
NetIQ® Identity Manager Identity Reporting Module Guide

December 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	7
About NetIQ Corporation	9
1 Welcome to the Identity Reporting Module	11
1.1 About the Identity Reporting Module	11
1.2 Identity Manager Reporting Architecture	12
1.3 Basic Setup and Configuration.	16
1.4 Working in the Identity Reporting Module	17
1.5 Security Considerations	17
1.5.1 Authentication Token Exposure	17
2 Installation	19
3 Getting Started	21
3.1 Accessing the Identity Reporting Module.	21
3.1.1 Launching the Reporting Module from the Identity Manager Home Page.	21
3.1.2 Starting the Reporting Module Directly with a URL	22
3.2 Exploring the Identity Reporting Module	22
3.2.1 Getting Help.	22
3.2.2 Token Timeout	23
4 Using the Overview Page	25
4.1 About the Overview Page	25
4.2 Viewing the Report Summary.	25
4.3 Searching for a Report Definition	26
4.4 Viewing the List of Recently Completed Reports	26
4.5 Viewing the List of Upcoming Reports	26
4.6 Viewing the Configurations.	26
5 Managing the Report Repository	27
5.1 Viewing the Report Definitions	27
5.2 Modifying a Report Definition	28
5.3 Creating a Custom Report Definition Based on an Existing Definition.	31
5.4 Running a Report On Demand.	31
5.5 Deleting a Report Definition	31
5.6 Performing Bulk Actions	31
5.7 Searching for a Report Definition	32
5.8 Sorting the List of Reports	33
5.9 Defining the Repository Display Options	33
5.10 Refreshing the Report Definition List	33
6 Using the Import Tool	35
6.1 Using the Import Page to Import Report Definitions.	35

6.2	Automatically Importing Report Definitions	36
6.3	Using the Download Page to Download Report Definitions	36
7	Using the Calendar Page	39
7.1	Viewing the Calendar	39
7.1.1	Displaying the Calendar Page	39
7.1.2	Scrolling within the Calendar Display	40
7.1.3	Viewing the Schedule for Today	40
7.2	Checking the Status of a Schedule Instance	40
7.3	Viewing the Summary Information for a Schedule Instance	40
7.4	Viewing a Completed Report	40
7.5	Editing a Schedule Instance	41
7.6	Deleting a Schedule Instance	42
7.7	Moving a Single Schedule Instance	42
7.8	Moving All Schedule Instances	42
7.9	Defining the Calendar Display Options	43
7.10	Refreshing the Display	43
8	Using the Completed and Running Reports Page	45
8.1	Viewing the List of Completed and Running Reports	45
8.2	Viewing a Completed Report	45
8.3	Viewing the Details for a Report	46
8.4	Deleting a Report	46
8.5	Performing Bulk Actions	46
8.6	Searching for a Report	47
8.7	Sorting the List of Reports	48
8.8	Defining the Reports Display Options	48
8.9	Refreshing the Completed Report List	48
9	Configuring Settings and Data Collection	49
9.1	Defining the General Settings	49
9.2	Managing Data Sources	50
9.3	Defining the Identity Vault Settings for Managed Systems	51
9.4	Defining the Settings for Non-Managed Applications	52
9.5	Defining the Auditing Configuration	54
9.6	Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver	56
9.6.1	Configuring EAS to Receive Events	56
9.6.2	Configuring Sentinel to Send Events	56
10	Creating Custom Report Definitions	59
10.1	About Custom Report Definitions	59
10.2	Starting the Report Packaging Tool	59
10.3	Creating a New Report Template	60
10.4	Configuring Your JDBC Connection in iReport	60
10.5	Setting the Description and Other Strings for Your Report	61
10.6	Setting the Report Definition Parameters	61
10.6.1	Defining the Parameter XML File	62
10.6.2	Defining the Type for a Parameter	63
10.6.3	Defining an OptionQuery Parameter	64
10.7	Customizing the Report in iReport	65
10.8	Displaying Parameters and Selected Criteria in the Report	68

10.9	Building Your Report	69
------	----------------------	----

11 Schema Documentation 71

11.1	About the Database Views	72
11.2	idmrpt_acct_link_v	73
11.3	idmrpt_approver_v	74
11.4	idmrpt_association_v	74
11.5	idmrpt_ext_idv_item_v	74
11.6	idmrpt_cat_item_types_v	75
11.7	idmrpt_cat_mappings_v	75
11.8	idmrpt_category_v	75
11.9	idmrpt_ms_collect_state_v	76
11.10	idmrpt_container_v	76
11.11	idmrpt_ext_attr_v	77
11.12	idmrpt_ext_obj_v	77
11.13	idmrpt_dc_service_cfg_v	77
11.14	idmrpt_ent_param_token_value_v	78
11.15	idmrpt_ent_type_v	78
11.16	idmrpt_ext_item_attr_v	79
11.17	idmrpt_group_v	79
11.18	idmrpt_identity_v	79
11.19	idmrpt_ms_identity_v	81
11.20	idmrpt_idv_v	83
11.21	idmrpt_idv_acct_v	83
11.22	idmrpt_idv_drivers_v	84
11.23	idmrpt_idv_ent_v	84
11.24	idmrpt_idv_ent_bindings_v	85
11.25	idmrpt_idv_identity_trust_v	85
11.26	idmrpt_idv_prd_v	86
11.27	idmrpt_idv_trust_types_v	87
11.28	idmrpt_container_types_v	87
11.29	idmrpt_ms_v	87
11.30	idmrpt_ms_acct_v	88
11.31	idmrpt_ms_acct_rule_v	89
11.32	idmrpt_ms_collector_v	90
11.33	idmrpt_ms_ent_v	91
11.34	idmrpt_ms_ent_type_v	91
11.35	idmrpt_ms_ent_trust_v	92
11.36	idmrpt_owners_v	93
11.37	idmrpt_res_parameter_v	93
11.38	idmrpt_resource_v	93
11.39	idmrpt_role_v	94
11.40	idmrpt_role_level_v	95
11.41	idmrpt_role_mappings_v	95
11.42	idmrpt_role_res_assoc_v	95
11.43	idmrpt_role_res_assoc_param_v	96
11.44	idmrpt_rpt_driver_v	96
11.45	idmrpt_rpt_driver_scope_v	97
11.46	idmrpt_sod_v	97
11.47	idmrpt_sod_violations_v	97
11.48	idmrpt_approval_v	98
11.49	idmrpt_team_v	98

11.50 idmrpt_team_assignments_v	99
12 REST Services for Reporting	101
13 Troubleshooting the Drivers	103
13.1 Issue: No Identity Vaults Presented on the Identity Vaults Screen.	103
13.2 Issue: Reports Are Missing Identity Vault Data	104
13.3 Issue: Object Already Exists Error	105
13.4 Issue: MSGW Driver is Missing from Identity Vaults Screen	106
13.5 Issue: Managed System Data is Missing from Reports	106
13.6 Issue: Status of Data Collection is Suspended	108
13.7 Issue: Status 400 Returned for Status Query	109
13.8 Issue: Driver Errors Occur in Multi-Driver Set Environment.	109
13.9 REST Endpoint Troubleshooting	109
14 String Customization	111
14.1 About String Customization in the Identity Reporting Module	111
14.2 Customizing the Strings for the Reporting Module.	112
A Payload Schema Information	113
A.1 Results Payload Schema	113
A.2 Fault Status Payload Schema	113
A.3 Managed System Information Schema	114
A.4 Entitlements Types Schema.	116
A.5 Entitlements Information Schema	116
A.6 Entitlements Assignments Schema	116
A.7 Accounts Rule Schema	117
A.8 Account Information Schema.	117
A.9 Profile Information Schema	118

About this Book and the Library

The *Identity Reporting Module Guide* describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as provides installation instructions.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides an overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provide implementation information about Identity Manager drivers.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit <http://community.netiq.com>.

1 Welcome to the Identity Reporting Module

This section provides an overview of the Identity Reporting Module.

- ◆ Section 1.1, “About the Identity Reporting Module,” on page 11
- ◆ Section 1.2, “Identity Manager Reporting Architecture,” on page 12
- ◆ Section 1.3, “Basic Setup and Configuration,” on page 16
- ◆ Section 1.4, “Working in the Identity Reporting Module,” on page 17
- ◆ Section 1.5, “Security Considerations,” on page 17

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 about the predefined reports, see *Using Identity Manager Reports* (http://www.netiq.com/documentation/idm45/idm_reports/data/bookinfo.html).

The core of the Reporting Module is the *Identity Information Warehouse*, 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 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 the following 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 4.5, 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 the engine does not manage.

