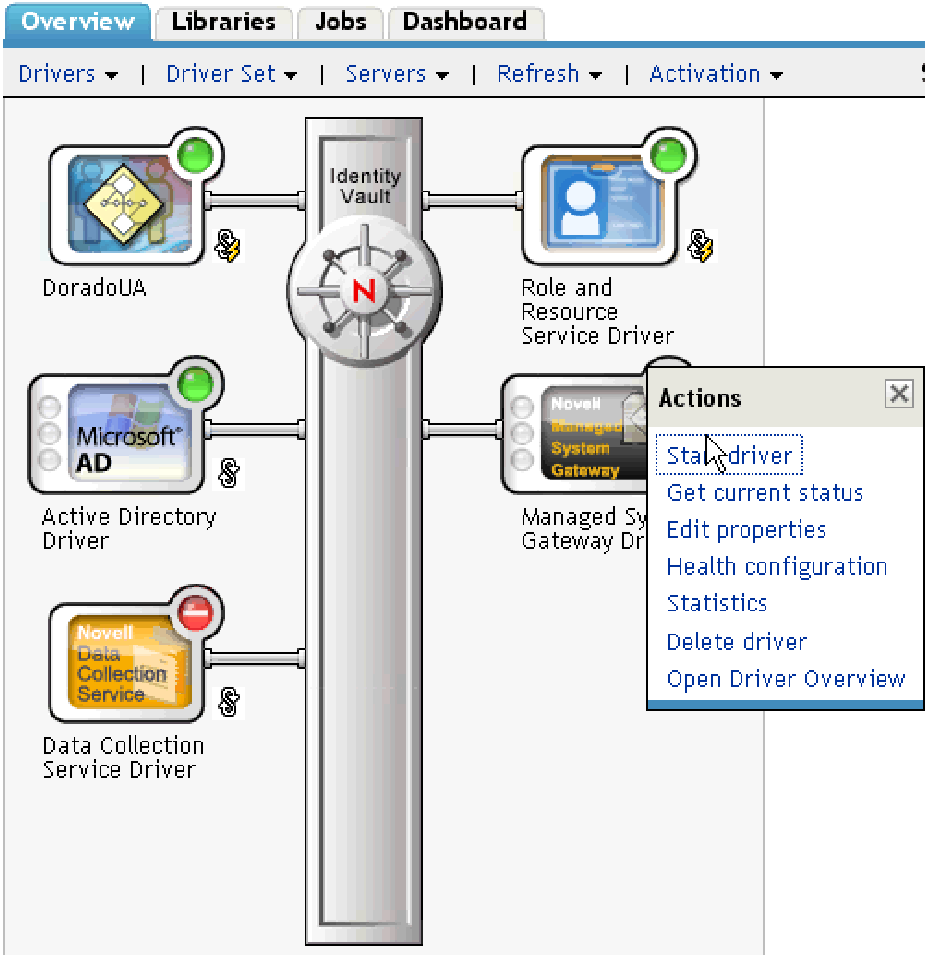
1-2 of 2

At this point, you can see that the underlying architecture for the managed system (in this case, Active Directory) is functioning properly. This can help you to troubleshoot any problems that might arise later on.

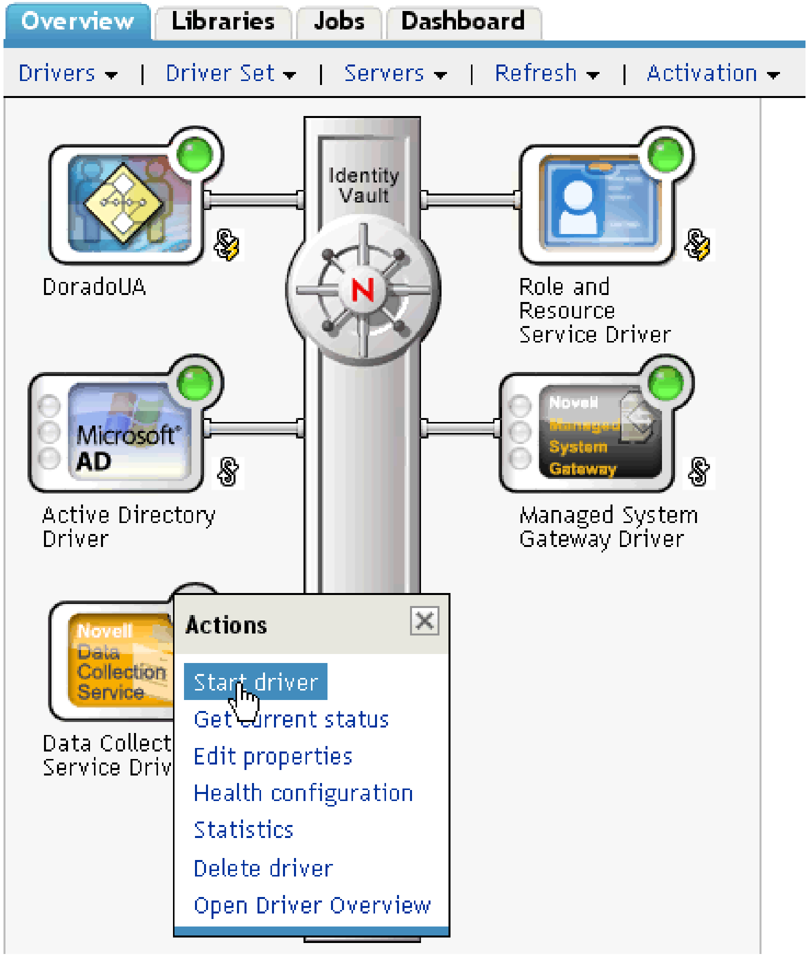
Starting the Drivers

This section provides instructions for starting the Managed System Gateway Driver and the Data Collection Service Driver.

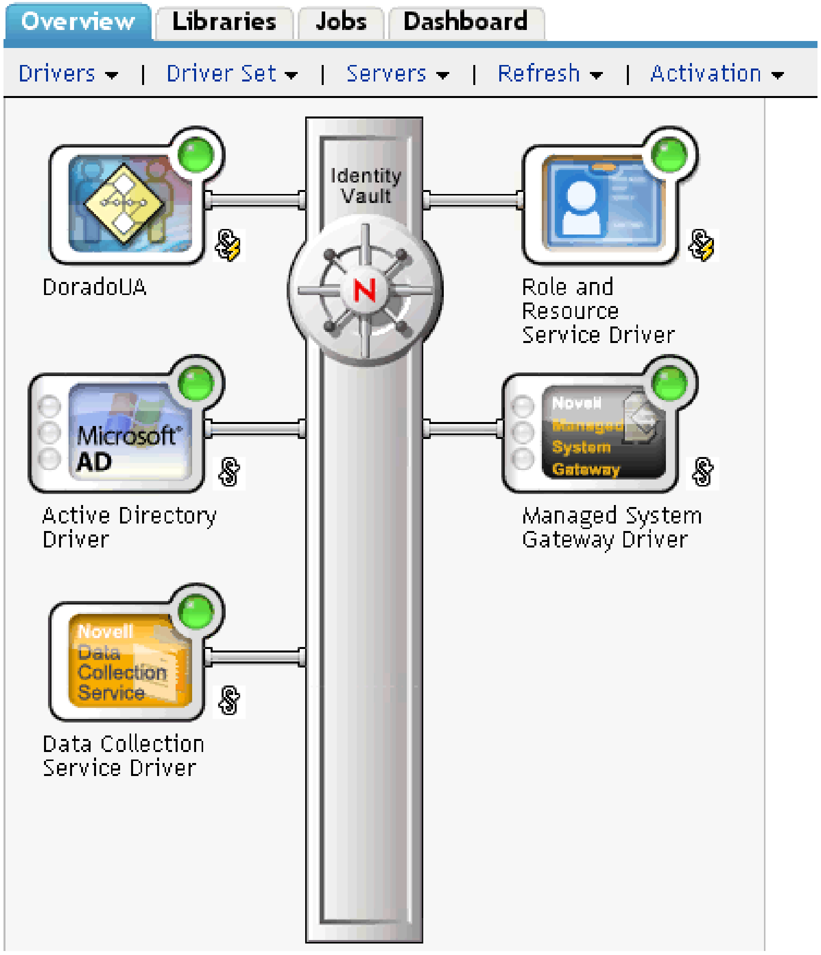
1 In iManager, first start the Managed System Gateway Driver:



2 Now start the Data Collection Service Driver:



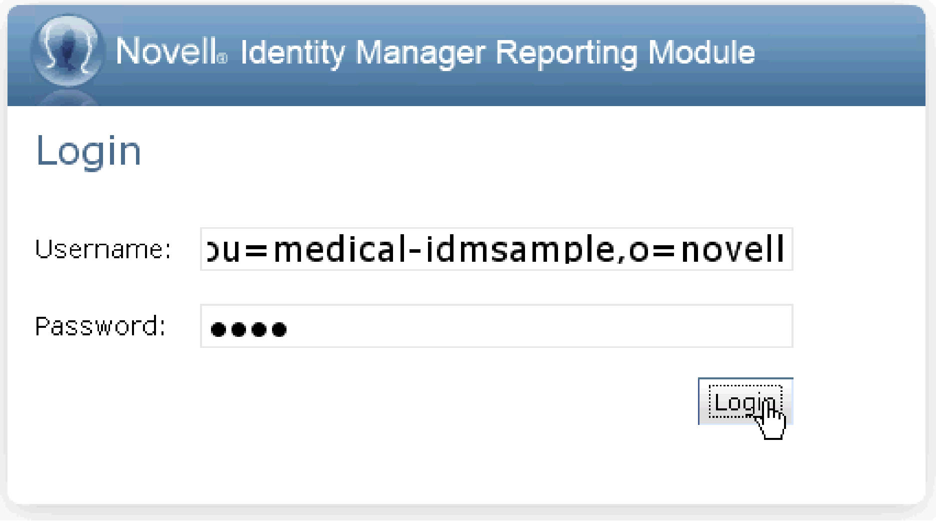
3 Verify that both drivers started successfully:


Overview
Libraries
Jobs
Dashboard
Drivers
Driver Set
Servers
Refresh
Activation
Identity Vault
DoradoUA
Role and Resource Service Driver
Microsoft AD
Active Directory Driver
Novell Managed System Gateway
Managed System Gateway Driver
Novell Data Collection Service
Data Collection Service Driver

4 After the drivers have started, you should see some additional information in the server console:

```
21:22:56,399 INFO  [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

5 Now log in to the reporting module as a Reporting Administrator:



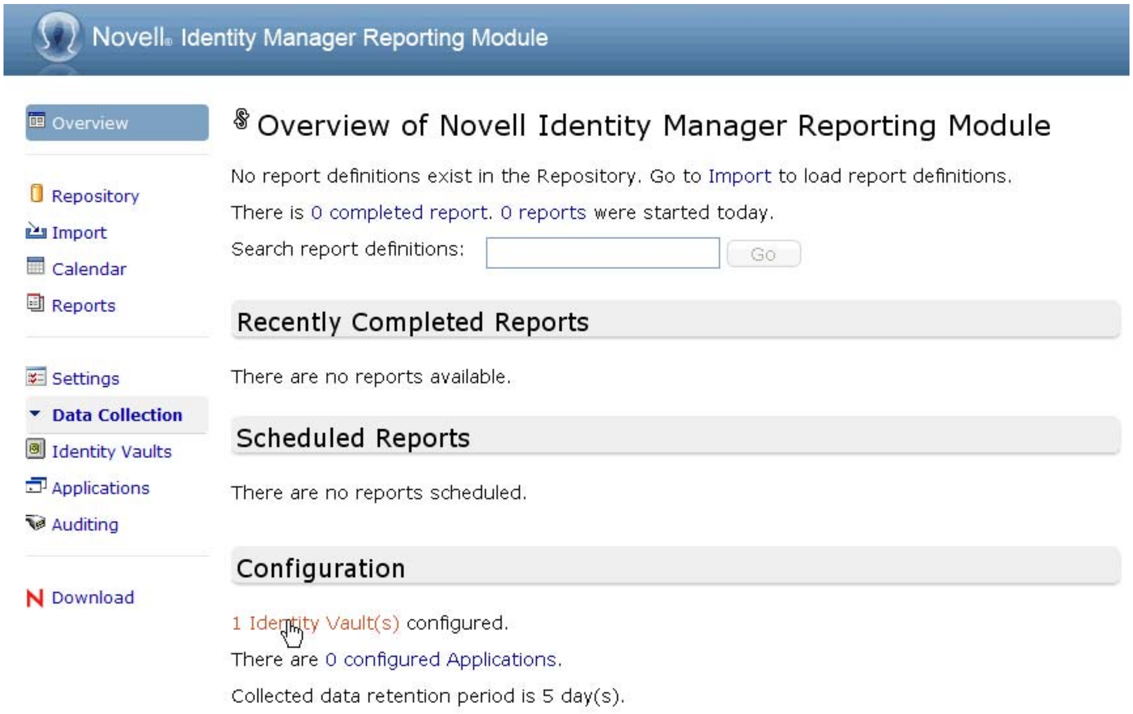
Novell® Identity Manager Reporting Module

Login

Username: ou=medical-idmsample,o=novell

Password: ●●●●

6 On the Overview page, verify that one Identity Vault has been configured:



Novell® Identity Manager Reporting Module

Overview of Novell Identity Manager Reporting Module

No report definitions exist in the Repository. Go to Import to load report definitions.

There is 0 completed report. 0 reports were started today.

Search report definitions:

Recently Completed Reports

There are no reports available.

Scheduled Reports

There are no reports scheduled.

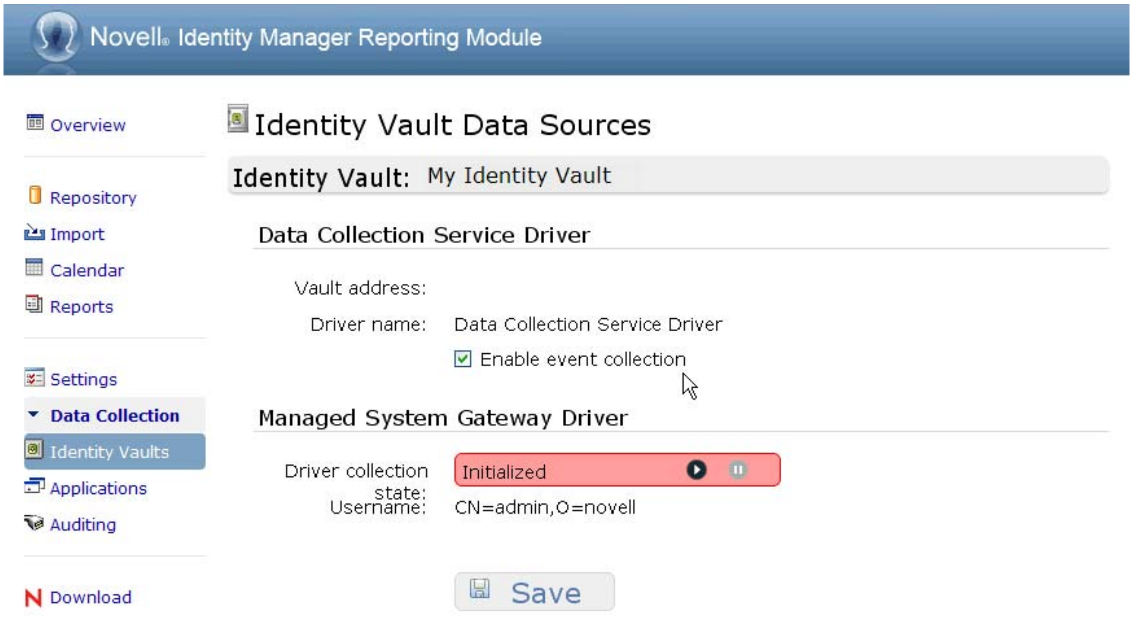
Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

Collected data retention period is 5 day(s).

7 Look at the Identity Vaults page to see details about the Data Collection Service Driver and the Managed System Gateway Driver. The Managed System Gateway Driver status should indicate that the driver has been initialized:



Identity Vault Data Sources

Identity Vault: My Identity Vault

Data Collection Service Driver

Vault address:

Driver name: Data Collection Service Driver

☑ Enable event collection

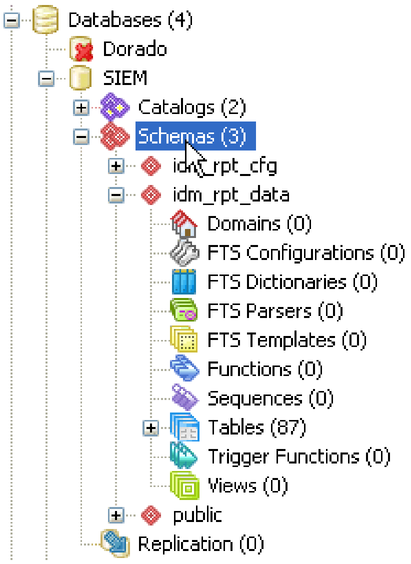
Managed System Gateway Driver

Driver collection state: Initialized

Username: CN=admin,O=novell

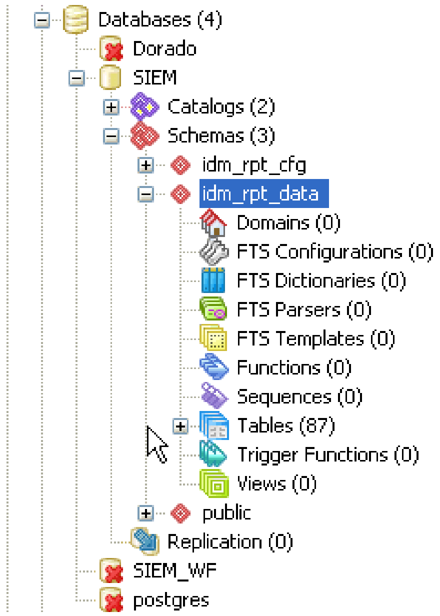
At this point, you can look at the contents of the Identity Information Warehouse to learn more about the rich data that is stored about the Identity Vault, as well as the managed systems in your enterprise.

8 To see the data in the Identity Information Warehouse, use a database administration tool such as PGAdmin for PostgreSQL to look at the contents of the SIEM database. When you look at the SIEM database, you should see three schemas:

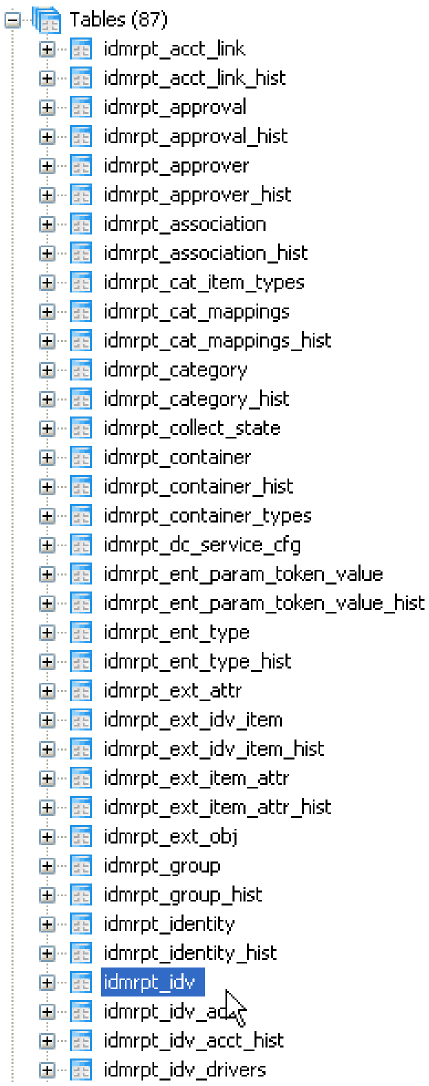


The SIEM database is installed by the EAS installer. The `public` schema includes information about events captured by EAS. The other two schemas, `idm_rpt_cfg` and `idm_rpt_data`, are added by the installer for the Identity Reporting Module. The `idm_rpt_cfg` schema contains reporting configuration data, such as report definitions and schedules. The `idm_rpt_data` schema contains information collected by the Managed System Gateway Driver and the Data Collection Service Driver.

9 To see data collected by the Managed System Gateway Driver and the Data Collection Service Driver, look at the `idm_rpt_data` schema:

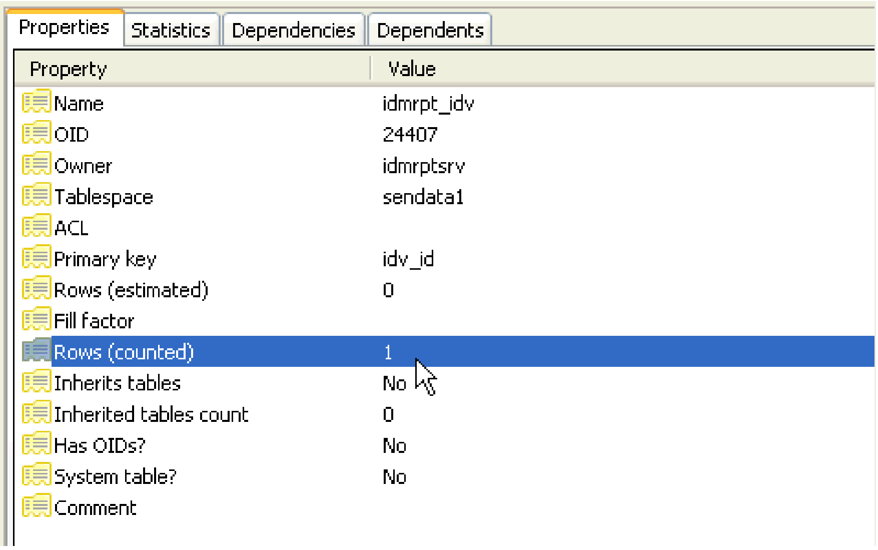


10 First, look at the idmrpt_idv table:



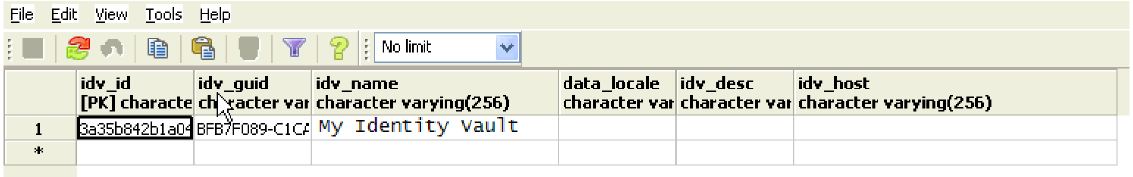
- Tables (87)
  - idmrpt_acct_link
  - idmrpt_acct_link_hist
  - idmrpt_approval
  - idmrpt_approval_hist
  - idmrpt_approver
  - idmrpt_approver_hist
  - idmrpt_association
  - idmrpt_association_hist
  - idmrpt_cat_item_types
  - idmrpt_cat_mappings
  - idmrpt_cat_mappings_hist
  - idmrpt_category
  - idmrpt_category_hist
  - idmrpt_collect_state
  - idmrpt_container
  - idmrpt_container_hist
  - idmrpt_container_types
  - idmrpt_dc_service_cfg
  - idmrpt_ent_param_token_value
  - idmrpt_ent_param_token_value_hist
  - idmrpt_ent_type
  - idmrpt_ent_type_hist
  - idmrpt_ext_attr
  - idmrpt_ext_idv_item
  - idmrpt_ext_idv_item_hist
  - idmrpt_ext_item_attr
  - idmrpt_ext_item_attr_hist
  - idmrpt_ext_obj
  - idmrpt_group
  - idmrpt_group_hist
  - idmrpt_identity
  - idmrpt_identity_hist
  - idmrpt_idv
  - idmrpt_idv_ac
  - idmrpt_idv_acct_hist
  - idmrpt_idv_drivers

11 Check to see if a single row was added to this table for the new Data Collection Service Driver that was registered:



Property	Value
Name	idmrpt_idv
OID	24407
Owner	idmrptsrv
Tablespace	sendata1
ACL	
Primary key	idv_id
Rows (estimated)	0
Fill factor	
Rows (counted)	1
Inherits tables	No
Inherited tables count	0
Has OIDs?	No
System table?	No
Comment	

12 Check to see if the data for this table shows the name of the Identity Vault:

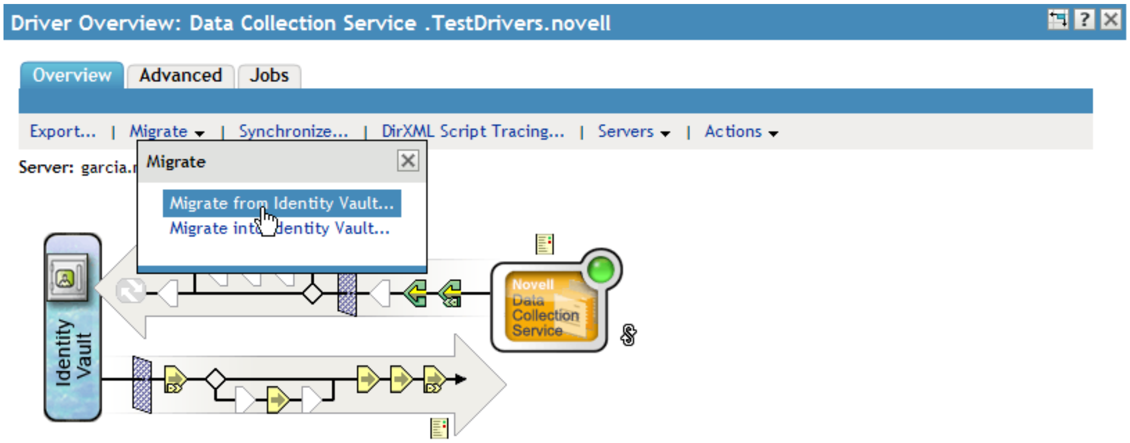


	idv_id [PK] characte	idv_guid character var	idv_name character varying(256)	data_locale character var	idv_desc character var	idv_host character varying(256)
1	3a35b842b1a04	BFB7F089-C1CA	My Identity Vault			
*						

If you see the new row in this table, the driver registration process was successful.

Migrating the Data Collection Service Driver

1 In iManager, go to the *Overview* panel for the Data Collection Service Driver, and select *Migrate From Identity Vault*:


Driver Overview: Data Collection Service .TestDrivers.novell
Overview
Advanced
Jobs
Export...
Migrate
Synchronize...
DirXML Script Tracing...
Servers
Actions
Server: garcia.r
Migrate
Migrate from Identity Vault...
Migrate into Identity Vault...
Identity Vault
Novell Data Collection Service

2 Select the organizations that contain relevant data, and click *Start*:

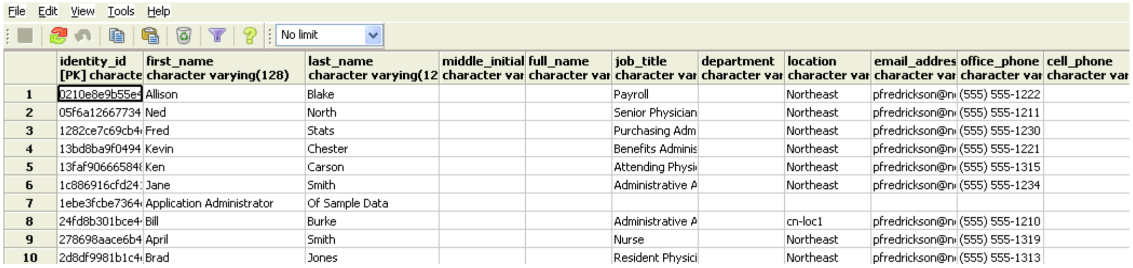
Depending on the amount of data you have, the migration process could take several minutes.

IMPORTANT: Be sure to wait until the migration process is complete before you proceed.

3 Look at the following tables, which provide information about the identities and accounts in the Identity Vault:

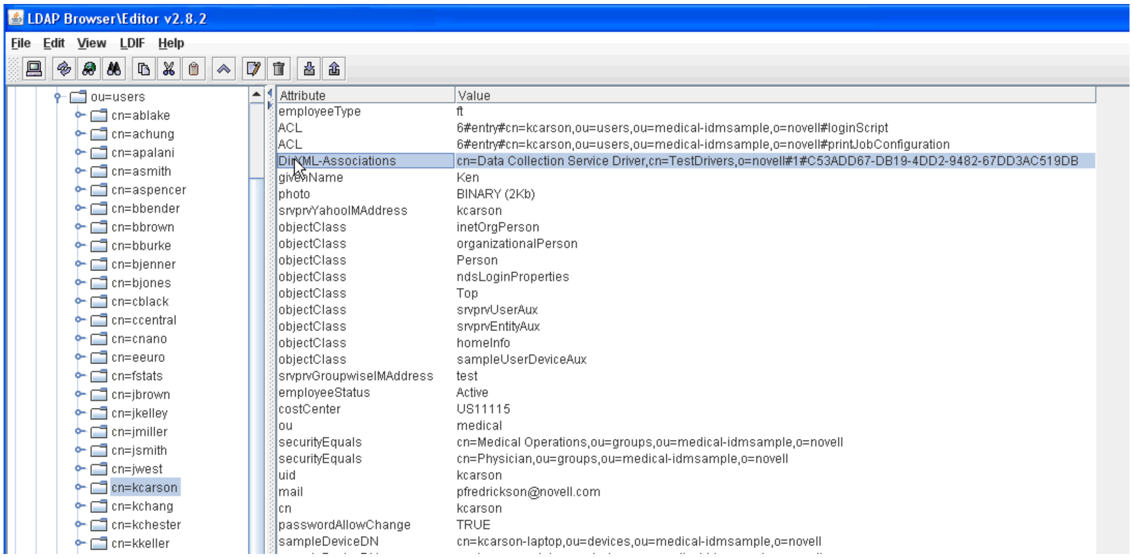
- idmrpt_identity
- idmrpt_acct

After the migration, the idmrpt_identity table, for example, contains the following types of information:



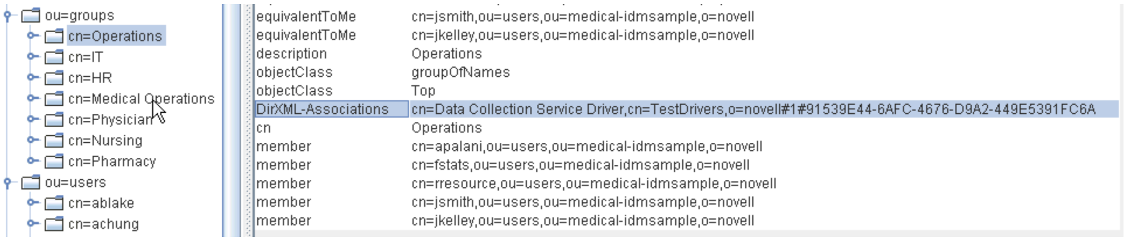
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(555) 555-1313	

4 Look at an LDAP browser to verify that the migration process also adds a DirXML-Associations reference for each user:



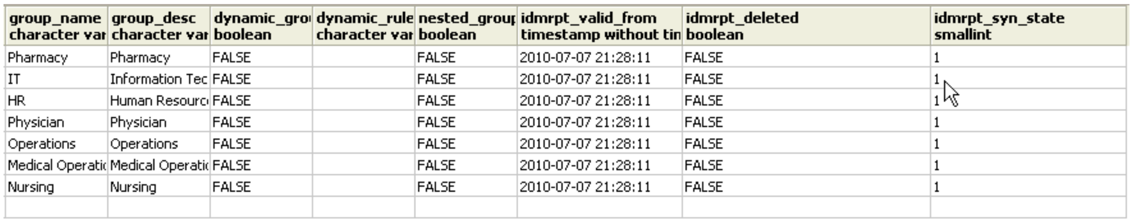
Attribute	Value
employeeType	ft
ACL	6#entry#cn=kcarson,ou=users,ou=medical-idmsample,o=novell#loginScript
ACL	6#entry#cn=kcarson,ou=users,ou=medical-idmsample,o=novell#printJobConfiguration
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#C53ADD67-DB19-4DD2-9482-67DD3AC519DB
givenName	Ken
photo	BINARY (2Kb)
srvprvYahooIMAddress	kcarson
objectClass	inetOrgPerson
objectClass	organizationalPerson
objectClass	Person
objectClass	ndsLoginProperties
objectClass	Top
objectClass	srvprvUserAux
objectClass	srvprvEntityAux
objectClass	homeInfo
objectClass	sampleUserDeviceAux
srvprvGroupwiseIMAddress	test
employeeStatus	Active
costCenter	US11115
ou	medical
securityEquals	cn=Medical Operations,ou=groups,ou=medical-idmsample,o=novell
securityEquals	cn=Physician,ou=groups,ou=medical-idmsample,o=novell
uid	kcarson
mail	pfredrickson@novell.com
cn	kcarson
passwordAllowChange	TRUE
sampleDeviceDN	cn=kcarson-laptop,ou=devices,ou=medical-idmsample,o=novell

5 Verify that the migration process adds a DirXML-Associations reference for each group, as well:



equivalentToMe	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
equivalentToMe	cn=jkelley,ou=users,ou=medical-idmsample,o=novell
description	Operations
objectClass	groupOfNames
objectClass	Top
DirXML-Associations	cn=Data Collection Service Driver,cn=TestDrivers,o=novell#1#91539E44-6AFC-4676-D9A2-449E5391FC6A
cn	Operations
member	cn=apalani,ou=users,ou=medical-idmsample,o=novell
member	cn=fstats,ou=users,ou=medical-idmsample,o=novell
member	cn=rresource,ou=users,ou=medical-idmsample,o=novell
member	cn=jsmith,ou=users,ou=medical-idmsample,o=novell
member	cn=jkelley,ou=users,ou=medical-idmsample,o=novell

6 Look at data in the idmrpt_group table:



group_name character var	group_desc character var	dynamic_grou boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resourc	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operati	Medical Operati	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

This table shows the name for each group, as well as flags indicating whether the group is dynamic or nested. It also shows whether the group has been migrated. The synchronization status (idmrpt_syn_state) could possibly be set to 0 if an object had been modified in the User Application but not yet migrated. For example, if a user were added to a group, and the driver had not been migrated yet, this value might be set to 0.

7 (Optional) Look at the following tables:

- idmrpt_approver
- idmrpt_association
- idmrpt_category
- idmrpt_container
- idmrpt_idv_drivers

- idmrpt_idv_prd
- idmrpt_role
- idmrpt_resource
- idmrpt_sod

8 (Optional) Look at the idmrpt_ms_collect_state table, which is of particular importance.

This table shows information about the data collection state for the Managed System Gateway Driver, which includes data about which REST endpoints for managed systems have been executed. At this point, the table has no rows, because the collection process has not yet been started for this driver.

Starting the Collection Process for the Managed System Gateway Driver

This section provides instructions for starting the data collection process for the Managed System Gateway Driver.

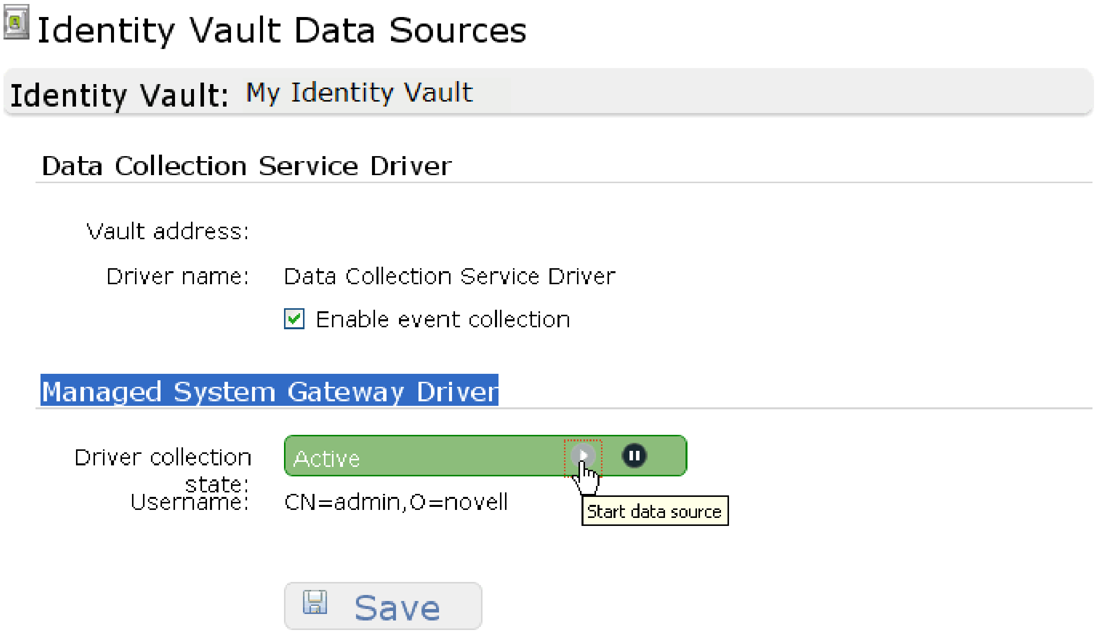
IMPORTANT: Before activating the data collection process for the first time, you need to be sure you have performed all of the configuration steps in the correct order.

1. Start the Data Collection Service Driver and the Managed System Gateway Driver.
2. Verify that the Data Collection Service Driver has registered properly with the DCS services.
3. Migrate the Data Collection Service Driver and wait until the migration process is complete.

If you do not follow these steps in order, some data might be in a transitional state, and you might see two rows for the same managed system. Because there is no way to determine programmatically whether the migration process is complete, you need to wait until the migration process is complete before you activate the data collection process.

After the configuration steps have been performed in order, you can proceed with the initial data collection.

1 In the user interface for the Identity Reporting Module, navigate to the Identity Vault Data Sources page. Then, click *Start data source* for the driver and click *Save*:



Identity Vault Data Sources

Identity Vault: My Identity Vault

Data Collection Service Driver

Vault address:

Driver name: Data Collection Service Driver

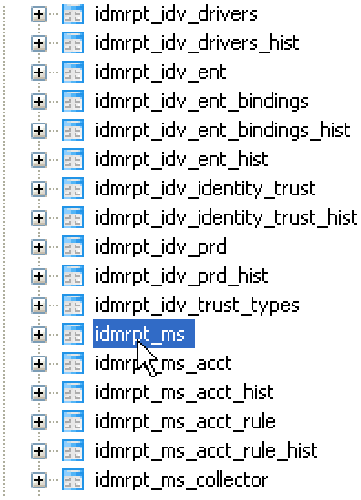
☑ Enable event collection

Managed System Gateway Driver

Driver collection state: Active

Username: CN=admin,O=novell

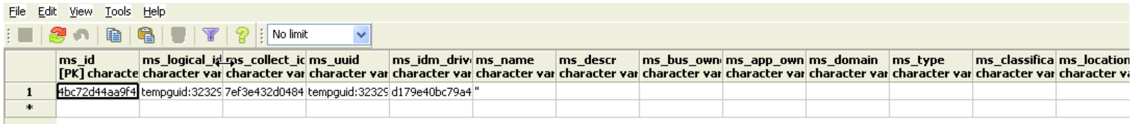
2 Now look at the idmrpt_ms table:



- idmrpt_idv_drivers
- idmrpt_idv_drivers_hist
- idmrpt_idv_ent
- idmrpt_idv_ent_bindings
- idmrpt_idv_ent_bindings_hist
- idmrpt_idv_ent_hist
- idmrpt_idv_identity_trust
- idmrpt_idv_identity_trust_hist
- idmrpt_idv_prd
- idmrpt_idv_prd_hist
- idmrpt_idv_trust_types
- idmrpt_ms
- idmrpt_ms_acct
- idmrpt_ms_acct_hist
- idmrpt_ms_acct_rule
- idmrpt_ms_acct_rule_hist
- idmrpt_ms_collector

This table contains information about the Managed System Gateway Driver.

3 In the data for this table, verify that there is a single row representing the Managed System Gateway Driver registration:

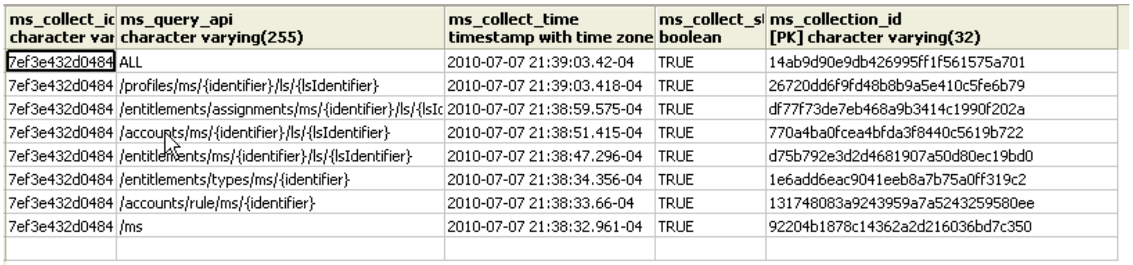


	ms_id [PK] characte	ms_logical_id character var	ms_collect_ic character var	ms_uuid character var	ms_idm_driv character var	ms_name character var	ms_descr character var	ms_bus_own character var	ms_app_own character var	ms_domain character var	ms_type character var	ms_classifica character var	ms_location character va
1	4bc72d44aa9f4	tempguid:32329	7ef3e432d0484	tempguid:32329	d179e40bc79a4	''							
*													

At this point, some of the information in this table is still blank, because the Data Collection Service Driver has not yet been migrated from the Identity Vault.

4 Verify that the idmrpt_ms_collect_state table contains several rows of data showing which endpoints have been executed.

5 (Optional) Sort the list by ms_collect_time to see the order in which they were executed:

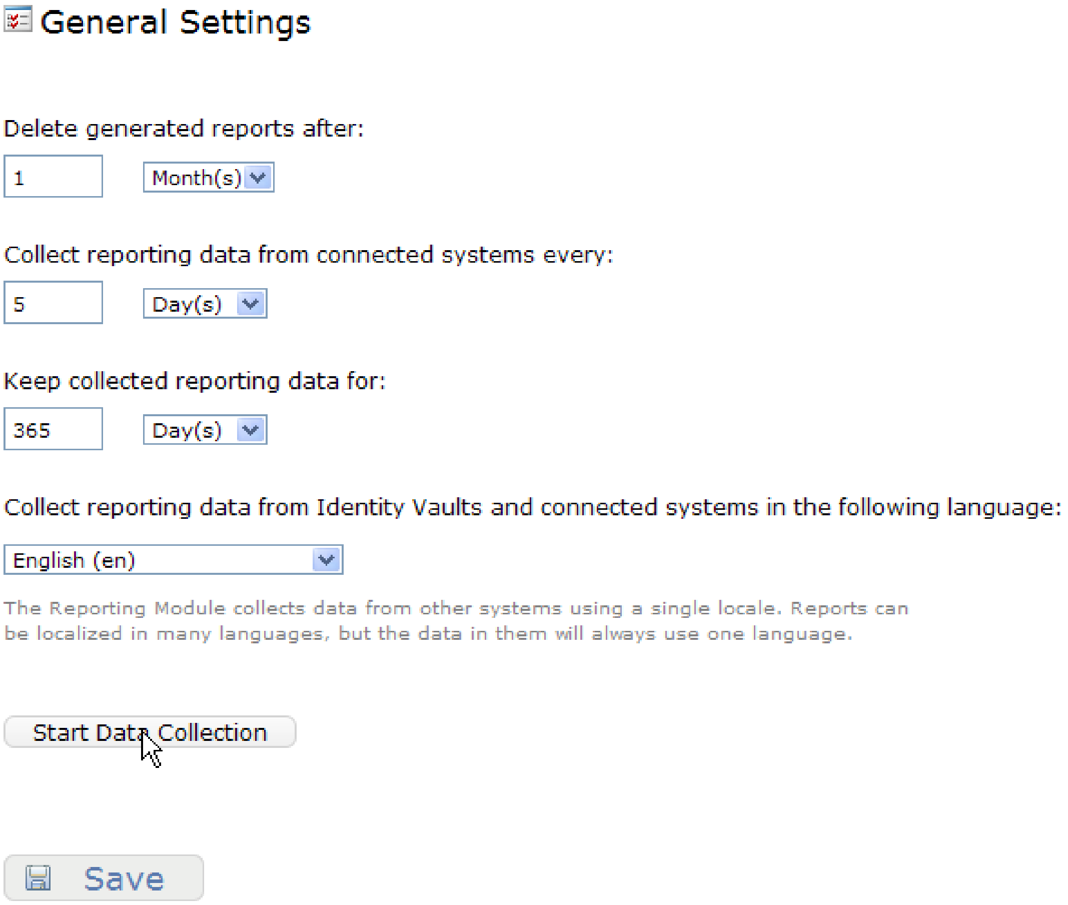


ms_collect_ic character var	ms_query_api character varying(255)	ms_collect_time timestamp with time zone	ms_collect_s boolean	ms_collection_id [PK] character varying(32)
7ef3e432d0484	ALL	2010-07-07 21:39:03.42-04	TRUE	14ab9d90e9db426995ff1f561575a701
7ef3e432d0484	/profiles/ms/{identifier}/ls/{lsIdentifier}	2010-07-07 21:39:03.418-04	TRUE	26720dd6f9fd48b8b9a5e410c5fe6b79
7ef3e432d0484	/entitlements/assignments/ms/{identifier}/ls/{lsIc	2010-07-07 21:38:59.575-04	TRUE	df77f73de7eb468a9b3414c1990f202a
7ef3e432d0484	/accounts/ms/{identifier}/ls/{lsIdentifier}	2010-07-07 21:38:51.415-04	TRUE	770a4ba0fcea4bfda3f8440c5619b722
7ef3e432d0484	/entitlements/ms/{identifier}/ls/{lsIdentifier}	2010-07-07 21:38:47.296-04	TRUE	d75b792e3d2d4681907a50d80ec19bd0
7ef3e432d0484	/entitlements/types/ms/{identifier}	2010-07-07 21:38:34.356-04	TRUE	1e6add6eac9041eeb8a7b75a0ff319c2
7ef3e432d0484	/accounts/rule/ms/{identifier}	2010-07-07 21:38:33.66-04	TRUE	131748083a9243959a7a5243259580ee
7ef3e432d0484	/ms	2010-07-07 21:38:32.961-04	TRUE	92204b1878c14362a2d216036bd7c350

If any of the endpoints fails to execute properly, the value for ms_collect_state is FALSE. If the driver is not configured properly, the ms_collect_state for the */ms* endpoint is FALSE, and the other endpoints are not not executed. If this happens, you should enable tracing on the driver to determine the underlying cause of the problem.

To initiate a subsequent data collection process for the Managed System Gateway Driver:

1 In the user interface for the Identity Reporting Module, click *Start Data Collection* on the General Settings page:



General Settings

Delete generated reports after:

1 Month(s)

Collect reporting data from connected systems every:

5 Day(s)

Keep collected reporting data for:

365 Day(s)

Collect reporting data from Identity Vaults and connected systems in the following language:

English (en)

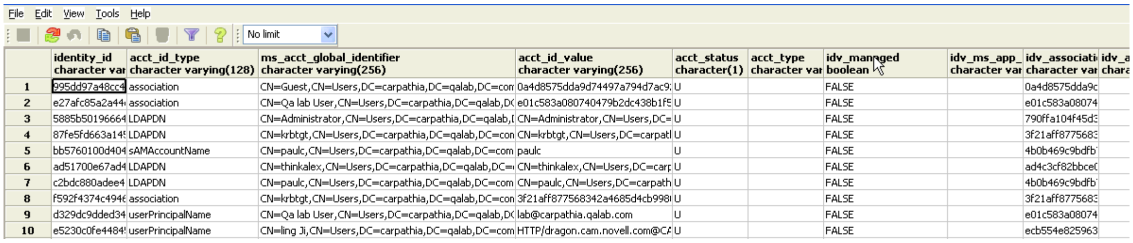
The Reporting Module collects data from other systems using a single locale. Reports can be localized in many languages, but the data in them will always use one language.

2 Look at the idmrpt_ms_collect_state table to verify that several additional rows have been added to show the execution of additional REST endpoints.

3 Look at the following tables to see the kinds of information that has been collected about the managed systems:

- idmrpt_ms_acct
- idmrpt_ms_ent_trust
- idmrpt_ms_identity

The idmrpt_ms_acct table, for example, provides useful information about the accounts for each of the managed systems.

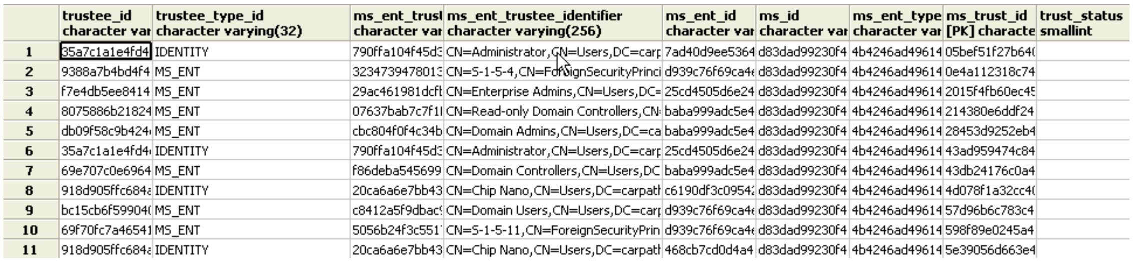


	identity_id character var	acct_id_type character varying(128)	ms_acct_global_identifier character varying(256)	acct_id_value character varying(256)	acct_status character(1)	acct_type character var	idv_managed boolean	idv_ms_app_ character var	idv_associati character var	idv_a chara
1	995dd97a48cc4	association	CN=Guest,CN=Users,DC=carpathia,DC=qalab,DC=com	0a4d8575dda9d74497a794d7ac9	U		FALSE		0a4d8575dda9c	
2	e27afc85a2a44	association	CN=Qa lab User,CN=Users,DC=carpathia,DC=qalab,DC	e01c583a080740479b2dc438b1f5	U		FALSE		e01c583a08074	
3	5885b50196664	LDAPDN	CN=Administrator,CN=Users,DC=carpathia,DC=qalab,D	CN=Administrator,CN=Users,DC=	U		FALSE		790ffa104f45d3	
4	87fe5fd663a145	LDAPDN	CN=krbtgt,CN=Users,DC=carpathia,DC=qalab,DC=con	CN=krbtgt,CN=Users,DC=carpatl	U		FALSE		3f21aff8775683	
5	bb5760100d404	sAMAccountName	CN=paulc,CN=Users,DC=carpathia,DC=qalab,DC=com	paulc	U		FALSE		4b0b469c9bdfb	
6	ad51700e67ad4	LDAPDN	CN=thinkalex,CN=Users,DC=carpathia,DC=qalab,DC=	CN=thinkalex,CN=Users,DC=carp	U		FALSE		ad4c3cf82bbce0	
7	c2bdc880adee4	LDAPDN	CN=paulc,CN=Users,DC=carpathia,DC=qalab,DC=com	CN=paulc,CN=Users,DC=carpath	U		FALSE		4b0b469c9bdfb	
8	f592f4374c4946	association	CN=krbtgt,CN=Users,DC=carpathia,DC=qalab,DC=con	3f21aff877568342a4685d4cb998	U		FALSE		3f21aff8775683	
9	d329dc9dded34	userPrincipalName	CN=Qa lab User,CN=Users,DC=carpathia,DC=qalab,DC	lab@carpathia.qalab.com	U		FALSE		e01c583a08074	
10	e5230c0fe44845	userPrincipalName	CN=ling Ji,CN=Users,DC=carpathia,DC=qalab,DC=com	HTTP/dragon.cam.novell.com@CA	U		FALSE		ecb554e825963	

The acct_id_type column shows the type for each account in the managed system (in this case, Active Directory). In addition, the idv_managed column indicates whether the account is currently being managed. In this particular situation, the user accounts in the Identity Vault are not actively being managed within Active Directory, so the column value is FALSE.

In this table, you might also want to look at the idv_sync column, which indicates whether the account has been migrated, as well as the idmrpt_valid_from and idmrpt_valid_to columns. The timestamps for the idmrpt_valid_from and idmrpt_valid_to columns are updated whenever data is modified, and a corresponding row is added to a history table.

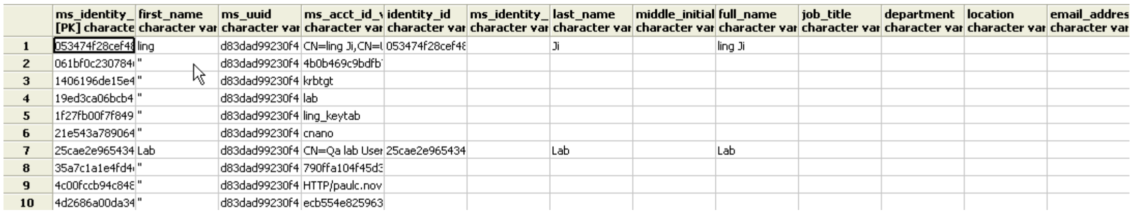
4 Look at the idmrpt_ms_ent_trust table to see information about the entitlements that have been assigned to trustees within the managed system:



	trustee_id character var	trustee_type_id character varying(32)	ms_ent_trust character var	ms_ent_trustee_identifier character varying(256)	ms_ent_id character var	ms_id character var	ms_ent_type character var	ms_trust_id [PK] characte	trust_status smallint
1	35a7c1a1e4fd4	IDENTITY	790ffa104f45d3	CN=Administrator,CN=Users,DC=carp	7ad40d9ee5364	d83dad99230f4	4b4246ad49614	05bef51f27b640	
2	9388a7b4bd4f4	MS_ENT	323473947801 3	CN=S-1-5-4,CN=ForeignSecurityPrinci	d939c76f69ca4e	d83dad99230f4	4b4246ad49614	0e4a112318c74	
3	f7e4db5ee8414	MS_ENT	29ac461981dcfb	CN=Enterprise Admins,CN=Users,DC=	25cd4505d6e24	d83dad99230f4	4b4246ad49614	2015f4fb60ec45	
4	8075886b21824	MS_ENT	07637bab7c7f1	CN=Read-only Domain Controllers,CN=	baba999adc5e4	d83dad99230f4	4b4246ad49614	214380e6ddf24	
5	db09f58c9b424	MS_ENT	cbc804f0f4c34b	CN=Domain Admins,CN=Users,DC=ca	baba999adc5e4	d83dad99230f4	4b4246ad49614	28453d9252eb4	
6	35a7c1a1e4fd4	IDENTITY	790ffa104f45d3	CN=Administrator,CN=Users,DC=carp	25cd4505d6e24	d83dad99230f4	4b4246ad49614	43ad959474c84	
7	69e707c0e6964	MS_ENT	f86deba545699	CN=Domain Controllers,CN=Users,DC	baba999adc5e4	d83dad99230f4	4b4246ad49614	43db24176c0a4	
8	918d905ffc684a	IDENTITY	20ca6a6e7bb43	CN=Chip Nano,CN=Users,DC=carpath	c6190df3c0954	d83dad99230f4	4b4246ad49614	4d078f1a32cc40	
9	bc15cb6f59904	MS_ENT	c8412a5f9dbac	CN=Domain Users,CN=Users,DC=carp	d939c76f69ca4e	d83dad99230f4	4b4246ad49614	57d96b6c783c4	
10	69f70fc7a46541	MS_ENT	5056b24f3c551	CN=S-1-5-11,CN=ForeignSecurityPrin	d939c76f69ca4e	d83dad99230f4	4b4246ad49614	598f89e0245a4	
11	918d905ffc684a	IDENTITY	20ca6a6e7bb43	CN=Chip Nano,CN=Users,DC=carpath	468cb7cd0d4a4	d83dad99230f4	4b4246ad49614	5e39056d663e4	

The trustee_type_id column indicates whether the trustee is an identity or a group.

5 Look at the idmrpt_ms_identity table to see the identities in the managed system:



	ms_identity_ [PK] characte	first_name character var	ms_uuid character var	ms_acct_id_v character var	identity_id character var	ms_identity_ character var	last_name character var	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var
1	053474f28cef48	ling	d83dad99230f4	CN=ling Ji,CN=U	053474f28cef48		Ji		ling Ji				
2	061bf0c230784	"	d83dad99230f4	4b0b469c9bdfb									
3	1406196de15e4	"	d83dad99230f4	krbtgt									
4	19ed3ca06bcb4	"	d83dad99230f4	lab									
5	1f27fb00f7f849	"	d83dad99230f4	ling_keytab									
6	21e543a789064	"	d83dad99230f4	cnano									
7	25cae2e965434	Lab	d83dad99230f4	CN=Qa lab User	25cae2e965434		Lab		Lab				
8	35a7c1a1e4fd4	"	d83dad99230f4	790ffa104f45d3									
9	4c00fccb94c848	"	d83dad99230f4	HTTP/paulc.nov									
10	4d2686a00da34	"	d83dad99230f4	ecb554e825963									

Notice that the first name is available for users, but not groups. This particular example shows data for a test system, so not all of the values are available.

Adding Support for Custom Attributes and Objects

You can configure the Data Collection Service driver to gather and persist data for custom attributes and objects that are not part of the default data collection scheme. To do this, you need to modify the Data Collection Service driver filter. Modifying the filter does not trigger object synchronization immediately. Instead, the newly added attributes and objects are sent to the data collection services when add, modify, or delete events occur in the Identity Vault.

When you add support for custom attributes and objects, you need to modify the reports in order to include the extended attribute and object information. The following views provide current and historic data on the extended objects and attributes:

- idm_rpt_cfg.idmrpt_ext_idv_item_v
- idm_rpt_cfg.idmrpt_ext_item_attr_v

Configuring the Driver to Use Extended Objects

You can add any object or attribute to the Data Collection Service filter policy. When you add a new object or attribute, you need to make sure you map the GUID (with subscriber sync) and the Object Class (with subscriber notify), as shown in the following example:

