NetIQ® Identity Manager

Using Identity Manager Reports

December 2014

Legal Notice

Contents

About this Book and the Library

The *Reporting Guide* provides general information for downloading and using reports as well as specific configuration information for reports as needed.

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 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

Provides 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. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions 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

Qmunity, 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, Qmunity 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 Common Report Information and Actions

This chapter provides details about working with Identity Manager reports, and list common report parameters and event auditing data.

1.1 Prerequisites

To work with Identity Manager report, you must have Identity Reporting installed and configured. For more information, see the *NetIQ Identity Manager Setup Guide* (http://www.netiq.com/documentation/idm45/setup_guide/data/front.html).

1.2 Downloading the Report

Identity Manager reports are included on the Identity Manager media; however, these reports are updated on a regular basis. Verify that you have the latest report version before proceeding.

1. Log into Identity Reporting as a user who is a Report Administrator.

   For more information, see "Administrator Assignments" in the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm45/agpro/data/bookinfo.html).
2. Click *Download* in the left navigation menu.
3. Find the report you want to run, then download the report.
4. Proceed to Section 1.3, "Importing the Report," on page 11.

1.3 Importing the Report

You must import each report into the Identity Reporting Module before you can run the report. After you import the report it is available for use throughout the reporting module.

The reports are imported when you install Identity Manager. If you have downloaded an updated report since the initial installation, continue with the following procedure. Otherwise, skip to Section 1.4, "Running the Report," on page 12.

To import the report:

1. Log into the Identity Reporting Module as a user who is a Report Administrator.
2. Click *Import* in the left navigation menu.
3. Click *Browse*, then browse to and select the report definition.
4. Click *Open*.

5 (Conditional) If the report exists in the repository, select *Overwrite existing reports*.

6 Click *Import*.

For more information about importing reports, see "Using the Import Tool" in the *Identity Reporting Module Guide* (http://www.netiq.com/documentation/idm45/reporting/data/bookinfo.html). For more information about running a report after it is in the repository, see Section 1.4, "Running the Report," on page 12.

1.4 Running the Report

You can either schedule a report to run at a specified time and frequency or you can run a report in real time. The following procedure explains how to run a report in real time. For information about scheduling reports, see "Using the Calendar Page" in the *Identity Reporting Module Guide* (http://www.netiq.com/documentation/idm45/reporting/data/bookinfo.html).

To run the Access Requests by Recipient report:

1 Log in to the Identity Reporting Module as a user who is a Report Administrator.

For more information, see "Administrator Assignments" in the *User Application: Administration Guide* (http://www.netiq.com/documentation/idm45/agpro/data/bookinfo.html).

2 Click *Repository* in the left navigation menu.

The reports are listed by name in ascending or descending order.

3 Select the report you want to run, then click *Edit*.

4 Specify the parameters to run the report.

5 (Optional) Click *Save* to save the parameters for the report's future scheduled runs.

6 Click *Run Now* to generate the report. If there is another report running, this report runs as soon as the first report finishes.

1.5 Common Report Parameters

The following section lists parameters common to most Identity Manager reports. Report parameters that are specific to a report are described in the corresponding report section.

Report name: The name of the report.

Report description: A description of the report.

Tags: A free-form field for any information to help you find this report. Specify multiple tags by delimiting them with commas.

Release date: The date the report was released.

Comments: Specify any comments about the report.

Output format: Select the type of format for the output. You can select *PDF* or *CSV*.

Criteria > Language: Select the language for the report.

Criteria > Date Range: Select a data range from the following options:

- Current Day
- Previous Day
- Week to Date

- Previous Week
- Month to Date
- Previous Month
- Custom Date Range

If you select *Custom Date Range*, you must specify a *From Date* and a *To Date*.

Criteria > Limit results to: Specify the number of results displayed in the report.

Criteria > Name order: Select the order the names are displayed in the report. The options are:

- Given-Name Initial Surname
- Surname Given-Name Initial
- Given-Name Surname
- Surname Given-Name

Criteria > Recipient(s): Specify the recipients for which you want to see access requests in the report.

Default Notifications > To: Specify one or more e-mail addresses of people that you want to receive an e-mail notification that the report ran. The report is attached to the notification e-mail.