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

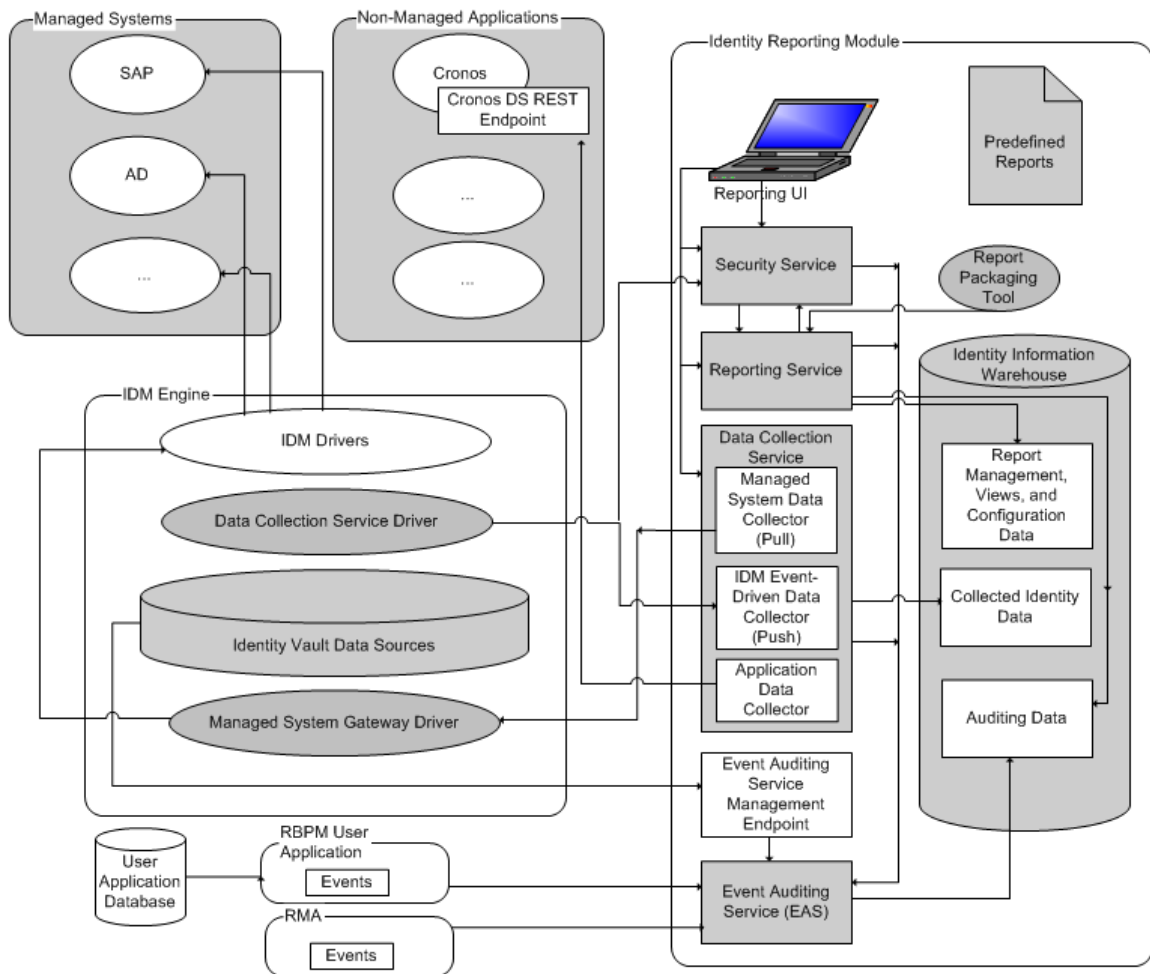
data that is pushed to the Identity Vault. To do this, you add a filter to the Data Collection Service Driver to add custom objects or attributes, causing these additional pieces of information to be stored in the warehouse. When this data is available, you can write custom reports to see this information.

The Reporting Module is tightly integrated with the *Event Auditing Service (EAS)*. The EAS is a software component that captures log events associated with actions performed in several NetIQ products, including the Reporting Module, the Roles Based Provisioning Module (RBPM), the Catalog Administrator, 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 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.

1.2 Identity Manager Reporting Architecture

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

Figure 1-1 Reporting Architecture



Each of the major components is described below:

Table 1-1 Major Components of the IDM Reporting Architecture

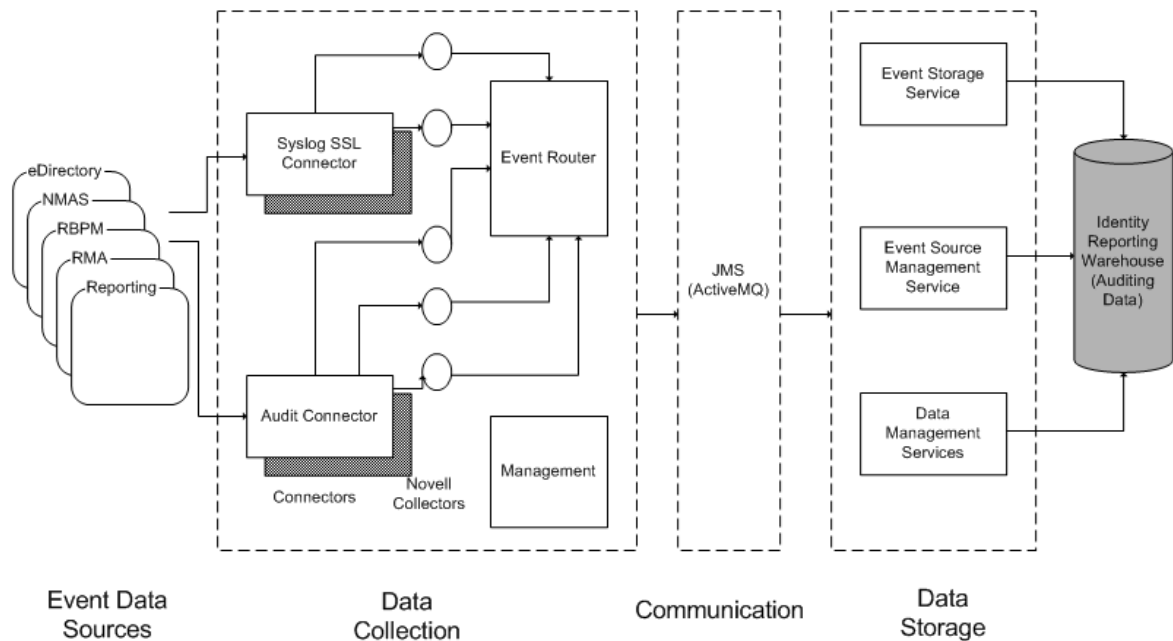
Component	Description
Identity Reporting Module	Browser-based application that generates reports by making calls to the Reporting Service.
Predefined Reports	<p>Set of predefined report definitions you can use to generate reports.</p> <p>You can also import custom reports you define in a third-party tool.</p> <p>For details about the predefined reports, see Using Identity Manager Reports (http://www.netiq.com/documentation/idm45/idm_reports/data/bookinfo.html).</p>
Report Packaging Tool	<p>Facilitates the process of creating new reports.</p> <p>You can customize reports in iReport and use the Report Packaging Tool to package them for use within the Reporting Module.</p>
Reporting Service	<p>Service that retrieves the data needed to generate reports 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</p> <p>To produce reports, the Reporting Service invokes the JasperReports engine, which compiles and executes report definitions according to schedules that the Report Administrator defines.</p>
Identity Information Warehouse	<p>Repository for the following kinds of information:</p> <ul style="list-style-type: none"> ◆ 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 <code>idm_rpt_cfg</code> 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 <code>idm_rpt_data</code> schema. ◆ Auditing data, which includes events that the EAS collects. This data is stored in tables within the <code>public</code> schema. <p>The Identity Information Warehouse stores its data in the Security Information and Event Management (SIEM) database.</p>
Data Collection Service	<p>Service that collects information from various sources within an organization.</p> <p>The Data Collection Service includes three subservices:</p> <ul style="list-style-type: none"> ◆ 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 that the Data Collection Service Driver captures. ◆ 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	<p data-bbox="651 218 1438 275">Driver that captures changes to objects stored in an Identity Vault, such as accounts, roles, resources, groups, and team memberships.</p> <p data-bbox="651 302 1438 384">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.</p> <p data-bbox="651 411 1438 438">The information that the driver captures records changes to these objects:</p> <ul data-bbox="678 466 1370 951" style="list-style-type: none"> <li data-bbox="678 466 1008 493">◆ User accounts and identities <li data-bbox="678 506 1370 533">◆ Roles and role levels (hierarchical relationships between roles) <li data-bbox="678 546 789 573">◆ Groups <ul data-bbox="706 590 1438 646" style="list-style-type: none"> <li data-bbox="706 590 1438 646">NOTE: The Reporting Module does not support dynamic groups and only generates reports on static group data. <li data-bbox="678 659 924 686">◆ Group memberships <li data-bbox="678 699 1138 726">◆ Provisioning Request Definitions (PRDs) <li data-bbox="678 739 1271 766">◆ Separation of Duties (SoDs) definitions and violations <li data-bbox="678 779 1019 806">◆ User entitlement associations <li data-bbox="678 819 1198 846">◆ Resource definitions and resource parameters <li data-bbox="678 858 1044 886">◆ Role and resource assignments <li data-bbox="678 898 1305 926">◆ Identity Vault entitlements, entitlement types, and drivers
Managed System Gateway Driver	<p data-bbox="651 978 1438 1005">Driver that collects information from managed systems.</p> <p data-bbox="651 1033 1438 1089">To retrieve the managed system data, the driver queries the Identity Vault. The driver retrieves the following information:</p> <ul data-bbox="678 1102 1403 1251" style="list-style-type: none"> <li data-bbox="678 1102 1003 1129">◆ List of all managed systems <li data-bbox="678 1142 1179 1169">◆ List of all accounts for the managed systems <li data-bbox="678 1182 1403 1251">◆ Entitlement types, values, and assignments (groupings), and user account profiles for the managed systems
Security Service	<p data-bbox="651 1278 1438 1335">Service that controls access to all other services within the Reporting Module.</p> <p data-bbox="651 1362 1438 1390">The Security Service includes these key components:</p> <ul data-bbox="678 1417 1438 1793" style="list-style-type: none"> <li data-bbox="678 1417 1438 1528">◆ 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. <li data-bbox="678 1541 1438 1623">◆ 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. <li data-bbox="678 1635 1438 1793">◆ 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)	<p>Captures log events associated with actions performed in several NetIQ products, including the Reporting Module, the Roles Based Provisioning Module (RBPM), Catalog Administrator, and eDirectory. These events are stored in the public schema within the warehouse.</p> <p>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 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.</p>
Identity Vault Data Sources	<p>Repositories for identity information.</p> <p>The 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.</p> <p>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.</p>
Managed Systems	<p>A system in an enterprise that is connected to the Identity Vault with an Identity Manager driver.</p> <p>The 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 Reporting Module allows you to report on current and past data from managed systems.</p>
Applications	<p>Any non-managed application running in an enterprise.</p> <p>A non-managed application is an application that is not connected to the Identity Vault.</p> <p>To include information from a non-managed application, implement a REST endpoint as outlined in the REST API documentation. Also configure a custom data source for the application on the Non-Managed Application Data Sources page within the Reporting Module, as described in the REST API documentation. The Reporting installation program deploys a special API WAR file, <code>rptdoc.war</code>, which contains the documentation of REST services needed for reporting. For more information accessing the REST API documentation, see Chapter 12, "REST Services for Reporting," on page 101.</p>

The following diagram shows the components of the EAS architecture:

Figure 1-2 EAS Architecture



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

- ♦ Syslog SSL Connector
- ♦ Syslog UDP Connector
- ♦ Audit Connector

Different NetIQ applications use different connectors:

- ♦ You can configure the Catalog Administrator to use the Audit Connector or the Syslog SSL Connector.
- ♦ You can configure Identity Manager and eDirectory to use the Audit Connector or the Syslog SSL Connector.
- ♦ The RBPM uses the Audit Connector.

