



SailPoint

Version 7.3 -3

Integration Guide

Copyright © 2019 SailPoint Technologies, Inc., All Rights Reserved.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Specially Designated Nationals (SDN) List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Copyright and Trademark Notices. Copyright © 2019 SailPoint Technologies, Inc. All Rights Reserved. All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet web site are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint Technologies & Design," "SailPoint," "IdentityIQ," "IdentityNow," "SecurityIQ" "IdentityAI" "AccessIQ," "Identity Cube," "Managing the Business of Identity" are registered trademarks of SailPoint Technologies, Inc. "Identity is Everything" and "The Power of Identity" are trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

Table of Contents

Chapter 1: Overview	1
What is SailPoint IdentityIQ?	1
SailPoint Integration Guide Overview	2

Section I: SailPoint IdentityIQ Infrastructure Modules

Access Management Infrastructure Modules 7

Chapter 2: IdentityIQ for Okta	9
Overview	9
Supported features	9
Pre-requisite	10
Configuration parameters	10
Additional configuration parameters	11
Schema attributes	11
Account attributes	12
Group attributes	13
Application attributes	13
Provisioning Policy attributes	14
Create Account Policy	14
Create Group Policy	15
Disable Policy	15
Additional information	15
Aggregation Best Practices	15
Supported Aggregation Filters	16
Account Status Mapping	17
Upgrade considerations	18
Delta Aggregation	18
Troubleshooting	19

Security Information And Event Management Infrastructure Modules 21

Chapter 3: IdentityIQ for ArcSight IT Security	23
Overview	23
Common Event Format (CEF)	23
Supported features	24
Supported platform	24
Pre-requisites	24
Configuration	24
Configuration to export IdentityIQ Data to ArcSight	24
Configuration to Import HP ArcSight CEF Flat File to SailPoint IdentityIQ	28

IT Service Management Infrastructure Modules 31

Chapter 4: IdentityIQ for ServiceNow Service Desk	33
Overview	33
Supported features	33

Supported platforms	33
Pre-requisites	34
Service Request	34
Incident and Change Request	34
Basic configuration	35
Basic flow of Service Request	37
Basic configuration of Service Request	37
Configuring IdentityIQ to integrate with ServiceNow	38
IntegrationConfig XML files for Service Request, Incident and Change Request	41
Configuration procedure	42
Verifying connectivity between IdentityIQ and ServiceNow	44
Retryable mechanism	44
Sample scenario	45
Troubleshooting	46
Chapter 5: IdentityIQ for MicroFocus Service Manager Service Desk	49
Overview	49
Supported features	49
Supported platforms	50
Pre-requisites	50
Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration	53
Verifying connectivity between IdentityIQ and HP Service Manager (Micro Focus)	60
Retryable mechanism	61
Additional information	61
Creating New Service Request Catalog Item	61
Exporting user details from HP Service Manager (Micro Focus)	62
Importing user details from HP Service Manager (Micro Focus) to IdentityIQ	62
Troubleshooting	62
Chapter 6: IdentityIQ for BMC Remedy Service Desk	65
Overview	65
Supported features	65
Supported platforms	65
Pre-requisites	66
Basic configuration	66
Configuring BMC Remedy AR System for IdentityIQ Integration	67
Configuring IdentityIQ for BMC Remedy Action Request System Integration	69
BMC Remedy Action Request System Integration	69
Creating multiple tickets in Remedy System	73
Verifying connectivity between IdentityIQ and BMC Remedy	74
Retryable mechanism	74
Sample scenario	75
Troubleshooting	76
Chapter 7: IdentityIQ for ServiceNow Catalog	77
Overview	77
Supported features	78
Supported platforms	79
Pre-requisites	79
Installation and configuration in ServiceNow	79
Installation	79
Configuration	81
Configuration in SailPoint IdentityIQ	83

Troubleshooting	83
Chapter 8: IdentityIQ for ServiceNow Catalog API	85
Overview	85
Supported features	86
Supported platforms	86
Pre-requisites	86
Installation and configuration in ServiceNow	86
Installation	86
Configuration	88
Configuration in SailPoint IdentityIQ	89
Status Maps	89
Troubleshooting	90
Enterprise Mobility Management Infrastructure Modules	91
Chapter 9: IdentityIQ for AirWatch Enterprise Mobility Management	93
Overview	93
Supported features	93
Supported platforms	94
Pre-requisites	94
Configuration	94
Application configuration	95
Operation specific configuration	95
Chapter 10: IdentityIQ for MobileIron Enterprise Mobility Management	97
Overview	97
Supported features	97
Supported platforms	98
Pre-requisites	98
Configuration	98
Application configuration	98
Operation specific configuration	99
Chapter 11: IdentityIQ for Good Technologies Enterprise Mobility Management	101
Overview	101
Supported features	101
Supported platform	102
Pre-requisites	102
Configuration	102
Application configuration	102
Operation specific configuration	103
Provisioning Infrastructure Modules	105
Chapter 12: IdentityIQ for Oracle Identity Manager	107
Overview	107
Supported features	107
Supported platforms	108
Installing the OIM Integration Web Application	108
Authentication for Web Application	108
Testing the OIM Integration Web Application	109
Properties that can be defined in xellerate.properties	110

Configuration for OIM application	111
Testing the OIM Integration Client	111
Aggregating from OIM	112
Known/Open issues	112
Chapter 13: IdentityIQ for IBM Security Identity Manager	113
Overview	113
Supported features	113
Supported platforms	114
General configuration	114
Configuration for Aggregation	114
Configuration for Provisioning	114
Troubleshooting	116
IaaS - Infrastructure-As-A-Service Module	117
Chapter 14: IdentityIQ for Amazon Web Services	119
IdentityIQ for Amazon Web Services Setup	119
IdentityIQ for Amazon Web Services	119
Supported features	120
Pre-requisites	121
Administrator permissions	122
Configuration parameters	125
Schema attributes	126
Provisioning Policy attributes	130
Additional information	132
(Optional) Upgrade Consideration	132
IdentityIQ for Amazon Web Services	132
 Section II: SailPoint IdentityIQ Application Modules	
Enterprise Resource Planning Application Modules	141
Chapter 15: IdentityIQ for SAP ERP - SAP Governance Module	143
Overview	143
Supported features	143
Supported Managed Systems	145
Pre-requisites	145
Administrator permissions	145
Configuration parameters	150
Schema attributes	152
Account attributes	152
Group attributes	156
Schema extension and custom attributes	157
Upgrade considerations	157
Provisioning Policy attributes	158
Create account attributes	158
Additional information	158
Entitlement validity period	158
CUA support	158
Entitlement Data	159
Password Change	159

Logon and Communication Language attributes	159
Delta Aggregation	160
Partitioning Aggregation	163
Troubleshooting	163
Chapter 16: IdentityIQ for Oracle ERP – Oracle E-Business Suite	167
Overview	167
Supported features	167
Supported Managed Systems	168
Pre-requisites	168
Administrator permissions	168
Configuration parameters	171
Additional configuration parameter	173
Schema attributes	174
Account attributes	174
Group attributes	176
Provisioning Policy attributes	177
Create account attributes	177
Create group attributes	177
Additional information	178
Upgrade considerations	178
Support for Oracle Security Feature	179
User Editions	179
Support of provisioning of Start Date, End Date and Justification attributes	179
Troubleshooting	180
Chapter 17: IdentityIQ for SAP ERP – SAP Portal - User Management Web Service 183	
Overview	183
Supported features	184
Supported Managed Systems	184
Pre-requisite	184
Administrator permission	185
Configuration parameters	185
Schema attributes	186
Account attributes	186
Group attributes	187
Provisioning Policy attributes	187
Create account attributes	187
Create Group attributes	188
Additional information	189
Undeploy .sda file	189
Troubleshooting	189
Chapter 18: IdentityIQ for Oracle ERP – PeopleSoft	191
Overview	191
Supported features	191
Supported Managed Systems	192
Pre-requisites	192
Administrator permission	192
Configuration parameters	192
Schema attributes	194
Account attributes	194
Group attributes	195

Additional information	195
Creating the Component Interfaces	196
Partitioning Aggregation	196
Performance improvement	196
Creating the Component interface jar file	198
Configuring the Component Interface Security	199
Upgrade considerations	200
Troubleshooting	200
Chapter 19: IdentityIQ for Oracle ERP – Siebel	203
Overview	203
Supported features	203
Supported Managed Systems	204
Pre-requisites	204
Administrator permission	204
Configuration parameters	204
Schema attributes	206
Account attributes	206
Account Group attributes	206
Adding new custom attributes in schema	207
Provisioning policy attributes	207
Additional information	208
Employment Status	209
Troubleshooting	209
Chapter 20: IdentityIQ for NetSuite ERP	211
Overview	211
Supported features	212
Supported Managed Systems	212
Administrator permissions	212
Configuration parameters	213
Schema attributes	213
Account attributes	213
Group attributes	214
Schema extension and custom attributes	214
Provisioning Policy attributes	215
Additional information	216
NetSuite Application Program Interface (API)	216
Troubleshooting	217
SAP Governance Modules	219
Chapter 21: SailPoint SAP Governance Module	221
SAP Governance Module Setup	221
SAP Governance Module	221
SAP Governance Application Modules	223
Chapter 22: IdentityIQ for SAP GRC	225
Introduction	225
Supported features	226
(<i>Optional</i>) Support of additional feature	227
Supported platforms	227

Pre-requisites	227
SAP GRC Server Settings	227
SAP Connector changes for supporting SAP GRC integration	228
Creating IdentityIQ application of type SAP GRC	229
SAP GRC workflows	230
Minimum permissions required for SAP GRC user	233
Custom workflows provided for SAP GRC integration	234
SAP GRC Data Generator	234
SAP GRC Request Executor	235
Importing SAP GRC Application Rule	237
Viewing the reports	238
Upgrade considerations	238
Support proactive check and SAP CUA integration	238
Upgrade settings	238
Additional information	239
Creating a RFC Connection on SAP GRC system	239
Configuring cross system on SAP GRC	240
(Optional) Support for additional parameters	241
Support for provisioning start and end date for role assignment	243
Troubleshooting	244

Healthcare Integration Modules 249

Chapter 23: IdentityIQ for Epic Healthcare 251

Overview	251
Important consideration	251
Supported features	252
Supported Managed System	252
Pre-requisites	252
Administrator permissions	253
Configuration parameters	253
Additional configurations for WS-Security	255
Schema Attributes	255
Account attributes	255
Group attributes	260
Provisioning Policy attributes	261
Troubleshooting	264

Chapter 24: IdentityIQ for Cerner Healthcare 267

Overview	267
Supported features	267
Pre-requisites	267
Configuration parameters	268
Additional configuration parameters	268
Schema attributes	268
Account attributes	268
Group attributes	270
Provisioning Policy attributes	270
Create Account	270
Update Account	270
Troubleshooting	272

Mainframe Integration Modules	275
Chapter 25: IdentityIQ for RACF Mainframe	277
Overview	277
Supported features	277
Installing IdentityIQ for RACF Mainframe	277
Chapter 26: IdentityIQ for TopSecret Mainframe	279
Overview	279
Supported features	279
Installing IdentityIQ for TopSecret Mainframe	279
Chapter 27: IdentityIQ for ACF2 Mainframe	281
Overview	281
Supported features	281
Installing IdentityIQ for ACF2 Mainframe	281
Chapter 28: IdentityIQ for RACF LDAP Mainframe	283
Overview	283
Supported features	283
Supported Managed Systems	284
Pre-requisites	285
Administrator permissions	285
Configuration parameters	285
Additional configuration parameter	286
Schema Attributes	286
Account attributes	287
Group attributes	289
Provisioning Policy Attributes	289
Additional information	290
Support for PassPhrase	290
Support for Connection Attributes	290
Implementing Secured Communication to RACF LDAP Server	290
Defining Search Scope	293
Troubleshooting	294
Chapter 29: IdentityIQ for TopSecret LDAP Mainframe	297
Overview	297
Supported features	297
Supported Managed Systems	298
Administrator permissions	298
Configuration parameters	298
Schema Attributes	299
Account attributes	299
TopSecretProfile attributes	301
TopSecretGroup attributes	302
Provisioning Policy Attributes	302
Additional information	303
Support for PassPhrase	303
Implementing Secured Communication to Top Secret LDAP Server	303
Partitioning Aggregation	306

Appendix309

Appendix A: Common Identity Management Integration Configuration311

Overview	311
Creating the IntegrationConfig Object	311
Provisioning	316

Appendix B: Component Interface319

Creating component interface for PeopleSoft	319
Basic structure of Custom Component (CI) from USERMAINT component for Users	319
Basic structure of Custom Component (CI) from ROLEMAINT component for Roles	325
Basic structure of Custom Component (CI) from RTE_CNTL_PROFILE component for Users	327
Basic structure of Custom Component (CI) from PURGE_USR_PROFILE component for Delete User	330
Basic structure of Component Interface (CI) from PURGE_ROLEDEFN component for Delete Role	332
Deleting the component interface	333

Appendix C: Connector Classloader.....335

Chapter 1: Overview

The following topics are discussed in this chapter:

What is SailPoint IdentityIQ?	1
SailPoint Integration Guide Overview	2

What is SailPoint IdentityIQ?

SailPoint is an identity and access management solution for enterprise customers that delivers a wide variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. Furthermore, IdentityIQ has a flexible connectivity model that simplifies the management of applications running in the datacenter or the cloud.

Compliance Manager — IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework. This enables you to streamline compliance processes and improve the effectiveness of identity governance, all while lowering costs.

Lifecycle Manager — IdentityIQ Lifecycle Manager manages changes to access through user - friendly self - service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

Privileged Account Management Module — IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.

Connectors and Integration Modules — IdentityIQ offers Integration Modules that support the extended enterprise IT infrastructure. Third party provisioning and service desk integration enable multiple sources of fulfillment to access change. Service catalog integration supports a unified service request experience with integrated governance and fulfillment. Mobile device management integration mitigates risk posed by mobile devices through centralized visibility, control and automation. And IdentityIQ's IT security integration provides enhanced security with improved responsiveness and controls.

Open Identity Platform — SailPoint's Open Identity Platform lays the foundation for effective and scalable IAM within the enterprise. It establishes a common framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources. The Open Identity Platform is fully extensible, providing robust analytics which transforms disparate and technical identity data into relevant business information, resource connectivity that allows organizations to directly connect IdentityIQ to applications running in the datacenter or in the cloud, and APIs and a plugin framework to allow customers and partners to extend IdentityIQ to meet a wide array of needs. An open platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications-in the datacenter and the cloud. SailPoint applies consistent governance across compliance, provisioning and access management processes, maximizing investment and eliminating the need to buy and integrate multiple products.

Password Manager — IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device. By providing intuitive self-service and delegated administration options to manage passwords while enforcing enterprise-grade password, IdentityIQ enables businesses to reduce operational costs and boost productivity.

Amazon Web Services (AWS) Governance Module — Enables organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide

a central point of visibility, administration, and governance across the entire enterprise. This includes policy discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support.

SAP Governance Module — Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities enable more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as T-Codes and Authorization Objects.

SailPoint Integration Guide Overview

SailPoint Integration Modules deliver extended value from standard IdentityIQ deployments. SailPoint is committed to providing design, configuration, troubleshooting and best practice information to deploy and maintain strategic integrations. SailPoint has modified the structure of this document to aid customers and partner deployments. The focus of this document is product configuration and integration. For more details on design, troubleshooting and deployment best practices, refer to the Connector and Integration Deployment Center in Compass, SailPoint's Online customer portal.

This document provides a guide to the integration between the following products and IdentityIQ:

- **SailPoint IdentityIQ Infrastructure Modules**
 - **Access Management Infrastructure Modules**
 - IdentityIQ for Okta
 - **Security Information And Event Management Infrastructure Modules**
 - IdentityIQ for ArcSight IT Security
 - **IT Service Management Infrastructure Modules**
 - IdentityIQ for ServiceNow Service Desk
 - IdentityIQ for MicroFocus Service Manager Service Desk
 - IdentityIQ for BMC Remedy Service Desk
 - IdentityIQ for ServiceNow Catalog
 - IdentityIQ for ServiceNow Catalog API
 - **Enterprise Mobility Management Infrastructure Modules**
 - IdentityIQ for AirWatch Enterprise Mobility Management
 - IdentityIQ for MobileIron Enterprise Mobility Management
 - IdentityIQ for Good Technologies Enterprise Mobility Management
 - **Provisioning Infrastructure Modules**
 - IdentityIQ for Oracle Identity Manager
 - IdentityIQ for IBM Security Identity Manager

- **IaaS - Infrastructure-As-A-Service Module**
 - IdentityIQ for Amazon Web Services
- **SailPoint IdentityIQ Application Modules**
 - **Enterprise Resource Planning Application Modules**
 - IdentityIQ for SAP ERP - SAP Governance Module
 - IdentityIQ for Oracle ERP – Oracle E-Business Suite
 - IdentityIQ for SAP ERP – SAP Portal - User Management Web Service
 - IdentityIQ for Oracle ERP – PeopleSoft
 - IdentityIQ for Oracle ERP – Siebel
 - IdentityIQ for NetSuite ERP
 - **SAP Governance Modules**
 - IdentityIQ for SAP ERP - SailPoint SAP Governance Module
 - **SAP Governance Application Modules**
 - IdentityIQ for SAP GRC
 - **Healthcare Integration Modules**
 - IdentityIQ for Epic Healthcare
 - IdentityIQ for Cerner Healthcare
 - **Mainframe Integration Modules**
 - IdentityIQ for RACF Mainframe
 - IdentityIQ for TopSecret Mainframe
 - IdentityIQ for ACF2 Mainframe
 - IdentityIQ for RACF LDAP Mainframe
 - IdentityIQ for TopSecret LDAP Mainframe

This document is intended for the above products and IdentityIQ System Administrators and assumes an advance level of technical knowledge.

Section I: SailPoint IdentityIQ Infrastructure Modules

The SailPoint IdentityIQ Infrastructure Modules section includes the following modules:

- "Access Management Infrastructure Modules"
- "Security Information And Event Management Infrastructure Modules"
- "IT Service Management Infrastructure Modules"
- "Enterprise Mobility Management Infrastructure Modules"
- "Provisioning Infrastructure Modules"
- "IaaS - Infrastructure-As-A-Service Module"

Access Management Infrastructure Modules

This section contains information on the following section:

- “IdentityIQ for Okta”

Chapter 2: IdentityIQ for Okta

The following topics are discussed in this chapter:

Overview	9
Supported features	9
Pre-requisite	10
Configuration parameters	10
Schema attributes	12
Account attributes	12
Group attributes	13
Application attributes	14
Provisioning Policy attributes	14
Create Account Policy	15
Create Group Policy	15
Disable Policy	16
Additional information	16
Aggregation Best Practices	16
Supported Aggregation Filters	17
Account Status Mapping	18
Delta Aggregation	19
Troubleshooting	19

Overview

IdentityIQ for Okta is an enterprise-level solution for centrally storing and managing user profiles and identity data. IdentityIQ for Okta enables single sign-on authentication across multiple applications and devices - even when they are behind firewalls or in the cloud and makes it easier for IT personnel to access essential employee information.

IdentityIQ for Okta manages Users, Groups, Roles and Application using Rest API provided by Okta. In IdentityIQ Okta users are managed as accounts and groups, roles and applications are managed as entitlement.

Supported features

The IdentityIQ for Okta supports the following features:

- Account Management
 - Manage Okta Person as Account
 - Create, Update, Delete
 - Enable, Disable, Unlock
 - Change Password, Refresh Accounts
 - Aggregation, Partitioning Aggregation, Delta Aggregation, Filter condition for Aggregation

Note: For more information on Delta Aggregation, see "Delta Aggregation" on page 19.
 - Add/Remove Groups, Roles and Applications
 - Discover Schema, Pass Through Authentication

Configuration parameters

- Account-Group Management
 - Aggregation, Refresh Group
 - Create, Update, Delete Groups
 - Manages Okta Groups and Applications as Account-Groups
- Custom Attributes
 - Support for aggregation
 - Support for provisioning

Note: For more information on provisioning, see "Create Account Policy" on page 15.

Pre-requisite

- An administrative user must be granted an Okta API token for authentication purposes.
To generate an Okta API token, perform the steps mentioned below:
 - a. Log in to Okta organization as a user with super administrator privileges. API tokens have the same permissions as the user who creates them, and if the user permissions change, the API token permissions also change.
 - b. On the Developer Console, select **Tokens** from the **API menu**.
 - c. On the Administrator's UI (Classic UI), select **API** from the **Security menu**, and select **Tokens**.
 - d. Click **Create Token** and provide a name for the token.
 - e. Note the created API Token.

Note: Okta API tokens generated from the above steps are valid for 30 days and automatically would be refreshed with each API call. Tokens that are not used for 30 days would expire.

- By default, connector account aggregation supports Okta's **List Users with Filter** feature.
For aggregation with Okta's **List Users with Search** feature, ensure that the following entry key is added in the application xml file:

```
<entry key="ListUsersWithSearch" value="true" />
```

Note: The **List Users with Search** parameter now searches for users based on the properties specified in the search parameter (case insensitive). This operation supports pagination (to a maximum of 50000 results).

Configuration parameters

This section contains the information that the connector uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for Okta uses the following connection parameters:

Attributes	Description
Okta Connection Settings	
URL*	The host URL of Okta instance.
API Token*	SSWS API token required for Okta authentication.

Attributes	Description
Page Size	The maximum size of each data set when querying large number of objects. Minimum value is 1 and maximum value is 200. Default: 200
Aggregation Filter Settings	
Filter Condition for Accounts	Optional condition to bring subset of Accounts during aggregation. For example, status eq "ACTIVE" Note: For more information on the Aggregation Filters supported on the managed system, see "Supported Aggregation Filters" on page 17.
Filter Condition for Groups	Optional condition to bring subset of Groups during aggregation. By default the value is set as follows: type eq "BUILT_IN" or type eq "OKTA_GROUP" Note: For more information on the Group Aggregation Filters supported on the managed system, see "Supported Aggregation Filters" on page 17.
Filter Condition for Applications	Optional condition to bring subset of Applications during aggregation. For example, status eq "ACTIVE"

Note: Attributes marked with * sign are the mandatory attributes.