Default Notification > cc: Specify one or more e-mail addresses of people that you want to receive a copy of the notification that the report ran. The report is attached to the notification e-mail.

Default Notifications > Subject: Specify a subject line for the notification that the report ran.

Default Notification > Message: Specify a message for the notification that the report ran.

Scheduled Run >Scheduled name: Specify a name for the scheduled run of the report.

Scheduled Run > Prepend report definition name: Select whether to prepend the report definition name to the report.

Scheduled Run > Start date: Specify the date when the scheduled run starts.

Scheduled Run > Time of day: Specify the time of day when the scheduled run starts.

Scheduled Run > Frequency: Specify how often the report runs during the scheduled dates.

Scheduled Run > End date: Specify the date when the scheduled run ends.

Scheduled Run > Attempt data collection before scheduled run: Select whether to attempt to collect the data before the report is scheduled to run.

Scheduled Run > Use default notifications: Select whether to use the default notification information. If you choose to not use the default notification information, you see additional fields for this run of the report:

- **To:** Specify one or more e-mail addresses of people that you want to receive the notification that this instance of the report ran. The report is attached to the notification e-mail.
- **cc:** Specify one or more e-mail addresses of people that you want to receive a copy of the notification that this instance of the report ran. The report is attached to the notification e-mail.
- **Subject:** Specify the subject line for the notification that this instance of the report ran.
- **Message:** Specify a message for the notification that this instance of the report ran.

1.6 Event Auditing Data in Identity Manager Reports

The following section identifies reports that include information gathered from Event Auditing Service (EAS). Audit event information from EAS is maintained in the Identity Manager database for 90 days before it is purged.

- Access Requests by Recipient
- Access Requests by Requester
- Access Requests by Resource
- Authentication by Server
- Authentication by User
- Database Statistics
- Object Provisioning
- Password Resets
- Self Password Changes
- User Password Change Event Summary

2 Access Requests by Recipient

This report displays resource assignment workflow process grouped by recipients.

2.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Recipient(s): The list of resources selected for this report.

Data Source: A connection from a database the user is accessing.

2.2 Report Content

This section displays the entries of requests to access the database based on user, status, and time.

Recipient: The name of the recipient for whom a request was made. The Recipient information includes details such as User Name, Job Title, Department, Email, and Office Phone.

Resource: The requested resource.

Requester: The name of the user who has requested the information.

Approver(s): The list of individuals who have been designated as approvers for the request.

Status: The status of the request.

Timestamp: The timestamp for each action taken by an approver.

Comments: Any comments made by the approver.

3 Access Requests by Requester

This report displays resource assignment workflow process grouped by requesters.

3.1 Report Criteria

Identity Manager displays the criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Requester(s): The list of resources selected for this report.

Data Source: A connection from a database the user is accessing.

3.2 Report Content

The report lists all workflow requests for selected requesters. It shows details for each requester and provides details about each workflow request made for a requester.

Requester: The name of the recipient for whom a request was made. The Recipient information includes details such as User Name, Job Title, Department, Email, and Office Phone.

Resource: The name of the resource requested.

Recipient: The name of the user who has requested access.

Approver(s): The list of individuals who have been designated as approvers for the request.

Status: The status of the request.

Timestamp: The timestamp for each action taken by an approver.

Comments: Any comments made by the approver.

4 Access Requests by Resource

This report displays resource assignment workflow process grouped by resources.

4.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Resource(s): The list of resources selected for this report.

Data Source: A connection from a database the user is accessing.

4.2 Report Content

This section displays the entries of activities performed for each database.

Requester: The name of the database domain.

Recipient: The name of the user who has requested access.

Approver(s): The list of individuals who have been designated as approvers for the request.

Status: The status of the request.

Timestamp: The timestamp for each action taken by an approver.

Comments: Any feedback or additional details regarding the request.

5 Account IDs in the Managed Systems

This report shows all account IDs in the managed system, and how they are associated with the users in the Identity Vault.

5.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Account type: The type accounts selected in the *Account type* parameter.

Managed systems: The systems specified in the *Managed systems* parameter.

Data Source: A connection from a database the user is accessing.