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

1.3 Basic Setup and Configuration

The prerequisites and configuration for installing the Reporting Module are described in “[Planning to Install Identity Reporting](#)” in the *NetIQ Identity Manager Setup Guide*.

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 users 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` within 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.

To customize the user interface using the `custom.css` file:

- 1 Create a new directory in the home directory of the user running the server.
For example, if you are running as `root`, run the following command:

```
mkdir /root/novl_rpt_custom
```
- 2 Add your `custom.css` file to the `novl_rpt_custom` folder created in [Step 1](#).
- 3 If the application server is already running, refresh your browser to see the changes. Otherwise, restart the application server and clear the cache from your browser.

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 to 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 the Internet Explorer address bar when users open PDF files for reports. This happens because the browser handles links to PDFs instead of JavaScript handling the links.

Do not copy and paste links to report PDFs. If the token has not yet expired and the user has not logged out, the link receiver, 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

The Identity Reporting Module is a component of Identity Information Warehouse (the Warehouse). The installation process for Information Warehouse includes all components required for the application:

- ♦ NetIQ Identity Reporting
- ♦ NetIQ Event Auditing System (EAS)
- ♦ Identity Manager Managed System Gateway Driver (MSGW driver)
- ♦ Identity Manager Data Collection Service Driver (DCS driver)

For installation information, see “[Installing the Identity Reporting Components](#)” in the *NetIQ Identity Manager Setup Guide*.

3 Getting Started

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

- ♦ [Section 3.1, “Accessing the Identity Reporting Module,” on page 21](#)
- ♦ [Section 3.2, “Exploring the Identity Reporting Module,” on page 22](#)

3.1 Accessing the Identity Reporting Module

You can launch Reporting Module from the Identity Manager Home page or access it directly from a browser.

By default, Identity Manager uses One SSO Provider (SSO) for single sign-on access in Identity Manager. When you install Identity Reporting, you specify the basic settings for user authentication. However, you can also configure the OSP authentication server to accept authentication from the Kerberos ticket server or SAML IDP. For example, you can use SAML to support authentication from NetIQ Access Manager. For more information, see [“Using Single Sign-on Access in Identity Manager”](#) in the *NetIQ Identity Manager Setup Guide*.

- ♦ [Section 3.1.1, “Launching the Reporting Module from the Identity Manager Home Page,” on page 21](#)
- ♦ [Section 3.1.2, “Starting the Reporting Module Directly with a URL,” on page 22](#)

NOTE: To access the Reporting Module, LDAP users must be a Reporting Administrator and be able to read all the attributes in their own user object. Therefore, grant the user read trustee rights to the user's own `nrfMemberOf` attribute.

3.1.1 Launching the Reporting Module from the Identity Manager Home Page

Identity Manager 4.5 includes Identity Manager Home and Identity Manager Provisioning Dashboard. Identity Manager Home (the Home page) provides a single access point for all Identity Manager users and administrators. It allows access to all existing functionality in RBPM and the User Application, as well as provides additional user-oriented features.

To access the Reporting Module from the Identity Manager Home page, log in to the Identity Manager Home page using the OSP login as a Report Administrator. For more information, see [“Accessing Identity Manager Home”](#) in the *NetIQ Identity Manager Home and Provisioning Dashboard User Guide*. After you log in, the Identity Manager Landing page displays. This page provides default links to the basic tasks users and administrators need to perform in Identity Manager. You can access the

Home page with any supported Web browser, from either a computer or a tablet. For more information, see “[System Requirements for the Identity Applications](#)” in the *NetIQ Identity Manager Setup Guide*.