```
<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>
```

Including a Name and Description in the Database

If you want the object to have a name and description in the database, you need to add a schema mapping policy for _dcsName and _dcsDescription. The schema mapping policy maps the attribute values on the object instance to the columns idmrpt_ext_idv_item.item_name and idmrpt_ext_idv_item.item_desc, respectively. If you do not add a schema mapping policy, the attributes will be populated in the child table idmrpt_ext_item_attr.

Here's an example:

```
<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>
```

Here is some sample SQL that allows you to show these object and attribute values in the database:

```
SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item, idm_rpt_data.idmrpt_ext_item_attr
itemAttr, idm_rpt_data.idmrpt_ext_attr as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id = attr.attribute_id
and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name
```

Adding Extended Attributes to Known Object Types

If an attribute is added to the filter policy on the Data Collection Service driver and not explicitly mapped to the reporting database in the XML reference file (`IdmrptIdentity.xml`), the value is populated and maintained in the idmrpt_ext_item_attr table, with an attribute reference in the idmrpt_ext_attr table.

Here is some sample SQL that shows these extended attributes:

```
SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal, idm_rpt_data.idmrpt_ext_attr as
attrDef, idm_rpt_data.idmrpt_identity as idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and cat_item_type_id =
'IDENTITY'
```

In addition to the User object, you can add extended attributes to the filter policy on the following objects and populate the database with these attributes:

- nrfRole
- nrfResource
- Containers

  NOTE: The installed product provides support for organizationUnit, Organization, and Domain. The container types are maintained in the idmrpt_container_types table.

- Group
- nrfSod

You can see the association of the extended attributes to the parent table or object by looking at the idmrpt_cat_item_types.idmrpt_table_name column. This column describes how to join the idm_rpt_data.idmrpt_ext_item_attr.cat_item_id column to the primary key of the parent table.

Adding Support for Multiple Driversets

The new Data Collection Service Scoping package (NOVLDCSSCPNG) provides static and dynamic scoping capabilities for enterprise environments with multiple driversets and multiple pairs of Data Collection Service Drivers and Managed System Gateway Drivers.

During or after installation, you need to determine the role for the Data Collection Service Driver that the package is being installed on. You need to select one of the following roles:

- **Primary** The driver synchronizes everything except subtrees of other driver sets. A primary Data Collection Service Driver may well service a whole Identity Vault or it may work in conjunction with one or multiple secondary drivers.
- **Secondary** The driver synchronizes only its own driver set, but nothing else. A secondary Data Collection Service Driver usually requires a primary driver to run in a different driverset or no data outside the local driver set is sent to the Data Collection Service.
- **Custom** Allows the administrator to define custom scoping rules. The only implicit scope is the local driver set, everything else is considered out-of-scope, unless it is explicitly added to the list of custom scopes. A custom scope is the distinguished name in slash format of a container in the Identity Vault whose subordinates or subtree should be synchronized.

The scoping package is only required in some configuration scenarios, as described below:

- **Single server with a single driver set Identity Vault** For this scenario, you do not need scoping, and, therefore, you do not need to install the scoping package.
- **Multiple servers with a single driver set Identity Vault** For this scenario, you need to follow these guidelines:
    - Make sure the Identity Manager server holds replicas of all partitions from which data should be collected.
    - For this scenario, no scoping is required, so do not install the scoping package
- **Multiple servers with a multiple driver set Identity Vault** In this scenario, there are two basic configurations:
    - All servers hold a replica of all partitions from which data should be collected.

      For this configuration, you need to follow these guidelines:
        - Scoping is required to avoid the same change being processed by multiple DCS drivers.
        - You need to install the scoping package on all DCS drivers.
        - You need to select one DCS driver to be the Primary driver.
        - You need to configure all other DCS drivers to be Secondary drivers.
    - All servers *do not* hold a replica of all partitions from which data should be collected.

      Within this configuration, there are two possible situations:
        - All partitions from which data should be collected are being held by *only one* Identity Manager server

          In this case, you need to follow these guidelines:
            - Scoping is required to avoid the same change being processed by multiple DCS drivers.
            - You need to install the scoping package on all DCS drivers.
            - You need to configure all DCS drivers to be Primary drivers.
        - All partitions from which data should be collected are *not being held by only one* Identity Manager server (some partitions are held by more than one Identity Manager server).

In this case, you need to follow these guidelines:

- Scoping is required to avoid the same change being processed by multiple DCS drivers.
- You need to install the scoping package on all DCS drivers.
- You need to configure all DCS drivers to be Custom drivers.

  You need to define custom scoping rules for each driver and be sure not to create any overlapping scopes.

Configuring the Drivers to Run in Remote Mode with SSL

When running in remote mode, you can configure the Data Collection Service and Managed System Gateway drivers to use SSL. This section provides steps for configuring the drivers to run in remote mode with SSL.

To configure SSL using a Keystore for the Managed System Gateway Driver:

1 Create a server certificate in iManager.

1a In the *Roles and Tasks* view, click *Novell Certificate Server* > *Create Server Certificate*.

1b Browse to and select the server object where the Managed System Gateway Driver is installed.

1c Specify a certificate nickname.

1d Select *Standard* as the creation method, then click *Next*.

1e Click *Finish*, then click *Close*.

2 Export the server certificate using iManager.

2a In the *Roles and Tasks* view, click *Novell Certificate Access* > *Server Certificates*.

2b Select the certificate created in Step 1 on page 95 and click *Export*.

2c Select your certificate name from the *Certificates* drop-down.

2d Ensure that the option *Export private key* is checked.

2e Enter a password and click *Next*.

2f Click *Save the exported certificate*, and save the exported pfx certificate.

3 Import the pfx certificate exported in Step 2 on page 95 into the java key-store.

3a Use the keytool available with Java. You must use JDK 6 or later.

3b Enter the following command at a command prompt:

```
keytool -importkeystore -srckeystore <pfx certificate> -srcstoretype
PKCS12 -destkeystore <Keystore Name>
```

For example:

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

3c Enter the password when prompted to do so.

4 Modify the Managed System Gateway Driver configuration to use the keystore using iManager.

4a From *Identity Manager Overview*, click the driverset containing the Managed System Gateway Driver.

4b Click on the driver state icon and select *Edit properties* > *Driver configuration*.

4c Set *Show Connection Parameters* to true and set the *Driver configuration mode* to remote.

4d Enter the complete path of the keystore file and the password.

4e Save and restart the driver.

5 Modify the Data Collection Service Driver configuration to use the keystore using iManager.

5a From *Identity Manager Overview*, click the driverset containing the Managed System Gateway Driver.

5b Click on the driver state icon and select *Edit properties* > *Driver configuration*.

5c Under the *Managed System Gateway Registration* header, set *Managed System Gateway Driver Configuration Mode* to remote.

5d Enter the complete path of the keystore, password and the alias enter in Step 1c on page 95.

5e Save and restart the driver.

Troubleshooting the Drivers

If you have problems with one or more of the drivers that are difficult to understand, see Chapter 14, "Troubleshooting the Drivers," on page 291.

2.4.7 Recommended Auditing Flags for the Drivers

This section outlines the recommended auditing settings for the Managed System Gateway Driver and the Data Collection Service Driver.

- "Recommended Identity Manager Auditing Flags" on page 96
- "Recommended eDirectory Auditing Flags" on page 98

Recommended Identity Manager Auditing Flags

The following Identity Manager auditing flags should be enabled for the drivers:

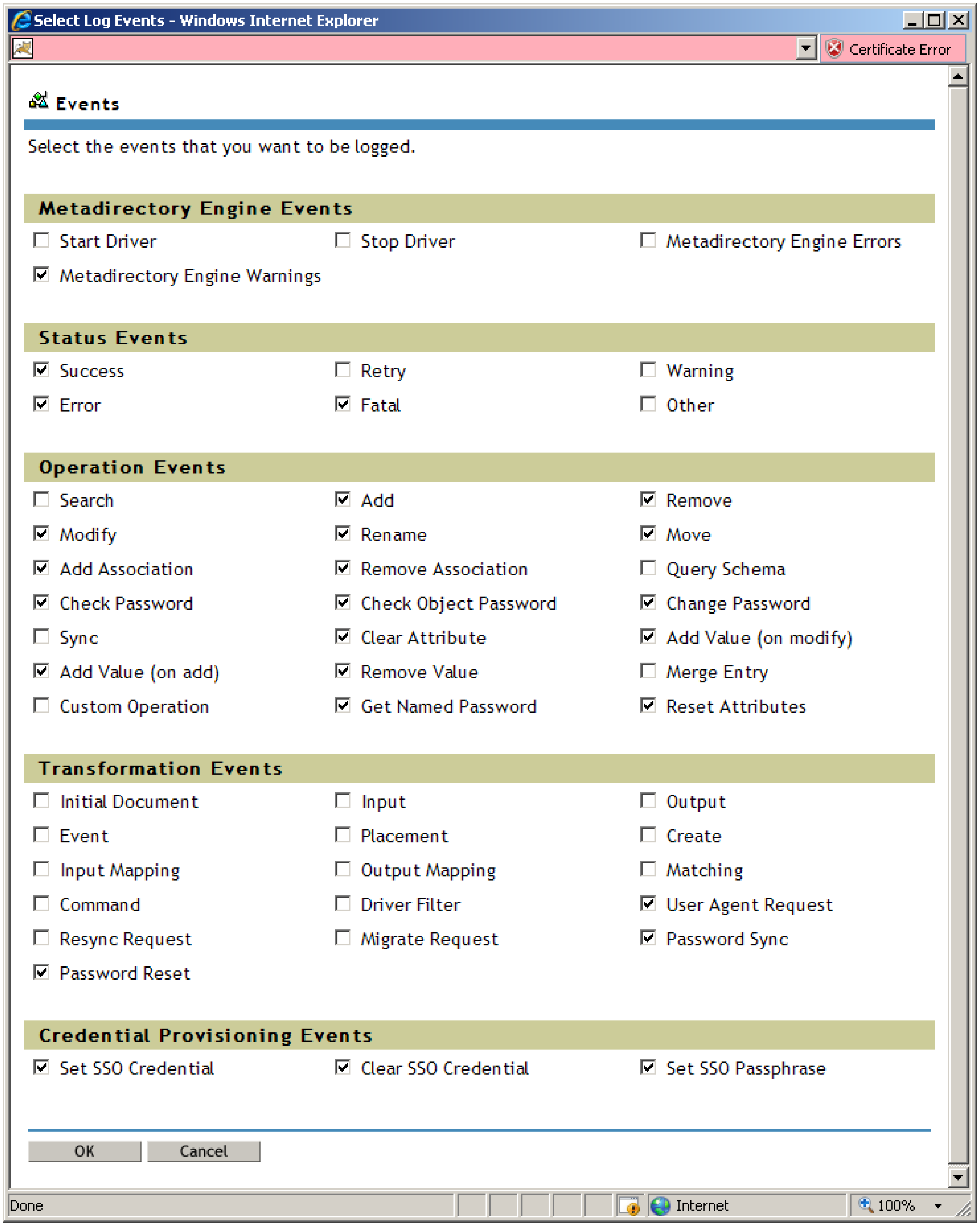
Table 2-3 *Identity Manager Auditing Flags*

Category	Recommended Flags
Metadirectory Engine Events	◆ Metadirectory Engine Warnings
Status Events	◆ Success **NOTE:** The *Correlated Resource Assignment Events per User* report requires the Success flag. If you want to be able to run this report or customized versions of it, then you need to enable the Success flag. ◆ Error ◆ Fatal

Category	Recommended Flags
Operation Events	◆ Modify ◆ Add Association ◆ Check Password ◆ Add Value ◆ Add ◆ Rename ◆ Remove Association ◆ Check Object Password ◆ Clear Attribute ◆ Remove Value ◆ Get Named Password ◆ Remove ◆ Move ◆ Change Password ◆ Add Value (on modify) ◆ Reset Attributes
Transformation Events	◆ Password Reset ◆ User Agent Request ◆ Password Sync
Credential Provisioning Events	◆ Set SSO Credentials ◆ Clear SSO Credentials ◆ Set SSO Passphrase

These flags are for Novell Auditing (not XDAS) and are set under *Driver Set Properties* > *Log Level* > *Log specific events* in iManager, as shown below:

Figure 2-1 *Events Selected in iManager*



Events

Select the events that you want to be logged.

Metadirectory Engine Events

□ Start Driver　□ Stop Driver　□ Metadirectory Engine Errors

☑ Metadirectory Engine Warnings

Status Events

☑ Success　□ Retry　□ Warning

☑ Error　☑ Fatal　□ Other

Operation Events

□ Search　☑ Add　☑ Remove

☑ Modify　☑ Rename　☑ Move

☑ Add Association　☑ Remove Association　□ Query Schema

☑ Check Password　☑ Check Object Password　☑ Change Password

□ Sync　☑ Clear Attribute　☑ Add Value (on modify)

☑ Add Value (on add)　☑ Remove Value　□ Merge Entry

□ Custom Operation　☑ Get Named Password　☑ Reset Attributes

Transformation Events

□ Initial Document　□ Input　□ Output

□ Event　□ Placement　□ Create

□ Input Mapping　□ Output Mapping　□ Matching

□ Command　□ Driver Filter　☑ User Agent Request

□ Resync Request　□ Migrate Request　☑ Password Sync

☑ Password Reset

Credential Provisioning Events

☑ Set SSO Credential　☑ Clear SSO Credential　☑ Set SSO Passphrase

Recommended eDirectory Auditing Flags

The following eDirectory auditing flags should be enabled for the drivers:

***Table 2-4** eDirectory Auditing Flags*

Category	Recommended Flags
Global	◆ Do Not Send Replicated Events
Meta	◆ (*Select all flags)*
Objects	◆ Add Property ◆ Allow Login ◆ Change Password ◆ Change Security Equals ◆ Create ◆ Delete ◆ Delete Property ◆ Login ◆ Logout ◆ Modify RDN ◆ Move (Source) ◆ Move (Destination) ◆ Remove ◆ Rename ◆ Restore ◆ Search ◆ Verify Password
Attributes	◆ *(Select all flags)*
Agent	◆ DS Reloaded ◆ Local Agent Opened ◆ Local Agent Closed ◆ NLM Loaded
Miscellaneous	◆ Generate CA Keys ◆ Recertified Public Key

Category	Recommended Flags
LDAP	◆ LDAP Bind ◆ LDAP Bind Response ◆ LDAP Modify ◆ LDAP Modify Response ◆ LDAP Password Modify ◆ LDAP Unbind ◆ LDAP Delete ◆ LDAP Delete Response ◆ LDAP Modify DN ◆ LDAP Modify DN Response ◆ LDAP Search ◆ LDAP Search Response ◆ LDAP Add ◆ LDAP Add Response

These flags need to be set under the *eDirectory Auditing* > *Audit Configuration* > *Novell Auditing* plug-in in iManager.

3 Getting Started

This section provides instructions on getting started with the Identity Reporting Module.

3.1 Accessing the Identity Reporting Module

You can access the Identity Reporting Module directly from a browser, or launch it from the Roles Based Provisioning Module.

NOTE: To access the reporting module, an LDAP user must be a Reporting Administrator and also be able to read all of the attributes in his/her own user object. Therefore, you need to grant the user read trustee rights to the user's own nrfMemberOf attribute.

3.1.1 Starting the Reporting Module Directly with a URL

To access the Identity Reporting Module directly, open a Web browser and go to the address (URL) for the module (as supplied by your system administrator). The URL will follow this pattern:

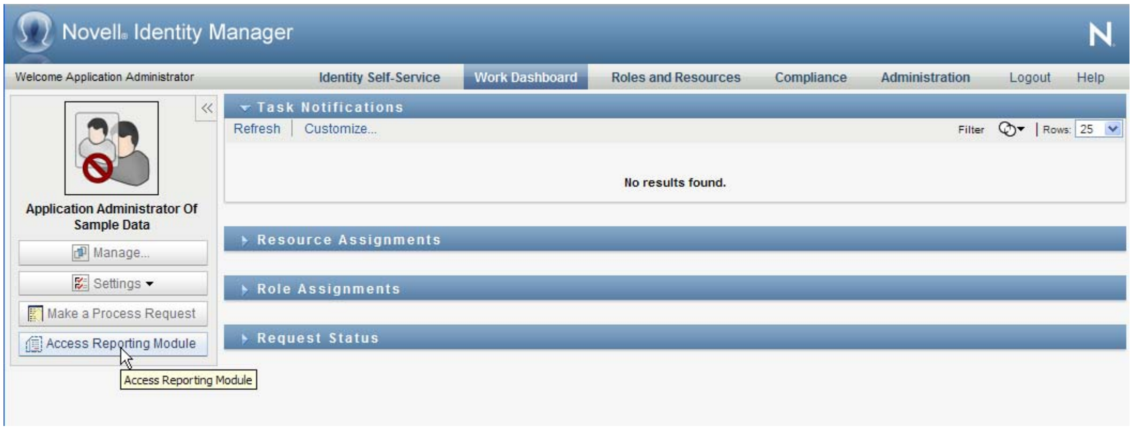
```
http://server:8180/IDMRPT/
```

3.1.2 Launching the Reporting Module from the User Application

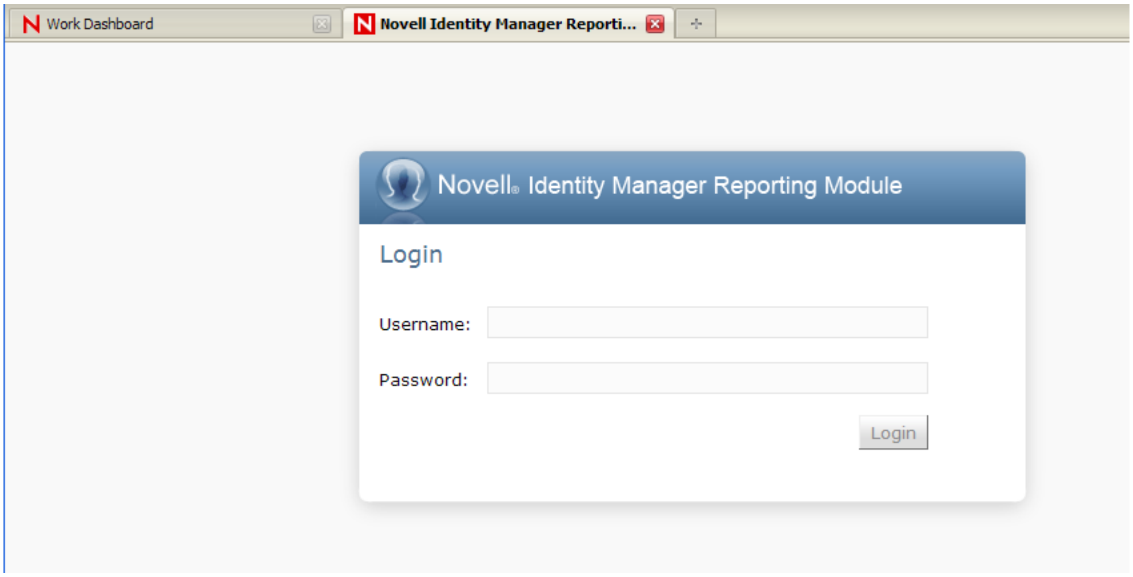
If you want to be able to launch the reporting module from the Work Dashboard in the User Application, you need to have your Configuration Administration specify the URL for the reporting module on the *Administration* tab. The Configuration Administrator needs to specify the URL in the *Novell Identity Manager Reporting Module URL* field within the *Provisioning UI Display Settings* page. In addition, you need to have the *Access Reporting Module* navigation permission. The Report Administrator is given this permission by default.

To access the Identity Reporting Module from the User Application:

1. Log into the User Application as a Report Administrator.
2. Click *Access Reporting Module* in the User Profile section of the Work Dashboard:



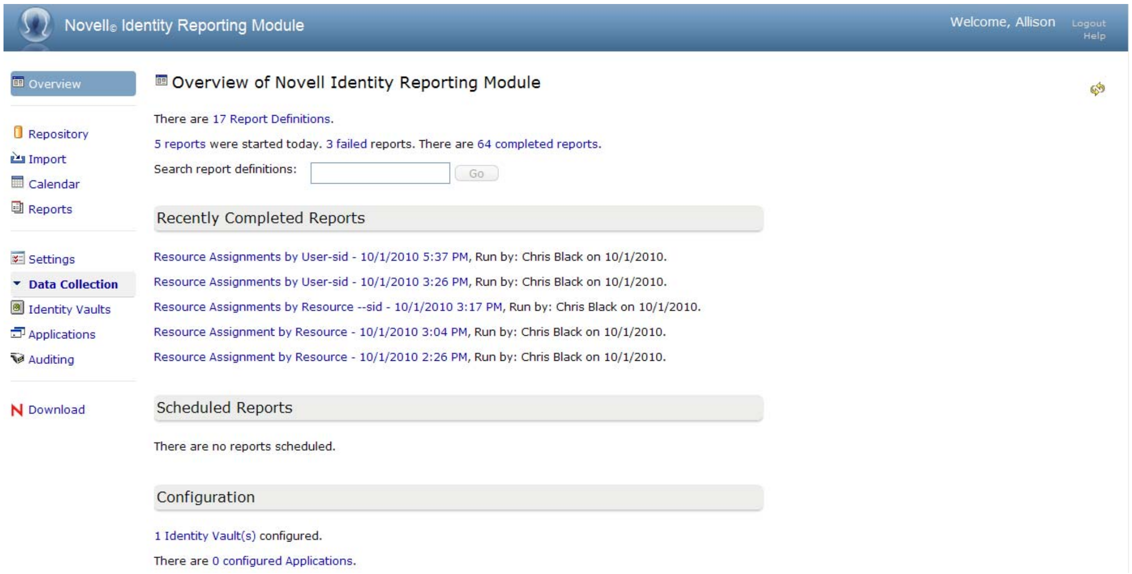
When you click this button, the login window for the reporting module opens in a new window:


Work Dashboard
Novell Identity Manager Reporti...
Novell® Identity Manager Reporting Module
Login
Username:
Password:
Login

When Single Sign-On (SSO) is enabled for the Roles Based Provisioning Module, you do not see the Login page. Instead, you are logged into the reporting module automatically.

3 If SSO has not been enabled, log in as a Report Administrator or other user that has the *Access Reporting Module* navigation permission.

The reporting module displays the *Overview* page:



Overview of Novell Identity Reporting Module

There are 17 Report Definitions.

5 reports were started today. 3 failed reports. There are 64 completed reports.

Search report definitions:

Recently Completed Reports

Resource Assignments by User-sid - 10/1/2010 5:37 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by User-sid - 10/1/2010 3:26 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by Resource --sid - 10/1/2010 3:17 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 3:04 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 2:26 PM, Run by: Chris Black on 10/1/2010.

Scheduled Reports

There are no reports scheduled.

Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

3.1.3 Configuring RBPM Access to the Reporting Module

To configure the Roles Based Provisioning Module so that it provides access to the Identity Reporting Module from the *Work Dashboard*:

1 Configure the URL for the reporting module, as follows:

- **1a** Log in to the RBPM User Application as a Configuration Administrator.
- **1b** On the *Administration* tab, navigate to *RBPM Provisioning and Security*.
- **1c** On the *Provisioning UI Display Settings* page, specify the URL for the reporting module in the *Novell Identity Manager Reporting Module URL* field. If the reporting module is running on the same server as the RBPM, you can use a relative URL such as /IDMRPT.

2 Optionally, enable SSO support:

- **2a** Log in to the RBPM User Application as an Application Administrator.
- **2b** On the *Administration* tab, navigate to *Application Configuration*.
- **2c** Select *Login* under *Password Module Setup*.
- **2d** On the *Login Settings* page, select *true* for *Enable SSO*.

NOTE: For SSO to work, cookies must be enabled on the client browser in which the user is running the User Application and the Identity Reporting Module. If cookies are disabled in the browser, the user sees the Login page when clicking on the *Access Reporting Module* button on the *Work Dashboard*.

3.1.4 Configuring Reporting to Work with Novell Access Manager

If you want to integrate Novell Access Manager and the Identity Reporting Module, you need to be aware that Novell does not currently support direct Single Sign On (SSO) between the two products. Instead, one must first access the User Application via Novell Access Manager, and then press the *Access Reporting Module* button on the left-hand navigation menu within the Work Dashboard.

To use this configuration, you need to perform some manual steps to configure the User Application and Novell Access Manager.

To configure the User Application:

1 Enable the *Enable SSO To Other Application* setting:

   1a Login to the User Application as the Administrator and go to *Administration* > *Application Configuration* > *Login*.

   1b Select the *true* radio button next to *Enable SSO To Other Application*.

   1c Press the *Save* button.

   1d Logout.

2 Correct the URL for the Identity Reporting Module:

   2a Login to the User Application as the Administrator and go to *Administration* > *RBPM Provisioning and Security* > *Provisioning UI Display Settings*.

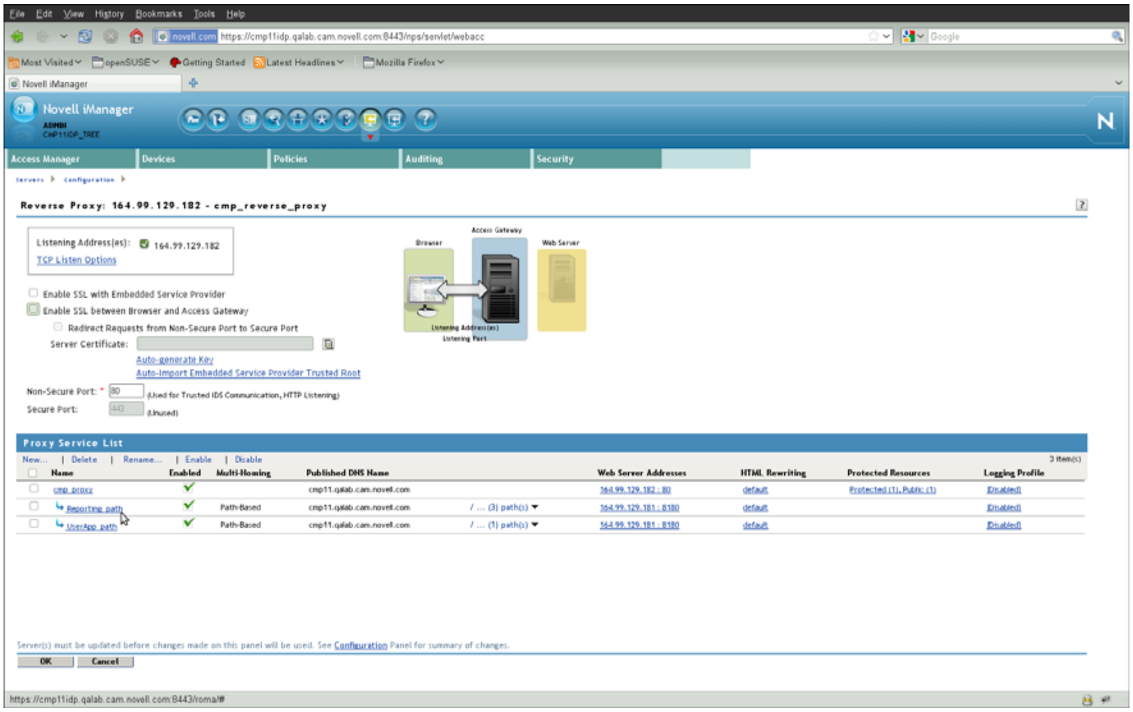
   2b In the text field to the right of *Novell Identity Reporting Module URL* ensure that the URL to the Reporting module is correct.

   2c Press *Save*.

   2d Logout.

To configure Novell Access Manager:

1 Create an entry for reporting in the *Proxy Service List*.



Reverse Proxy: 164.99.129.182 - cmp_reverse_proxy

Listening Address(es): ☑ 164.99.129.182

TCP Listen Options

□ Enable SSL with Embedded Service Provider

□ Enable SSL between Browser and Access Gateway

□ Redirect Requests from Non-Secure Port to Secure Port

Server Certificate:

Auto-generate Key

Auto-Import Embedded Service Provider Trusted Root

Non-Secure Port: * 80 (Used for Trusted IDS Communication, HTTP Listening)

Secure Port: 443 (Unused)

Proxy Service List

New... | Delete | Rename... | Enable | Disable — 3 item(s)

□	Name	Enabled	Multi-Homing	Published DNS Name		Web Server Addresses	HTML Rewriting	Protected Resources	Logging Profile
□	cmp_proxy	✓		cmp11.qalab.cam.novell.com		164.99.129.182 : 80	default	Protected (1), Public (1)	[Disabled]
□	↳ Reporting_path	✓	Path-Based	cmp11.qalab.cam.novell.com	/ ... (3) path(s) ▾	164.99.129.181 : 8180	default		[Disabled]
□	↳ UserApp_path	✓	Path-Based	cmp11.qalab.cam.novell.com	/ ... (1) path(s) ▾	164.99.129.181 : 8180	default		[Disabled]

Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.

2 You must add all three WAR files to the Path List:

   - /IDMRPT
   - /IDMRPT-AUTH
   - /IDMRPT-CORE

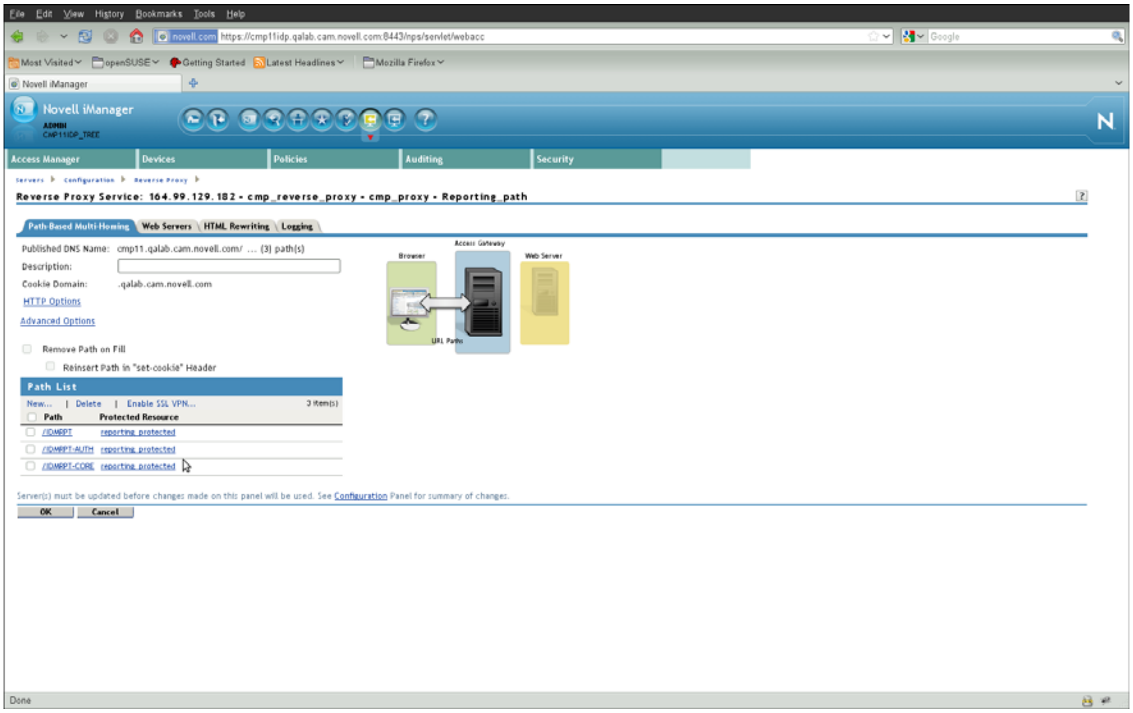
3 In the *Advanced Options* section add the follow entry:

```
ProxyErrorOverride on -401 -403
```

4 On the *Web Servers* Tab, make sure that the *Web Server Host Name* entry is the actual DNS name of the machine that the reporting module is deployed on.

5 Configure the Protected Resource.

It is not necessary to create or enable Authorization, Identity Injection, or Form Fill for the Identity Reporting Module. You only need to configure the Protected Resource. You can apply the same entries you are using for the User Application, but keep in mind that the end user will not be signed on with SSO directly from Access Manager. The end user will still see the login for the Identity Reporting Module.


File Edit View History Bookmarks Tools Help
novell.com https://cmp11idp.qalab.cam.novell.com:8443/nps/servlet/webacc
Google
Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox
Novell iManager
Novell iManager
ADMIN
CMP11IDP_TREE
N
Access Manager
Devices
Policies
Auditing
Security
Servers ▸ Configuration ▸ Reverse Proxy ▸
Path-Based Multi-Homing
Web Servers
HTML Rewriting
Logging
Access Gateway
Browser
Web Server
URL Paths
Done

Reverse Proxy Service: 164.99.129.182 - cmp_reverse_proxy - cmp_proxy - Reporting_path

Published DNS Name: cmp11.qalab.cam.novell.com/ ... (3) path(s)

Description:

Cookie Domain: .qalab.cam.novell.com

HTTP Options

Advanced Options

□ Remove Path on Fill

□ Reinsert Path in "set-cookie" Header

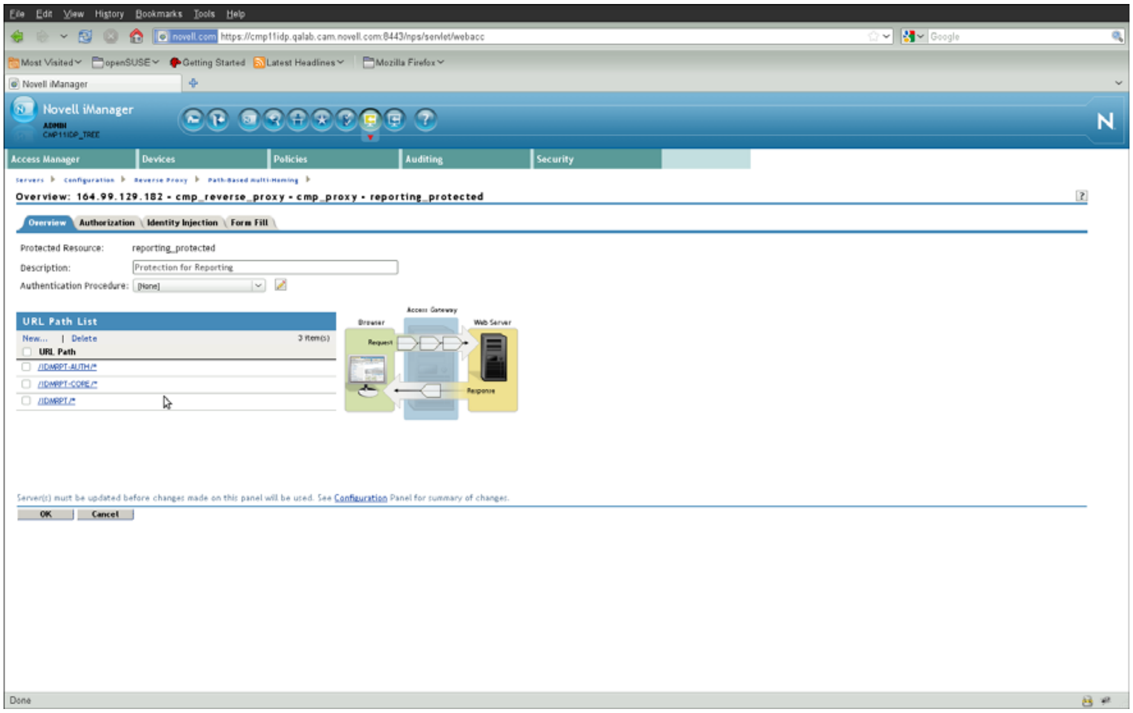
Path List

New... | Delete | Enable SSL VPN... 3 item(s)

□ Path	Protected Resource
□ /IDMRPT	reporting_protected
□ /IDMRPT-AUTH	reporting_protected
□ /IDMRPT-CORE	reporting_protected

Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.

OK Cancel


File Edit View History Bookmarks Tools Help
novell.com https://cmp11idp.qalab.cam.novell.com:8443/nps/servlet/webacc
Google
Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox
Novell iManager
Novell iManager
ADMIN
CMP11IDP_TREE
N
Access Manager
Devices
Policies
Auditing
Security
Servers ▸ Configuration ▸ Reverse Proxy ▸ Path-Based Multi-Homing ▸
Overview
Authorization
Identity Injection
Form Fill
Access Gateway
Browser
Web Server
Request
Response
Done

Overview: 164.99.129.182 - cmp_reverse_proxy - cmp_proxy - reporting_protected

Protected Resource: reporting_protected

Description: Protection for Reporting

Authentication Procedure: [None]

URL Path List

New... | Delete 3 item(s)

□ URL Path
□ /IDMRPT-AUTH/*
□ /IDMRPT-CORE/*
□ /IDMRPT/*

Server(s) must be updated before changes made on this panel will be used. See Configuration Panel for summary of changes.

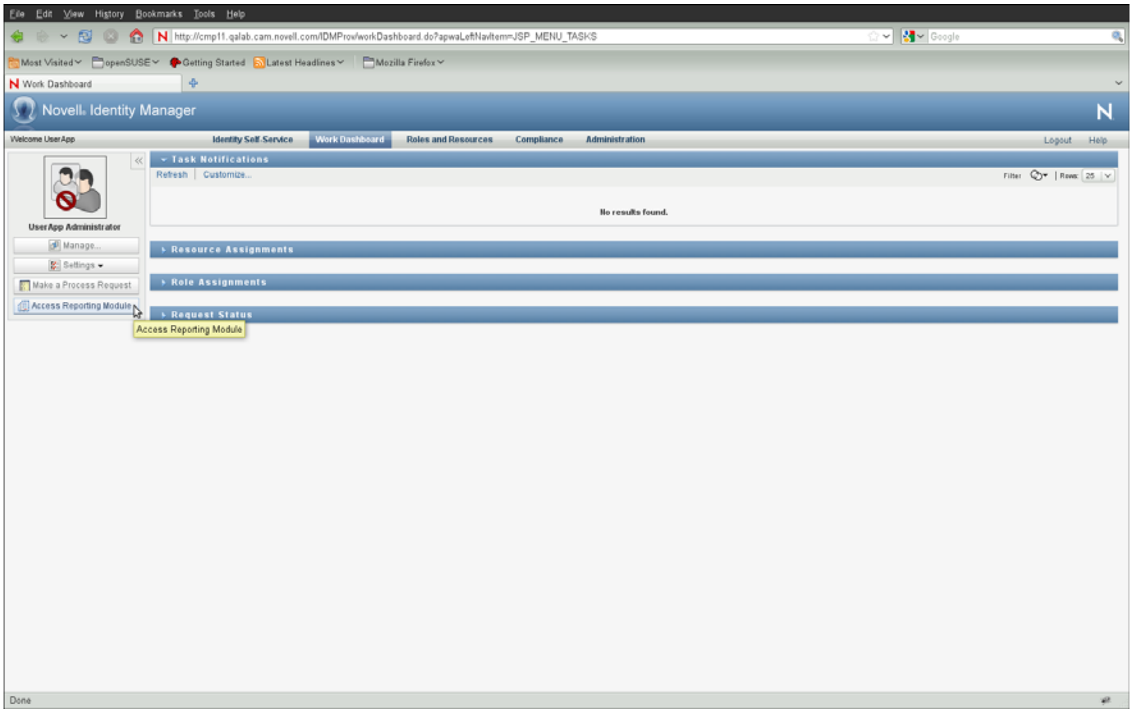
OK Cancel

Once these manual steps have been performed, the Reporting Administrator can use the configuration.

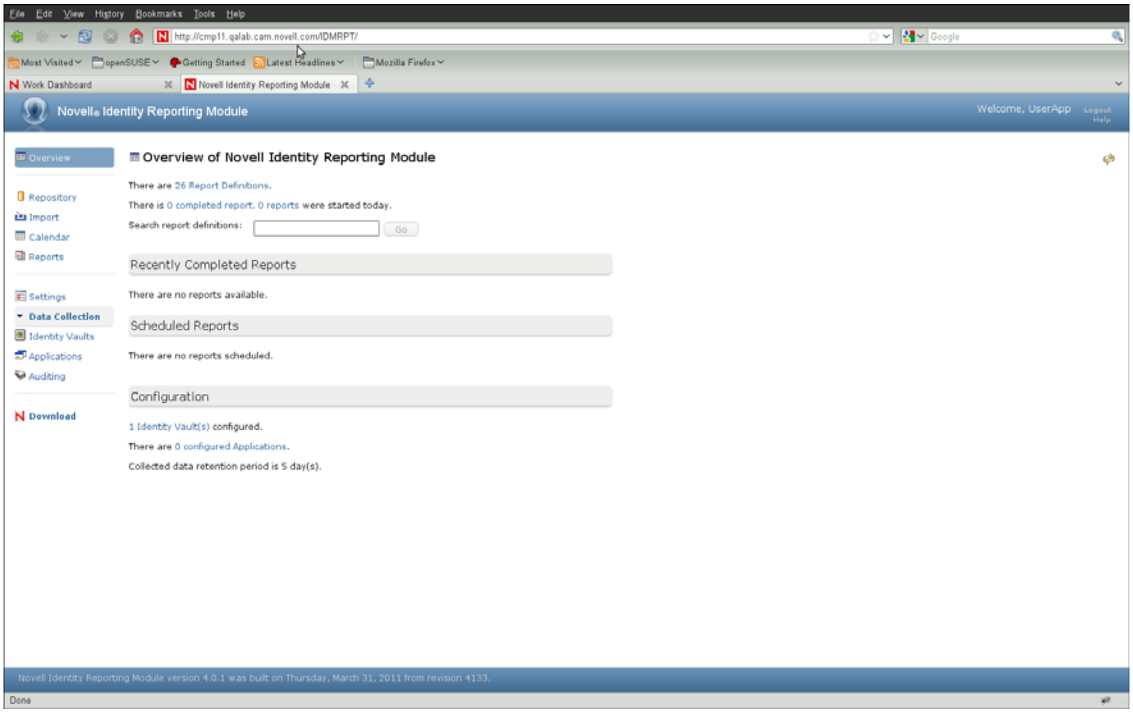
To use the configuration:

1 Access the User Application via Access Manager, where you will be signed on with SSO.

2 Press the *Access Reporting Module* button on the left-hand navigation menu on the Work Dashboard.



3 A new browser window will appear and the Reporting Administrator will be automatically logged into the Reporting Module. The URL in the browser will appear as the one controlled by Access Manager.


File Edit View History Bookmarks Tools Help
http://cmp11.qalab.cam.novell.com/IDMRPT/
Most Visited openSUSE Getting Started Latest Headlines Mozilla Firefox
Work Dashboard
Novell Identity Reporting Module
Novell® Identity Reporting Module
Welcome, UserApp
Logout
Help
Overview
Repository
Import
Calendar
Reports
Settings
Data Collection
Identity Vaults
Applications
Auditing
Download
Go
Done

Overview of Novell Identity Reporting Module

There are 26 Report Definitions.

There is 0 completed report. 0 reports were started today.

Search report definitions:

Recently Completed Reports

There are no reports available.

Scheduled Reports

There are no reports scheduled.

Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

Collected data retention period is 5 day(s).

Novell Identity Reporting Module version 4.0.1 was built on Thursday, March 31, 2011 from revision 4133.

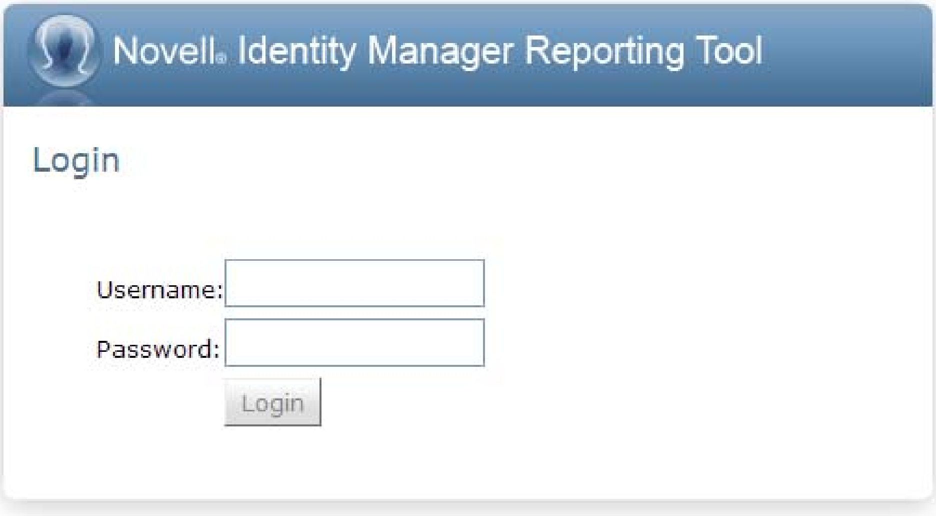
3.2 Logging In

You must be a Report Administrator to log in to the Identity Reporting Module. If you need help getting a username and password to supply for the login, see your system administrator.

To log in to the reporting module:

1 Start the application, as described under Section 3.1, “Accessing the Identity Reporting Module,” on page 101.

The reporting module displays the login page:



2 Type your user name and password.

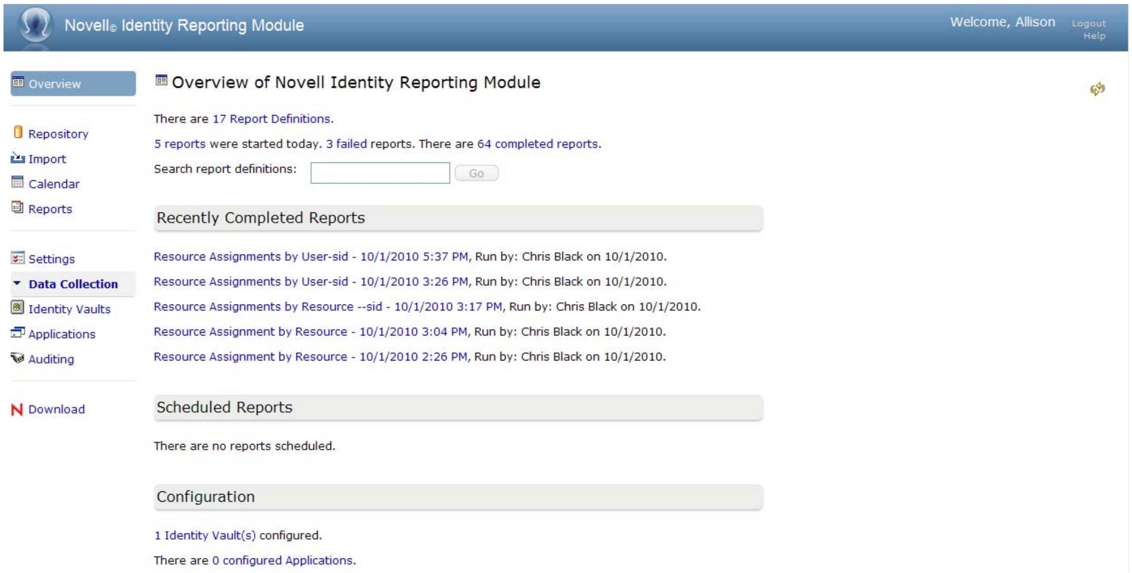
The Login page accepts two formats for user names:

Format	Rules
Full DN	You **must** escape special characters (if there are any) in a full DN according to RFC 2253/4514 section 2.4. You need to use the backslash character to escape special characters. By escaping special characters, you can avoid ambiguity.
Simple name	Do **not** escape special characters in a simple name. If subcontainer search is enabled (the LDAP administration credential and login attribute need to be configured at install time to enable it), the simple name is used in an LDAP search in the sub-tree of the user container. **NOTE:** If multiple accounts match the user name after a search has been performed, the reporting user interface displays an error message, instead of providing a list of accounts to choose from. This behavior ensures proper security for the user accounts within the Identity Vault. If multiple accounts are found, you can supply a full DN to ensure that the correct account is used for authentication. If subcontainer search is disabled, the simple name is treated as an attribute value for the CN, which is then combined with the user container DN to form a user DN. In both cases, the login facility is able to escape special characters appropriately.

At installation time, the administrator needs to escape special characters (if there are any) for the User Application Driver, driver set, and driver set container.

3 Click *Login*.

The module displays the *Overview* page, with a *Welcome* message in the upper right corner that shows the first name of the logged in user:



Overview of Novell Identity Reporting Module

There are 17 Report Definitions.

5 reports were started today. 3 failed reports. There are 64 completed reports.

Search report definitions:

Recently Completed Reports

Resource Assignments by User-sid - 10/1/2010 5:37 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by User-sid - 10/1/2010 3:26 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by Resource --sid - 10/1/2010 3:17 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 3:04 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 2:26 PM, Run by: Chris Black on 10/1/2010.

Scheduled Reports

There are no reports scheduled.

Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

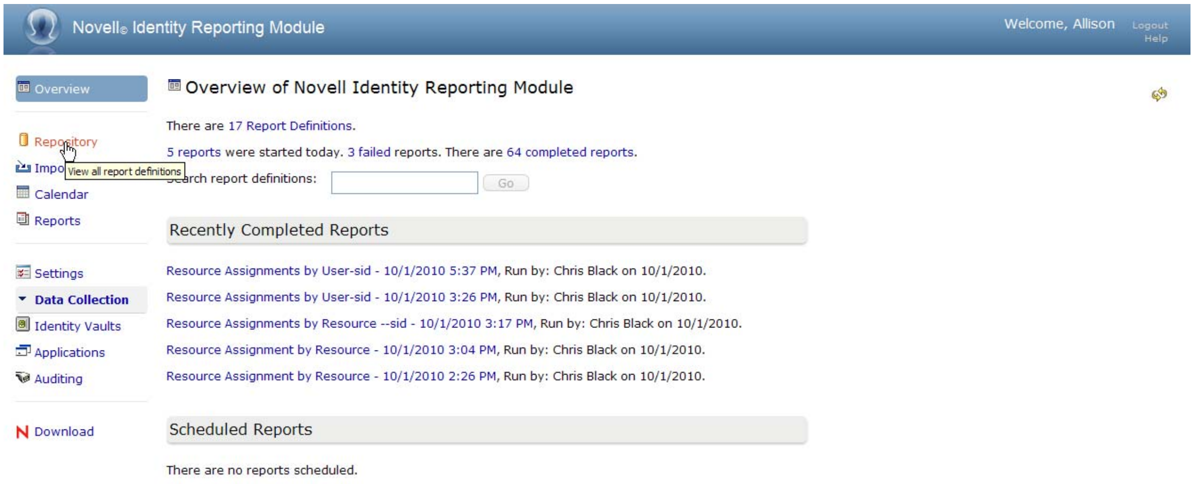
When you log in to the reporting module as a Report Administrator, you have access to the full range of reporting capabilities within the application.

If your user name and password are not entered correctly, or if you are not a Report Administrator, the Login page displays an error message and does not permit you to use the application.

3.3 Exploring the Identity Reporting Module

After you log in, the Identity Reporting Module shows a left navigation menu that provides access to various pages that let you perform reporting actions. To navigate to a particular page, click the menu item for the page you want to view:

Figure 3-1 *Navigating within the Identity Reporting Module*



Overview of Novell Identity Reporting Module

There are 17 Report Definitions.

5 reports were started today. 3 failed reports. There are 64 completed reports.

Search report definitions:

Recently Completed Reports

Resource Assignments by User-sid - 10/1/2010 5:37 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by User-sid - 10/1/2010 3:26 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by Resource --sid - 10/1/2010 3:17 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 3:04 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 2:26 PM, Run by: Chris Black on 10/1/2010.

Scheduled Reports

There are no reports scheduled.

If you look at the left navigation menu, you see the following menu choices:

- *Overview* (which is open by default)

  To learn about this tab and how to work with it, see Chapter 4, “Using the Overview Page,” on page 111.

- *Repository*

  To learn about this tab and how to work with it, see Chapter 5, “Using the Repository Page,” on page 115.

- *Import*

  To learn about this tab and how to work with it, see Chapter 6, “Using the Import Tool,” on page 127.

- *Calendar*

  To learn about this tab and how to work with it, see Chapter 7, “Using the Calendar Page,” on page 131.

- *Reports*

  To learn about this tab and how to work with it, see Chapter 8, “Using the Completed and Running Reports Page,” on page 143.

- *Settings*

To learn about this tab and how to work with it, see Chapter 9, "Configuring Settings and Data Collection," on page 149.

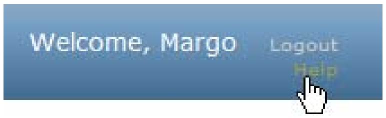
- *Data Collection*

  To learn about this tab and how to work with it, see Chapter 9, "Configuring Settings and Data Collection," on page 149.

3.3.1 Getting Help

While working in the Identity Reporting Module, you can display the online version of this guide to get help on a particular feature of the product:

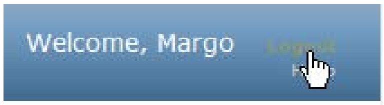
1 Click the *Help* link (in the top right corner of the page).



3.3.2 Logging Out

When you finish working in the Identity Reporting Module and want to end your session, you can log out.

1 Click the *Logout* link (in the top right corner of the page).



3.3.3 Token Timeout

Instead of timing out when a user session is idle, the Identity Reporting Module implements a token timeout strategy to manage user logins. The token associated with each user login times out automatically after a specified period of time, regardless of what the user does. After a token timeout occurs, the reporting module preserves the user's data. The user can log in again and resume work without losing any data.

The administrator can set the token timeout value at installation time, or configure it later by using the post-installation utility provided with the Identity Reporting Module.

The token timeout feature greatly reduces the risk that an unauthorized user could impersonate a user who had previously logged in to the reporting module. After a timeout has occurred, the token is no longer valid and cannot be reused. This is not the case with many applications that rely on a conventional session timeout mechanism, because the session information can be passed on and reused by another person.

4 Using the Overview Page

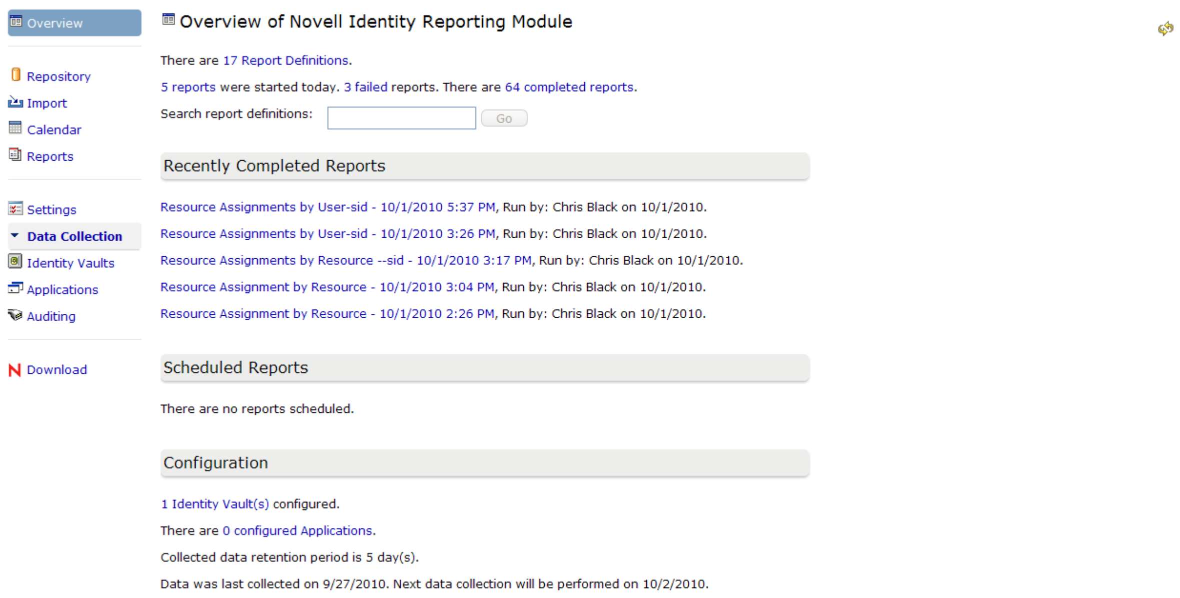
This section provides instructions for using the Overview page in the Identity Reporting Module.

4.1 About the Overview Page

The Overview page is the first page you see when you log into the Identity Reporting Module. This page provides an overview of the data in the system. The top of the page includes summary information, such as the number of report definitions and the number of started, failed, and completed reports. The page also includes a search facility that provides a quick way to find report definitions by name.

Below the report summary area, the Overview page shows several additional sections. These sections give you a convenient way to see a list of the most recently completed reports and the reports scheduled to be run. At the bottom of the Overview page, you can find details about the reporting module configuration, such as the number of Identity Vaults and non-managed applications configured, and the current setting for data retention.

Figure 4-1 *Overview Page*



Overview of Novell Identity Reporting Module

There are 17 Report Definitions.

5 reports were started today. 3 failed reports. There are 64 completed reports.

Search report definitions:

Recently Completed Reports

Resource Assignments by User-sid - 10/1/2010 5:37 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by User-sid - 10/1/2010 3:26 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by Resource --sid - 10/1/2010 3:17 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 3:04 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 2:26 PM, Run by: Chris Black on 10/1/2010.

Scheduled Reports

There are no reports scheduled.

Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

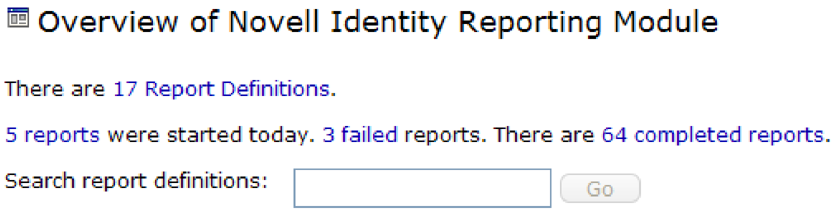
Collected data retention period is 5 day(s).

Data was last collected on 9/27/2010. Next data collection will be performed on 10/2/2010.

4.2 Viewing the Report Summary

The top of the Overview page provides a summary count of the number of report definitions, reports generated today, and completed reports in the system at the current time:

Figure 4-2 *Top of the Overview Page*



Overview of Novell Identity Reporting Module

There are 17 Report Definitions.

5 reports were started today. 3 failed reports. There are 64 completed reports.

Search report definitions:

To see a list of the report definitions on the Repository page, click the text that shows the summary count (for example, *17 Report Definitions*).

To see a list of the completed reports on the Completed and Running Reports page, click the text that shows the count (for example, *64 completed reports*).

4.3 Searching for a Report Definition

1 Type a search string in the *Search report definitions* text field.

For complete details on entering a search string, see Section 5.7, “Searching for a Report Definition,” on page 124.

2 Click *Go*.

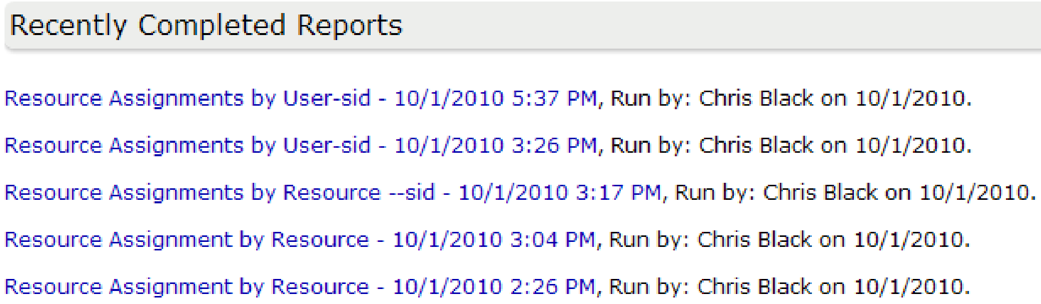
The interface displays the Repository page with a list of the reports that satisfy your search criteria.

You can clear the current search criteria and refresh the display by clicking *Overview* on the left navigation menu, or by clearing the *Search report definitions* field and clicking the *Go* button again.

4.4 Viewing the List of Recently Completed Reports

The *Recently Completed Reports* section of the page lists the reports that finished most recently:

Figure 4-3 *Recently Completed Reports Section of the Overview Page*



Recently Completed Reports

Resource Assignments by User-sid - 10/1/2010 5:37 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by User-sid - 10/1/2010 3:26 PM, Run by: Chris Black on 10/1/2010.

Resource Assignments by Resource --sid - 10/1/2010 3:17 PM, Run by: Chris Black on 10/1/2010.

Resource Assignment by Resource - 10/1/2010 3:04 PM, Run by: Chris Black on 10/1/2010.

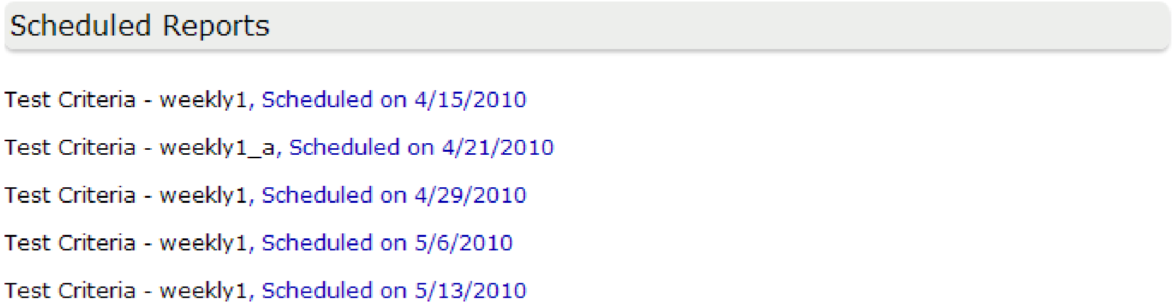
Resource Assignment by Resource - 10/1/2010 2:26 PM, Run by: Chris Black on 10/1/2010.

To open the generated PDF (or CSV) file for a particular report in the list, click the text that shows the report name (for example, *Resource Assignments by Resource - 10/1/2010 3:04 PM*).

4.5 Viewing the List of Upcoming Reports

The *Upcoming Reports* section of the page lists the next five reports that are scheduled to run:

Figure 4-4 *Scheduled Reports Section of the Overview Page*



Scheduled Reports

Test Criteria - weekly1, Scheduled on 4/15/2010

Test Criteria - weekly1_a, Scheduled on 4/21/2010

Test Criteria - weekly1, Scheduled on 4/29/2010

Test Criteria - weekly1, Scheduled on 5/6/2010

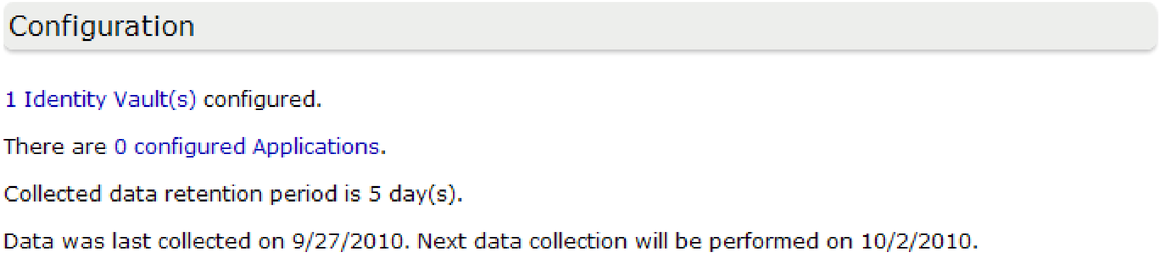
Test Criteria - weekly1, Scheduled on 5/13/2010

To see a particular scheduled report on the *Calendar* page, click the text that shows the schedule date for the report (for example, *Scheduled on 5/6/2010*).

4.6 Viewing the Configurations

The *Configurations* section of the page shows all of the managed systems and Identity Vaults that have been configured for the reporting system, as well as the retention period specified for the collected data and the date that the data was last collected:

Figure 4-5 *Configuration Section of the Overview Page*



Configuration

1 Identity Vault(s) configured.

There are 0 configured Applications.

Collected data retention period is 5 day(s).

Data was last collected on 9/27/2010. Next data collection will be performed on 10/2/2010.

To see the settings for the configured Identity Vaults on the Identity Vault Data Sources page, click the text that shows the number of vaults configured (for example, *1 Identity Vault(s)*. To see the settings for the non-managed applications, click the text that shows the number of applications configured (for example, *0 configured Applications*).

5 Using the Repository Page

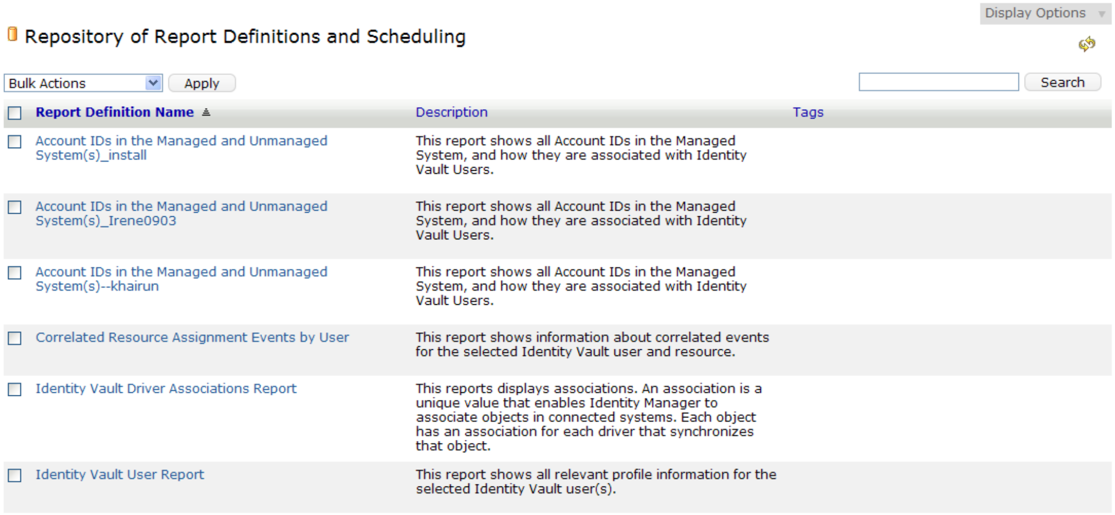
This section provides instructions for using the Repository page in the Identity Reporting Module.

- Section 5.1, “Viewing the List of Existing Reporting Definitions,” on page 115
- Section 5.2, “Editing a Report Definition,” on page 116
- Section 5.3, “Copying an Existing Report Definition,” on page 122
- Section 5.4, “Running a Report,” on page 123
- Section 5.5, “Deleting a Report Definition,” on page 123
- Section 5.6, “Performing Bulk Actions,” on page 124
- Section 5.7, “Searching for a Report Definition,” on page 124
- Section 5.8, “Sorting the List of Reports,” on page 125
- Section 5.9, “Defining the Repository Display Options,” on page 125
- Section 5.10, “Refreshing the Report Definition List,” on page 126

5.1 Viewing the List of Existing Reporting Definitions

1 Click *Repository* in the left navigation menu.

The Repository shows the list of reports that have been imported into the reporting module.



☐	Report Definition Name	Description	Tags
☐	Account IDs in the Managed and Unmanaged System(s)_install	This report shows all Account IDs in the Managed System, and how they are associated with Identity Vault Users.	
☐	Account IDs in the Managed and Unmanaged System(s)_Irene0903	This report shows all Account IDs in the Managed System, and how they are associated with Identity Vault Users.	
☐	Account IDs in the Managed and Unmanaged System(s)--khairun	This report shows all Account IDs in the Managed System, and how they are associated with Identity Vault Users.	
☐	Correlated Resource Assignment Events by User	This report shows information about correlated events for the selected Identity Vault user and resource.	
☐	Identity Vault Driver Associations Report	This reports displays associations. An association is a unique value that enables Identity Manager to associate objects in connected systems. Each object has an association for each driver that synchronizes that object.	
☐	Identity Vault User Report	This report shows all relevant profile information for the selected Identity Vault user(s).	

For each report definition, the list shows report name and description, as well as any tags that have been specified for the report.

The Repository includes a special report called *Template*. This report is included as a subreport within other reports added to the system. It displays a header and footer in any report with which it is included. This report cannot be deleted and should not be run by itself. In addition, this report does not show a check box next to it in the list, because it can not be included in bulk actions. When you edit the *Template* item, you do not see the *Output Format*, *Default Notifications*, *Schedule*, and *Run Now* controls.

The Identity Reporting Module ships with a set of predefined reports. You need to import these into the reporting module. After they have been imported, these reports are added to the list on the Repository page. You can define a new report by copying one of the predefined report definitions and giving it a new name.

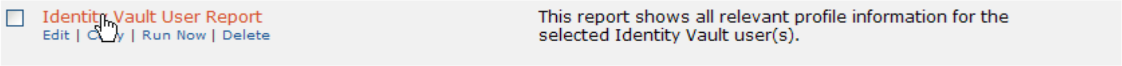
For details on the predefined reports, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm402/idm_reports/data/bookinfo.html).

You cannot create a new report from scratch on the Repository page. To create a new report definition from scratch, you need to design the report layout outside of the Identity Reporting Module, and use the Import facility to import the report into the reporting module.

The reporting module stores all report definitions, report schedules, and completed reports in the Identity Information Warehouse. These objects are stored in tables within the idm_rpt_cfg schema in the SIEM database.

5.2 Editing a Report Definition

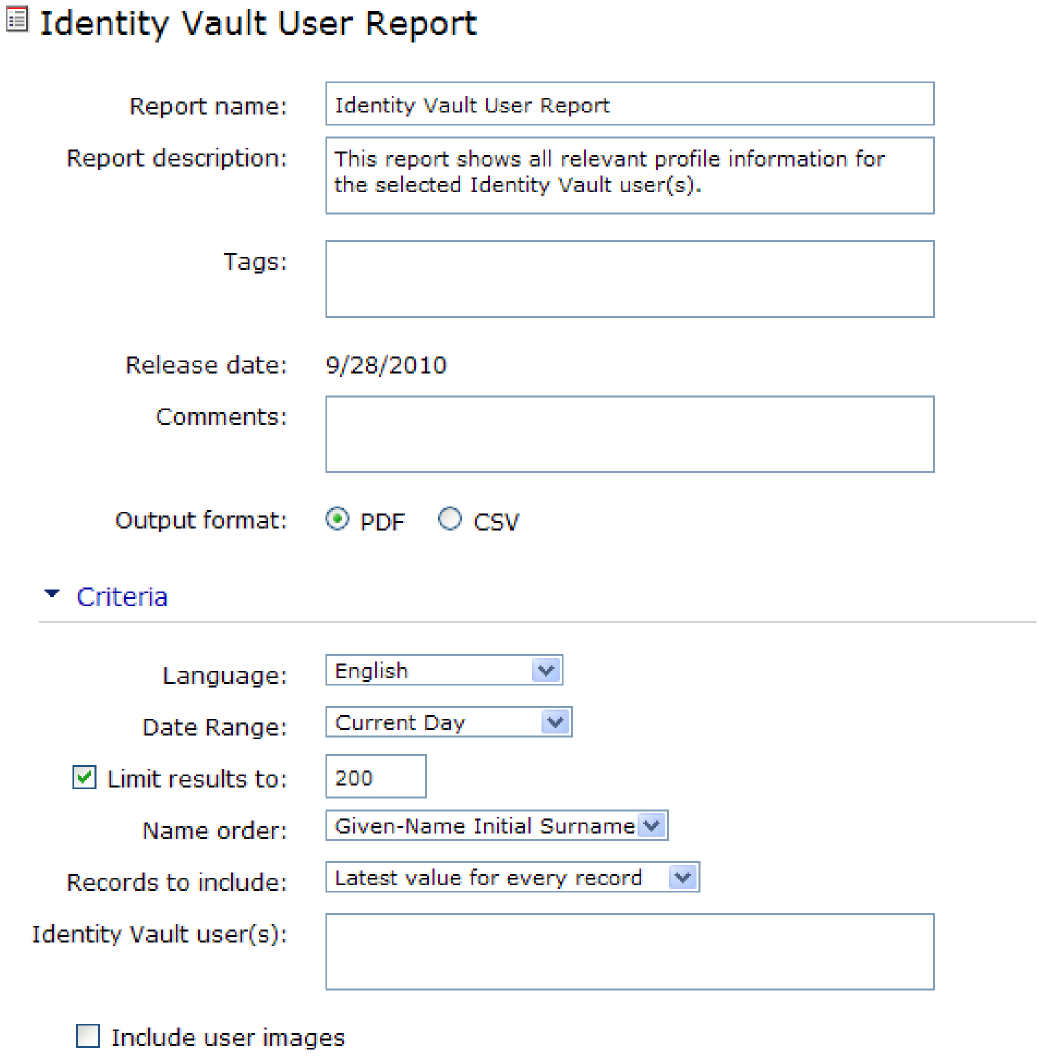
1 Click the name of the report definition in the list on the Repository page.



This report shows all relevant profile information for the selected Identity Vault user(s).

Alternatively, you can mouse over the report definition (or select the check box beside the name) and click *Edit*.

When you edit a report definition, a page displays to allow you to make changes to the definition:



Identity Vault User Report

Report name: Identity Vault User Report

Report description: This report shows all relevant profile information for the selected Identity Vault user(s).

Tags:

Release date: 9/28/2010

Comments:

Output format: ● PDF ○ CSV

▼ Criteria

Language: English

Date Range: Current Day

☑ Limit results to: 200

Name order: Given-Name Initial Surname

Records to include: Latest value for every record

Identity Vault user(s):

□ Include user images

The fields at the top of the page allow you to modify the name, description, tags, comments, and output format (PDF or CSV) for the report. Tags can be used to organize reports according to common words or phrases that suggest how the reports are related. Tag names share a common namespace for all users, so you need to specify tag names that make sense for all users. Tag names cannot be localized.

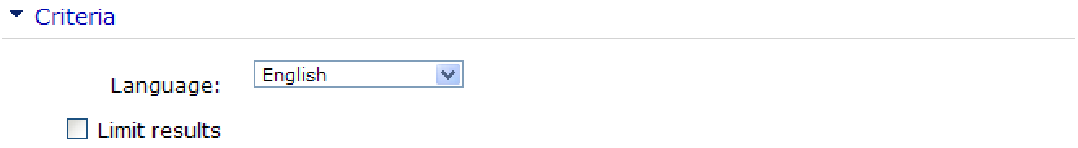
You can specify one or more tags for a report definition. If you specify multiple tags, the tags must be separated by commas. After they are defined, tags are also shown in the list displayed on the Repository page, and in the Detail dialog box for a report listed on the Completed and Running Reports page. In the list displayed on the Repository page, the tags are alphabetized to allow for sorting.

NOTE: The next time you edit the report definition, the tags appear in alphabetical order, regardless of how they were originally entered. The tags are also alphabetized in the Repository list, even if you did not alphabetize them when you first entered them.

The other fields on the page are organized into the following sections:

- Criteria
- Default Notifications
- Schedule

2 To edit the criteria for the report, open the Criteria section and make changes as necessary:



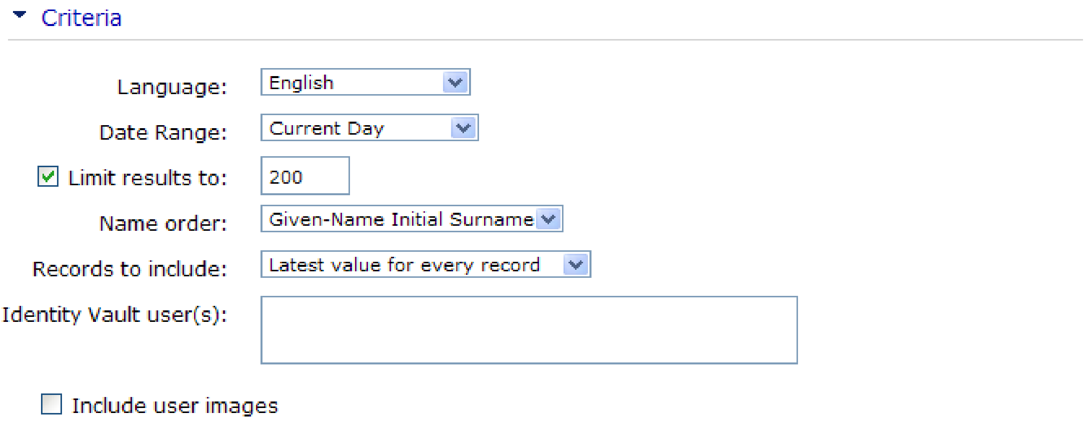
Criteria

Language: English

□ Limit results

The Criteria section does not appear unless the imported definition included one or more report parameters.

The number of fields displayed in the Criteria section and the way these fields behave depend on how they were specified in the original report definition object imported into the reporting module. For example, this object includes several fields for defining criteria:



Criteria

Language: English

Date Range: Current Day

☑ Limit results to: 200

Name order: Given-Name Initial Surname

Records to include: Latest value for every record

Identity Vault user(s):

□ Include user images

The reporting module supports the following data types for criteria fields:

- String
- String with Options
- Date
- Integer
- Boolean
- Lookup

The control displayed for each data type varies depending on how the parameter is defined in the report definition. For multivalued options, a multiselect control is displayed, but a single value control is displayed for a parameter that only accepts a single value.

Some criteria fields are required by the report definition, but others are optional. If you do not provide a value for a required field, the user interface displays an error message.

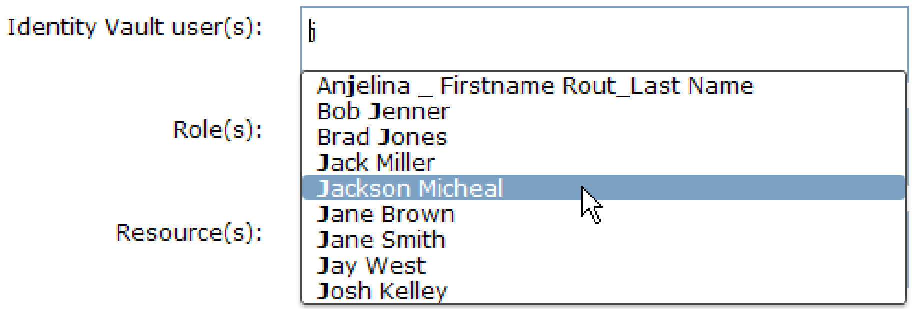
The following criteria parameters are available with most of the reports installed with the reporting module:

Parameter	Description
Language	Defines the target language for the report.

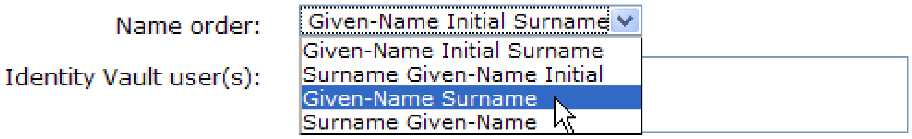
Parameter	Description
Date Range	Allows you to define a range of dates for the data include in the report. The following choices are available: ◆ *Current Day* ◆ *Previous Day* ◆ *Week to Date* ◆ *Previous Week* ◆ *Month to Date* ◆ *Previous Month* ◆ *Custom Date Range*
From Date	Allows you to specify a fixed start date for the report data. This parameter is only enabled when *Custom Data Range* is selected for the *Data Range* parameter.
To Date	Allows you to specify a fixed end date for the report data. This parameter is only enabled when *Custom Data Range* is selected for the *Data Range* parameter.
Limit Results to	Controls the maximum number of rows that will be included in the report data.

If a report definition includes one or more fields for defining dates, such as *Date Range*, *From Date*, and *To Date*, you need to be aware that the date range you specify affects the data returned with the report, not the dates on which the report is run. Therefore, if a report is run on a monthly basis, you should not define a custom date range that fixes the dates in the *From Date* and *To Date* fields. It does not make sense for a monthly scheduled report to report on a fixed date range (such as 3/10/2010 - 3/17/2010). If you want to report on a fixed date range, you should schedule the report to run only once. For a monthly report, use one of the relative date range settings included in the *Date Range* field, such as *Month to Date*. This ensures that the data in the report is updated each month.

Some criteria fields support automatic completion, which allows you to type several characters and then select an item from a list of possible choices. For example, an *Identity Vault user(s)* field might allow you to type the first few characters of a user's name and then select the user from a list of users whose names contain the characters you have typed:

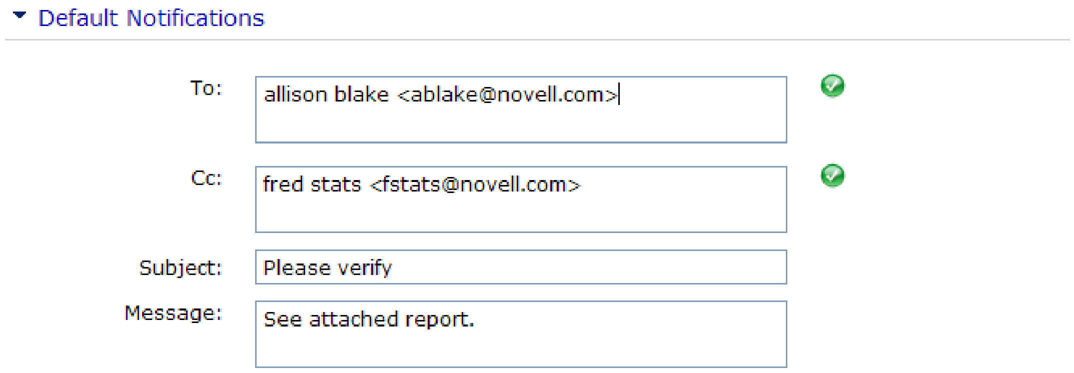


Some reports allow you to define the display name order used by other criteria fields that support the auto complete feature. For example, a report definition might include a *Name order* field that lets you specify the name order pattern used for the *Identity Vault user(s)* criteria field. The *Name order* field allows you to select one of the following name order patterns:


Name order: Given-Name Initial Surname

Identity Vault user(s):

3 To edit the e-mail settings associated with the report definition, open the Default Notifications section and make changes as necessary:



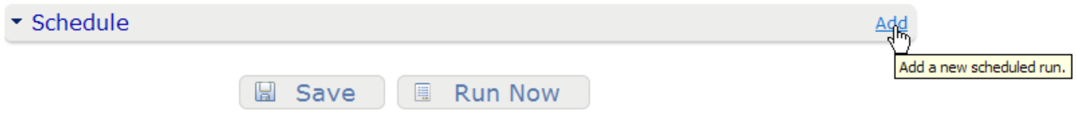
To: allison blake <ablake@novell.com>

Cc: fred stats <fstats@novell.com>

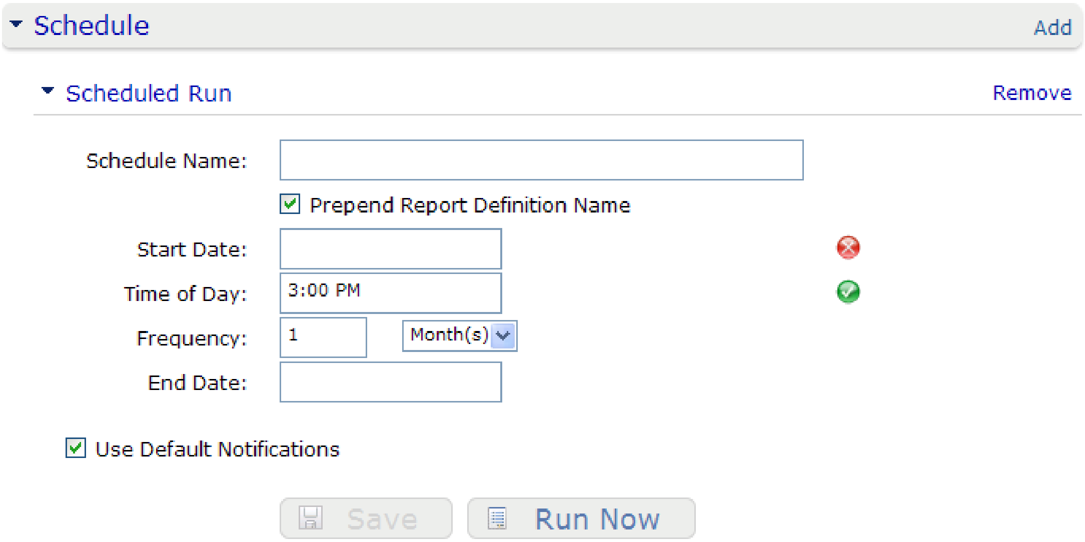
Subject: Please verify

Message: See attached report.

4 To add a new schedule for the report definition, click the *Add* button on the far right side of the Schedule section:



The page displays the following fields to allow you to define the schedule:



Schedule | Add

Scheduled Run | Remove

Schedule Name:

☑ Prepend Report Definition Name

Start Date:

Time of Day: 3:00 PM

Frequency: 1 Month(s)

End Date:

☑ Use Default Notifications

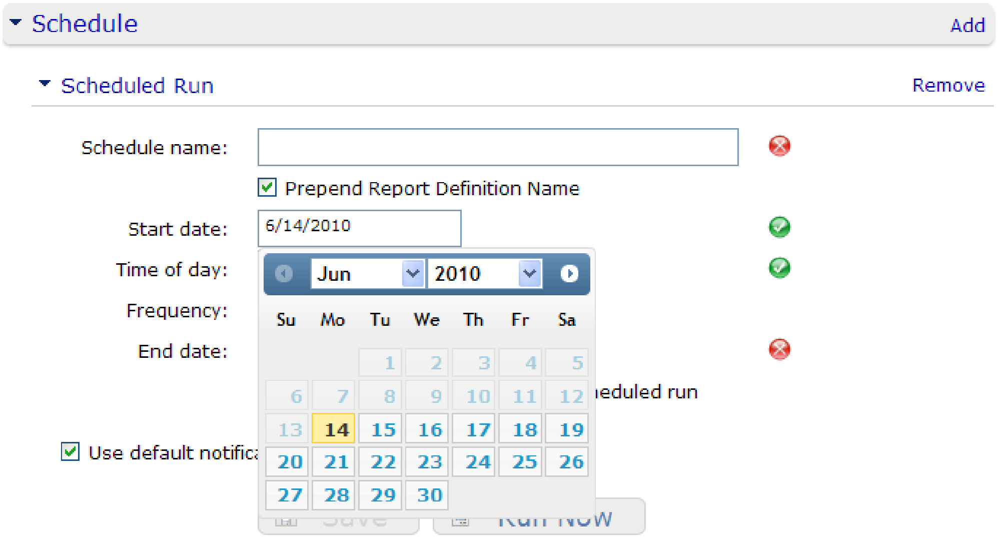
4a Provide a name for the schedule in the *Schedule Name* field.

The name for a schedule must be unique within the report definition, but does not need to be unique within the Identity Reporting Module as a whole.

4b If you want the name of the report definition to be added to the beginning of the schedule name, select the *Prepend Report Definition Name* field.

This option allows you to see which report has been scheduled with each schedule instance in the *Calendar* page. This option is enabled by default.

4c Click in the *Start Date* field to display a simplified calendar for selecting dates.



Schedule | Add

Scheduled Run | Remove

Schedule name:

☑ Prepend Report Definition Name

Start date: 6/14/2010

Time of day:

Frequency:

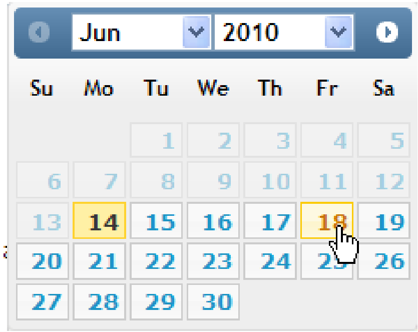
End date:

☑ Use default notific

Jun 2010

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

4d Select the date in the calendar on which you want to initiate the first run of the report.



Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

4e Select the approximate time of day for each run in the *Time of day* field. The time of day is based on the clock on the server where the report is executed. The actual execution time depends on server activity.

4f In the *Frequency* field, type the repeat interval (a number that specifies how often the report will run) and select the time period for report runs, such as Month(s), Week(s), or Day(s).

4g Click in the *End date* field to display the calendar. Select the date in the calendar after which no more runs should occur. Note that the last report run may not actually occur on this date. For example, if you choose October 15 as the start date, and specify a repeat interval of two weeks and an end date of November 1, the report will be run on October 15 and October 29. In this case, October 29 is the last run.

4h If you want the reporting module to execute a data collection procedure prior to report generation, select the *Attempt data collection before scheduled run* check box.

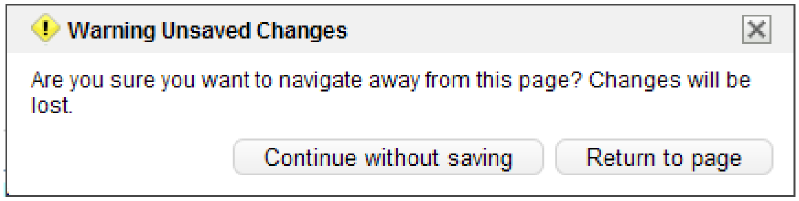
The report runs at its scheduled time, regardless of whether the data collection completed successfully.

5 To edit an existing schedule, open the Scheduled Run section for the schedule you want to edit and make any changes you like.

6 To save the report definition and schedule, click *Save*.

7 To queue a report to run immediately, click *Run Now*.

If you make changes to a report definition, and then try to go to another page in the Identity Reporting Module, the interface displays a warning message:



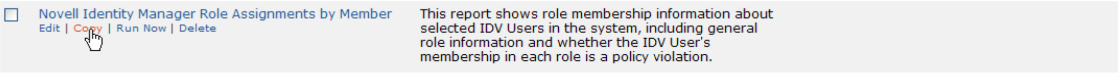
Warning Unsaved Changes

Are you sure you want to navigate away from this page? Changes will be lost.

5.3 Copying an Existing Report Definition

To create a new report definition by making a copy of an existing report definition:

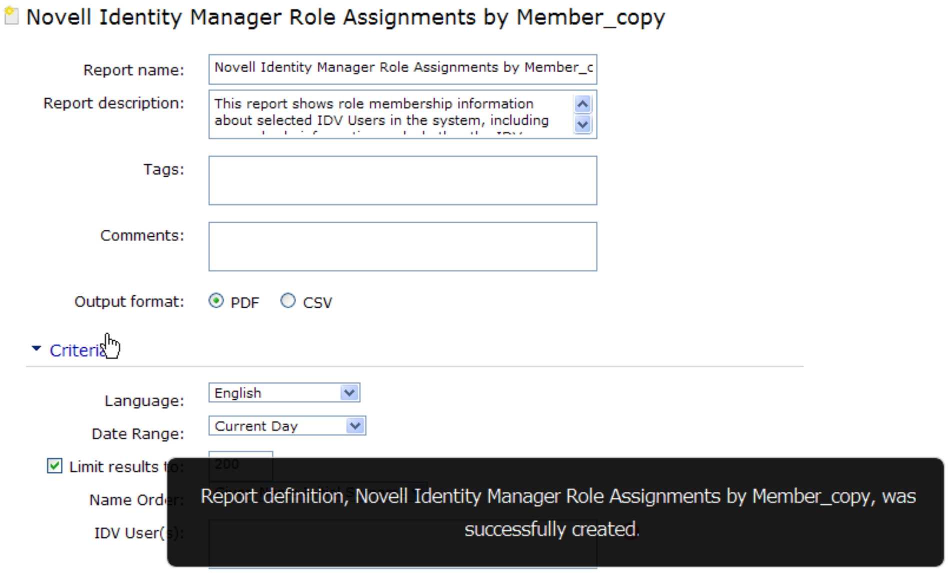
1 Mouse over the report definition (or select the check box next to the name) and click *Copy*.



□ Novell Identity Manager Role Assignments by Member
Edit | Copy | Run Now | Delete

This report shows role membership information about selected IDV Users in the system, including general role information and whether the IDV User's membership in each role is a policy violation.

The interface displays the report definition editing page with a message indicating that the new report was created. The name of the new report definition has a number appended to the name of the original report used for the copy operation:



Novell Identity Manager Role Assignments by Member_copy

Report name: Novell Identity Manager Role Assignments by Member_c

Report description: This report shows role membership information about selected IDV Users in the system, including

Tags:

Comments:

Output format: ● PDF ○ CSV

Criteria

Language: English

Date Range: Current Day

☑ Limit results to: 200

Name Order:

IDV User(s):

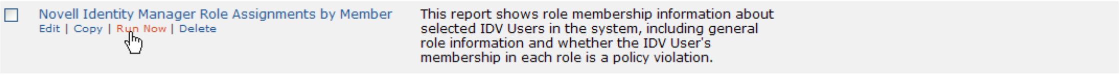
Report definition, Novell Identity Manager Role Assignments by Member_copy, was successfully created.

After the editing page appears, you can make changes to the definition just as you would to any other report definition in the repository. Because the default report name is not very informative, you should change the name to something more meaningful.

5.4 Running a Report

To queue a report to run immediately from the Repository list view:

1 Mouse over the report definition (or select the check box next to the name) and click *Run Now*.



□ Novell Identity Manager Role Assignments by Member
Edit | Copy | Run Now | Delete

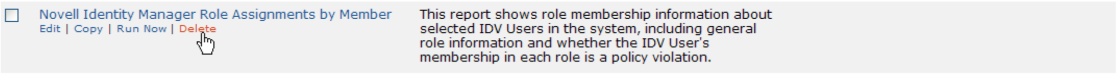
This report shows role membership information about selected IDV Users in the system, including general role information and whether the IDV User's membership in each role is a policy violation.

Startup process requires extra time before reports can be generated When you first start the Identity Reporting Module, wait 5 minutes before running a report. The startup process consumes a lot of memory, leaving less memory for the report generation. If you do not wait 5 minutes, you may encounter memory errors.

5.5 Deleting a Report Definition

To delete a report definition:

1 Mouse over the report definition (or select the check box next to the name) and click *Delete*.



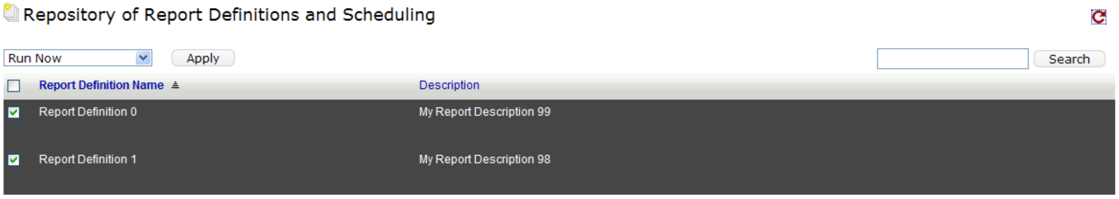
□ Novell Identity Manager Role Assignments by Member
Edit | Copy | Run Now | Delete

This report shows role membership information about selected IDV Users in the system, including general role information and whether the IDV User's membership in each role is a policy violation.

5.6 Performing Bulk Actions

To run (or delete) several reports at once:

1. Select the check box to the left of each report definition you want to run or delete.
2. Select the operation (*Run Now* or *Delete*) in the *Bulk Actions* drop-down list.
3. Click *Apply*.



☐ Report Definition Name ▲	Description
☑ Report Definition 0	My Report Description 99
☑ Report Definition 1	My Report Description 98

Bulk actions apply to the current page only. If you select several items on one page, then navigate to the next page to select some additional items, a subsequent attempt to perform a bulk action such as *Run Now* or *Delete* only applies to the second set of items you selected. The previous selections are retained and still appear selected if you navigate back to the first page. However, the bulk action is not performed on these items.

5.7 Searching for a Report Definition

To search for a report definition in the Repository:

1. Type a search string in the *Search* text field.

   The search facility allows you to pass in search strings for any of the following items:

Filter Value	Description
Name	Performs a contains search. The search is case insensitive, and it uses the locale of the user.
Description	Performs a contains search. The search is case insensitive, and it uses the locale of the user.
Tags	Performs an exact string search. The search is case insensitive. You need to pass in a single tag only.

   You can enter one or more words in the *Search* field, with or without quotes:

   - If you enter multiple words without quotes, the search results include reports that contain all of the words anywhere in the Name or Description, or that have all of the words as tags (that match exactly).

     For example, suppose you enter the following:

     ```
     identity users
     ```

     In this case, the following report definitions are in the results:

     - Reports with a Name containing the words `identity` and `users` anywhere in the string

    - Reports with a Description containing the words `identity` and `users` anywhere in the string
    - Reports with Tags having both `identity` and `users` as exact tags
- If you enter multiple words surrounded by double quotes, the search results include reports that include the entire phrase anywhere in the Name or Description, or that have a tag that matches the entire phrase.

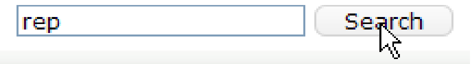
  For example, suppose you enter the following:

  ```
  "identity users"
  ```

  In this case, the following report definitions are in the results:

    - Reports with Name containing the phrase “identity users”.
    - Reports with Description containing the phrase “identity users”.
    - Reports with a Tag that exactly matches “identity users”.

2 Click *Search*.



You can clear the current search criteria and refresh the display by clicking *Repository* on the left navigation menu, or by emptying the *Search* field and clicking the *Search* button again.

5.8 Sorting the List of Reports

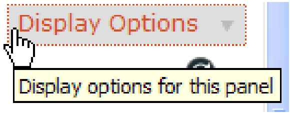
1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position. When the sort is descending, the sort indicator is upside down.

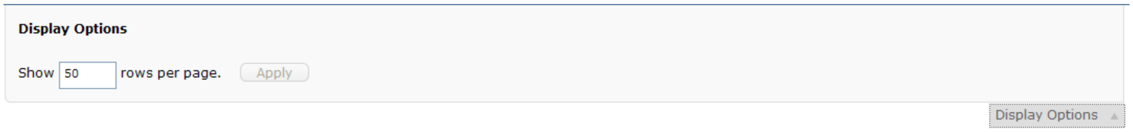
5.9 Defining the Repository Display Options

You can control how many rows are displayed on the Repository page.

1 Click *Display Options* in the upper right corner of the page:



2 Type the number of rows to display in *Show rows per page* field:


Display Options

Show 50 rows per page.

The number you enter must be greater than zero. This preference is saved across sessions, and applies to all users. It affects both the Repository and Reports lists.

3 Click *Apply*.

4 To hide the Display Options control, click *Display Options* again.

5.10 Refreshing the Report Definition List

1 Click the Refresh icon in the upper right corner of the page.

6 Using the Import Tool

This section provides instructions on using the Import page in the Identity Reporting Module.

- Section 6.1, "Using the Import Page to Import Report Definitions," on page 127
- Section 6.2, "Automatically Importing Report Definitions," on page 130

6.1 Using the Import Page to Import Report Definitions

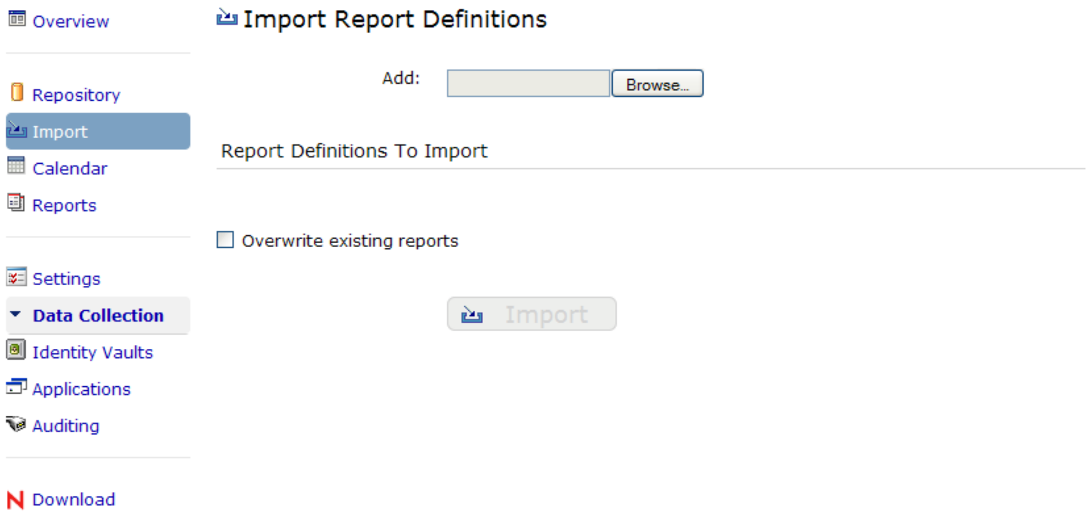
The Import page lets you import report definitions into the Identity Reporting Module. After the reports have been imported, these definitions are available for use throughout the reporting module. You can add scheduled runs for the imported definitions and make changes to the settings associated with the report definitions, such as the criteria, default notifications, and configuration. You can also add scheduled runs for the imported report definitions, or use the imported report to create a new report definition.

If you make changes to the Template report, you need to restart the server after importing the new definition. If you don't restart the server, your changes are not visible in the reporting module.

The Import Report Definitions page allows you to import a single report definition (in an RPZ file) or an archive that contains multiple report definitions (in an SPZ file). You can include multiple RPZ and SPZ files in a single import procedure.

To import a report definition:

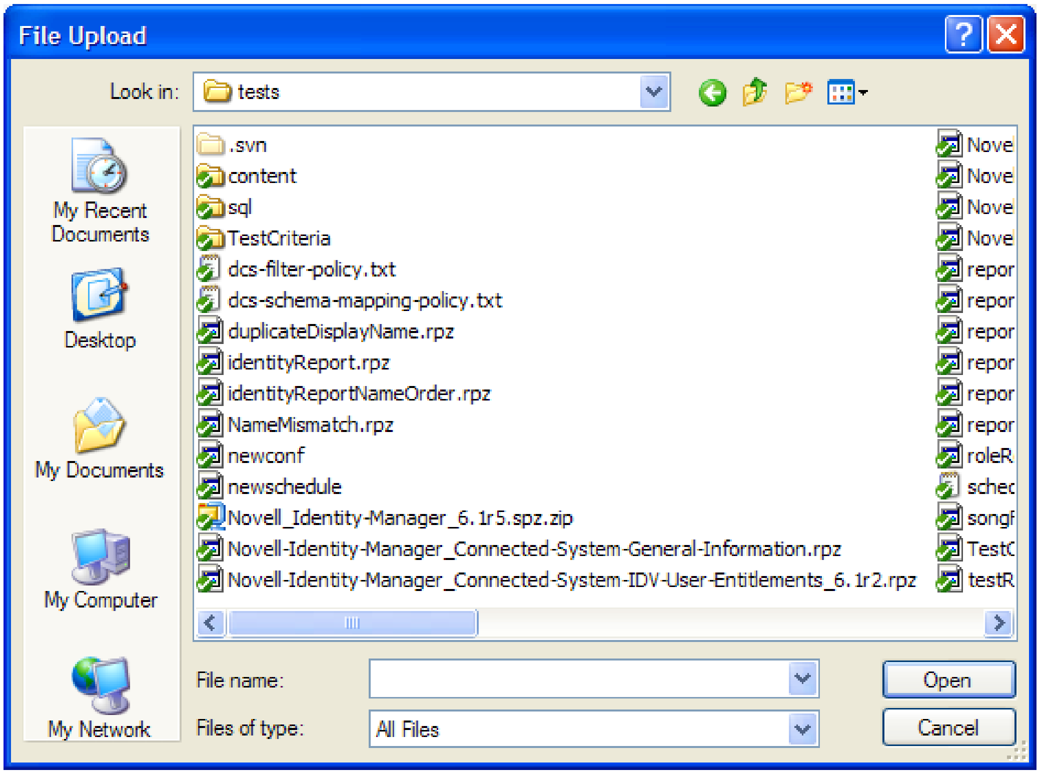
1 Click *Import* in the left navigation menu.



2 Select the files you want to include in the import procedure:

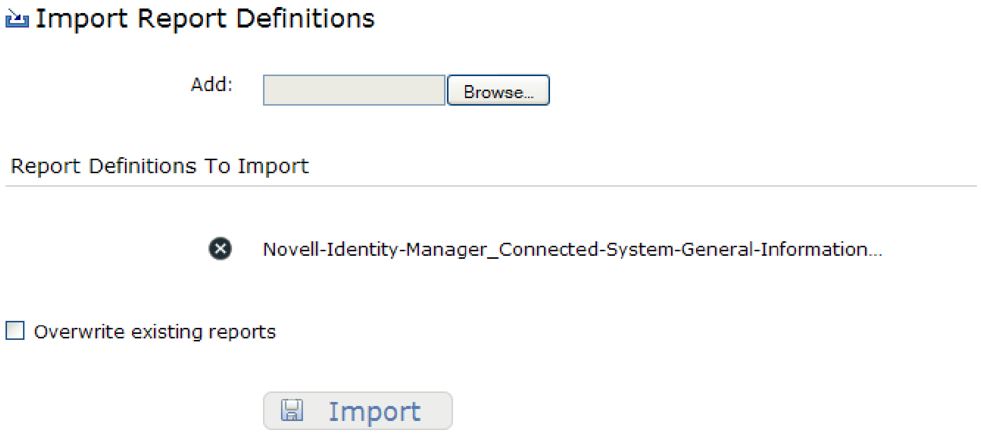
2a For each file you want to include, click the *Browse* button to the right of the *Add* control.

2b Navigate to the file and select it.



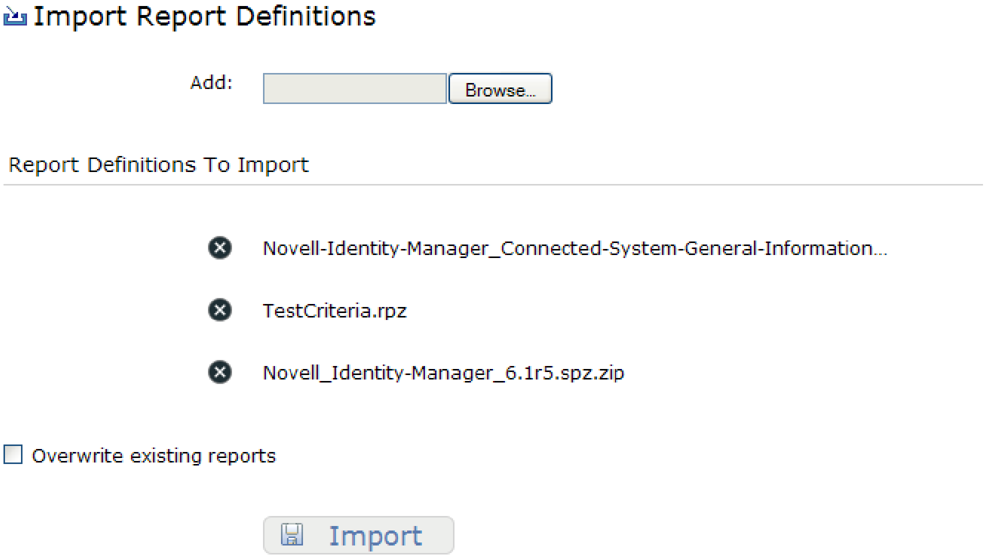
2c Click *Open*.

The page shows the file you added in the Report Definitions To Import section of the page.


Import Report Definitions
Add:
Browse...
Report Definitions To Import
Novell-Identity-Manager_Connected-System-General-Information...
☐ Overwrite existing reports
Import

2d Repeat Step 2a through Step 2c to include additional files.

3 When you have finished adding the files, review the list of files shown in the Report Definitions To Import section of the page:



Import Report Definitions

Add: [ ] Browse...

Report Definitions To Import

⊗ Novell-Identity-Manager_Connected-System-General-Information...

⊗ TestCriteria.rpz

⊗ Novell_Identity-Manager_6.1r5.spz.zip

□ Overwrite existing reports

Import

To remove a file from the import procedure, click the delete icon to the left of the filename:

⊗

4 Specify whether you want to overwrite the contents of any existing report definitions with the same names as those being imported by selecting or deselecting the *Overwrite existing reports* check box.

□ Overwrite existing reports

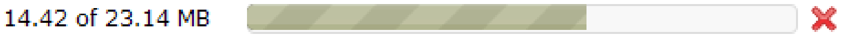
When this option is selected, the import operation overwrites the contents of existing report definitions that have the same names as those imported. However, some of the fields associated with an existing report definition are retained:

- The e-mail addresses to send the report to
- Comments added to the report definition
- Default report format (CSV or PDF)
- Categories defined for the report definition

All other settings associated with the report definition are overwritten by the imported values.

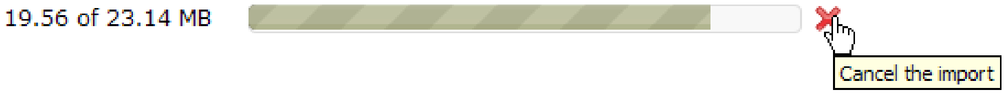
5 When you are ready, click *Import* to begin the import procedure.

The Import Report Definitions page displays a progress bar:


14.42 of 23.14 MB

The progress bar is updated every four seconds to show the status of the import procedure.

6 If you want to cancel the import procedure, click the *Cancel the import* icon to the right of the progress bar.


19.56 of 23.14 MB

If you cancel the import procedure, none of the report definitions you selected are imported.

After importing one or more report definitions, you can see the reports and make changes to them on the Repository page.

6.2 Automatically Importing Report Definitions

The Identity Reporting Module includes an automatic import facility, which provides an alternative method for importing report definitions. This facility automatically imports `.rpz` and `.spz` files into the reporting module at startup and at regular intervals after startup.

To import report definitions automatically, you need to place your reports into the imports directory, which is defined as `\reportContent\plugins`. The physical location of this directory is based on the system configuration value specified for the *Location of the Reports* setting. For example, suppose you configure your system to use this file system directory:

```
C:\Documents and Settings\John Smith
```

In this case, the import facility checks for `.rpz` and `.spz` files in the following location:

```
C:\Documents and Settings\John Smith\reportContent\plugins
```

The steps performed by the automatic import facility are outlined below:

1. At startup and every 60 seconds from then on, the reporting module checks to see if there are any `.rpz` or `.spz` files in the imports directory (as described above).
2. If any files are detected, these files are moved to a temporary location and processed one by one. Internally, the import facility sets the import override flag to On, which causes existing files with the same names to be overwritten.
3. The results of each import operation are logged through Novell Audit logging.

7 Using the Calendar Page

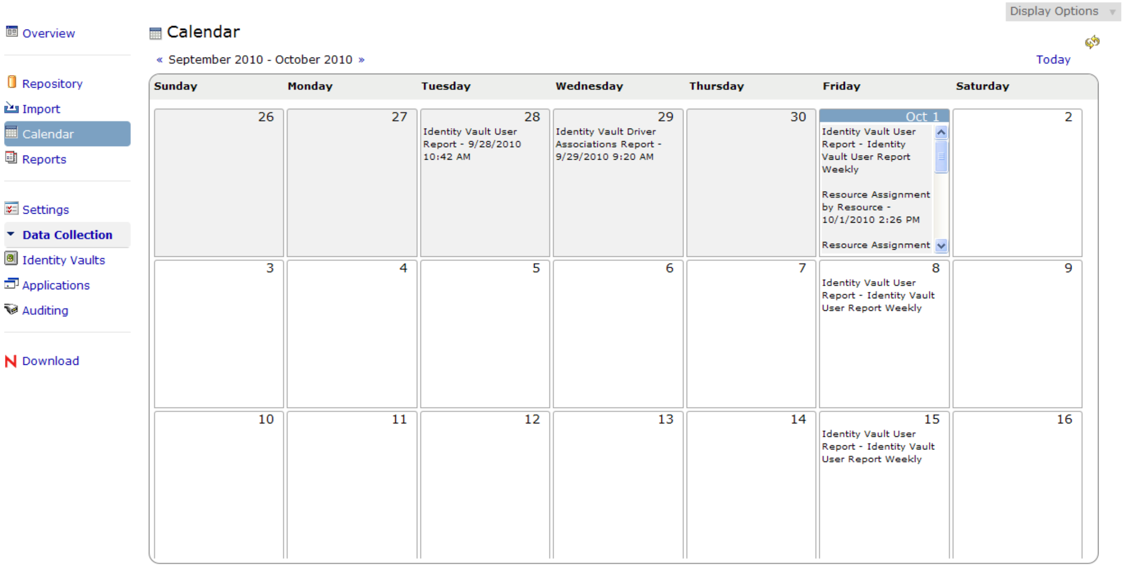
This section provides instructions on using the Calendar page.

7.1 Viewing the Calendar

This section provides instructions for viewing the calendar.

7.1.1 Displaying the Calendar Page

1 Click *Calendar* in the left navigation menu.



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
26	27	28 Identity Vault User Report - 9/28/2010 10:42 AM	29 Identity Vault Driver Associations Report - 9/29/2010 9:20 AM	30	Oct 1 Identity Vault User Report - Identity Vault User Report Weekly Resource Assignment by Resource - 10/1/2010 2:26 PM Resource Assignment	2
3	4	5	6	7	8 Identity Vault User Report - Identity Vault User Report Weekly	9
10	11	12	13	14	15 Identity Vault User Report - Identity Vault User Report Weekly	16

The Calendar page shows scheduled reports, as well as reports that have been initiated with the *Run Now* button. In addition, it shows finished reports, reports that are still in progress, and reports that failed during execution. Finished reports, reports that are still in progress, and failed reports are shown with a gray background, and reports that have not been executed yet appear with a white background. All days that have already passed are shown with a gray background.

The Calendar page presents a continuous view of the calendar, rather than a simple month-by-month view. This means that the data is not separated based on calendar months. Instead, it is presented in chunks of several weeks at a time, where each row corresponds to a week. You can adjust the number of weeks displayed by setting the *Calendar Options* for the page.

The Calendar page shows scheduled runs in the user's time zone, not the server's time zone. However, scheduled runs are executed according to the server's time zone, and the time stamp on an executed report reflects the time on the server at the time of the run.

The scroll bar for the browser lets you scroll within the current view, but does not move forward to show additional weeks in the calendar.

7.1.2 Scrolling within the Calendar Display

To include an additional row (move forward one week) in the calendar view:

1. Press the Down-arrow key.

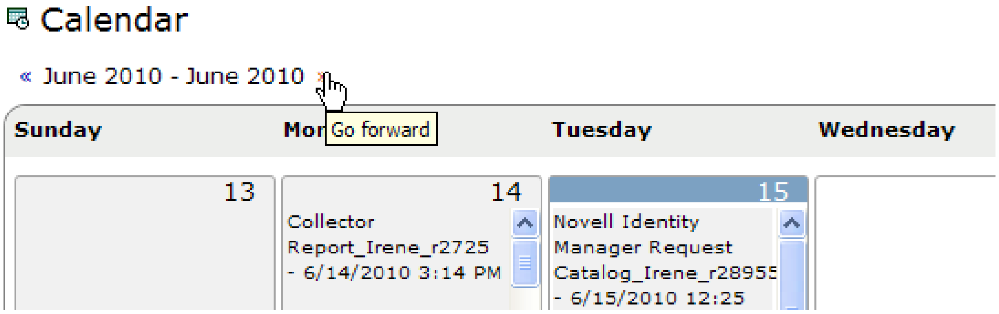
To remove a row (go back one week) in the calendar view:

1. Press the Up-arrow key.

To scroll down to the next set of weeks in the calendar view:

1. Press Ctrl+Down-arrow.

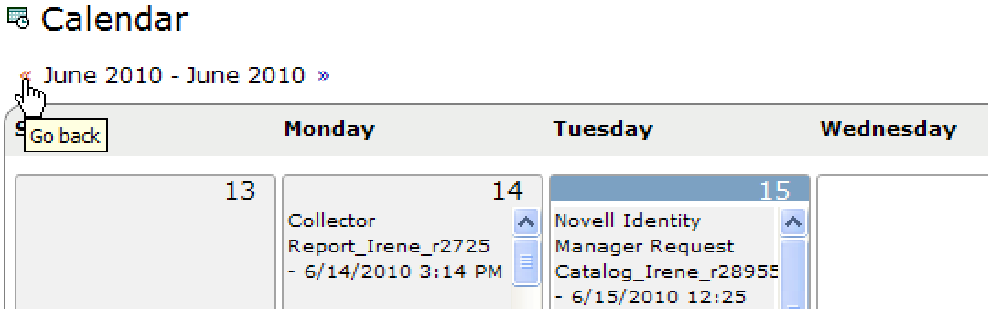
   You can also scroll down clicking the *Go forward* icon:


Calendar
« June 2010 - June 2010 »
Go forward
Sunday
Mon
Tuesday
Wednesday
13
14
Collector Report_Irene_r2725 - 6/14/2010 3:14 PM
15
Novell Identity Manager Request Catalog_Irene_r28955 - 6/15/2010 12:25

Alternatively, you can use the mouse wheel to scroll weeks in the calendar view.

To scroll up to the next set of weeks in the calendar view:

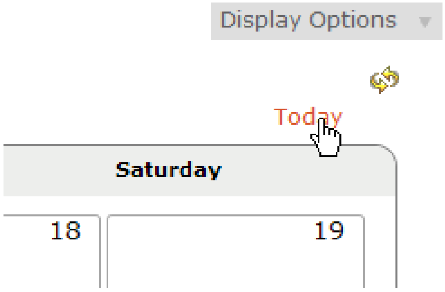
1 Press Ctrl+Up-arrow or click the *Go back* icon:


Calendar
« June 2010 - June 2010 »
Go back
Monday
Tuesday
Wednesday
13
14
Collector Report_Irene_r2725 - 6/14/2010 3:14 PM
15
Novell Identity Manager Request Catalog_Irene_r28955 - 6/15/2010 12:25

7.1.3 Viewing the Schedule for Today

When you first display the Calendar page, today's report runs are shown in the display. If you scroll away from today's schedule, you might need to return to it later.

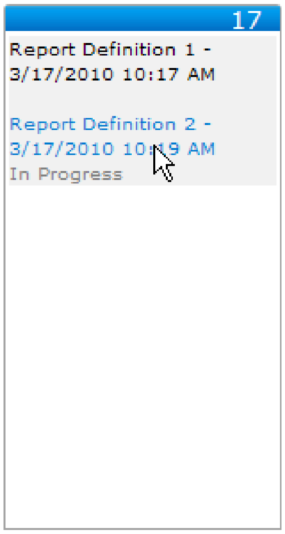
1 Click the *Today* button:



7.2 Checking the Status of a Schedule Instance

To check the status of a particular schedule instance in the calendar:

1 Mouse over the schedule name:



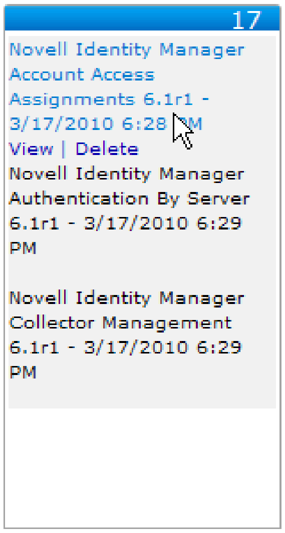
17

Report Definition 1 -
3/17/2010 10:17 AM

Report Definition 2 -
3/17/2010 10:19 AM
In Progress

If the schedule instance is still running, the Calendar shows *In Progress* under the schedule name, as shown above.

If the schedule instance has completed processing, the *View* and *Delete* links appear under the schedule name:



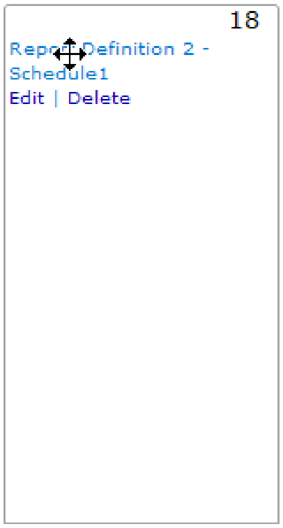
17

Novell Identity Manager Account Access Assignments 6.1r1 -
3/17/2010 6:28 PM
View | Delete

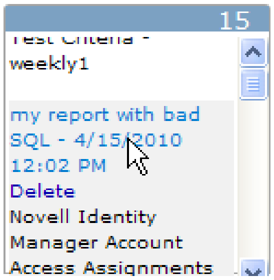
Novell Identity Manager Authentication By Server 6.1r1 - 3/17/2010 6:29 PM

Novell Identity Manager Collector Management 6.1r1 - 3/17/2010 6:29 PM

If the schedule instance has not run yet because it is scheduled for sometime in the future, the *Edit* and *Delete* links appear under the schedule name:



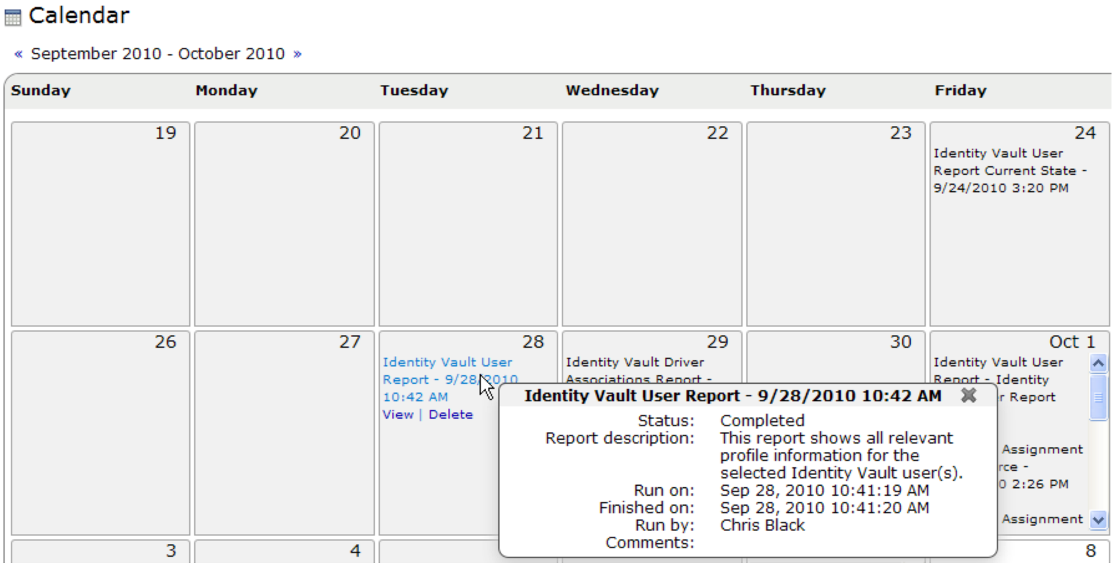
If the report failed during execution, only the *Delete* link appears under the schedule name:


15
Test Criteria - weekly1
my report with bad SQL - 4/15/2010 12:02 PM
Delete
Novell Identity Manager Account Access Assignments

7.3 Viewing the Summary Information for a Schedule Instance

To view the summary information for a particular schedule instance in the calendar:

1 Click the name of the schedule instance:


Calendar
« September 2010 - October 2010 »
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
19
20
21
22
23
24
Identity Vault User Report Current State - 9/24/2010 3:20 PM
26
27
28
Identity Vault User Report - 9/28/2010 10:42 AM
View | Delete
29
Identity Vault Driver Associations Report -
30
Oct 1
Identity Vault User Report - Identity
r Report
Assignment
rce -
0 2:26 PM
Assignment
3
4
8

Identity Vault User Report - 9/28/2010 10:42 AM

Status:	Completed
Report description:	This report shows all relevant profile information for the selected Identity Vault user(s).
Run on:	Sep 28, 2010 10:41:19 AM
Finished on:	Sep 28, 2010 10:41:20 AM
Run by:	Chris Black
Comments:	

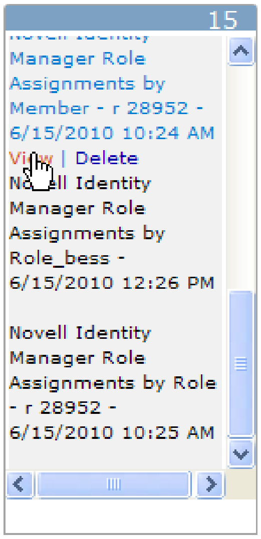
The Calendar page displays a pop-up window showing the description, status, and comments for the report, as well as the date and time on which it was run, and the name of the user who ran the report.

If the report failed during execution, the pop-up window indicates this in the status and also provides the reason for the failure.

7.4 Viewing a Completed Report

To view a generated report:

1 Click *View* under the schedule name:



15

Novell Identity
Manager Role
Assignments by
Member - r 28952 -
6/15/2010 10:24 AM
View | Delete

Novell Identity
Manager Role
Assignments by
Role_bess -
6/15/2010 12:26 PM

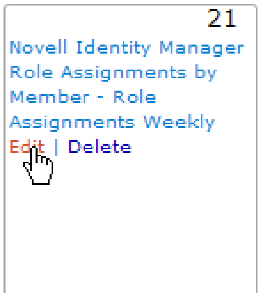
Novell Identity
Manager Role
Assignments by Role
- r 28952 -
6/15/2010 10:25 AM

When you view a report, the generated report appears in a new window. The report is shown in PDF or CSV format, depending on how the report was defined.

7.5 Editing a Schedule Instance

To edit a schedule instance for a report that has not been run yet:

1 Click *Edit* under the schedule name:



21

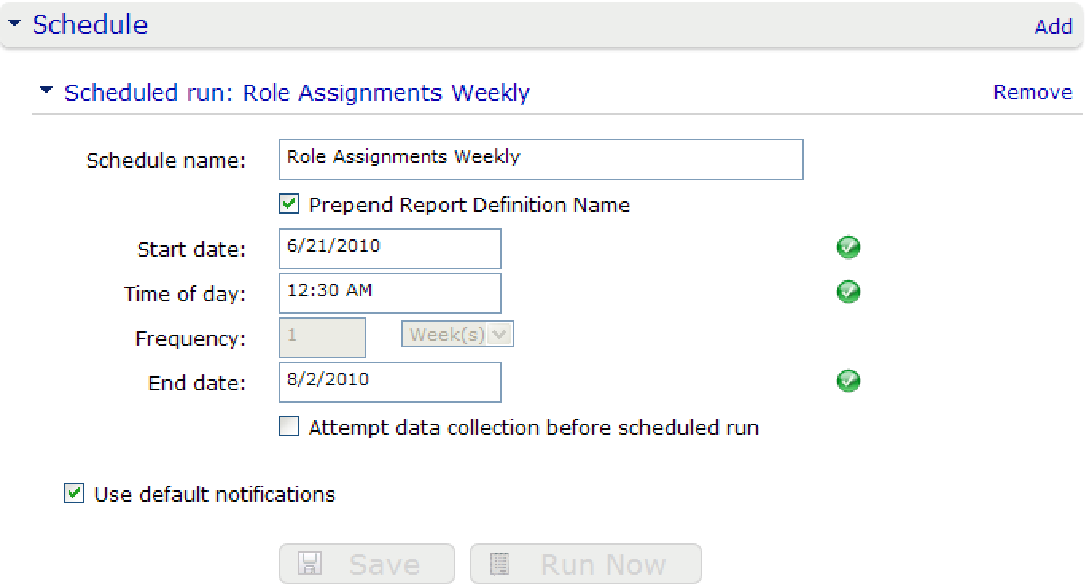
Novell Identity Manager
Role Assignments by
Member - Role
Assignments Weekly
Edit | Delete

You can also click the report schedule.

The reporting module displays a page that lets you edit the report definition and schedule. The page opens to the schedule instance you selected in the Calendar page. However, you can work on a different schedule instance, or create a new one from the editing page. In addition, you can make modifications to the report definition.

The report definition has a one-to-many relationship with schedules, which means that a report definition can have one or more schedules, but a schedule can only be associated with a single report definition.

2 To edit the settings for the schedule, scroll down to the *Schedule* section of the page and open the section for this scheduled run:



Schedule

Scheduled run: Role Assignments Weekly

Schedule name: Role Assignments Weekly

☑ Prepend Report Definition Name

Start date: 6/21/2010

Time of day: 12:30 AM

Frequency: 1 Week(s)

End date: 8/2/2010

□ Attempt data collection before scheduled run

☑ Use default notifications

3 Make changes as necessary to the scheduled run.

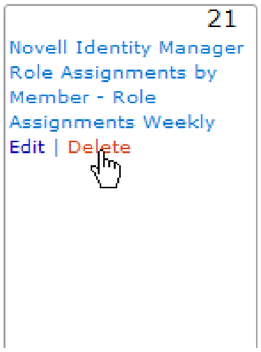
Schedule Property	Description
Start date	Specifies the date in the calendar on which you want to initiate the first run of the report. This property also determines the date for all subsequent runs. You can change the start date for a schedule after it has been created, even if the calendar already includes one or more scheduled runs. If you change the start date for a schedule, all of the runs for this schedule shift to the new date.
Time of day	Specifies the approximate time of day for each report run. The time of day is based on the clock on the server where the report is executed. The actual execution time depends on server activity. The run time specified for each schedule instance is set to the hour or the half hour (for example, 1:00 AM or 1:30 PM). You can change the time of day for a schedule after it has been created. If you change the time of day, all of the runs for this schedule execute at the new time.
Frequency	Specifies the repeat interval (a number that specifies how often the report will run) and the time period for report runs: (Month(s), Week(s), or Day(s). You cannot modify the frequency for a schedule after the schedule has been created.
End date	Specifies the date in the calendar after which no more runs should occur. Note that the last report run may not actually occur on this date. For example, if you choose October 15 as the start date, and specify a repeat interval of two weeks and an end date of November 1, the report will be run on October 15 and October 29. In this case, October 29 is the last run. You can change the end date for a schedule after it has been created.
Use default notifications	Specifies the e-mail settings associated with the schedule instance.

4 Click *Save*.

7.6 Deleting a Schedule Instance

To delete a particular scheduled instance:

1 Mouse over the scheduled instance and click *Delete*.



21

Novell Identity Manager Role Assignments by Member - Role Assignments Weekly

If you delete the first run in a schedule, the Start date for the schedule is changed to the next upcoming run date. If you delete the last run, the End date for the schedule is not modified.

7.7 Moving a Single Schedule Instance

The Calendar page allows you to move a single schedule instance by dragging and dropping the item from one date to another within the calendar. However, when you move a single schedule instance, the Calendar page automatically creates a new schedule with a new name and places the moved schedule instance on the new date that you selected as a the target for the move operation.

After you have moved a schedule instance, this run is effectively deleted from the original schedule definition, and is now added to the new schedule definition. All of the text-based attributes from the original schedule instance are copied to the new schedule instance.

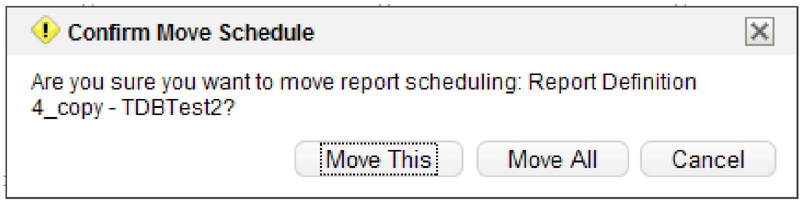
The name you specify for the new schedule need not be unique across all of the report definitions within the reporting module. However, it does need to be unique within the list of schedules for the report definition.

You cannot move a schedule instance into the past (before the current date and time) or to a day that already has a run scheduled for the same report definition.

To move a single schedule instance to a new date:

1 Select the schedule instance you want to move and drag it to the desired date.

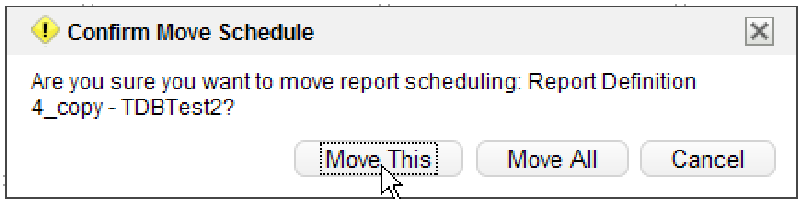
The *Calendar* page displays the Confirm Move Schedule dialog box:



Confirm Move Schedule

Are you sure you want to move report scheduling: Report Definition 4_copy - TDBTest2?

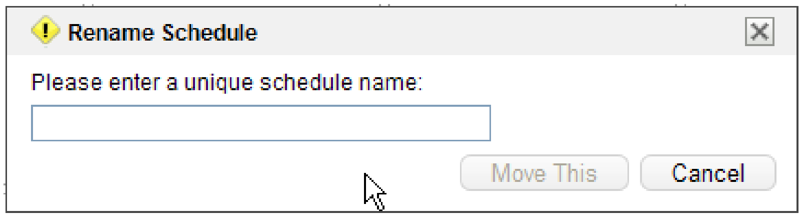
2 Click *Move This*:



Confirm Move Schedule

Are you sure you want to move report scheduling: Report Definition 4_copy - TDBTest2?

The Calendar page displays the Rename Schedule dialog box:

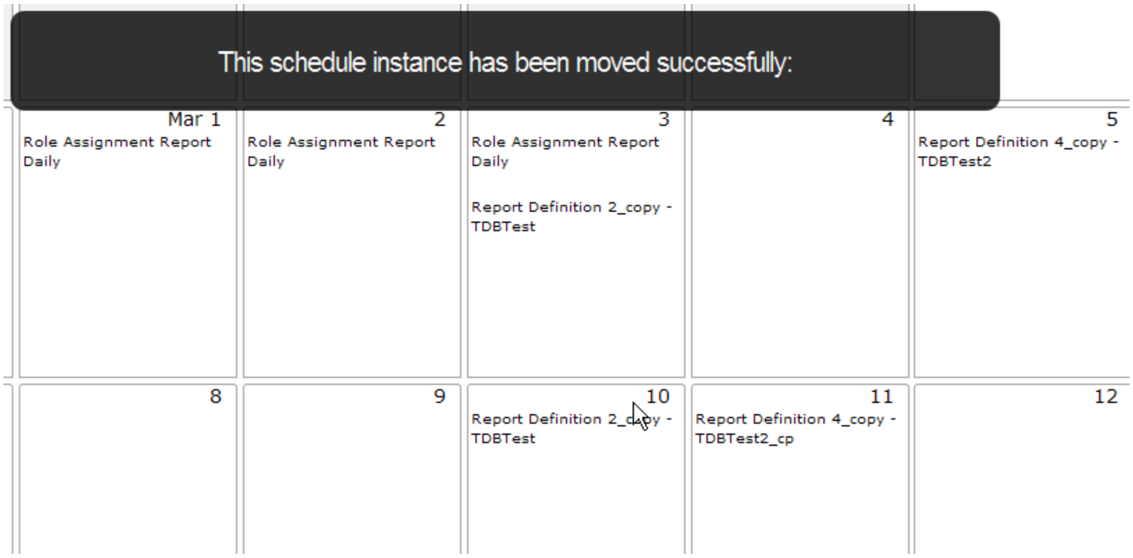


Rename Schedule

Please enter a unique schedule name:

3 Specify a name for the new schedule and click *Move This*.

The Calendar page creates the new schedule, moves the scheduled instance, and displays a confirmation message.



This schedule instance has been moved successfully:

Mar 1
Role Assignment Report Daily
2
Role Assignment Report Daily
3
Role Assignment Report Daily
Report Definition 2_copy - TDBTest
4
5
Report Definition 4_copy - TDBTest2
8
9
10
Report Definition 2_copy - TDBTest
11
Report Definition 4_copy - TDBTest2_cp
12

7.8 Moving All Schedule Instances

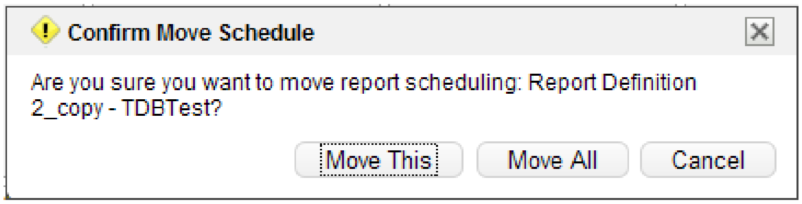
The Calendar page also allows you to move all of the scheduled runs for a schedule simply by dragging and dropping a particular run within the schedule from one date to another within the calendar. When you move all schedule instances for a particular schedule, the Calendar page retains the original repeat pattern specified in the *Frequency* field, but updates the start date to reflect the new date for execution of the report.

The target date for the move need not be within the original start and end period dates specified for the schedule. If you move outside the original range of the schedule, the schedule start and end dates change accordingly.

To move all of the scheduled runs for a schedule:

1 Select the schedule instance you want to move and drag it to the desired date.

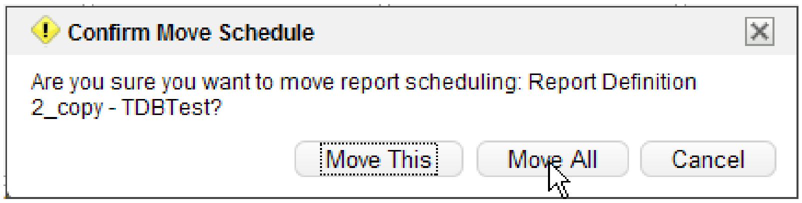
The Calendar page displays the Confirm Move Schedule dialog box:



Confirm Move Schedule

Are you sure you want to move report scheduling: Report Definition 2_copy - TDBTest?

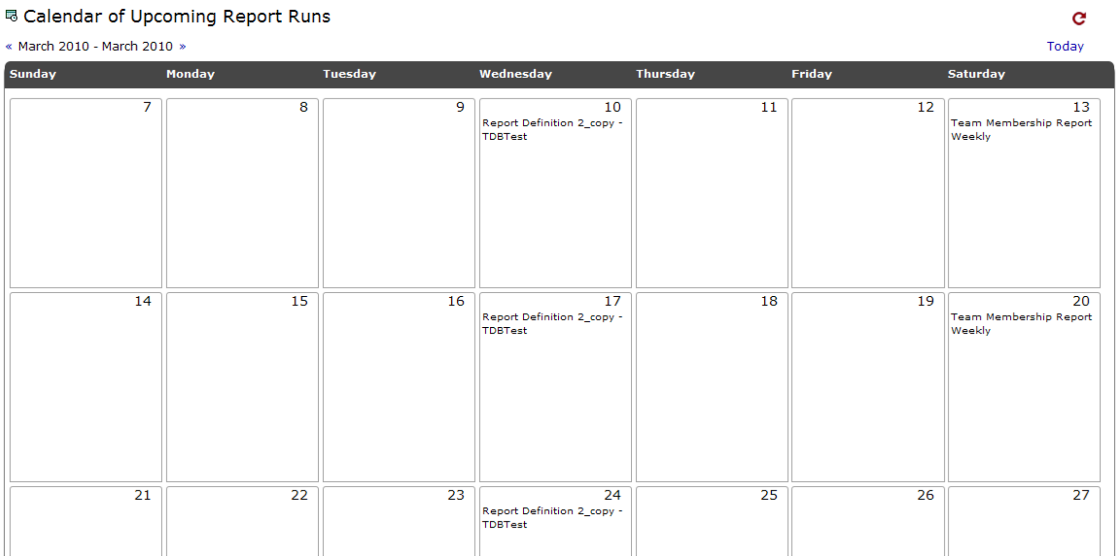
2 Click *Move All*.



Confirm Move Schedule

Are you sure you want to move report scheduling: Report Definition 2_copy - TDBTest?

The Calendar page shifts all of the scheduled runs to align with the new run date:



Calendar of Upcoming Report Runs

« March 2010 - March 2010 »

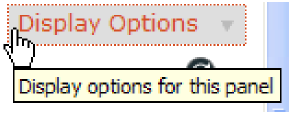
Today

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
7	8	9	10 Report Definition 2_copy - TDBTest	11	12	13 Team Membership Report Weekly
14	15	16	17 Report Definition 2_copy - TDBTest	18	19	20 Team Membership Report Weekly
21	22	23	24 Report Definition 2_copy - TDBTest	25	26	27

7.9 Defining the Calendar Display Options

You can control how many weeks are shown on the Calendar page.

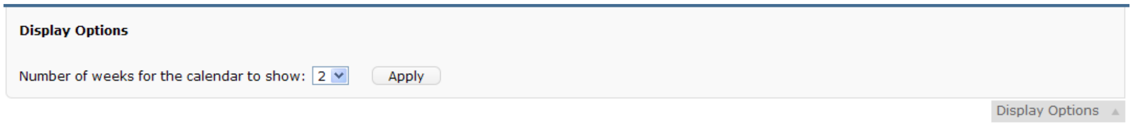
1 Click *Display Options* in the upper right corner of the page:



Display Options

Display options for this panel

2 Select the number of weeks to display in the *Number of weeks for the calendar to show* field:



Display Options

Number of weeks for the calendar to show: 2

You might want to set the number to a low number, such as one, if you want to be able to zoom in on the reports scheduled for a particular day.

The number you enter must be greater than zero and less than five. If you attempt to type a number outside this range, an error message is displayed. This preference is saved across sessions.

3 Click *Apply*.

4 To hide the Display Options control, click *Display Options* again.

7.10 Refreshing the Display

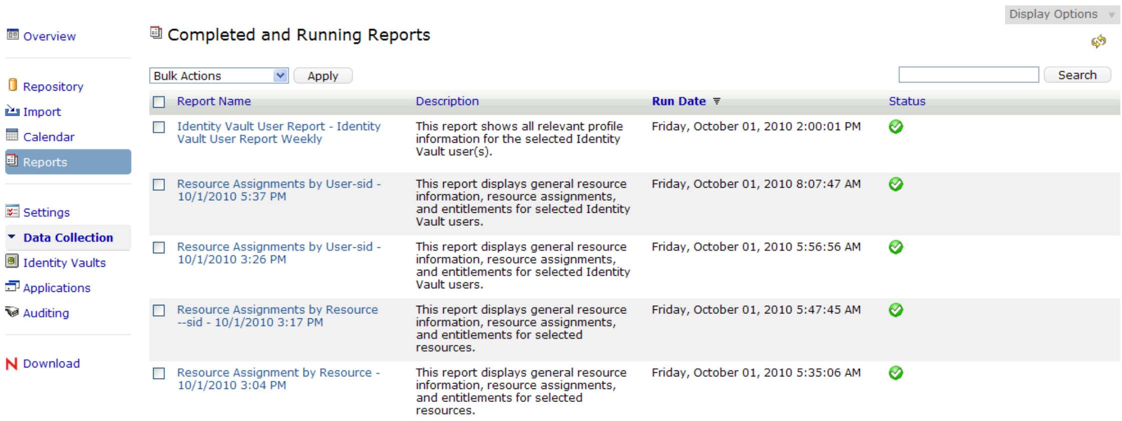
1 Click the *Refresh* icon in the upper right corner of the page.

8 Using the Completed and Running Reports Page

This section provides instructions for using the Completed and Running Reports page in the Identity Reporting Module.

8.1 Viewing the List of Completed and Running Reports

1 Click *Reports* in the left navigation menu.



Completed and Running Reports

□	Report Name	Description	Run Date	Status
□	Identity Vault User Report - Identity Vault User Report Weekly	This report shows all relevant profile information for the selected Identity Vault user(s).	Friday, October 01, 2010 2:00:01 PM	✓
□	Resource Assignments by User-sid - 10/1/2010 5:37 PM	This report displays general resource information, resource assignments, and entitlements for selected Identity Vault users.	Friday, October 01, 2010 8:07:47 AM	✓
□	Resource Assignments by User-sid - 10/1/2010 3:26 PM	This report displays general resource information, resource assignments, and entitlements for selected Identity Vault users.	Friday, October 01, 2010 5:56:56 AM	✓
□	Resource Assignments by Resource --sid - 10/1/2010 3:17 PM	This report displays general resource information, resource assignments, and entitlements for selected resources.	Friday, October 01, 2010 5:47:45 AM	✓
□	Resource Assignment by Resource - 10/1/2010 3:04 PM	This report displays general resource information, resource assignments, and entitlements for selected resources.	Friday, October 01, 2010 5:35:06 AM	✓

The Completed And Running Reports page shows all reports that have completed processing, as well as reports that are still in progress or have failed during execution. The list of reports includes reports that were scheduled, as well as reports that were initiated with the *Run Now* button. For each report listed, the page shows the report name, description, run date, and status.

Reports that have completed show this status icon:

✓

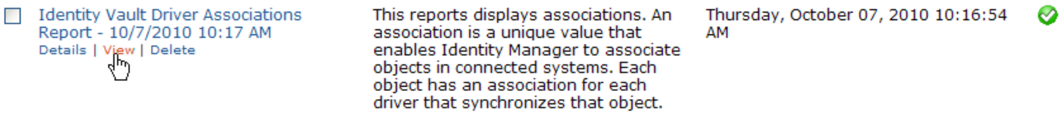
Reports that are still running show this status icon:

Reports that have failed during execution show this status icon:

If a report is run multiple times very quickly (each run is within a fraction of a second of the other runs), the time format shows one or more periods after AM or PM. For example, you might see “PM.” or “PM..” after the time the report was run.

8.2 Viewing a Completed Report

1 Click the *View* link below the report you want to display:

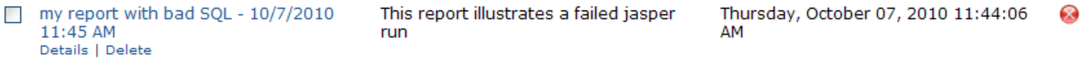


□	Identity Vault Driver Associations Report - 10/7/2010 10:17 AM Details | View | Delete	This reports displays associations. An association is a unique value that enables Identity Manager to associate objects in connected systems. Each object has an association for each driver that synchronizes that object.	Thursday, October 07, 2010 10:16:54 AM	✓

When you view a report, the generated report appears in a new window. The report is shown in PDF or CSV format, depending on how the report was defined.

IMPORTANT: Please do not try to copy and send links to files within the reporting module, because this action might potentially expose your login information.

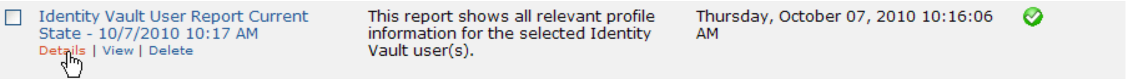
The *View* link is not available for reports that are still in progress or have failed:



□	my report with bad SQL - 10/7/2010 11:45 AM Details | Delete	This report illustrates a failed jasper run	Thursday, October 07, 2010 11:44:06 AM	⊗

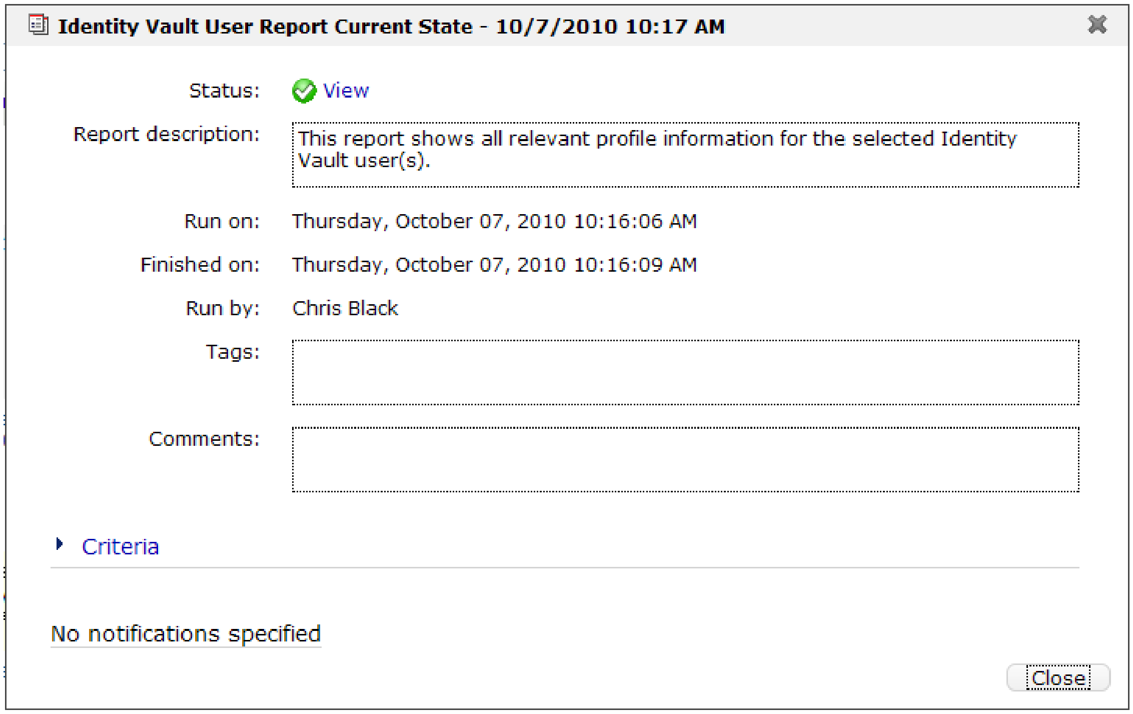
8.3 Viewing the Details for a Report

1 Click the *Details* link below the report for which you want to see the details:



□	Identity Vault User Report Current State - 10/7/2010 10:17 AM Details | View | Delete	This report shows all relevant profile information for the selected Identity Vault user(s).	Thursday, October 07, 2010 10:16:06 AM	✓

The details are displayed in a pop-up window:



Identity Vault User Report Current State - 10/7/2010 10:17 AM

Status: ✓ View

Report description: This report shows all relevant profile information for the selected Identity Vault user(s).

Run on: Thursday, October 07, 2010 10:16:06 AM

Finished on: Thursday, October 07, 2010 10:16:09 AM

Run by: Chris Black

Tags:

Comments:

If the report definition includes one or more parameters, a *Criteria* section is added to the page that shows the parameters.

The fields shown in the pop-up window are not editable, because the report has already been submitted to be run.

The Run By user is the logged-in user who creates a schedule or clicks *Run Now*. If the user `cblack` creates a schedule, and then `mmackenzie` logs in and modifies the schedule, the Run By user is still the original creator, `cblack`. If `mmackenzie` moves the item by clicking *Move This*, thereby creating a new schedule, `mmackenzie` is the creator for the report generated by that one-off schedule.

2 If the report has completed processing, you can display the generated report from this window by clicking the *View* link next to the status icon at the top of the window:

This link is not available if the report is still in progress or has failed.

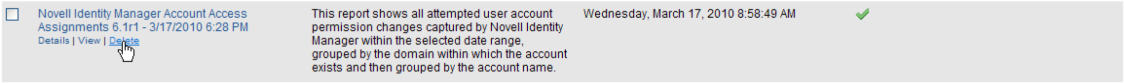
3 To return to the report list, click *Close*.

This window is non-modal, so you can continue to work outside the window while it is still open.

8.4 Deleting a Report

To delete a generated report:

1 Click the *Delete* link below the report you want to delete:



□ Novell Identity Manager Account Access Assignments 6.1r1 - 3/17/2010 6:28 PM
Details | View | Delete

This report shows all attempted user account permission changes captured by Novell Identity Manager within the selected date range, grouped by the domain within which the account exists and then grouped by the account name.

Wednesday, March 17, 2010 8:58:49 AM ✓

If you choose multiple reports by selecting the check box for each report, and then click the *Delete* link for another report in the list, the delete operation applies only to the report for which you clicked the *Delete* link.

8.5 Performing Bulk Actions

To delete several reports at once:

1. Select the check box to the left of each report definition you want to run or delete.
2. Select the operation (*Delete*) in the *Bulk Actions* drop-down list.
3. Click *Apply*.

Bulk actions apply to the current page only. If you select several items on one page, then navigate to the next page to select some additional items, a subsequent attempt to perform a bulk delete only applies to the second set of items you selected. The previous selections are retained and still appear checked if you navigate back to the first page. However, the bulk action is not performed on these items.

8.6 Searching for a Report

To search for a report definition:

1. Type a search string in the *Search* text field.

   The search facility allows you to pass in search strings for any of the following items:

Filter Value	Description
Name	Performs a contains search. The search is case insensitive, and it uses the locale of the user.
Description	Performs a contains search. The search is case insensitive, and it uses the locale of the user.
Tags	Performs an exact string search. The search is case insensitive. You need to pass in a single tag only.
Run By	Performs a search on the first name and last name of the creator of the schedule. The creator is the logged-in user who creates a schedule or clicks *Run Now*. If the user `cblack` creates a schedule, and then `mmackenzie` logs in and modifies the schedule, the Run By user is still the original creator, `cblack`. If `mmackenzie` moves the item by clicking *Move This*, thereby creating a new schedule, `mmackenzie` is the creator for the report generated by that one-off schedule.

You can enter one or more words in the *Search* field, with or without quotes:

- If you enter multiple words without quotes, the search results include reports that contain all of the words anywhere in the Name or Description, or that have all of the words as tags (that match exactly).

  For example, suppose you enter the following:

```
chris black
```

In this case, the following report definitions are in the results:

  - Reports with a Name containing the words `chris` and `black` anywhere in the string
  - Reports with a Description containing the words `chris` and `black` anywhere in the string
  - Reports with Tags having `chris` and `black` as exact tags
  - Reports with Run By having a first name or last name of `chris` and last name or first name of `black`.

- If you enter multiple words surrounded by double quotes, the search results include reports that include the entire phrase anywhere in the Name or Description, or that have a tag that matches the entire phrase.

  For example, suppose you enter the following:

  ```
  "margo mackenzie"
  ```

  In this case, the following report definitions are in the results:

  - Reports with Name containing the phrase "margo mackenzie".
  - Reports with Description containing the phrase "margo mackenzie".
  - Reports with a Tag that exactly matches "margo mackenzie".
  - Reports with Run By having "margo mackenzie" as the first name and last name or last name and first name.

2 Click *Search*.

You can clear the current search criteria and refresh the display by clicking *Reports* on the left navigation menu, or by emptying the *Search* field and clicking the *Search* button again.

8.7 Sorting the List of Reports

To sort the list of reports on the Completed and Running Reports page:

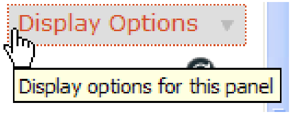
1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position. When the sort is descending, the sort indicator is upside down.

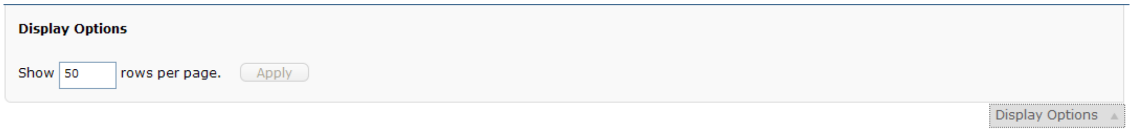
8.8 Defining the Reports Display Options

You can control how many rows are displayed on the Completed and Running Reports page.

1 Click *Display Options* in the upper right corner of the page:



2 Type the number of rows to display in *Show rows per page* field:



Display Options

Show 50 rows per page.

The number you enter must be greater than zero. This preference is saved across sessions.

3. Click *Apply*.
4. To hide the *Display Options* control, click *Display Options* again.

8.9 Refreshing the Completed Report List

1. Click the *Refresh* icon in the upper right corner of the page.

9 Configuring Settings and Data Collection

This section provides instructions on configuring settings for the Identity Reporting Module.

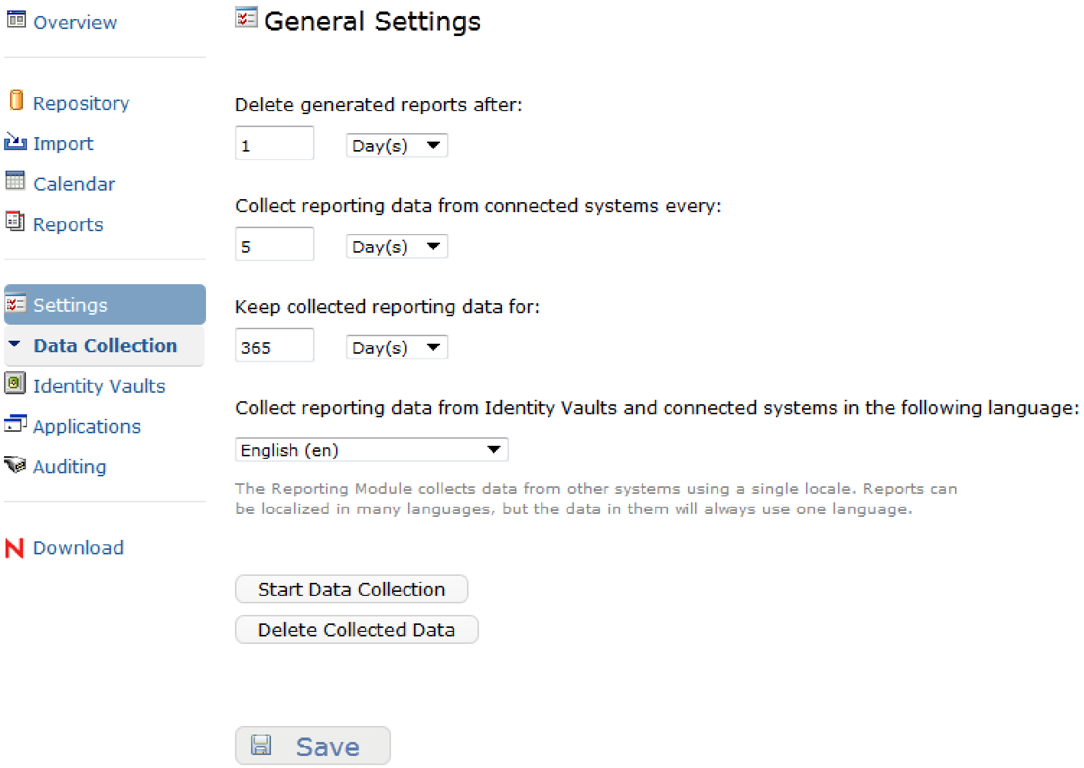
- Section 9.1, “Defining the General Settings,” on page 149
- Section 9.2, “Defining the Identity Vault Settings for Managed Systems,” on page 151
- Section 9.3, “Defining the Settings for Non-Managed Applications,” on page 153
- Section 9.4, “Defining the Auditing Configuration,” on page 157
- Section 9.5, “Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver,” on page 158

9.1 Defining the General Settings

The General Settings page allows you to define global settings that control the behavior of the Identity Reporting Module.

1 Click *Settings* in the left navigation menu.

The reporting module displays the General Settings page:



General Settings

Delete generated reports after: 1 Day(s)

Collect reporting data from connected systems every: 5 Day(s)

Keep collected reporting data for: 365 Day(s)

Collect reporting data from Identity Vaults and connected systems in the following language: English (en)

The Reporting Module collects data from other systems using a single locale. Reports can be localized in many languages, but the data in them will always use one language.

2 To define the general settings:

2a To specify how long completed reports should be retained, specify the unit of time (days, weeks, or months) and a number in the *Delete generated reports after* field.

2b To specify how often data should be collected, specify the unit of time (days, weeks, or months) and a number in the *Collect reporting data from connected systems every* field. This value defines a schedule for data collection.

2c To specify how long data should be retained, specify the unit of time (days, weeks, or months) and a number in the *Keep collected reporting data for* field.

2d To specify the preferred language that will be used for data collection, select the language in the *Collect reporting data from Identity Vaults and connected systems in the following language in* field. Generated reports will always show data in this language.

3 To save your changes, click *Save*.

4 To manage your data:

4a Click *Start Data Collection* to collect data from all defined data sources immediately.

When the reporting module executes a data collection operation, it stores all data collected in the Identity Information Warehouse. The data are stored in tables within the idm_rpt_data schema in the SIEM database. Some tables are not updated until the objects they contain are assigned to related objects. For example, the categories that are added to the DAL choice lists for roles and resources are not populated in the idmrpt_category table until they have been assigned to an object.

4b Click *Delete Collected Data* to purge historical data from the reporting database immediately.

When the reporting module executes a data purge operation, it only purges data from the history tables that is older than the retention value specified for the *Keep collected reporting data interval* setting. Any historical data that is more recent than the retention interval permits will be retained.

To determine whether the data should be retained or purged, the reporting module calculates the difference (in seconds) between the current time and the timestamp for the collected data and compares this value to the retention interval. To make the comparison, the reporting module translates the retention interval to a value in seconds. For example, if you specify 1 day as the retention interval, the reporting module compares the age of the historical data to 864000 seconds.

The *Delete Collected Data* action does not remove any of the current state data.

Archiving reporting data If you want to archive data in the reporting database, you need to use the archiving tools provided with PostgreSQL. For more information, see the PostgreSQL documentation (http://www.postgresql.org/docs/).

9.2 Defining the Identity Vault Settings for Managed Systems

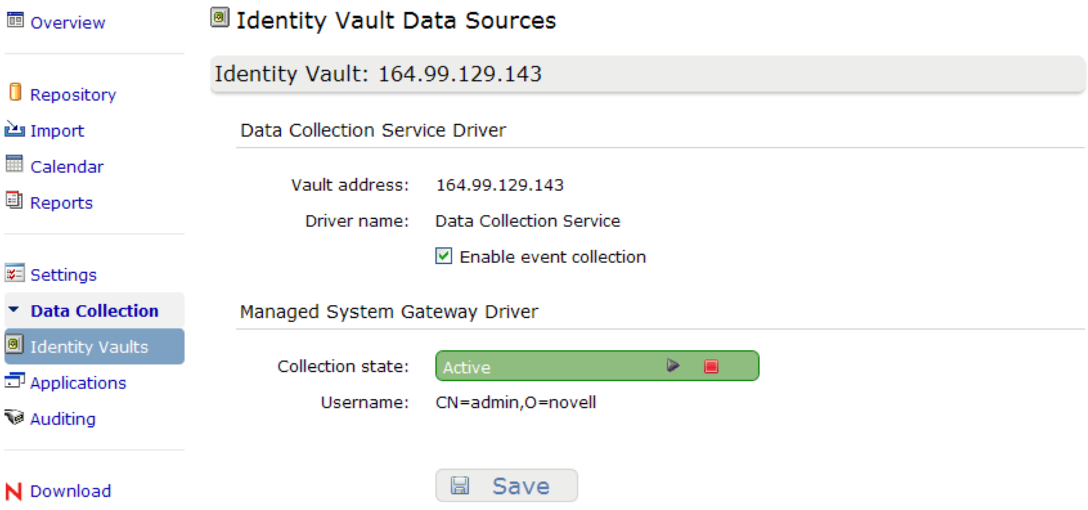
The Identity Vault Data Sources page allows you to configure settings for the managed systems (referred to as connected systems in earlier releases of Identity Manager) that you want to report on, and provide information about where the reporting module can find the Identity Vaults associated with these managed systems. The reporting module can work with data sources for one or more Identity Vaults. Each Identity Vault you work with on this page must have a separate registration for each of the following drivers:

- Identity Manager Driver for Data Collection Service
- Identity Manager Managed System Gateway Driver

To define the Identity Vault settings:

1 Click *Identity Vaults* under *Data Collection* in the left navigation menu.

The reporting module displays the Identity Vault Data Sources page:



Identity Vault Data Sources

Identity Vault: 164.99.129.143

Data Collection Service Driver

Vault address: 164.99.129.143

Driver name: Data Collection Service

☑ Enable event collection

Managed System Gateway Driver

Collection state: Active

Username: CN=admin,O=novell

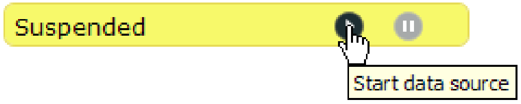
If you have more than one Identity Vault registration, you might need to scroll down to see the other Identity Vaults.

2 Provide details about each Identity Vault you want to configure, as follows:

Driver	Identity Vault Setting	Description
Data Collection Service Driver	*Vault address*	The network address of the Identity Vault. (Read only)
	Driver name	The name given to the Data Collection Service Driver. (Read only)
	Enable event collection	Controls whether the Data Collection Service Driver collects event data for this data source. Ordinarily, this check box should be enabled, unless you need to shut down event collection in order to perform a system maintenance procedure that might conflict with the collection of data.
Managed System Gateway Driver	*Collection state*	Indicates whether the data source is running or suspended. You can use the *Start data source* and *Stop data source* buttons to control the data source state. **NOTE:** If RBPM and the Identity Reporting Module are configured from an Advanced Edition .iso file, and the tree to which they are connected is a Standard Edition tree, the collection state of the Managed System Gateway driver may be active when it should not be. Because the reporting module is configured from an Advanced Edition .iso file, it tries to configure the Managed System Gateway driver, and the Managed System Gateway driver registration parameter is set to *Yes* in the Data Collection Service driver.
	Username	The user name required to authenticate to the driver. (Read only)

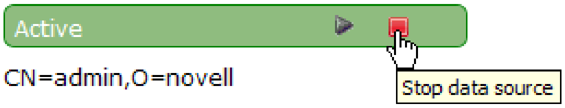
3 To save your changes, click *Save*.

4 To start the data source for the Managed System Gateway Driver, click *Start data source* to the right of *Collection state*:



The first time you activate data collection, the state is shown as *Initialized*, rather than *Suspended*.

5 To stop a running data source, click *Stop data source*:



CN=admin,O=novell

9.3 Defining the Settings for Non-Managed Applications

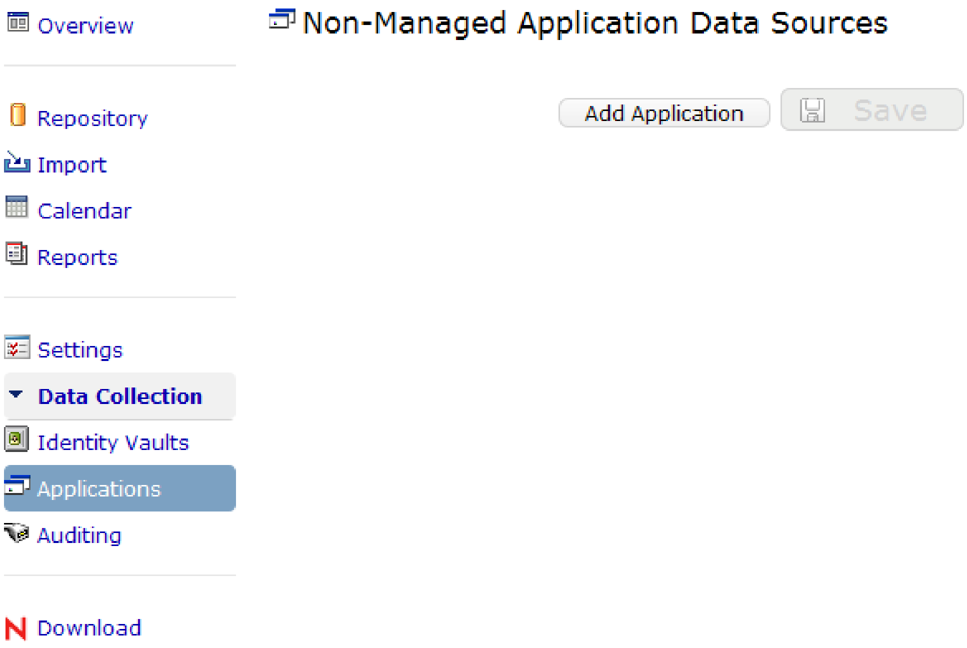
The Non-Managed Application Data Sources page allows you to specify which non-managed applications you want to report on, and provide information about where the reporting module can find these applications. A non-managed application is any application running in an enterprise that you want to include in your reports. Each application has its own set of application entitlements, which are distinct from Identity Manager entitlements. The application entitlements might include groups, roles, accounts, profiles, or other types of permissions associated with the application.

If a system is connected to the Identity Vault with an Identity Manager driver, it is referred to as a managed system. The Application Data Sources page is used to configure applications that are not connected to the Identity Vault through Identity Managed drivers. The ability to access managed systems (connected systems) is controlled through the Identity Vaults, which are configured on the Identity Vaults page.

To include information from a non-managed application in your reports, you need to implement a REST endpoint for the application and specify the context for this endpoint in the *Context* field in the *Non-Managed Application Data Sources* page. If the endpoint cannot be found, the application data will not be available for reporting.

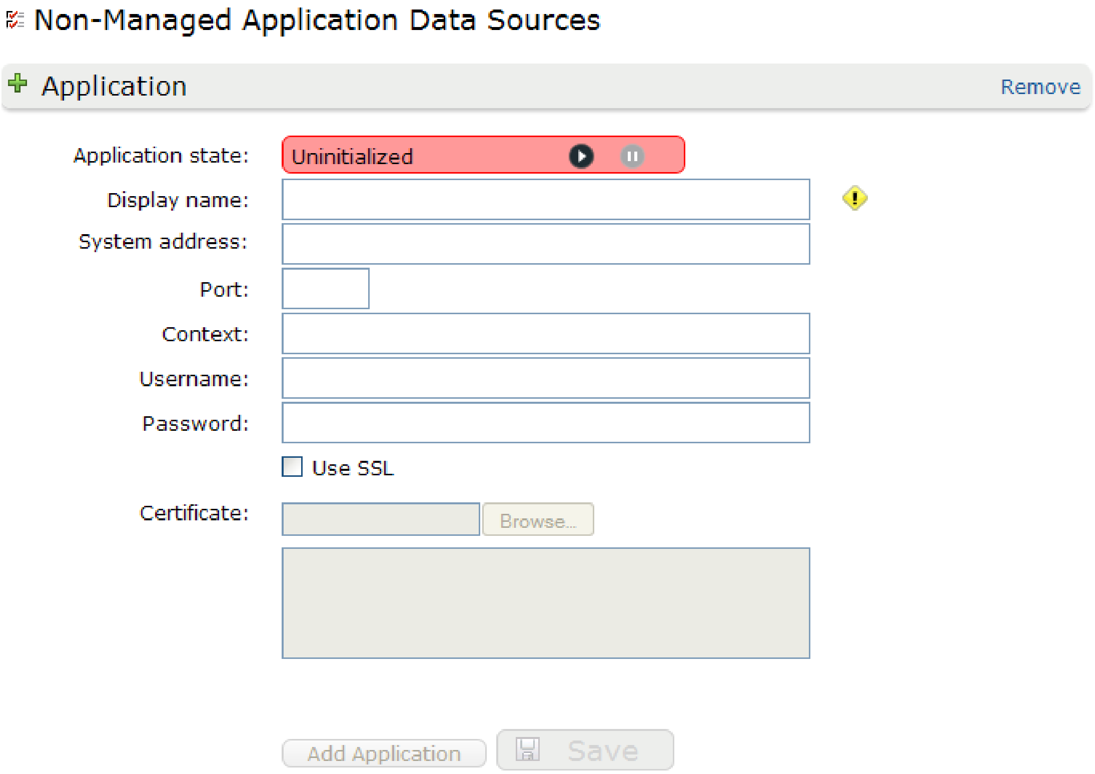
1 Click *Applications* under *Data Collection* in the left navigation menu.

The reporting module displays the Non-Managed Application Data Sources page. If any applications have been defined previously, the page shows a separate section for each application. If no applications have been defined, the page is empty:



2 To add a non-managed application, click *Add Application*.

The reporting module displays the *Application* section on the page:

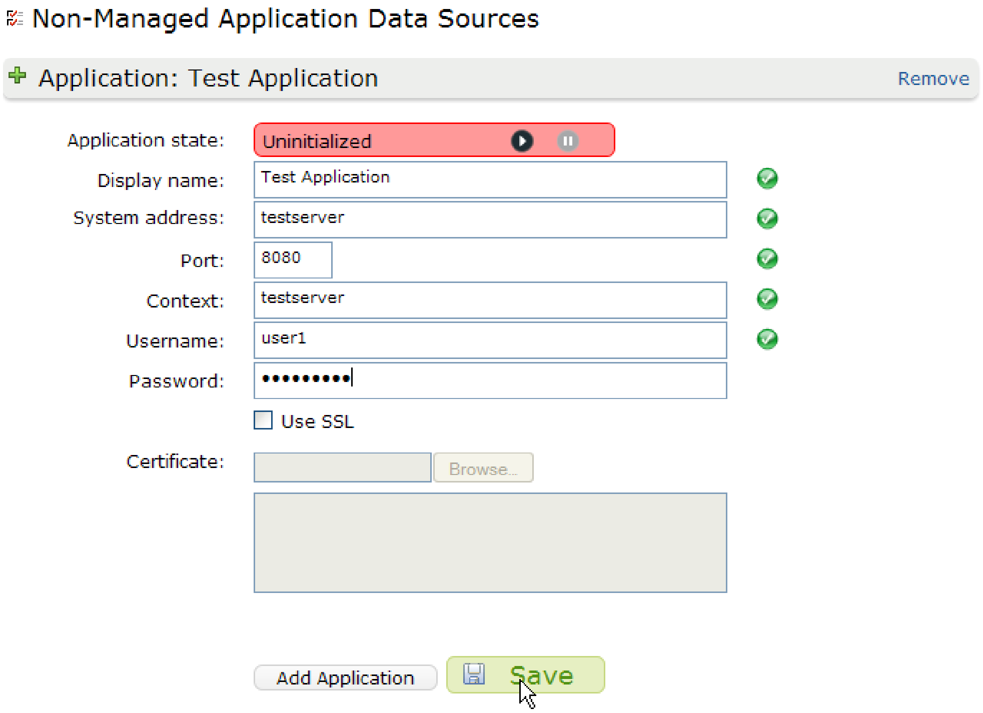


3 Provide details about the application, as follows:

Application Setting	Description
Application State	Controls whether the data source for the application is running or suspended. You can use the *Start data source* and *Stop data source* buttons to control the application state.
Display Name	A text string you use to identify the application within the reporting module.
System address	The network address of the application data source (REST endpoint).
Port	The port number on which the application data source (REST endpoint) is listening.
Context	The context for the REST endpoint associated with the application data source. To include data from an application in your reports, you need to implement a REST endpoint for the application and specify the context for this endpoint in the *Context* field. If the endpoint cannot be found, the application data is not available for reporting.
Username	The username required to authenticate to the application data source (REST endpoint).
Password	The password required to authenticate to the application data source (REST endpoint).
Use SSL	Indicates whether communication with this application data source (REST endpoint) uses a Secure Socket Layer (SSL).

Application Setting	Description
Certificate	The SSL certificate for the application data source (REST endpoint). Click *Browse* to locate the certificate file.

4 To save your changes, click *Save*.



Non-Managed Application Data Sources

Application: Test Application

Application state: Uninitialized

Display name: Test Application

System address: testserver

Port: 8080

Context: testserver

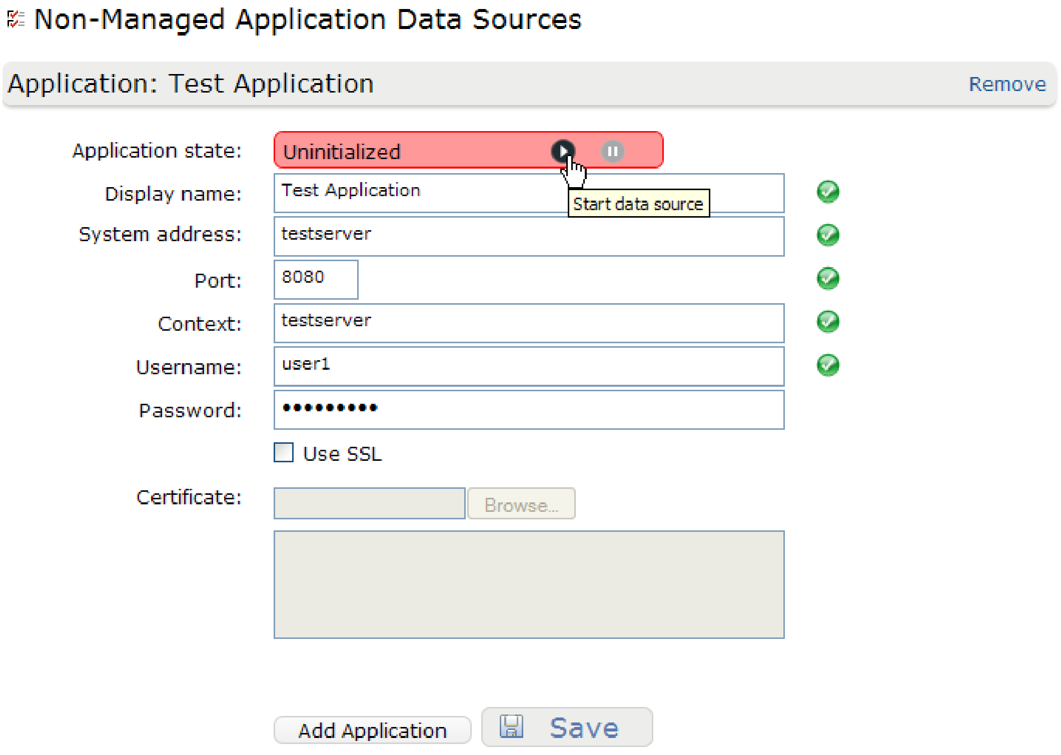
Username: user1

Password: •••••••••

☐ Use SSL

Certificate:

5 To start the data source associated with the application, click *Start data source* to the right of *Application state*.



Non-Managed Application Data Sources

Application: Test Application

Application state: Uninitialized

Display name: Test Application

System address: testserver

Port: 8080

Context: testserver

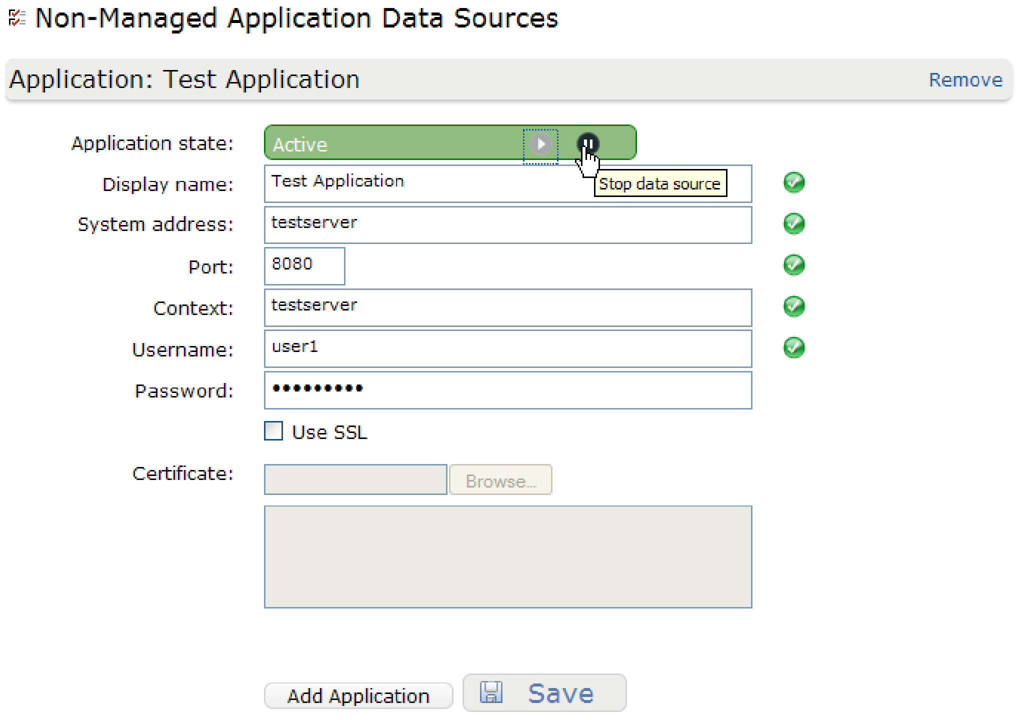
Username: user1

Password: •••••••••

□ Use SSL

Certificate:

6 To stop a data source that is already running, click *Stop data source*:



Non-Managed Application Data Sources

Application: Test Application

Application state: Active

Display name: Test Application

System address: testserver

Port: 8080

Context: testserver

Username: user1

Password: •••••••••

□ Use SSL

Certificate:

7 To remove the application you just added, click *Remove* in the upper right corner of the *Application* section of the page.

9.4 Defining the Auditing Configuration

The Event Auditing Service Settings page allows you to specify the settings for the Event Auditing Service, which captures log events associated with actions performed in various Novell tools, such as RBPM, RMA, Designer, and the Identity Reporting Module. Within the reporting module, the events captured include the import, modification, deletion, or scheduling of a report definition.

1 Click *Auditing* under *Data Collection* in the left navigation menu.

The reporting module displays the Event Auditing Service Settings page.

2 To define the port for the Syslog SSL Connector, specify the port number in the *Syslog SSL Connector port* field.

3 To define the port for the UDP connector, specify the port number in the *UDP port* field.

4 To define the port for the audit connector, specify the port number in the *Audit Connector port* field.

5 To test the connection to EAS, click *Test Connection*.

6 To forward events from Sentinel to EAS, follow the instructions presented under Section 9.5, "Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver," on page 158.

IMPORTANT: You can forward events from EAS to Sentinel or Sentinel to EAS. However, Novell recommends that you forward events from Sentinel to EAS.

7 To forward events from EAS to Sentinel:

7a Specify the network address for the Event Router in the *Address* field.

7b Specify the port number for the Event Router in the *Port* field.

7c To specify a filter for event forwarding, specify the filter in the *Filter* field.

The event forwarding filter allows you to control which events are actually forwarded to Sentinel. The *Filter* field supports the Lucene Query syntax implemented by Apache. Therefore, you can use this field to specify any query filter that would be supported by the Lucene query filter. For more information on Apache Lucene, see the Apache Lucene Web site (http://lucene.apache.org/java/docs/).

7d To start event forwarding, select the *Enable event forwarding* checkbox.

Event forwarding is the ability to forward events to a Sentinel server for further processing. In order for the Sentinel server to receive events, a Link Connector must be configured. Refer to the Sentinel documentation for more information about creating a Link Connector.

For more information, see the *Sentinel User Guide* (http://www.netiq.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bnm03ok.html).

7e To test the event forwarding configuration, click *Test Ports*.

8 To save your changes, click *Save*.

EAS stores all auditing data in the Identity Information Warehouse. Auditing events are stored in tables within the public schema in the SIEM database.

9.5 Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver

You can forward events from EAS to Sentinel or Sentinel to EAS. However, Novell recommends that you forward events from Sentinel to EAS. Details for configuring event forwarding from Sentinel to EAS are presented below.

To configure event forwarding from Sentinel to EAS, you need to configure some components on both the Sentinel and EAS servers, as described in the sections that follow:

- Section 9.5.1, "Configuring EAS to Receive Events," on page 158
- Section 9.5.2, "Configuring Sentinel to Send Events," on page 158

9.5.1 Configuring EAS to Receive Events

To configure EAS to receive events, you need to:

1. Start the Event Source Manager from the Auditing page by clicking *Launch Event Source Manager*.
2. Follow the steps in Section 2 of the *Sentinel Link Solution Guide* (http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution_6.1r5.pdf).

   NOTE: You can skip the first section on accessing Event Source Manager, since the reporting module allows you to launch the tool directly.

9.5.2 Configuring Sentinel to Send Events

This section provides instructions for configuring a Sentinel server to send events to EAS. These instructions describe the approach Novell recommends for an initial setup.

NOTE: If you use a different method to configure a Sentinel server to send events to EAS, you need to be sure that all events are sent. If you do not send all events, your Identity Manager reports will not run successfully.

Detailed steps for configuring a Sentinel server to send events to another Sentinel system are provided in Section 3 of the *Sentinel Link Solution Guide* (http://support.novell.com/products/sentinel/zip/utilities/Sentinel-Link_Solution_6.1r5.pdf). If you want to refine your configuration after performing the steps below, you should refer to this document for additional information.

To configure a Sentinel server to send events to EAS:

1. Log in to your Sentinel server as user "novell".

   Set a password for user "novell" if you have not done so already. The Sentinel installer creates the user "novell" without password credentials.
2. Download the Sentinel Link Solution from *Sentinel Link Solution Downloads* (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).
3. Unzip the downloaded Sentinel Link Solution package.
4. Start Sentinel Control Center.

5 Import the new Integrator for the Sentinel Link Solution:

5a In the Novell Sentinel Control Center, select *Tools* > *Integrator Manager*. The Integrator Manager window displays.

5b Click *Manage Plug-Ins*.

5c Click the *Import* (plus sign) icon in the Integrator Plugin Manager window.

The Plugin Import Type window displays.

5d Select *Import an Integrator plugin file (.zip)*, then click *Next*.

The Choose Plugin Package File window displays.

5e Click *Browse* to locate the `slink_integrator.zip` file and click *Next*.

5f Click *Finish*.

5g Dismiss the dialogs.

6 From the Integrator Manager interface, configure an Integrator:

6a Click the *Add Integrator* icon in the bottom left corner.

6b Choose *Sentinel Link Integrator* from the *Select Integrator* drop down

6c Specify a name for your Integrator, such as “Sentinel Link Integrator to EAS”.

6d Specify a new *Service Category*, such as “SL - Sentinel Link”.

6e Provide a description for the Integrator in the *Description* field.

6f Click *Next*.

6g Specify the IP address of the EAS Server in the *Host Name* text field.

6h Specify the port number for the Sentinel Link configured on EAS. The default is 1290.

6i Click *Next* on each of the remaining dialogs.

6j Click *Finish*.

7 Import the Action plugin:

7a In the Sentinel Control Center, select *Tools* > *Action Manager*.

7b In the Action Manager window, click *Manage Plugins*.

7c In the Action Plugin Manager, click the *Import* (plus sign) icon.

7d In the Import Plugin wizard, select *Import an Action plugin file (zip,inz)*, then click *Next*.

7e Click *Browse* to locate the `Sentinel-Link_6.1r3.acz.zip` file and click *Next*.

7f Click *Next*.

7g Click *Finish*.

8 Create a new Action:

8a In Action Manager, click the *Add* (plus-sign) icon.

8b Specify an *Action Name* (for example, “SLinkEAS”).

8c Choose *Sentinel Link* from the *Action* drop down

8d Choose your Sentinel Link Integrator.

8e Click *Save*.

8f Dismiss the Action Manager dialog.

9 Create the Global Filters:

9a In the Sentinel Control Center, click on the *Admin* tab.

9b In the left navigation bar, select *Global Filter Configuration*.

9c Click *Add*.

9d Click the button under *Filter Name*. Perform the steps below for each of the following product names (note that some of the products have more than one name):

- Novell Identity Manager
- Novell eDirectory and EDIRECTORY
- Identity Vault
- Novell Modular Authentication
- Novell iManager

9d1 Click *Add*.

1. Specify a *Filter Name*.
2. Set *Property* to `ProductName`.
3. Set *Operator* to the equals sign (`=`).
4. Set *Value* to one of the product names listed above.

9d2 Click *Save*.

9e From the Global Filter Configuration dialog, perform these steps for each of the Filter Names you just created:

9e1 Click *Add*.

9e2 Select your newly created filter.

9e3 Check the *Active* check box.

9e4 Set *Action* to the Sentinel Link action configured earlier (“SLinkEAS”, in this example).

9f Set *Default Action* to database.

9g Click *Save*.

10 Downloading Reports

This section provides instructions for downloading reports.

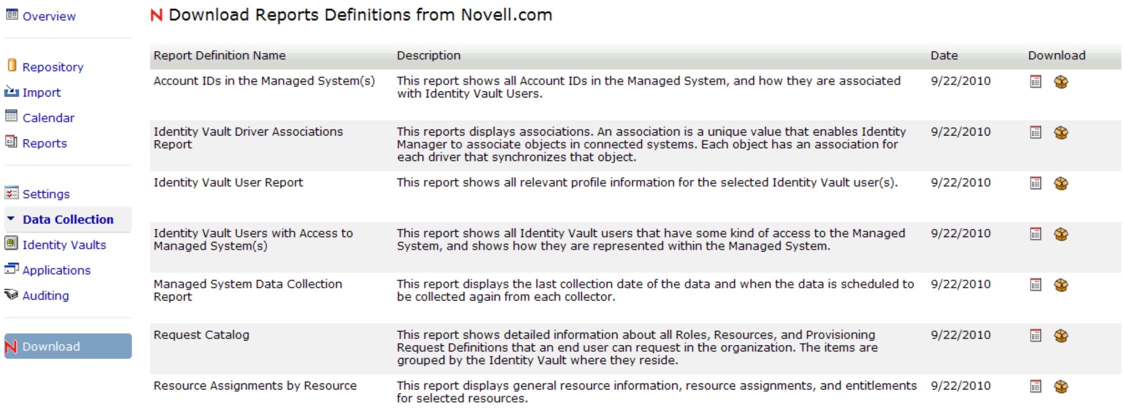
- Section 10.1, "Using the Download Page to Download Report Definitions," on page 161

10.1 Using the Download Page to Download Report Definitions

The reporting module provides the ability to download a set of predefined report definitions from the Novell.com site.

To download a predefined report:

1 Click *Download* in the left navigation menu:

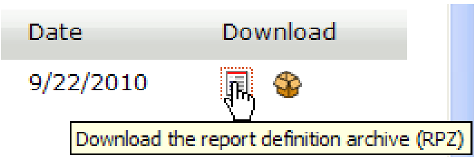


Download Reports Definitions from Novell.com

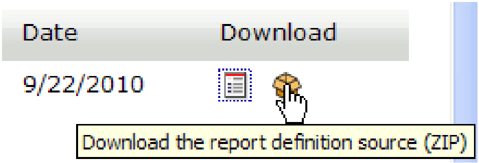
Report Definition Name	Description	Date	Download
Account IDs in the Managed System(s)	This report shows all Account IDs in the Managed System, and how they are associated with Identity Vault Users.	9/22/2010	▤ 📦
Identity Vault Driver Associations Report	This reports displays associations. An association is a unique value that enables Identity Manager to associate objects in connected systems. Each object has an association for each driver that synchronizes that object.	9/22/2010	▤ 📦
Identity Vault User Report	This report shows all relevant profile information for the selected Identity Vault user(s).	9/22/2010	▤ 📦
Identity Vault Users with Access to Managed System(s)	This report shows all Identity Vault users that have some kind of access to the Managed System, and shows how they are represented within the Managed System.	9/22/2010	▤ 📦
Managed System Data Collection Report	This report displays the last collection date of the data and when the data is scheduled to be collected again from each collector.	9/22/2010	▤ 📦
Request Catalog	This report shows detailed information about all Roles, Resources, and Provisioning Request Definitions that an end user can request in the organization. The items are grouped by the Identity Vault where they reside.	9/22/2010	▤ 📦
Resource Assignments by Resource	This report displays general resource information, resource assignments, and entitlements for selected resources.	9/22/2010	▤ 📦

2 Find the report definition you want to use in the list and click the icon under the *Download* heading for that report.

To download the report definition in a `.RPZ` file, click this icon:



To download the source for a report definition in a `.ZIP` file, click this icon:



Date	Download
9/22/2010	

Download the report definition source (ZIP)

3 Save the file to disk.

After you download a report definition archive, you can import the report definition into the Repository by using the Import page. For details, see Chapter 6, “Using the Import Tool,” on page 127.

For details on the predefined reports, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm402/idm_reports/data/bookinfo.html).

11 Creating Custom Report Definitions

This section provides instructions for creating custom report definitions.

11.1 About Custom Report Definitions

The Identity Reporting Module ships with a set of predefined report definitions. You can use them as is, or customize them to suit the requirements of your organization. You can also create new report definitions if you prefer to design your reports from scratch.

Skills requirement To create custom report definitions, you need to have a background in Structured Query Language (SQL). SQL is used to construct the database query for a report.

To facilitate the process of creating new reports, Novell provides the Novell Identity Manager Report Packaging Tool. You can customize reports in iReport and use the Reporting Packaging Tool to package them. The Novell Identity Manager Report Packaging Tool is installed on the same server where you install the Identity Reporting Module.

You can use iReport to customize your report definitions. iReport is a free, open source tool made available by the Jasper Reports project. It is available for Windows and Linux. You need to download and install iReport before you begin customizing reports.

You can find the iReport download at this location:

JasperForge.org (http://jasperforge.org/projects/ireport)

On Linux, you need to unpack the TAR file to your home directory. On Windows, you need to run an executable installer.

11.2 Starting the Report Packaging Tool

The Novell Identity Manager Report Packaging Tool is installed in the `root` folder or the Identity Reporting Module installation folder, depending on your environment. By default, the `reportpkg.jar` file is located in the `/opt/novell/idm/rbpm/IDMReporting` folder.

To start the Novell Identity Manager Report Packaging Tool:

1 On Linux, execute this command:

```
java -jar reportpkg.jar
```

or

On Windows, simply double-click the JAR file.

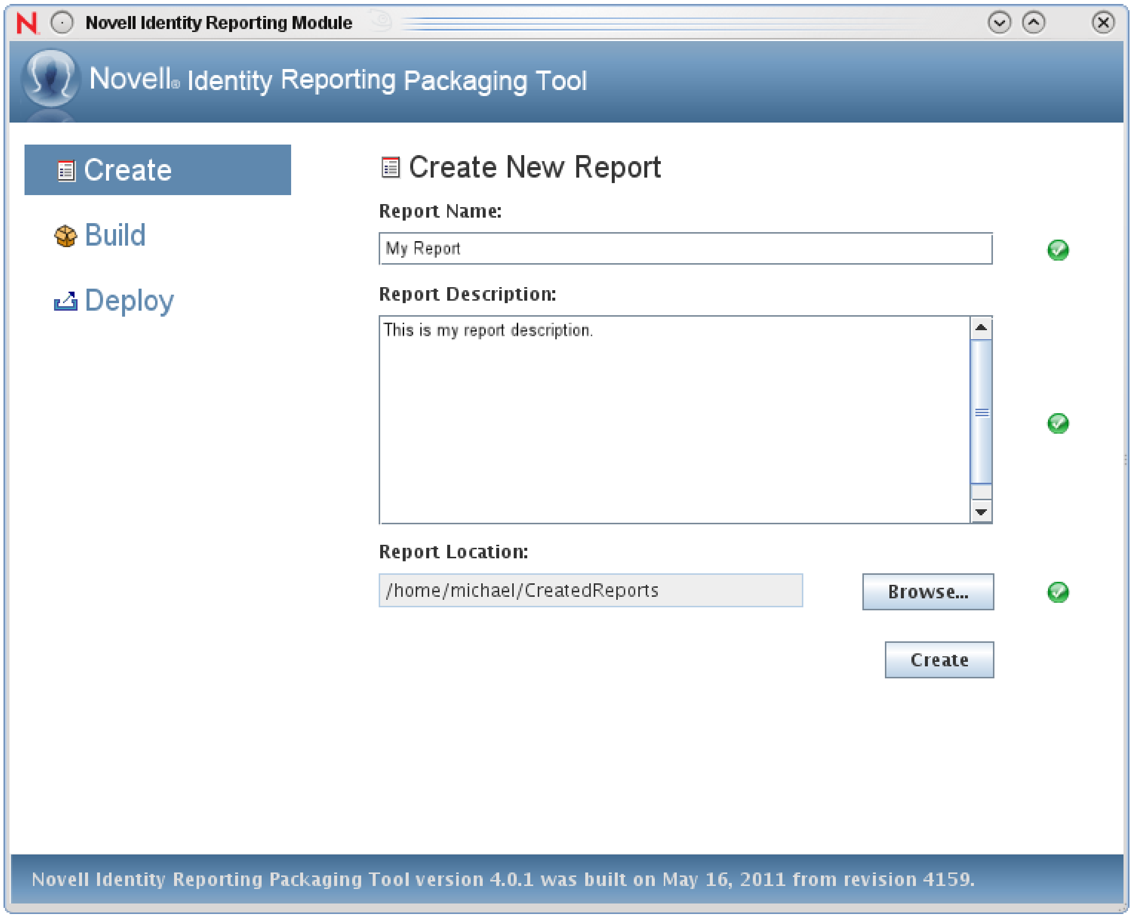
11.3 Creating a New Report Template

The Report Packaging Tool has three primary functions:

- Creating new report templates
- Building existing templates
- Deploying built templates

The first step in the process is to create a new report template.

1 Select *Create* in the left navigation menu:


Novell Identity Reporting Module
Novell® Identity Reporting Packaging Tool
Create
Build
Deploy
Browse...
Create

Create New Report

Report Name: My Report

Report Description: This is my report description.

Report Location: /home/michael/CreatedReports

Novell Identity Reporting Packaging Tool version 4.0.1 was built on May 16, 2011 from revision 4159.

2. On the Create New Report screen, specify the report name and description.
3. Select the location for the report.
4. Click the *Create* button.

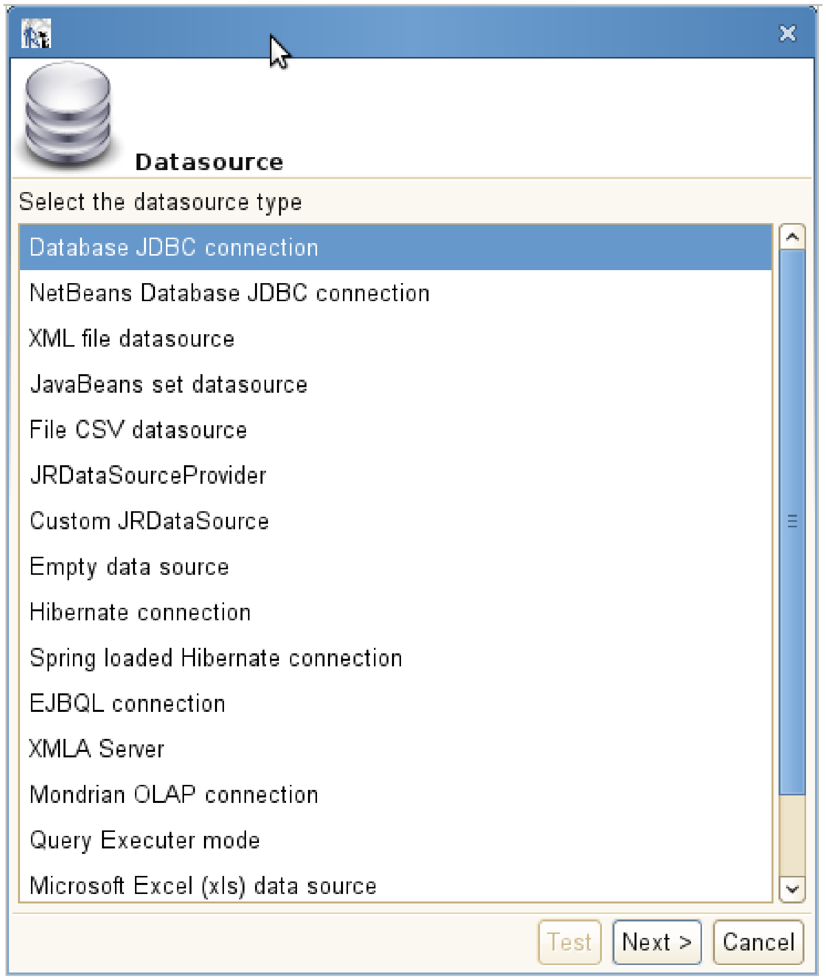
   The report contents are written to the location specified for the report.
5. In iReport, open the JRXML report.

   This file will always be called `TemplateReport.jrxml` and be located in the `IDM/6.1` directory. You cannot change the name or the location. You can specify the file by this name and location.

11.4 Configuring Your JDBC Connection in iReport

Before customizing your report, you need to configure a new datasource for the reporting PostgreSQL database within iReport. You only need to perform this step once.

1. Launch iReport, if you have not done so already.
2. Click the *Report Datasources* button on the main toolbar to open the Connections/Datasources dialog box.
3. Click the *New* button to open the Datasource dialog box.



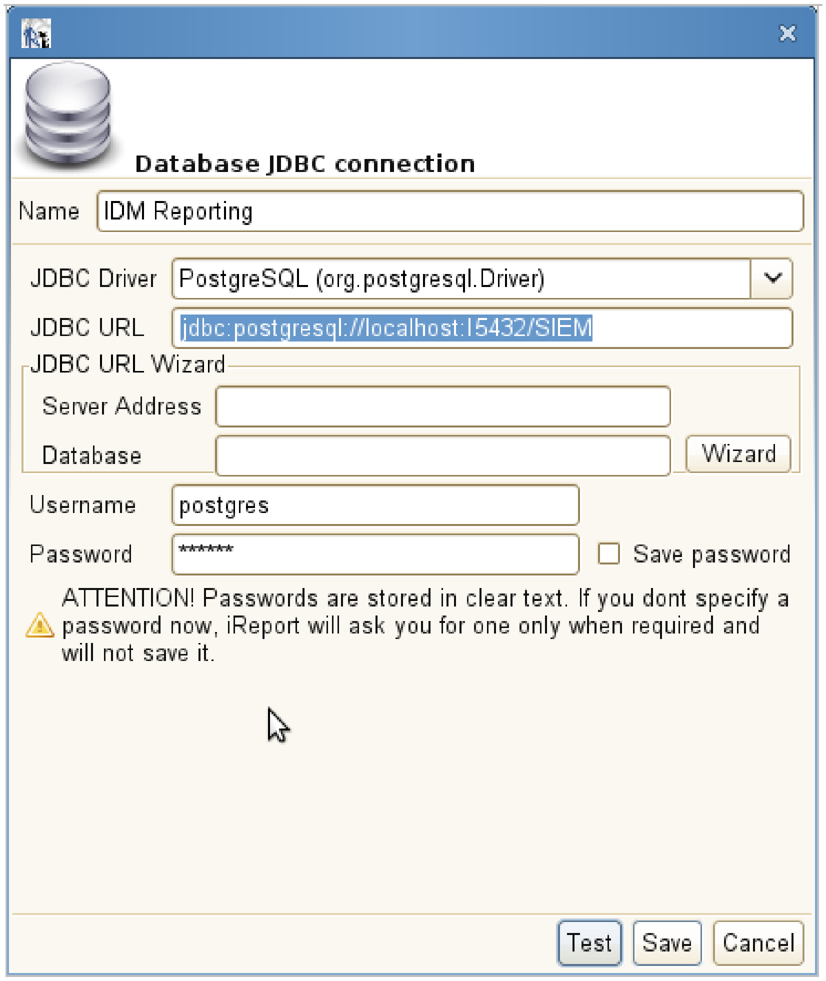
4 Select *Database JDBC Connection* and click *Next* to advance to the Database JDBC connection page.

5 Configure the PostgreSQL JDBC connection:

5a Select the *PostgreSQL (org.postgresql.Driver)* JDBC driver.

5b Specify the database URL to your database (*jdbc:postgresql://localhost:15432/SIEM*).

5c Supply your database username and password.



Database JDBC connection

Name: IDM Reporting

JDBC Driver: PostgreSQL (org.postgresql.Driver)

JDBC URL: jdbc:postgresql://localhost:15432/SIEM

JDBC URL Wizard

Server Address:

Database:

Username: postgres

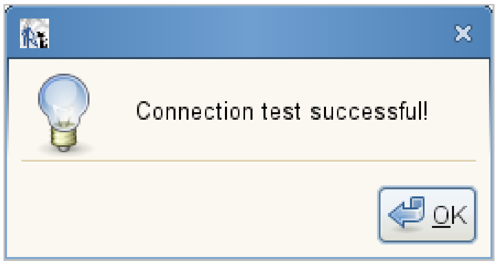
Password: *******

□ Save password

ATTENTION! Passwords are stored in clear text. If you dont specify a password now, iReport will ask you for one only when required and will not save it.

NOTE: The database username displayed in the screenshot above is intended only as an example and is not necessarily the default username. Please specify the database username and password you use for your PostgreSQL database.

5d Click the *Test* button to test your database connection:



Connection test successful!

5e Click *OK* to close the message box.

5f Save the database connection information.

6 Close the JDBC configuration dialog box.

11.5 Setting the Description and Other Strings for Your Report

The description for your report, and other strings it uses, are defined in the TemplateReport.properties file in the 6.1 directory of your new report. This file contains a set of keys and values for the string that appear in the report. The strings in the TemplateReport.properties file make it possible for your report to support multiple languages.

NOTE: The TemplateReport.properties file must end with a blank line. When you build your report archive, the localized strings defined for the report are appended to the TemplateReport.properties file, so a blank line is necessary to avoid having two lines merged.

To set the report description, you would need to edit the DESC1 key:

```
DESC1=This report shows all [authentication attempts] by users captured by
@CATEGORY@ within the selected date range, grouped by the [domain within which the
user account exists] and then grouped by the [account name].
MAXROWS=Maximum Rows
MAXROWSDESC=Specifies the maximum number of rows to return for this query
USER_DISPLAY_NAME=IDV User(s)
USER_DESCRIPTION=List of Identity Vault users to report on
```

Edit these properties to change your report description or any other string. You must rebuild and redeploy your report each time you change this file.

11.6 Setting the Report Definition Parameters

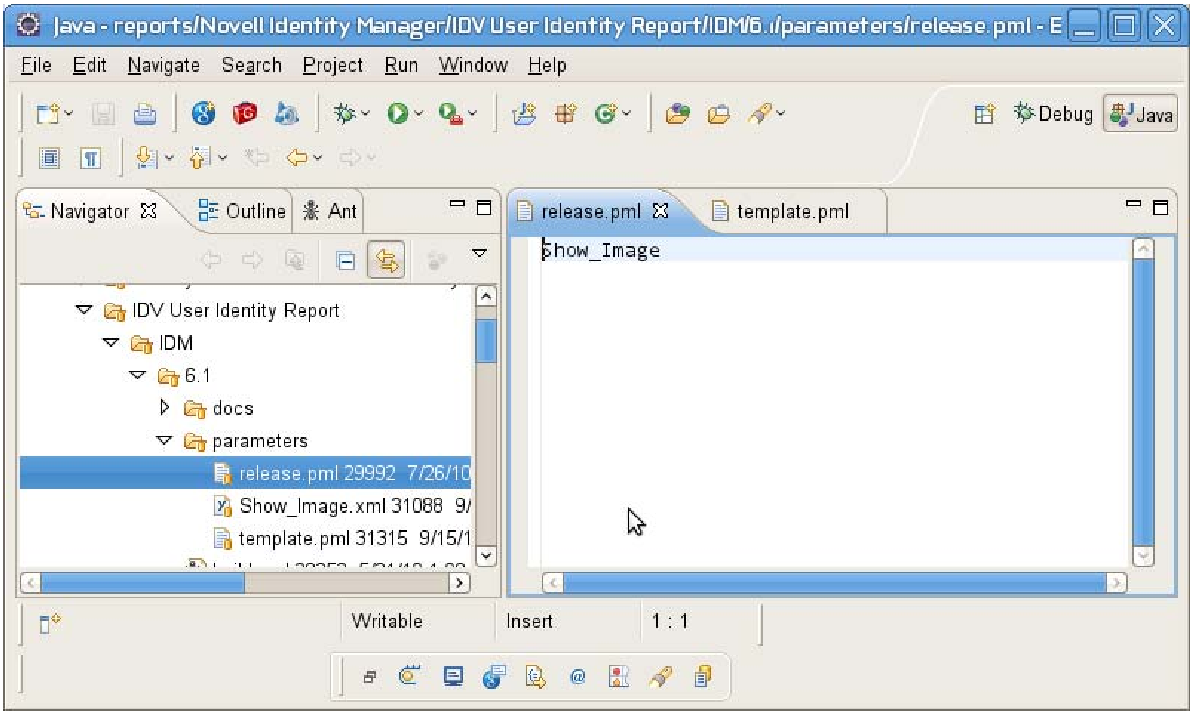
Reports support runtime parameters that allow users to specify values when they run a report. This section provides instructions for defining runtime parameters.

- Section 11.6.1, “Defining the Parameter XML File,” on page 168
- Section 11.6.2, “Defining the Type for a Parameter,” on page 170
- Section 11.6.3, “Defining an OptionQuery Parameter,” on page 170

11.6.1 Defining the Parameter XML File

Parameters specific to your report are located in the 6.1/parameters directory for your report. Each parameter is in its own XML file. Each of these XML files must be referenced in the release.pml file in the order in which you want them to appear. The release.pml file lists the parameters by name (without the file extension), as shown below:

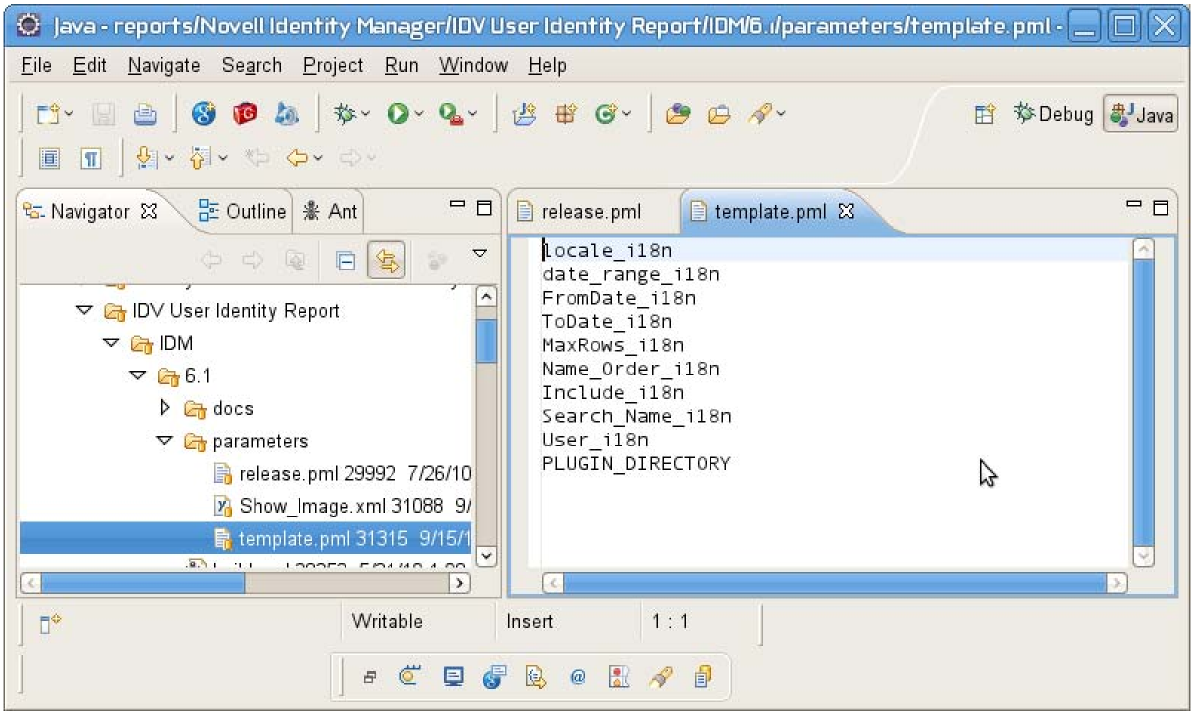
Figure 11-1 Release.pml file


Java - reports/Novell Identity Manager/IDV User Identity Report/IDM/6.1/parameters/release.pml - E
File Edit Navigate Search Project Run Window Help
Debug
Java
Navigator
Outline
Ant
IDV User Identity Report
IDM
6.1
docs
parameters
release.pml 29992 7/26/10
Show_Image.xml 31088 9/
template.pml 31315 9/15/1
release.pml
template.pml
Writable
Insert
1 : 1

```
Show_Image
```

The template.pml file lists commonly shared parameters:

Figure 11-2 Template.pml file


Java - reports/Novell Identity Manager/IDV User Identity Report/IDM/6.1/parameters/template.pml -
File Edit Navigate Search Project Run Window Help
Debug
Java
Navigator
Outline
Ant
IDV User Identity Report
IDM
6.1
docs
parameters
release.pml 29992 7/26/10
Show_Image.xml 31088 9/
template.pml 31315 9/15/1
release.pml
template.pml
Writable
Insert
1 : 1

```
locale_i18n
date_range_i18n
FromDate_i18n
ToDate_i18n
MaxRows_i18n
Name_Order_i18n
Include_i18n
Search_Name_i18n
User_i18n
PLUGIN_DIRECTORY
```

11.6.2 Defining the Type for a Parameter

The reporting module supports the following values for <Type>:

- String
- Date
- Integer
- Boolean

The user interface shows a specific control for each data type:

Table 11-1 *Controls for Parameter Data Types*

Data Type	Control
String	TextBox
String with Options	ListBox
String with OptionQuery	Autocompleter
Date	DatePicker
Integer	IntegerTextBox
Boolean	Checkbox

All of the parameters need to have this setting:

```
<IsForPrompting>1</IsForPrompting>
```

If you know that your report cannot run without a particular value specified, you can mark a parameter as required with the following setting:

```
<Required>1</Required>
```

To make an Options parameter or OptionQuery parameter allow for multiple values, you should include these two settings:

```
<OptionMultivalue>1</OptionMultivalue>
<OptionMultivalueDelimiter>;</OptionMultivalueDelimiter>
```

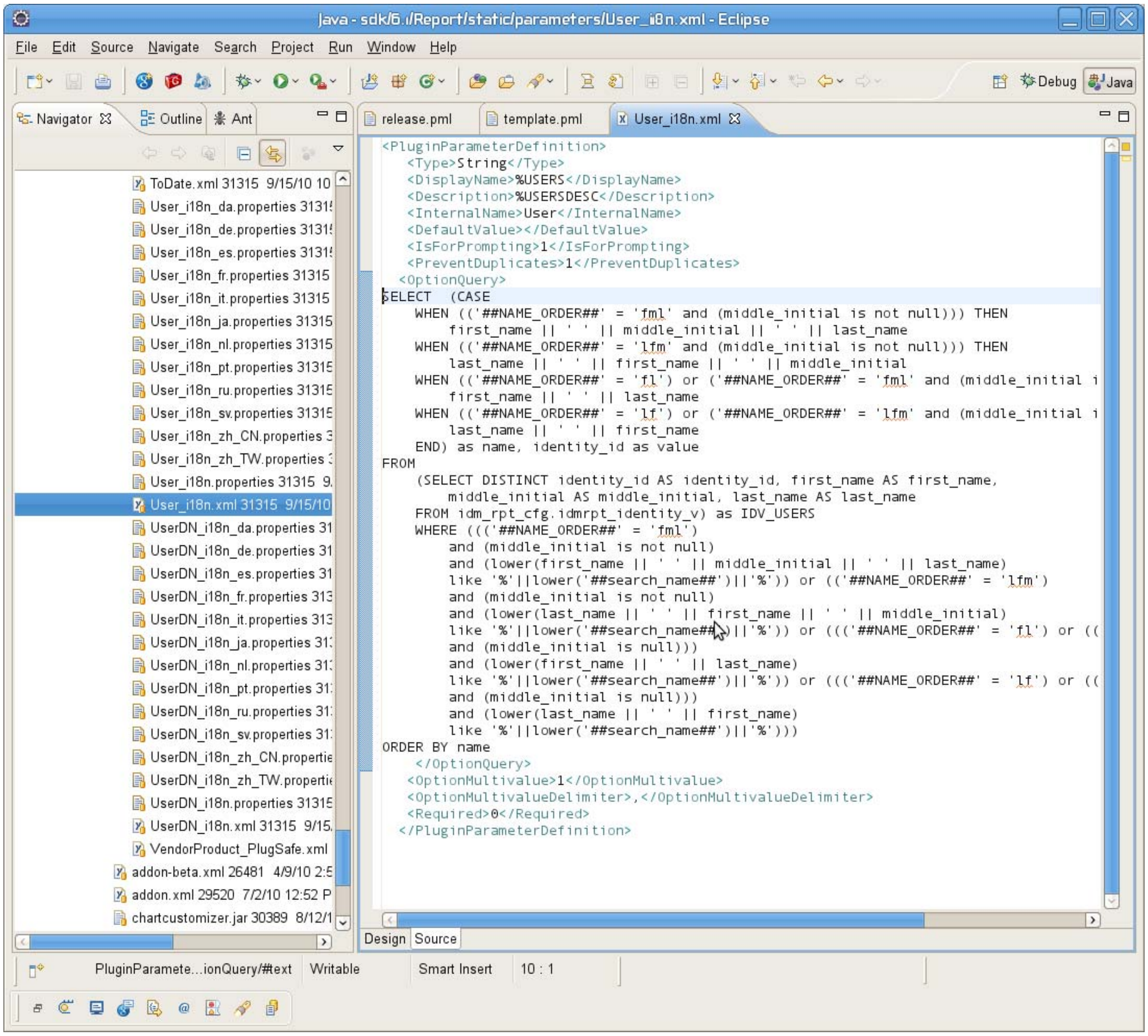
11.6.3 Defining an OptionQuery Parameter

Suppose you want to generate a report that shows role information, and you want to allow the role as a parameter, so that the definition can be scoped at runtime. In this case, you can use an OptionQuery so that the reporting module shows you a list and allows for typeahead automatic completion, based on the roles that are stored in the database on which to report. To provide support for this capability, you need to follow a specific syntax that uses cascaded parameters. The syntax *##parameter_name##* within the OptionQuery references another parameter definition. Novell provides shared common parameters that serve this purpose already, `Role_i18n.xml` and `Search_Role_i18n.xml`. They can be reused by specifying them in the `template.pml` or copied into your local parameters folder and modified to suit your needs.

The `User_i18n.xml` and `Search_Name_i18n.xml` are the respective parameters for allowing Identity Vault user to be a parameter. The `User_i18n.xml` parameter also demonstrates the ability to include a special cascaded parameter, *##NAME_ORDER##*. This allows you to localize the Name Order of a name (Given-name Surname vs. Surname Given-name), or allow for a Middle Initial in the name. If you would like your OptionQuery to make use of this feature, follow the name order example shown below.

Here’s what the User_i18n.xml file looks like:

Figure 11-3 *User_i18n.xml file*


Java - sdk/6.i/Report/static/parameters/User_i18n.xml - Eclipse
File Edit Source Navigate Search Project Run Window Help
Debug
Java
Navigator
Outline
Ant
release.pml
template.pml
User_i18n.xml
ToDate.xml 31315 9/15/10 10
User_i18n_da.properties 3131
User_i18n_de.properties 3131
User_i18n_es.properties 3131
User_i18n_fr.properties 31315
User_i18n_it.properties 31315
User_i18n_ja.properties 31315
User_i18n_nl.properties 31315
User_i18n_pt.properties 31315
User_i18n_ru.properties 31315
User_i18n_sv.properties 31315
User_i18n_zh_CN.properties 3
User_i18n_zh_TW.properties
User_i18n.properties 31315 9.
User_i18n.xml 31315 9/15/10
UserDN_i18n_da.properties 31
UserDN_i18n_de.properties 31
UserDN_i18n_es.properties 31
UserDN_i18n_fr.properties 313
UserDN_i18n_it.properties 313
UserDN_i18n_ja.properties 31
UserDN_i18n_nl.properties 31
UserDN_i18n_pt.properties 31
UserDN_i18n_ru.properties 31
UserDN_i18n_sv.properties 31
UserDN_i18n_zh_CN.propertie
UserDN_i18n_zh_TW.propertie
UserDN_i18n.properties 31315
UserDN_i18n.xml 31315 9/15.
VendorProduct_PlugSafe.xml
addon-beta.xml 26481 4/9/10 2:5
addon.xml 29520 7/2/10 12:52 P
chartcustomizer.jar 30389 8/12/1
Design
Source
PluginParamete...ionQuery/#text
Writable
Smart Insert
10 : 1

```
<PluginParameterDefinition>
   <Type>String</Type>
   <DisplayName>%USERS</DisplayName>
   <Description>%USERSDESC</Description>
   <InternalName>User</InternalName>
   <DefaultValue></DefaultValue>
   <IsForPrompting>1</IsForPrompting>
   <PreventDuplicates>1</PreventDuplicates>
  <OptionQuery>
SELECT  (CASE
    WHEN (('##NAME_ORDER##' = 'fml' and (middle_initial is not null))) THEN
        first_name || ' ' || middle_initial || ' ' || last_name
    WHEN (('##NAME_ORDER##' = 'lfm' and (middle_initial is not null))) THEN
        last_name || ' ' || first_name || ' ' || middle_initial
    WHEN (('##NAME_ORDER##' = 'fl') or ('##NAME_ORDER##' = 'fml' and (middle_initial i
        first_name || ' ' || last_name
    WHEN (('##NAME_ORDER##' = 'lf') or ('##NAME_ORDER##' = 'lfm' and (middle_initial i
        last_name || ' ' || first_name
    END) as name, identity_id as value
FROM
    (SELECT DISTINCT identity_id AS identity_id, first_name AS first_name,
        middle_initial AS middle_initial, last_name AS last_name
    FROM idm_rpt_cfg.idmrpt_identity_v) as IDV_USERS
    WHERE ((('##NAME_ORDER##' = 'fml')
        and (middle_initial is not null)
        and (lower(first_name || ' ' || middle_initial || ' ' || last_name)
        like '%'||lower('##search_name##')||'%')) or (('##NAME_ORDER##' = 'lfm')
        and (middle_initial is not null)
        and (lower(last_name || ' ' || first_name || ' ' || middle_initial)
        like '%'||lower('##search_name##')||'%')) or ((('##NAME_ORDER##' = 'fl') or ((
        and (middle_initial is null)))
        and (lower(first_name || ' ' || last_name)
        like '%'||lower('##search_name##')||'%')) or ((('##NAME_ORDER##' = 'lf') or ((
        and (middle_initial is null)))
        and (lower(last_name || ' ' || first_name)
        like '%'||lower('##search_name##')||'%')))
ORDER BY name
    </OptionQuery>
   <OptionMultivalue>1</OptionMultivalue>
   <OptionMultivalueDelimiter>,</OptionMultivalueDelimiter>
   <Required>0</Required>
  </PluginParameterDefinition>
```

For this example to work properly, the ##NAME_ORDER## cascaded parameter must match the <InternalName>NAME_ORDER</InternalName> of the name order parameter.

All OptionQuery parameters *must* have a cascaded parameter such as a search_name, where the OptionQuery SQL is using it as its WHERE clause. Its internal name does not matter, as long as it is unique and is used in the SQL appropriately. It should have these settings:

```
<DefaultValue></DefaultValue>
<IsForPrompting>0</IsForPrompting>
```

11.7 Customizing the Report in iReport

1 In iReport, open the new JRXML file that you generated by using the Report Packaging Tool.

The JRXML file should be located in the `IDM/6.1` subdirectory under the directory where when you created the report template.

Error Messages in iReport When you load a *TemplateReport.jrxml* file into iReport you may see the following error in the *Report Problems* window of iReport.

```
com.jaspersoft.ireport.designer.errorhandler.ProblemItem@136425a2
java.lang.ClassNotFoundException:com.novell.sentinel.content.reports.TemplateR
eportScriptlet
com.jaspersoft.ireport.designer.outline.nodes.StylesNode@531d5c7d[Name=,displa
yName=Styles]
```

This is not a serious error, so you can simply ignore the message.

2 After you have opened the report in iReport, you can make the necessary customizations:

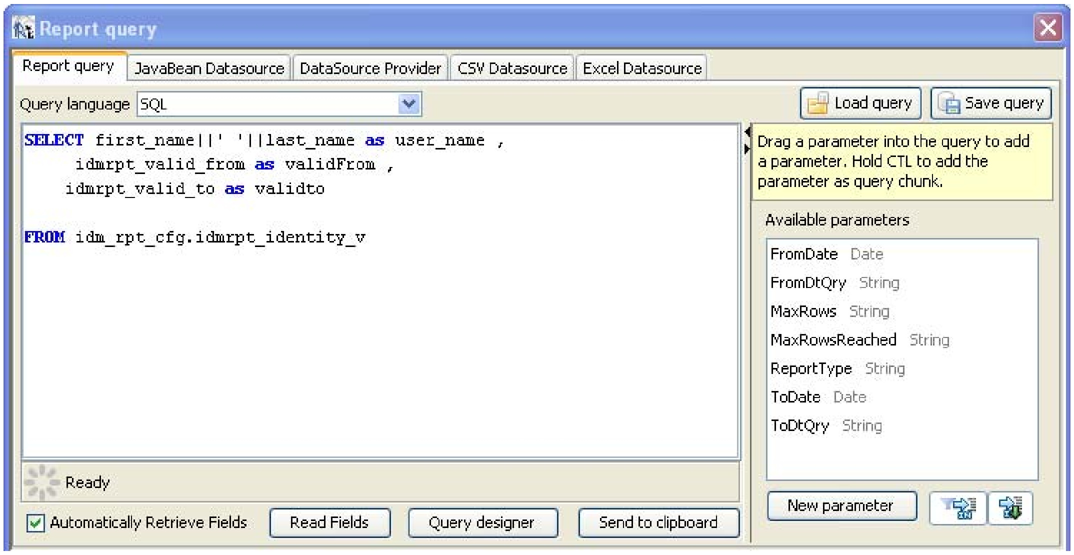
2a Define a SQL query to get the data for your report.

To provide data for your custom reports, you need to use database views. The core database views that ship with the product include both current state and history information for reporting. In addition to these views, there is a separate set of views that includes only the current state information, thereby providing a slight improvement in reporting performance. For example, the "idmrpt_approver_v" view provides both current state and history information, whereas the "idmrpt_approver_cs_v" view provides just the current state information. The structure of the two views is identical, so the columns used are exactly the same. Only the view names are different. The name for each current state view includes "_cs" before the "_v" suffix.

For most applications, you can use the views that provide both current state and history information. These views are described in Chapter 12, "Schema Documentation," on page 177.

NOTE: You can only use views in custom reports. If you use your root username to log into the database, iReport will let you select data from the tables. However, the report will fail when you deploy it and try to run it.

To define the SQL query for a report, select the *Detail* node in the *Report Inspector* and click the database icon in the designer toolbar at the top of the report definition window. Then, enter the SQL statement on the *Report query* tab:



Query language SQL

```
SELECT first_name||' '||last_name as user_name ,
     idmrpt_valid_from as validFrom ,
    idmrpt_valid_to as validto

FROM idm_rpt_cfg.idmrpt_identity_v
```

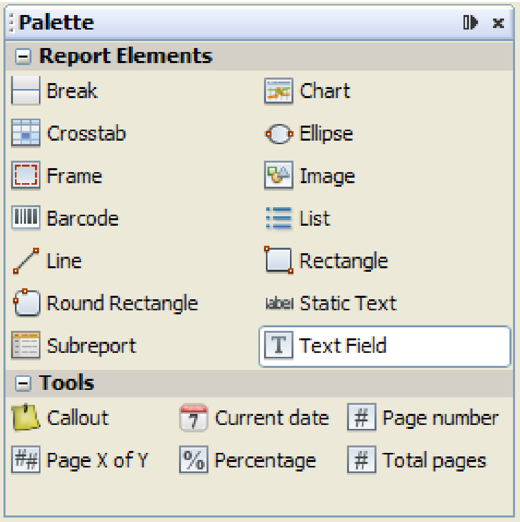
Drag a parameter into the query to add a parameter. Hold CTL to add the parameter as query chunk.

FromDate	Date
FromDtQry	String
MaxRows	String
MaxRowsReached	String
ReportType	String
ToDate	Date
ToDtQry	String

☑ Automatically Retrieve Fields

2b Define the report layout.

To define the report layout, you need to add elements to the report definition. iReport supports many different types of report elements. You can choose the elements you need from the *Report Elements* section of the *Palette*.

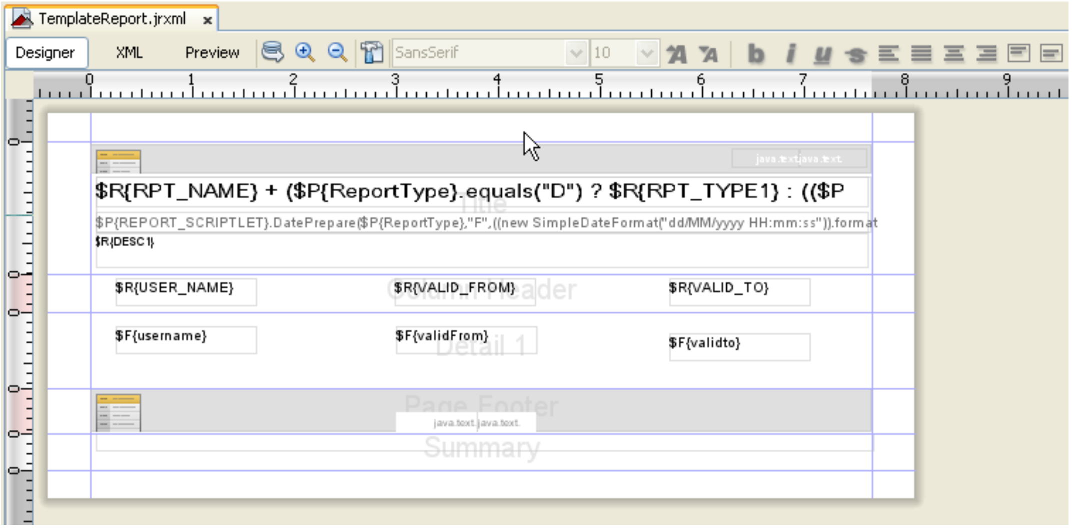


For example, to add a column header, drag the *Text Field* icon from the *Palette* onto the header band of the report layout canvas.

To add a data field, drag the field name from the *Fields* node in the *Report Inspector* onto the detail band of the report layout canvas.

When you drag a field onto a report, iReport creates an expression to bind the display element to the appropriate database value.

Once you've added the fields you need, you can format the fields to suit your requirements by stretching them or moving them on the report canvas.