5.2 Report Content

This section displays the details for each Managed or Unmanaged account including the account ID, type, status, and user for a given date range.

5.2.1 Managed Accounts

Account ID: The account ID for the user in the managed system.

Account Type: The account type for the account ID value in the managed system.

Account Status: The status of the account in the managed system.

Associated Identity Vault Account: The DN of the user account in the Identity Vault.

Identity Vault Account Status: The status of the user account in the Identity Vault.

User: The name of the user.

Managed System: The name of the driver from where the information is retrieved.

5.2.2 Unmanaged Accounts

Account ID: The account ID for the user in the managed system.

Account Type: The account type for the account ID value in the managed system.

Account Status: The status of the account in the managed system.

Managed System: The name of the driver from where the information is retrieved.

6 Accounts IDs in the Managed Systems Current State

This report displays the current state of the account IDs in the managed systems, and how they are associated with the users in the Identity Vault.

6.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Account type: The type accounts selected in the *Account type* parameter.

Managed systems: The systems specified in the *Managed systems* parameter.

Data Source: A connection from a database the user is accessing.

6.2 Report Content

This section displays the details for each Managed or Unmanaged account including the account ID, type, status, and user for the most current date and time range.

6.2.1 Managed Accounts

Account ID: The account ID for the user in the managed system.

Account Type: The account type for the account ID value in the managed system.

Account Status: The status of the account in the managed system.

Associated Identity Vault Account: The DN of the user account in the Identity Vault.

Identity Vault Account Status: The status of the user account in the Identity Vault.

User: The name of the user.

Managed System: The name of the driver from where the information is retrieved.

6.2.2 Unmanaged Accounts

Account ID: The account ID for the user in the managed system.

Account Type: The account type for the account ID value in the managed system.

Account Status: The status of the account in the managed system.

Managed System: The name of the driver from where the information is retrieved.

7 Authentication by Server

This report displays all authentication attempts captured by Identity Manager within the selected date range, grouped by the target asset (hostname - IP) against which the attempt was made.

7.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

7.2 Report Content

This report lists all authentication attempts captured within the specified date rage. The events are grouped by the domain within which the user account exists and then grouped by the target asset.

Target asset: The hostname IP.

Event name: The event that occurred.

Initiator: The user name that initiated the event.

Details: The domain name and extended information.

8 Authentication by User

This report shows all authentication attempts by users captured by Identity Manager within the selected date range, grouped by the domain within which the user account exists, and then grouped by the account name.

8.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

8.2 Report Content

This report lists all authentication attempts by the users captured within the specified date rage. The events are grouped by the domain within which the user account exists and then grouped by the account name.

Domain: The domain within which the user account exists.

Event name: The event that occurred.

Initiator: The user name that initiated the event.

Target Host name - Target IP: The IP address and extended information.

9 Available Permissions

This report displays detailed information about all roles, resources, and provisioning request Definitions that an end user can request in the organization. The items are grouped by the Identity Vault in which they reside.

9.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Records to Include: The type of records that are included in the report.

Request items types: The type of items requested in the report. The report can contain roles, resources, and provisioning request definitions. This section also displays a count of the items and the Identity Vault from where these items came.

Data Source: A connection from a database the user is accessing.

9.2 Report Content

The report displays the following information about each item type:

Item Type: The item type for the report and all items of this type are listed in this section. This report displays roles, resources, and request definitions.

Name: The name of the item.

Description: The description of the specific item in the report.

Owner: The owner of the item. If there is no owner, the field is blank.

Category: The category of the item. If there is no category, the field is blank.

Identity Vault Name: The name of the Identity Vault where the item resides.

10 Available Permissions Current State

This report displays detailed information about the current state of all roles, resources, and provisioning request definitions that an end user can request in the organization. The items are grouped by the Identity Vault in which they reside.

10.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Date: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Request items types: The type of items requested in the report. The report can contain roles, resources, and provisioning request definitions. This also displays a count of the items and the Identity Vault where these items came from.

Data Source: A connection from a database the user is accessing.

10.2 Report Content

The report displays the following information about each item type:

Item Type: The item type for the report and all items of this type are listed in this section. This report displays roles, resources, and request definitions.