3.1.2 Starting the Reporting Module Directly with a URL

To access the 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/
```

3.2 Exploring the Identity Reporting Module

After you log in, the 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.

The following menu choices are available:

- ◆ *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 25](#).
- ◆ *Repository*
To learn about this tab and how to work with it, see [Chapter 5, “Managing the Report Repository,” on page 27](#).
- ◆ *Import*
To learn about this tab and how to work with it, see [Chapter 6, “Using the Import Tool,” on page 35](#).
- ◆ *Calendar*
To learn about this tab and how to work with it, see [Chapter 7, “Using the Calendar Page,” on page 39](#).
- ◆ *Reports*
To learn about this tab and how to work with it, see [Chapter 8, “Using the Completed and Running Reports Page,” on page 45](#).
- ◆ *Settings*
To learn about this tab and how to work with it, see [Chapter 9, “Configuring Settings and Data Collection,” on page 49](#).
- ◆ *Data Sources*
To learn about this tab and how to work with it, see [Chapter 9, “Configuring Settings and Data Collection,” on page 49](#).
- ◆ *Data Collection*
To learn about this tab and how to work with it, see [Chapter 9, “Configuring Settings and Data Collection,” on page 49](#).

3.2.1 Getting Help

While working in the Reporting Module, click the **Help** link to display the online version of this guide.

3.2.2 Token Timeout

Instead of timing out when a user session is idle, the 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 Reporting Module.

The token timeout feature reduces the risk that an unauthorized user could impersonate a user who had previously logged in to the Reporting Module. After a timeout occurs, 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 another person can reuse the session information.

4 Using the Overview Page

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

- ♦ [Section 4.1, “About the Overview Page,” on page 25](#)
- ♦ [Section 4.2, “Viewing the Report Summary,” on page 25](#)
- ♦ [Section 4.3, “Searching for a Report Definition,” on page 26](#)
- ♦ [Section 4.4, “Viewing the List of Recently Completed Reports,” on page 26](#)
- ♦ [Section 4.5, “Viewing the List of Upcoming Reports,” on page 26](#)
- ♦ [Section 4.6, “Viewing the Configurations,” on page 26](#)

4.1 About the Overview Page

The **Overview** page is the first page you see when you log in to the 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 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 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.

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.

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 about entering a search string, see [Section 5.7, “Searching for a Report Definition,”](#) on page 32.

- 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.

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.

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.

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 Managing the Report Repository

This section provides instructions about managing the **Repository** page in the Identity Reporting Module.

- ◆ [Section 5.1, “Viewing the Report Definitions,” on page 27](#)
- ◆ [Section 5.2, “Modifying a Report Definition,” on page 28](#)
- ◆ [Section 5.3, “Creating a Custom Report Definition Based on an Existing Definition,” on page 31](#)
- ◆ [Section 5.4, “Running a Report On Demand,” on page 31](#)
- ◆ [Section 5.5, “Deleting a Report Definition,” on page 31](#)
- ◆ [Section 5.6, “Performing Bulk Actions,” on page 31](#)
- ◆ [Section 5.7, “Searching for a Report Definition,” on page 32](#)
- ◆ [Section 5.8, “Sorting the List of Reports,” on page 33](#)
- ◆ [Section 5.9, “Defining the Repository Display Options,” on page 33](#)
- ◆ [Section 5.10, “Refreshing the Report Definition List,” on page 33](#)

5.1 Viewing the Report Definitions

When you click **Repository** in the left navigation menu, the Repository shows the list of reports that have been imported into the Reporting Module.

For each report definition, the list shows the report name and description, as well as any tags that have been specified for the report. The reports that ship with the product include one version with both historical and current state information and one version with only current state information. The reports that include only current state information include “Current State” in the report name.

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. You cannot delete this report and you should not run it by itself. In addition, this report does not show a check box next to it in the list, because it cannot 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 Reporting Module ships with a set of predefined reports. Import these into the Reporting Module. After you import them, the reports are included in 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 about the predefined reports, see [Using Identity Manager Reports \(http://www.netiq.com/documentation/idm45/idm_reports/data/bookinfo.html\)](http://www.netiq.com/documentation/idm45/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, design the report layout outside of the 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 Modifying a Report Definition

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

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.

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. Use tags 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 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, separate them with commas. Defined tags are 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.

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.

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.

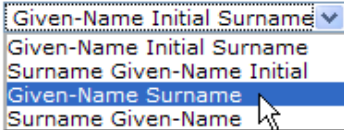
The following criteria parameters are available with most of the reports installed with the Reporting Module:

Parameter	Description
Data Source	<p>Defines the data source on which you want to report. This parameter is required for all reports.</p> <p>To run a report on multiple data sources, copy the report and then select the desired data source when you define the report criteria for the copied reports. For information about copying a report, see Section 5.3, "Creating a Custom Report Definition Based on an Existing Definition," on page 31.</p> <p>For a data source to be available for reports, you must first add it on the Data Sources page. For more information, see Section 9.2, "Managing Data Sources," on page 50.</p>
Language	Defines the target language for the report.
Date Range	<p>Allows you to define a range of dates for the data included in the report. The following choices are available:</p> <ul style="list-style-type: none"> ◆ 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 if you selected Custom Data Range for the Data Range parameter.
To Date	Allows you to specify a fixed end date for the report data. This parameter is only enabled if you selected Custom Data Range for the Data Range parameter.
Limit Results	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**, 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 monthly, do 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). To report on a fixed date range, 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: 

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.
- 4 To add a new schedule for the report definition, click the **Add** button on the far right side of the **Schedule** section.
 - 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 Reporting Module as a whole.
 - 4b (Conditional) 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.
 - 4d Select the date in the calendar on which you want to initiate the first run of the report.
 - 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**.

5.3 Creating a Custom Report Definition Based on an Existing Definition

To create a new report definition by making a copy of an existing report definition, mouse over the report definition (or select the check box next to the name) and click **Copy**.

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.

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, change the name to something more meaningful.

5.4 Running a Report On Demand

To queue a report to run immediately from the Repository list view, mouse over the report definition (or select the check box next to the name) and click **Run Now**.

Startup process requires extra time before reports can be generated When you first start the 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 might encounter memory errors.

5.5 Deleting a Report Definition

To delete a report definition, mouse over the report definition (or select the check box next to the name) and click **Delete**.

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**.

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. 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

To sort the list of reports, click the header for the column on which you want to sort.

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.

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

To refresh the report definition list, 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 35](#)
- ◆ [Section 6.2, “Automatically Importing Report Definitions,” on page 36](#)
- ◆ [Section 6.3, “Using the Download Page to Download Report Definitions,” on page 36](#)

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 **Browse** to the right of **Add**.
 - 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.

- 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.

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 clearing the **Overwrite existing reports**.

When you select this option, 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

The imported values overwrite all other settings associated with the report definition.

- 5 Click **Import** to begin 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.

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 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 in 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 automatic import facility performs the following steps:

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.

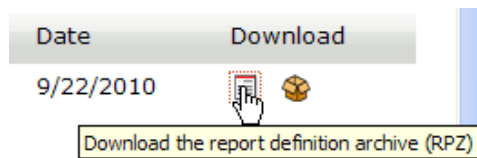
6.3 Using the Download Page to Download Report Definitions

The Reporting Module provides the ability to download a set of predefined report definitions from the NetIQ.com site.

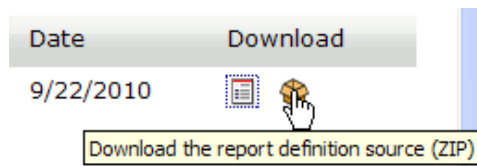
To download a predefined report:

- 1 Click **Download** in the left navigation menu.
- 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:



3 Save the file.

After you download a report definition archive, you can import the report definition into the Repository by using the Import page. For details, see [Section 6.1, "Using the Import Page to Import Report Definitions,"](#) on page 35.

For details on the predefined reports, see [Using Identity Manager Reports \(http://www.netiq.com/documentation/idm45/idm_reports/data/bookinfo.html\)](http://www.netiq.com/documentation/idm45/idm_reports/data/bookinfo.html).

7 Using the Calendar Page

This section provides instructions on using the Calendar page.

- ◆ [Section 7.1, “Viewing the Calendar,” on page 39](#)
- ◆ [Section 7.2, “Checking the Status of a Schedule Instance,” on page 40](#)
- ◆ [Section 7.3, “Viewing the Summary Information for a Schedule Instance,” on page 40](#)
- ◆ [Section 7.4, “Viewing a Completed Report,” on page 40](#)
- ◆ [Section 7.5, “Editing a Schedule Instance,” on page 41](#)
- ◆ [Section 7.6, “Deleting a Schedule Instance,” on page 42](#)
- ◆ [Section 7.7, “Moving a Single Schedule Instance,” on page 42](#)
- ◆ [Section 7.8, “Moving All Schedule Instances,” on page 42](#)
- ◆ [Section 7.9, “Defining the Calendar Display Options,” on page 43](#)
- ◆ [Section 7.10, “Refreshing the Display,” on page 43](#)

7.1 Viewing the Calendar

This section provides instructions for viewing the calendar.

- ◆ [Section 7.1.1, “Displaying the Calendar Page,” on page 39](#)
- ◆ [Section 7.1.2, “Scrolling within the Calendar Display,” on page 40](#)
- ◆ [Section 7.1.3, “Viewing the Schedule for Today,” on page 40](#)

7.1.1 Displaying the Calendar Page

To display the calendar, click **Calendar** in the left navigation menu.

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, press the down-arrow key.

To remove a row (go back one week) in the calendar view, press the up-arrow key.

To scroll down to the next set of weeks in the calendar view, press Ctrl+down-arrow.

You can also scroll down by clicking the **Go forward** icon.

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, press Ctrl+up-arrow or click the **Go back** icon.

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. If so, 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, mouse over the schedule name.

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

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

If the schedule instance has not run yet because it is scheduled for some time 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.

7.3 Viewing the Summary Information for a Schedule Instance

To view the summary information for a particular schedule instance in the calendar, click the name of the schedule instance.

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, click **View** under the schedule name.

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.

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.
- 3 Make changes as necessary to the scheduled run.

Schedule Property	Description
Start date	<p>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.</p> <p>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.</p>
Time of day	<p>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.</p> <p>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).</p> <p>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.</p>
Frequency	<p>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)).</p> <p>You cannot modify the frequency for a schedule after the schedule has been created.</p>
End date	<p>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.</p> <p>You can change the end date for a schedule after it has been created.</p>
Use default notifications	<p>Specifies the e-mail settings associated with the schedule instance.</p>

- 4 Click **Save**.

7.6 Deleting a Schedule Instance

To delete a particular scheduled instance, mouse over the scheduled instance and click **Delete**.

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.

- 2 Click **Move This**.

- 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.

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.

- 2 Click **Move All**.

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

7.9 Defining the Calendar Display Options

To control how many weeks are shown on the Calendar page:

- 1 Click **Display Options** in the upper right corner of the page.
- 2 Select the number of weeks to display in the **Number of weeks for the calendar to show** field.
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

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.

- ◆ [Section 8.1, “Viewing the List of Completed and Running Reports,” on page 45](#)
- ◆ [Section 8.2, “Viewing a Completed Report,” on page 45](#)
- ◆ [Section 8.3, “Viewing the Details for a Report,” on page 46](#)
- ◆ [Section 8.4, “Deleting a Report,” on page 46](#)
- ◆ [Section 8.5, “Performing Bulk Actions,” on page 46](#)
- ◆ [Section 8.6, “Searching for a Report,” on page 47](#)
- ◆ [Section 8.7, “Sorting the List of Reports,” on page 48](#)
- ◆ [Section 8.8, “Defining the Reports Display Options,” on page 48](#)
- ◆ [Section 8.9, “Refreshing the Completed Report List,” on page 48](#)

8.1 Viewing the List of Completed and Running Reports

To view a list of completed and running reports, click **Reports** in the left navigation menu.

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, data source on which you ran the report, description, run date, and 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

To view a completed report, click the **View** link below the report you want to display.

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.

8.3 Viewing the Details for a Report

- 1 Click the **Details** link below the report for which you want to see the details.

The details are displayed in a pop-up window.

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, click the **Delete** link below the report you want to delete.

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 <code>cblack</code> creates a schedule, and then <code>mmackenzie</code> logs in and modifies the schedule, the Run By user is still the original creator, <code>cblack</code> . If <code>mmackenzie</code> moves the item by clicking Move This , thereby creating a new schedule, <code>mmackenzie</code> 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, 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

To 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.
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

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 49](#)
- ♦ [Section 9.2, “Managing Data Sources,” on page 50](#)
- ♦ [Section 9.3, “Defining the Identity Vault Settings for Managed Systems,” on page 51](#)
- ♦ [Section 9.4, “Defining the Settings for Non-Managed Applications,” on page 52](#)
- ♦ [Section 9.5, “Defining the Auditing Configuration,” on page 54](#)
- ♦ [Section 9.6, “Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver,” on page 56](#)

9.1 Defining the General Settings

The General Settings page allows you to define global settings that control the behavior of the Reporting Module.

- 1 Click **Settings** in the left navigation menu.
The Reporting Module displays the General Settings page.
- 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 \(http://www.postgresql.org/docs/\)](http://www.postgresql.org/docs/).

9.2 Managing Data Sources

The Data Sources page allows you to add, modify, and remove PostgreSQL and Oracle data sources on which you want to run reports. You can select data sources from a pre-defined list of installed Java Naming and Directory Interface (JNDI) data sources that the reporting server manages or define new, external Java Database Connectivity (JDBC) data sources. For a data source to be available when you run reports, you must first add it using this page.

After you add a pre-defined JNDI data source, you can use the Data Sources page to modify the display name. For JDBC data sources, you can modify the display name and the password that the Reporting Module uses to connect to the data source.

You cannot remove the pre-defined data source named `IDMRPTCfgDataSource`. This is the default data source that the Reporting Module uses to run reports against the internal database.

To add a data source:

- 1 Click **Data Sources** in the left navigation menu.
- 2 Click **Add**.
- 3 Select the appropriate method for connecting to the data source.
- 4 (Conditional) If you are adding a pre-defined data source, select the source from the list.
- 5 (Conditional) If you are defining a new data source, provide the following information for connecting to the data source:
 - ◆ Name of the data source
 - ◆ DNS name or IP address of the computer that hosts the data source
 - ◆ Whether to use SSL to connect to the data source
 - ◆ Port on which the data source listens
 - ◆ Database name
 - ◆ User name and password for the data source user account
- 6 (Optional) To test whether the Reporting Module can connect to the data source, click **Test Connection**.

A successful connection is not required to add the data source.
- 7 Click **Save**.

To modify a data source:

- 1 Click **Data Sources** in the left navigation menu.
- 2 Click the data source name, and then modify the information.

To remove a data source:

- 1 Click **Data Sources** in the left navigation menu.
- 2 Click **Remove** next to the data source you want to remove.

After you remove a data source, it is no longer available for running reports.

9.3 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.

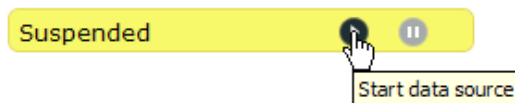
If you have more than one Identity Vault registration, you might need to scroll down to see the other Identity Vaults.

- 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.

Driver	Identity Vault Setting	Description
Managed System Gateway Driver	Collection state	<p>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.</p> <p>NOTE: If RBPM and the 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.</p> <p>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.</p>
	Username	The user name required to authenticate to the driver. (Read only)

- To save your changes, click **Save**.
- 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**.

- To stop a running data source, click **Stop data source**:



9.4 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).
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**.

- 5 To start the data source associated with the application, click the start icon to the right of **Application state**.
- 6 To stop a data source that is already running, click the stop icon.
- 7 To remove the application you just added, click **Remove** in the upper right corner of the **Application** section of the page.

9.5 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 NetIQ tools, such as RBPM, Catalog Administrator, Designer, and the 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 audit connector, specify the port number in the **Audit Connector port** field.
- 4 To test the connection to EAS, click **Test Connection**.
- 5 To forward events from Sentinel to EAS, follow the instructions presented under [Section 9.6, “Configuring Sentinel Link to Use Sentinel as the Sender and EAS as the Receiver,” on page 56](#).

IMPORTANT: You can forward events from EAS to Sentinel or Sentinel to EAS. However, NetIQ recommends that you forward events from Sentinel to EAS.

- 6 To forward events from EAS to Sentinel:
 - 6a Specify the network address for the Event Router in the **Address** field.
 - 6b Specify the port number for the Event Router in the **Port** field.
 - 6c 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 \(http://lucene.apache.org/java/docs/\)](http://lucene.apache.org/java/docs/).
 - 6d To start event forwarding, select **Enable event forwarding**.
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 \(http://www.netiq.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bnm03ok.html\)](http://www.netiq.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/bnm03ok.html).
 - 6e To test the event forwarding configuration, click **Test Ports**.
- 7 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.

EAS automatically captures the following log events from the Reporting Module:

Event ID	Process	NetIQ Identity Audit Event	Severity
31700	Authentication token created	Create_Auth-Token	Info
31701	Authentication token failed	Create_Auth-Token_Failure	Error
31702	Authentication token revoked	Auth-Token_Revoked	Info
31721	DCS driver registration added	DCS_Driver_Registration_Add	Info
31722	DCS driver registration modified	DCS_Driver_Registration_Modify	Info
31723	DCS driver collection enabled	DCS_Driver_Collection_Enabled	Info
31724	DCS driver collection disabled	DCS_Driver_Collection_Disabled	Info
31725	Data source registered	Data_Source_Registered	Info
31726	Data source modified	Data_Source_Modified	Info
31727	Data source removed	Data_Source_Removed	Info
31728	Data collection suspended	Data_Collection_Suspended	Info
31729	Data collection activated	Data_Collection_Activated	Info
31730	Data collection started	Data_Collection_Started	Info
31731	Data collection completed	Data_Collection_Completed	Info
31732	Data collection failed	Data_Collection_Failed	Error
31733	Data collection requested	Data_Collection_Requested	Info
	Data cleanup requested	Data_Cleanup_Requested	
31771	Report definition created	Report_Defn_Created	Info
31772	Report definition modified	Report_Defn_Modified	Info
31773	Report definition deleted	Report_Defn_Deleted	Info
31774	Schedule created	Schedule_Created	Info
31775	Schedule modified	Schedule_Modified	Info
31776	Schedule deleted	Schedule_Deleted	Info
31777	Report generated	Report_Generated	Info
31778	Report delivered	Report_Delivered	Info

9.6 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, NetIQ 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 9.6.1, “Configuring EAS to Receive Events,” on page 56](#)
- ♦ [Section 9.6.2, “Configuring Sentinel to Send Events,” on page 56](#)

9.6.1 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* (https://www.netiq.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html).

NOTE: You can skip the first section on accessing Event Source Manager, since the Reporting Module allows you to launch the tool directly.

9.6.2 Configuring Sentinel to Send Events

This section provides instructions for configuring a Sentinel server to send events to EAS. These instructions describe the approach NetIQ 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* (https://www.netiq.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html). 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 NetIQ 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):

- ♦ NetIQ Identity Manager
- ♦ NetIQ eDirectory and EDIRECTORY
- ♦ Identity Vault
- ♦ NetIQ Modular Authentication
- ♦ NetIQ 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 Creating Custom Report Definitions

This section provides instructions for creating custom report definitions.

- ♦ [Section 10.1, “About Custom Report Definitions,” on page 59](#)
- ♦ [Section 10.2, “Starting the Report Packaging Tool,” on page 59](#)
- ♦ [Section 10.3, “Creating a New Report Template,” on page 60](#)
- ♦ [Section 10.4, “Configuring Your JDBC Connection in iReport,” on page 60](#)
- ♦ [Section 10.5, “Setting the Description and Other Strings for Your Report,” on page 61](#)
- ♦ [Section 10.6, “Setting the Report Definition Parameters,” on page 61](#)
- ♦ [Section 10.7, “Customizing the Report in iReport,” on page 65](#)
- ♦ [Section 10.8, “Displaying Parameters and Selected Criteria in the Report,” on page 68](#)
- ♦ [Section 10.9, “Building Your Report,” on page 69](#)

10.1 About Custom Report Definitions

The 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, NetIQ provides the NetIQ Identity Manager Report Packaging Tool. You can customize reports in iReport and use the Reporting Packaging Tool to package them. The NetIQ Identity Manager Report Packaging Tool is installed on the same server where you install the 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:

community.jaspersoft.com (<http://community.jaspersoft.com/project/jaspersoft-studio>)

On Linux, you need to unpack the TAR file to your home directory. On Windows, you need to run an executable installer.

10.2 Starting the Report Packaging Tool

The NetIQ Identity Manager Report Packaging Tool is installed in the `root` folder or the Reporting Module installation folder, depending on your environment. By default, the `reportpkg.jar` file is located in the `/opt/netiq/idm/apps/IDMReporting` folder.

To start the NetIQ Identity Manager Report Packaging Tool on Linux, execute this command:

```
java -jar reportpkg.jar
```

On Windows, simply double-click the JAR file.

10.3 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.
- 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.

10.4 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.

NOTE: Specify the database username and password you use for your PostgreSQL database.

- 5d Click the **Test** button to test your database connection.
 - 5e Click **OK** to close the message box.
 - 5f Save the database connection information.
- 6 Close the JDBC configuration dialog box.

10.5 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.

10.6 Setting the Report Definition Parameters

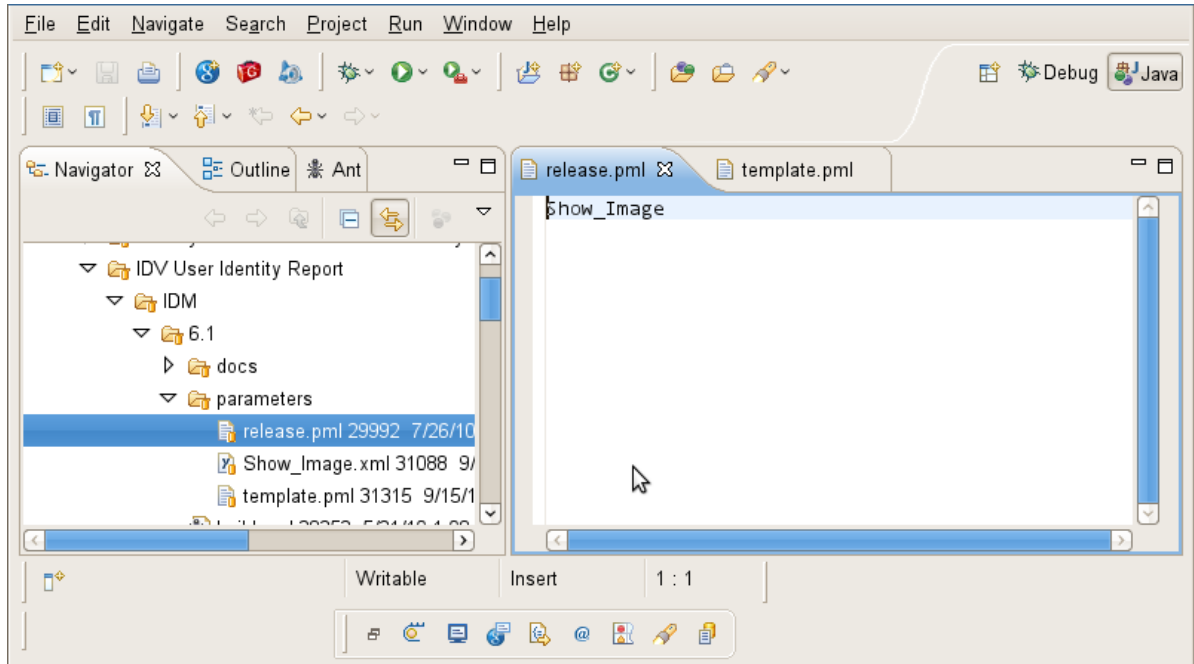
Reports support runtime parameters that allow users to specify values when they run a report. This section provides instructions for defining runtime parameters.

- [Section 10.6.1, “Defining the Parameter XML File,” on page 62](#)
- [Section 10.6.2, “Defining the Type for a Parameter,” on page 63](#)
- [Section 10.6.3, “Defining an OptionQuery Parameter,” on page 64](#)

10.6.1 Defining the Parameter XML File

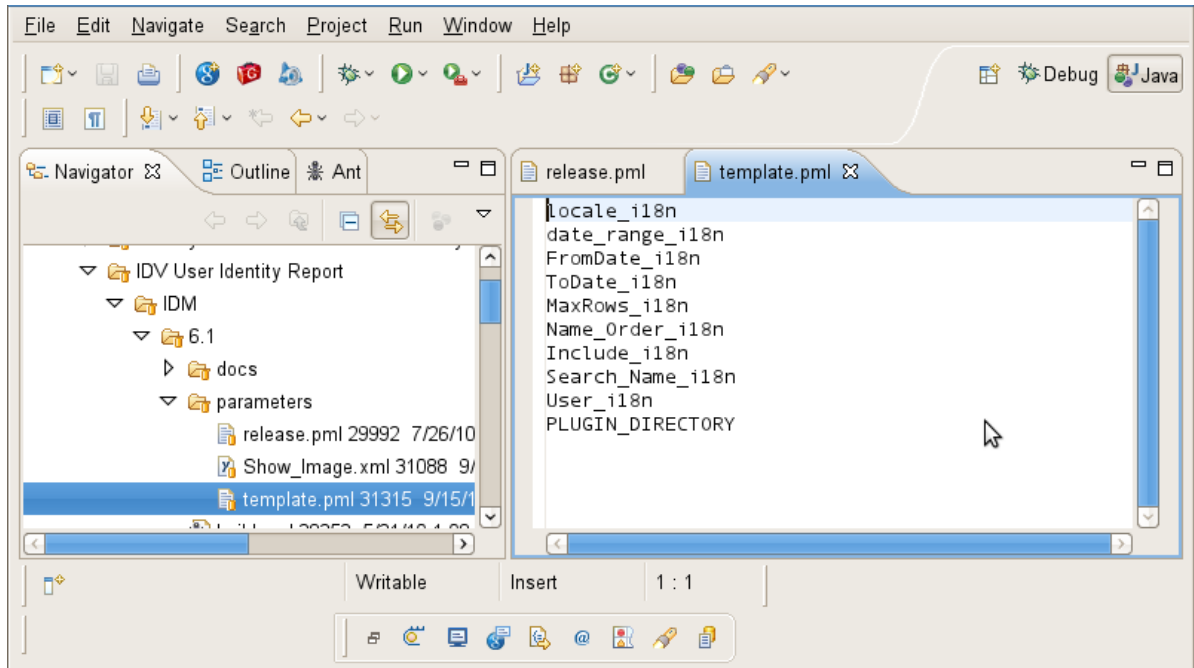
Parameters specific to your report are located in the `6.1/parameters` directory for your report. Each parameter is in its own XML file. Each of these XML files must be referenced in the `release.pml` file in the order in which you want them to appear. The `release.pml` file lists the parameters by name (without the file extension), as shown below:

Figure 10-1 Release.pml file



The `template.pml` file lists commonly shared parameters:

Figure 10-2 *Template.pml file*



10.6.2 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 10-1 *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>
```