```
$R{RPT_NAME} + ($P{ReportType}.equals("D") ? $R{RPT_TYPE1} : (($P
$P{REPORT_SCRIPTLET}.DatePrepare($P{ReportType},"F",((new SimpleDateFormat("dd/MM/yyyy HH:mm:ss")).format
$R{DESC1}
$R{USER_NAME}        $R{VALID_FROM}        $R{VALID_TO}
$F{username}         $F{validFrom}         $F{validto}
```

3 Save your report.

After saving your report, you need to package the report before you can import or deploy it. For details on packaging the report, see Section 11.9, "Building Your Report," on page 175.

11.8 Displaying Parameters and Selected Criteria in the Report

You can display parameters and selected criteria in a report. To do this, you need to make some changes in the JRXML file.

First, locate the textField-2 of the `TemplateReport.jrxml` file, which has “$P{REPORT_SCRIPTLET}.DatePrepare...” showing. This text field is where the selected values of report parameters are displayed. The generated `TemplateReport.jrxml` file automatically displays the Date/Time Range of the report and the MaxRows parameter and selected value.

```
$P{REPORT_SCRIPTLET}.DatePrepare($P{ReportType},"F",((new SimpleDateFormat("dd/MM/
yyyy HH:mm:ss")).format($P{FromDate})),"D") + " " + $R{HEADER6} + " "  +
$P{REPORT_SCRIPTLET}.DatePrepare($P{ReportType},"T",((new SimpleDateFormat("dd/MM/
yyyy HH:mm:ss")).format($P{ToDate})),"D") + "\n" +
java.text.MessageFormat.format($R{MAXROWS_COLON}, new
Object[]{
$P{MaxRows}.equals("ALL") ? $R{ALL} :
$P{MaxRows}
})
```

To add more parameters, simply append to this text field by right-clicking the field and selecting *Edit Expression*. Add a + “\n” + parameter's label and value for each parameter. To add a label, add the localized label to the properties file as a parameterized string, such as USERS_COLON=Users: {0}. Then, use java.text.MessageFormat to fill in the value.

When the parameter is an OptionQuery, you must also pass the cascaded search name parameter to the JRXML. Then, you can use that value to display on the report for readability instead of showing the IDs. For example, this is the value of textField-2 in the Role Assignments by Member report:

```
$P{REPORT_SCRIPTLET}.DatePrepare($P{ReportType},"F",((new SimpleDateFormat("dd/MM/
yyyy HH:mm:ss")).format($P{FromDate})),"D") + " " + $R{HEADER6} + " "  +
$P{REPORT_SCRIPTLET}.DatePrepare($P{ReportType},"T",((new SimpleDateFormat("dd/MM/
yyyy HH:mm:ss")).format($P{ToDate})),"D") + "\n" +
java.text.MessageFormat.format($R{MAXROWS_COLON}, new
Object[]{
$P{MaxRows}.equals("ALL") ? $R{ALL} :
$P{MaxRows}
}) + "\n" +
java.text.MessageFormat.format($R{NAME_ORDER_COLON}, new
Object[]{
$P{NAME_ORDER}.equals("lfm") ? $R{NAME_ORDER_LFM} :
$P{NAME_ORDER}.equals("fl") ? $R{NAME_ORDER_FL} :
$P{NAME_ORDER}.equals("lf") ? $R{NAME_ORDER_LF} : $R{NAME_ORDER_FML}
}) + "\n" +
java.text.MessageFormat.format($R{USERS_COLON}, new Object[]{
(($P{User} != null && $P{User}.size() > 0) ? $P{search_name} : $R{ALL})
}) +
"" + ($P{Only_Show_SOD}.booleanValue() ? "\n" + $R{SHOW_SOD} : "")
```

The Role Assignments by Member parameters displayed are:

- Data Range
- Max Rows
- Name Order
- Users
- Separation of Duties information only

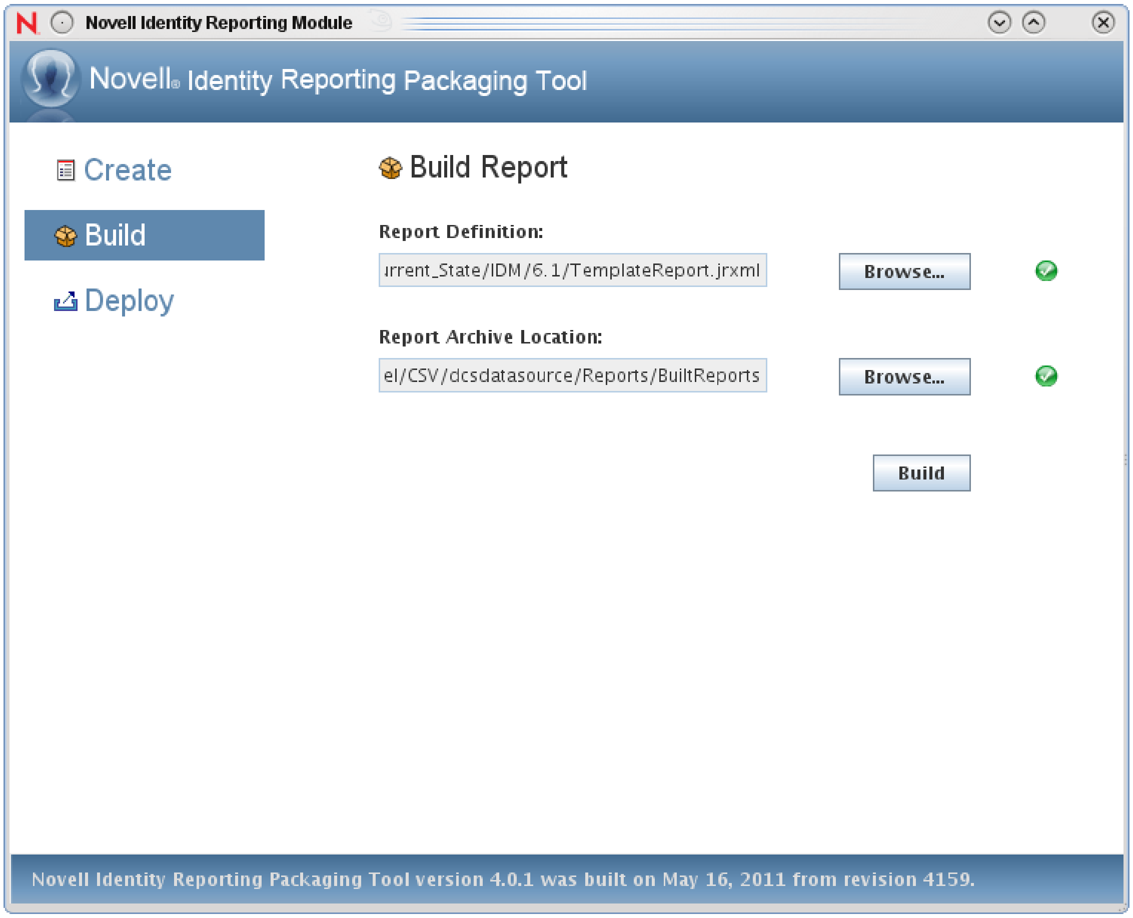
11.9 Building Your Report

Before you deploy your report, you need to build it. The source of the report is a set of properties, images, and the JRXML file. You must bundle these files into a report archive before you can deploy the report template.

The process of building the report archive creates an RPZ file. This is a report definition archive containing your report and the report metadata. There might also be additional files such as images or properties that your report depends on.

1. Select *Build* in the left-navigation menu in the Report Packaging Tool.
2. On the Build Report screen, specify the report definition.

   This is the JRXML file generated when you created your report.
3. Specify the location of your report archive and the report author.
4. Click the *Build* button to build the RPZ file for your report definition.


Novell Identity Reporting Module
Novell® Identity Reporting Packaging Tool
Create
Build
Deploy
Build Report
Browse...
Browse...
Build

Report Definition: ırrent_State/IDM/6.1/TemplateReport.jrxml

Report Archive Location: el/CSV/dcsdatasource/Reports/BuiltReports

Novell Identity Reporting Packaging Tool version 4.0.1 was built on May 16, 2011 from revision 4159.

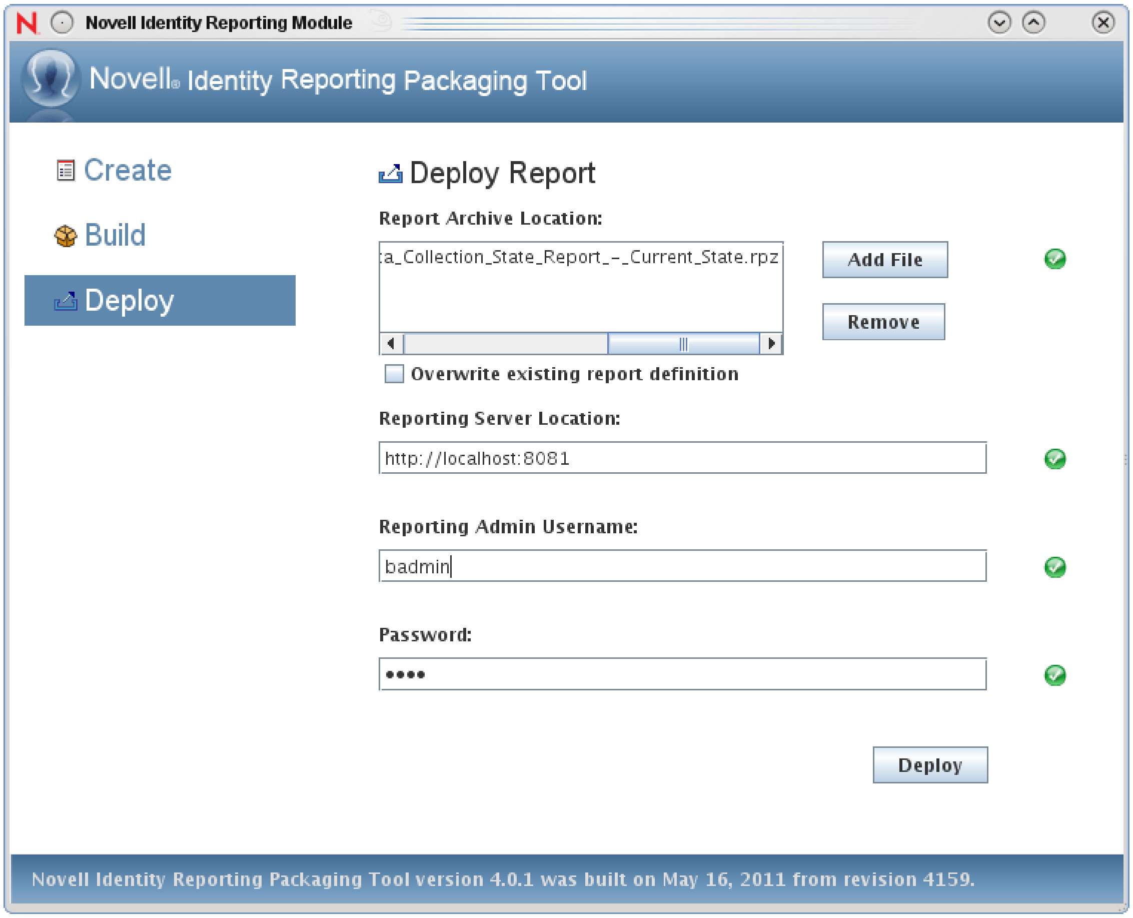
11.10 Deploying Your Report

After you build the report template archive, you are ready to deploy the report to the reporting server.

1 Select *Deploy* in the left-navigation menu.

2 On the Deploy Report screen, select the RPZ file and specify the address of your server and the credentials for accessing the server.

3 Click the *Deploy* button.


Novell Identity Reporting Module
Novell® Identity Reporting Packaging Tool
Create
Build
Deploy
Add File
Remove
Deploy

Deploy Report

Report Archive Location:
a_Collection_State_Report_-_Current_State.rpz

□ Overwrite existing report definition

Reporting Server Location:
http://localhost:8081

Reporting Admin Username:
badmin

Password:
••••

Novell Identity Reporting Packaging Tool version 4.0.1 was built on May 16, 2011 from revision 4159.

The Report Packaging Tool deploys the report template to the reporting server. You do not need to import the report on the Import page to use the report. After the template has been deployed, you can access it on the Repository page in the reporting module.

12 Schema Documentation

This section provides reference documentation for the database views for reporting.

12.1 About the Database Views

To provide data for your custom reports, you need to use database views. The core database views that ship with the product include both current state and history information for reporting. For most applications, you can use the views that provide both current state and history information. These views are described in the sections that follow.

In addition to the core set of views, there is a separate set of views that includes only the current state information, thereby providing a slight improvement in reporting performance. For example, the “idmrpt_approver_v” view provides both current state and history information, whereas the “idmrpt_approver_cs_v” view provides just the current state information. The structure of the two views is identical, so the columns used are exactly the same. Only the view names are different. The name for each current state view includes “_cs” before the “_v” suffix.

For most applications, you can use the views that provide both current state and history information. However, if you want to use the views that provide current state information only, here is the complete list of current state views:

- idmrpt_acct_link_cs_v
- idmrpt_approver_cs_v
- idmrpt_association_cs_v
- idmrpt_ext_idv_item_cs_v
- idmrpt_cat_mappings_cs_v
- idmrpt_category_cs_v
- idmrpt_container_cs_v
- idmrpt_ent_param_token_value_cs_v

- idmrpt_ent_type_cs_v
- idmrpt_ext_item_attr_cs_v
- idmrpt_group_cs_v
- idmrpt_identity_cs_v
- idmrpt_ms_identity_cs_v
- idmrpt_idv_acct_cs_v
- idmrpt_idv_drivers_cs_v
- idmrpt_idv_ent_bindings_cs_v
- idmrpt_idv_ent_cs_v
- idmrpt_idv_identity_trust_cs_v
- idmrpt_idv_prd_cs_v
- idmrpt_ms_acct_rule_cs_v
- idmrpt_ms_acct_cs_v
- idmrpt_ms_ent_type_cs_v
- idmrpt_ms_ent_cs_v
- idmrpt_ms_ent_trust_cs_v
- idmrpt_ms_cs_v
- idmrpt_owners_cs_v
- idmrpt_res_parameter_cs_v
- idmrpt_resource_cs_v
- idmrpt_role_level_cs_v
- idmrpt_role_mappings_cs_v
- idmrpt_role_resource_association_cs_v
- idmrpt_role_cs_v
- idmrpt_sod_cs_v
- idmrpt_sod_violations_cs_v
- idmrpt_team_assignments_cs_v
- idmrpt_team_cs_v
- idmrpt_approval_cs_v

12.2 idmrpt_acct_link_v

Information about the links between managed system accounts and IDM accounts.

ms_acct_id	VARCHAR(32)	This is the account ID
idv_acct_id	VARCHAR(32)	
idv_association	VARCHAR(128)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
act_link_id	VARCHAR(32)	

idmrpt_deleted	bool
idmrpt_syn_state	int2

12.3 idmrpt_approver_v

Contains role approver information.

approver_assoc_id	VARCHAR(32)	The ID of the role approval object
cat_item_id	VARCHAR(32)	The ID of the role category
cat_item_type_id	VARCHAR(32)	The role category type. For example, RESOURCE, SOD, or ROLE
approver_id	VARCHAR(32)	The ID of the user approving the role
approver_dn	VARCHAR(255)	The DN of the user approving the role
approver_type	VARCHAR(32)	The type of approval. Fox example, IDENTITY, GROUP, or CONTAINER
approval_type	int2	A number indicating the type of approval: 1-grant, 2-revoke, grant & 3-revoke
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The time the role will be valid from
idmrpt_deleted	bool	TRUE if the role is deleted and FALSE otherwise
idmrpt_syn_state	int2	The current sync state of the role

12.4 idmrpt_association_v

association_id	VARCHAR(32)
drv_id	VARCHAR(32)
assoc_uid	VARCHAR(256)
assoc_state	int2
item_id	VARCHAR(32)
item_type_id	VARCHAR(32)
idmrpt_deleted	bool
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_syn_state	int2

12.5 idmrpt_ext_idv_item_v

Stores information about extended objects in the identity vault.

item_id	VARCHAR(32)
item_dn	VARCHAR(255)
item_guid	VARCHAR(64)
object_id	VARCHAR(32)
item_name	VARCHAR(128)
item_desc	VARCHAR(1024)
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_deleted	bool
idv_id	VARCHAR(32)
idmrpt_syn_state	int2

12.6 idmrpt_cat_item_types_v

Contains information about the catalog items stored within the database.

item_type_id	VARCHAR(4000)	The ID for the type of catalog information. For example, ROLE, RESOURCE, GROUP, or SOD
item_type_name	VARCHAR(128)	The name of the catalog. For example, IDM RBPM Role, IDM RBPM Resource, or IDM GROUP
item_type	int2	Numeric representation of item type : 1-user, 2-role, 3-group, 4-resource, 5-container, 6-prd, ...
idmrpt_table_name	VARCHAR(4000)	The name of the table containing the information for this catalog

12.7 idmrpt_cat_mappings_v

mapping_id	VARCHAR(32)
mapped_id	VARCHAR(32)
category_id	VARCHAR(32)
mapped_id_type	VARCHAR(32)
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_deleted	bool
idmrpt_syn_state	int2

12.8 idmrpt_category_v

Table that stores custom catalog item information

category_id	VARCHAR(32)	
category_type_id	VARCHAR(32)	
category_key	VARCHAR(255)	
category_name	VARCHAR(4000)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
idv_id	VARCHAR(32)	
idmrpt_syn_state	int2	

12.9 idmrpt_ms_collect_state_v

contains information about the state of the collectors.

ms_collect_id	VARCHAR(32)	The ID of the collectors
ms_query_api	VARCHAR(4000)	
ms_collect_time	TIMESTAMP WITH TIME ZONE	The last collection time
ms_collect_state	bool	The collection state
ms_collection_id	VARCHAR(32)	The ID of the latest collection
ms_collect_payload	VARCHAR(4000)	
ms_collect_error	VARCHAR(4000)	

12.10 idmrpt_container_v

Contains information about the Identity Vault containers.

container_id	VARCHAR(32)	The ID of the container
container_dn	VARCHAR(255)	The DN of the container
container_guid	VARCHAR(64)	The GUID of the container
container_name	VARCHAR(4000)	The display name of the container
container_desc	VARCHAR(4000)	The description of the container
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date the container is valid from
idmrpt_deleted	bool	TRUE if the container has been deleted and FALSE otherwise

idv_id	VARCHAR(32)	The ID of the Identity Vault
container_type_id	VARCHAR(32)	
idmrpt_syn_state	int2	The synchronization state

12.11 idmrpt_ext_attr_v

Stores extended or customized attribute definitions. This table does not require historical data, because it used as taxonomy of custom attributes.

attribute_id	VARCHAR(32)	
attribute_name	VARCHAR(128)	
display_value	VARCHAR(128)	
attribute_type	VARCHAR(64)	java attribute type (simple type: int, boolean, timestamp (as long), long, string, boolean

12.12 idmrpt_ext_obj_v

Stores extended or custom object definitions. This table does not require historical data, because it used as taxonomy of custom attributes.

object_id	VARCHAR(32)	
object_name	VARCHAR(128)	
object_class	VARCHAR(128)	

12.13 idmrpt_dc_service_cfg_v

Contains information about the reporting data collection service configuration.

data_collect_locale	VARCHAR(32)	The locale that will be used in when collecting data from this data collection service. This value defaults to the system default locale of the data collection service.
data_collect_interval	int2	The data collection interval
data_collect_interval_units	int2	The units for the data collection interval. This value indicates days, weeks, or months: 1- day, 2- week, 3- month
data_retention_interval	int2	The data retention interval. This controls how long reporting data will be stored in the reporting warehouse.
data_retention_interval_units	int2	The units for the data retention interval. This value indicates days, weeks, or months: 1- day, 2- week, 3- month

data_cleanup_interval	int2	The data retention interval. This controls how long reporting data will be stored in the reporting warehouse.
data_cleanup_interval_units	int2	The units for the data clean up interval. This value indicates days, weeks, or months: 1- day, 2- week, 3- month
next_data_cleanup	int8	The time for the next data cleanup.
min_dc_interval	int8	The units for the minimum data collection interval. This value indicates days, weeks, or months: 1- day, 2- week, 3- month
data_collect_query_timeout	int8	
next_data_collect_date	int8	
data_collect_srv_id	VARCHAR(32)	

12.14 idmrpt_ent_param_token_value_v

Stores custom entitlement parameter token values parsed out of the entitlement parameter string

binding_id	VARCHAR(32)	
ent_id	VARCHAR(32)	
ent_token_id	VARCHAR(32)	auto generated uuid
bnd_cat_item_type_id	VARCHAR(32)	
ent_token_key	VARCHAR(64)	
ent_token_val	VARCHAR(512)	
idmrpt_deleted	bool	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_syn_state	int2	

12.15 idmrpt_ent_type_v

Stores entitlement types and categories

ent_type_id	VARCHAR(32)	The auto generated entitlement type id.
ent_type_cat	VARCHAR(512)	The entitlement type name. Examples: security account, security grouping, other account
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	Date this entitlement is valid from
idmrpt_deleted	bool	TRUE if this value has been deleted and FALSE otherwise.
idmrpt_syn_state	int2	The synchronization state

12.16 idmrpt_ext_item_attr_v

Stores extended catalog item information

cat_item_id	VARCHAR(32)
cat_item_type_id	VARCHAR(32)
attribute_id	VARCHAR(32)
attribute_value	VARCHAR(512)
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
cat_item_attr_id	VARCHAR(32)
idmrpt_deleted	bool
idmrpt_syn_state	int2

12.17 idmrpt_group_v

Contains data about groups stored in the Identity Vault.

group_id	VARCHAR(32)	The unique ID for this group in the Identity Warehouse
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this group.
group_dn	VARCHAR(255)	The DN of the group
group_guid	VARCHAR(64)	The GUID of the group from the Identity Vault
group_name	VARCHAR(4000)	The display name of the group
group_desc	VARCHAR(4000)	The group description
dynamic_group	bool	TRUE if this group is a dynamic group and FALSE otherwise
dynamic_rule	VARCHAR(1024)	The dynamic rule for this group if it is dynamic.
nested_group	bool	TRUE if this group is a nested group and FALSE otherwise
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	Date this group became valid
idmrpt_deleted	bool	TRUE if this group has been deleted and FALSE otherwise
idmrpt_syn_state	int2	The sync state for this group

12.18 idmrpt_identity_v

Contains identity profile information about users that have been collected by the reporting tool

identity_id	VARCHAR(32)	Auto generated unique identity identifier
first_name	VARCHAR(4000)	First name
last_name	VARCHAR(4000)	Last name
middle_initial	VARCHAR(4000)	Middle name
full_name	VARCHAR(4000)	Full name
job_title	VARCHAR(4000)	Job title
department	VARCHAR(4000)	Department
location	VARCHAR(4000)	Location
email_address	VARCHAR(4000)	Email address
office_phone	VARCHAR(4000)	Office phone
cell_phone	VARCHAR(4000)	Cell phone
private_phone	VARCHAR(4000)	Private phone
im_id	VARCHAR(64)	Instant messanger id
mgr_id	VARCHAR(32)	The UUID for this user's manager
photo	TEXT(2147483647)	This users photo
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	Date the user was created
generational_qualifier	VARCHAR(8)	
prefix	VARCHAR(4000)	Prefix
preferred_name	VARCHAR(4000)	The prefix name
preferred_language	VARCHAR(4000)	The prefix language
job_code	VARCHAR(4000)	The user's job code
workforce_id	VARCHAR(4000)	The user's workforce ID
cost_center	VARCHAR(4000)	The user's cost center
cost_center_description	VARCHAR(4000)	The description of the user's cost center
employee_status	VARCHAR(4000)	The user's employee status
employee_type	VARCHAR(4000)	The user's employee type
company	VARCHAR(4000)	The company
department_number	VARCHAR(4000)	The department number
mailstop	VARCHAR(4000)	The mailstop
office_number	VARCHAR(4000)	Physical Delivery Office Name
street_address	VARCHAR(4000)	The street address
city	VARCHAR(4000)	The city
postal_code	VARCHAR(4000)	The postal code

po_box	VARCHAR(4000)	The PO box
fax_number	VARCHAR(4000)	The FAX number
state	VARCHAR(4000)	The state the user resides in
country	VARCHAR(4000)	The country the user resides in
pager_number	VARCHAR(4000)	The user's pager number
manager_flag	bool	TRUE if this user is a manager and FALSE otherwise
manager_workforce_id	VARCHAR(4000)	The workforce ID of this user's manager
hire_date	TIMESTAMP WITH TIME ZONE	The date this user was hired
transfer_date	TIMESTAMP WITH TIME ZONE	The date this user was transferred
termination_date	TIMESTAMP WITH TIME ZONE	The date this user's employment was terminated
first_working_day	TIMESTAMP WITH TIME ZONE	The user's first working day
last_working_day	TIMESTAMP WITH TIME ZONE	The user's last working day
identity_desc	VARCHAR(4000)	
idmrpt_syn_state	int2	

12.19 idmrpt_ms_identity_v

Stores application identity profile information

ms_identity_id	VARCHAR(32)	The auto-generated application identity identifier
first_name	VARCHAR(4000)	The identity first name
ms_uuid	VARCHAR(4000)	The application UUID
ms_acct_id_value	VARCHAR(4000)	The application account ID value
identity_id	VARCHAR(32)	The application UUID
ms_identity_identifier	VARCHAR(128)	application identity identifier
last_name	VARCHAR(4000)	identity last name
middle_initial	VARCHAR(4000)	identity middle name
full_name	VARCHAR(4000)	identity full name
job_title	VARCHAR(4000)	job title
department	VARCHAR(4000)	
location	VARCHAR(4000)	
email_address	VARCHAR(4000)	

office_phone	VARCHAR(4000)	
cell_phone	VARCHAR(4000)	
private_phone	VARCHAR(4000)	
im_id	VARCHAR(64)	instant messanger id.
photo	TEXT(2147483647)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
generational_qualifier	VARCHAR(8)	
prefix	VARCHAR(4000)	
preferred_name	VARCHAR(4000)	
preferred_language	VARCHAR(8)	
job_code	VARCHAR(4000)	
workforce_id	VARCHAR(4000)	
cost_center	VARCHAR(4000)	
cost_center_description	VARCHAR(4000)	
employee_status	VARCHAR(4000)	
employee_type	VARCHAR(4000)	
company	VARCHAR(4000)	
department_number	VARCHAR(4000)	
mailstop	VARCHAR(4000)	
office_number	VARCHAR(4000)	Physical Delivery Office Name
street_address	VARCHAR(4000)	
city	VARCHAR(4000)	
postal_code	VARCHAR(4000)	
state	VARCHAR(4000)	
country	VARCHAR(4000)	
pager_number	VARCHAR(4000)	
manager_flag	bool	
manager_workforce_id	VARCHAR(4000)	
hire_date	TIMESTAMP WITH TIME ZONE	
transfer_date	TIMESTAMP WITH TIME ZONE	
termination_date	TIMESTAMP WITH TIME ZONE	
first_working_day	TIMESTAMP WITH TIME ZONE	

last_working_day	TIMESTAMP WITH TIME ZONE	
identity_desc	VARCHAR(4000)	
idmrpt_deleted	bool	
idmrpt_syn_state	int2	

12.20 idmrpt_idv_v

Stores the set of Identity Vaults that participate in data collection for the reporting warehouse.

idv_id	VARCHAR(32)	The ID for this Identity Vault in the resporting warehouse
idv_guid	VARCHAR(255)	The GUID of this Identity Vault on the Identity Vault
idv_name	VARCHAR(256)	The name of this Identity Vault
data_locale	VARCHAR(16)	The locale the reporting tool will use when collecting data from this database.
idv_desc	VARCHAR(1024)	The description of this Identity Vault
idv_host	VARCHAR(256)	The host address of this Identity Vault

12.21 idmrpt_idv_acct_v

Contains information about the accounts in all of the Identity Vaults the reportings warehouse is collecting data about.

idv_acct_id	VARCHAR(32)	The unique ID for this account in the reporting warehouse
identity_id	VARCHAR(32)	The ID of the account in the Identity Vault
idv_acct_dn	VARCHAR(255)	The DN of the account in the identity vault
idv_acct_guid	VARCHAR(64)	The GUID of the account in the Identity Vault
idv_acct_status	CHAR(1)	The status of the account in the Identity Vault
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date the account was made active
idmrpt_deleted	bool	TRUE if the account was deleted and FALSE otherwise
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this account
idmrpt_syn_state	int2	The synchronized state of this account.

12.22 idmrpt_idv_drivers_v

Contains information about the driver configured in the Identity Vault connected tot he reporting warehouse.

idv_id	VARCHAR(32)	The ID of the Identity Vault containing this driver
idv_driver_id	VARCHAR(32)	The automatically generated unique ID of this driver in the reporting warehouse
drv_dn	VARCHAR(255)	The DN of the driver
drv_guid	VARCHAR(64)	The GUID of the driver
drv_name	VARCHAR(128)	The name of the driver
idmrpt_valid_from	TIMESTAMP WITH TIME ZONE	The date the driver was created
idmrpt_deleted	bool	
idmrpt_syn_state	int2	The sync state of this driver

12.23 idmrpt_idv_ent_v

Stores information about the entitlements available in the Identity Vaults.

idv_id	VARCHAR(32)	The ID of the Identity Vault containing this entitlement
idv_ent_id	VARCHAR(32)	The automatically generated ID for this entitlement
idv_driver_id	VARCHAR(32)	The ID of the driver containing this entitlement
idmrpt_ent_dn	VARCHAR(255)	The DN of this entitlement
idmrpt_ent_guid	VARCHAR(64)	The GUID of this entitlement
idmrpt_ent_name	VARCHAR(4000)	The name of this entitlement
idmrpt_ent_desc	VARCHAR(4000)	The description of this entitlement
idmrpt_ent_type_id	VARCHAR(32)	The ID of this type for this entitlement
idmrpt_ent_type_name	VARCHAR(512)	The name of the type of this entitlement
idm_ent_param_format	VARCHAR(32)	The format of the parameter of this entitlement
idmrpt_valid_from	TIMESTAMP WITH TIME ZONE	The date this entitlement record is valid from
idmrpt_deleted	bool	TRUE if this entitlement has been deleted and false otherwise
idmrpt_syn_state	int2	The sync state of this entitlement

12.24 idmrpt_idv_ent_bindings_v

Contains information about the Identity Vault entitlement bindings

binding_id	VARCHAR(32)	The unique ID for this entitlement binding
ent_id	VARCHAR(32)	The ID for this entitlement
cat_item_id	VARCHAR(32)	The ID for the category of this entitlement
cat_item_type_id	VARCHAR(32)	The ID of the category type.
ent_param_str	VARCHAR(4000)	The parameter for this entitlement
ms_ent_id	VARCHAR(128)	
ms_id	VARCHAR(32)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this entitlement is valid from
idmrpt_deleted	bool	TRUE if this entitlement has been deleted and false otherwise
ent_src	VARCHAR(64)	The type of the source of the entitlement
ent_param_val	VARCHAR(4000)	The parameter value
idmrpt_syn_state	int2	The sync state for this entitlement
ent_param_id	VARCHAR(512)	
ent_param_id2	VARCHAR(512)	
ent_param_liid	VARCHAR(512)	
ent_corr_id	VARCHAR(512)	

12.25 idmrpt_idv_identity_trust_v

Contains role, resource, and group identity assignment information.

trust_id	VARCHAR(32)	The ID of this relationship
identity_id	VARCHAR(32)	The ID of the Identity Vault containing this assignment
trust_obj_id	VARCHAR(32)	The ID of the trust object
trust_type_id	VARCHAR(32)	The type of assignment this is. For example, ROLE_ASSIGNMENT, RESOURCE_ASSIGNMENT, or GROUP_ASSIGNMENT
trust_status	int2	The status of the trust relationship
requester_id	VARCHAR(32)	The ID of the requester of this resource
request_date	timestamptz	The date the request was made
request_comment	VARCHAR(4000)	The comment with the request

cause	VARCHAR(4000)	The cause for the grant of this request. For example, role request
cause_type	VARCHAR(4000)	The cause type for the grant of this request. For example, explicit, container, or group.
approval_info	VARCHAR(4000)	
trust_params	VARCHAR(4000)	
idv_ent_id	VARCHAR(32)	
idv_ent_ref	VARCHAR(4000)	
ms_ent_id	VARCHAR(32)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
trust_start_time	TIMESTAMP WITH TIME ZONE	
trust_expiration_time	TIMESTAMP WITH TIME ZONE	
idmrpt_syn_state	int2	

12.26 idmrpt_idv_prd_v

Contains a list of the provisioning request definitions contained in all the Identity Vaults connected to the reporting warehouse

idv_id	VARCHAR(32)	The ID of the Identity Vault containing this PRD
prd_id	VARCHAR(32)	The unique ID of this PRD in the reporting warehouse.
prd_guid	VARCHAR(64)	The GUID of the PRD in the Identity Vault
prd_dn	VARCHAR(256)	The DN of the PRD
prd_name	VARCHAR(4000)	The display name of the PRD
prd_desc	VARCHAR(4000)	The description of the PRD.
idmrpt_deleted	bool	TRUE if this PRD has been delete from the Identity Vault and FALSE otherwise
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this PRD was valid on
idmrpt_syn_state	int2	The sync state of this PRD

12.27 idmrpt_idv_trust_types_v

Stores the Identity Vault trust types. This view is a fixed list of types and is populatd during the initial installation or upgrade of the reporting warehouse.

trust_type_id	VARCHAR(32)	The ID for this trust type. For example, ROLE_ASSIGNMENT, RESOURCE_ASSIGNMENT, or GROUP_ASSIGNMENT.
trust_type_name	VARCHAR(128)	The display name of this trust type.
trust_type_descr	VARCHAR(512)	The description of this trust type.
idmrpt_deleted	bool	TRUE if this trust type has been deleted and FALSE otherwise.

12.28 idmrpt_container_types_v

table that stores allowable container types that are synced from the idv.

container_type_id	VARCHAR(32)	
naming_attr	VARCHAR(32)	
object_class	VARCHAR(512)	
idmrpt_deleted	bool	

12.29 idmrpt_ms_v

Contains information about managed systems the reporting information is collecting data from.

ms_id	VARCHAR(32)	The uniqeu ID for this managed system in the reporting warehouse
ms_logical_id	VARCHAR(4000)	The logical ID of this managed system
ms_collect_id	VARCHAR(32)	The collection ID of this managed system.
ms_uuid	VARCHAR(4000)	
ms_idm_driver	VARCHAR(4000)	
ms_name	VARCHAR(4000)	
ms_descr	VARCHAR(4000)	The description of this managed system
ms_bus_owner	VARCHAR(32)	The ID of the business owner of this managed system
ms_app_owner	VARCHAR(32)	The ID of the application owner of this managed system
ms_domain	VARCHAR(4000)	The domain host address of this managed system
ms_type	VARCHAR(4000)	The type of this managed system. For example, Active Directory
ms_classification	VARCHAR(4000)	The classification of this managed system. For example, windows
ms_location	VARCHAR(4000)	The physical location of this managed system

ms_environment	VARCHAR(4000)	The operating system of this managed system
ms_conn_ip	VARCHAR(255)	The IP address of this managed system
ms_conn_auth_id	VARCHAR(255)	The ID used when connecting to the managed system
ms_conn_port	int4	The port used when connecting to this managed system
ms_vendor	VARCHAR(256)	The vendor of this managed system
ms_version	VARCHAR(128)	The version of this managed system
ms_hierarchical	bool	
ls_name	VARCHAR(4000)	
ls_descr	VARCHAR(4000)	
ls_bus_owner	VARCHAR(32)	
ls_app_owner	VARCHAR(32)	
ls_type	VARCHAR(4000)	
ls_classification	VARCHAR(4000)	
ls_location	VARCHAR(4000)	
ls_environment	VARCHAR(4000)	
ls_conn_ip	VARCHAR(255)	
ls_conn_auth_id	VARCHAR(255)	
ls_conn_port	int4	
ls_vendor	VARCHAR(256)	
ls_version	VARCHAR(128)	
ls_hierarchical	bool	
idmrpt_deleted	bool	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_syn_state	int2	

12.30 idmrpt_ms_acct_v

table that stores managed system accounts

identity_id	VARCHAR(32)

acct_id_type	VARCHAR(128)	an account might have login id's or unique account identifiers per application. this field indicates the type of login id or account identifier that is used in the account identifier field. e.g, in active directory accounts can be identified by and users can login using the samaccountname attribute, the userprincipalname attribute or its object * distinguished name* (dn).
ms_acct_global_identifier	VARCHAR(4000)	unique identifier of account in ms (provides ability to link all accounts)
acct_id_value	VARCHAR(4000)	the identifier that uniquely identifies this account in an application. an account might have multiple unique identifiers per application. e.g. in active directory an account is identified by its samaccountname, userprincipalname and ldap dn. and in the idm world the account is known by its association.
acct_status	CHAR(1)	status of the account (if applicable: active, inactive, disabled)active (a), inactive (i), or undefined (u)
acct_type	VARCHAR(32)	account type string (not used) : regular, admin, elevated, ...
idv_managed	bool	boolean flag, if set to true - means account is managed by IDM and idv association is not disabled
idv_ms_app_name	VARCHAR(4000)	IDV name for managed systenm application
idv_association	VARCHAR(256)	the IDV accoutnt Association
idv_acct_id	VARCHAR(32)	the IDV accoutnt id, nullable fk to idv acct table
idv_sync	bool	boolean flag, if set to true - means account is synchronied in IDV and MS
ms_idv_acct_status	CHAR(1)	status of the account ms account according to idv record
ms_id	VARCHAR(32)	
ms_ent_type_id	VARCHAR(32)	
ms_acct_id	VARCHAR(32)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
idmrpt_syn_state	int2	

12.31 idmrpt_ms_acct_rule_v

ms_uuid	VARCHAR(4000)

acct_rule	int4
match_attr_name	VARCHAR(256)
ext_attr	bool
attr_rule_id	VARCHAR(32)
idmrpt_deleted	bool
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_syn_state	int2

12.32 idmrpt_ms_collector_v

idmrpt_ms_collector contains information about the connected systems. This is the data that drives the Identity Vaults page in the reporting tool. These connected systems are used to collect reporting data.

ms_collect_id	VARCHAR(32)	The unique id for the collector
collect_name	VARCHAR(4000)	The name of the collector
collect_port	int4	The port for connecting to the collector
collect_host	VARCHAR(64)	The host name of the collector
collect_context	VARCHAR(32)	The context for the collector
collect_protocol	VARCHAR(8)	The protocol for the collector. Values: http, hhtps
collect_acct	VARCHAR(128)	The account name used to connect to the collector
collector_pswd	VARCHAR(128)	The password used for connecting to this collector
collect_cert	bytea	The optional certificate used when connecting to this collector. This is only used for SSL.
collect_desc	VARCHAR(4000)	The description of the collector
data_locales	VARCHAR(255)	The locales to use when collecting data from this collector. Locale data is available in the managed system.(coma separated list).
last_collect_date	TIMESTAMP WITH TIME ZONE	The last date data was collected from this collector
next_collect_date	timestamptz	The next date data will be collected from this collector
collect_type	int2	The type of the pooling collector: 1 -idm engine rest endpoint collector 2 - enterprize application collector

collect_state	int2	The current state of the collection operation. Possible states are: 0- uninitialized, 1 - initialized, 2 - active, 3-running, 4 - suspended, 5- deleted
ms_cert_info	VARCHAR(4000)	The public information about the certificate including the certificate name and file name.
idmrpt_deleted	bool	TRUE if this collector has been deleted and FALSE otherwise

12.33 idmrpt_ms_ent_v

Stores managed system entitlement values. This table does not contain managed system accounts.

ms_id	VARCHAR(32)	The managed system UUID
ent_type_id	VARCHAR(32)	The entitlement type UUID
ms_ent_id	VARCHAR(32)	They auto-generated entitlement value UUID
ms_ent_val	VARCHAR(4000)	
idv_ent_param_val	VARCHAR(4000)	The corresponding Identity Vault entitlement parmeter value string
idv_ent_pt_id2	VARCHAR(4000)	The corresponding Identity Vault entitlement parmeter ID token value
idv_ent_pt_liid	VARCHAR(4000)	The corresponding Identity Vault entitlement parmeter LIID token value
ms_ent_desc	VARCHAR(4000)	
ms_ent_val_disp_name	VARCHAR(4000)	The entitlement value display name
idmrpt_deleted	bool	
entitlement_sub_type	VARCHAR(4000)	The entitlement sub type
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_syn_state	int2	

12.34 idmrpt_ms_ent_type_v

idv_ent_dn	VARCHAR(256)	Identifier of entitllement type within idv (entitlement dn for connected system queried through REST API)
idv_ent_id	VARCHAR(32)	Nullable foreing key to idmrpt_idv_ent.ent_ id.
ent_type	VARCHAR(256)	Managed system entitlement type key (MS_ENT_TYPE).
ms_ent_type_uuid	VARCHAR(256)	Managed system entitlement type id key (MS_ENT_TYPE_ID).

ms_ent_type_cat	VARCHAR(256)	Managed system entitlement type category key (MS_ENT_CATEGORY).
ms_ent_type_name	VARCHAR(4000)	Managed system entitlement type display name.
ms_ent_name	VARCHAR(4000)	Managed system entitlement description name.
ms_ent_desc	VARCHAR(4000)	Managed system entitlement description name.
ms_ent_type_id	VARCHAR(32)	
ms_uuid	VARCHAR(4000)	Managed system uuid (managed system driver uuid), that this entitlement type belongs to.
idmrpt_deleted	bool	
idmrpt_syn_state	int2	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	

12.35 idmrpt_ms_ent_trust_v

table that contains information about managed system entitlement assignments, excluding accounts

trustee_id	VARCHAR(32)	nullable foreing key, that points to trustee id (either idmrpt_ms_identity.identity_id or idmrpt_ms_ent.ms_ent_id
trustee_type_id	VARCHAR(32)	
ms_ent_trustee_idv_assoc	VARCHAR(256)	
ms_ent_trustee_identifier	VARCHAR(4000)	
ms_ent_id	VARCHAR(32)	
ms_id	VARCHAR(32)	
ms_ent_type_id	VARCHAR(32)	
ms_trust_id	VARCHAR(32)	
trust_status	int2	not used for now, reserved for the future: 1-grant, 0 -revoke, 2 -deactivated
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
idmrpt_syn_state	int2	

12.36 idmrpt_owners_v

ownership_id	VARCHAR(32)
cat_item_id	VARCHAR(32)
cat_item_type_id	VARCHAR(32)
owner_id	VARCHAR(32)
owner_dn	VARCHAR(255)
owner_type	VARCHAR(32)
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_deleted	bool
idmrpt_syn_state	int2

12.37 idmrpt_res_parameter_v

Stores resource parameters. It excludes code map keys because it is runtime only.

param_id	VARCHAR(32)
res_id	VARCHAR(32)
param_key	VARCHAR(128)
param_disp_name	VARCHAR(4000)
hidden	bool
static_param	bool
param_type	VARCHAR(32)
param_value	VARCHAR(4000)
idv_ent_id	VARCHAR(32)
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_deleted	bool
idmrpt_syn_state	int2

12.38 idmrpt_resource_v

Stores Identity Vault resource catalog information

res_id	VARCHAR(32)	The unique ID of this resource in the resporting warehouse
res_dn	VARCHAR(255)	The DN of the resource

res_guid	VARCHAR(64)	The GUID of this resource in the Identity Vault
res_name	VARCHAR(4000)	The name of this resource
res_desc	VARCHAR(4000)	The description of this resource
grant_approval_prd	VARCHAR(255)	The PRD used to grant approval for this resource
revoke_approval_prd	VARCHAR(255)	The PRD used to remove approval for this resource
grant_quorum	VARCHAR(8)	The quorum percentage required to grant access to this resource
revoke_quorum	VARCHAR(8)	The quorum percentage required to revoke the access to this resource
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this resource is valid from
idmrpt_deleted	bool	TRUE if this resource has been deleted and FALSE otherwise
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this resource
idmrpt_syn_state	int2	The sync state of this resource

12.39 idmrpt_role_v

Contains all of the roles in all of the Identity Vaults connected to the reporting tool

role_id	VARCHAR(32)	The ID of this role in this reporting warehouse
role_dn	VARCHAR(255)	The DN of this role
role_guid	VARCHAR(64)	The GUID of this role in the Identity Vault
role_name	VARCHAR(4000)	The name of this role
role_desc	VARCHAR(4000)	The description of this role
approval_prd	VARCHAR(255)	The PRD used to grant this role
quorum	VARCHAR(8)	The quorum percentage required to gain access to this role
role_level	int2	The level of this role. The levels are 10, 20, or 30
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this role is valid from
idmrpt_deleted	bool	TRUE if this value is deleted and FALSE otherwise
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this role
idmrpt_syn_state	int2	The sync state of this role

12.40 idmrpt_role_level_v

Stores information about available role levels in the Identity Vaults connected to the reporting warehouse.

role_level	int2	The role level. This is a number of 10, 20, and 30
role_level_name	VARCHAR(255)	The name of the role level
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this role level was made valid
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this role level
idmrpt_syn_state	int2	The sync state of this role level
role_level_id	VARCHAR(32)	The ID for this role level

12.41 idmrpt_role_mappings_v

Stores parent-child roles and implicit assignments

role_id	VARCHAR(32)	
mapped_id	VARCHAR(32)	
info	VARCHAR(4000)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
mapping_id	VARCHAR(32)	
mapped_id_type	VARCHAR(32)	mapped item type uuid based on catalog item type. if item type points to role, than it is a child role.
idmrpt_syn_state	int2	

12.42 idmrpt_role_res_assoc_v

table that stores role to resource associations

role_id	VARCHAR(32)
res_id	VARCHAR(32)
assoc_dn	VARCHAR(255)
assoc_guid	VARCHAR(64)
idv_id	VARCHAR(32)
association_id	VARCHAR(32)

assoc_desc	VARCHAR(4000)
assoc_status	int2
aproval_override	bool
idmrpt_deleted	bool
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_syn_state	int2

12.43 idmrpt_role_res_assoc_param_v

table that stores role to resource association dynamic parameter values

assoc_param_id	VARCHAR(32)
assoc_id	VARCHAR(32)
param_value	VARCHAR(4000)
param_key	VARCHAR(128)
idmrpt_deleted	bool
idmrpt_valid_from	TIMESTAMP WITH TIME ZONE
idmrpt_syn_state	int2

12.44 idmrpt_rpt_driver_v

Represents the registry of data collection drivers per Identity Vault

idv_id	VARCHAR(32)	The ID of the Identity Vault containing this driver
rpt_drv_id	VARCHAR(32)	The ID of this driver
drv_dn	VARCHAR(255)	The DN of this driver
drv_guid	VARCHAR(64)	The GUID of this driver in the Identity Vault
drv_name	VARCHAR(256)	The name of this driver
data_locale	VARCHAR(16)	The locale used when collecting data from this driver
collect_events	bool	Flag that determines if the driver collector is ready to start receiving events from the data collection driver. By default this will be true.
collector_id	VARCHAR(32)	The ID of this collector
drv_desc	VARCHAR(1024)	The description of this driver
drvset_guid	VARCHAR(64)	The GUID of the driver set containing this driver

12.45 idmrpt_rpt_driver_scope_v

Stores the scope for all data collection drivers per Identity Vault, driver to enforce not inteceting scopes within one Identity Vault.

idv_id	VARCHAR(32)	The ID of the Identity Vault
rpt_drv_id	VARCHAR(32)	The ID of the data collection driver
driver_scope	VARCHAR(255)	The scope of the driver

12.46 idmrpt_sod_v

Catalog of separation of duties information

sod_id	VARCHAR(32)	The unique ID of this SOD in the reporting warehouse
sod_dn	VARCHAR(255)	The DN of this SOD
sod_guid	VARCHAR(64)	The GUID of this SOD in the Identity Vault
idv_id	VARCHAR(32)	The ID of the Identity Vault containing this SOD
role_id_1	VARCHAR(32)	
role_id_2	VARCHAR(32)	
sod_name	VARCHAR(4000)	The name of this SOD
sod_desc	VARCHAR(4000)	The description of the SOD
sod_approval_type	int2	The approval type of this SOD
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	The date this SOD became valid
idmrpt_deleted	bool	TRUE if this SOD has been deleted and FALSE otherwise
idmrpt_syn_state	int2	The sync state of this SOD
custom_appr	bool	TRUE if this SOD is a custom approval type and false otherwise

12.47 idmrpt_sod_violations_v

Stores approved separation of duties violations for identities

sod_id	VARCHAR(32)
identity_id	VARCHAR(32)
approval_date	TIMESTAMP WITH TIME ZONE
approval_info	VARCHAR(4000)

idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE
idmrpt_deleted	bool
sod_violation_id	VARCHAR(32)
justification	VARCHAR(4000)
idmrpt_syn_state	int2

12.48 idmrpt_approval_v

Information about the approval activities for resource and role assignments as well as separation of duties exceptions.

approval_id	VARCHAR(32)	
identity_id	VARCHAR(32)	
item_type_id	VARCHAR(32)	
item_id	VARCHAR(32)	
approval_date	TIMESTAMP WITH TIME ZONE	
approval_type	int2	approval type; grant? 1, revoke 2, grant & revoke 3
action	VARCHAR(16)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
idmrpt_syn_state	int2	

12.49 idmrpt_team_v

Stores Roles Based Provisioning Module team definitions

team_id	VARCHAR(32)
idv_id	char(32)
team_type	VARCHAR(8)
team_dn	VARCHAR(255)
team_guid	VARCHAR(64)
team_name	VARCHAR(4000)
team_desc	VARCHAR(4000)
manager_not_member	bool
team_all_users	bool

team_memb_relationship	VARCHAR(128)	
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
idmrpt_syn_state	int2	

12.50 idmrpt_team_assignments_v

Stores the roles based provisioning module team member and manager assignments

team_id	VARCHAR(32)	
assigned_id	VARCHAR(32)	
assigned_id_type	VARCHAR(32)	
assignment_type	int2	type of assignments: 1 - member, 2 - manager
idmrpt_valid_from	TIMESTAMP WITHOUT TIME ZONE	
idmrpt_deleted	bool	
assignment_id	VARCHAR(32)	
idmrpt_syn_state	int2	

13 REST Services for Reporting

This section provides instructions for using the REST services provided with the Identity Reporting Module.

- Section 13.1, “Overview of the REST Services for Reporting,” on page 207
- Section 13.2, “Non-Managed Application REST API,” on page 207
- Section 13.3, “Authentication REST API,” on page 224
- Section 13.4, “Reporting REST API,” on page 229

13.1 Overview of the REST Services for Reporting

The Identity Reporting Module provides support for three REST APIs:

- Non-Managed Application REST API
- Authentication REST API
- Reporting REST API

These APIs are described below.

13.2 Non-Managed Application REST API

This API allows you to implement a REST endpoint for a non-managed application. A non-managed application is an application that is not connected to an Identity Vault, but nonetheless includes data that you want to be able to report on. By defining a REST endpoint for an application, you make it possible for the reporting module to collect data from this application.

After you have defined the REST endpoint for a non-managed application, you need to provide details about this application, including its location and context, on the Non-Managed Application Data Sources page in the reporting module.

Managed System Prefix: The REST API described in this section is also used by the reporting module to perform data queries for managed systems, so some of the URIs use the prefix “ms”, which refers to managed systems.

Logical system identifier: Some of the URIs include a parameter for logical system identifier. This is an identifier for the instance of a managed system.

NOTE: In Identity Manager 4.0.2 and later, you must define at least one logical system for the reporting module to be able to collect data from the application. The reporting module no longer collects data from the primary system.

- Section 13.2.1, “Overview,” on page 208
- Section 13.2.2, “Generic Service APIs,” on page 208

13.2.1 Overview

These APIs use an asynchronous *Query* architecture. The Identity Manager Reporting Service will call the various *Query* APIs and expect to receive a unique `REQID` field value in response. This `REQID` field value will be passed in a subsequent call to determine if the requested data Results are available, obtain the Results set, and ultimately to purge the `REQID` and associated Results data. It is the responsibility of the application service to create and cache the unique `REQID` fields and associated data until a request is made to purge the data.

A JSON (Java Script Object Notation) interface is used for all APIs. Ensure that the Content-Type in the headers for all HTTP messages is “application/json” when testing application service implementations.

NOTE: All PUT operations require a content payload. For some APIs, this may simply be an empty payload "{ }".

13.2.2 Generic Service APIs

These APIs are used by the Identity Manager Reporting Service during the processing of the various data collection *query* activities.

GET – /results/<requestID>/status

Verifies the result status after data collection. The identifier is a request identifier obtained when the *query* API is invoked.

The REQID value returned from a preceding data collection query API call is used in the URI to identify the request whose status is being obtained.

URI

```
context/results/requestID/status
```

HTTP Method

This operation supports the GET method.

Input

None.

Output

STATUS: A *Boolean* flag that indicates if the result set is ready to be consumed. If the value returned is `false`, subsequent calls can be expected.

Sample Output

```
{"STATUS":"true"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /purge

This API is used to inform the application service that the results set associated with the REQID will no longer be accessed and can be released.

URI

context/purge

HTTP Method

This operation supports the PUT method.

Input

REQID: *String* (mandatory)

Sample Input

```
{"REQID":"5ac00e5660ec435aae966ca2975b98f3"}
```

Output

SUBMITTED: A *Boolean* flag that indicates if the purge request was received.