Name: The name of the item.

Description: The description of the specific item in the report.

Owner: The owner of the item. If there is no owner, the field is blank.

Category: The category of the item. If there is no category, the field is blank.

Identity Vault Name: The name of the Identity Vault where the item resides.

11 Correlated Resource Assignment Events by Users

This report displays information about correlated events for the select Identity Vault user and resource.

Events are sorted by the time they are listed in the Event Auditing Service (EAS), not when they actually occurred. On some machines, the User Application events take a longer time to be listed in the EAS than the Identity Manager events.

11.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates when the resource was assigned.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault user: The name of the select Identity Vault user.

Resource: The resource the report ran against.

(Conditional) Show detailed message: This line is displayed if you selected the *Show detailed message* parameter.

Data Source: A connection from the database the user is accessing.

11.2 Report Content

The report displays the activities for the selected Identity Vault user.

Event name: The event that occurred. For example Workflow Started.

Actor: The account that performed the event.

Event time: The time of the event.

12 Data Collection State Report

This report displays information about the current state of the data collectors, including detailed information about each executed collection.

12.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates when the resource was assigned.

Limits results to: The number of items displayed in the report.

Data Source: A connection from the database the user is accessing.

12.2 Report Content

The report lists information about the data collectors.

Collector name: The name of the collector.

Description: The unique description of the collector.

Type: Type of collector.

Host: The IP address.

Last collection: The timestamp of the last collection date.

Current state: The current state of the collection.

Port: The port number.

Next collection: The timestamp of the next collection date.

13 Database Statistics

This report displays key statistics for the specified data source. The Identity Vault Overview and Database Overview sections represent current state information. The Audit Event Overview section represents the summary of events during the given date range.

13.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Limits results to: The number of items displayed in the report.

Data Source: A connection from the database the user is accessing.

13.2 Report Content

This section displays the subcomponents of each data source for a given date range.

13.2.1 Identity Vault Overview

This section displays the total number of entries in each current state view related to the Identity Vault.

Classification: The name of the Identity Vault from which the information is retrieved.

View: The current state view.

Total Entries: The total number of entries in each view.

13.2.2 Audit Event Overview

This section displays event counts by source for all audit events that occurred during the specified date range.

Source: The name of the object assigned to the role.

Event: The event that occurred. For example Publisher Status Success heartbeat.

Count: The number of times the event occurred during a specified date range.

Severity: The intensity of importance of each audit event.

13.2.3 Database Overview

This section displays estimated row counts for tables greater than 64 KB grouped by schema. The table size includes the data and all associated indexes and toast tables. The date in the Last Analyzed column indicates when the last ANALYZE or VACUUM operations were run on the table. Configure the PostgreSQL autovacuum daemon to run periodically on the database; this will keep the accuracy of the row count estimates and table sizes more current.

Table: Name of the table for the given schema.

Estimated rows: A rough calculation of number of rows for each table greater than 64 kilobytes (KB) grouped by schema.

Size(MB): The size of each table in megabytes.

Last Analyzed: Indicates when the last ANALYZE or VACUUM operations were run on the table.

14 Identity Vault Driver Associations Report

This report displays the associations for the selected driver. An association is a unique value that enables Identity Manager to associate objects in connected systems. Each object has an association for each driver that synchronizes that object.

14.1 Report Criteria

Identity Manager displays the report criteria used to run the report in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Sort on: How the information in the report is sorted. It can be sorted by user or by driver name.

Data source: A connection from the database the user is accessing.

14.2 Report Content

The report displays the association between the users and drivers for a given date and time range.

Not Associated:

- **User name:** The name of the user that is not associated with a driver.
- **Driver name:** The name of the driver that is not associated with a user.

Associated:

- **User name:**The name of the user that is associated with a driver.
- **Driver name:**The name of the driver that is associated with a user.

15 Identity Vault Driver Associations Report Current State

This report displays the current associations for the drivers. An association is a unique value that enables Identity Manager to associate objects in connected systems. Each object has an association for each driver that synchronizes that object.

15.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Sort on: How the information in the report is sorted. It can be sorted by user or by driver name.

Data Source: A connection from a database the user is accessing.