Additional configuration parameters

To change the default values, add the following parameters in the application debug page:

Attributes	Description
groupsPageSize	Sets the maximum size of each data set when querying large number of Groups by adding the entry key as follows: <entry key="groupsPageSize" value="10000" /> Default value of 10000 can be changed.
logsPageSize	Sets the maximum size of each data set when querying large number of Logs by adding the entry key as follows: <entry key="logsPageSize" value="1000" /> Default value of 1000 can be changed.
appsPageSize	Sets the maximum size of each data set when querying large number of Applications by adding the entry key as follows: <entry key="appsPageSize" value="200" /> Default value of 200 can be changed.

Schema attributes

Attributes	Description
applicationSkinnyUsers	<i>(Applicable only for caching approach of account partitioning aggregation)</i> Enables skinny_user endpoint to bring applications connected to user in Okta connector by adding the entry key as follows: <code><entry key="applicationSkinnyUsers" value="true"/></code> Default value is false.
groupSkinnyUsers	<i>(Applicable only for caching approach of account partitioning aggregation)</i> Enables skinny_user endpoint to bring groups connected to user in Okta connector by adding the entry key as follows: <code><entry key="groupSkinnyUsers" value="true"/></code> Default value is false.

Schema attributes

This section describes the different schema attributes.

Account attributes

The following table lists the account attributes:

Name	Description
id	Unique key for user.
login	Unique identifier for the user (username).
email	Primary address of the user.
secondEmail	Secondary email address of user typically used for account recovery.
firstName	First name of the user.
lastName	Last name of the user.
middleName	Middle name(s) of the user(s).
displayName	Name of the user, suitable for display to end users.
nickName	Casual way to address the user in real life.
title	User's title, such as 'Vice President'
honorificPrefix	Honorific prefix(es) of the user, or title in most western languages.
honorificSuffix	Honorific suffix(es) of the user.
profileUrl	URL of user's Online profile. For example, a web page.
primaryPhone	Primary phone number of user such as home number.
mobilePhone	Mobile phone number of user.
streetAddress	Full street address component of user's address

Name	Description
city	City or locality component of user's address.
state	State or region component of user's address.
zipCode	Zipcode or postal code component of user's address.
countryCode	Country name component of user's address.
postalAddress	Mailing address component of user's address.
preferredLanguage	User's preferred written or spoken languages.
locale	User's default location for purposes of localizing items such as currency, date time format, numerical representations, and so on.
timezone	User's time zone.
userType	Used to identify the organization to user relationship such as 'Employee' or 'Contractor'.
employeeNumber	Organization or company assigned unique identifier for the user.
costCenter	Name of cost center assigned to the user.
organization	Name of user's organization.
division	Name of user's division.
department	Name of user's department.
manager	Display name of the user's manager.
managerId	ID of a user's manager.
status	Status of the user. For example, ACTIVE, PROVISIONED, DEPROVISIONED and so on.
created	Timestamp of user creation.
activated	Timestamp when transition to ACTIVE status completed.
statusChanged	Timestamp when status last changed.
lastUpdated	Timestamp when user was last updated.
lastLogin	Timestamp of last login.
passwordChanged	Timestamp when password was last changed.
groups	Groups assigned to the user.
applications	Applications assigned to the user.
roles	Administrator roles assigned to the user.

Note: Custom attributes of User profile from Okta can be populated using the Discover Schema functionality.

Group attributes

The following table lists the group attributes:

Provisioning Policy attributes

Name	Description
groupId	Unique key for group.
name	Name of the group.
created	Timestamp when group was created.
description	Description of the group.
lastMembershipUpdated	Timestamp when group's memberships were last updated.
type	Determines how a group's profile and memberships are managed.
lastUpdated	Timestamp when group's profile was last updated.
objectClass	Determines the group's profile.
applications	Applications assigned to group.

Application attributes

The following table lists the application attributes:

Name	Description
applicationId	Unique key for application.
name	Unique key for application definition.
label	Unique user-defined display name for application.
created	Timestamp when application was created.
status	Status of application.
signOnMode	Authentication mode of application.
features	Enabled application features.
lastUpdated	Timestamp when application was last updated.

Provisioning Policy attributes

This section lists different policy attributes for IdentityIQ for Okta.

Note: The attributes marked with * sign are required attributes.

Create Account Policy

Following table describes various attributes in the create account policy.

Attribute	Description
FirstName*	First name of the user.
LastName*	Last name of the user.
Email*	Primary address of the user.
Login*	Must be an email.
Activate	Checked to set the status as provisioned, unchecked to set status as staged.
Password	Login password for the user.

To provision custom attributes, add a similar attribute in the provisioning policy.

For example, if there are custom attributes **customAttr1** and **customAttr2** on Okta and provisioning is required for them, in that case the provisioning plan must contain attributes with the same names that is, **customAttr1** and **customAttr2**.

Following table describes the status of created account according to different parameters provided in create account policy above.

Activate checkbox	Password	Okta Status	IdentityIQ Status
Unchecked	Provided/Not Provided	STAGED	Disabled
Checked	Not Provided	PROVISIONED	Enabled
Checked	Provided	PASSWORD_RESET	Enabled

Create Group Policy

Following table describes various attributes in the create group policy.

Attribute	Description
Group Name*	Name of the group.
Group Description	Description of the group.

Disable Policy

Following table describes various attributes in the disable policy.

Attribute	Value	Description
Status*	Suspend	Temporarily disables the account.
	Deprovision	Delete all the applications and deactivate the account.

For more information on the various mapped status of Okta and IdentityIQ, see "Account Status Mapping" on page 18.

Additional information

This section describes the additional information related to the IdentityIQ for Okta.

Aggregation Best Practices

Aggregation with Partitioning approach is implemented using the following alternatives to cater to different system configurations:

- **Caching:** works best when the number of connected entitlements are large.
- **Sequential:** works best when there are large number of accounts having less number of connected entitlements with an ability to execute multiple partitions in parallel.

For a better performance outcome, the IdentityIQ for Okta works by creating an application and group cache as explained in the following steps:

1. IdentityIQ for Okta creates cache of user connected to groups.
2. IdentityIQ for Okta creates cache of user connected to applications.
3. IdentityIQ for Okta then fetches the user profiles.
4. IdentityIQ for Okta maps the groups and applications of the fetched user profiles to the caches created during steps 1 and 2 above.

The above approach works best in environments having less number of connections (users to groups and/or application). The problem arises when the groups and applications connections are high. Due to API limitations the cache creation takes a longer time than expected.

To resolve this an alternative approach called as sequential approach is used in the connector. In this approach, the connector first fetches the user profiles followed by groups and applications. The sequential approach can be enabled by configuring the following parameters in the application debug page:

- To skip creation of application cache:

```
<entry key="noAppCaching">
  <value>
    <Boolean>true</Boolean>
  </value>
</entry>
```

- To skip creation of group cache:

```
<entry key="noGroupCaching">
  <value>
    <Boolean>true</Boolean>
  </value>
</entry>
```

Supported Aggregation Filters

Based on added Accounts/Groups Aggregation Filter, only respective accounts/groups are aggregated in IdentityIQ.

Account Aggregation Filters

For example, if the added filter is **status eq "STAGED"** then only staged account must be aggregated in IdentityIQ.

Aggregation Filters	Description
status eq "STAGED"	Users that have a status of STAGED.
status eq "PROVISIONED"	Users that have a status of PROVISIONED.
status eq "ACTIVE"	Users that have a status of ACTIVE.
status eq "RECOVERY"	Users that have a status of RECOVERY.
status eq "PASSWORD_EXPIRED"	Users that have a status of PASSWORD_EXPIRED.
status eq "LOCKED_OUT"	Users that have a status of LOCKED_OUT.
status eq "DEPROVISIONED"	Users that have a status of DEPROVISIONED.
lastUpdated lt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Users last updated before a specific timestamp.
lastUpdated eq "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Users last updated at a specific timestamp.
lastUpdated gt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Users last updated after a specific timestamp.
id eq "00u1ero7vZFVEIYLWPBN"	Users with a specified id.
profile.login eq "login@example.com"	Users with a specified login.
profile.email eq "email@example.com"	Users with a specified email*.
profile.firstName eq "John"	Users with a specified firstName*.
profile.lastName eq "Smith"	Users with a specified lastName*.
profile.Custom_Integer_Array eq "23"	Users with a specified array attribute*.
profile.Custom_String eq "Custom Value for String_Updated"	Users with a specified custom attribute*.

Group Aggregation Filters

By default group Aggregation filter would aggregate **type eq "OKTA_GROUP"** or **type eq "BUILD_IN"** groups.

Additional information

Aggregation Filters	Description
type eq "OKTA_GROUP"	Groups that have a type of OKTA_GROUP
type eq "APP_GROUP"	Groups that have a type of APP_GROUP
type eq "BUILT_IN"	Groups that have a type of BUILT_IN
lastUpdated lt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with profile last updated before a specific timestamp
lastUpdated eq "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with profile last updated at a specific timestamp
lastUpdated gt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with profile last updated after a specific timestamp
lastMembershipUpdated lt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with memberships last updated before a specific timestamp
lastMembershipUpdated eq "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with memberships last updated at a specific timestamp
lastMembershipUpdated gt "yyyy-MM-dd'T'HH:mm:ss.SSSZ"	Groups with memberships last updated after a specific timestamp
id eq "00g1emaKYZTWRYYRRTSK"	Group with a specified id

Account Status Mapping

Following table lists the mapped status of Okta on IdentityIQ:

Okta Account Status	IdentityIQ Account Status
PROVISIONED	Active
PASSWORD_EXPIRED	
ACTIVE	
RECOVERY	
DEPROVISIONED	Disable
SUSPEND	
STAGED	
LOCKED_OUT	Locked

Upgrade considerations

For applications created before applying 7.3 Patch 3, application definition would have an entry for Events API. After upgrading IdentityIQ version 7.3 Patch 3, users must manually remove the Events API entry.

Delta Aggregation

The IdentityIQ for Okta supports only account delta aggregation. On Full Aggregation, the respective timestamp of account aggregation is stored in the Application object which is used by Delta Aggregation to retrieve the changed data into IdentityIQ. This timestamp is updated after each account delta aggregation.

In account delta aggregation changes to user profile attributes and their entitlements are populated.

The delta for Okta user profile attributes are populated from the users API by comparing the timestamp of last successful account aggregation against the last updated attribute.

To detect entitlement changes and deleted users, the data is populated from logs API by comparing the timestamp of last successful account aggregation against the published attribute.

Note: Log data older than 90 days is not returned, in accordance with Okta's Data Retention Policy. This means, that any data change done prior to 90 days of the last successful account aggregation timestamp, would not be captured and a full account aggregation would be required.

For all delta aggregations after applying 7.3 Patch 3, logs API would be considered regardless of application definition.

Troubleshooting

1 - Issues in Delta Aggregation

Following are the various scenarios where data is not populated in Delta Aggregation:

- Roles assigned to account from API are not populated in delta aggregation
- Sometimes applications which are removed from users are not aggregated in account delta aggregation

Resolution: Perform full account aggregation task.

- Sometimes groups which are deleted from managed system are not captured in account delta aggregation

Resolution: Perform full group aggregation to refresh entitlements.

- For account created with only Default group **Everyone** event system logs are not captured.

Resolution: To see the Default group assigned to account, perform full account aggregation or create account with other group so that in delta aggregation for account, both groups details (default and other group) are aggregated.

2 - For Unlocked Okta account from IdentityIQ, account details page does not display correct status

In IdentityIQ, managed account refresh action only affects the status of the account in IdentityIQ. Account Details are not changed and **Status** is one of the account attribute.

Resolution: To get the correct account details and value of the **Account status**, execute account aggregation task.

3 - Create Account fails for account created with group assigned as 'Everyone'

By default, on Okta managed system the group 'Everyone' gets assigned to every account created. Create account would fail with following error message is displayed:

Troubleshooting

```
sailpoint.connector.ConnectorException: [ConnectorException] [Error details] Request execution failed. HTTP Error code: 501, Okta Error code: E0000060, errorSummary: Unsupported operation., errorCauses:[].
```

Resolution: While performing create account with **Manage user access** select the group type other than **Everyone**.

4 - Account Aggregation fails with an error message

Account Aggregation fails with the following error message:

```
Exception during aggregation of Object Type account on Application Okta. Reason: Unable to create iterator sailpoint.connector.InsufficientPermissionException: [InsufficientPermissionException]
```

```
[Possible suggestions] Furnish appropriate permission to the Okta API token owner.
```

```
[Error details] Insufficient privileges detected. HTTP Error code: 401, Okta Error code: E0000015, errorSummary: You do not have permission to access the feature you are requesting
```

Resolution:

- Ensure that correct permission/roles are assigned to the API Owner (the user whose api token is getting used in Okta application). The API Owner must have SUPER ADMIN roles assigned to him for aggregation.

Note: To aggregate Okta roles, SUPER_ADMIN role is required.

- The **List Users with Search** parameter supports pagination (to a maximum of 50000 results).
- For aggregation with Okta's **List Users with Search** feature, ensure that the following entry key is added in the application xml file:

```
<entry key="ListUsersWithSearch" value="true"/>
```

Note: The **List Users with Search** parameter is moved to **General Availability (GA)**. This operation supports pagination (to a maximum of 50000 results).

5 - Account Preview does not work/displays any data on Okta application page

If the IdentityIQ for Okta is having huge number of user to group/user to application connection, the account preview functionality would not work as it takes more time to get data from Okta.

Resolution: To verify Okta accounts run the account aggregation task instead of Account Preview. For more information on best practices of Okta account aggregation, see "Aggregation Best Practices" on page 16.

6 - While performing Account Aggregation warnings are displayed in the logs

While performing account aggregation the following warnings are displayed in the logs:

```
2019-04-18 18:43:25,708 WARN Thread-743
openconnector.connector.okta.OktaConnector:5425 - API rate limit exceeded for
endpoint, Retrying the failed request now
```

```
2019-04-18 18:43:25,709 WARN Thread-742
openconnector.connector.okta.OktaConnector:5425 - API rate limit exceeded for
endpoint, Retrying the failed request now
```

Resolution: If required warnings can be ignored. But to improve Okta aggregation performance, increase Okta API rate limit.

Security Information And Event Management Infrastructure Modules

This section contains information on the following section:

- “IdentityIQ for ArcSight IT Security”

Chapter 3: IdentityIQ for ArcSight IT Security

The following topics are discussed in this chapter:

Overview	23
Supported features	24
Supported platform	24
Pre-requisites	24
Configuration	24
Configuration to export IdentityIQ Data to ArcSight	24
Configuration to Import HP ArcSight CEF Flat File to SailPoint IdentityIQ	28

Overview

ArcSight IT Security Information and Event Management Infrastructure Module (SEIM) is a Universal log management solution that helps enterprises identify and prioritize current and potential security threats. SailPoint IdentityIQ collects the security event information such as Audit information. The SailPoint IdentityIQ integration with ArcSight IT Security allows both end systems to take remediation action in case of security threats.

IdentityIQ integration with ArcSight enables the following scenarios:

1. IdentityIQ data (Identity, Account, Audit, and Syslog) stored in IdentityIQ can be exported to ArcSight. ArcSight administrator can store this data in an ArcSight Active List. IdentityIQ data can be exported to ArcSight for correlation, such as successful provisioning of privileged accounts, password changes, login failure and so on. For more information on ways to export data, see “Export from IdentityIQ to ArcSight” point in “Supported features” section.
2. IdentityIQ can import filtered activity event data from ArcSight; based on which activity-based remediation processing can be triggered. Event records are expected in standard ArcSight Common Event Format (CEF). Events received are matched with users held within the IdentityIQ warehouse, and used to trigger activity policies when certain types of event are recognized. These triggers result in a business process being executed which generates a full re-certification for the affected user, and also causes a re-calculation of the user's risk score and update of risk reports and dashboard content to highlight the activity.

Note: Creating an ArcSight Active Channel or Active List is outside the scope of this document. This document assumes the ArcSight administrator is familiar with steps to create an ArcSight Active Channel or Active List. It provides the IdentityIQ information an ArcSight administrator will require to create an ArcSight Active Channel or Active List.

Common Event Format (CEF)

CEF is an extensible, text-based, high-performance format designed to support multiple device types in the simplest manner possible. CEF defines syntax for log records comprised of a standard header and a variable extension, formatted as key-value pairs. CEF uses syslog as a transport mechanism and the following format, comprised of a syslog prefix, a header and an extension, as shown below:

For example,

Supported features

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device  
Version|Signature ID|Name|Severity|[Extension]  
  
Dec 19 08:31:10 host CEF:0|Security|threatmanager|1.0|101|out of hours workstation  
login|10|suser=hbutler src=activedirectorydomain ip=10.1.76.224
```

Supported features

- **Export from IdentityIQ to ArcSight:** The IdentityIQ data can be exported in:
 - **Flat file in CEF:** Using Advanced Analytics we can export Identity, Account, Audit and Syslog data in CEF.
 - **Database tables:** The **ArcSight Data Export** task enables you to export Identity (which includes account and identity data) and Audit data to external tables.
- **Import into IdentityIQ from ArcSight:** This integration supports including event logging data from ArcSight and associate it to Identities in IdentityIQ so that potential policy violations can be triggered or provide greater visibility as part of access reviews as to any suspicious or error prone access a user may have.

Supported platform

IdentityIQ for ArcSight IT Security supports the HP ArcSight Enterprise Security Manager version 6.9.

Pre-requisites

(Applicable for import of ArcSight Events into SailPoint IdentityIQ) At least one application must be configured in SailPoint IdentityIQ and Users/Groups aggregated into SailPoint IdentityIQ system.

Note: Users present in HP ArcSight must also be present in SailPoint IdentityIQ.

Configuration

This section describes the general, operation specific configurations and the steps that must be performed to configure the IdentityIQ for ArcSight IT Security.

Configuration to export IdentityIQ Data to ArcSight

The Identity, Account and Audit information from SailPoint IdentityIQ can be exported to ArcSight using CEF flat file or database:

1. Export data from SailPoint IdentityIQ to ArcSight tables.
2. Export data from SailPoint IdentityIQ to Flat file in Common Event Format.

Export Data from SailPoint IdentityIQ to ArcSight tables

The **ArcSight Data Export** task enables you to export Identity and Audit data to external tables. You can select to export Identity information and Audit events from IdentityIQ Database.

Create the export databases on your destination data source before using the ArcSight Data Export task.

1. Navigate to **Monitor => Tasks**.
2. Create a new ArcSight Data export task.
3. Provide the Data Source Parameters.

ArcSight Data Export options are:

Options	Description
Datasource Parameters	
Database	Select a database type from the drop-down list.
User Name	Enter the user name parameter of the database.
Password	Enter the password of the database.
Driver Class	Enter the driver class used for the database.
URL	Enter the URL of the database.

4. Click on **Generate table Creation SQL** to generate table's schema and create database that includes export tables which you can hand off to a database administrator for execution.
The task adds the following tables in database:

Tables	Description
sptr_arcsight_export	Table to maintain the task execution history.
sptr_arcsight_identity	Table contains exported data of Identity.
sptr_arcsight_audit_event	Table contains Audit Events information.

5. Select **Object Export** options.
The **Object Export** options are:

Options	Description
Export Identities	<p>Select the check box to export Identity related data in ArcSight tables. It provides the following options:</p> <ul style="list-style-type: none"> • Full: Exports all the records irrespective if they were exported earlier. • Incremental: Exports only records that are updated since last run of this task. This option can even be selected when running the task for first time. When the task is running for first time, this option exports all records similar to the Full option.

Configuration

Options	Description
Export Audits	Select the check box to export Audit Events in ArcSight table. It provides the following options: <ul style="list-style-type: none">• Full: Exports all the records irrespective if they were exported earlier.• Incremental: Exports only records that are updated since last run of this task. This option can even be selected when running the task for first time. When the task is running for first time, this option exports all records similar to the Full option.

6. After completing the customizing report options, click **Save** for later use or **Save and Execute** to save the report and run it immediately.

Configuring HP ArcSight Task to populate host name or IP

The value of column `application_host` can be populated by adding a map **arcsightAppNameHostMap**. Adding the **arcsightAppNameHostMap** map the administrator configuring this integration can define the hostname (or IP address) which must be used for an Account. It is recommended this hostname (or IP address) is same as the configured in the ArcSight configuration.

The **arcsightAppNameHostMap** map must be defined in the **ArcSight Data Export** Task created above. The key in the map should be name of the application defined in IdentityIQ and value should be hostname, IP, or any string that ArcSight administrator understands.

1. To add the map, navigate to debug page, navigate to TaskDefinition and open the ArcSight task configured above.
2. Add the entry as key = Name of Application defined in IdentityIQ and value as the string to identify host of Account like Hostname or IP.
3. Save the task definition.

For example:

```
<entry key="arcsightAppNameHostMap">
  <value>
    <Map>
      <entry key="LinuxApp1" value="linux01.sailpoint.com"/>
      <entry key="LinuxApp2" value="127.15.19.21"/>
      <entry key="ADDirectApp" value="AD.sailpoint.com"/>
      <entry key="ServiceNowApp" value="https://sailpoint.service-now.com"/>
      <entry key="ACF2App" value="ACF2-Mainframe"/>
    </Map>
  </value>
</entry>
```

Note: If the application name is not defined in the map the host field will be blank.

As mentioned above, this document provides the information an ArcSight administrator requires to create an ArcSight Active List or Active Channel. The information below provides the same. Following fields are added in export table:

Table 1—IdentityIQ spt_arsight_identity export table

Fields	Description
linkid	Primary key for Link table in IdentityIQ database. This field will be copied from spt_link table id field. This will be the primary key for export table.
identityid	Primary key in Identity table. This field will be copied from spt_identity table.
modified_dt	Populates timestamp when the record will be exported in export table. The field can be referred while configuring time based ArcSight database connector.
identity_display_name	Represents Display Name of Identity which will be copied from spt_identity table field (display_name).
identity_firstname	Represents first name of Identity which will be copied from spt_identity table field (firstname).
identity_lastname	Represents last name of Identity which will be copied from spt_identity table field (lastname).
application_type	Populates the type of Account which is connected to the Identity like ActiveDirectory – Direct, ACF2 – Full, Box, Cloud Gateway, ServiceNow and so on.
application_host	The host name, IP, or any string which can be used by ArcSight administrator to identify the host of link/account uniquely. Customer can enter any string which can be sent to ArcSight to identify the host of link. This field can be populated as explained in “Configuring HP ArcSight Task to populate host name or IP” on page 26.
application_name	Populates the name of Application of the Account connected to the Identity.
link_display_name	The account connected to the identity which will be copied from spt_link table, field display_name.
entitlements	Represents comma separated list of entitlements to the link of Identity.
risk_score	Represents the composite risk score of Identity.

Table 2—IdentityIQ spt_arsight_audit_event export table

Fields	Description
auditid	The audit ID which is primary key for the export Audit table. The field will be copied from spt_audit_event table id field.
created_dt	Populates timestamp when the record will be exported in export table. The field can be referred while configuring time based ArcSight database connector.
owner	Describes the Owner of the audit generated.
source	Provides more details to help ArcSight administrator determine the source of audit.
action	Describes the action taken on entity.
target	Provides target details.

Table 2—IdentityIQ sptr_arcsight_audit_event export table

Fields	Description
application	Describes the name of application the target belongs to.
account_name	The name of Account is populated in this field.
attribute_name	The name of attribute modified.
attribute_value	The value provided to the attribute.

Export Data from SailPoint IdentityIQ to Flat file

1. Navigate to **Analyze => Advanced Analytics**.
2. Navigate to Identity Search/ Audit Search/Account Search Tab.
3. Select the Search Criteria and Fields to display.
4. Click on **Run Search**.
5. Click on **CEF Flat file** export button to export search results to file in CEF.
The Search Results page have the following options to save:
 - **Save Search:** It is used to save the search criteria and fields to display.
 - **Save Search as Report:** These type of reports can be accessed as a report, as schedules or for execution by performing the procedure:
 - a. Navigate to **Analyze => Reports**.
 - b. Right click on the report and schedule or execute the report.
 - c. Navigate to Report Results tab to see the report result.
 - d. Click on the **Report**.
 - e. Click on the **CEF Flat file** export button to export the report to file in CEF.

This will generate a file with data in CEF which can be used by ArcSight to import events in ArcSight ESM.

Note: For more information on Advanced Analytics, see *SailPoint IdentityIQ User Guide*.

Configuration to Import HP ArcSight CEF Flat File to SailPoint IdentityIQ

1. Access the Application Configuration Console.
2. Navigate to Schema tab.
Mark the field as correlation key for which you want to correlate activity from HP ArcSight to SailPoint IdentityIQ.
For Example: sAMAccountName for Active Directory application.
3. Navigate to Activity Data Sources tab.
Note: For more information on Activity Data Source, see *SailPoint IdentityIQ Administration Guide*.
4. Click on **Add** to add new Activity Data Source.
5. Select Activity Data source Type as **CEF Log File**. The default Transformation rule and Correlation rule will be automatically selected.
Note: You can change the value of `cefLinkAttribute` in correlation rule to set correlation key as per application.

6. Navigate to Transport Settings tab, select the Transport Type as local, ftp or scp.
 7. Navigate to Log File Settings tab and in the File name provide the exact path of the CEF Flat file. For example, C:\ArcSight\activedirectory.csv
 8. Click on **Save** button to save activity data source configuration.
 9. Click on **Save** button to save the application.
If the correlation key is not marked and aggregation of account for that application is already performed, then perform the following:
 - Access the Application Configuration console.
 - Navigate to the Correlation tab.
 - Click on **New** button to create a new Account Correlation.
 - Click on next button and provide the name of the configuration.
 - Select the Application Attributes and Identity Attributes and click on **Add** button.
 - Click on **Save**.
 - Click on **Save** to save the application.

After the correlation configuration is done, execute the account aggregation (with optimization turned off to pick up the existing accounts) again.
 10. Navigate to **Define => Identities**.
 11. Click on the identity for which you want to enable Activity monitoring and import data from ArcSight.
 12. Navigate to Activity Tab.
 13. Select the **Activity Monitoring** checkbox.
 14. Save the Identity.
 15. Navigate to **Monitor => Tasks**.
 16. Create a new Activity Aggregation Task.
 17. Select an activity data source which is configured above in Step 8.
 18. Save and execute the task.
 - To see the result of the task executed in previous step navigate to Task Results tab and click on the task.
 - To see the correlated events navigate to **Define => Identities**. Select the identity for which you have correlated the event. Navigate to Activity Tab. Check the Recent Activities section.
- Note:** After correlating the HP ArcSight event to Identity, the Policy Violation and Certification can be created and used to notify for any activity for that identity using the workflow.

IT Service Management Infrastructure Modules

The Service Management Infrastructure Module helps to perform effective and efficient service management for IdentityIQ services offered to the organization in the ServiceNow Catalog and Service Desk. The information contained within the Service Catalog and Service Desk relates to all IdentityIQ services provided by the IT department to the Business. The IdentityIQ services are purely Role based access that can be requested or revoked through Service Catalog and Service Desk. This integration is simple to configure and fast to deploy, so organizations can go live quickly with confidence, while scaling to an organization's business needs.

This section contains information on the following sections:

- "IdentityIQ for ServiceNow Service Desk"
- "IdentityIQ for MicroFocus Service Manager Service Desk"
- "IdentityIQ for BMC Remedy Service Desk"
- "IdentityIQ for ServiceNow Catalog"

SailPoint Service Catalog Integration is an integration between ServiceNow and SailPoint IdentityIQ. This allows users of both systems to easily navigate from ServiceNow into IdentityIQ, and gives users a "one stop shop" to request all IT related items.

- "IdentityIQ for ServiceNow Catalog API"

SailPoint ServiceNow Service Catalog API Integration is an integration between ServiceNow and SailPoint IdentityIQ. This integration allows access request for roles using Service Catalog approach with ServiceNow UI experience.

Chapter 4: IdentityIQ for ServiceNow Service Desk

The following topics are discussed in this chapter:

Overview	33
Supported features	33
Supported platforms	33
Pre-requisites	34
Service Request	34
Incident and Change Request	34
Basic configuration	35
Basic flow of Service Request	37
Basic configuration of Service Request.	37
Configuring IdentityIQ to integrate with ServiceNow.	38
IntegrationConfig XML files for Service Request, Incident and Change Request	41
Configuration procedure	42
Verifying connectivity between IdentityIQ and ServiceNow	44
Retryable mechanism	44
Sample scenario	45
Troubleshooting	46

Overview

The integration between SailPoint and ServiceNow enables customers to create service requests, incidents, and change requests in ServiceNow for the configured operations (for example, creating account, removing/deleting access and other operations) for the configured application. The seamless integration of SailPoint and IdentityIQ for ServiceNow Service Desk eliminates the need to build and maintain a custom integration, and reduces time-to-deployment.

Supported features

IdentityIQ for ServiceNow Service Desk supports the following features:

- Creating ticket for all provisioning operations
- Syncing ticket status between the two systems
- Retry Mechanism for Create Ticket request failure

Supported platforms

IdentityIQ for ServiceNow Service Desk supports the following ServiceNow releases:

- Madrid
- London
- Kingston

Pre-requisites

Ensure that the pre-requisites for Service Request, Incident and Change Request specified in this section are performed.

Service Request

- ServiceNow Instance must be up and running.
The IdentityIQ for ServiceNow Service Desk Administrator must be assigned the `x_sap_iiq_sim.admin` role.
- Apply the IdentityIQ for ServiceNow Service Desk update set:
 - Copy the relevant update set from the following directory to a temporary directory:


```
identityiq-releaseVersion.zip\integration\servicenow\iiqIntegration-ServiceNow.zip\ServiceIntegrationModuleUpdateSet
```

 In the above directory, *releaseVersion* is the version of the current IdentityIQ release.

ServiceNow release	Update Sets
Kingston or Later	IdentityIQServiceNowServiceIntegrationModule.v2.1.4.xml SailPointServiceRequestGenerator.v1.1.xml

- Import the above mentioned update set in ServiceNow instance. For more information and guidelines on usage of the update set, refer to the following wiki link:
<http://wiki.servicenow.com/>
- Create the following ACLs in Global scope to view the application logs:

Name	Type	Operation	Active	Required Roles
App Log Entry[syslog_app_scope]	record	read	true	x_sap_iiq_sim.admin

For more information on the procedure for creating the ACL, see the following link:

http://wiki.servicenow.com/index.php?title=Using_Access_Control_Rules#Creating_ACL_Rules

- ServiceNow Integration provides `ServiceNowServiceIntegrationModule.xml` file located in `iiqHome/WEB-INF/config/` directory.

Incident and Change Request

- ServiceNow Instance must be up and running.
The IdentityIQ for ServiceNow Service Desk Administrator must be assigned the `x_sapo_iiq_sim.admin` role.
- Apply the IdentityIQ for ServiceNow Service Desk update set:
 - Copy the relevant update set from the following directory to a temporary directory:


```
identityiq-releaseVersion.zip\integration\servicenow\iiqIntegration-ServiceNow.zip\ServiceIntegrationModuleUpdateSet
```

 In the above directory, *releaseVersion* is the version of the current IdentityIQ release.

ServiceNow release	Update Sets
Kingston or Later	IdentityIQServiceNowServiceIntegrationModuleForIncidentAndChange.v1.4.xml

- b. Import the above mentioned update set in ServiceNow instance. For more information and guidelines on usage of the update set, refer to the following wiki link:
<http://wiki.servicenow.com/>
- Ensure that **ServiceNowIntegrationExecutor** is being called: ServiceNowIntegrationExecutor class is responsible for creating and sending SOAP requests to ServiceNow. You can add a simple `System.out.println` statement in ServiceNowServiceIntegration rule to ensure that this is being called when a provisioning request is submitted for this integration.
- ServiceNow Integration provides ServiceNowSIMForIncidentAndChange.xml file located in `iiqHome/WEB-INF/config/` directory.

When integrating with the following service operations, open and modify the respective sections in the above files and import in IdentityIQ:

- for Incident: #INCIDENT

For Kingston or later uncomment the following entry in the statusMap:

```
<entry key='8' value='failure' />
```

- for Change Request: #CHANGE REQUEST
 - a. For Kingston or later, replace `<state>1</state>` with `<state>-5</state>` in the soap-message.
 - b. For Kingston or later, replace the statusMap with the following:


```
<entry key='statusMap'>
  <value>
    <Map>
      <entry key='-5' value='inProcess' />
      <entry key='-4' value='inProcess' />
      <entry key='-3' value='inProcess' />
      <entry key='-2' value='inProcess' />
      <entry key='-1' value='inProcess' />
      <entry key='0' value='inProcess' />
      <entry key='3' value='committed' />
      <entry key='4' value='failure' />
    </Map>
  </value>
</entry>
```

For more information, see “Configuring IdentityIQ to integrate with ServiceNow” on page 38.

Note: If the field is a reference field and the reference value is other than those available, then ServiceNow implicitly creates those reference records. If you do not want to allow creation of reference records, then set Choice action to ignore in the transform map for the reference field.

Basic configuration

The integrated solution speeds the detection and remediation of identity management issues that increase the risk of compliance violations or security breaches, such as orphaned accounts, policy violations, and inappropriate access privileges. Organizations can take advantage of a centralized approach spanning thousands

Basic configuration

of users and hundreds of resources to strengthen IT controls and provide proof of compliance to auditors and executive management. The seamless integration of SailPoint and ServiceNow eliminates the need to build and maintain a custom integration, and speeds time-to-deployment.

For any IT resources managed by ServiceNow Service Desk, IdentityIQ automatically creates a trouble ticket within ServiceNow Service Desk, passing along all relevant identity data and reviewer comments to populate the ticket.

To ensure revocation requests get delivered and implemented, IdentityIQ manages all remediation and revocation requests within a guaranteed delivery model.

To determine the status of user accounts, IdentityIQ performs closed-loop audits on remediation requests and compares the actual state of user privileges with the original change request. If the request is still open, an alert will be sent to the reviewer for prompt action and closure.

The integration itself has been designed to be quick to install and easy to use. It makes use of Web Services for communications between the SailPoint server and the ServiceNow. On the backside of a user recertification, policy remediation action or access request action, the IdentityIQ server will direct provisioning and service desk requests to the configured implementers. Based on the `IntegrationConfig` configured for each target application, service desk request are issues to a given remediation/implementation point. Once the `IntegrationConfig` file for ServiceNow has been loaded into the IdentityIQ server, all change/remediation actions result in the creation of new service desk request as shown in Figure 1—Basic configuration.

The IdentityIQ for ServiceNow Service Desk generates tickets for provisioning requests. These tickets generate service requests on `sc_request` and `sc_req_item` table, incidents on `incident` table, or change requests on the `change_request` table. The module fetches the status of ticket by using the direct web services of target tables that is, `sc_req_item`, `incident` or `change_request` and updates the SailPoint IdentityIQ database with the status.

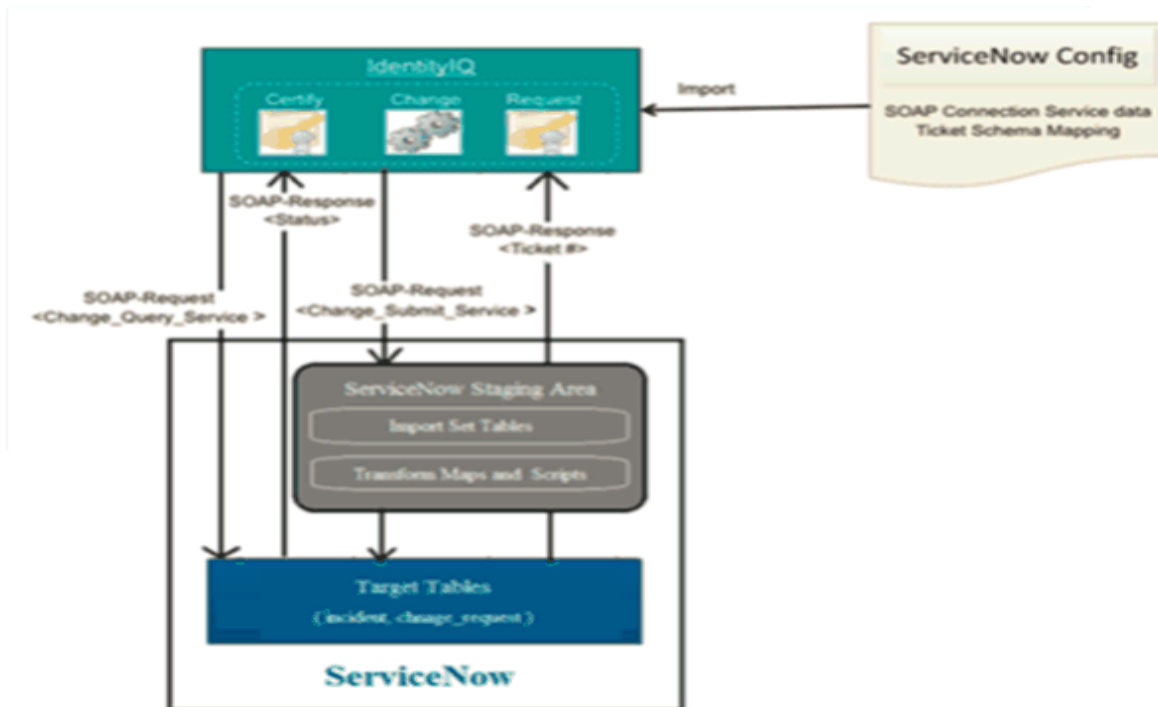


Figure 1—Basic configuration

At the completion of the change control cycle within IdentityIQ, an “Open Ticket” request is made over the appropriate SOAP channel to the ServiceNow web service. From here, tickets are opened and the new ticket number is returned to IdentityIQ. The schema for the service request is defined in the `IntegrationConfig` and allows for the flexibility to transfer complete details on the service desk request.

Basic flow of Service Request

IdentityIQ creates ticket by requesting a Catalog item on ServiceNow. Each application on IdentityIQ has a Catalog item defined on ServiceNow. IdentityIQ calls ServiceNow's Web Service requesting the Catalog Item. The Web service creates a Cart and adds the Catalog item to the cart. The Catalog item has Catalog Variables. The information is taken from the IdentityIQ's request and passed on to these Catalog Variables. The Catalog Item has a Workflow attached to it. After adding Catalog Item to the cart, Cart is submitted. Submission of cart triggers the Workflow. The workflow creates a task by passing the information from Catalog Variables to Service Request. The Requested Item ticket number is returned as the response which is later used to check the status.

Depending on the workflow configuration, the task is assigned to the user (group or individual), who then performs the action which results in change in the State of the Requested Item.

Basic configuration of Service Request

- Create Catalog items on ServiceNow for each application on IdentityIQ that user wants to manage using IdentityIQ for ServiceNow Service Desk. The name must contain “IdentityIQ” to filter and display in IdentityIQ for ServiceNow Service Desk under Catalog Items.

For more information on the procedure for creating the catalog item, see the following link:

http://wiki.servicenow.com/index.php?title=Defining_Catalog_Items

Note: Refer to the default Catalog Items provided in the update set.

- Catalog Variables must be created for each element defined in SOAP message in ServiceNow Integration Configuration file. The name of the Catalog variable must be same as the respective SOAP element in the SOAP message.

For more information on the procedure for creating the catalog variable, see the following link:

http://wiki.servicenow.com/index.php?title=Using_Service_Catalog_Variables

- Catalog variable must be created with name **tracking_id** of type **Single Line Text** for each newly created Catalog item. This field is used to update Request Item (RITM) number on the IdentityIQ Access Request items.
- The **opened_by** and **requested_for** fields receives values using the default Rule in ServiceNow Configuration file. Modify the rule as per requirement to populate the fields.

For example, see **requested_for** catalog variable in the default Catalog item (IdentityIQ Access Request).

Note: If the user is not present on ServiceNow, then ‘opened_by’ and ‘requested_for’ fields will display default ServiceNow Administrator.

- Provide the mapping between Application and Catalog item in the **catalogItem** field in ServiceNow Integration Configuration file.

For example, `<entry key="Active_Directory" value="IdentityIQ Access Request" />`
`<entry key="Procurement_System" value="IdentityIQ Access Request" />`

Note: The Catalog item name is case sensitive.

Configuring IdentityIQ to integrate with ServiceNow

- Verify the default mapping between ServiceNow's Request Item (RITM) Status field and IdentityIQ status in ServiceNow Integration Configuration file. This is used to update the status of IdentityIQ line item.
- Create and publish a workflow and attach it to the respective Catalog Item to handle the Requested Item (RITM). The name must contain "IdentityIQ" to filter and display in IdentityIQ for ServiceNow Service Desk under Workflow versions.

The workflow must be able to create a Catalog Task.

For more information on procedure for creating the workflow, see the following link:

http://wiki.servicenow.com/index.php?title=Creating_a_Workflow

Note: Refer the default workflow given in the update set. Login with the Admin user or user with 'workflow_admin' to create or update workflow.

- The default workflow, in the **Run Script** activity has a scripting logic to get values from Catalog Variables and assign to the fields of Service Request and Requested Item. Use that or modify accordingly. Configure the Workflow as per requirement.
- The **State** of Requested Item (RITM) changes when the **State** field of the Task changes due to the Workflow defined on the Catalog Item. The **Request State** on the Service Request changes due to the default 'Service Catalog Request' workflow.
- If some records or columns are not displayed with Minimum permission user, add the specific ACLs to view the records.

For more information on procedure for creating the ACL, see the following link:

http://wiki.servicenow.com/index.php?title=Using_Access_Control_Rules#Creating_ACL_Rules

- The OOTB catalog item has **req_short_description** catalog variable in the ServiceNow application and is mapped to the **Short Description** field of the Service Request ticket on the ServiceNow. To populate a different value in the Service Request description, add the following line under **<screquest>** in the **soapMessage** of the provision map (in the Integration configuration XML):
<req_short_description> </req_short_description>

Configuring IdentityIQ to integrate with ServiceNow

This section provides the required information for configuring IdentityIQ to integrate with ServiceNow.

This is intended as an introduction to the configuration needed to integrate IdentityIQ with ServiceNow. It outlines some examples that must be used as a reference point for implementation. Some changes may be required to meet specific use case and expertise around both systems are a must for the successful implementations.

SailPoint provides a default ServiceNow configuration. This configuration implements the integration between IdentityIQ and the ServiceNow to fulfill creation of tickets based on IdentityIQ access certification remediation events.

The default configuration is located in the following directory, where *iiqHome* is the location where IdentityIQ was installed:

- Service Request: *iiqHome*/WEB-INF/config/ServiceNowServiceIntegrationModule.xml
- Incident and Change Request: *iiqHome*/WEB-INF/ServiceNowSIMForIncidentAndChange.xml

This section explains the various entries that are specific for this integration. For more information of the entries in the *IntegrationConfig* file, see Appendix: A: Common Identity Management Integration Configuration.

The integration configuration must include the following entries:

- **endpoint:** URL to the web service

Endpoint task	Service operation	Kingston or Later
ServiceNow endpoint to create a ticket	Service Request	https://demo.service-now.com/ScRequestGenerator.do?SOAP
	Incident	https://demo.service-now.com/x_sapo_iiq_sim_incident.do?SOAP
	Change Request	https://demo.service-now.com/x_sapo_iiq_sim_change_request.do?SOAP
ServiceNow endpoint to get ticket status	Service Request	https://demo.service-now.com/sc_req_item.do?SOAP
	Incident	https://demo.service-now.com/incident.do?SOAP
	Change Request	https://demo.service-now.com/change_request.do?SOAP

- **namespace:** namespace of the XML returned by the web service
- **prefix:** prefix associated with the namespace

The integration configuration includes the following entries if the web service side of the integration is configured for authentication using the SOAP authentication specifications:

- username (Can be blank if **Require basic authorization for incoming SOAP requests** is not selected on ServiceNow side)
- password (Can be blank if **Require basic authorization for incoming SOAP requests** is not selected on ServiceNow side)
- authentication
- locale
- timeZone
- statusMap

The integration configuration also includes the following properties if WS-Security is enabled on service-now side:

- authType
- keystorePath
- keystorePass
- keystoreType
- alias
- keyPass
- catalogItem (For Service Request)

For more information on enabling the WS-Security on ServiceNow side, see “Configuration required on ServiceNow side for WS-Security” on page 43.

The web services and authentication entries are consumed by configuration entries for each web service. They can be positioned either within the configuration entries themselves or as children of the Attributes element. Entries that are children of the Attributes element can be thought of as global values, while entries within the configuration entities can be thought of as local.

For example, if both entries share the same authentication credentials, those credentials might be placed in the Attributes element as peers of the configuration entries and the integration code searches the parent entry for the credentials if they are not found in the configuration entries. Conversely, if the configuration entries have different endpoints (are handled by separate web services), each configuration entry specifies the endpoint of the web service to call and any value outside of the configuration entry is ignored.

Configuring IdentityIQ to integrate with ServiceNow

There are two supported configuration entries for integration with ServiceNow. These entries are children of the integration Attributes element:

- `getRequestStatus`
- `provision`

The values of each are Map elements containing key/value pairings of the configuration data. They contain the specific data needed by the `getRequestStatus()` and `provision()` methods of the IdentityIQ integration executor and correspond to ServiceNow Web Service methods.

The `getRequestStatus` and `provision` entries contain the following entries:

Entries	Description
<code>soapMessage*</code>	Full XML template of the entire SOAP envelope that is sent to the web service. The integration code first runs this template through Apache's Velocity template engine to provide the data needed by the web service.
<code>responseElement*</code>	name of the element containing the results of the web service call (for example, the element containing the ticket number opened by the web service in response to the call from IdentityIQ).
<code>statusMap</code>	For example, see "IntegrationConfig XML files for Service Request, Incident and Change Request" on page 41.
<code>username</code>	Can be blank if Require basic authorization for incoming SOAP requests is not selected on ServiceNow side.
<code>password</code>	Can be blank if Require basic authorization for incoming SOAP requests is not selected on ServiceNow side.
<code>authentication</code>	
<code>locale</code>	<i>(Optional)</i>
<code>timeZone</code>	<i>(Optional)</i>
<code>endpoint</code>	<i>(Optional)</i>
<code>namespace</code>	<i>(Optional)</i>
<code>prefix</code>	<i>(Optional)</i>
<code>authType</code>	<i>(Optional)</i> Use "WS-Security" if WS Security is enabled on service-now side. Otherwise leave it blank.
<code>keystorePath</code>	<i>(Optional)</i> Full path of keystore.
<code>keystorePass</code>	<i>(Optional)</i> Password of keystore.
<code>keystoreType</code>	<i>(Optional)</i> Type of keystore. For example, jks
<code>alias</code>	<i>(Optional)</i> The alias of certificate in keystore.
<code>keyPass</code>	<i>(Optional)</i> The password of alias.
<code>catalogItem</code>	<i>(For Service Request only)</i> Map of Catalog items on ServiceNow defined for IdentityIQ applications.

Before a template is sent to the web service, it is processed by the **Velocity template engine**. The integration code provides different data objects to Velocity for evaluation based on the integration method.

The **provision** call passes the following objects to Velocity:

- **config**: the integration configuration for provision, represented as a Map
- **provisioningPlan**: the data model of the provision request

The **getRequestStatus** call passes the following objects to Velocity:

- **config**: the integration configuration for getRequestStatus, represented as a Map
- **requestID**: the string ID of the request whose status is being queried

Both calls have access to a timestamp variable containing a current Date object and a dateFormatter object. The `dateFormatter` is built using an optional **dateFormat** attribute from the **config** object. If the `dateFormat` attribute does not exist, the formatter defaults to the pattern `EEE, d MMM yyyy HH:mm:ss z`.

Note: Do not modify the **provisioningPlan** using the "ServiceNowServiceIntegration" default rule in the ServiceNow Configuration file.

IntegrationConfig XML files for Service Request, Incident and Change Request

The entries contained in the Map are the only required entries. Any authentication information required by this integration is inherited from the parent Attributes element.

For more information and examples of the sample files, see the following sample files:

- Service Request: `ServiceNowServiceIntegrationModule.xml`
- Incident and Change Request: `ServiceNowSIMForIncidentAndChange.xml`

The `IntegrationConfig.xml` file provides configuration for the following ServiceNow service operations:

- Service Request
- Incident
- Change Request

Note: The IdentityIQ integration for 'Service Request' service operation uses Requested Item (RITM) based approach.

If any changes required in the mapping, change the default value/key values in **statusMap** and **statusMapCloserCode** as mentioned in the following tables:

- statusMap for Service Request:

Entry key (ServiceNow)	Value (IdentityIQ)
-5	inProcess
1	inProcess
2	inProcess
4	failure
7	failure
3	committed

- statusMap and statusMapCloserCode for Incident

Configuring IdentityIQ to integrate with ServiceNow

Entry key (ServiceNow)	Values (IdentityIQ)
statusMap	
1	inProcess
2	inProcess
3	inProcess
4	inProcess
5	inProcess
6	committed
7	committed
8 (For Kingston or later)	failure
statusMapCloserCode	
Solved (Work Around)	committed
Solved (Permanently)	committed
Solved Remotely (Work Around)	committed
Solved Remotely (Permanently)	committed
Closed/Resolved by Caller	committed
Not Solved (Not Reproducible)	failure
Not Solved (Too Costly)	failure

- statusMap for Change Request

Entry key (ServiceNow)	Value (IdentityIQ)
-5	inProcess
-4	inProcess
-3	inProcess
-2	inProcess
-1	inProcess
0	inProcess
3	committed
4	failure

Configuration procedure

The following steps should be performed to modify the default ServiceNow integration configuration for a specific ServiceNow instance.

1. Obtain the environment-specific Web Service “endpoint”, for example, <https://demo.service-now.com/incident.do?SOAP>
A web service can be created or a web service pointing to system table can be used, for example, <https://demo.service-now.com/incident.do?SOAP>
2. Once you are familiar with the WSDL, modify the default IdentityIQ ServiceNow configuration using the information collected about the web service.
 - a. In the <IntegrationConfig> element of the integration configuration, modify the **username** and **password** entries in the attributes map to contain the credentials required for authentication to the web service.
 - b. If you have enabled WS-Security on ServiceNow side, modify entries for **authType**, **keystorePath**, **keystorePass**, **keystoreType**, **alias**, **keyPass** to contain keystore related details.
 - c. In the <IntegrationConfig> element of the integration configuration, modify the provision entry of the Attributes map by setting the endpoint, and, if necessary, the namespace, the prefix, the responseElement, and the soapMessage attributes (the default values: IdentityIQ ServiceNow IntegrationConfig):

- i. Set the value for endpoint to the value located in the WSDL earlier.

Note: The value in the IdentityIQ integration configuration must be a valid HTTP URL and have any special characters escaped. The most common change that must be made is to replace all & symbols with &

- ii. The value for namespace comes from the **targetNamespace** attribute of the **xsd:schema** element in the WSDL.
 - iii. The value for prefix is the prefix of the XML elements that will be contained in the SOAP response.
 - iv. The value for responseElement should be the ServiceNow form field that corresponds to the id of the form that the web service creates.
 - v. The value for soapMessage should be the SOAP message body that IdentityIQ will send to ServiceNow. The exact format of this message is a function of the form that is published as described by the form's WSDL. The XML elements in the **soapenv:Body** element should be changed to match the ServiceNow form fields for the published web service. Each required ServiceNow form field must have an element in the SOAP message. The value can be fixed or can be a variable that will be substituted using IdentityIQ's Velocity templating

The information in the reference section above show the variables that are provided and the example integration configuration provides examples of how they are used.

Configuration required on ServiceNow side for WS-Security

Perform the following steps to enable WS-Security on ServiceNow side:

1. Login to service-now instance with user having access to do system changes for example, admin.
2. Navigate to **System Definition => Certificates** and click on **New** button.
3. Enter some name for the certificate.
4. In your organization, get access to the existing PEM certificates or create a new one for this integration.

Configuring IdentityIQ to integrate with ServiceNow

5. Copy the contents of PEM certificates (including Begin and End Certificate lines) and navigate to service-now and paste the copied contents into **PEM Certificate** field.
6. Save the certificate.
7. Navigate to System **Web Services => WS Security Profiles** and click on **New**.
8. In **Type** field, select X509 and in **X509 Certificate** field, select certificate which we uploaded.
9. Select bind session checkbox.
10. In Run as user field, select name of user on behalf of whom, you want to execute web-services for example, System Administrator.
11. Click on **Submit** button.
12. Navigate to **System Web Services => Properties**.
13. Select the **Require WS-Security header verification for all incoming SOAP requests** check box and save it.

Verifying connectivity between IdentityIQ and ServiceNow

Note: Obtain the integration configuration name and an existing ticket number from ServiceNow Service Desk System.

Perform the following procedure for verifying the connection between IdentityIQ and ServiceNow:

1. Using the IdentityIQ integration console, launch the console by using the following IdentityIQ script in the `WEB-INF/bin` directory of the IdentityIQ installation to run IdentityIQ integration:
`iiq integration`
2. From the console enter the following:
`use applicationName`
where *applicationName* is the name of the ServiceNow Service Desk Integration Module. Therefore the command would be as follows:
`use ServiceNowServiceIntegrationModule`
This makes the application ready for further console commands.
3. Enter the following command to get the connection status:
`getRequestStatus ticketNumber`
where *ticketNumber* is the number of the existing ticket obtained from ServiceNow Service Desk System.
For example, `getRequestStatus REQ1001`
In the above example, REQ1001 is the *ticketNumber*. The following status is returned:
Result: status = committed; request ID = REQ1001; warnings = null; errors = null
This indicates that the connection is successful.

Retryable mechanism

By default IdentityIQ for ServiceNow Service Desk provides retry mechanism for Connection reset and for unknown host problems occurred from network issues.

However you can configure **retryableErrors** list in integration configuration (`IntegrationConfig`) file to add new exception strings to the attributes map in integration configuration file.

The **retryableErrors** entry is a list of strings through which the integration searches when it receives a message from the IdentityIQ for ServiceNow Service Desk. Only **SOAPException** strings are considered for retry that is, the exceptions raised from SOAP web service. If one of the strings in the entry exists in the error, the integration

attempts to retry the request. When the configured error string is not a part of the error message returned from ServiceNow Service Desk, then IdentityIQ will not attempt a retry.

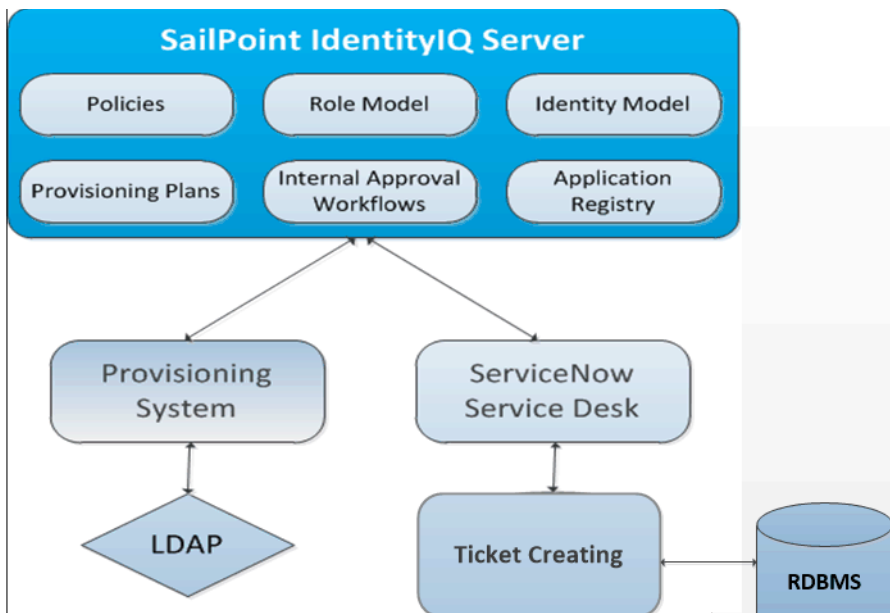
For example,

```
<entry key="retryableErrors">
  <value>
    <List>
      <String>Connection reset</String>
    </List>
  </value>
</entry>
```

Note: Error messages containing very specific information about date/time, sequence ID and so on must be avoided. Error codes or error message substrings would be good candidates for inclusion. Only exceptions raised from soap web service are considered for retry.

Sample scenario

The sample integration scenario is built around a sample system as shown in the following figure:



In the sample scenario IdentityIQ will be issuing change request to ServiceNow based on the results of a scheduled user entitlement and access review. As a result of managing user access process, IdentityIQ will open ServiceNow tickets to control the flow of the manual fulfillment process.

Scenario

1. The LifeCycleManager request for the access of an employee (Identity) on business critical applications.

Troubleshooting

2. IdentityIQ evaluates the provisioning plan to enact the access requests required for the user:
 - a. IdentityIQ policy describes the integration execution path for LDAP as being via an automated provisioning system.
 - b. IdentityIQ policy describes the integration execution path for RDBMS as being via an automated IdentityIQ for ServiceNow Service Desk.
3. IdentityIQ creates a ticket in ServiceNow:
 - a. IdentityIQ uses the **provision** interface to open a ticket within ServiceNow, passing in details of the changes required to the RDBMS system.
 - b. ServiceNow responds with the ticket number.
 - c. IdentityIQ stores the ticket number under the Access Request for later audit and review.
4. IdentityIQ synchronizes ticket status:
 - a. The ticket is assigned to the appropriate ServiceDesk user/ group in the ServiceNow.
 - b. The status of ticket in ServiceNow is updated by ServiceDesk user/ group.
 - c. IdentityIQ synchronizes the status of ticket from ServiceNow and update the access request items status.

Troubleshooting

This section provides the resolutions for the following errors that may be encountered while setting up and configuring IdentityIQ for ServiceNow Service Desk.

Note: Enter the following command to enable log4j tracing on ServiceNow component:

```
log4j.logger.sailpoint.integration.servicenow=debug,file
```

1 - 'Authorization Required' error messages

The following type of error messages appear when the authorization data is not sent to ServiceNow:

Caused by: org.apache.axis2.AxisFault: Transport error: 401 Error: Authorization Required

Resolution: Verify the procedure to configure appropriate authorization mechanism. For more information on the procedure, see "Configuration procedure" on page 42.

2 - For certificate based authentication the IdentityIQ Server and ServiceNow instance must have correct time set.

For certificate based authentication, ensure that the IdentityIQ Server and ServiceNow instance have the correct date, time, and timezone set.

3 - When the Test Connection fails error messages are displayed in IdentityIQ and log file of WebSphere

The following error message is displayed in IdentityIQ:

Unable to engage module: rampart

The following error message is displayed in the log file of WebSphere:

```
ERROR WebContainer: apache.axis2.deployment.ModuleDeployer:113 - The  
rampart-1.6.1.mar module, which is not valid, caused Could not initialize  
class org.apache.axis2.deployment.util.TempFileManager
```

Resolution: If the above error message is displayed in the log file of WebSphere, set the temporary directory in **Generic JVM arguments of Java Virtual Machine** by setting the following variable:

```
-Djava.io.tmpdir=<FullPathOfTempDir>
```

Note: Ensure that the UNIX user where WebSphere is installed should be the owner of the temporary directory.

4 - Duplicate tickets are created during Identity Refresh task execution with Synchronize Attributes enabled

This issue is caused when modifying the provisioningPlan using the **ServiceNowServiceIntegration** default Rule present in the ServiceNow Configuration file.

Resolution: Do not modify the provisioningPlan.

5 - Ticket creation fails with an error message

When the ticket creation fails the following error message appears:

```
java.lang.ClassCastException: org.apache.axis2.saa.j.SOAPMessageImpl cannot be cast to org.apache.axis.Message
```

Resolution: Perform the following:

1. Verify the Web Server VM arguments and delete the following entries if configured:
 - -Djavax.xml.soap.SOAPConnectionFactory=org.apache.axis.soap.SOAPConnectionFactoryImpl
 - -Djavax.xml.soap.MessageFactory=org.apache.axis.soap.MessageFactoryImpl
 - -Djavax.xml.soap.SOAPFactory=org.apache.axis.soap.SOAPFactoryImpl
2. Restart the Web Server.

6 - Duplicate tickets are getting created for request due to non-unique Cart GUIDs

Resolution: Ensure that the Cart GUIDs generated by the Global Cart API script are unique.

ServiceNow recommends not to modify the script included by ServiceNow. For more information, see https://docs.servicenow.com/bundle/kingston-application-development/page/script/server-scripting/concept/c_ScriptIncludes.html

7 - Response gets timed out with an error message

Response gets timed out with the following error message:

```
java.net.SocketTimeoutException: Read timed out
```

Resolution: Add the following entry in the integration configuration page to configure **SO_TIMEOUT** and **CONNECTION_TIMEOUT** attributes in millisecond.

```
<entry key="SO_TIMEOUT" value="" />
<entry key="CONNECTION_TIMEOUT" value="" />
```

8 - Duplicate Incident/Change request ticket numbers are getting generated on ServiceNow

Incident/Change request ticket creation logic uses the import set approach to create tickets where import set table's **number** column is mapped to the target table's **number** column.

Troubleshooting

The mapping of **number** field is done so that a user can customize the generated ticket number. This configuration provides the customer additional flexibility to decide the ticket number generation logic by changing the ticket Prefix/Number/Number of digits on the import set table. ServiceNow instance can have several processes creating tickets in ServiceNow. This may cause a short window of time where the number is chosen by the integration but not committed into the ServiceNow system allowing for another ticket to acquire that number in the interim.

Resolution: Change the prefix/Number/Number of digits. To perform this change:

1. Log in to the ServiceNow instance.
2. Navigate to **System Definition ==> Tables**.
3. Search for a table with name as follows;
 - For Incident request: `x_sapo_iiq_sim_incident`
 - For Change request: `x_sapo_iiq_sim_change_request`
4. Open the record and navigate to **Controls** tab and perform the changes as required.

9 - Access Request line item does not display Provisioning Request ID

Access Request line item does not display Provisioning Request ID, that is ServiceNow ticket number for IdentityIQ for ServiceNow Service Desk.

Resolution: Open the **ServiceNowServiceIntegrationModule** in the application debug page and replace the following line:

```
$requestList = $!requestGroupByApp.get($request.application)
with
#set ($requestList = $!requestGroupByApp.get($request.application))
```

10 - Roles cannot be dragged across slush-buckets for an instance of ServiceNow Madrid release

Resolution: Perform the following steps on ServiceNow Madrid release:

1. Navigate to Service Portal ==> Widgets option and go to the SailPoint custom widget **catalog_access_request**.
2. Open the **catalog_access_request** widget and navigate to the dependency section click on the edit tab to provide require widget dependency.
3. Search for **ng-sortable-1.3.4** dependency in collection slush bucket and move it to the right side bucket.
4. Save the changes.

Chapter 5: IdentityIQ for MicroFocus Service Manager Service Desk

The following topics are discussed in this chapter:

Overview	49
Supported features	49
Supported platforms	50
Pre-requisites	50
Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration	53
Verifying connectivity between IdentityIQ and HP Service Manager (Micro Focus)	60
Retryable mechanism	61
Additional information	61
Troubleshooting	62

Overview

This Integration Module creates Service Requests, Incidents and Change Requests in HP Service Manager for the configured operations (for example, Change Password, Request Entitlement and so on) for the configured application.

Supported features

IdentityIQ for MicroFocus Service Manager Service Desk supports the following features:

- Creates the following types of tickets in HP Service Manager (known as Micro Focus) through provisioning request in IdentityIQ:
 - Service Request
 - Incident
 - Change
- Support for Service Catalog, Incident Management and Change Management Modules in HP Service Manager.

Note: For Service Catalog Module, following options of the Connector drop down list are supported:

 - Open New Request
 - Open an Incident
 - Open a Change
- Fetching the status of Service Request, Incident or Change from HP Service Manager and update the status of the respective Access Requests in IdentityIQ.
- Retry mechanism for Create Ticket request failure

Supported platforms

IdentityIQ for MicroFocus Service Manager Service Desk supports the following version of Service Manager:

- HP Service Manager version 9.6 (now known as Micro Focus Service Manager 9.6)
- HP Service Manager version 9.5
- HP Service Manager version 9.4
- HP Service Manager version 9.3

Pre-requisites

- Ensure that the (one of the) following WSDL is accessible:
 - For Service Request: **http://<host>:<port>/SM/7/SM/7/ServiceCatalogAPI.wsdl**
 - For Incident Request: **http://<host>:<port>/SM/7/IncidentManagement.wsdl**
 - For Change Request: **http://<host>:<port>/SM/7/ChangeManagement.wsdl**

Where <host> is the host name of the system where HP Service Manager is setup and <port> is port number configured for the above web services on HP Service Manager setup. Alternatively, use a Soap UI tool to submit a simple request (for example, incident). For convenience you can use the basic authentication mechanism for authorization with SOAP UI tool to confirm that the web service layer is functional.

- *(Only for Service Request)*
 - To enable Service Request and perform any operation, you must create a Catalog Item in Service Catalog module. For more information on the procedure for creating a Catalog Item, see “Creating New Service Request Catalog Item” on page 61.
 - If Identity Name on IdentityIQ does not match the Contact Name on HP Service Manager, perform the steps mentioned in “Exporting user details from HP Service Manager (Micro Focus)” on page 62 and “Importing user details from HP Service Manager (Micro Focus) to IdentityIQ” on page 62.

Permission for HP Service Manager User

To obtain the minimum permission required for a HP Service Manager User, perform the following:

1. Create a new contact as follows:
 - On HP Service Manager page, navigate to **System Administration ==> Base System Configuration ==> Scheduled Maintenance ==> Contacts**Under the **Contact** tab, enter **Contact Name** and **Full Name**. Click on **Add** button on the top of the page.
2. Create new operators as follows:
 - On the left page, navigate to **System Administration ==> Ongoing Maintenance ==> Operators**
 - Enter the following details and click on **Add**.
 - Login Name
 - Full Name
 - Contact ID
 - Default Company

3. Create new application profiles as follows:

- **Service Request:** To create Request Fulfillment in HP Service Manager from IdentityIQ through integration, minimum permission required is **Request Co-ordinator** as a user role who has right to create any new request fulfillment.

Administrator can create a customized role to create Request Fulfillment from IdentityIQ. Customized user can be created as follows:

- Navigate to System Administration ==> Ongoing Maintenance ==> User Roles and enter the following parameters:

Tab	Field name	Supported field value
Profiles	Configuration Profile	Default
	Security Roles	Default
		Request co-ordinator
Startup	Capability Words	SOAP API
Data Access	Table Name	Application

- **Incident Request:** To create incident in HP Service Manager from IdentityIQ through integration, minimum permission required is **Incident Co-ordinator** as a user role who has right to create any new incident and perform workflow which is capable of closing the incident.

By selecting user role as **Incident Co-ordinator**, select the following under the Startup tab:

- SOAP API as execute capabilities
- Interactions and Service Desk as Query Groups

Administrator can create a customized role to create incident from IdentityIQ. Customized user can be created as follows:

- Navigate to System Administration ==> Ongoing Maintenance ==> User Roles and enter the following parameters:

Tab	Field name	Supported field value
Profiles	Configuration Profile	Default
	Security Roles	Default
		Incident coordinator
Startup	Capability Words	SOAP API
Data Access	Table Name	Application

- **Change Management:** To create change in HP Service Manager from IdentityIQ through integration, minimum permission required is **Change Co-ordinator** as a user role who has right to create any new change.

Administrator can create a customized role to create change from IdentityIQ. Customized user can be created as follows:

- Navigate to System Administration ==> Ongoing Maintenance ==> User Roles and enter the following parameters:

Pre-requisites

Tab	Field name	Supported field value
Profiles	Configuration Profile	Default
	Security Roles	Default
		Change coordinator change
		Change coordinator tasks
Startup	Capability Words	SOAP API
Data Access	Table Name	Application

To perform workflow and close change ticket, select a user with role as **Change Manager**. This role activates the **Next Phase** button which helps to move tickets from one phase to another.

At **Change Approval** stage, the following users are required to approve the tickets and move them to next phase:

- **Change.Approver**: User having group membership of **Change.Approver**
- **Change.Manager**: User having group membership of **Change.Manager**

Once these users submit their approval, ticket gets moved to the next phase and then it can be moved to closure phase.

4. On the Operator Record page, under the Security tab, enter the **Password** and select the **Unlimited Sessions** and **Prevent Lockout** check boxes.
5. Create new login profiles as follows:
On the Operator Record page, under the Login Profiles tab, enter the details of the following parameters (as shown in the following figure) and select the **Named User** check box:
 - Date Format: mm/dd/yy
 - Message Level: Information
6. On the Operator Record page, under the Startup tab, enter the details of the following parameters and select the **Activate Command Line on Startup** checkbox:

Parameters	Value
RAD Name	menu.manager
name	MAIN MENU
prompt	
string1	HOME

Under the startup, select the values for Executive Capabilities and Query Groups from the drop down list as follows and click the **Save** button:

- Execute Capabilities
 - partial.key
 - SysAdmin
 - SQLAdmin

- SOAP API
- user.favorites
- Query Groups
 - Service Desk
 - Interactions

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

This section provides the required information for configuring IdentityIQ to integrate with HP Service Manager. This integration enables IdentityIQ to create tickets for requested revocations, track ticket numbers in association with revocation tasks, and update IdentityIQ with the status of current tickets.

SailPoint provides a default HP Service Manager Service Integration configuration. This configuration implements the integration between IdentityIQ and the HP to fulfill creation of tickets based on IdentityIQ access certification remediation events.

Configuration

- The default configuration is located in `iiqHome/WEB-INF/config/` directory, where `iiqHome` is the location where IdentityIQ was installed.
- When integrating with the following requests, modify the respective config files and import in IdentityIQ:

Request	XML files
Service Request	<code>HPServiceManagerIntegrationConfigForRequest.xml</code>
Incident Request	<code>HPServiceManagerIntegrationConfigForIncident.xml</code>
Change Request	<code>HPServiceManagerIntegrationConfigForChange.xml</code>

For more information, refer to the “Sample XML files for Service, Incident and Change Request” on page 55 section.

- The integration configuration must include the following entries:
 - **endpoint:** URL to the web service
 - **namespace:** namespace of the XML returned by the web service
 - **prefix:** prefix associated with the namespace
- Note:** For more information of the entries in the `IntegrationConfig` file, see Appendix: A: Common Identity Management Integration Configuration.

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

- The integration configuration includes the following entries if the web service side of the integration is configured for authentication using the SOAP authentication specifications:
 - username
 - password
 - statusMap
 - statusMapClosureCode

The web services and authentication entries are consumed by configuration entries for each web service. They can be positioned either within the configuration entries themselves or as children of the **Attributes** element. Entries that are children of the **Attributes** element can be thought of as global values, while entries within the configuration entities can be thought of as local.

For example, if both entries share the same authentication credentials, those credentials might be placed in the **Attributes** element as peers of the configuration entries and the integration code searches the parent entry for the credentials if they are not found in the configuration entries. Conversely, if the configuration entries have different endpoints (are handled by separate web services), each configuration entry specifies the endpoint of the web service to call and any value outside of the configuration entry is ignored.

- Following are the supported configuration entries for integration with HP Service Manager. These entries are children of the integration **Attributes** element:
 - **provision**
 - **getRequestStatus**

The values of each are Map elements containing key/value pairings of the configuration data. They contain the specific data needed by the **provision()** and **getRequestStatus()** methods of the **IdentityIQ** integration executor and correspond to HP Service Manager Web Service methods.

The **provision** and **getRequestStatus** entries contain the following entries:

Entries	Description
soapMessage*	Full XML template of the entire SOAP envelope that is sent to the web service. The integration code first runs this template through Apache's Velocity template engine to provide the data needed by the web service.
responseElement*	Name of the element containing the results of the web service call (for example, the element containing the ticket number opened by the web service in response to the call from IdentityIQ).
SOAPAction*	SOAP requests action
endpoint*	HP Service Manager endpoint to send create and get ticket status
namespace*	Namespace of the XML returned by the web service
prefix*	Prefix associated with the namespace

Note: The (asterisk) * sign represents the required entries.

Before a template is sent to the web service, it is processed by the Velocity template engine. The integration code provides different data objects to Velocity for evaluation based on the integration method.

The following calls pass the respective objects to Velocity:

Call	Objects	Description
provision	config	The integration configuration for provision, represented as a Map
	provisioninPlan	The data model of the provision request
getRequestStatus	config	The integration configuration for getRequestStatus, represented as a Map
	requestID	The string ID of the request whose status is being queried

Both calls have access to a `timestamp` variable containing a current Date object and a `dateFormatter` object. The `dateFormatter` is built using an optional `dateFormat` attribute from the config object. If the `dateFormat` attribute does not exist, the formatter defaults to the pattern `EEE, d MMM yyyy HH:mm:ss z`.

Sample XML files for Service, Incident and Change Request

If any changes required in the mapping, change the value/key values in “statusMap” and “statusMapClosureCode” as mentioned in the following tables for Service, Incident and Change Request:

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

Service Request

Entry Key	Values
statusMap	
Categorize	inProcess
Assign	inProcess
Dispatched	inProcess
In Progress	inProcess
Resolved	committed
Suspended	inProcess
Closed	committed
Pending Other	inProcess
Referred	inProcess
Replaced Problem	inProcess
Open	inProcess
Open - Linked	inProcess
Open - Idle	inProcess
Accepted	inProcess
Rejected	failure
Work In Progress	inProcess
Pending Customer	inProcess
Pending Vendor	inProcess
Pending Change	inProcess
Pending Evidence	inProcess
Pending Vendor/Supplier	inProcess
Withdrawal Requested	failure
initial	inProcess
waiting	inProcess
reopened	inProcess
closed	committed
Denied Service Catalog Request	failure
Status Map Closure Codes	
<i>Incident Closure Codes</i>	
Automatically Closed	committed
Cancelled	failure

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

Entry Key	Values
Fulfilled	committed
Not Reproducible	committed
Out of Scope	committed
Request Rejected	failure
Solved by Change/Service Request	committed
Solved by User Instruction	committed
Solved by Workaround	committed
Unable to solve	failure
Withdrawn by User	failure
Invalid	failure
<i>Request Fulfilment Closure Codes</i>	
1 - Successful	committed
2 - Successful (with problems)	committed
3 - Failed	failure
4 - Rejected (financial)	failure
5 - Rejected (technical)	failure
6 - Rejected (security)	failure
7 - Withdrawn	failure
8 - Withdrawal requested by customer	failure
9 - Cancelled	failure
10 - Denied request fulfillment	failure
11 - Automatically Closed	committed
<i>Change Request Closure Codes</i>	
1	committed
2	committed
3	failure
4	failure
5	failure
6	failure

Incident Request

Entry key	Values
statusMap	
Closed	committed

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

Entry key	Values
Pending Other	inProcess
Referred	inProcess
Replaced Problem	inProcess
Resolved	committed
Open	inProcess
Accepted	inProcess
Rejected	failure
Work In Progress	inProcess
Pending Customer	inProcess
Pending Vendor	inProcess
Pending Change	inProcess
Status Map Closure Codes	
Automatically Closed	committed
Not Reproducible	committed
Out of Scope	committed
Request Rejected	committed
Solved by Change/Service Request	committed
Solved by User Instruction	committed
Solved by Workaround	committed
Unable to solve	failure
Withdrawn by User	failure
Diagnosed Successfully	committed
No Fault Found	committed
No User Response	failure
Resolved Successfully	committed

Change Request

Entry Key	Values
statusMap	
initial	inProcess
waiting	inProcess
reopened	inProcess
closed	committed
Status Map Closure Codes	

Entry Key	Values
1 - Successful	committed
2 - Successful (with problems)	committed
3 - Failed	failure
4 - Rejected	failure
5 - Withdrawn	failure
6 - Cancelled	failure

Configuration procedure

The following steps should be performed to modify the default HP Service Manager Service Integration configuration for a specific HP Service Manager Server.

1. Obtain the environment-specific Web Service “endpoint”, for example, **http://<host>:<port>/SM/7/ws**.
2. (For HP Service Manager 9.5)

- **HPServiceManagerIntegrationConfigForIncident:** Set **Service** as a Configuration Item Identifier.

For example, `<ns:Service type="String" mandatory=" " readonly=" ">CI1001030</ns:Service>`

- **HPServiceManagerIntegrationConfigForChange:**

- Set **Category** as a Standard Change.

For example, `<ns:Category type="String" mandatory=" " readonly=" ">Standard Change</ns:Category>`

- Set **Service** as a Configuration Item Identifier. For example, **CI1001030**

For example, `<ns:Service type="String" mandatory=" " readonly=" ">CI1001030</ns:Service>`

3. Once you are familiar with the WSDL, modify the default IdentityIQ HP Service Manager configuration using the information collected about the web service.

- In the `<IntegrationConfig>` element of the integration configuration, modify the **username** and **password** entries in the attributes map to contain the credentials required for authentication to the web service.
- In the `<IntegrationConfig>` element of the integration configuration, modify the provision entry of the Attributes map by setting the endpoint, and, if necessary, the namespace, the prefix, the responseElement, and the soapMessage attributes (the default values: IdentityIQ HP Service Manager IntegrationConfig):
 - a. Set the value for endpoint to the value located in the WSDL earlier.

Note: The value in the IdentityIQ integration configuration must be a valid HTTP URL and have any special characters escaped. The most common change that must be made is to replace all **and** symbols with **&**;

- b. The value for namespace comes from the **targetNamespace** attribute of the **xsd:schema** element in the WSDL.
- c. The value for prefix is the prefix of the XML elements that will be contained in the SOAP response.
- d. The value for **responseElement** should be the HP Service Manager form field that corresponds to the id of the form that the web service creates.

Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration

- e. The value for **soapMessage** should be the SOAP message body that IdentityIQ will send to HP Service Manager. The exact format of this message is a function of the form that is published as described by the form's WSDL. The XML elements in the **soapenv:Body** element should be changed to match the HP Service Manager form fields for the published web service. Each required HP Service Manager form field must have an element in the SOAP message. The value can be fixed or can be a variable that will be substituted using IdentityIQ's Velocity templating

Note: For more information on **<ManagedResources>** in the *IntegrationConfig* file, see **Appendix: A: Common Identity Management Integration Configuration.**

4. (Only for Service Request) In the **<IntegrationConfig>** element of the integration configuration, modify the *catalogItem* entry of attributes map. Provide key as Managed Application name and value as Request Item Name. This request item must be present on HP Service Manager's Service Request.
For example, `<entry key="Demo Appl" value="Identity Access Request Item"/>`
5. (Only for Service Request) Modify the Rule for **applicationName** and provide its value same as that of application created while importing HP Users in IdentityIQ.

Note: In Rule, the 'attributeName' represents the Application's link attribute and is used to populate the 'requestedFor' field in Service Request.

The information in the reference section above show the variables that are provided and the example integration configuration provides examples of how they are used.

Verifying connectivity between IdentityIQ and HP Service Manager (Micro Focus)

Note: Obtain the integration configuration name and an existing ticket number from MicroFocus Service Manager Service Desk System.

Perform the following procedure for verifying the connection between IdentityIQ and HP Service Manager:

1. Using the IdentityIQ integration console, launch the console by using the following IdentityIQ script in the *WEB-INF/bin* directory of the IdentityIQ installation to run IdentityIQ integration:
`iiq integration`
2. From the console enter the following:
`use applicationName`
where *applicationName* is the name of the MicroFocus Service Manager Service Desk Integration Module. Therefore the command would be as follows:
`use HPSMSServiceIntegrationModuleRequest`
This makes the application ready for further console commands.
3. Enter the following command to get the connection status:
`getRequestStatus ticketNumber`
where *ticketNumber* is the number of the existing ticket obtained from MicroFocus Service Manager Service Desk System.

For example, `getRequestStatus SD10001`

In the above example, SD10001 is the *ticketNumber*. The following status is returned:

Result: status = committed; request ID = SD10001; warnings = null; errors = null

This indicates that the connection is successful.

Retryable mechanism

By default IdentityIQ for MicroFocus Service Manager Service Desk provides retry mechanism for Connection reset and for unknown host problems occurred from network issues.

However you can configure **retryableErrors** list in integration configuration (`IntegrationConfig`) file to add new exception strings to the attributes map in integration configuration file.

The **retryableErrors** entry is a list of strings through which the integration searches when it receives a message from the IdentityIQ for MicroFocus Service Manager Service Desk. Only **SOAPException** strings are considered for retry that is, the exceptions raised from SOAP web service. If one of the strings in the entry exists in the error, the integration attempts to retry the request. When the configured error string is not a part of the error message returned from MicroFocus Service Manager Service Desk, then IdentityIQ will not attempt a retry.

For example,

```
<entry key="retryableErrors">
  <value>
    <List>
      <String>Connection reset</String>
    </List>
  </value>
</entry>
```

Note: Error messages containing very specific information about date/time, sequence ID and so on must be avoided. Error codes or error message substrings would be good candidates for inclusion. Only exceptions raised from soap web service are considered for retry.

Additional information

This section describes the additional information related to IdentityIQ for MicroFocus Service Manager Service Desk.

Creating New Service Request Catalog Item

1. Log on to HP Service Manager as an administrator.
2. (*Only for 9.5*) Navigate to **Service Catalog => Administration => Manage Items** and click on **Add New Service Item** link.
(*Only for 9.4 and 9.3*) Navigate to **Service Catalog => Administration => Manage Catalog** and click on **Add New Service Catalog Item** link.
3. Mention the mandatory details and click **Next**.
4. Select the Connector as **Open New Request**.
5. Select **Service Desk** as the option from the In Category as drop down and click **Next**.

Troubleshooting

6. (Only for 9.4 and 9.5) Provide appropriate values to the following fields and click **Next**:

- Request Category
- Request SubCategory
- Department
- Request Model

Select appropriate values from the drop down of **Urgency**, **Impact** and **Assignment**.

7. (Only for 9.3) Provide appropriate value for **Request Category**.

8. Click **Finish**.

9. (For 9.6 only) Make Service Catalog Item status to **Operational** and click **Save**.

Exporting user details from HP Service Manager (Micro Focus)

1. Log on to HP Service Manager as an Administrator.
2. Navigate to **System Administration => Base System Configuration => Contacts** and click on **Search**. All user contact list must be displayed.
3. Navigate to **More => Export to Text File** and select the check box for **Export Column Headers**.
4. Select the radio button for **Comma Separated Value (CSV)** in the Delimiter selection.
5. Click on **OK**.
6. A file with name **export.csv** will get downloaded to your location.

Importing user details from HP Service Manager (Micro Focus) to IdentityIQ

1. Navigate to application definition and click on **Add New Application** button.
2. Enter the application name in the **Name** field and select the owner.
3. Select the application type as **DelimitedFile**.
4. Mention the **File Path** details under the Configuration tab and list the column names under the **Columns** section in the same order as that present in the **export.csv** file.
5. Insert the value as **'** in the **Delimiter** field.
6. Under the **Schema** tab click on **Discover Schema Attributes** and mention Identity attribute as **Contact Name**.
7. Click on **Preview** and **Save** the application.

Note: For more information on correlating the users on HP Service Manager with identities on IdentityIQ, see “SailPoint Delimited Connector” chapter of the *SailPoint Direct Connectors Administration and Configuration Guide*.

Troubleshooting

This section provides the resolutions for the following errors that may be encountered while setting up and configuring IdentityIQ for MicroFocus Service Manager Service Desk.

1 - 'Authorization Required' error messages

The following type of error messages appear when the authorization data is not sent to HP Service Manager:

Caused by: org.apache.axis2.AxisFault: Transport error: 401 Error:
Authorization Required

Resolution: Verify the procedure to configure appropriate authorization mechanism. For more information on the procedure, see "Configuration procedure" on page 59.

2 - Document Type Declaration (DTD) parsing errors

The DTD parsing errors appear when the following JVM arguments are not defined for your application server:

- -Djavax.xml.soap.SOAPConnectionFactory=org.apache.axis2.saa.j.SOAPConnectionFactoryImpl
- -Djavax.xml.soap.MessageFactory=org.apache.axis2.saa.j.MessageFactoryImpl
- -Djavax.xml.soap.SOAPFactory=org.apache.axis2.saa.j.SOAPFactoryImpl

Resolution: Ensure that the application is pointing to the correct java runtime (that is, 1.6) and the above mentioned JVM arguments are defined for application server.

3 - Max session exceeded error

When multiple requests are in open state and IdentityIQ tries to fetch the latest status with those requests, the following error message is displayed:

Max session exceeded error

Resolution: Perform the following:

1. Increase the shared memory in `sm.ini` file to twice or thrice the size.
2. Add the following attribute to `sm.ini` file:
`threadsperprocess:50`

4 - Change Ticket status gets committed on IdentityIQ even though ticket is open on HP Service Manager.

Resolution: Perform the following:

1. On HP Service Manager navigate to **Tailoring => Web Services => Format control** and search for `cm3r` name.
2. Delete the following parameter line from Initialization Expressions of `cm3r`:
 - HP Service Manager 9.5:


```
if (jscall("ProcessDesignerEnablement.isChangeEnabled")=true and
jscall("ProcessDesignerEnablement.isMigratedWorkflowUsed", "cm3r", category
in $file)=false and null(completion.code in $file)) then (completion.code in
$file=1)
```
 - HP Service Manager 9.4 or 9.3:


```
if (jscall("ProcessDesignerEnablement.isChangeEnabled")=true and
null(completion.code in $file)) then (completion.code in $file=1)
```
3. Click **Save**.

5 - When performing any provisioning action an error message is displayed.

The following error message is displayed, when performing any of the provisioning actions:

```
sailpoint.integration.hpservicemanager.HPServiceManagerSoapIntegration$MissingResponseElementException: Unable to find a response element matching qname {http://schemas.hp.com/SM/7}CartItemId. Check the integration config.
```

Resolution: Ensure that the user is present on HP Service Manager for which the ticket is being created.

6 - Change Ticket status displays pending status on IdentityIQ even when ticket is closed on HP Service Manager.

When HP status and closure code are not mapped in integration configuration file, change ticket status displays pending status on IdentityIQ even when ticket is closed on HP Service Manager.

For example,

```
In 2016-08-02 16:52:48,870 ERROR Workflow Event Thread 1
sailpoint.integration.AbstractIntegrationExecutor:380 - Unknown request status: 1 -
Successful is retryable
```

```
java.lang.Exception: Unknown request status: 1 - Successful
```

Resolution: Map HP status code with corresponding IdentityIQ status code in statusMap or statusMapCloserCode in Integration configuration file.