Sample Output

```
{"SUBMITTED":"true"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)
- 500: Internal Application Service failure

13.2.3 Managed System Information APIs

These APIs are used to request and obtain the Managed System information of the non-managed application. The supported fields for the Results objects can be found under Section A.3, "Managed System Information Schema," on page 308.

PUT – /ms

Returns a list of the applications and managed systems that are available for data collection. This operation also provides the attributes for each application.

URI

`context/ms`

HTTP Method

This operation supports the PUT method.

Input

Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{"Locale":"EN"}
```

Output

REQID

Sample Output

```
{"REQID":"5ac00e5660ec435aae966ca2975b98f3"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

PUT – /ms/results

Retrieves the results of system query execution.

If the application service provides connectivity to more than 1 application instance, each instance is considered a Logical System to the Identity Manager Reporting Service. For each Logical System, the application service must return a Results instance.

The GUID value returned will be used as the application identifier in the URI of subsequent data collection API calls from the Identity Manager Reporting Service. If there are no Logical Systems identified by the application service, the same value will be used as the *ls-identifier* in those calls. Otherwise, the LogicalInstance:ID values will be used as the *ls-identifier* in those calls.

URI

`context/ms/results`

HTTP Method

This operation supports the PUT method.

Input Fields

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{"REQID":"5ac00e5660ec435aae966ca2975b98f3"}
```

Output

Results Payload (see Section A.1, “Results Payload Schema,” on page 307 and Section A.3, “Managed System Information Schema,” on page 308)

Sample Output (No Logical Systems)

```
{
  "SIDX":0,"EIDX":1,"MORE":0,
  "Results":
  [
    {
      "GUID":"SAPUM-151.155.161.8-300",
      "Name":"SAP DEV Central",
      "Description":"SAP CUA Central Development Server",
      "Type":"Enterprise",
      "Classification":"Development",
      "Vendor":"SAP",
      "Version":"Basis 700",
      "BusinessOwner":"Mark Jeffrey",
      "ApplicationOwner":"HCM-ADMIN",
      "Location":"Provo QA Lab, PRV-H-622",
      "Environment":"Development",
      "AuthenticationIPAddress":"151.155.161.8",
      "AuthenticationPort":"sapgw00",
      "AuthenticationID":"admin",
      "Hierarchical":"false"
    }
  ]
}
```

Sample Output (2 Logical Systems)

```
{
  "SIDX":0,"EIDX":2,"MORE":0,
  "Results":
  [
    {
      "GUID":"SAPUM-151.155.161.8",
      "Name":"SAP DEV",
      "Description":"SAP CUA Development Server",
      "Type":"Enterprise",
      "Classification":"Development",
      "Vendor":"SAP",
      "Version":"Basis 700",
      "BusinessOwner":"Mark Jeffrey",
      "ApplicationOwner":"ADMIN",
      "Location":"Provo QA Lab, PRV-H-622",
      "Environment":"Development",
      "AuthenticationIPAddress":"192.168.1.10",
      "AuthenticationPort":"sapgw00",
      "AuthenticationID":"ADMIN",
      "Hierarchical":"false",
      "LogicalInstance:ID":"ADMCLNT300",
      "LogicalInstance:Name":"Client 300",
      "LogicalInstance:Description":"CUA Central Client",
      "LogicalInstance:Type":"Enterprise",
      "LogicalInstance:Classification":"Development",
      "LogicalInstance:Vendor":"SAP",
      "LogicalInstance:Version":"Basis 700",
      "LogicalInstance:BusinessOwner":"Mark Jeffrey",
      "LogicalInstance:ApplicationOwner":"CUAADMIN",
      "LogicalInstance:Location":"Provo QA Lab, PRV-H-622",
      "LogicalInstance:Environment":"Development",
      "LogicalInstance:AuthenticationIPAddress":"192.168.1.10",
      "LogicalInstance:AuthenticationPort":"sapgw00",
      "LogicalInstance:AuthenticationID":"CUAADMIN",
      "LogicalInstance:Hierarchical":"false"
    },
    {
      "GUID":"SAPUM-151.155.161.8",
      "Name":"SAP DEV",
      "Description":"SAP CUA Development Server",
      "Type":"Enterprise",
      "Classification":"Development",
      "Vendor":"SAP",
      "Version":"Basis 700",
      "BusinessOwner":"Mark Jeffrey",
      "ApplicationOwner":"ADMIN",
      "Location":"Provo QA Lab, PRV-H-622",
      "Environment":"Development",
      "AuthenticationIPAddress":"192.168.1.10",
      "AuthenticationPort":"sapgw00",
      "AuthenticationID":"ADMIN",
      "Hierarchical":"false",
      "LogicalInstance:ID":"ADMCLNT400",
      "LogicalInstance:Name":"Client 400",
      "LogicalInstance:Description":"CUA Child Client",
      "LogicalInstance:Type":"Enterprise",
      "LogicalInstance:Classification":"Development",
      "LogicalInstance:Vendor":"SAP",
      "LogicalInstance:Version":"Basis 700",
      "LogicalInstance:BusinessOwner":"Jon Doe",
      "LogicalInstance:ApplicationOwner":"CHLDADM",
      "LogicalInstance:Location":"Provo QA Lab, PRV-H-622",
      "LogicalInstance:Environment":"Development",
      "LogicalInstance:AuthenticationIPAddress":"192.168.1.10",
      "LogicalInstance:AuthenticationPort":"sapgw00",
      "LogicalInstance:AuthenticationID":"CHLDADM",
      "LogicalInstance:Hierarchical":"false"
    }
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Result set is empty
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

13.2.4 Account Matching Rules APIs

These APIs are used to request and obtain the a set of matching rules that can be used by the IDM Reporting Service information of the non-managed application. The supported fields for the *Results* objects can be found in Section A.7, “Accounts Rule Schema,” on page 311.

NOTE: In Identity Manager 4.0, these APIs are in a proposal stage in the Identity Manager Reporting Service. Data is collected but is not yet used.

PUT – /accounts/rule/ms/<identitifer>

Requests managed and application account rules data.

URI

`context/accounts/rule/ms/identifier`

- *identifier*: Managed System GUID value (see "PUT – /ms/results" on page 210)

HTTP Method

This operation supports the PUT method.

Input

Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{"Locale":"DE"}
```

Output

REQID

Sample Output

```
{"REQID":"e6bf4fd18817449885caa34bd8e84781"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /accounts/rule/ms/<identitifer>/results

Requests system account rules data.

URI

`context/accounts/rule/ms/identifier/results`

- *identifier*: Managed System GUID value (see "PUT – /ms/results" on page 210)

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{
  "REQID":"e6bf4fd18817449885caa34bd8e84781",
  "SIDX":0,
  "SIZE":100
}
```

Output

Results Payload (see Section A.1, “Results Payload Schema,” on page 307 and Section A.7, “Accounts Rule Schema,” on page 311)

Sample Output

```
{
  "SIDX":0,"EIDX":1,"MORE":0,
  "Results":
  [
          {"Order":1, "MatchAttrName":"USERNAME:BAPIBNAME"},
          {"Order":2, "MatchAttrname":"ADDRESS:FIRSTNAME,ADDRESS:LASTNAME"}
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Result set is empty
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

13.2.5 Entitlement Types APIs

These APIs are used to request and obtain the various types of application Entitlements that can be assigned to application identities. Examples of entitlements may be a User account, Roles, User Profiles, Group Memberships, Email access, home directories, and so forth.

The supported fields for the *Results* objects can be found under Section A.4, “Entitlements Types Schema,” on page 310.

PUT – /entitlements/types/ms/<identifier>

Requests entitlement type data for each system.

URI

`context``/entitlements/types/ms/`*`identifier`*

- *identifier*: Managed System Information GUID value (see “PUT – /ms/results” on page 210)

HTTP Method

This operation supports the PUT method.

Input

Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{"Locale":"DE"}
```

Output

REQID

Sample Output

```
{"REQID":"faae9d07cf7f47d5bb7c5179819da9ea"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

PUT – /entitlements/types/ms/<identifier>/results

Retrieves the results of query execution for entitlement types.

URI

`context/entitlements/types/ms/identifier/results`

- *identifier*: Managed System Information GUID value (see “PUT – /ms/results” on page 210)

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{
  "REQID":"faae9d07cf7f47d5bb7c5179819da9ea",
  "SIDX":0,
  "SIZE":20
}
```

Output

Results Payload (see Section A.1, “Results Payload Schema,” on page 307 and Section A.7, “Accounts Rule Schema,” on page 311)

Sample Output

```
{
  "SIDX":0,"EIDX":3,"MORE":0,
  "Results":
  [
    {
      "ENT_TYPE":"ActivityGroup",
      "ENT_TYPE_DISPLAY_NAME":"Rolle",
      "ENT_ID":"AG",
      "ENT_CATEGORY":"Sicherheit Gruppe",
      "ENT_DESCRIPTION":"SAP Rolle",
      "ENT_DISPLAY_NAME":"Rolle"
    },
    ...
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Result set is empty
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

13.2.6 Entitlements Information APIs

These APIs are used to request and obtain detailed information about all Entitlements of the non-managed application. The supported fields for the *Results* objects can be found under Section A.5, “Entitlements Information Schema,” on page 310.

PUT – /entitlements/ms/<identifier>/ls/<ls-identifier>

Requests application entitlement data.

URI

context/entitlements/ms/*identifier*/ls/*ls-identifier*

- *identifier*: Managed System Information *GUID* value (see “PUT – /ms/results” on page 210)
- *ls-identitifer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see “PUT – /ms/results” on page 210).

HTTP Method

This operation supports the PUT method.

Input

- ENT_ID: *String (mandatory)*. Identifies the type of Entitlement information being obtained from the target application or logical systems. The value will be the ENT_ID from one of the entitlement types previously collected from the application service.
- Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{
  "ENT_ID":"AG",
  "Locale":"EN"
}
```

Output

REQID

Sample Output

{"REQID":"f8977b3bdce34b3f8e2e44ff10567746"}

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /entitlements/ms/<identifier>/ls/<ls-identifier>/results

Some entitlements, such as a User account entitlement, may not be represented by an actual application object or value. Such entitlements are considered granted based on the presence of an account for a User. It is therefore appropriate for an application to return an empty results set for non-valued entitlements.

URI

`context/entitlements/ms/identifier/ls/ls-identifier/results`

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identititfer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{"REQID":"f8977b3bdce34b3f8e2e44ff10567746", "SIZE":200}
```

Output

Results Payload (see Section A.1, “Results Payload Schema,” on page 307 and Section A.5, “Entitlements Information Schema,” on page 310)

Sample Output

```
{
  "SIDX":0,"EIDX":200,"MORE":1,
  "Results":
  [
    {
      "MS_ENT_DESC":"Employee Self-Service Germany",
      "MS_ENT_VAL":"SAP_HR_EMPLOYEE_DE",
      "MS_ENT_VAL_DISP_NAME":"SAP_HR_EMPLOYEE_DE"
    },
    {
      "MS_ENT_DESC":"Auth. for RFC Service User in Client System (RFC)",
      "MS_ENT_VAL":"SAP_BC_USR_CUA_CLIENT_RFC",
      "MS_ENT_VAL_DISP_NAME":"SAP_BC_USR_CUA_CLIENT_RFC"
    },
    ....
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Result set is empty
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

13.2.7 Entitlement Assignment APIs

These APIs are used to request and obtain the information about the assignment of a specified Entitlement type to Identities within the non-managed application. The supported fields for the *Results* objects can be found under Section A.6, “Entitlements Assignments Schema,” on page 310.

PUT – /entitlements/assignments/ms/<identifier>/ls/<ls-identifier>

Requests entitlement assignment data.

URI

`context/entitlements/assignments/ms/identifier/ls/ls-identifier`

- *identifier*: Managed System Information *GUID* value (see “PUT – /ms/results” on page 210)
- *ls-identititer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see “PUT – /ms/results” on page 210).

HTTP Method

This operation supports the PUT method.

Input

- ENT_ID: String (mandatory). Identifies the type of Entitlement assignment information being obtained from the target application or logical systems. The value will be the ENT_ID from one of the entitlement types previously collected from the application service.
- Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{
  "ENT_ID":"PROFILE"
}
```

Output

REQID

Sample Output

```
{"REQID":"87d95b44c7bf4db1aafeb54ad840008d"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /entitlements/assignments/ms/<identifier>/ls/<ls-identifier>/results

Some entitlements, such as a User account entitlement, may not be represented by an actual application object or value. Such entitlements are considered granted based on the presence of an account for a User. It is therefore appropriate for an application to return an empty results set for non-valued entitlements.

URI

context/entitlements/assignments/ms/*identifier*/ls/*ls-identifier*/results

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identititfer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
"REQID":"87d95b44c7bf4db1aafeb54ad840008d", "SIZE":100}
```

Output

Results Payload (see Section A.1, "Results Payload Schema," on page 307 and Section A.6, "Entitlements Assignments Schema," on page 310)

Sample Output

```
{
  "SIDX":0,"EIDX":20,"MORE":0,
  "Results":
  [
    {
      "MS_ENT_VAL":"SAP_ALL",
      "MS_MEMBER":"DDIC"
    },
    {
      "MS_ENT_VAL":"S_A.SYSTEM",
      "MS_MEMBER":"DDIC"
    },
    {
      "MS_ENT_VAL":"SAP_ALL",
      "MS_MEMBER":"SENTINEL"
    },
    ...
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Result set is empty
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

13.2.8 Account Information APIs

These APIs are used to request and obtain the Accounts information of the non-managed application. The supported fields for the *Results* objects can be found under Section A.8, "Account Information Schema," on page 311.

NOTE: If the application service does not support the concept of Logical Systems (see Section 13.2.3, "Managed System Information APIs," on page 209), the Identity Manager Reporting Service will use the Managed System *GUID* field value for both *identifier* and *ls-identifier* in the URI.

PUT – /accounts/ms/<identifier>/ls/<ls-identifier>

Requests accounts information for an application.

URI

context/accounts/ms/*identifier*/ls/*ls-identifier*

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identitifer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{"Locale":"EN"}
```

Output

REQID

Sample Output

```
{"REQID":"e6cfbe0747604fa7ad8d20da6abeb203"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /accounts/ms/<identifier>/ls/<ls-identifier>results

Retrieves the results of a query execution for application accounts data.

URI

context/accounts/ms/*identifier*/ls/*ls-identifier*/results

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identitifer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID

- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{"REQID":"e6cfbe0747604fa7ad8d20da6abeb203"}
```

Output

Results Payload (see Section A.1, "Results Payload Schema," on page 307 and Section A.8, "Account Information Schema," on page 311)

Sample Output

```
{
  "SIDX":0,"EIDX":81,"MORE":0
  "Results":
  [
    {
      "ACCT_ID_VALUE":"NSLUSER",
      "ACCT_ID_TYPE":"USER",
      "Managed":"false",
      "APP_NAME":"SAPUM-151.155.161.8-300",
      "Synchronized":"false",
      "ACCT_STATUS":"A"
    },
    ....
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Results set is empty
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

13.2.9 Profile Information APIs

These APIs are used to request and obtain the detailed Identity profile information for all accounts in the non-managed application. The supported fields for the Results objects can be found under Section A.9, "Profile Information Schema," on page 312.

PUT – /profiles/ms/<identifier>/ls/<ls-identifier>

Requests profiles information for an application.

URI

```
context/profiles/ms/identifier/ls/ls-identifier
```

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identititfer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

Locale: *String (optional)*. This field is a 2-character Language ISO code that may be passed by the Identity Manager Reporting Service. The application service is requested to return results in the specified language if possible.

Sample Input

```
{"Locale":"EN"}
```

Output

REQID

Sample Output

```
{"REQID":"23549fc57b924ec1924d978792a2b684"}
```

Return HTTP Status

- 200: Success
- 489: Service Processing failure (see Section A.2, "Fault Status Payload Schema," on page 307)

PUT – /profiles/ms/<identifier>/ls/<ls-identifier>results

Retrieves the results of a query execution for application profiles data.

URI

```
context/profiles/ms/identifier/ls/ls-identifier/results
```

- *identifier*: Managed System Information *GUID* value (see "PUT – /ms/results" on page 210)
- *ls-identitifer*: Managed System Information *LogicalInstance:ID* value (if present) otherwise Managed System Information *GUID* value (see "PUT – /ms/results" on page 210).

HTTP Method

This operation supports the PUT method.

Input

- REQID: *String (mandatory)*. Request ID
- SIDX: *Integer (optional)*. Optional starting index. First result is at index 0.
- SIZE: *Integer (optional)*. Optional number of results in *Results* set.

Sample Input

```
{"REQID":"23549fc57b924ec1924d978792a2b684", "SIZE":200}
```

Output

Results Payload (see Section A.1, "Results Payload Schema," on page 307 and Section A.9, "Profile Information Schema," on page 312)

Sample Output

```
{
  "SIDX":0,"EIDX":81,"MORE":0,
  "Results":
  [
    {
      "ACCT_ID_VALUE":"CNANO",
      "FIRST_NAME":"Chip",
      "LAST_NAME":"Nano",
      "FULL_NAME":"Chip Nano",
      "JOB_TITLE":"Chief Information Officer",
      "CITY":"Provo",
      "EMAIL_ADDRESS":"cnano@novell.com",
      "OFFICE_PHONE":"(555) 555-1223",
      "PREFERRED_LANG":"EN",
      "COST_CENTER":"US1122",
      "COMPANY":"NOVELL",
      "STREET_ADDRESS":"1800 Novell Place",
      "POSTAL_CODE":"84606","
      COUNTRY":"US",
      "SUITE_NUMBER":"Suite 200",
      "STATE":"UT"
    },
    ....
  ]
}
```

Return HTTP Status

- 200: Success
- 204: Results set is empty
- 489: Service Processing failure (see Section A.2, “Fault Status Payload Schema,” on page 307)

13.3 Authentication REST API

If you want to use the Reporting REST API to write custom reporting applications, you need to use the Authentication Service to authenticate before making reporting API calls. This section provides an overview of the authentication process, as well as details on using the Authentication API. For more information on the reporting API, see Section 13.4, “Reporting REST API,” on page 229.

The Authentication Service is a standalone Java Web application that provides the following functions through REST:

- Programmable login and logout functions that return an authentication token to the caller.

  The Authentication Service maintains the status of all issued tokens.
- Token validation

  The Core Service call backs to the Authentication server to validate the token.
- Token revocation/expiration notification

  The token has a fixed expiration, which is not based on user activity. When a token expires, it is removed from the Authentication Service.

13.3.1 POST auth/tokens

Performs a client login in to the Authentication Service. This operation creates an authentication token. It returns a different token each time it is called.

Format JSON, XML

URL Parameters

None.

Request Headers

This operation uses the Authorization request header to specify these values:

- BASIC
- <*credential*>

  The <*credential*> must provide a valid user name and password for authentication.

The Authorization request header must, therefore, look like this:

```
Authorization: BASIC <credential>
```

Return Codes

A successful login operation returns 200, along with the token (specified by the JSON or XML key of "Token").

Here is an example JSON payload:

```
{"Token":"3f597a4d311a3e00..."}
```

Response Headers

None.

Error Codes

If this operation is unsuccessful, it may return one of the following error codes:

- 401 Invalid credentials
- 500 InternalError: Server problem (Receiver)

13.3.2 DELETE auth/tokens{token}

Performs a client logout from the Authentication Service.

Format JSON, XML

URL Parameters

None.

Request Headers

None.

Return Codes

A successful logout operation returns 200.

Response Headers

None.

Error Codes

If this operation is unsuccessful, it may return one of the following error codes:

- 410 Does not exist (occurs if the token has expired, the user has already logged out, or the token never existed)
- 500 InternalError: Server problem (Receiver)

13.3.3 Example

The following Java code example shows you might use the REST APIs to login and logout of the reporting application. In this example, the login operation is followed immediately by a logout operation. You would need to modify this code for your own application:

```
package com.netiq;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.net.URLEncoder;

import org.apache.commons.codec.binary.Base64;
import org.apache.http.HttpEntity;
import org.apache.http.HttpResponse;
import org.apache.http.client.HttpClient;
import org.apache.http.client.methods.HttpDelete;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.impl.client.DefaultHttpClient;
import org.json.JSONException;
import org.json.JSONObject;

public class LoginSample
{
    private static final String BASIC_AUTH = "BASIC";
    private static final String TOKEN_JSON_KEY = "Token";

    public static void main (String args[])
    {


System.out.println("\n\n\n\n===========================================\n\n");
        try {
            doLogin("badmin", "test", "http://localhost:8081/IDMRPT-AUTH/auth/
tokens");
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    private static void doLogin(String user, String pwd, String tsUrl)
        throws IOException, JSONException
    {
        System.out.println("Making login request for " + user + " to server " +
tsUrl);

        HttpClient httpclient = new DefaultHttpClient();

        URL url = new URL(tsUrl);

        HttpPost httppost = new HttpPost(tsUrl);

        httppost.setHeader("Accept", "application/json");
        httppost.setHeader("Accept-Charset", "UTF-8");

        httppost.setHeader("Authorization", BASIC_AUTH + " " +
                           new String(Base64.encodeBase64(new String(user + ":" +
pwd).getBytes("UTF-8"))));

        // Execute the request
        HttpResponse authResponse = httpclient.execute(httppost);

        int status = authResponse.getStatusLine().getStatusCode();
        System.out.println("The server responded with status code: " + status);

        HttpEntity entity = authResponse.getEntity();

        StringBuffer response = new StringBuffer();

        // If the response does not enclose an entity, there is no need
        // to worry about connection release
        if (entity != null) {
            InputStream instream = entity.getContent();
            BufferedReader reader = null;
            try {
                reader = new BufferedReader(new InputStreamReader(instream));
                String line = null;

                while ((line = reader.readLine()) != null) {
                    response.append(line);
                }
            } catch (RuntimeException ex) {
                // In case of an unexpected exception you may want to abort
                // the HTTP request in order to shut down the underlying
                // connection and release it back to the connection manager.
                httppost.abort();
                throw ex;
            } finally {
                // Closing the input stream will trigger connection release
                if (reader != null) {
                    reader.close();
                }
            }

            // When HttpClient instance is no longer needed,
            // shut down the connection manager to ensure
            // immediate deallocation of all system resources
            httpclient.getConnectionManager().shutdown();
        }

        JSONObject obj = new JSONObject(response.toString());
        String token = obj.getString(TOKEN_JSON_KEY);

        System.out.println("The login completed successfully and the server
generated the following token\n\n\t" + token);

        doLogout(token, tsUrl);
    }

    private static void doLogout(String token, String tsUrl)
        throws IOException
    {
       System.out.println("\n\nMaking logout request for " + token + " to server "
+ tsUrl);

        HttpClient httpclient = new DefaultHttpClient();

        URL url = new URL(tsUrl);

        HttpDelete httpdel = new HttpDelete(tsUrl + "/" + URLEncoder.encode(token,
"UTF-8"));

        httpdel.setHeader("Accept", "application/json");
        httpdel.setHeader("Accept-Charset", "UTF-8");
        //httpdel.setHeader("Authorization", request.getHeader("Authorization"));


        // Execute the request
        HttpResponse authResponse = httpclient.execute(httpdel);

        int status = authResponse.getStatusLine().getStatusCode();

        System.out.println("The server responded with status code: " + status);

        // Get hold of the response entity
        HttpEntity entity = authResponse.getEntity();

        StringBuffer authResponseData = new StringBuffer();

        // If the response does not enclose an entity, there is no need
        // to worry about connection release
        if (entity != null) {
            InputStream instream = entity.getContent();
            BufferedReader reader = null;
            try {
                reader = new BufferedReader(new InputStreamReader(instream));

                String line = null;

                while ((line = reader.readLine()) != null) {
                    authResponseData.append(line);
                }
            } catch (RuntimeException ex) {
                // In case of an unexpected exception you may want to abort
                // the HTTP request in order to shut down the underlying
                // connection and release it back to the connection manager.
                httpdel.abort();
                throw ex;
            } finally {
                // Closing the input stream will trigger connection release
                if (reader != null) {
                    reader.close();
                }
            }

            // When HttpClient instance is no longer needed,
            // shut down the connection manager to ensure
            // immediate deallocation of all system resources
            httpclient.getConnectionManager().shutdown();
        }


        System.out.println("The logout was successful and the server responded
with\n\n\t" + authResponseData.toString());


System.out.println("\n\n============================================\n\n\n\n");
    }
}
```

13.4 Reporting REST API

The Reporting REST API provides the ability to write custom reporting applications, as well to create a custom command-line client for automation.

To use the Reporting REST API, you need to follow these steps:

1. Use the Authentication REST API to get an authentication token. For details, see Section 13.3, “Authentication REST API,” on page 224.
2. Carry the token with the Reporting REST API you want to use in the HTTP header. For details, see the appropriate REST API below.
3. Detect token expiration. When the Reporting REST API returns a 401 (even if you carry the token in the request), this means the token has expired. In this case, repeat Step 1 on page 229.
4. When you are done using the Reporting REST APIs, invalidate the token by performing a Logout operation. To do this, issue a DELETE request for the token. For details, see Section 13.3.2, “DELETE auth/tokens{token},” on page 225.

The remainder of this section describes the REST endpoints available for reporting:

- Section 13.4.1, “GET /rpt/definitions,” on page 230
- Section 13.4.2, “POST /rpt/definitions,” on page 232
- Section 13.4.3, “GET /rpt/defintions/<GUID>,” on page 233
- Section 13.4.4, “PUT /rpt/definitions/<GUID>,” on page 236
- Section 13.4.5, “DELETE /rpt/definitions/<GUID>,” on page 238
- Section 13.4.6, “GET /rpt/definitions/<GUID>/rpz,” on page 239
- Section 13.4.7, “GET /rpt/definitions/<guid>/paramdefs/<paramName>,” on page 240
- Section 13.4.8, “POST /rpt/definitions/import,” on page 243
- Section 13.4.9, “GET /rpt/definitions/import/<upload id>,” on page 245
- Section 13.4.10, “DELETE /rpt/definitions/import/<upload id>,” on page 246
- Section 13.4.11, “GET /rpt/definition/<GUID> /sched,” on page 247
- Section 13.4.12, “POST /rpt/definition/<GUID>/sched,” on page 248
- Section 13.4.13, “GET /rpt/definition/<GUID>/sched/<sched GUID>,” on page 251
- Section 13.4.14, “DELETE /rpt/definition/<GUID>/sched/<sched GUID>,” on page 253
- Section 13.4.15, “POST /rpt/definition/<GUID>/sched/<sched GUID>,” on page 254
- Section 13.4.16, “PUT /rpt/definition/<GUID>/sched/<sched GUID>,” on page 256
- Section 13.4.17, “GET /rpt/reports,” on page 257
- Section 13.4.18, “GET /rpt/reports/<report id>,” on page 259
- Section 13.4.19, “GET /rpt/reports/<report id>/file,” on page 261
- Section 13.4.20, “DELETE /rpt/reports/<report id>,” on page 262
- Section 13.4.21, “GET /rpt/calendar,” on page 264
- Section 13.4.22, “GET /rpt/buildinfo,” on page 265
- Section 13.4.23, “GET /rpt/collectors,” on page 266
- Section 13.4.24, “GET /rpt/collectors/<collector id>/config,” on page 268
- Section 13.4.25, “GET /rpt/rptusers/<token>,” on page 269
- Section 13.4.26, “GET /rpt/rptusers/user,” on page 270

13.4.1 GET /rpt/definitions

Gets report definitions.

This operation returns summary information about report definitions. The server sorts the data. The DisplayName and Description are localized based on the Accept-Language HTTP header.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

These URL parameters are required:

- sortBy: The column to sort by. Valid values: DisplayName, Description, Tags. The server validates the value.
- sortOrder: The sort order. Valid values: ASC or DESC. The server validates the value.
- idxFrom: The starting row index. 0 is the first.
- idxTo: The ending row index, inclusive. The server validates that the idxTo value is greater than the idxFrom value.

These URL parameters are optional:

- DisplayName: Specifies a “contains ignore case” filter on DisplayName. When occurring in the URL multiple times, the filter strings are ANDed together.
- Description: Specifies a “contains ignore case” filter on Description. When occurring in the URL multiple times, the filter strings are ANDed together.
- Category: Specifies a “string match ignore case” filter on Category. When occurring in the URL multiple times, the filter strings are ANDed together.

- Tags: Specifies a “string match ignore case” filter on a Tag. When occurring in the URL multiple times, the filter strings are ANDed together.
- LOP: Indicates whether to OR/AND the conditions together. The default is AND if not present.

Data to Send

None.

Response

None.

Status Code: 200 OK

Here is the payload:

```
{
  "TotalSize":10,
  "Definitions":[
    {"GUID":"myResource0",
    "DisplayName":"My Resource0",
    "Description":"My Resource Description99",
    "Categories":["resource"],
    "Link":"definitions/myResource0"},
more...
  ]
}
```

Status Code: 400 Parameter Error

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"InvalidOrderBy"}
    },
   "Reason":{"Text":"Invalid sortOrder url parameter specified: ASCENDING.  Valid 
values are ASC, DESC"}
  }
}
```

Here are the fault subcodes:

- InvalidOrderBy: if the order by was not a valid value
- InvalidTemplateRange
- InvalidSortBy

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.2 POST /rpt/definitions

Copies a report definition.

This operation copies a definition and returns the generated GUID.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

This URL parameter is required:

- copy=<GUID>: Copies an existing defintion, but does not include any Data to Send. The server copies an existing definition and appends localized “_copy[n]” to DisplayName in every locale bundle where n is a number starting with 1.

Data to Send

None.

Response

None.

Status Code: 200 OK

Here is the payload:

```
{"GUID":"f3aed01ef7ed4783b636ef3dfecf6321","Status":"OK"}
```

Status Code: 404 Not Found

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportTemplateCreateCopyNotExist"}
     },
   "Reason":
     {"Text":"Report template creation failed.  The report template created failed
because report template to copy 'f3aed01ef7ed4783b636ef3dfecf6321' does not
exist."}
   }
}
```

Here are the fault subcodes:

- ReportTemplateCreateCopyNotExist: If the template to copy was not found.
- ReportTemplateCreateNoContent: Not a copy and no content.
- ReportTemplateCreateFailedBadMediaType: If report format is not PDF or CSV.
- ReportTemplateCreateFailedNeedDisplayName: If display name is not supplied.

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.3 GET /rpt/defintions/<GUID>

Gets a definition.

Gets the detailed info on the definition specified. Display name, description of the report as well as display name and description of the report parameters will be sent in the language based upon the Accept-Language http header.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None.

Data to Send

None.

Response

None.

Status Code: 200 OK

Here is the payload:

```
{
  "DisplayName":"My Resource0_copy1",
  "Description":"My Resource Description99",
  "Categories":["resource"],
  "Tags":["resources","mary"],
  "PluginParameterDefinitions":
      [{"Type":"String",
        "DisplayName":"PLUGIN_DIRECTORY",
        "InternalName":"PLUGIN_DIRECTORY",
        "Description":"Location of plugin files",
        "DefaultValue":"",
        "IsForPrompting":"0"},
       {"Type":"String",
        "DisplayName":"Language",
        "InternalName":"REPORT_LOCALE",
        "Description":"Select the language in which the report will be generated.",
        "DefaultValue":"en",
        "IsForPrompting":"1",
        "Options":
          {"Property":
              [{"Value":"en","DisplayName":"English","Name":"%English"},
               {"Value":"fr","DisplayName":"French","Name":"%French"},
               {"Value":"de","DisplayName":"German","Name":"%German"},
               {"Value":"it","DisplayName":"Italian","Name":"%Italian"},
               {"Value":"ja","DisplayName":"Japanese","Name":"%Japanese"},
               {"Value":"zh_TW","DisplayName":"Traditional 
Chinese","Name":"%Traditional Chinese"},
              {"Value":"zh","DisplayName":"Simplified Chinese","Name":"%Simplified 
Chinese"},
               {"Value":"es","DisplayName":"Spanish","Name":"%Spanish"},
               {"Value":"pt","DisplayName":"Portuguese","Name":"%Portuguese"}]
          }
      ]
    },
  "Comments":"This is my comment",
  "Email":
    {"To":
      ["allison blake <ablake@novell.com>",
       "chip nano <cnano@novell.com>"],
     "Cc":
       ["fred stats <fstats@novell.com>",
       "bob bender <bbender@novell.com>"],
     "Subject":"Please verify",
     "Message":"See attached report."},
  "Format":"PDF",
  "Links":
    {"Export":"templates/b7785943f5ea48329d0c5b1c4af1a1cc/rpz",
     "Scheduling":"templates/b7785943f5ea48329d0c5b1c4af1a1cc/sched"}
}
```

Response header: Etag: {hex string}

Status Code: 404 Not Found

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportTemplateDoesNotExist"}
     },
   "Reason":
     {"Text":"The report template 'b7785943f5ea48329d0c5b1c4af1a1cc11' does not 
exist."}
   }
}
```

Here is the fault subcode:

- ReportTemplateDoesNotExist: If the template was not found.

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.4 PUT /rpt/definitions/<GUID>

Updates a definition.

Update an existing definition. Display name, description of the report as well as display name and description of the report parameters will be interpreted to be in the language based on the Accept-Language HTTP header.

RepeatUnit: Valid values are NONE, DAY, WEEK, MONTH (12 MONTH = 1 year, 3 MONTH = 1 quarter). NONE is used only in REST API (not to the end user) to represent non-repeating (one time) schedule. When repeat unit is set to NONE, only start date is meaningful.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

Here is the payload:

```
{
  "DisplayName":"My Resource0_copy1",
  "Description":"My Resource Description99",
  "Categories":["resource"],
  "Tags":["resources","mary"],
  "PluginParameterDefinitions":
      [{"Type":"String",
      "DisplayName":"PLUGIN_DIRECTORY",
      "InternalName":"PLUGIN_DIRECTORY",
      "Description":"Location of plugin files",
      "IsForPrompting":"0"}
     ],
  "Comments":"This is my comment",
  "Email":
    {"To":
      ["allison blake <ablake@novell.com>",
       "chip nano <cnano@novell.com>"],
     "Cc":
       ["fred stats <fstats@novell.com>",
       "bob bender <bbender@novell.com>"],
     "Subject":"Please verify",
     "Message":"See attached report."},
  "Format":"PDF",
}
```

Request Header (optional) If-Match: {hex string}

If this string is sent, it is is compared to the current etag for the report. If it does not match, an ncac “ReportChangedSinceRetrieve” is thrown.

Response

None.

Status Code: 200 OK

Here is the payload:

```
{"GUID":"f3aed01ef7ed4783b636ef3dfecf6321","Status":"OK"}
```

Response Header Etag: {hex string}

Status Code: 404 Not Found, 409 Conflict

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportTemplateDoesNotExist"}
    },
   "Reason":
     {"Text":"Report template 'f3aed01ef7ed4783b636ef3dfecf6321' does not exist."}
   }
}
```

Here are the fault subcodes:

- ReportTemplateDoesNotExist: If the template was not found.
- ReportTemplateUpdateDuplicateDisplayName: For duplicate display name
- ReportTemplateCreateFailedBadMediaType: If report format is not PDF or CSV
- ReportTemplateCreateFailedNeedDisplayName: If display name is not supplied
- ReportChangedSinceRetrieve: If contents have changed since the retrieval

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.5 DELETE /rpt/definitions/<GUID>

Deletes an existing definition. Any scheduled runs are also deleted.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None.

Response

None.

Status Code: 200 OK

Here is the payload:

```
{"GUID":"f3aed01ef7ed4783b636ef3dfecf6321","Status":"OK"}
```

Status Code 404: Not Found

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportTemplateDoesNotExist"}
    },
   "Reason":
     {"Text":"Report template 'f3aed01ef7ed4783b636ef3dfecf6321' does not exist."}
   }
}
```

Here are the fault subcodes:

- ReportTemplateDoesNotExist: If the template was not found.

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.6 GET /rpt/definitions/<GUID>/rpz

Gets a definition RPZ.

Gets the JAR of the definition for export. The JAR includes the jrxml, localization bundle, and tempate meta-data.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None.

Data to Send

None.

Response

None.

Status Code: 200 OK

Here is the payload:

```
application/zip
```

Status Code: 404 Not Found

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportTemplateDoesNotExist"}
    },
   "Reason":
     {"Text":"Report template 'f3aed01ef7ed4783b636ef3dfecf6321' does not exist."}
   }
}
```

Here are the fault subcodes:

- ReportTemplateDoesNotExist: If the template was not found.

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.7 GET /rpt/definitions/<guid>/paramdefs/<paramName>

Gets parameter name/value pairs.

This operation will return a list of allowable values for a given parameter. These values may come from the database, or they may be part of hardcoded options.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following URL parameters are required:

- casading parameter value if cascading parameters are used for the paramName. This is illustrated in the following example:

```
<PluginParameterDefinition>
   <Type>String</Type>
   <DisplayName>Search User(s)</DisplayName>
   <Description>Specifies the search criteria to choose user(s) to be 
reported.</Description>
   <InternalName>search_name</InternalName>
   <DefaultValue></DefaultValue>
   <IsForPrompting>0</IsForPrompting>
  </PluginParameterDefinition>
  <PluginParameterDefinition>
   <Type>String</Type>
   <DisplayName>User(s)</DisplayName>
   <Description>Specifies the user(s) from which data will be reported.</
Description>
   <InternalName>sample</InternalName>
   <DefaultValue></DefaultValue>
   <IsForPrompting>1</IsForPrompting>
   <OptionQuery>SELECT first_name || ' ' || last_name as name, '\'' || 
identity_id || '\'' as value FROM idm_rpt_data.idmrpt_identity where 
lower(first_name || ' ' || last_name) like lower('##search_name##') order by 
name</OptionQuery>
  </PluginParameterDefinition>
```

The following URL parameters are optional:

- idxFrom: The starting row index. 0 is the first.
- idxTo: The ending row index, inclusive. Server will validate that idxTo >= idxFrom

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"TotalSize":19,"ParameterValues":[
{"DisplayName":"Abby Spencer","Value":"'cee9e6b0fb654adfb5ec22eb62c39557'"},
{"DisplayName":"Adam Marsden","Value":"'cee9e6b0fb654adfb5ec22eb62c393f8'"},
{"DisplayName":"Allison Blake","Value":"'cee9e6b0fb654adfb5ec22eb62c39556'"},
{"DisplayName":"Angie Chung","Value":"'cee9e6b0fb654adfb5ec22eb62c39558'"},
{"DisplayName":"Anthony Palani","Value":"'cee9e6b0fb654adfb5ec22eb62c39559'"},
{"DisplayName":"April Smith","Value":"'cee9e6b0fb654adfb5ec22eb62c39560'"},
{"DisplayName":"Bill Bender","Value":"'cee9e6b0fb654adfb5ec22eb62c39561'"},
{"DisplayName":"Bill Brown","Value":"'cee9e6b0fb654adfb5ec22eb62c39563'"},
{"DisplayName":"Bill Burke","Value":"'cee9e6b0fb654adfb5ec22eb62c39562'"},
{"DisplayName":"Bob Jenner","Value":"'cee9e6b0fb654adfb5ec22eb62c39564'"},
{"DisplayName":"Brad Jones","Value":"'cee9e6b0fb654adfb5ec22eb62c39565'"},
{"DisplayName":"Cal Central","Value":"'cee9e6b0fb654adfb5ec22eb62c39566'"},
{"DisplayName":"Chip Nano","Value":"'cee9e6b0fb654adfb5ec22eb62c39567'"},
{"DisplayName":"Chris Black","Value":"'cee9e6b0fb654adfb5ec22eb62c39568'"},
{"DisplayName":"David Decker","Value":"'cee9e6b0fb654adfb5ec22eb62c39555'"},
{"DisplayName":"Josh Kelley","Value":"'cee9e6b0fb654adfb5ec22eb62c39570'"},
{"DisplayName":"Kelly Kilpatrick","Value":"'cee9e6b0fb654adfb5ec22eb62c39569'"},
{"DisplayName":"Kip Keller","Value":"'cee9e6b0fb654adfb5ec22eb62c39571'"},
{"DisplayName":"Rashelle Bradley","Value":"'cee9e6b0fb654adfb5ec22eb62c393f6'"}]}
```

Status Code: 400 parameter error

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"ReportParamNotFound"}
    },
   "Reason":{"Text":"Unable to return parameter values because supplied parameter
'abc' not found in report."}
  }
}
```

Here are the fault subcodes:

- ReportParamNotFound
- InvalidReportDefinitionRange
- RequiredCascadingParamMissing

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.8 POST /rpt/definitions/import

Imports .spz or .rpz report(s).

Imports a zip file for a single definition or a zip of a zip for multiple definitions. The following rules apply:

- The format of each zip must follow the Sentinel plugin standard, with data from the package.xml containing the definition metadata. The file must have the extension .rpz for a single report, or use the extension .spz for the case of multiple reports.
- Each zip within the spz will be processed as if uploaded separately.
- If overwrite parameter is true, then if a name already exists, it will be overwritten and have an individual status of OK.
- If overwrite parameter is false or not present, anything that already exists will have individual status of FAILED, but overall status is still OK.
- PlatformName must be included in the package.xml of the .rpz and that must be IDM, else error.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

There are no required URL parameters.

The following URL parameters are optional:

- overwrite: true or false
- token: the user authentication token
- ts_url: the token server URL
- format: the format of the content to return
- content: the content type of the return value separate from the format
- uploadid: the temporary id to use for this current upload

Data to Send

Multipart application/octet-stream.

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  “Status”: “OK”,
  “Imports”: [
     {“Filename” : “mary.rpz”, “GUID”: “24352345”, “Status”, “OK”},
     {“Filename” : “frank.rpz”, “Status”: “FAILED”,
         "Fault":
           {"Code":
             {"Value":"Sender",
              "Subcode": {"Value":"ReportTemplateUpdateDuplicateDisplayName"}
             },
            "Reason": {"Text":"Report template update failed.  The report template 
update with GUID 'roleReport' failed because display name 'Role Report' is used in 
another report template."}
           }
      },
      more jars...
   ]
}
```

Possible Errors

These are the possible errors:

- ReportDefinitionCreateDuplicateDisplayName
- ReportTemplateCreateFailedBadMediaType
- ReportTemplateCreateFailedNeedDisplayName
- ReportUploadFailed
- RpzFileUploadFailedZipException
- RpzFileUploadFailedZipExceptionBadPackageXml
- RpzFileUploadFailedZipExceptionBadPackageXmlNameTooLong
- RpzFileUploadFailedReportContentNotIdm

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.9 GET /rpt/definitions/import/<upload id>

Gets the status of the JAR upload in progress.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  “CompletedPercent”: 50,
  “Completed”: “10Mb”,
  “Total”: “20Mb”
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.10 DELETE /rpt/definitions/import/<upload id>

Cancels an upload.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  “Cancelled”: “true”
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.11 GET /rpt/definition/<GUID>/sched

Gets schedules.

Get an array of schedules belonging to a specific definition.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
"TotalSize":1,
"Schedules":[
  {
  "ScheduleID":"e20cc23f-4de1-4002-8d5a-fecb8ccfceda",
  "DisplayName":"Identity Report - kkk","Schedule":{
    "StartDate":1275053400000,
    "EndDate":1275139800000,
    "RepeatNumber":1,
    "RepeatUnit":"MONTH"
  },
  "CollectOnRun":false
  }]
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportdefinitionDoesNotExist"}
     },
   "Reason":
     {"Text":"The report definition 'b7785943f5ea48329d0c5b1c4af1a1cc11' does not
exist."}
   }
}
```

Here are the fault codes:

- 404 InvalidURI: URI not found (Sender)
- 500 InternalError: Server problem (Receiver)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.12 POST /rpt/definition/<GUID>/sched

Creates a schedule.

Creates a new schedule for a specific definition. Here is the logic used for inheriting and overwriting attributes during schedule creation:

- If an attribute is missing in the payload, its value is inherited from the definition; Otherwise, the value in payload will be taken.
- For a mandatory attribute, there is no problem of doing so. However for an optional attribute, the ability of overwriting is limited. Here is an example:
  - Suppose definition A has an attribute called "attr1", which is *optional*. The default value of attr1 defined in definition A is "value1".
  - Now, suppose we create a schedule from definition A, and we do NOT want the optional attr1. How can we do it? If we don't put attr1 in the payload, the schedule will inherit "value1" from definition; If we put attr1 in the payload, then we have to specify its value.

  - The solution is that for optional attribute, we have to use composite value such as JSONObject or JSONArray. This way if we want to get rid of attr1, we put "attr1" : "{}" in the payload.
  - Fortunately we only have one optional attribute in our design, which is "Email". The rule is simple:
- If there is no "Email" in payload, inherits definition's.
- If there is "Email" in payload, but it has no "To" list or has empty "To" list, the schedule will not have email delivery.
- If there is "Email" in payload, and it's "To" list contains at least one recipient, it overwrites definition's.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

```
{
"DisplayName":"Identity Report",
"Description":"This report shows first name, last name, and job title for a given
Identity used by the User Application",
"Comments":"",
"Format":"PDF",
"CollectOnRun":false,
"Email":{"To":[], "Cc":[], "Subject":"", "Message":""},
"Parameters":[
  {
  "Value":"",
  "Description":"Location of plugin files",
  "DisplayName":"PLUGIN_DIRECTORY",
  "InternalName":"PLUGIN_DIRECTORY",
  "IsForPrompting":"0",
  "Type":"String",
  "Required":"0"
  },
  {
  "Value":"D",
  "Description":"Specifies the time period over which this report is run.",
  "DisplayName":"Date Range",
  "InternalName":"ReportType",
  "IsForPrompting":"1",
  "Type":"String",
  "DisplayValue":"Current Day",
  "OptionMultivalue":"0",
  "Required":"0"
  },
  {
  "Value":"en",
  "Description":"Select the language in which the report will be generated.",
  "DisplayName":"Language",
  "InternalName":"REPORT_LOCALE",
  "IsForPrompting":"1",
  "Type":"String",
  "DisplayValue":"English",
  "OptionMultivalue":"0",
  "Required":"0"
  }
],
"Schedule":{"StartDate":1275053400000, "RepeatNumber":1, "RepeatUnit":"MONTH",
"EndDate":1275139800000}}
```

Response

None

Status Code: 201 OK

Here is the payload:

```
{"GUID":"e3dd599e-0476-4b76-b140-625d51372e79","Status":"OK"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"ReportdefinitionDoesNotExist"}
     },
   "Reason":
     {"Text":"The report definition 'b7785943f5ea48329d0c5b1c4af1a1cc11' does not
exist."}
   }
}
```

Here are the fault codes:

- Sender
  - 404 InvalidURI: URI not found
  - 400 InvalidInput: Various input problems
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.13 GET /rpt/definition/<GUID>/sched/<sched GUID>

Gets a schedule.

Retrieves detailed information about the scheduled report.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  "DisplayName":"My Resource0_copy1",
  "Description":"My Resource Description99",
  “CollectOnRun”:false,
  "Tags":["resources","mary"],
  "Parameters":
      [{"Type":"String",
      "DisplayName":"PLUGIN_DIRECTORY",
      "InternalName":"PLUGIN_DIRECTORY",
      "Description":"Location of plugin files",
      "IsForPrompting":"0",
      “Value”:”value”,
      “DisplayValue”:”value's display name”}
     ],
  "Comments":"This is my comment",
  "Email":
    {"To":
      ["allison blake <ablake@novell.com>",
       "chip nano <cnano@novell.com>"],
     "Cc":
       ["fred stats <fstats@novell.com>",
       "bob bender <bbender@novell.com>"],
     "Subject":"Please verify",
     "Message":"See attached report."},
  "Format":"PDF",},
  "Schedule":
    {"StartDate":1264873989592,
     "RepeatNumber":1,
     "RepeatUnit":"NONE",
     "EndDate":1264874049592}
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"?"}
     },
   "Reason":
     {"Text":"?"}
   }
}
```

Here are the fault codes:

- 404 InvalidURI: URI not found (Sender)
- 500 InternalError: Server problem (Sender)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.14 DELETE /rpt/definition/<GUID>/sched/<sched GUID>

Deletes a schedule, and also removes all planned runs belonging to the schedule.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"GUID":"e3dd599e-0476-4b76-b140-625d51372e79","Status":"OK"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"?"}
     },
   "Reason":
     {"Text":"?"}
   }
}
```

Here are the fault codes:

- 404 InvalidURI: URI not found (Sender)
- 500 InternalError: Server problem (Receiver)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.15 POST /rpt/definition/<GUID>/sched/<sched GUID>

Updates a schedule.

This operation modifies planned runs based on the parameter's value. There are two exclusive parameter sets. One and only one of them has to be present.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

This operation must have one and only one of the following parameter sets:

- runToDel: the planned run to be deleted from this schedule.
- shift: a delta that all planned runs will be shifted by. runToShift: which run the shift is based on. Both shift and runToShift have to be present.

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"GUID":"e3dd599e-0476-4b76-b140-625d51372e79","Status":"OK"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"?"}
     },
   "Reason":
     {"Text":"?"}
   }
}
```

Here are the fault codes:

- Sender
  - 404 InvalidURI: URI not found
  - 400 InvalidInput: Various input problems
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.16 PUT /rpt/definition/<GUID>/sched/<sched GUID>

Updates a schedule.

Modifies an existing schedule.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

Same as POST /rpt/definition/<GUID>/sched

Response

None

Status Code: 200 OK

Here is the payload:

```
{"GUID":"e3dd599e-0476-4b76-b140-625d51372e79","Status":"OK"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"?"}
     },
   "Reason":
     {"Text":"?"}
   }
}
```

Here are the fault codes:

- Sender
  - 404 InvalidURI: URI not found
  - 400 InvalidInput: Various input problems
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.17 GET /rpt/reports

Gets completed reports.

Returns a list of minimal information on reports. The server performs the sorting.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

There are no required parameters.

The following URL parameters are optional:

- sortBy: The column to sort by. Valid values: DisplayName, RunDate, Description. It defaults to DisplayName.
- sortOrder: The sort order. Valid values: ASC or DESC. It defaults to ASC.
- idxFrom: The starting index. 0 is the first.
- idxTo: The ending index (inclusive).

  idxTo must be greater than or equal to idxFrom.
- dateFrom: the starting date in epoch time since Jan 1, 1970 in milliseconds, inclusive
- dateTo: the end date in epoch time since Jan 1, 1970 in milliseconds, inclusive
- state: absent - same as "all"
  - all - return all reports
  - unfinished - only return in-progress ones, subset of "all"
  - finished - return non in-progress ones, subset of "all"
  - success - return successfully finished ones, subset of "finished"
  - failed - return failed ones, subset of "finished"

The following logic applies to completed reports:

- dateFrom/To applies first, if present.
- sortBy/sortOrder applies second.
- idxFrom/To applies last, if present.

Here are the filters:

- filterDisplayName
- filterDescription
- filterCreator
- filterTags
- filterLOP (OR or AND)

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"TotalSize":3,
 "Results":[{"ReportID":"3c604da1-9a3e-4c77-bff1-
4ceaac9e6b33","DisplayName":"CCC","RunDate":1265213805296},
            {"ReportID":"05b988af-3f03-4c42-b2b1-
067e40d3dca7","DisplayName":"DDD","RunDate":1265213805234},
           {"ReportID":"85710ba9-8980-40d8-b796-72c854f473fd","DisplayName":"Role
Assignment Report Daily","RunDate":1265217393687}
           ]
}
```

TotalSize reflects the amount without idxFrom/To applied.

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"InvalidInput"}
    },
   "Reason":{"Text":"Invalid sortOrder url parameter specified: ASCENDING.  Valid
values are ASC, DESC"}
  }
}
```

Here are the fault codes:

- 400 InvalidInput: Various input problems (Sender)
- 500 InternalError: Server problem (Receiver)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.18 GET /rpt/reports/<report id>

Gets a completed report.

Retrieves detailed information on the report specified.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  "Name":"My Resource_20100110142266",
  "InProgress":false,
  "failed":false,
  "DisplayName":"My Resource0",
  "RunDate":1264827600000,
  "PluginParameterDefinitions":
      [{"Type":"String",
      "DisplayName":"PLUGIN_DIRECTORY",
      "InternalName":"PLUGIN_DIRECTORY",
      "Description":"Location of plugin files",
      "IsForPrompting":"0"}
     ],
  "Email":
    {"To":
      ["allison blake <ablake@novell.com>",
       "chip nano <cnano@novell.com>"],
     "Cc":
       ["fred stats <fstats@novell.com>",
       "bob bender <bbender@novell.com>"],
     "Subject":"Please verify",
     "Message":"See attached report."}
  "RunBy":
    {"Value":<run_user_id>,
     "DisplayName":"Fred Stats",
    },
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- 404 InvalidURI: URI not found (Sender)
- 500 InternalError: Server problem (Receiver)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.19 GET /rpt/reports/<report id>/file

Gets the actual report file.

Get the actual report file for the report specified.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format PDF, CSV

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
Content-Disposition: inline; filename="Report_<timestamp>.<file_extension>"
Content-Type: <one of application/pdf and application/csv
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- 404 InvalidURI: URI not found (Sender)
- 500 InternalError: Server problem (Receiver)

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.20 DELETE /rpt/reports/<report id>

Deletes a completed report.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"GUID":"e3dd599e-0476-4b76-b140-625d51372e79","Status":"OK"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- Sender
  - 404 InvalidURI: URI not found
  - 400 InvalidInput: the report to be deleted is in progress
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.21 GET /rpt/calendar

Gets upcoming runs.

Retrieves detailed information on the report specified. Returns an array of planned runs in running order, optionally filtered. There are two exclusive filter sets which cannot be applied together in one request. Both are optional.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

There are no required parameters:

The following parameters are optional:

- dateFrom (inclusive) /dateTo (inclusive) defines the time range. Either of them is optional. The value must be specified as POSIX milliseconds.
- upcomingRuns defines up to how many planned runs will be returned. Must be an integer greater than 0.

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{ “Entries” : [
  {"ScheduleDisplayName":"My Resource2",
   "definitionName":"myResource2",
   “definitionDisplayName”: “My Resource2”,
   "RunDate":1264827600000,
   "ScheduleID":"e3dd599e-0476-4b76-b140-625d51372e79"},
more...
])
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- Sender
  - 400 InvalidInput: Various input problems
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.22 GET /rpt/buildinfo

Gets information about the build.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"rev":"630","date":"Jan 30, 2010 9:31:23 AM","user":"bsiegal","version":"1.0"}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.23 GET /rpt/collectors

Gets collectors.

Retrieves a list of systems that data is being collected on localized by server-side.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  "TotalSize":10,
  "Collector":[
    {"ID":"idvault",
    "DisplayName":"Identity Vault",
    "Link":"collector/idvault"},
    {"ID":"sentinel",
    "DisplayName":"Sentinel Event System",
    "Link":"collector/sentinel"},
more...
  ]
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
     },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token

- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.24 GET /rpt/collectors/<collector id>/config

Gets the configuration of the specified data collector.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  "TotalSize":10,
  "Collector":[
    {"ID":"idvault",
    "DisplayName":"Identity Vault",
    "Link":"collector/idvault"},
    {"ID":"sentinel",
    "DisplayName":"Sentinel Event System",
    "Link":"collector/sentinel"},
more...
  ]
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.25 GET /rpt/rptusers/<token>

Gets a reporting user’s information.

Retrieves information such as name, email address, and so forth.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  "DN": …,
  "Name":"...",
  "Locale":"...",
  "Email":...
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- Sender
  - 401: Query tokens other than owned is not allowed

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.26 GET /rpt/rptusers/user

Gets the current user's information and redirects the client to /rpt/rptusers/<token>.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 307 Temporary Redirect

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.27 GET /rpt/idmusers

Get a list of users to report on sorted by display expression with localized display expression (for example, if in English FirstName LastName, else if in Chinese LastName FirstName).

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following optional parameter may be specified:

- filter: filter=FirstName LIKE a% OR LastName LIKE a%

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
[
  {
     “ID”: “13413”,
     “Value”: “Angie Chung”,
     “Link”: “/rpt/idmusers/13413”
  },
  {
     “ID”: “23413”,
     “Value”: “Allison Blake”,
     “Link”: “/rpt/idmusers/23413”
  },
  more...
]
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
     },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.28 GET /rpt/idmusers/<idmuser id>

Get details on the specified user.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
  “ID”: “13413”,
  “Value”: “Angie Chung”,
  “Link”: “/rpt/idmusers/13413/attributes”,
what else?
}
```

Status Code: 4xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.29 GET /rpt/idmroles

Get a list of of roles TO REPORT ON, sorted by localized Display Name.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following optional parameter may be specified:

- filter: filter=DisplayName LIKE a%

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
[
  {
     “ID”: “adsa13413”,
     “Value”: “Doctor”,
     “Link”: “/rpt/idmroles/adsa13413”
  },
  {
     “ID”: “2341sdf3”,
     “Value”: “Nurse”,
     “Link”: “/rpt/idmroles/2341sdf3”
  },
  more...
]
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.30 GET /rpt/idmroles/<idmrole id>

Gets details on the specified role.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
     “ID”: “adsa13413”,
     “Value”: “Doctor”,
what else?
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.31 GET /rpt/idmresources

Get a list of of resources to report on, sorted by localized Display Name.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following optional parameter may be specified:

- filter: filter=DisplayName LIKE a%

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
[
  {
     “ID”: “16h3413”,
     “Value”: “Resources A”,
     “Link”: “/rpt/idmresources/16h3413”
  },
  {
     “ID”: “23ba413”,
     “Value”: “Resources B”,
     “Link”: “/rpt/idmresources/23ba413”
  },
  more...
]
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
     },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.32 GET /rpt/idmresources/<idmresource id>

Retrieves details for a specified resource.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
     “ID”: “adsa13413”,
     “Value”: “Doctor”,
what else?
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.33 GET /rpt/idmentitlements

Gets a list of of entitlements to report on, sorted by localized Display Name.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following optional parameter may be specified:

- filter: filter=DisplayName LIKE a%

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
[
  {
     "ID": "13aa413",
     "Value": "Entitlement A",
     "Link": "/rpt/idmentitlements/13aa413"
  },
  {
     "ID": "2sd3413",
     "Value": "Entitlement B",
     "Link": "/rpt/idmentitlements/2sd3413"
  },
  more...
]
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
     },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.34 GET /rpt/idmentitlements/<idmentitlement id>

Retrieves details on a specified entitlement.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
     “ID”: “13aa413”,
     “Value”: “Entitlement A”,
what else?
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.35 GET /rpt/idmteams

Gets a list of of teams to report on, sorted by localized Display Name.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

The following optional parameter may be specified:

- filter: filter=DisplayName LIKE a%

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
[
  {
     “ID”: “13354413”,
     “Value”: “Jake Prov Team”,
     “Link”: “/rpt/idmteams/13354413”
  },
  {
     “ID”: “2dsvs”,
     “Value”: “Flora Role Team”,
     “Link”: “/rpt/idmteams/2dsvs”
  },
  more...
]
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.36 GET /rpt/idmteams/<idmteam id>

Retrieves details on a specified team.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
     “ID”: “13354413”,
     “Value”: “Jake Prov Team”,
     “Link”: “/rpt/teams/13354413/members”
}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.37 GET /rpt/conf

Get global configuration of the core server.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{
"SmtpHost":"...",
"SmtpPort":465,
"SmtpAuth":true,
"SmtpUser":"...",
"SmtpPass":"noguessing",
"SmtpSsl":true,
"DefaultEmail":"test@novell.com",
"ReportFolder":"/home/alex",
"RetentionInterval":1,
"RetentionUnit":"MONTH",
"NameOrder":"default|$FN $LN",
"ExpectedDataCollectionTime":3600000}
```

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- Sender
  - 401: Query tokens other than owned is not allowed
- Receiver
  - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.38 POST /rpt/conf

Sets the global configuration for the core server.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

```
{"SmtpHost":"...",
"SmtpPort":465,
"SmtpAuth":true,
"SmtpUser":"...",
"SmtpPass":"noguessing",
"SmtpSsl":true,
"DefaultEmail":"test@novell.com",
"ReportFolder":"/home/alex",
"RetentionInterval":1,
"RetentionUnit":"week",
"NameOrder":"default|$FN $LN",
"ExpectedDataCollectionTime":3600000}
```

Response

None

Status Code: 200 OK

Status Code: 4xx/5xx

Here is the payload:

```
{"Fault":{
   "Code":{"Value":"Sender",
           "Subcode":{"Value":"?"}
    },
   "Reason":{"Text":?}
  }
}
```

Here are the fault codes:

- Sender
  - 400 InvalidInput: Various input problems
  - 401: Query tokens other than owned is not allowed

- Receiver
    - 500 InternalError: Server problem

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.39 GET /locales/default

Gets the default locale from the core server.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"DefaultLocale":"en_us"}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

13.4.40 GET /locales/supported

Sets the global configuration for the core server.

This operation requires authentication. You need to set the Authorization request header for this operation, giving it a type of X-OPAQUE, as well as the token you received during the login operation. It looks like this:

```
Authorization: X-OPAQUE <token>
```

Format JSON, XML

URL Parameters

None

Data to Send

None

Response

None

Status Code: 200 OK

Here is the payload:

```
{"SupportedLocales":[da,de,en,es,fr,it,ja,nl,pt,ru,sv,zh_cn,zh_tw]}
```

Status Code: 401 Unauthorized

Here is the payload:

```
{"Fault":
  {"Code":
    {"Value":"Sender",
     "Subcode":
       {"Value":"InvalidAuthHeader"}
     },
   "Reason":
     {"Text":"User carries unrecognized/expired/invalid authentication token."}
   }
}
```

Here are the fault subcodes:

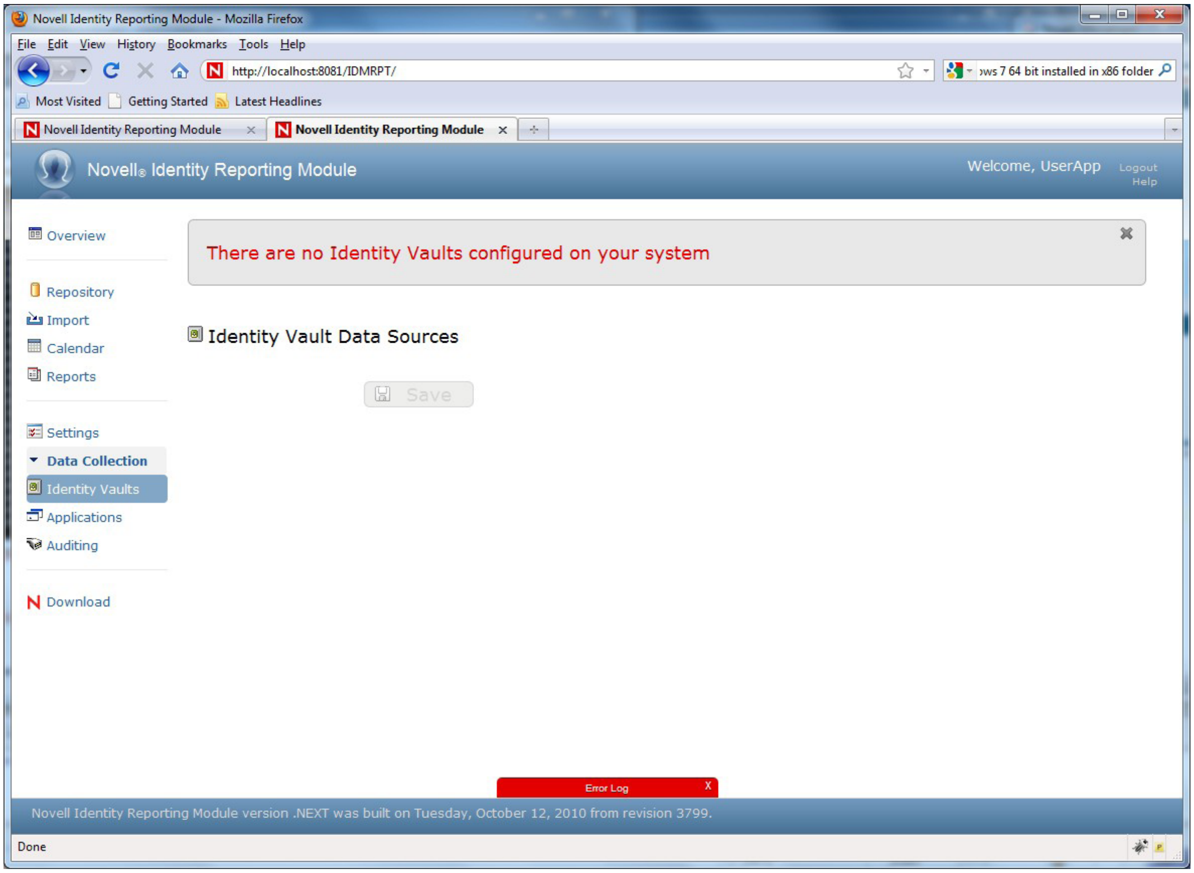
- InvalidAuthHeader: Bad token or expired token
- NoAuthHeader: Token not carried
- NoPrivilege: Token valid but user is not a reporting administrator, and therefore has no access to the REST API

14 Troubleshooting the Drivers

This section describes many of the most common issues that arise in driver configuration and provides tips for resolving these issues.

14.1 Issue: No Identity Vaults Presented on the Identity Vaults Screen

If you look at the Identity Vaults screen in the Identity Reporting Module, you may notice that no Identity Vaults are listed. You will also see an error message at the top of the screen.



There are no Identity Vaults configured on your system

Identity Vault Data Sources

Novell Identity Reporting Module version .NEXT was built on Tuesday, October 12, 2010 from revision 3799.

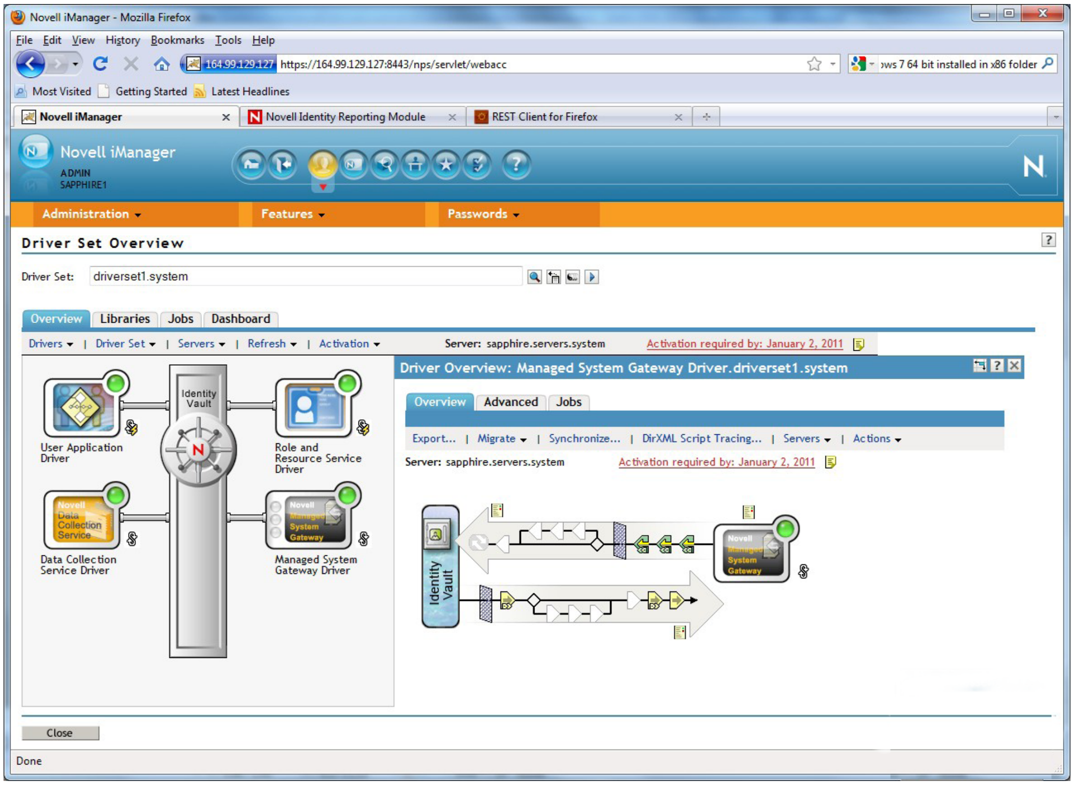
Novell Identity Reporting Module - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8081/IDMRPT/
ows 7 64 bit installed in x86 folder
Most Visited
Getting Started
Latest Headlines
Novell Identity Reporting Module
Novell Identity Reporting Module
Novell® Identity Reporting Module
Welcome, UserApp
Logout
Help
Overview
Repository
Import
Calendar
Reports
Settings
Data Collection
Identity Vaults
Applications
Auditing
Download
Save
Error Log
X
Done

Here are some of the possible causes for this problem:

- The Data Collection Service driver is not configured or started.
- The Data Collection Service driver is configured incorrectly. Here are some things that may be not be properly defined:
  - You have specified an invalid user account, account password, or the account does not have sufficient privileges (is not assigned as Report Administrator).
  - The reporting connection configuration is wrong.

Here are some troubleshooting tips:

- Verify that the Data Collection Service driver is configured and running. To do this:
  - Check in iManager that the driver is present and that the driver state is *Running*. If it is not running, start the driver.


Novell iManager - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://164.99.129.127:8443/nps/servlet/webacc
Most Visited Getting Started Latest Headlines
Novell iManager
Novell Identity Reporting Module
REST Client for Firefox
Novell iManager
ADMIN
SAPPHIRE1
Administration
Features
Passwords
Overview Libraries Jobs Dashboard
Drivers | Driver Set | Servers | Refresh | Activation
Identity Vault
User Application Driver
Role and Resource Service Driver
Data Collection Service Driver
Managed System Gateway Driver
Overview Advanced Jobs
Export... | Migrate | Synchronize... | DirXML Script Tracing... | Servers | Actions
Close
Done

Driver Set Overview

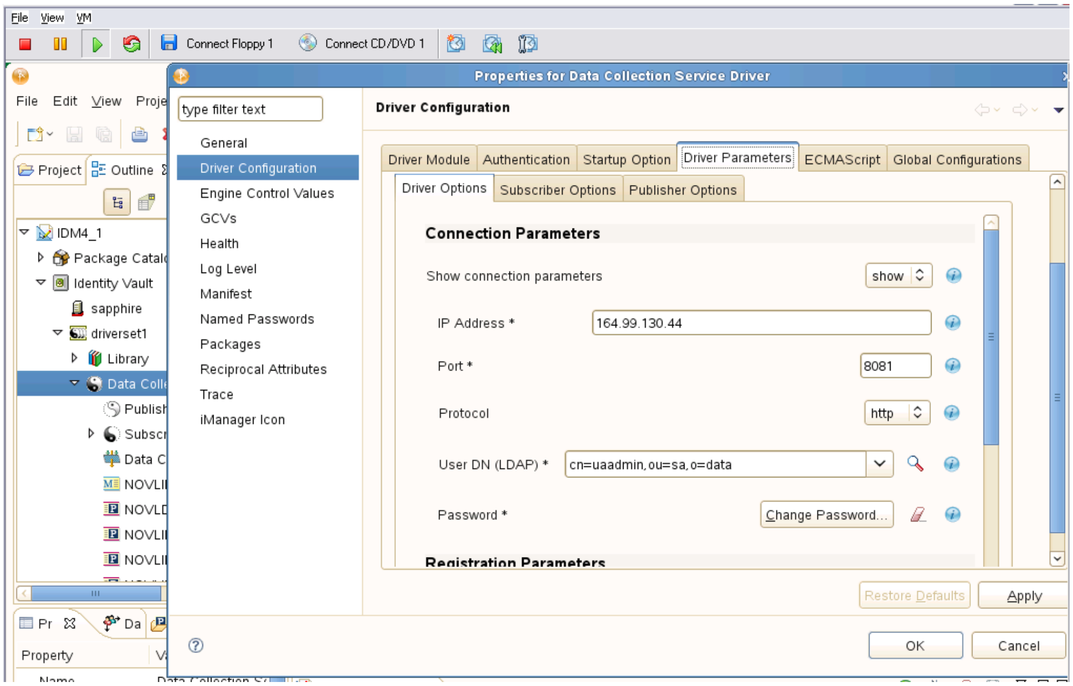
Driver Set: driverset1.system

Server: sapphire.servers.system Activation required by: January 2, 2011

Driver Overview: Managed System Gateway Driver.driverset1.system

Server: sapphire.servers.system Activation required by: January 2, 2011

- Check in Designer that the driver configuration points to the reporting services and has a valid account and password configured. If you need to modify the configuration settings, make your changes in Designer. Stop the driver before you redeploy, and start the driver after a successful deployment. Novell recommends that you synchronize the driver prior to modifying and redeploying it.



Properties for Data Collection Service Driver

Driver Configuration

Connection Parameters

Show connection parameters: show

IP Address *: 164.99.130.44

Port *: 8081

Protocol: http

User DN (LDAP) *: cn=uaadmin,ou=sa,o=data

Password *

Registration Parameters

- Verify that RBPM is installed and the Reporting Administrator role assignment has been processed and assigned to the user account configured in the reporting connection parameters for the Data Collection Service driver.

  To verify the role assignment, log into the User Application with the Role Administrator account. Then, go to the Work Dashboard and look at the list of assigned roles for accounts used by the Data Collection Service driver. If you don't see the role assigned, verify that the Role and Resource driver has been started.

If the Data Collection Service configuration seems correct, enable DS Trace for the Data Collection Service driver at level 5, and verify that there are no communication or connection errors in the log.

Verify that the Data Collection Service driver is sending registration events to the REST services. The best way to do this is to add the following trace to the idmrptcore_logging.xml file and tail the console log (by using `tail -f server.log`). You should see trace messages with recognizable DNs, names, and so forth.

```
<logger name="com.novell.idm.rpt.core.server.events.rptdriver" level="TRACE"
additivity="true"/>
```

14.2 Issue: Reports Are Missing Identity Vault Data

If you notice that some of your reports are missing Identity Vault data, you should look at the following list of possible causes:

- Report definition is out of date.
- The Data Collection Service driver or the reporting module is not started.
- The Data Collection Service driver was not migrated. If the driver has not been migrated, the objects are not synchronized into the Identity Information Warehouse.
- The timeout setting on the Data Collection Service driver is set too high and the events are not immediately propagated into the database. This could appear to be a problem if you don't wait until the event is sent and processed.
- The Data Collection Service driver is not configured correctly. Here are some things to look at:
  - Objects are missing from the Filter Policy.
  - Objects are not under the Data Collection Service scope.

Here are troubleshooting tips:

- Verify that the data missing from the reports is present in the idm_rpt_data schema tables:
  - If the data is present in the database, verify that you have the latest report definitions installed. On the detail page of each report is a field showing the data it was built or customized. You need to compare the date on the detail for that report with the data on the download page http://cdn.novell.com'cached/designer/idmrpt/.
  - If the data is missing from the database, verify that the Data Collection Service driver is sending events to the REST services and that they are being processed correctly:
    1. Make sure there are no errors in event processing. View the JBoss console log (server.log) and look for errors (for example, `grep -i "error" server.log`)
    2. If there are no errors, make sure that the events are being received from the Data Collection Service driver.

Add the following trace to the idmrptcore_logging.xml file and tail the console log (by using `tail -f server.log`). You should see trace messages with recognizable DNs, names, and so forth.

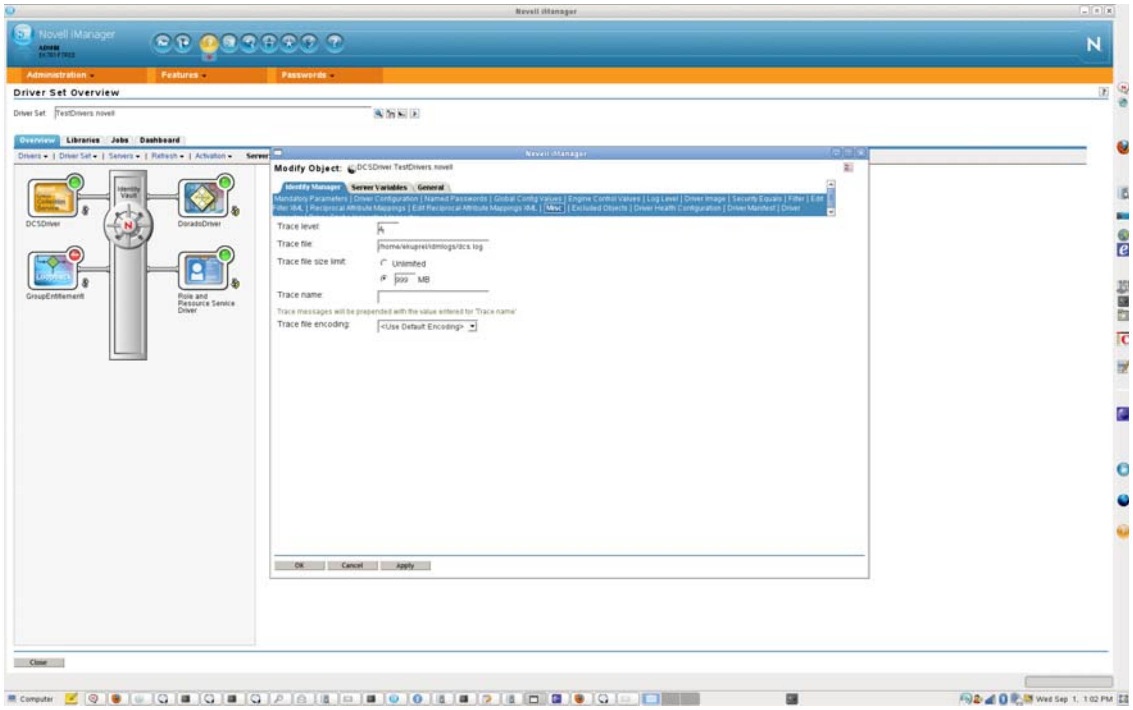
```
<logger name="com.novell.idm.rpt.core.server.events.rptdriver"
level="TRACE" additivity="true"/>
```

- Verify that the Data Collection Service driver is configured and running:
  - Check in iManager to see that the driver was deployed and the driver state is *Running*.
  - Check the following settings for the Data Collection Service driver in iManager:
    - Reporting connection information
    - Reporting access account
    - Data Collection Service driver filter policy
    - Data Collection Service driver scope
    - Data Collection Service driver event processing settings

      Look at the *Time interval between submitting events* and the *Number of events to be sent in batch*. Set these to lower values for more immediate results.

When you are confident that your configuration is correct, and you still don't see the expected data populated, you need to check for Data Collection Service driver errors. Check the DS Trace from the driver to see if there are errors:

- Check the DS Trace from the driver to see if there are any errors.
- Enable the driver trace at level 5.
- Delete the old trace file (if one exists) and restart the Data Collection Service driver. (The trace file can become very large.)


Novell iManager
Administration
Features
Passwords
Overview
Libraries
Jobs
Dashboard
Drivers | Driver Set | Servers | Refresh | Activation
Identity Vault
DCSDriver
DoradoDriver
GroupEntitlement
Role and Resource Service Driver
Identity Manager
Server Variables
General
Mandatory Parameters | Driver Configuration | Named Passwords | Global Config Values | Engine Control Values | Log Level | Driver Image | Security Equals | Filter | Edit Filter XML | Reciprocal Attribute Mappings | Edit Reciprocal Attribute Mappings XML | Misc | Excluded Objects | Driver Health Configuration | Driver Manifest | Driver
OK
Cancel
Apply
Close

Driver Set Overview

Driver Set: TestDrivers.novell

Modify Object: DCSDriver.TestDrivers.novell

Trace level: 5

Trace file: /home/ekuprei/idmlogs/dcs.log

Trace file size limit: ○ Unlimited ● 999 MB

Trace name:

Trace messages will be prepended with the value entered for 'Trace name'

Trace file encoding: <Use Default Encoding>

14.3 Issue: Object Already Exists Error

In your server log (server.log), you may see the following error:

```
Associated object already exists in database with GUID:...
```

Here are some common causes for this error:

- The Data Collection Service driver was removed and re-added/ When you remove the Data Collection Service driver, you must also refresh the database. Otherwise, the new Data Collection Service driver will attempt to re-add the objects that already exist in the database.
- There is an overlap in scope between two Data Collection Service drivers. They are both trying to synchronize objects in the database.

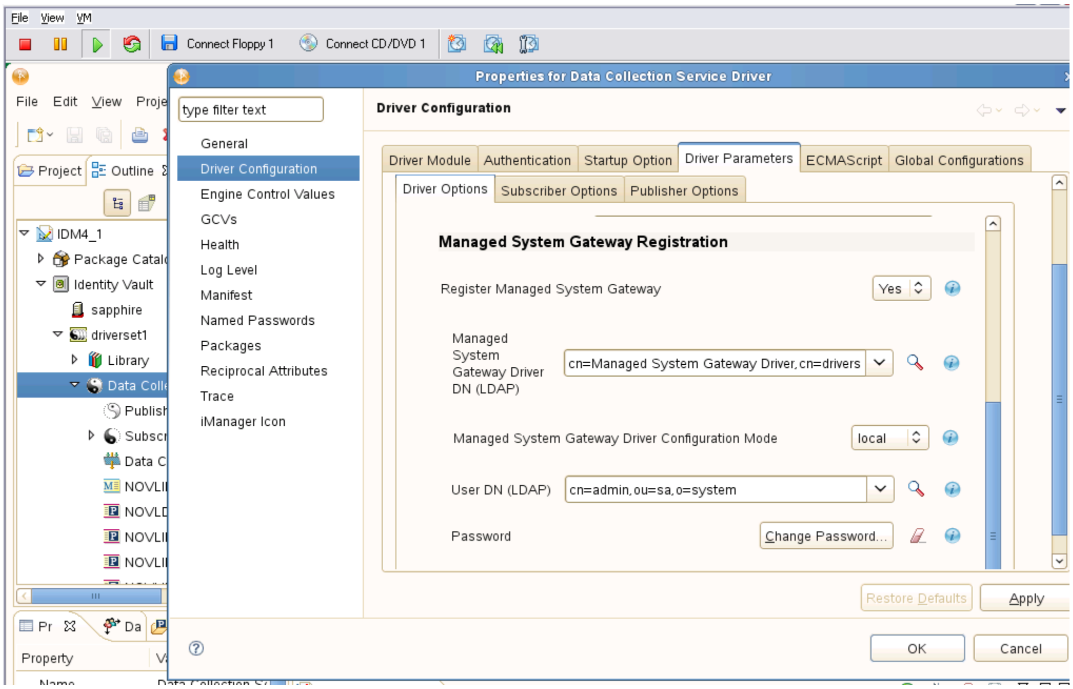
14.4 Issue: MSGW Driver is Missing from Identity Vaults Screen

If you see that the Managed System Gateway Driver is missing from the Identity Vaults screen in the Identity Reporting Module, look at the following list of possible causes:

- The Managed System Gateway driver has not been configured and deployed.
- The Data Collection Service driver is not configured to register the Managed System Gateway driver.
- The Data Collection Service driver is not running or cannot connect to the reporting module. The connection may fail if the account that the Data Collection Service driver is configured with does not have sufficient privileges, or if the reporting connection information is wrong in the Data Collection Service driver.

Here are some troubleshooting tips:

- Verify in iManager that the Managed System Gateway driver is configured and deployed to the Identity Vault.
- Verify that the Data Collection Service driver settings are correct:
    - In iManager or Designer, verify that the Data Collection Service state is *Running*.
    - In Designer, verify that the Managed System Gateway driver parameter section of the Data Collection Service driver is set to register the Managed System Gateway driver.



Driver Configuration

Managed System Gateway Registration

Register Managed System Gateway: Yes

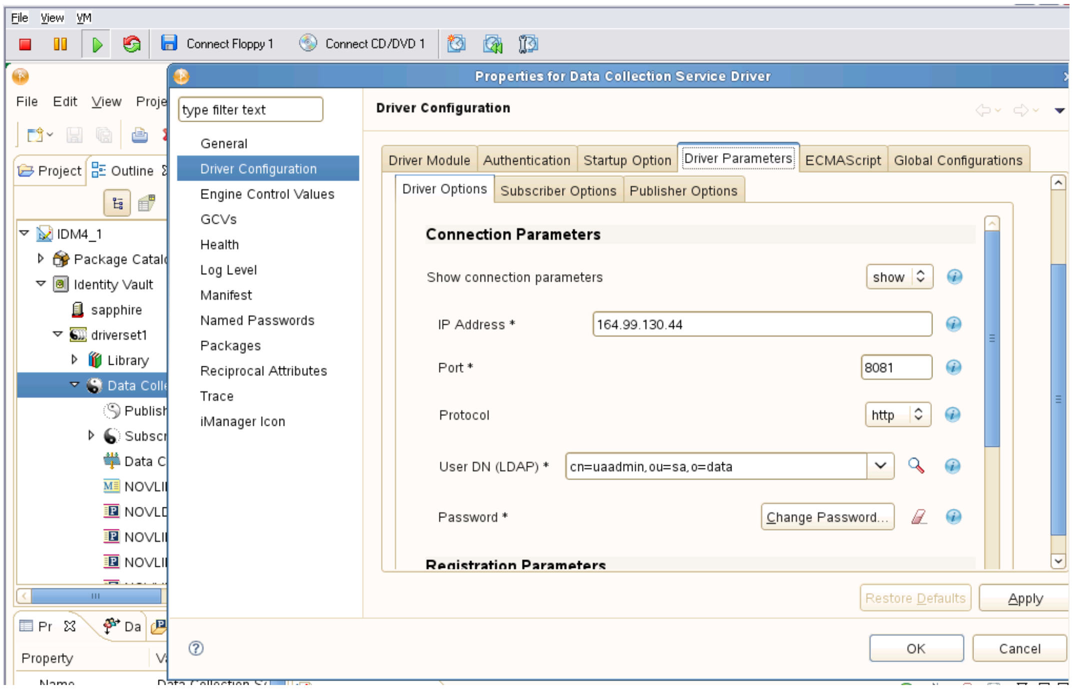
Managed System Gateway Driver DN (LDAP): cn=Managed System Gateway Driver,cn=drivers

Managed System Gateway Driver Configuration Mode: local

User DN (LDAP): cn=admin,ou=sa,o=system

Password: Change Password...

- Verify that the reporting connection information is correct in the Data Collection Service driver configuration. Check the connection URL, account, and password:



Driver Configuration

Connection Parameters

Show connection parameters: show

IP Address *: 164.99.130.44

Port *: 8081

Protocol: http

User DN (LDAP) *: cn=uaadmin,ou=sa,o=data

Password *: Change Password...

Registration Parameters

14.5 Issue: Managed System Data is Missing from Reports

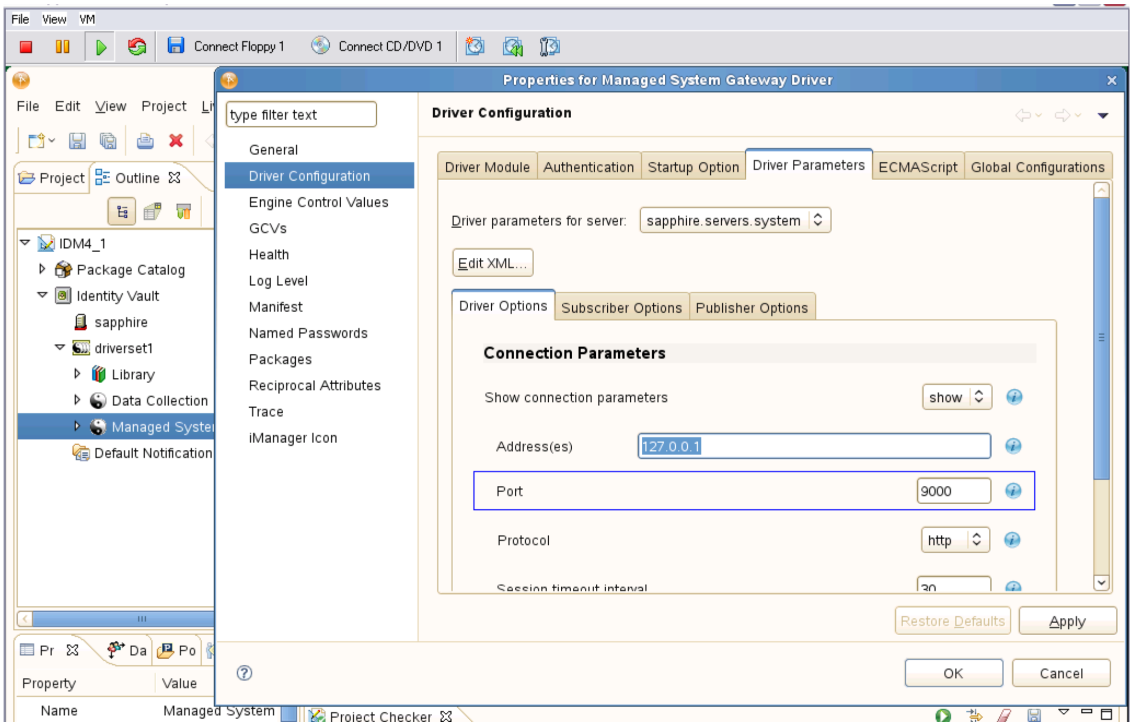
If you notice that some of the managed system data is missing from the reports, look at the following list of possible causes:

- Reports are not up-to-date.

- Pulled data collection has not been activated for the Data Collection Service driver.
- The next data collection time is in the future. Data has been changed in the managed system between data collections.
- The Managed System Gateway driver is not running.
- The Identity Manager driver for the managed system (Active Directory, SAP, and so forth) is not running.
- The managed system can be reached by the Identity Manager driver.
- The data collection process was suspended because of errors.

Here are some troubleshooting tips:

- Check to see if data missing from the report is present in the Identity Information Warehouse.
    - The data collection services use the idm_rpt_data schema space. Tables starting with the idmrpt_ms_ prefix are used to store data retrieved from the Managed System Gateway driver.
    - If the data is present, verify that the report definitions are up-to-date. Down, import, and rerun the report that is missing data.
- Verify that the Managed System Gateway driver is running. Check in iManager to see that the driver is present and the driver state is *Running*. If it is not running, start the driver and activate the data collection process on the Identity Vaults screen.
- Verify that the Managed System Gateway driver is accessible from the machine that the reporting module is running on. If the reporting module and Identity Manager are not running on the same box, verify that the Managed System Gateway driver configuration references the real IP address, rather than 127.0.0.1 (the default setting).



Driver parameters for server: sapphire.servers.system

Show connection parameters: show

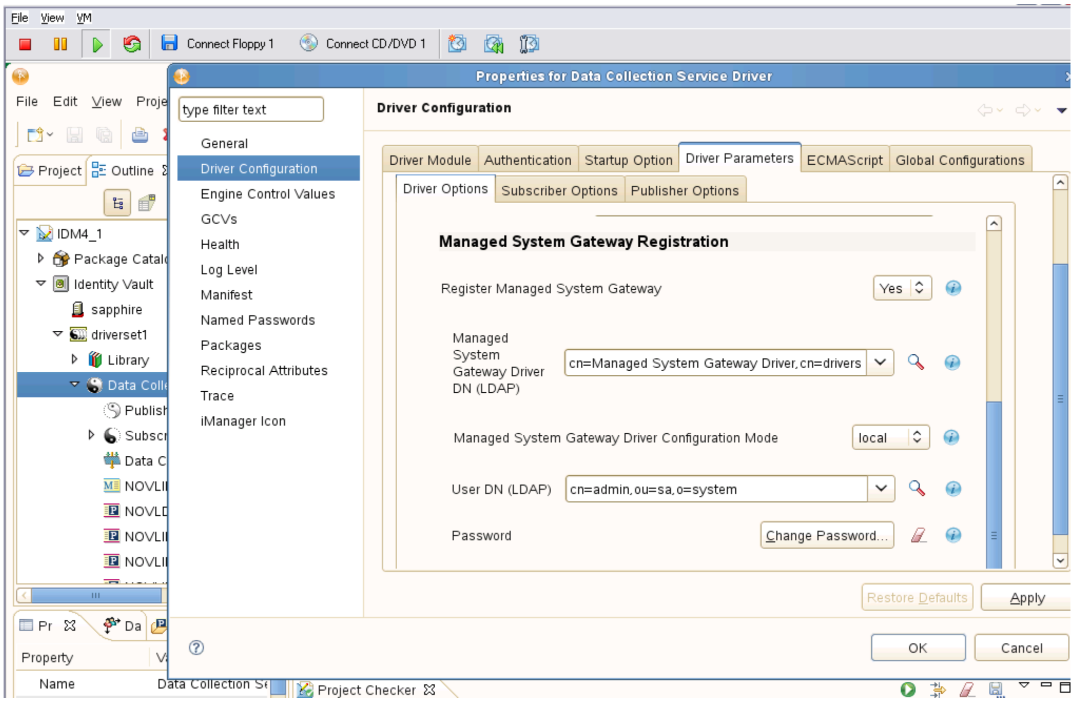
Address(es): 127.0.0.1

Port: 9000

Protocol: http

Session timeout interval: 30

- Verify that the Managed System Gateway connection information is correct.
    - In Designer, check the Managed System Gateway Registration section of the Data Collection Service driver:



Driver Configuration

Managed System Gateway Registration

Register Managed System Gateway: Yes

Managed System Gateway Driver DN (LDAP): cn=Managed System Gateway Driver,cn=drivers

Managed System Gateway Driver Configuration Mode: local

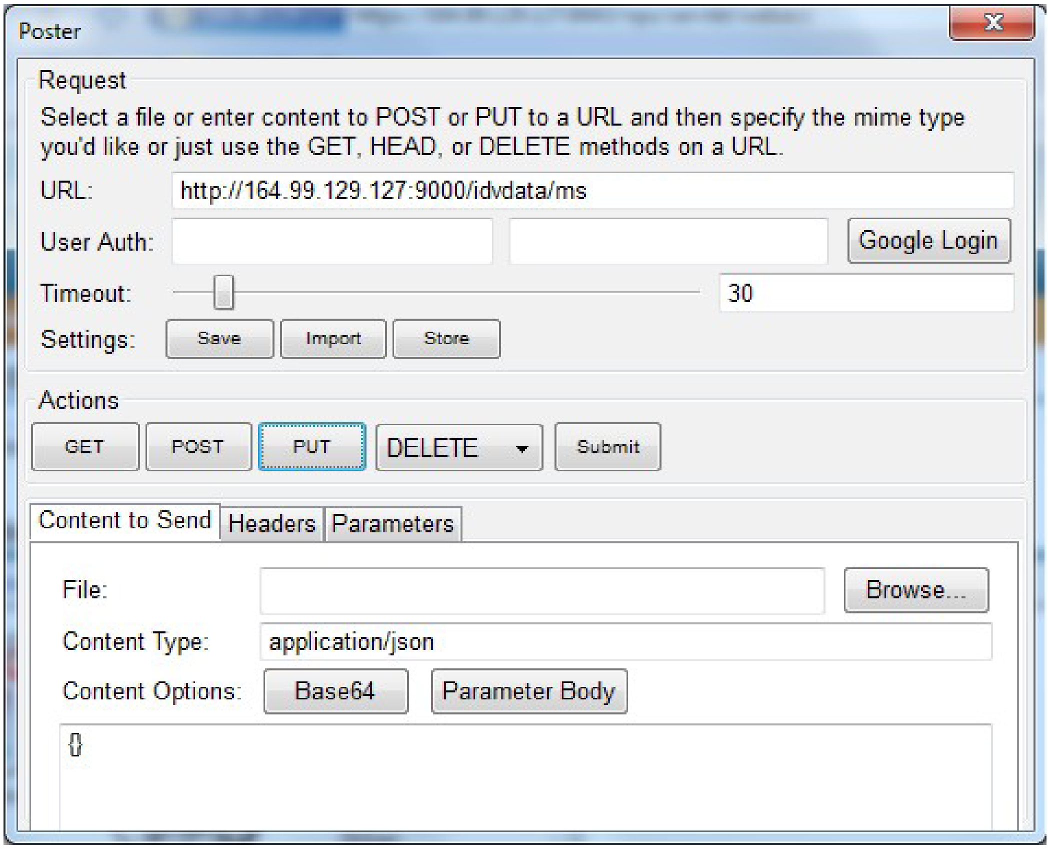
User DN (LDAP): cn=admin,ou=sa,o=system

Password: Change Password...

- Check that the proper configuration information is reflected in the idm_rpt_data.idmrpt_ms_collector table.

  ```
  select * from idm_rpt_data.idmrpt_ms_collector
  ```

- Verify that you can connect to the Managed System Gateway driver and get a response using Poster or the RESTClient Firefox plug-in.



Select a file or enter content to POST or PUT to a URL and then specify the mime type you'd like or just use the GET, HEAD, or DELETE methods on a URL.

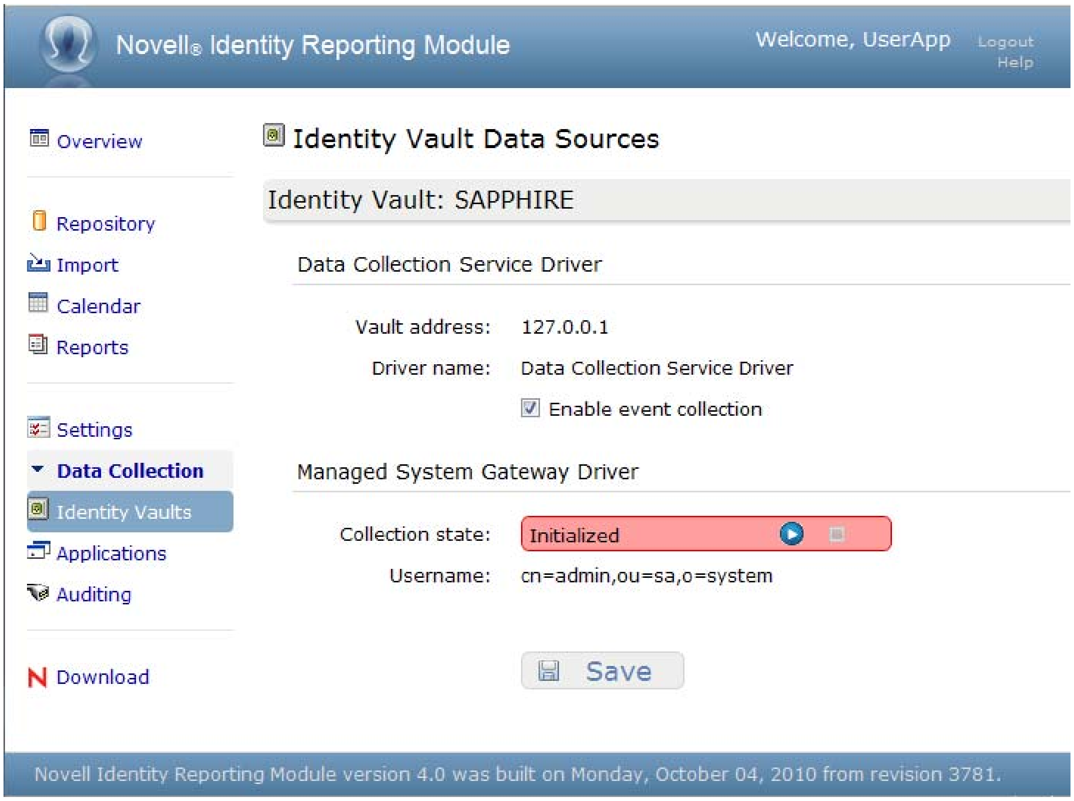
URL: http://164.99.129.127:9000/idvdata/ms

Timeout: 30

Content Type: application/json

```
{}
```

- Check the data collection status:
  - Log into the reporting module. Then, navigate to the Identity Vaults screen and verify the status of data collection for the Managed System Gateway driver.
  - If the collection status is *Initialized*, activate data collection. Then, wait until it completes, and check if the data is present.



Identity Vault Data Sources

Identity Vault: SAPPHIRE

Data Collection Service Driver

Vault address: 127.0.0.1

Driver name: Data Collection Service Driver

☑ Enable event collection

Managed System Gateway Driver

Collection state: Initialized

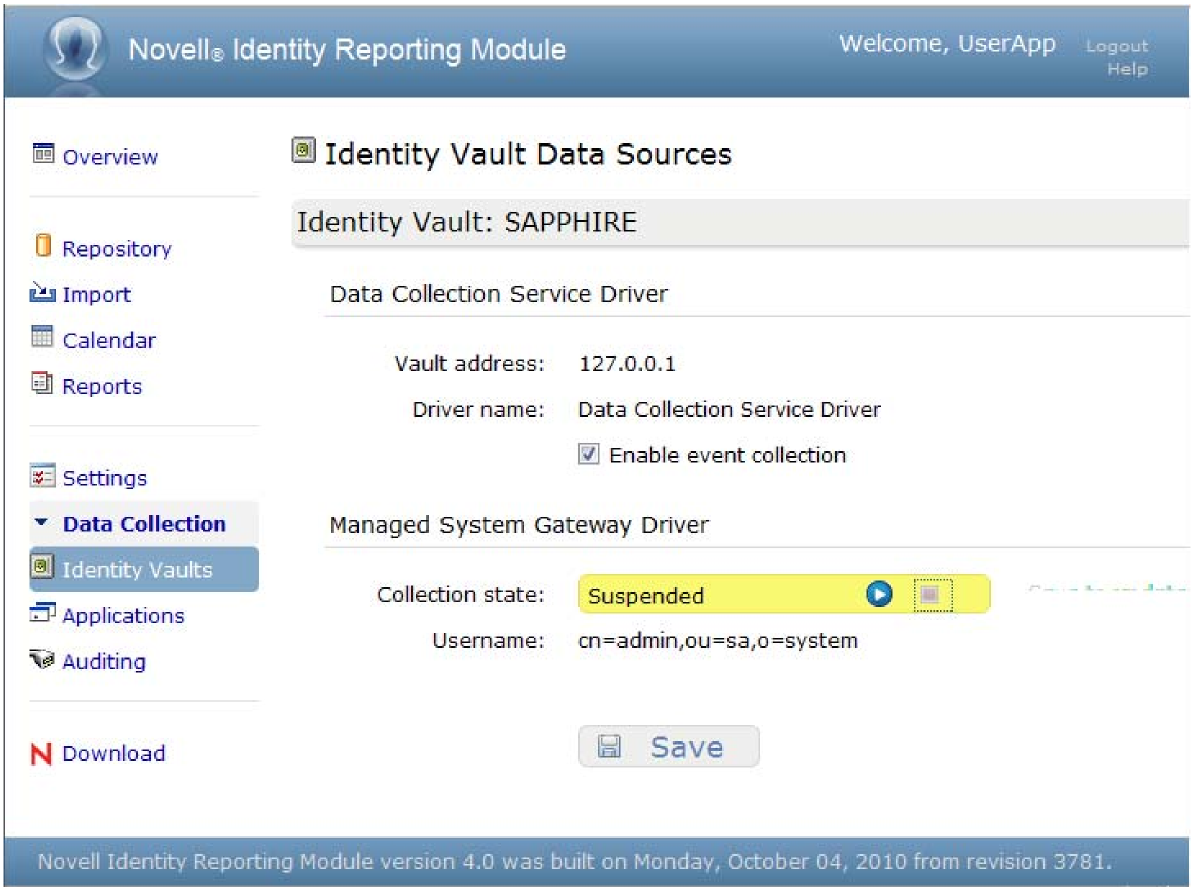
Username: cn=admin,ou=sa,o=system

Novell Identity Reporting Module version 4.0 was built on Monday, October 04, 2010 from revision 3781.

  - If the collection status is Suspended, see Section 14.6, "Issue: Status of Data Collection is Suspended," on page 301 for details on what to do.
- Verify that the managed system can be reached:
  - Check if the Identity Manager driver for the managed system is running.
  - Check to see if there are any errors in the log for the Identity Manager driver for the managed system. If there are errors, enable driver trace and reactivate data collection.

14.6 Issue: Status of Data Collection is Suspended

You may see that the data collection status is Suspended on the Identity Vaults screen, as shown below:



Identity Vault Data Sources

Identity Vault: SAPPHIRE

Data Collection Service Driver

Vault address: 127.0.0.1

Driver name: Data Collection Service Driver

☑ Enable event collection

Managed System Gateway Driver

Collection state: Suspended

Username: cn=admin,ou=sa,o=system

Novell Identity Reporting Module version 4.0 was built on Monday, October 04, 2010 from revision 3781.

In this case, you should look at the following list of possible causes:

- The Managed System Gateway driver is not running.
- The Managed System Gateway driver has incorrect connection information.
- Errors have occurred in collection services for the Data Collection Service driver.

Here are some troubleshooting tips:

- Look at the database to see if it provides any clues about what might be causing the suspension:
  - The data collection status and failure reasons are stored in the idm_rpt_data.idmrp_ms_collect_state table.
  - The Managed System Gateway driver registration is stored in the idm_rpt_data.idmrpt_ms_collector table.
  - The Data Collection Service driver registration is stored in the idm_rpt_data.idmrpt_rpt_driver table:

    ```
    select ms_collect_id, ms_query_api, ms_collect_time, ms_collect_error from
    idm_rpt_data.idmrpt_ms_collect_state where
    idm_rpt_data.idmrpt_ms_collect_state.ms_collect_state = FALSE;
    ```
- If you see a failure to connect error:
  - Verify that the Managed System Gateway driver is running. In iManager, check that the driver is present and the current status is running. If not, start the driver and activate data collection on the Identity Vaults screen.

    - Verify that the Managed System Gateway driver is accessible from the machine that the reporting module is running on. If the reporting module and Identity Manager are not running on the same box, verify that the Managed System Gateway driver configuration references the real IP address, rather than 127.0.0.1 (the default setting).

      Also, check the Managed System Gateway parameter section.

      Check that the proper configuration information is reflected in the idm_rpt_data.idmrpt_ms_collector table.

      ```
      select * from idm_rpt_data.idmrpt_ms_collector;
      ```

    - If you see an HTTP status other than 200, verify that you can execute a query from a different tool such as Poster or RESTClient.

- If you see other kinds of errors, enable logging and reactive data collection.
    - Enable Managed System Gateway driver trace logging at level 5. Delete the old trace file (if one exists) and restart the Data Collection Service driver.
    - Enabled pulled Data Collection Service driver trace logging.

      Add the following trace to the idmrptcore_logging.xml file and tail the console log (by using `tail -f server.log`). You should see trace messages with recognizable DNs, names, and so forth.

      ```
      <logger
      name="com.novell.idm.rpt.core.server.service.DataCollectMgrService"
      level="TRACE" dditivity="true"/>
      <logger name="com.novell.idm.rpt.core.server.dc" level="TRACE"
      additivity="true"/>
      ```

14.7 Issue: Status 400 Returned for Status Query

You may see a status 400 returned for a status query REST call (/idvdata/results/{requestId}/status Query). This error may occur when you execute a query with a large data set. With a large data set, a query may cause the Managed System Gateway driver to restart, which resets the session, and causes the data collection to fail.

To fix this problem, set the publisher heartbeat interval to zero.

14.8 Issue: Driver Errors Occur in Multi-Driver Set Environment

If you see Data Collection Service errors occur in a multiple driver set environment, the cause may be that the driver scope is not correctly configured.

To correct this problem, verify the driver scope settings, and make changes as necessary.

14.9 REST Endpoint Troubleshooting

To troubleshoot problems with the REST endpoints, you can use any of the following tools:

- Poster (Firefox plug-in)

  To install this tool, click on *Tools* > *Add Ons*. Then search for Poster. Select this plug-in from the list and click *Add to Firefox...* button.

- RESTClient (Firefox plug-in)

To install this tool, click on *Tools* > *Add Ons*. Then search for RESTClient. Select this plug-in from the list and click *Add to Firefox...* button.

- Curl command line client

```
curl -XGET http://myserver:8180/IDMRPT/version
```

15 String Customization

This section outlines the procedure for customizing strings in the Identity Reporting Module.

- Section 15.1, “About String Customization in the Identity Reporting Module,” on page 305
- Section 15.2, “Customizing the Strings for the Reporting Module,” on page 306

15.1 About String Customization in the Identity Reporting Module

You can customize the strings for the Identity Reporting Module into any of several supported languages. These are the supported languages:

Table 15-1 *Supported Languages*

Locale Code	Language
da	Danish
de	German
en	English
es	Spanish
fr	French
it	Italian
ja	Japanese
nl	Dutch
pt	Portuguese
ru	Russian
sv	Swedish
zh-CN	Chinese (China)
zh-TW	Chinese (Taiwan)

The strings for the reporting module are contained with a set of language-specific JAR files associated with the three main WARs used by the reporting module:

- Client WAR
- Authorization WAR
- Core WAR

The language-specific JAR files follow this pattern:

```
IDMRPT-AUTH_language.jar
IDMRPT-CORE_language.jar
IDMRPT_language.jar
```

For example, the following JAR files apply to strings in French:

```
IDMRPT-AUTH_fr.jar
IDMRPT-CORE_fr.jar
IDMRPT_fr.jar
```

15.2 Customizing the Strings for the Reporting Module

To customize the strings for one of the supported languages:

1. Customize the appropriate language-specific properties JAR file.
2. Add the new JAR file to the appropriate WAR's WEB-INF/lib directory using the `jar`command.

A Payload Schema Information

This section provides reference information for the payload schemas used with the reporting REST APIs.

A.1 Results Payload Schema

Table A-1 *JSONObject Fields*

Field	Description
SIDX	*Integer* - Starting Index. All results sets begin at index "0"
EIDX	*Integer* - Ending Index. The last result in the set is at index "EIDX – 1". When obtaining batched results, EIDX should be used as the SIDX for subsequent calls.
MORE	*Integer* - (0 or 1). Indicates if more results are available.
Results	*JSONArray* containing 0 or more JSONObject results

A.2 Fault Status Payload Schema

Table A-2 *JSONObject Fields*

Field	Description
Fault	*JSONObject* containing fault "Code" and "Reason"
Fault/Code	*JSONObject* containing fault "Value" and "Subcode"
Fault/CodeValue	*String* – Indicates if problem lies with the "Sender" or "Receiver"
Fault/Code/Subcode	*JSONObject* containing application service-specific error code or message type "Value"
Fault/Code/Subcode/Value	*String* – application service-specific error code
Fault/Reason	*JSONObject* containing descriptive "Text"
Fault/Reason/Text	*String* – Details of reason for the fault

Here is some sample output:

```
{
  "Fault":
  {
    "Code":
    {
      "Value":"Sender",
      "Subcode":
      {
        "Value":"Managed System data does not exist"
      }
    },
    "Reason":
    {
      "Text":"Managed System information is not available"
    }
  }
}
```

A.3 Managed System Information Schema

Table A-3 *JSONObject Fields*

Field	Description
GUID	*String* - Namespace Unique identifier for the non-managed application. This field is used as the Primary Key for identifying the system data in the Reporting application. The identifier must be in the 32-character hexadecimal format expected for a GUID (globally unique identifier). If the identifier does not conform to this format, you may get an exception of the type `com.novell.idm.rpt.core.server.spi.exception.DCException`. **NOTE:** This value will also be used by the Identity Manager Reporting Service as the <identifier> for all query operations to the application service.
Name	*String* - Common Name for the non-managed application
Description	*String* - Description for the application
Type	*String* - Type of application (ie. Enterprise, Email, DB, etc)
Classification	*String* - Sensitivity classification (ie. Critical, Departmental, etc.)
Vendor	*String* - Application vendor
Version	*String* - Application version
BusinessOwner	*String* - Business Owner of the application. If the owner has an account in the application, the account ID should be used in this field
ApplicationOwner	*String* - IT Owner of the application If the owner has an account in the application, the account ID should be used in this field

Field	Description
Location	*String* - Physical Location of the application
Environment	*String* - Type of application environment (ie Production, Test, Dev)
AuthenticationIPAddress	*String*
AuthenticationPort	*String*
AuthenticationID	*String* - Account ID that will be used to obtain application data
Hierarchical	*String* - Indicates if the application uses a hierarchical namespace

The following fields are present if the application service supports the concept of a Logical System:

Table A-4 *Fields for Application Services that Support a Logical System*

Field	Description
LogicalInstance:ID	Similar to GUID. **NOTE:** This value(s) will also be used by the Identity Manager Reporting Service as the <ls-identifier> for all query operations to the application service.
LogicalInstance:Name	Similar to Name
LogicalInstance:Description	Similar to Description
LogicalInstance:Type	Similar to Type
LogicalInstance:Classification	Similar to Classification
LogicalInstance:Vendor	Similar to Vendor
LogicalInstance:Version	Similar to Version
LogicalInstance:BusinessOwner	Similar to BusinessOwner
LogicalInstance:ApplicationOwner	Similar to ApplicationOwner
LogicalInstance:Location	Similar to Location
LogicalInstance:Environment	Similar to Environment
LogicalInstance:AuthenticationIPAddress	Similar to AuthenticationIPAddress
LogicalInstance:AuthenticationPort	Similar to AuthenticationPort
LogicalInstance:AuthenticationID	Similar to AuthenticationID

A.4 Entitlements Types Schema

Table A-5 *JSONObject Fields*

Field	Description
ENT_ID	*String* – Application-specific identifier of the entitlement type. This may be an object classname, well-known identifier, etc.
ENT_TYPE	*String* – Type of entitlement
ENT_TYPE_DISPLAY_NAME	*String* – User readable form of ENT-TYPE
ENT_CATEGORY	*String* – general categorization of entitlement (ie. Group, Security Profile, ACL, etc.)
ENT_DESCRIPTION	*String* – Description of entitlement
ENT_DISPLAY_NAME	*String* – User readable form of ENT-ID

A.5 Entitlements Information Schema

Table A-6 *JSONObject Fields*

Field	Description
MS_ENT_VAL	*String* – Entitlement value (ie. Group name, Role Name, etc)
MS_ENT_DESC	*String* – Description of entitlement
MS_ENT_VAL_DISP_NAME	*String* – User-readable form of entitlement (Useful if MS_ENT_VAL is a GUID)

A.6 Entitlements Assignments Schema

Table A-7 *JSONObject Fields*

Field	Description
MS_ENT_VAL	*String* – For valued entitlements, the name of the particular entitlement assigned. For non-valued entitlements, the entitlement type identifier (ENT_ID)
MS_MEMBER	*String* – The ID of the application Account that has been assigned the entitlement
MS_MEM_IDV_ASSOC	*String* – Identity Vault Association value for theaccount in the connected system. **NOTE:** This field exists for use by Novell Identity Manager. It should be omitted from Results from non-managed application systems.

A.7 Accounts Rule Schema

***Table A-8** Field Description*

Field	Description
Order	*Integer* – indicates the evaluation priority of the rule when more than one result is present.
MatchAttrName	*String* – contains one or more comma-separated attribute names that will be used for matching accounts with accounts information collected from other systems.

A.8 Account Information Schema

***Table A-9** JSONObject FIelds*

Field	Description
ACCT_ID_VALUE	*String* - Account Identifier in application. This value is generally the application Primary Key value in the IDM Reporting database. Once a Primary key attribute is used for the account, the application service must use that value for the ACCT_ID_VALUE in the /profiles API results.
ACCT_ID_TYPE	*String* - Type of Account (ie. USER, EMAIL, etc.)
Managed	*Boolean* – Indicates if the account is within a connected system being managed by Novell Identity Manager. A non-managed system should return false.
APP_NAME	*String* – Name to be used to identify the application (See "Name" in the Managed System Information Schema)
Synchronized	*Boolean* – Indicates if the account is being synchronized using Novell Identity Manager. A non-managed system should return false
ACCT_STATUS	*Enum* – Status of the account in the application: ◆ "A" – Active ◆ "I" – Inactive ◆ "U" – Undefined

Field	Description
MS_ACCT_GLOBAL_IDENTIFIER	*String* – This field should ONLY be used if a single GUID is used to identify multiple accounts in the application. If it IS used, this value will be used as the Primary Key in the Reporting database. Once a Primary key attribute is used for the account, the application service must use that value for the ACCT_ID_VALUE in the /profiles API results.
IDV_ASSOCIATION	*String* – Identity Vault Association value for theaccount in the connected system. **NOTE:** This field exists for use by Novell Identity Manager. It should be omitted from Results from non-managed application systems.
IDV_ACCT_STATUS	*Enum* – Status of the account in the application: ◆ "A" – Active ◆ "I" – Inactive ◆ "U" – Undefined **NOTE:** This field exists for use by Novell Identity Manager. It should be omitted from Results from non-managed application systems.
IDV_ACCT_DN	*String* – Identity Vault distinguished name for the associated account. **NOTE:** This field exists for use by Novell Identity Manager. It should be omitted from Results from non-managed application systems.

A.9 Profile Information Schema

Table A-10 *JSONObject Fields*

Field	Description
ACCT_ID_VALUE	*String* - Account ID for Identity
FIRST_NAME	*String*
LAST_NAME	*String*
MIDDLE_INITIAL	*String*
FULL_NAME	*String*
JOB_TITLE	*String*
DEPARTMENT	*String*
LOCATION	*String*
EMAIL_ADDRESS	*String*
OFFICE_PHONE	*String*

Field	**Description**
CELL_PHONE	*String*
PRIVATE_PHONE	*String*
IM_ID	*String*
PHOTO	*Octet-String*
GEN_QAL	*String* – Generational Qualifier
PREFIX	*String* – Salutory prefix (ie. Mr., Mdm., Dr., etc.)
PREFERRED_NAME	*String*
PREFERRED_LANG	*String* – 2 character Language ISO code
JOB_CODE	*String*
WORKFORCE_ID	*String*
COST_CENTER	*String*
EMPLOYEE_STATUS	*String*
EMPLOYEE_TYPE	*String*
COMPANY	*String*
DEPARTMENT_NUMBER	*String*
MAILSTOP	*String*
SUITE_NUMBER	*String*
STREET_ADDRESS	*String*
CITY	*String*
POSTAL_CODE	*String*
STATE	*String*
COUNTRY	*String*
PAGER_NUMBER	*String*
IS_MANAGER	*String*
MANAGER_WF_ID	*String* – Manager Workforce ID
HIRE_DATE	*String*
TRANSFER_DATE	*String*
TERMINATION_DATE	*String*
FIRST_WRK_DAY	*String*
LAST_WRK_DAY	*String*
IDENTITY_DESC	*String* – Description