15.2 Report Content

The report lists the users with the associated drivers, then it lists any users that are not associated.

Not Associated:

- **User name:** The name of the user that is not associated with a driver.
- **Driver name:** The name of the driver that is not associated with a user.

Associated:

- **User name:**The name of the user that is associated with a driver.
- **Driver name:**The name of the driver that is associated with a user.

16 Identity Vault User

This report displays all relevant profile information for the selected Identity Vault users.

16.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Records to include: Whether the latest changes are included in the report or whether it shows all changes for changed records.

Data Source: A connection from a database the user is accessing.

16.2 Report Content

The report starts by listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults. The following of information is displayed for each Identity Vault user:

Full name: The full name of the user.

The full name is the first_name, middle_name, and last_name concatenated together, based on the *Name order* parameter. This is not the same as the full_name field in the database, which is mapped to the fullName attribute in the Identity Vault. The full_name database file is not included in this report, and if you change the full_name attribute on the user in the Identity Vault, but not the first_name, middle_name, or last_name attributes, there are duplicate records displayed in the report.

Pref name: The preferred name of the user.

Prefix: The prefix for the username.

Suffix: The suffix for the username.

Pref lang: The preferred language for the user.

Company: The name of the company.

Job code: The user's job code.

Job title: The user's job title.

Work ID: The user's workforce ID.

Emp status: The user's employee status.

Emp type: The user's employee type. For example, full time.

Manager: The user's manager.

ID Vault DN: The user's Identity Vault distinguished name (DN).

ID Vault st: The user's status in the Identity Vault.

Acct desc: A description of the user's account in the Identity. Vault.

Cost center: The cost center assigned to the user.

CC desc: A description of the cost center assigned to the user.

Mail stop: The user's mail stop.

Office name: The name of the user's office.

Dept #: The user's department number.

Department: The user's department name.

Location: The physical location of the user.

Address: The address of the user.

Phone: The user's phone number.

e-mail: The user's e-mail address.

IM: The user's instant message username.

Hire date: The user's hire date.

Trans date: The user's transfer date.

Term date: The user's termination date.

First w. day: The first day a user starts working.

Last w. day: The last day a user works.

Eff. date: The user's effective start date.

User image: If you selected to include the user's image, it is the last item displayed in the report.

If the user's image changed and the option to *Include user image* is not selected there might be two entries displayed for the user's image.

17 Identity Vault User Report Current State

This report displays the current state of all relevant profile information for the selected Identity Vault users.

17.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Date: The date when the report was run is listed in the title bar.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Data Source: A connection from a database the user is accessing.

17.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults. The following information is displayed for each Identity Vault user:

Full name: The full name of the user.

The full name is constructed to be the first_name, middle_name, and last_name concatenated together base on the *Name order* parameter. This is not the same as the full_name field in the database, which is mapped to the fullName attribute in the Identity Vault. The full_name database file is not included in this report, and if you change the full_name attribute on the user in the Identity Vault, but not the first_name, middle_name, or last_name attributes, there are duplicate records displayed in the report.

Pref name: The preferred name of the user.

Prefix: The prefix for the username.

Suffix: The suffix for the username.

Pref lang: The preferred language for the user.

Company: The name of the company.

Job code: The user's job code.

Job title: The user's job title.

Work ID: The user's workforce ID.

Emp status: The user's employee status.

Emp type: The user's employee type. For example, full time.

Manager: The user's manager.

ID Vault DN: The user's Identity Vault distinguished name (DN).

ID Vault st: The user's status in the Identity Vault.

Acct desc: A description of the user's account in the Identity. Vault.

Cost center: The cost center assigned to the user.

CC desc: A description of the cost center assigned to the user.

Mail stop: The user's mail stop.

Office name: The name of the user's office.

Dept #: The user's department number.

Department: The user's department name.

Location: The physical location of the user.

Address: The address of the user.

Phone: The user's phone number.

e-mail: The user's e-mail address.

IM: The user's instant message username.

Hire date: The user's hire date.

Trans date: The user's transfer date.

Term date: The user's termination date.

First w. day: The first day a user starts working.

Last w. day: The last day a user works.