```
<entry key="1 - Successful " value="committed" />
```

7 - Ticket does not exist on HP Service Manager

When IdentityIQ access request is updated with ticket number, ticket does not exist on HP Service Manager version 9.5.

Resolution: For HP Service Manager version 9.5 there are changes in Incident and Change configuration files. Ensure that the configuration steps mentioned in the “Configuring HP Service Manager (Micro Focus) for IdentityIQ Integration” on page 53 for Incident and Change Requests are performed appropriately.

Chapter 6: IdentityIQ for BMC Remedy Service Desk

The following topics are discussed in this chapter:

Overview	65
Supported features	65
Supported platforms	65
Pre-requisites	66
Basic configuration	66
Configuring BMC Remedy AR System for IdentityIQ Integration	67
Configuring IdentityIQ for BMC Remedy Action Request System Integration	69
BMC Remedy Action Request System Integration	69
Creating multiple tickets in Remedy System	73
Verifying connectivity between IdentityIQ and BMC Remedy	74
Retryable mechanism	74
Sample scenario	75
Troubleshooting	76

Overview

The integration between SailPoint and BMC Remedy Service Desk enables customers to create incidents and change requests in BMC Remedy Service Desk for the configured operations (for example, Change Password, Request Entitlement and so on) for the configured application. The seamless integration of SailPoint and BMC Remedy Service Desk Integration Module eliminates the need to build and maintain a custom integration, and speeds time-to-deployment.

Note: Enter the following command to enable log4j tracing on BMC Remedy Service Desk component:

```
log4j.logger.sailpoint.integration.SOAPIntegration=trace,file
```

Supported features

IdentityIQ for BMC Remedy Service Desk supports the following features:

- creating ticket for all provisioning operations that can be performed on Target Application accounts
- getting the status of the created tickets
- creating multiple tickets in Remedy System via IdentityIQ

Supported platforms

IdentityIQ for BMC Remedy Service Desk supports the following versions of BMC Remedy AR System:

- BMC Remedy AR System 18.05
- BMC Remedy AR System 9.1.00
- BMC Remedy AR System 9.0.00

Pre-requisites

- BMC Remedy Change Management Application must be installed
- Ensure that the following softwares are operating correctly:
 - BMC Remedy AR System
 - BMC Remedy Change Management Application

Basic configuration

The integrated solution speeds the detection and remediation of identity management issues that increase the risk of compliance violations or security breaches, such as orphaned accounts, policy violations, and inappropriate access privileges. Organizations can take advantage of a centralized approach spanning thousands of users and hundreds of resources to strengthen IT controls and provide proof of compliance to auditors and executive management. The seamless integration of SailPoint and BMC Remedy eliminates the need to build and maintain a custom integration, and speeds time-to-deployment.

For any IT resources managed by BMC Remedy Service Desk, IdentityIQ automatically creates a trouble ticket within Remedy Service Desk, passing along all relevant identity data and reviewer comments to populate the ticket.

To ensure revocation requests get delivered and implemented, IdentityIQ manages all remediation and revocation requests within a guaranteed delivery model.

To determine the status of user accounts, IdentityIQ performs closed-loop audits on remediation requests and compares the actual state of user privileges with the original change request. If the request is still open, an alert will be sent to the reviewer for prompt action and closure.

The integration itself has been designed to be quick to install and easy to use. It makes use of Web Services via the Remedy Mid Tier to broker communications between the SailPoint server and the AR System server. On the backside of a user recertification, policy remediation action or access request action, the IdentityIQ server will direct provisioning and service desk requests to the configured implementers. Based on the IntegrationConfig configured for each target application, service desk request are issues to a given remediation/implementation point. Once the IntegrationConfig for Remedy has been loaded into the IdentityIQ server, all change/remediation actions result in the creation of new service desk request.

At the completion of the change control cycle within IdentityIQ, an “Open Ticket” request is made over the appropriate SOAP channel to the Mid Tier. From here change request tickets are opened and the new ticket number is returned to IdentityIQ. The schema for the service request is defined in the IntegrationConfig and allows for the flexibility to transfer complete details on the service desk request. The default settings will create a basic ticket as shown in the following figure ([Figure 1—Change request](#)).

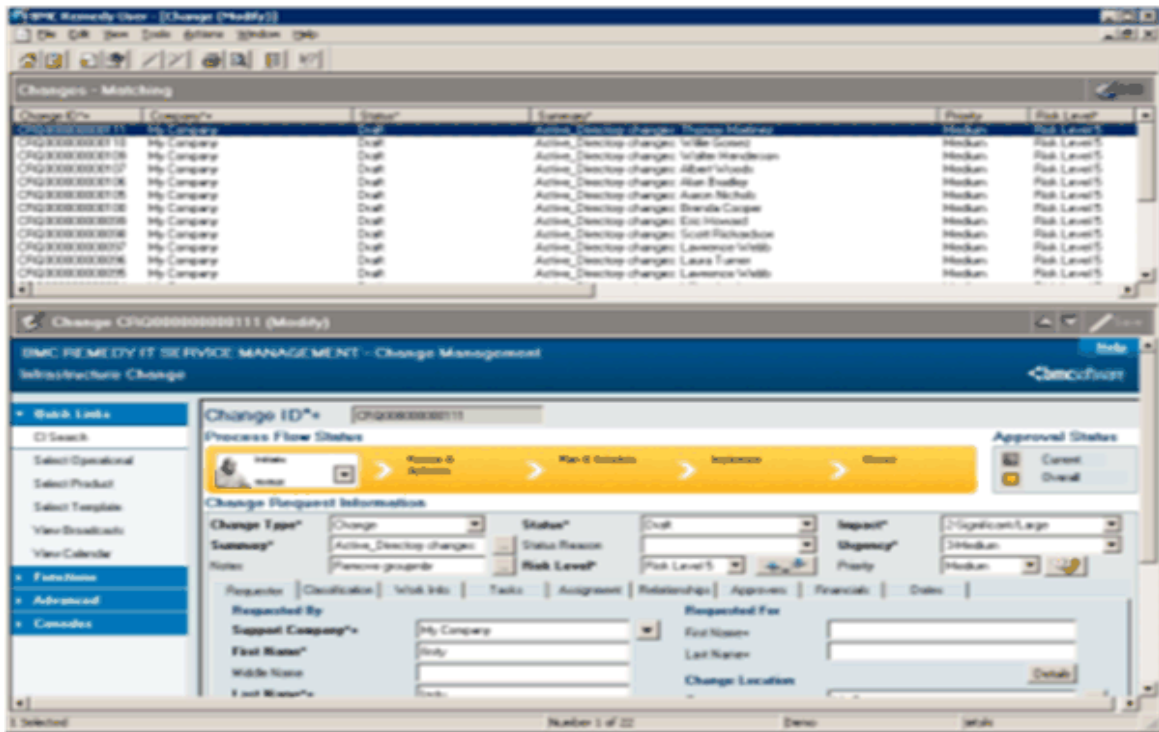


Figure 1—Change request

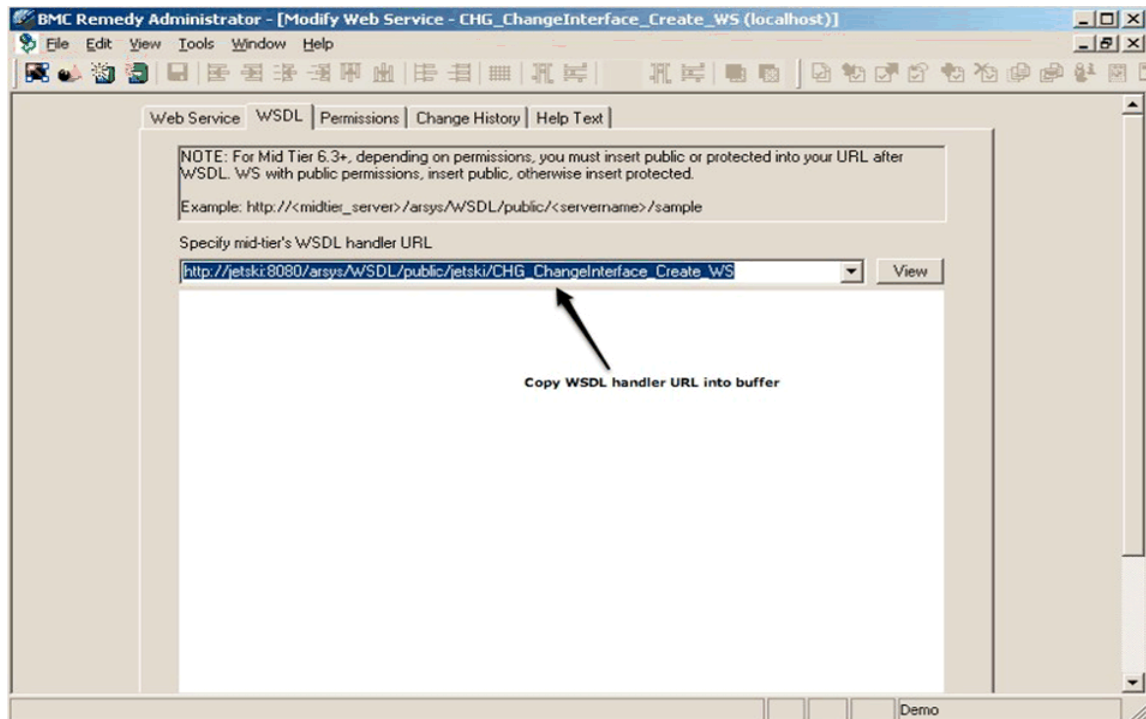
Configuring BMC Remedy AR System for IdentityIQ Integration

This section provides the required information for configuring IdentityIQ to integrate with BMC Remedy Action Request System (AR System). This integration enables IdentityIQ to create Change Management tickets for requested revocations, track ticket numbers in association with revocation tasks, and update IdentityIQ with the status of current Change Management tickets.

The following steps should be performed to modify the default Remedy integration configuration for a specific BMC Remedy application instance.

1. Confirm the default Remedy Change Management Application Web Services exist. This is done by launching the BMC Remedy Administrator, expanding the appropriate server object and clicking on the “Web Services” object.
2. Next, obtain the environment-specific Web Service “endpoint” by performing the following steps:
 - a. Double-click on the Web Service and select the WSDL tab. Copy the WSDL handler URL into your buffer (For example, Ctrl-C)

Configuring BMC Remedy AR System for IdentityIQ Integration



- b. With a web browser, visit the WSDL URL for the web service by entering the URL into the browser address field and pressing return.
- c. Search for **soap:address location=** to find the endpoint URL. Copy this value. It will be used to replace the endpoint URL in the default IdentityIQ Remedy IntegrationConfig object.

```
- <wsdl:port binding="s0:CHG_ChangeInterface_Create_WSSoapBinding" name="CHG_ChangeInterface_Create_WSSoap">
  <soap:address location="http://jetski:8080/arsys/services/ARService?server=jetski&webService=CHG_ChangeInterface_Create_WS"/>
</wsdl:port>
```

- d. Review the Create InputMap section of the WSDL to understand the fields available for population through the Web Service. These fields should correspond to the fields listed in the <soapenv:Body> section of the default IdentityIQ IntegrationConfig object
3. Once you are familiar with the WSDL, modify the default IdentityIQ Remedy integration using the information collected about the web service.
 - a. In the <IntegrationConfig> element of the integration configuration, modify the **username** and **password** entries in the attributes map to contain the credentials required for authentication to the web service.
 - b. In the <IntegrationConfig> element of the integration configuration, modify the provision entry of the Attributes map by setting the endpoint, and, if necessary, the namespace, the prefix, the responseElement, and the soapMessage attributes (the default values: IdentityIQ Remedy IntegrationConfig):
 - i. Set the value for endpoint to the value located in the WSDL earlier.

Note: The value in the IdentityIQ integration configuration must be a valid HTTP URL and have any special characters escaped. The most common change that must be made is to replace all & symbols with &

- ii. The value for namespace comes from the **targetNamespace** attribute of the **xsd:schema** element in the WSDL.

- iii. The value for prefix is the prefix of the XML elements that will be contained in the SOAP response sent by the mid tier server.
- iv. The value for responseElement should be the ARS form field that corresponds to the id of the form that the web service creates.
- v. The value for soapMessage should be the SOAP message body that IdentityIQ will send to ARS. The exact format of this message is a function of the form that is published as described by the form's WSDL. The XML elements in the **soapenv:Body** element should be changed to match the ARS form fields for the published web service. Each required ARS form field must have an element in the SOAP message. The value can be fixed or can be a variable that will be substituted using IdentityIQ's Velocity templating.

The information in the reference section above show the variables that are provided and the example integration configuration provides examples of how they are used.

Configuring IdentityIQ for BMC Remedy Action Request System Integration

This is intended as an introduction to the configuration needed to integrate **IdentityIQ** with the BMC Remedy Action Request System. This integration enables **IdentityIQ** to interact with many of the product solutions that are built on top of the AR System Server including BMC Remedy Change Management, BMC Remedy IT Service Management Suite, and BMC Remedy Service Desk.

BMC Remedy Action Request System Integration

SailPoint provides a default Remedy integration configuration. This configuration implements the integration between IdentityIQ and the Remedy Change Management Application to fulfill creation of tickets based on IdentityIQ access certification remediation events.

The default configuration is located in `iiqHome/WEB-INF/config/remedy-integration.xml` directory, where *iiqHome* is the location where IdentityIQ was installed.

This section explains the various entries that are specific for this integration. For more information of the entries in the `IntegrationConfig` file, see Appendix A: Common Identity Management Integration Configuration.

The integration configuration must include the following entries:

- **endpoint**: URL to the web service
- **namespace**: namespace of the XML returned by the web service
- **prefix**: prefix associated with the namespace

The integration configuration includes the following entries if the web service side of the integration is configured for authentication using the SOAP authentication specifications:

- username
- password
- authentication
- locale
- timeZone
- statusMap

Configuring IdentityIQ for BMC Remedy Action Request System Integration

The integration configuration includes the following entries if the http authentication is configured:

- **basicAuthType**: if http authentication is configured the value of **basicAuthType** is true.
- **httpUserName**
- **httpUserPass**

User must modify remedy integration configuration file with the following entries to create incident in BMC Remedy Action Request System:

- **endpoint**
- **responseElement key**
- SOAP envelop and body details
- status mapping

The web services and authentication entries are consumed by configuration entries for each web service. They can be positioned either within the configuration entries themselves or as children of the **Attributes** element. Entries that are children of the **Attributes** element can be thought of as global values, while entries within the configuration entities can be thought of as local.

For example, if both entries share the same authentication credentials, those credentials might be placed in the **Attributes** element as peers of the configuration entries and the integration code searches the parent entry for the credentials if they are not found in the configuration entries. Conversely, if the configuration entries have different endpoints (are handled by separate web services), each configuration entry specifies the endpoint of the web service to call and any value outside of the configuration entry is ignored.

There are two supported configuration entries for integration with Remedy. These entries are children of the integration **Attributes** element:

- **getRequestStatus**
- **provision**

The values of each are Map elements containing key/value pairings of the configuration data. They contain the specific data needed by the **getRequestStatus()** and **provision()** methods of the IdentityIQ integration executor and correspond to Remedy Web Service methods.

The **getRequestStatus** and **provision** entries contain the following entries:

- **soapMessage** (required): full XML template of the entire SOAP envelope that is sent to the web service. The integration code first runs this template through Apache's Velocity template engine to provide the data needed by the web service.
- **responseElement** (required): name of the element containing the results of the web service call (for example, the element containing the ticket number opened by the web service in response to the call from IdentityIQ).
- **statusMap** (optional, see "Sample getRequestStatus entry" on page 71 for an example)
- **username** (optional)
- **password** (optional)
- **authentication** (optional)
- **locale** (optional)
- **timeZone** (optional)
- **endpoint** (optional)
- **namespace** (optional)
- **prefix** (optional)

Before a template is sent to the web service, it is processed by the **Velocity template engine**. The integration code provides different data objects to Velocity for evaluation based on the integration method.

The **provision** call passes the following objects to Velocity:

- **config**: the integration configuration for provision, represented as a Map
- **provisioningPlan**: the data model of the provision request

The **getRequestStatus** call passes the following objects to Velocity:

- **config**: the integration configuration for `getRequestStatus`, represented as a `Map`
- **requestID**: the string ID of the request whose status is being queried

Both calls have access to a `timestamp` variable containing a current `Date` object and a `dateFormatter` object. The `dateFormatter` is built using an optional `dateFormat` attribute from the **config** object. If the `dateFormat` attribute does not exist, the formatter defaults to the pattern `EEE, d MMM yyyy HH:mm:ss z`.

Sample `getRequestStatus` entry

Note: The entries contained in the Map are the only required entries. Any authentication information required by this integration is inherited from the parent Attributes element.

```
<entry key="getRequestStatus">
  <value>
    <Map>
      <entry key="responseElement" value="Status"/>
      <entry key="soapMessage">
        <!-- XML template - DO NOT add line breaks before the CDATA! -->
        <value><String><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
# if ($config.username)
<soapenv:Header>
<ns1:AuthenticationInfo xmlns:ns1="urn:AuthenticationInfo">
  <ns1:userName>$config.username</ns1:userName>
  <ns1:password>$config.password</ns1:password>
  # if ($config.authentication)
    <ns1:authorization>$config.authentication</ns1:password>
# end
# if ($config.locale)
    <ns1:locale>$config.locale</ns1:password>
# end
# if ($config.timeZone)
    <ns1:timeZone>$config.timeZone</ns1:password>
# end
</ns1:AuthenticationInfo>
</soapenv:Header>
# end
<soapenv:Body>
  <iiq:Get xmlns:iiq="urn:GetAgreementWebService">
    <iiq:Issue_ID>$requestID</iiq:Issue_ID>
  </iiq:Get>
</soapenv:Body>
</soapenv:Envelope>
]]>
      </value>
    </entry>
  </Map>
</value>
</entry>
```

Configuring IdentityIQ for BMC Remedy Action Request System Integration

Sample provision entry

Note: This Map contains its own web services information. Any authentication information required by this integration is inherited from the parent Attributes element.

```
<entry key="provision">
  <value>
    <Map>
      <entry key="endpoint"
value="http://my.server.com:8080/path/to/WS"/>
      <entry key="namespace" value="urn:openTicketWebService"/>
      <entry key="prefix" value="xyz"/>
      <entry key="responseElement" value="Issue_ID"/>
      <entry key="soapMessage">
        <!-- XML template - DO NOT add line breaks before the CDATA!
-->
        <value><String><![CDATA[<?xml version="1.0"
encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <!--
  #if ($config.username)
  <soapenv:Header>
  <ns1:AuthenticationInfo xmlns:ns1="urn:AuthenticationInfo">
    <ns1:userName>$config.username</ns1:userName>
    <ns1:password>$config.password</ns1:password>
  #if ($config.authentication)
    <ns1:authorization>$config.authentication</ns1:password>
  #end
  #if ($config.locale)
    <ns1:locale>$config.locale</ns1:password>
  #end
  #if ($config.timeZone)
    <ns1:timeZone>$config.timeZone</ns1:password>
  #end
  </ns1:AuthenticationInfo>
  </soapenv:Header>
  #end
  <soapenv:Body>
    <iiq:Get xmlns:iiq="urn:openTicketWebService">
      <iiq:Submitter>
        #foreach ($req in $provisionPlan.requesters)
          $req.name
        #end
      </iiq:Submitter>
      <iiq:SubmitDate>$timestamp</iiq:SubmitDate>
      <iiq:Summary>
        Remediation request from IIQ
      </iiq:Summary>
      <iiq:Description>
        Remove Active Directory for $provisionPlan.identity.fullname
      </iiq:Description>
      <iiq:Issue_ID>$requestID</iiq:Issue_ID>
    </iiq:Get>
  </soapenv:Body>
</soapenv:Envelope>
]]>
        </value>
      </entry>
```

```

    </Map>
  </value>
</entry>

```

Sample statusMap entry

The **noMappingFromWS** entries are placeholders as there are no results from the web service corresponding to those IdentityIQ result codes.