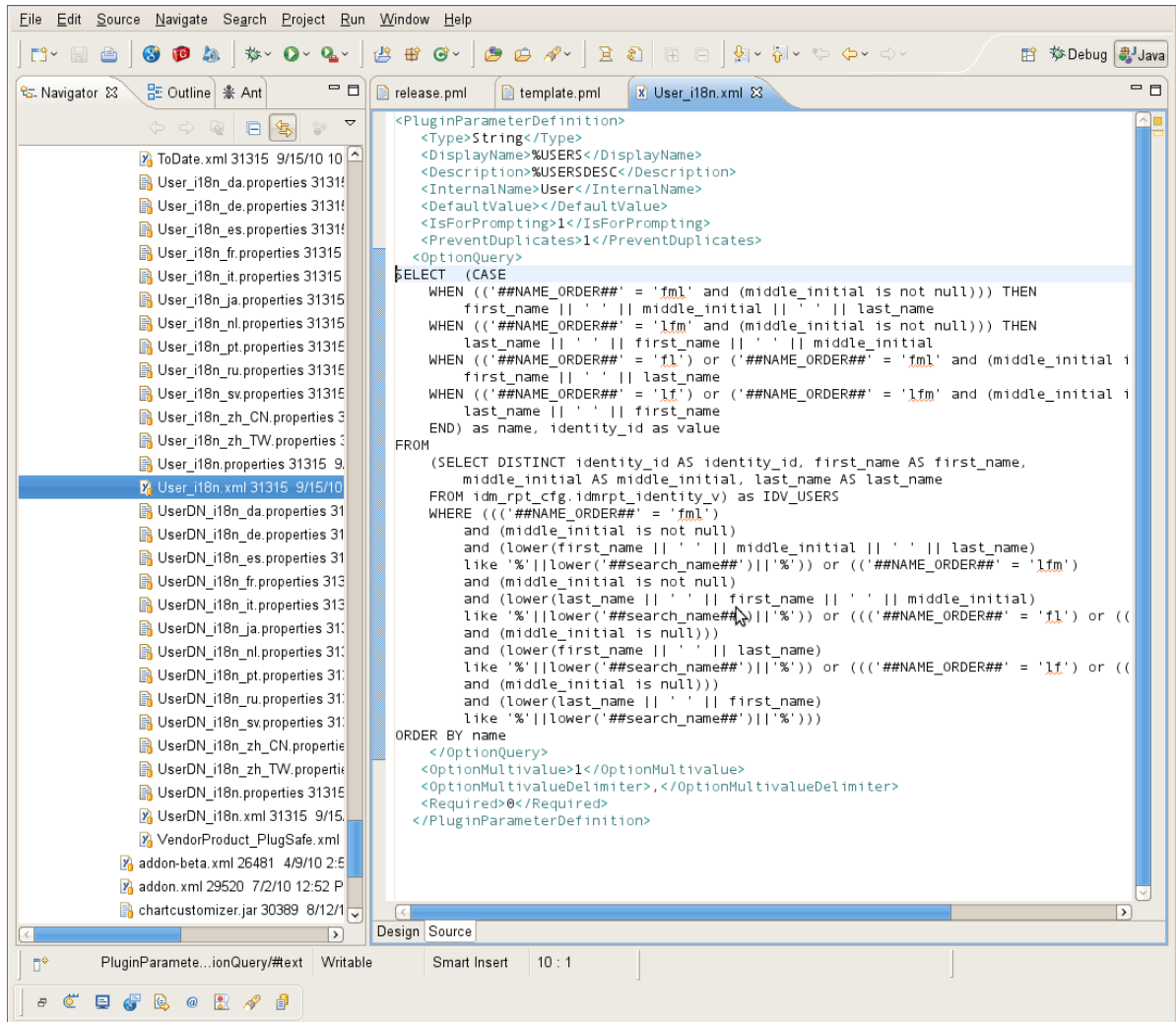
10.6.3 Defining an OptionQuery Parameter

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. NetIQ 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.

The User_i18n.xml file is shown below:

Figure 10-3 User_i18n.xml file



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>
```

10.7 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:

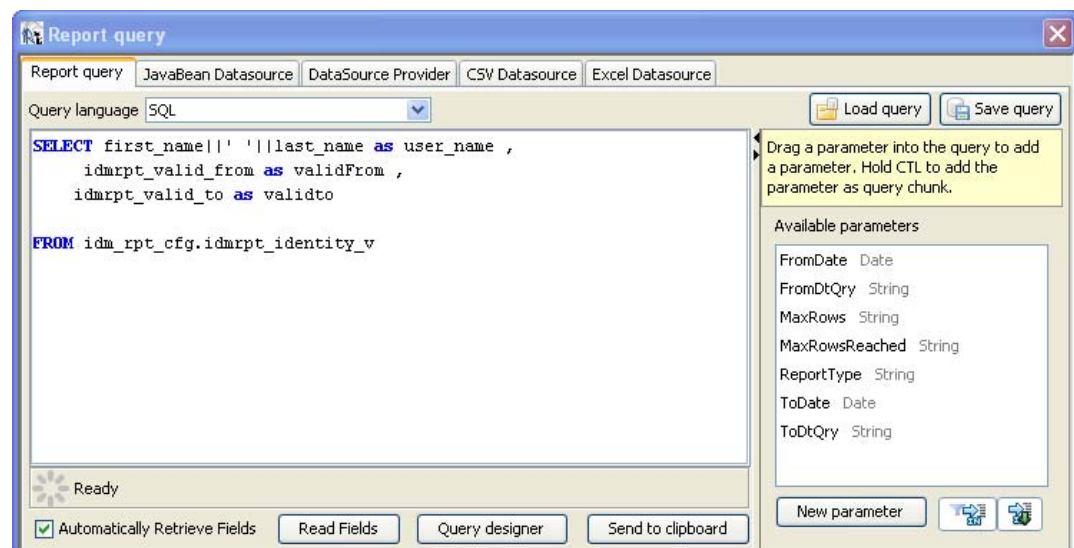
2a Define a SQL query to get the data for your report.

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 11, “Schema Documentation,” on page 71](#).

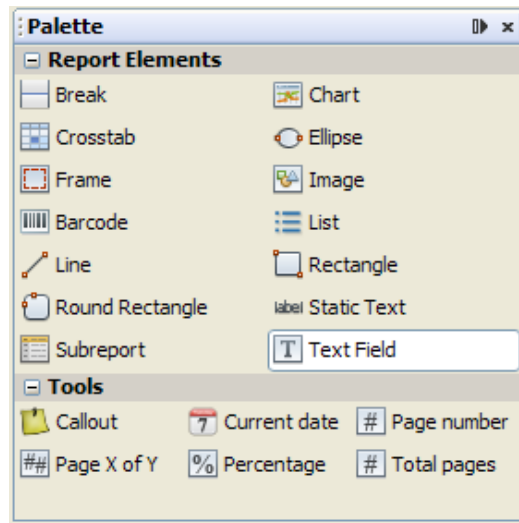
NOTE: You can only use views in custom reports. If you use your root username to log into the database, iReport will let you select data from the tables. However, the report will fail when you deploy it and try to run it.

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:



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**.

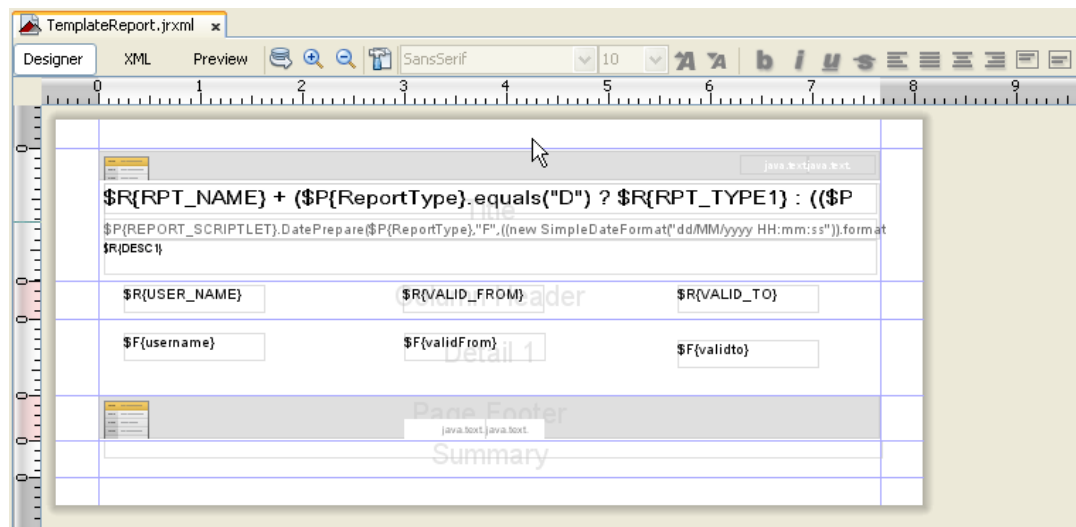


For example, to add a column header, drag the **Text Field** icon from the **Palette** onto the header band of the report layout canvas.

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.



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 10.9, "Building Your Report,"](#) on page 69.

10.8 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 “`#{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.