Eff. date: The user's effective start date.

User image: If you selected to include the user's image, it is the last item displayed in the report.

18 Identity Vault Users with Access to Managed Systems

This report displays the last collection date of the data and when the data is scheduled to be collected again from each collector.

18.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Managed Systems: The managed systems that are included in the report.

Data Source: A connection from a database the user is accessing.

18.2 Report Content

The report starts with listing the users by the name order that you selected in the report parameters.

Name: The name of the user. It is displayed according to the criteria you selected in the name order report parameter.

Managed System: The name of the managed system.

Account ID: The user account ID in the managed system.

Account Status: The status of the account in the managed system.

Entitlement Value: The value of the managed system entitlement that grants the account access in the managed system.

19 Identity Vault Users with Access to Managed Systems Current State

This report shows the current state of all Identity Vault users that have some kind of access to the Managed System, and shows how they are represented within the Managed System.

19.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Date The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Name order: How the user records are displayed in the report.

Identity Vault users: The users that are included in the report.

Managed Systems: The managed systems that are included in the report.

Data Source: A connection from a database the user is accessing.

19.2 Report Content

The report starts with listing the users by the name order that you selected in the report parameters.

Name: The name of the user. It is displayed according to the criteria you selected in the name order report parameter.

Managed System: The name of the managed system.

Account ID: The user account ID in the managed system.

Account Status: The status of the account in the managed system.

Entitlement Value: The value of the managed system entitlement that grants the account access in the managed system.

20 Managed System Data Collection Report

This report displays the last collection date of the data and when the data is scheduled to be collected again from each collector.

20.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

20.2 Report Content

The report displays the last collection date of the data, and indicates when the data is scheduled to be collected again from each collector.

Collector Name: The name of the collector.

Last Collected Date Time: The time the collector last collected data.

Next Collection Data Time: The time the collector is scheduled to collect data next.

21 Managed System Entitlement and Account Summary

This report provides a summary of entitlements associated with Managed Systems grouped by data collector. For each Managed System, the number of entitlements by type, assigned entitlements by type, and the account entitlement types are provided.

21.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

21.2 Report Content

This section lists all entitlements associated with Managed Systems. The entitlements are grouped by data collector. The details namely number of entitlements, assigned entitlements, account entitlements are provided for each type.

Collector: The name of the data collector.

Driver: The name of the driver that corresponds to the collector.

Number of Managed Systems: The number of managed systems.

Number of Logical Systems: The number of logical systems.

Entitlements: The entitlements associated with the managed systems.

Potential values: The number of entitlement types.

Number of assignments: The number of assigned entitlements by type.

Number of assigned accounts: The number of account entitlements by type.

22 Object Provisioning

This report shows all attempted data object provisioning and de-provisioning events captured by Identity Manager within the selected date range, grouped by the subcomponent of the initiating service that caused this event and then grouped by the context for the data object.

22.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

22.2 Report Content

This section displays subcomponents belonging to the desired group name under each event.

Initiating Service: The subcomponent of the initiating service.

Data Context: Context for the data object.

Event: The activity that occurred.

Initiator: The user who initiated the event.

Extended Information: Additional information about the event.

23 Password Resets

This report shows all password changes captured by Identity Manager within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.

23.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits collectors to: The number of items displayed in the report.

Show System Password Events: Displays password changes to a system. The user has the ability to enable or disable this feature.

Data Source: A connection from a database the user is accessing.

23.2 Report Content

This section displays the changes made to passwords for each account, grouped by its domain.

Event & Time: The activity that occurred and when it was performed.

Initiator: The user who initiated the event.

Extended Information: Additional information about the event.

24 Resource Assignments by Resource

This report displays general resource information for selected resources.

24.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Resources: The resources contained in the report.

Data Source: A connection from a database the user is accessing.

24.2 Report Content

The report starts with listing the Identity Vault where the resource records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

Resource: The name of the resource.

Assigned to: The user that is assigned to the resource.

Effective date: The effective dates of the resource for the resource.

Entitlement: The name of the entitlement that granted the resource to the resource.

Driver: The name of the driver that granted the entitlement.

25 Resource Assignments by Resource Current State

This report displays the current state of the general resource information, resource assignments, and entitlements for selected resources.

25.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Resources: The resources contained in the report.

Data Source: A connection from a database the user is accessing.

25.2 Report Content

The report starts with listing the Identity Vault where the resource records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

Resource: The name of the resource.

Assigned to: The user that is assigned to the resource.

Effective date: The effective dates of the resource for the resource.

Entitlement: The name of the entitlement that granted the resource to the resource.

Driver: The name of the driver that granted the entitlement.

26 Resource Assignments by User

This report displays general resource information, resource assignments, and entitlements for selected resources.

26.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Identity Vault users: The users that are included in the report.

Data Source: A connection from a database the user is accessing.

26.2 Report Content

The report lists information according to the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

User Name: The name of the user account.

Resource: The name of the resource.

Effective date: The effective dates of the resource for the user account.

Entitlement: The name of the entitlement that granted the resource to the user account.

Driver: The name of the driver that granted the entitlement.

27 Resource Assignments by User Current State

This report displays the current state of the general resource information, resource assignments, and entitlements for selected Identity Vault users.

27.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Identity Vault users: The users that are included in the report.

Data Source: A connection from a database the user is accessing.

27.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

User Name: The name of the user account.

Resource: The name of the resource.

Effective date: The effective dates of the resource for the user account.

Entitlement: The name of the entitlement that granted the resource to the user account.

Driver: The name of the driver that granted the entitlement.

28 Role Assignments by Role

This report displays general role information and memberships for selected roles.

28.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Roles: The roles that are included in the report.

Data Source: A connection from a database the user is accessing.

28.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

Role: The name of the role and a description of the role.

Assigned to: The object the role is assigned to.

Effective date: The effective dates of the role.

Source: The name of the object assigned to the role.

29 Role Assignments by Role Current State

This report displays the current state of the role membership information about the selected Identity Vault users, including general role information and whether the Identity Vault user's membership in each role is a policy violation.

29.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates The date range the report was run.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Roles: The roles that are included in the report.

Data Source: A connection from a database the user is accessing.

29.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

Role: The name of the role and a description of the role.

Assigned to: The object the role is assigned to.

Effective date: The effective dates of the role.

Source: The name of the object assigned to the role.

30 Role Assignments by User

This report displays role membership information about the selected Identity Vault users, including general role information and whether the Identity Vault user's membership in each role is a policy violation.

30.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Identity Vault users: The users that are included in the report.

Data Source: A connection from a database the user is accessing.

30.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

User Name: The name of the user account.

Role: The name of the role.

Effective date: The effective dates of the resource for the user account.

Source: The name of the object assigned to the role.

If there is a conflict, the reports lists the conflicting role, the conflicting dates, and the separation of duties constraint.

31 Role Assignments by User Current State

This report displays the current state of the role membership information about the current state of the selected Identity Vault users, including general role information and whether the Identity Vault user's membership in each role is a policy violation.

31.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Limit results to: The number of items displayed in the report.

Name order: The order the names are displayed in the report.

Identity Vault users: The users that are included in the report.

Data Source: A connection from a database the user is accessing.

31.2 Report Content

The report starts with listing the Identity Vault where the user records came from. If you have more than one Identity Vault, the records are sorted by Identity Vaults.

User Name: The name of the user account.

Role: The name of the role.

Effective date: The effective dates of the resource for the user account.

Source: The name of the object assigned to the role.

If there is a conflict, the reports lists the conflicting role, the conflicting dates, and the separation of duties constraint.

32 Role Hierarchy Report

This report lists the hierarchy of all roles within your organization. The highest level roles are Business Roles, followed by IT and Permission Roles in that order. Indentation is used to demonstrate this hierarchy throughout the report. One possible use of this report is to help in effectively assigning roles and permissions to users. The report data can be configured by selecting from a predefined list of criteria.

32.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Limit results to: The number of items displayed in the report.

Report Type: The type of report selected.

Show Resources: Indicates whether the resources associated with each role are included in the report output.

Data Source: A connection from a database the user is accessing.

32.2 Report Content

The report sorts the data in ascending order alphabetically at each level of the role hierarchy. For each role in the hierarchy, the report shows the resources associated with the role.