```
#{REPORT_SCRIPTLET}.DatePrepare("#{ReportType}", "F", ((new SimpleDateFormat("dd/MM/yyyy HH:mm:ss")).format("#{FromDate})), "D") + " " + #{HEADER6} + " " +
#{REPORT_SCRIPTLET}.DatePrepare("#{ReportType}", "T", ((new SimpleDateFormat("dd/MM/yyyy HH:mm:ss")).format("#{ToDate})), "D") + "\n" +
java.text.MessageFormat.format("#{MAXROWS_COLON}", new
Object[]{
#{MaxRows}.equals("ALL") ? #{ALL} :
#{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:

```
#{REPORT_SCRIPTLET}.DatePrepare("#{ReportType}", "F", ((new SimpleDateFormat("dd/MM/yyyy HH:mm:ss")).format("#{FromDate})), "D") + " " + #{HEADER6} + " " +
#{REPORT_SCRIPTLET}.DatePrepare("#{ReportType}", "T", ((new SimpleDateFormat("dd/MM/yyyy HH:mm:ss")).format("#{ToDate})), "D") + "\n" +
java.text.MessageFormat.format("#{MAXROWS_COLON}", new
Object[]{
#{MaxRows}.equals("ALL") ? #{ALL} :
#{MaxRows}
}) + "\n" +
java.text.MessageFormat.format("#{NAME_ORDER_COLON}", new
Object[]{
#{NAME_ORDER}.equals("lfm") ? #{NAME_ORDER_LFM} :
#{NAME_ORDER}.equals("fl") ? #{NAME_ORDER_FL} :
#{NAME_ORDER}.equals("lf") ? #{NAME_ORDER_LF} : #{NAME_ORDER_FML}
}) + "\n" +
java.text.MessageFormat.format("#{USERS_COLON}", new Object[]{
((#{User} != null && #{User}.size() > 0) ? #{search_name} : #{ALL})
}) +
"" + (#{Only_Show_SOD}.booleanValue() ? "\n" + #{SHOW_SOD} : "")
```

The Role Assignments by Member parameters displayed are:

- ◆ Data Range
- ◆ Max Rows
- ◆ Name Order
- ◆ Users
- ◆ Separation of Duties information only

10.9 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.

4 Select the type of report.

5 Select the template to use for the report header and footer.

6 (Optional) Select to build the report using data source constraints, and then click **Next**.

Data source constraints declare the tables, views, and databases that the report requires to run successfully and allow the Reporting Module to inform the user that a target data source does not have the required schema to run the report successfully. Data source constraints are not required.

You can also specify SQL test constraints that test whether a report and data source are compatible beyond simply checking for the required views and tables. For example, you can check that a required function or columns in a table exist.

7 (Conditional) Select the type of constraint to add, then specify the constraint name and schema name, if required.

The schema name is optional for tables and views, and required for databases.

For example, if a report requires the `idmrpt_role_v` view in the `idm_rpt_cfg` schema, select the **View** type, enter `idmrpt_role_v` for the name, and enter `idm_rpt_cfg` for the schema.

8 (Optional) Add SQL test constraints.

Provide a syntactically correct SQL statement and, optionally, the expected result. For example, to verify that the `identity_cleanup` function exists, enter the following SQL statement:

```
SELECT routine_name FROM Information_schema.Routines WHERE  
Specific_schema = 'public'  
AND routine_name = 'identity_cleanup'  
AND Routine_type = 'FUNCTION'
```

9 Click the **Build** button to build the RPZ file for your report definition.

After you have built your report, you must import the report in order to use the report. For more information, see [Chapter 6, “Using the Import Tool,” on page 35](#).

11 Schema Documentation

This section provides reference documentation for the database views for reporting.

- ♦ [Section 11.1, “About the Database Views,” on page 72](#)
- ♦ [Section 11.2, “idmrpt_acct_link_v,” on page 73](#)
- ♦ [Section 11.3, “idmrpt_approver_v,” on page 74](#)
- ♦ [Section 11.4, “idmrpt_association_v,” on page 74](#)
- ♦ [Section 11.5, “idmrpt_ext_idv_item_v,” on page 74](#)
- ♦ [Section 11.6, “idmrpt_cat_item_types_v,” on page 75](#)
- ♦ [Section 11.7, “idmrpt_cat_mappings_v,” on page 75](#)
- ♦ [Section 11.8, “idmrpt_category_v,” on page 75](#)
- ♦ [Section 11.9, “idmrpt_ms_collect_state_v,” on page 76](#)
- ♦ [Section 11.10, “idmrpt_container_v,” on page 76](#)
- ♦ [Section 11.11, “idmrpt_ext_attr_v,” on page 77](#)
- ♦ [Section 11.12, “idmrpt_ext_obj_v,” on page 77](#)
- ♦ [Section 11.13, “idmrpt_dc_service_cfg_v,” on page 77](#)
- ♦ [Section 11.14, “idmrpt_ent_param_token_value_v,” on page 78](#)
- ♦ [Section 11.15, “idmrpt_ent_type_v,” on page 78](#)
- ♦ [Section 11.16, “idmrpt_ext_item_attr_v,” on page 79](#)
- ♦ [Section 11.17, “idmrpt_group_v,” on page 79](#)
- ♦ [Section 11.18, “idmrpt_identity_v,” on page 79](#)
- ♦ [Section 11.19, “idmrpt_ms_identity_v,” on page 81](#)
- ♦ [Section 11.20, “idmrpt_idv_v,” on page 83](#)
- ♦ [Section 11.21, “idmrpt_idv_acct_v,” on page 83](#)
- ♦ [Section 11.22, “idmrpt_idv_drivers_v,” on page 84](#)
- ♦ [Section 11.23, “idmrpt_idv_ent_v,” on page 84](#)
- ♦ [Section 11.24, “idmrpt_idv_ent_bindings_v,” on page 85](#)
- ♦ [Section 11.25, “idmrpt_idv_identity_trust_v,” on page 85](#)
- ♦ [Section 11.26, “idmrpt_idv_prd_v,” on page 86](#)
- ♦ [Section 11.27, “idmrpt_idv_trust_types_v,” on page 87](#)
- ♦ [Section 11.28, “idmrpt_container_types_v,” on page 87](#)
- ♦ [Section 11.29, “idmrpt_ms_v,” on page 87](#)
- ♦ [Section 11.30, “idmrpt_ms_acct_v,” on page 88](#)
- ♦ [Section 11.31, “idmrpt_ms_acct_rule_v,” on page 89](#)
- ♦ [Section 11.32, “idmrpt_ms_collector_v,” on page 90](#)
- ♦ [Section 11.33, “idmrpt_ms_ent_v,” on page 91](#)
- ♦ [Section 11.34, “idmrpt_ms_ent_type_v,” on page 91](#)

- ◆ Section 11.35, “idmrpt_ms_ent_trust_v,” on page 92
- ◆ Section 11.36, “idmrpt_owners_v,” on page 93
- ◆ Section 11.37, “idmrpt_res_parameter_v,” on page 93
- ◆ Section 11.38, “idmrpt_resource_v,” on page 93
- ◆ Section 11.39, “idmrpt_role_v,” on page 94
- ◆ Section 11.40, “idmrpt_role_level_v,” on page 95
- ◆ Section 11.41, “idmrpt_role_mappings_v,” on page 95
- ◆ Section 11.42, “idmrpt_role_res_assoc_v,” on page 95
- ◆ Section 11.43, “idmrpt_role_res_assoc_param_v,” on page 96
- ◆ Section 11.44, “idmrpt_rpt_driver_v,” on page 96
- ◆ Section 11.45, “idmrpt_rpt_driver_scope_v,” on page 97
- ◆ Section 11.46, “idmrpt_sod_v,” on page 97
- ◆ Section 11.47, “idmrpt_sod_violations_v,” on page 97
- ◆ Section 11.48, “idmrpt_approval_v,” on page 98
- ◆ Section 11.49, “idmrpt_team_v,” on page 98
- ◆ Section 11.50, “idmrpt_team_assignments_v,” on page 99

11.1 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

11.2 idmrpt_acct_link_v

Contains 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	

11.3 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. For 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

11.4 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

11.5 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

11.6 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

11.7 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

11.8 idmrpt_category_v

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

11.9 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)	

11.10 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
------------------	------	---------------------------

11.11 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

11.12 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)	

11.13 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_unit s	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_timeou t	int8	
next_data_collect_date	int8	
data_collect_srv_id	VARCHAR(32)	

11.14 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	

11.15 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

11.16 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

11.17 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

11.18 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 messenger id
mgr_id	VARCHAR(32)	The UUID for this user's manager
photo	TEXT(2147483647)	This users photo
idm rpt_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	

11.19 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 messenger 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

11.20 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 reporting 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

11.21 idmrpt_idv_acct_v

Contains information about the accounts in all of the Identity Vaults the reporting 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.

11.22 idmrpt_idv_drivers_v

Contains information about the driver configured in the Identity Vault connected to the 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

11.23 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

11.24 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)	

11.25 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	

11.26 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

11.27 idmrpt_idv_trust_types_v

Stores the Identity Vault trust types. This view is a fixed list of types and is populated 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.