Business Roles: The name of each business role and a description of the role.

IT Roles: The name of each IT role and a description of the role.

Permission Roles: The name of each Permission Role and a description of the role.

33 Sample Parameters Report

This report contains many common parameters and examples of the different report parameter types that can be used to customize a report.

33.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The date range when the report was run.

Limit results to: The number of items displayed in the report.

Records to include: The records included in the report.

Name order: The order the names are displayed in the report.

Identity Vault users: The Identity Vault users included in the report.

Roles: The roles that are included in the report.

Resource: The resource included in the report.

Managed Systems: The managed systems included in the report.

Identity Vault user: The Identity Vault user included in the report.

Sort on: How the information is displayed in the report.

Request item types: The request item types included in the report.

Integer example: The integer example field.

String example: The string example field.

Show detailed message: The detailed message for the report.

Data Source: A connection from a database the user is accessing.

33.2 Report Content

The report contains the following information:

Name: The name of the users in the report.

Title: The title of the users.

Status: The status of the users.

34 Self Password Changes

This report shows all self-password change attempts captured by Identity Manager within the selected date range, grouped by the domain within which the account exists and then grouped by the name of the user who attempted to change their password.

34.1 Report Criteria

The report criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Identity Vault Users: The users for whom you want to run the report.

Departments: The departments included in the report.

Name Order Specifies how the user records are displayed in the report.

Data Source: A connection from a database the user is accessing.

34.2 Report Content

The report starts with listing the domain within which the account exists and then grouped by the name of the user. The following information is displayed for each user who attempted to change their password.

Domain Name: Specifies the name of the domain.

First Name: Specifies the first name of the user associated with the user name.

Last Name: Specifies the last name of the user associated with the user name.

Username: Specifies the user name.

Department: Specifies the department associated with the user.

Event: Specifies password failure or success and the timestamp. duties.

Message: Specifies a message when a user changes their password and lists whether or not it was successful.

35 Separation of Duty Conflicts by Use

This report displays Identity Vault users whose role memberships are violations of separation of duties policies.

35.1 Report Criteria

The report criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Identity Vault Users: The users for whom you want to run the report.

Data Source: A connection from a database the user is accessing.

35.2 Report Content

This report starts with listing the Identity Vault Name and then grouped by the name of the user. The following information is displayed for those users whose role memberships are violations of separation of duties policies.

Identity Vault Name: Specifies the name of the localhost.

Name: The name of the user whose role membership is in violation.

Roles in Conflict: Specifies the conflicting role.

Conflict Dates: Specifies the date when the conflict occurred.

Separation of Duties Constraint: The constraint that shows the separation of duties.

36 User Password Change Events Summary

This report shows user password change events captured by Identity Manager within the selected date range.

36.1 Report Criteria

The report criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

36.2 Report Content

This report shows the total password change events by the given event date.

Event Date: The date of the event captured.

Number of Password Change Events: The total number of password changes for all users.

37 User Password Changes within the Identity Vault

This report shows all password status changes for users within the Identity Vault.

37.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

37.2 Report Content

The report first shows a summary of Identity Vault users whose passwords changed. The report then lists Identity Vault users whose passwords did not change.

37.2.1 IDV Users Who Changed Password During Report Period

IDV Users: The names of the users whose passwords changed.

Account ID: The account ID for the user whose password changed.

When Changed: The timestamp of the change.

Changed By: The user who made the change.

37.2.2 IDV Users Who Did Not Changed Password During Report Period

IDV Users: The names of the users whose passwords did not change.

Account ID: The account ID for the user whose password did not change.

38 User Status Changes within the Identity Vault

This report shows all status changes for users in the Identity Vault.

38.1 Report Criteria

The criteria used to run the report are displayed in the top section of the report.

Dates: The range of dates and times when the report was run.

Limits results to: The number of items displayed in the report.

Data Source: A connection from a database the user is accessing.

38.2 Report Content

The report shows the types of changes that have occurred for Identity Vault users within a particular period of time.

Type of Change: A brief description of the type of status change.

IDV User: The name of the user whose status changed.

Account ID: The account ID for the user.

When Changed: The timestamp for the status change.