11.28 idmrpt_container_types_v

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	

11.29 idmrpt_ms_v

Contains information about managed systems the reporting information is collecting data from.

ms_id	VARCHAR(32)	The unique 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	

11.30 idmrpt_ms_acct_v

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 system application
idv_association	VARCHAR(256)	the IDV account Association
idv_acct_id	VARCHAR(32)	the IDV account 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	

11.31 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

11.32 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, https
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	timestampz	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

11.33 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 parameter value string
idv_ent_pt_id2	VARCHAR(4000)	The corresponding Identity Vault entitlement parameter ID token value
idv_ent_pt_liid	VARCHAR(4000)	The corresponding Identity Vault entitlement parameter 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	

11.34 idmrpt_ms_ent_type_v

idv_ent_dn	VARCHAR(256)	Identifier of entitlement type within idv (entitlement dn for connected system queried through REST API)
idv_ent_id	VARCHAR(32)	Nullable foreign 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	

11.35 idmrpt_ms_ent_trust_v

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	

11.36 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

11.37 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

11.38 idmrpt_resource_v

Stores Identity Vault resource catalog information.

res_id	VARCHAR(32)	The unique ID of this resource in the reporting 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

11.39 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

11.40 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

11.41 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 id based on catalog item type. if item type points to role, than it is a child role.
idmrpt_syn_state	int2	

11.42 idmrpt_role_res_assoc_v

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

11.43 idmrpt_role_res_assoc_param_v

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

11.44 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

11.45 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

11.46 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

11.47 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

11.48 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	

11.49 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

11.50 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	

12 REST Services for Reporting

The Identity Reporting Module incorporates several REST APIs that enable different features within the reporting functionality. The Reporting Module provides support for the following REST APIs:

- ♦ Non-Managed Application REST API
- ♦ Managed Application REST API
- ♦ Authentication REST API
- ♦ Reporting REST API

The REST APIs for reporting use the OAuth2 protocol for authentication.

The installation program deploys a special API WAR file, `rptdoc.war`, which contains the documentation of REST services needed for reporting. On Tomcat and JBoss, the `rptdoc.war` is automatically deployed when Reporting Module is installed. On WebSphere, the war is installed in the `%Reporting-install-folder%`. For example: `/opt/netiq/idm/apps/IdentityReporting`. You need to manually deploy it like other Reporting WARs.

To access the REST API documentation on the server where Reporting Module is installed, specify the path of `/rptdoc` in the address bar of your browser. For example, if you installed Reporting on a host called `servername` on port 8180, you can access the REST API documentation at `http://servername:8180/rptdoc`. If you installed Reporting using `https`, substitute `https` for `http`.

Be aware that while working in a staging or production environment, you must manually delete the `rptdoc.war` files and folders from your environment on Tomcat and JBoss. Do not deploy these files on WebSphere.

13 Troubleshooting the Drivers

This section describes many of the most common issues that arise in driver configuration and provides tips for resolving these issues.

- ♦ [Section 13.1, “Issue: No Identity Vaults Presented on the Identity Vaults Screen,” on page 103](#)
- ♦ [Section 13.2, “Issue: Reports Are Missing Identity Vault Data,” on page 104](#)
- ♦ [Section 13.3, “Issue: Object Already Exists Error,” on page 105](#)
- ♦ [Section 13.4, “Issue: MSGW Driver is Missing from Identity Vaults Screen,” on page 106](#)
- ♦ [Section 13.5, “Issue: Managed System Data is Missing from Reports,” on page 106](#)
- ♦ [Section 13.6, “Issue: Status of Data Collection is Suspended,” on page 108](#)
- ♦ [Section 13.7, “Issue: Status 400 Returned for Status Query,” on page 109](#)
- ♦ [Section 13.8, “Issue: Driver Errors Occur in Multi-Driver Set Environment,” on page 109](#)
- ♦ [Section 13.9, “REST Endpoint Troubleshooting,” on page 109](#)

13.1 Issue: No Identity Vaults Presented on the Identity Vaults Screen

If you look at the Identity Vaults screen in the Reporting Module, you may notice that no Identity Vaults are listed. You will also see an error message at the top of the screen.

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 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.
 - ♦ 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. NetIQ recommends that you synchronize the driver prior to modifying and redeploying it.

- ◆ 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"/>
```

13.2 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 idmptcore_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.)

13.3 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.

13.4 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 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.
 - ◆ Verify that the reporting connection information is correct in the Data Collection Service driver configuration. Check the connection URL, account, and password.

13.5 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.

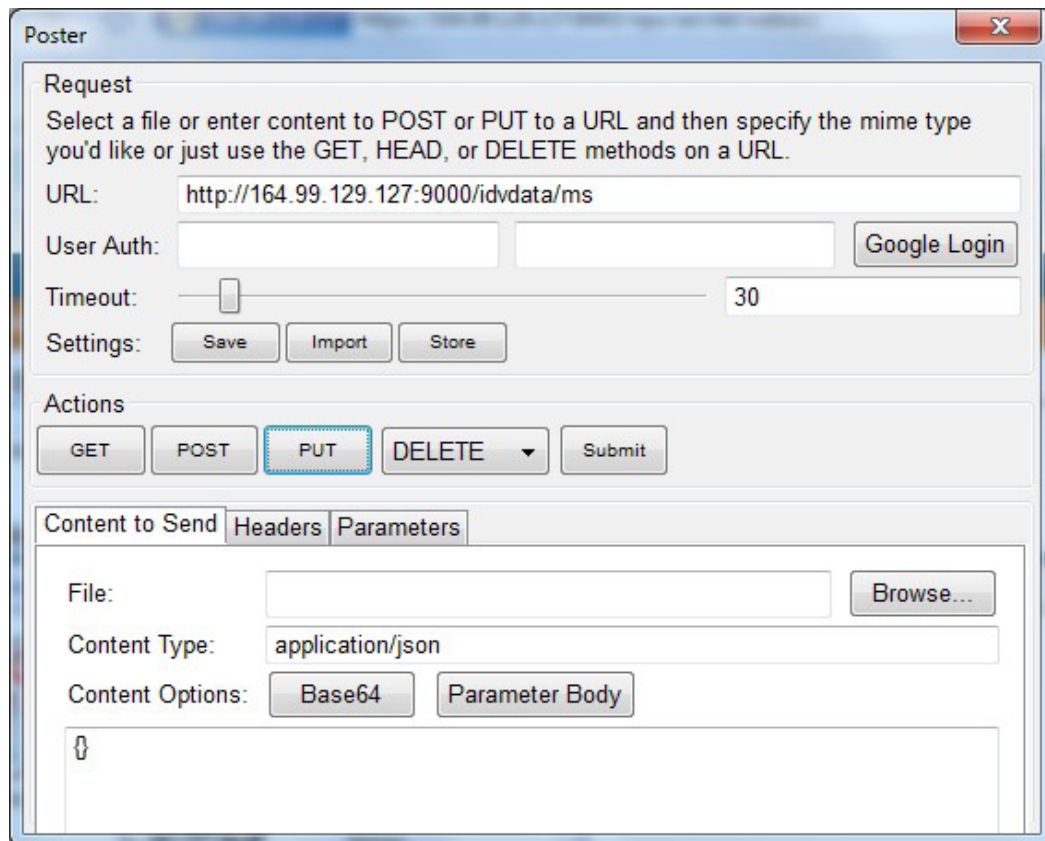
Here are some troubleshooting tips:

- ◆ 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).
- ◆ 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.
 - ◆ 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.



- ◆ 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.
 - ◆ If the collection status is Suspended, see [Section 13.6, "Issue: Status of Data Collection is Suspended,"](#) on page 108 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.

13.6 Issue: Status of Data Collection is Suspended

You may see that the data collection status is Suspended on the Identity Vaults screen.

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" additivity="true"/>
<logger name="com.novell.idm.rpt.core.server.dc" level="TRACE"
additivity="true"/>
```

13.7 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.

13.8 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.

13.9 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
```

14 String Customization

This section outlines the procedure for customizing strings in the Identity Reporting Module.

- ♦ [Section 14.1, “About String Customization in the Identity Reporting Module,” on page 111](#)
- ♦ [Section 14.2, “Customizing the Strings for the Reporting Module,” on page 112](#)

14.1 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 14-1 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
- ♦ Core WAR

The language-specific JAR files follow this pattern:

```
IDMRPT-CORE_ language . jar  
IDMRPT_ language . jar
```

For example, the following JAR files apply to strings in French:

```
IDMRPT-CORE_fr.jar  
IDMRPT_fr.jar
```

14.2 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	<p>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.</p> <p>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 <code>com.novell.idm.rpt.core.server.spi.exception.DCException</code>.</p> <p>NOTE: This value will also be used by the Identity Manager Reporting Service as the <identifier> for all query operations to the application service.</p>
Name	<p>String - Common Name for the non-managed application</p>
Description	<p>String - Description for the application</p>
Type	<p>String - Type of application (ie. Enterprise, Email, DB, etc)</p>
Classification	<p>String - Sensitivity classification (ie. Critical, Departmental, etc.)</p>
Vendor	<p>String - Application vendor</p>
Version	<p>String - Application version</p>
BusinessOwner	<p>String - Business Owner of the application. If the owner has an account in the application, the account ID should be used in this field</p>

Field	Description
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
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 the account in the connected system. NOTE: This field exists for use by NetIQ 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 NetIQ 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 NetIQ Identity Manager. A non-managed system should return false
ACCT_STATUS	Enum – Status of the account in the application: <ul style="list-style-type: none">◆ "A" – Active◆ "I" – Inactive◆ "U" – Undefined

Field	Description
MS_ACCT_GLOBAL_IDENTIFIER	<p>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.</p> <p>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.</p>
IDV_ASSOCIATION	<p>String – Identity Vault Association value for the account in the connected system.</p> <p>NOTE: This field exists for use by NetIQ Identity Manager. It should be omitted from Results from non-managed application systems.</p>
IDV_ACCT_STATUS	<p>Enum – Status of the account in the application:</p> <ul style="list-style-type: none"> ♦ "A" – Active ♦ "I" – Inactive ♦ "U" – Undefined <p>NOTE: This field exists for use by NetIQ Identity Manager. It should be omitted from Results from non-managed application systems.</p>
IDV_ACCT_DN	<p>String – Identity Vault distinguished name for the associated account.</p> <p>NOTE: This field exists for use by NetIQ Identity Manager. It should be omitted from Results from non-managed application systems.</p>

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