```

<entry key="statusMap">
  <value>
    <Map>
      <entry key="Closed" value="committed" />
      <entry key="Rejected" value="failure" />
      <entry key="Draft" value="inProcess" />
      <entry key="Pending" value="inProcess" />
      <entry key="noMappingFromWS" value="retry" />
      <entry key="noMappingFromWS" value="warning" />
    </Map>
  </value>
</entry>

```

Creating multiple tickets in Remedy System

To create multiple tickets in Remedy System via IdentityIQ, add the following attributes in `remedy-integration.xml` file:

- **multipleTicket**: If `multipleTicket` attribute is defined, then the value can be one of the following:
 - **True**: A separate Remedy ticket would be created for each line item from the IdentityIQ access request.
 - **False**: Single Remedy ticket would be created against all line items from the IdentityIQ access request.

Default value: true

The format of the entry is as follows:

```
<entry key='multipleTicket' value='true' />
```

- **groupTicketBy**: If `groupTicketBy` attribute is defined, then value can be one of the following:
 - **none**: If the attribute is not defined or if attribute value is other than Application, then IdentityIQ sets this attribute to none.
 - **Application**: If the attribute value is Application and `multipleTicket=true`, then IdentityIQ access request lines from the same application would be moved to a single ticket.

The format of the entry is as follows:

```
<entry key='groupTicketBy' value='none' />
```

Default value: none

For example, the **multipleTicket** and **groupTicketBy** keys can be placed in the Integration configuration file as follows:

```

<IntegrationConfig>
  <Attributes>
    <Map>
      <entry key="multipleTicket" value="true"/>
      <entry key='groupTicketBy' value='none' />
      <entry key="provision">

```

Configuring IdentityIQ for BMC Remedy Action Request System Integration

```
<value>
  <Map>
    <entry key="endpoint" value="%%REMEDY_REQ_TICKET_ENDPOINT%%"/>
    ...
    ...
    ...
  </Map>
</value>
</entry>
</Map>
</Attributes>
<IntegrationConfig>
```

Verifying connectivity between IdentityIQ and BMC Remedy

Note: Obtain the integration configuration name and an existing ticket number from BMC Remedy Service Desk System.

Perform the following procedure for verifying the connection between IdentityIQ and BMC Remedy:

1. Using the IdentityIQ integration console, launch the console by using the following IdentityIQ script in the `WEB-INF/bin` directory of the IdentityIQ installation to run IdentityIQ integration:
`iiq integration`
2. From the console enter the following:
`use applicationName`
where *applicationName* is the name of the BMC Remedy Service Desk. Therefore the command would be as follows:
`use tst_RemedyIntegration`
This makes the application ready for further console commands.
3. Enter the following command to get the connection status:
`getRequestStatus ticketNumber`
where *ticketNumber* is the number of the existing ticket obtained from BMC Remedy Service Desk System.
For example, `getRequestStatus IM10001`
In the above example, IM10001 is the *ticketNumber*. The following status is returned:
Result: status = committed; request ID = IM10001; warnings = null; errors = null
This indicates that the connection is successful.

Retryable mechanism

By default IdentityIQ for BMC Remedy Service Desk provides retry mechanism for Connection reset and for unknown host problems occurred from network issues.

However you can configure **retryableErrors** list in integration configuration (`IntegrationConfig`) file to add new exception strings to the attributes map in the file.

The **retryableErrors** entry is a list of strings through which the Remedy Integration searches when it receives a message from the BMC Remedy Service Desk. Only **SOAPException** strings are considered for retry that is, the exceptions raised from SOAP web service. If one of the strings in the entry exists in the error, the integration attempts to retry the request. When the configured error string is not a part of the error message returned from the BMC Remedy Service Desk, then IdentityIQ will not attempt a retry.

For example,

```
<entry key="retryableErrors">
  <value>
    <List>
      <String>Connection reset</String>
    </List>
  </value>
</entry>
```

Additionally IdentityIQ would retry for following exception strings:

```
<entry key="retryableErrors">
  <value>
    <List>
      <String>Connection refused: connect</String>
      <String>Connection timed out</String>
      <String>Connection reset</String>
    </List>
  </value>
</entry>
```

Note: Error messages containing very specific information about date/time, sequence ID and so on must be avoided. Error codes or error message substrings would be good candidates for inclusion. Only exceptions raised from soap web service are considered for retry.

Sample scenario

The sample integration scenario is built around a sample system. In the sample scenario IdentityIQ (IIQ) would be issuing a change request to BMC Remedy Change Management (RCM) based on the results of a scheduled user entitlement and access review. As a result of remediation actions in this account recertification process, IdentityIQ would open change requests to control the flow of the manual remediation process.

Scenario

1. The ComplianceManager1 schedules an access review for a business critical application:
 - a. The certification is scheduled and assigned to ApplicationOwner1.
 - b. ApplicationOwner1 receives an email with a link to the Online certification process as scheduled. The link is followed to the open certification.
 - c. ApplicationOwner1 decides that GroupA on system LDAP should be removed.
 - d. ApplicationOwner1 decides that RoleA on system RDBMS should be removed.
 - e. ApplicationOwner1 completes the certification and signs off the process.
2. IdentityIQ evaluates the provisioning plan to enact the remediation requests from the certification:
 - a. IdentityIQ policy describes the integration execution path for LDAP as being via an automated provisioning system.
 - b. IdentityIQ policy describes the integration execution path for RDBMS as being via an automated RCM integration.

Troubleshooting

3. IdentityIQ creates a service request in RCM:
 - a. IdentityIQ uses the **provision** interface to open a service request within Remedy, passing in details of the changes required to the RDBMS system.
 - b. RCM responds with the service request number.
 - c. IdentityIQ stores the service request number for later audit and review.

Troubleshooting

1 - During ticket creation the system is not responding in a normal amount of time

During ticket creation the system is not responding in a normal amount of time resulting in a time out and not returning the ticket number.

Resolution: Add the timeout additional configuration parameter to the application debug page as follows for setting the timeout per operation (that is, provision, getrequest):

```
<entry key="timeout" value="1"/>
```

Here value is in seconds.

Chapter 7: IdentityIQ for ServiceNow Catalog

The following topics are discussed in this chapter:

Overview	77
Supported features	78
Supported platforms	79
Pre-requisites	79
Installation and configuration in ServiceNow	79
Configuration in SailPoint IdentityIQ	83
Troubleshooting	83

Overview

IdentityIQ for ServiceNow Catalog is an integration between ServiceNow and SailPoint IdentityIQ. This allows users of both systems to easily navigate from ServiceNow into IdentityIQ, and gives users a "one stop shop" to request all IT related items.

The integration between SailPoint and ServiceNow gives mutual customers a complementary identity access governance and service management solution that works together to ensure strong controls are in place to meet ever stringent security and compliance requirements around user access to sensitive applications. The integration also allows users to perform other activities (such as password changes, approve access, manage account) that are configured within the system.

The chapter describe the implementation approach and configuration of the IdentityIQ for ServiceNow Catalog in ServiceNow. The following information enables administrators to deploy and maintain the integration.

The flow of IdentityIQ for ServiceNow Catalog in ServiceNow is as follows:

- User logs in to ServiceNow.
- The **IdentityIQ for ServiceNow Catalog** application is available to the logged in user.
- Click on any of the links mentioned in the request section of IdentityIQ for ServiceNow Catalog Application. Request flows to IdentityIQ and IdentityIQ page is opened in ServiceNow.
- Complete the request in IdentityIQ page opened in ServiceNow and Ticket would be generated in ServiceNow for the same request. Initially the status of ServiceNow ticket would be **open** or **openNoApproval**.
- Once the request is approved in IdentityIQ, ServiceNow ticket's status would be updated.
- Once the provisioning of request is done on IdentityIQ side, the ticket's status would be updated (closed) in ServiceNow.

Supported features

The following diagram represents the high level flow diagram for ServiceNow Catalog with SailPoint IdentityIQ:

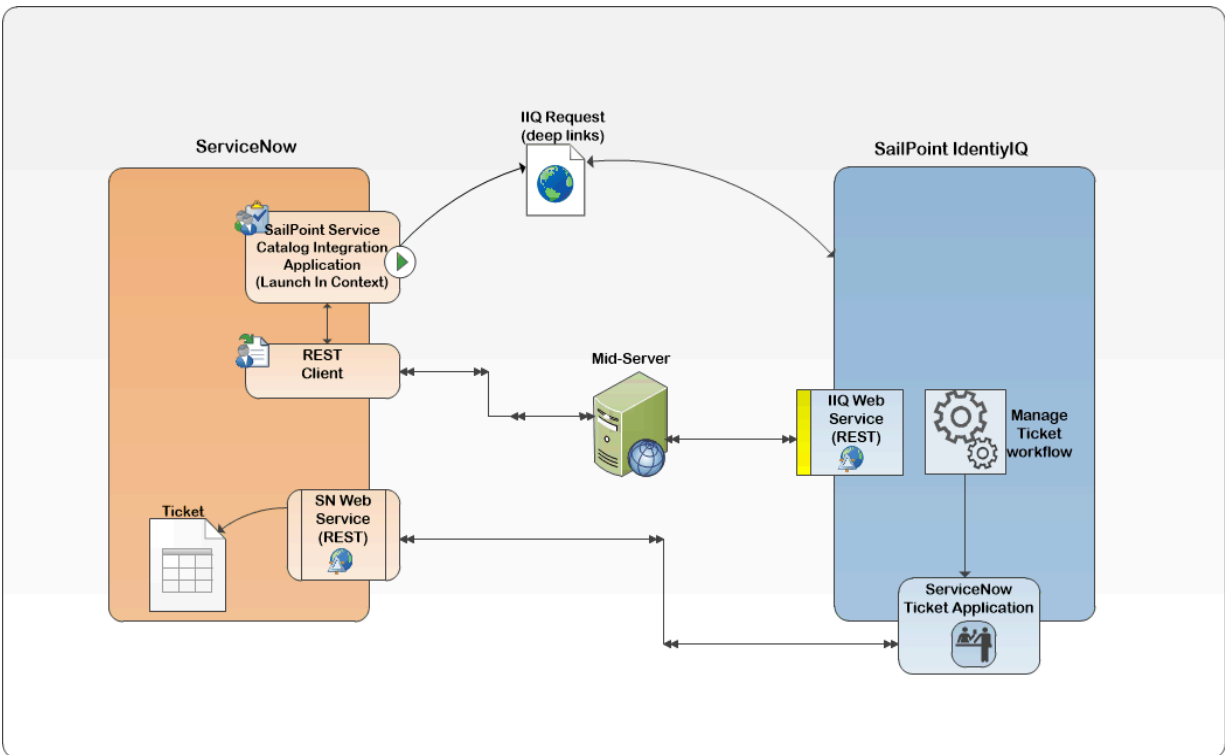


Figure 1—Basic Configuration

If a request is submitted from ServiceNow then SailPoint IdentityIQ creates or updates tickets in ServiceNow using ServiceNow Ticket Application from IdentityIQ.

Supported features

The IdentityIQ for ServiceNow Catalog enables the use of IdentityIQ Lifecycle Manager within ServiceNow user interfaces. The inclusion of the IdentityIQ for ServiceNow Catalog Application provides the following functionality within ServiceNow:

- Manage Account for Me
 - Enable/Disable/Unlock/Delete Accounts
- Request Access for Me/Others
 - Request for Entitlement
 - Request for Roles
- Request Password Changes
- My Access Approvals

- Track My Requests
 - Get Request Status
 - Get complete details of request Item

Supported platforms

IdentityIQ for ServiceNow Catalog supports the following ServiceNow releases:

- Madrid
- London
- Kingston

Pre-requisites

- For the integration to successfully authenticate the user, the ServiceNow accounts (users) must have correlated identities in IdentityIQ.
- ServiceNow Mid Server must be installed. See “Mid server installation” on page 81.

Note: Ensure that the WebServer hosting IdentityIQ must be SSL enabled.

Installation and configuration in ServiceNow

This section describes the installation and configuration procedures for SailPoint IdentityIQ ServiceNow Service Catalog Integration.

Following roles on ServiceNow can be assigned to the user:

- **x_sapo_iiq_catalog.spnt_admin:** IdentityIQ for ServiceNow Catalog Administrator Role. The user with this role can access all the modules of the application.
- **x_sapo_iiq_catalog.spnt_manager:** IdentityIQ for ServiceNow Catalog Manager Role. The user with this role can access all modules except Setup.
- **x_sapo_iiq_catalog.spnt_user:** IdentityIQ for ServiceNow Catalog User Role. The user with this role does not have access to Setup module and can request only for himself.

Installation

This section describes the installation procedure.

Install update set in ServiceNow

Apply the IdentityIQ ServiceNow Catalog Integration update set:

1. Copy the relevant update set from the following directory to a temporary directory:
`identityiq-releaseVersion.zip\integration\servicenow\iiqIntegration-ServiceNow.zip\ServiceCatalogUpdateSet`

In the above directory, *releaseVersion* is the version of the current IdentityIQ release.

ServiceNow version	Update Sets
Kingston or later	IdentityIQServiceNowServiceCatalog.v1.2.2.xml

2. Import relevant update set in ServiceNow instance. For more information and guidelines on usage of the update set, refer to the following wiki link:
http://wiki.servicenow.com/index.php?title=Saving_Customizations_in_a_Single_XML_File
In the above link, refer to section 3 “Loading Customizations from a Single XML File”.
After successfully applying the update set in ServiceNow the **IdentityIQ for ServiceNow Catalog** application is created.
3. After committing the update set for IdentityIQ for ServiceNow Catalog, add read operation ACLs on **sys-log_app_scope** and **sys_script_include** tables as mentioned in the following steps:
 - a. Login to ServiceNow instance with administrator credentials.
 - b. Ensure that, the **Global** application is selected.
 - c. Create wildcard field rules (*) ACL for **syslog_app_scope** table for Read operation with required **x_sapo_iiq_catalog.spnt_admin** role.
 - d. Create wildcard field rules (*) ACL for **sys_script_include** table for Read operation with required **x_sapo_iiq_catalog.spnt_admin** role.

Overview “SailPoint IdentityIQ ServiceNow Catalog Integration” Application

The IdentityIQ ServiceNow Catalog Integration provides easy access to IdentityIQ Services, Access Requests and Access Approvals.

Note: The IdentityIQ for ServiceNow Catalog application is available only to those users who have the **x_sapo_iiq_catalog.spnt_user** role assigned.

1. My Access Requests
 - Displays a list of access requests which include the Access Requests Opened By or Requests for the current user logged in.
 - By clicking into the IdentityIQ request, a user can see the Request information, as well as all of the Request Items with a brief description of what the Request Item entailed.
 - By clicking on the **View Detail** button a user can view the details of this Request in IdentityIQ.
2. My Access Approvals
 - Allows user to view the pending approvals in IdentityIQ for the logged in user. In addition to this, the module shows number of pending approvals for the logged in user with count next to link.
 - The **My Access Approvals** link does not display the number of pending approvals on ServiceNow Kingston or later version.
3. Request Access for Me
 - Allows user to request application access.
 - The **Request Access for Me** directly links to the request access page, allowing currently logged in user to request entitlements and roles.

4. Request Access for Others

- The **Request Access for Others** link displays a dialog box so that the current user can select a different user to request access on their behalf. Once a user is selected, this links to the request access page.

Note: The “Request Access for Others” requires either the ServiceNow `admin` or the `x_sapo_iiq_catalog.spnt_manager` role to display.
The above role is the custom role created to give to managers of other users from IdentityIQ in ServiceNow.

5. Change Password

- Manages password for different accounts managed in IdentityIQ.
- The **Change Password** link directs the link to the logged in users to manage the passwords in IdentityIQ.

6. Manage Accounts for Me

- The **Manage Accounts for Me** opens the manage accounts page in IdentityIQ.

7. Track My Request

- Allows user to check status regarding a recent access request.
- Track My Requests opens the Access Request page in IdentityIQ.

8. Properties

- Provides the form for logging in to the IdentityIQ API and performing a REST request to the MID SERVER and writing debug inform action to the Log.

9. Logs

- Allows to view debugging, error and general information messages as they are written to the Log.

10. Customer Support

- Allows the user to navigate to a support page located at Customer Support.

Mid server installation

For an overview and installation instructions on setting up the mid server, see the following ServiceNow wiki:

http://wiki.servicenow.com/index.php?title=MID_Server

For Kingston or later version has an additional installation step of mid server validation. For more information, see the following ServiceNow wiki:

https://docs.servicenow.com/bundle/kingston-servicenow-platform/page/product/mid-server/concept/c_MIDServerInstallation.html

Configuration

Set “IdentityIQ for ServiceNow Catalog” Application properties in ServiceNow to point to the SailPoint IdentityIQ instance

Open the **Properties** module from **IdentityIQ for ServiceNow Catalog** Application and modify the following properties:

Note: The properties module from IdentityIQ for ServiceNow Catalog application is available only to those user who have the `x_sapo_iiq_catalog.spnt_admin` role in ServiceNow.

- **Use Single-Sign On for IdentityIQ Requests:** Determines whether SailPoint IdentityIQ is setup for Single Sign On.
 - True: ServiceNow assumes no authentication is required when opening direct links into IdentityIQ.
 - False: ServiceNow uses the `remoteLogin` web service to retrieve a one-time use authentication token to login the current user.
- **IdentityIQ Instance Endpoint URL:** URL specifying the SailPoint IdentityIQ endpoint.
- **User to login to the IdentityIQ API:** Username for authentication during REST Requests to IdentityIQ.

Note: This user must have **WebServices Executor Permission** in IdentityIQ.

- **Password to login to the IdentityIQ API:** Password for authenticating during REST Requests to IdentityIQ.
- **Mid Server to use to make REST requests to IdentityIQ:** The name of the Mid Server to make REST Requests through to IdentityIQ.
- **IdentityIQ Log Level:** The IdentityIQ for ServiceNow Catalog application's properties module contains the following new properties related to logger:
 - Logging Level: The default value for this property is **warn**.
 - Logging Destination: The default value for this property is **DB**.

If **DB** is selected, then logs will be transformed to system tables.

If **FILE** is selected, then logs will be transformed to system node files.

- **Interval in which to poll for approvals:** Identifies the interval in which the approvals on the server side are verified. Default: 15 minutes.
If the IdentityIQ Approval record for the user logged in has not been updated within 15 minutes, the user is logged out to IdentityIQ to request an update of the number of approvals outstanding.
- **Application Name within IdentityIQ for the ServiceNow Integration:** Application Name within IdentityIQ for the ServiceNow Integration. Default: `SailPointServiceCatalog`
- **IdentityIQ ServiceNow Application Name:** ServiceNow users are aggregated in IdentityIQ through ServiceNow connector application.
- **ServiceNow username for Ticket creation:** The username used to create ticket in ServiceNow as configured in the `SailPointServiceCatalog` ticketing application.

Mid server Setup

The Mid Server must be setup with a polling time lower than normal. This allows the shortest lag time when loading IdentityIQ pages when ServiceNow must request a `remoteLogin` token.

MID Server poll time: Sets the MID Server polling interval (in seconds).

Type: integer (seconds)

Default value: 15

`mid.poll.time`

Note: It is suggested to set the "MID Server poll time" property to 5 seconds, to increase the rate in which REST Message Requests will be picked up and processed.

Note: ServiceNow and IdentityIQ instance must be accessible to Mid-server.

Configuration in SailPoint IdentityIQ

Perform the following procedure to create Application in IdentityIQ to manipulate Tickets in ServiceNow:

1. Create **SailPointServiceCatalog** ticketing application using default configuration file located in `iiqHome/WEB-INF/config/SailPointServiceCatalog.xml` directory.
In the above directory, *iiqHome* is the location where IdentityIQ is installed.
This creates **SailPointServiceCatalogIntegration** rule in IdentityIQ.
2. Modify the following parameters:
 - **url**: Service Now JSON API endpoint

`https://<servicenow-base-url>/x_sapo_iiq_catalog_processor.do?action=POST`
 - **username**: ServiceNow user who has `x_sapo_iiq_catalog.spnt_admin` role
 - **password**: Password of the ServiceNow user
3. Modify the following parameter in the **SailPointServiceCatalogIntegration** rule:
 - **connectorAppName**: Provide the ServiceNow connector application name through which ServiceNow users are aggregated in IdentityIQ. The value for this parameter must be the name of the Connector Application pointing to ServiceNow instance where ServiceNow Catalog Integration is configured. Default value is **null**

Note: - If the rule name is changed in Step 1. then change the value for `ticketDataGenerationRule` entry in `SailPointServiceCatalog.xml` file.
- If Application Name is changed in SailPoint Identity Access Request Application properties then change name in `SailPointServiceCatalog.xml` file.
4. Enable **iFrame** option in IdentityIQ by performing the following steps:
 - a. Navigate to IdentityIQ debug page.
 - b. Select **System Configuration** from **Configuration Objects**.
 - c. Find the key **allowiFrame** and set the value to **true**.
 - d. Save the **System Configuration**.

Troubleshooting

1 - Enable Traces for IdentityIQ for ServiceNow Catalog application in ServiceNow

Resolution: To enable the traces in IdentityIQ for ServiceNow Catalog application set the following property to debug:

Logging Level (`x_sapo_iiq_catalog.logging.verbosity`)

2 - Enable Stack Tracing for IdentityIQ

Resolution: Set the workflow **Trace** attribute to **true** when configuring the ServiceNow Catalog Integration application parameters to enable logging. This enables any IdentityIQ provisioning actions traceable.

Chapter 8: IdentityIQ for ServiceNow Catalog API

The following topics are discussed in this chapter:

Overview	85
Supported features	86
Supported platforms	86
Pre-requisites	86
Installation and configuration in ServiceNow	86
Configuration in SailPoint IdentityIQ	89
Troubleshooting	90

Overview

IdentityIQ for ServiceNow Catalog API is an integration between ServiceNow and SailPoint IdentityIQ. This integration allows access request for roles using Service Catalog approach with ServiceNow UI experience.

The integration between SailPoint and ServiceNow gives mutual customers a complementary identity access governance and service management solution that works together to ensure strong controls are in place to meet ever stringent security and compliance requirements around user access to sensitive applications.

The chapter describe the implementation approach and configuration of the IdentityIQ for ServiceNow Catalog API. The following information enables administrators to deploy and maintain the integration.

The flow of IdentityIQ for ServiceNow Catalog API in ServiceNow to request the SailPoint roles is as follows:

- User logs in to ServiceNow Service Portal (for example, https://<your_instance>.service-now.com/sp).
- User opens the Service Catalog and selects the **SailPoint Catalog Access Request** item.
- User selects a user if he/she is requesting on someone else's behalf, or user selects self-service.
- User clicks the **Check Access** button. This populates the available roles and assigned roles buckets with role names.
- User assigns/revokes roles and clicks on Submit. This generates the Service Request tickets in the ServiceNow and its corresponding access request in the IdentityIQ.

Note: Number of tickets equals to the number of roles selected by the user while requesting access. Also, a provisioning request is generated in the SailPoint IdentityIQ for each role selected by the user. Initially the status of each ServiceNow ticket would be 'Pending Approval'.

- Once the access request is approved in IdentityIQ, depending on how that access request progresses, the ServiceNow ticket's status would be updated back automatically in ServiceNow.
- Once the provisioning of request is done on IdentityIQ side, the ticket's status would be updated (closed) in ServiceNow.

Note: This integration does not support 'Add to Cart' functionality of Service Catalog. Use only submit.

Supported features

The IdentityIQ for ServiceNow Catalog API enables the use of IdentityIQ Lifecycle Manager within ServiceNow user interfaces. The inclusion of the IdentityIQ for ServiceNow Catalog API Application provides the following functionality within ServiceNow:

- **Request for roles through Service Catalog:** Brings IdentityIQ roles as a service which is a request able item in Service Catalog
- **My Access Requests:** List of access requests which include the Access Requests Opened By or Requests for the current user logged in.

Supported platforms

IdentityIQ for ServiceNow Catalog API supports the following ServiceNow releases:

- Madrid
- London
- Kingston

Pre-requisites

- For the integration to successfully authenticate the user, the ServiceNow accounts (users) must have correlated identities in IdentityIQ.
- ServiceNow Mid Server must be installed. See “Mid server installation” on page 87.

Note: SailPoint recommends that the WebServer hosting IdentityIQ must be TLS enabled.

Installation and configuration in ServiceNow

This section describes the installation and configuration procedures for SailPoint ServiceNow Service Catalog API Integration.

Following role on ServiceNow can be assigned to the user:

- **x_sap_servcat_api.admin:** The user with this role has access to the integration application on ServiceNow platform.

Installation

This section describes the installation procedure.

Install update set in ServiceNow

Apply the IdentityIQ for ServiceNow Catalog API Integration update set:

1. Copy the relevant update set from the following directory to a temporary directory:
`identityiq-releaseVersion.zip\integration\servicenow\iiqIntegration-ServiceNow.zip\ServiceCatalogUpdateSet\SailPointServiceCatalog.v1.1.0.xml`

In the above directory, *releaseVersion* is the version of the current IdentityIQ release.

2. Import relevant update set in ServiceNow instance. For more information and guidelines on usage of the update set, refer to the following wiki link:
https://docs.servicenow.com/bundle/Kingston-application-development/page/build/system-update-sets/task/t_SaveAnUpdateSetAsAnXMLFile.html?title=Saving_Customizations_in_a_Single_XML_File#ari-aid-title2.
 After successfully applying the update set in ServiceNow the **IdentityIQ for ServiceNow Catalog API** application is created.
3. After committing the update set for IdentityIQ for ServiceNow Catalog API, add read operation ACLs on **syslog_app_scope** and **sys_script_include** tables as mentioned in the following steps:
 - a. Login to ServiceNow instance with administrator credentials.
 - b. Ensure that, the **Global** application is selected.
 - c. Create wildcard field rules (*) ACL for **syslog_app_scope** table for Read operation with required **x_sap_servcat_api.admin** role.
 - d. Create wildcard field rules (*) ACL for **sys_script_include** table for Read operation with required **x_sap_servcat_api.admin** role.

Overview “IdentityIQ for ServiceNow Catalog API” Application

The IdentityIQ for ServiceNow Catalog API provides easy access to Role Access Requests.

Note: The IdentityIQ for ServiceNow Catalog API application is available only to those users who have the **x_sap_servcat_api.admin** role assigned.

Following are the modules present in the application on ServiceNow:

1. My Access Requests
 - Displays a list of access requests which include the Access Requests Opened By or Requests for the current user logged in.
 - By clicking into the IdentityIQ request, a user can see the Request information, as well as all of the Request Items with a brief description of what the Request Item entailed.
2. Properties
 - Application Configuration page
3. Logs
 - Allows to view debugging, error and general information messages as they are written to the Log.
4. Customer Support
 - Allows the user to navigate to a support page located at Customer Support.

Mid server installation

For an overview and installation instructions on setting up the mid server, see the following ServiceNow wiki:

https://docs.servicenow.com/bundle/kingston-servicenow-platform/page/product/mid-server/concept/c_MIDServerInstallation.html

The Mid server must be setup with a polling time less than the normal time. This allows the shortest lag time when sending a REST request from ServiceNow to SailPoint IdentityIQ.

MID Server poll time: Sets the MID Server polling interval (in seconds) using **mid.poll.time**

Type: integer (seconds)

Default value: 40

Configuration

Set “IdentityIQ for ServiceNow Catalog API” Application properties in ServiceNow to point to the SailPoint IdentityIQ instance

Open the **Properties** module from **IdentityIQ for ServiceNow Catalog API** application and modify the following properties:

Note: The properties module from IdentityIQ for ServiceNow Catalog API application is available only to those user who have the `x_sap_servcat_api.admin` role in ServiceNow. To configure properties, change the application scope to 'IdentityIQ for ServiceNow Catalog API'

Properties	Description
URL to connect to SailPoint instance	URL specifying the SailPoint IdentityIQ endpoint.
Authentication type	<ul style="list-style-type: none"> Basic: Username/Password would be used for the authentication. OAuth 2.0: Client Id/Client Secret would be used for the authentication. <p>Note: For more information on creating OAuth 2.0 client credentials, see <i>SailPoint IdentityIQ Administration Guide</i>.</p>
Client id	<p>The Client id for the OAuth 2.0 authentication.</p> <p>Note: IdentityIQ supports the use of OAuth 2.0 (client credentials) for API authentication. Set up a proxy user that connects on behalf of the user. This proxy user must have SCIM Executor Permission in IdentityIQ.</p>
Client Secret	The Client secret for OAuth 2.0 authentication.
User to login to the SailPoint instance	<p>Username for authentication during REST Requests to SailPoint IdentityIQ.</p> <p>Note: This user must have SCIM Executor Permission in IdentityIQ.</p>
Password to authenticate on SailPoint instance	Password for authenticating during REST Requests to SailPoint IdentityIQ.
MID server name	The name of the Mid Server to make REST Requests through to SailPoint IdentityIQ.
Involved SailPoint Roles	<p>Role types to request or remove. Different role types can be requested and should be separated by comma (,).</p> <p>Default: it, business</p>
Name of the application or source in the SailPoint instance that manages ServiceNow accounts	Name of the application in the SailPoint instance that manages ServiceNow accounts.

Properties	Description
Page size of each data set when querying over large number of Role objects	Page size of each data set when querying over large number of Role objects. Default: 1000
Name of the application or source in the SailPoint instance that handles ticket requests	Name of the application in the SailPoint instance that handles ticket requests. Default: servicenow-ticket-management-app
SailPoint Request Access business process name	SailPoint Request Access business process name. Default: LCM Provisioning
Use SailPoint approval model	Default: Yes
Logging level	Logging level. Default: Error

Configuration in SailPoint IdentityIQ

Perform the following procedure to create Application in IdentityIQ to update back Tickets in ServiceNow:

1. Create ticket management application in IdentityIQ using default configuration file located in `iiqHome/WEB-INF/config/ServiceNowServiceCatalogAPIIntegration.xml` directory. In the above directory, `iiqHome` is the location where IdentityIQ is installed.

This creates the application **`servicenow-ticket-management-app`** and the **`servicenow-ticket-plan-generator`** rule in IdentityIQ.

2. Modify the following parameters:
 - **url:** Service Now API endpoint
`https://<servicenow-base-url>/api/x_sap_servcat_api/iam/update_ticket`
 - **username:** ServiceNow user who has `import_transformer` role
 - **password:** Password of the ServiceNow user

Status Maps

To map the various status of IdentityIQ to its counterpart status on ServiceNow, following are the status maps available in IdentityIQ ticket management application:

Status maps	Description
requestStateMap	Mapping between Access Request state in IdentityIQ and Request state of Service Request (REQ) in ServiceNow.
approvalStateMap	Mapping between Access Request Approval state in IdentityIQ and Approval of Requested Item (RITM) in ServiceNow.

Status maps	Description
provisioningStateMap	Mapping between Access Request Provisioning state in IdentityIQ and Provisioning State of Requested Item (RITM) in ServiceNow.

Troubleshooting

1 - Enable Traces for IdentityIQ for ServiceNow Catalog API application in ServiceNow

Resolution: To enable the traces in IdentityIQ for ServiceNow Catalog API application, set the following property to debug:

Logging Level (`x_sap_servcat_api.logging.verbosity`)

2 - Enable Stack Tracing for IdentityIQ

Resolution: Set the workflow **Trace** attribute to **true** when configuring the IdentityIQ for ServiceNow Catalog API application parameters to enable logging. This enables any IdentityIQ provisioning actions traceable.

3 - SailPoint Catalog Access Request item is not visible in the Service Catalog on ServiceNow

Resolution: OOTB item is a part of Service Catalog but is not organized in any Service Catalog Category. Create a new Service Catalog Category and add the OOTB catalog item to this new category. For more information on creating the category, see

https://docs.servicenow.com/bundle/london-it-service-management/page/product/service-catalog-management/task/t_CreateACategory.html

4 - Notification covers the whole page when item is requested for the first time

Resolution: No resolution required. This is a one-time activity. ServiceNow adds the required Cross scope privileges to the application.

5 - Unable to retrieve roles on check access click

The following error message is displayed when the check access is clicked and roles are not retrieved:

```
SailPointCatalogRESTClient - executeRequest - Error in executing request: [Method failed: (/identityiq/scim/v2/Accounts) with code: 404]
```

Resolution: Ensure that the URL to connect to SailPoint instance in the Properties does not end with a / (slash).

6 - Roles cannot be dragged across slush-buckets for an instance of ServiceNow Madrid release

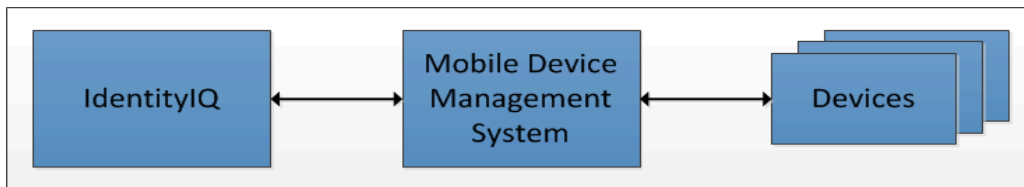
Resolution: Perform the following steps on ServiceNow Madrid release:

1. Navigate to Service Portal ==> Widgets option and go to the SailPoint custom widget **catalog_access_request**.
2. Open the **catalog_access_request** widget and navigate to the dependency section click on the edit tab to provide require widget dependency.

3. Search for **ng-sortable-1.3.4** dependency in collection slush bucket and move it to the right side bucket.
4. Save the changes.

Enterprise Mobility Management Infrastructure Modules

Enterprise Mobility Management Infrastructure Modules (EMM) manages Devices enrolled in Mobile Device Management (MDM) System. EMM also manages Users/Administrators of MDM System. Following is an architecture diagram of EMM:



MDM systems import users from a central directory server or maintains its own repository. Operations to be performed on devices are sent to the respective MDM System which then performs the specified action on the target device. EMM does not communicate with the devices directly.

EMM uses two separate applications to manage users and devices. Main EMM application manages users in the MDM System and the proxy EMM application manages devices in the MDM System. In some cases there is one application which manages devices.

This section contains information on the following:

- "IdentityIQ for AirWatch Enterprise Mobility Management"
- "IdentityIQ for MobileIron Enterprise Mobility Management"
- "IdentityIQ for Good Technologies Enterprise Mobility Management"

Chapter 9: IdentityIQ for AirWatch Enterprise Mobility Management

The following topics are discussed in this chapter:

Overview	93
Supported features	93
Supported platforms	94
Pre-requisites	94
Configuration	94
Application configuration	95
Operation specific configuration	95

Overview

This document provides a guide to the AirWatch Enterprise Mobility Management (EMM) integration and configuration for your enterprise.

Using this integration, IdentityIQ can retrieve the devices managed by AirWatch, perform operations on them, and manage AirWatch's user account. These entities are managed in IdentityIQ using separate applications named as follows:

- AirWatch Enterprise Mobility Management (EMM) Application (referred to as User Application in this document) for managing AirWatch user accounts
- Device Application (containing the prefix **-Devices**) is created by IdentityIQ during aggregation and is used for managing devices.

Supported features

The AirWatch EMM Infrastructure Module supports the following features:

- Account Management
 - Account Aggregation on the user application to bring in AirWatch user accounts
 - Account Aggregation on the device application to bring in devices managed in AirWatch EMM
 - Delete, Unlock devices

The following table represents what each of the above operation implies to IdentityIQ and AirWatch EMM:

Supported platforms

IdentityIQ operation	Resulting change on AirWatch
Account aggregation on user application	The AirWatch user accounts are brought into IdentityIQ.
Account aggregation on device application	The devices that are managed by the AirWatch EMM are retrieved into IdentityIQ.
Delete account for AirWatch device application	Enterprise/Device Wipe and Delete device is triggered on the device via AirWatch EMM system. For more information, see “Operation specific configuration” on page 95.
Unlock account for AirWatch device application	Unlock device is triggered on the device via AirWatch EMM system.
Adding entitlements to account	Adding profiles to device from AirWatch system.
Deleting entitlements from account	Removing profiles from AirWatch system.

- Account - Group Management
 - Device Group Aggregation where device profiles are addressed as groups.
 - Add and remove entitlement (profile) from device.

Supported platforms

IdentityIQ for AirWatch EMM Infrastructure Module supports the following version of AirWatch:

- AirWatch API version 9.5.0.16 and above

Pre-requisites

Administrator user configured for AirWatch EMM Application must have the following role for provisioning activities:

- REST API Devices Read
- REST API Devices Write
- REST API Devices Execute
- REST API Devices Delete
- REST API Devices Advanced

Note: If AirWatch EMM application is behind proxy server, see the “Special Java Considerations” section of the *SailPoint IdentityIQ Installation Guide*.

Configuration

This section describes the application and additional operation specific configurations.

Application configuration

To create an application in IdentityIQ for AirWatch the following parameters are required:

Parameters	Description
Application Type	AirWatch EMM (Enterprise Mobility Management Infrastructure Module).
AirWatch Server	AirWatch server URL where it's REST API are accessible. For example, https://apidev-as.awmdm.com .
AirWatch Administrator	Administrator of AirWatch server.
AirWatch Administrator Password	Password of the administrator.
API Key	AirWatch server's API key defined for REST API.

Operation specific configuration

This section describes the various configurations required for the following operations:

- Aggregation
- Provisioning

Aggregation

- **Aggregation of devices:** Before aggregating devices against the device application create a correlation rule in the device application to map devices to its AirWatch user. For example, **UserName** is an attribute of the device which specifies the name of the user it belongs to, and **Display Name** of the identity is also **UserName**. So in correlation rule specify application attribute as **UserName** and Identity attribute as **Display Name**.
- **Parameterized device aggregation:** By default AirWatch device aggregation retrieves device profiles and device applications. If you do not want to manage these entities, you can filter them for not being retrieved into IdentityIQ.

The following configurable parameters impact aggregation:

- **aggregateDeviceProfile:** (is an application attribute on AirWatch EMM application) determines if the profiles connected to devices are to be retrieved or not. The default behavior is to retrieve the profiles connected to the devices. To change this behavior, set the following value through the debug pages:

```
<entry key="aggregateDeviceProfile" value="false"/>
```

- **aggregateDeviceApp:** (is an application attribute on AirWatch EMM Application) determines if the application installed on devices must be retrieved or not. The default behavior is to retrieve the applications installed on the device. To change this behavior, set the following value through the debug pages:

```
<entry key="aggregateDeviceApp" value="false"/>
```

Configuration

Provisioning

The following provisioning operations are available in IdentityIQ when integrating with AirWatch:

- Delete device

Delete device

- **Delete Device operation from LCM:** In addition to Delete Device, you will be prompted to select **Entire Device Wipe** or **Enterprise Wipe Only** options before deleting the device.
- **Delete Device operation from Certification:** The default wipe operation will be the **Enterprise Wipe Only**. To change this default behavior to **Entire Device Wipe** add the following entry in the application debug of the device application:

```
<entry key="defaultWipeFromCertification" value="Entire Device Wipe"/>
```

Note: If the AirWatch application is already created, update the delete provisioning policy with new field, name as `SecurityPIN` and type as `String`.

Chapter 10: IdentityIQ for MobileIron Enterprise Mobility Management

The following topics are discussed in this chapter:

Overview	97
Supported features	97
Supported platforms	98
Pre-requisites	98
Configuration	98
Application configuration	98
Operation specific configuration	99

Overview

SailPoint IdentityIQ manages MobileIron devices. It does not handle MobileIron users because MobileIron has not provided the supporting User API. It manages these MobileIron entities using the MobileIron REST API's over HTTPS. All the devices are aggregated under MobileIron Enterprise Mobility Management (EMM) Application.

Supported features

The MobileIron EMM provides the ability to provision MobileIron devices from IdentityIQ.

The MobileIron EMM supports the following functions:

- Account Management
 - Device aggregation which include device Attribute, Group Attribute - Labels and Entitlements - Apps, Labels.
 - MobileIron EMM support Create, Delete and unlock operations where Create is Registering a Device, Delete is Retire a Device along with Device Wipe that will wipe all the existing device applications and Unlock means unlocking a device by removing a PIN if Set.
- Account - Group Management
 - Device Group Aggregation where groups are Labels in MobileIron.

The following table displays a comparison between operations from IdentityIQ and resultant operations in MobileIron EMM:

IdentityIQ operation	Resulting change on MobileIron
Account aggregation on MobileIron application	The devices that are managed by the MobileIron EMM are retrieved into IdentityIQ with the label attribute represented as the entitlement for that device.

Supported platforms

IdentityIQ operation	Resulting change on MobileIron
Account group aggregation on MobileIron application	The labels present in the MobileIron EMM are retrieved into IdentityIQ.
Create account of MobileIron application	Registering a device on MobileIron system. For more information, see “Operation specific configuration” on page 99.
Delete account of MobileIron application	Wipe/Retire device is triggered on the device via MobileIron EMM System. For more information, see “Operation specific configuration” on page 99.
Unlock account for MobileIron application	Unlock device is triggered on the device via MobileIron EMM system.
Adding entitlements to account	Adding labels to device from MobileIron EMM system.
Deleting entitlements from account	Removing device labels from MobileIron EMM system.

Supported platforms

IdentityIQ for MobileIron EMM Infrastructure Module supports the following version of MobileIron WebService

- API version for MobileIron WebService 5.7.1

Pre-requisites

Administrator user configured for MobileIron EMM application must have the API role for provisioning activities.

Note: If MobileIron EMM application is behind proxy server, see the “Special Java Considerations” section of the *SailPoint IdentityIQ Installation Guide*.

Configuration

This section describes the application and additional operation specific configurations.

Application configuration

To create an application in IdentityIQ for MobileIron the following parameters are required:

Parameters	Description
Application Type	MobileIron EMM (Enterprise Mobility Management Infrastructure Module).
MobileIron URL	The URL pointing to the MobileIron system.
MobileIron Administrator	Administrator of MobileIron system.
MobileIron Administrator Password	Password of the administrator.

Operation specific configuration

This section describes the various configurations required for the following operations:

- Aggregation
- Provisioning

Aggregation

MobileIron Device Aggregation retrieves all active status devices, their connected Labels and Applications. IdentityIQ manages labels as entitlement.

Default aggregation without importing or selecting **MobileIron MIM Correlation** for the MobileIron MIM application will create identity in IdentityIQ with **model** name attribute of MobileIron.

For example, User Name: SM-T301 Account ID: SM-T301
User Name: iPhone4 Account ID: iPhone4

The **MobileIron MIM Correlation** will display the effect only if identity are already created before account aggregation with same name as of **userDisplayName** attribute of MobileIron.

For example, User Name: slupinson Account ID: SM-T301,
User Name: AJohn Account ID: iPhone4

Select the **MobileIron MIM Correlation** under the Correlation tab.

The **MobileIron MIM Correlation** would be populated only if, the following correlation xml input is imported before running the account aggregation task:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE CorrelationConfig PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<CorrelationConfig name="MobileIron MIM Correlation">
  <AttributeAssignments>
    <Filter operation="EQ" property="displayName" value="userDisplayName"/>
  </AttributeAssignments>
</CorrelationConfig>
```

Provisioning

The following provisioning operations are available in IdentityIQ when integrating with MobileIron:

- Add device
- Delete device

Add device

Default template is present for adding a device (Registering a device to a user). If the user is not present, add a user in the MobileIron system (Local repository) and then assign a device to it.

Note: If new local user is created during “Device Registration” through IdentityIQ then the VSP (MobileIron Server) sets the password for a new local user to the userid.

Configuration

Valid values for the platform attribute in the **Create Device Provisioning policy** are as follows:

- M - Windows Mobile
- B - BlackBerry
- I - iOS
- S - Symbian
- P - Palm webOS
- A - Android
- L - Mac OS X

Delete device

- **Delete Device via LCM:** In delete device operation, in addition to delete device, user is prompted to select one of the following options:
 - **Device Wipe** (Factory data reset): Device wipe wipes all the data from the device and sets it back to the factory setting.
 - **Enterprise Wipe (Retire):** Enterprise Wipe removes the MobileIron Client present on the device.
- **Delete Device via Certification:** When a delete device operation is performed from certification, it does not respect the additional operations **Device Wipe** and **Enterprise Wipe**. Hence, IdentityIQ provides an extra MobileIron application attribute named **defaultWipeFromCertification**. Users have to manually add this attribute in the MobileIron MIM application debug page and provide values as **Device Wipe** or **Enterprise Wipe**.

```
<entry key="defaultWipeFromCertification" value="Device Wipe"/>
```

When deleting a device from IdentityIQ using the Device Wipe option, the operation first wipes the device (Data Reset) and then IdentityIQ waits (sleep) for 5 second (default). After the sleep duration IdentityIQ deletes the device from MobileIron system and changes the status from wiped to retire.

The sleep duration for Wipe operation is a configurable application attribute which can be configured as follows:

```
<entry key="WipeSleepInterval" value="5"/>
```

Chapter 11: IdentityIQ for Good Technologies Enterprise Mobility Management

The following topics are discussed in this chapter:

Overview	101
Supported features	101
Supported platform	102
Pre-requisites	102
Configuration	102
Application configuration	102
Operation specific configuration	103

Overview

This document provides a guide to the Good Technologies Enterprise Mobility Management (EMM) integration and configuration for your enterprise.

Using this integration, IdentityIQ can retrieve the devices managed by Good Technologies and perform few operations on them. In addition, this integration also enables IdentityIQ to manage Good Technologies devices. These entities are managed in IdentityIQ using separate applications, named as follows:

- Good Technologies EMM Application (referred to as User Application in this document) for managing Good Technologies user accounts.
- Device Application (containing the suffix - **Devices**) is created by IdentityIQ during user aggregation and is used for managing devices.

Supported features

The Good Technologies EMM Infrastructure Module supports the following features:

- Account Management
 - Account Aggregation on the user application to bring in Good Technologies role member
 - Device Aggregation on the device application to bring in devices managed in Good Technologies EMM
 - Add, Unlock Delete devices
- Account-Group Management:
 - Account Group Aggregation on the user application to bring in Good Technologies roles
 - Account Group Aggregation on the device application to bring in policy sets managed in Good Technologies EMM
 - Adding/ Removing Entitlement (Policy Set) to device account.

Supported platform

IdentityIQ for Good Technologies Enterprise Mobility Management Infrastructure Module supports the following version of Good Mobile:

- Good Mobile Control version 2.6.4.972

Pre-requisites

Administrator user configured for Good Technologies EMM Application must have the Role with All Rights or following rights for provisioning activities:

- Add handheld for a user
- Add additional handhelds for a user
- Delete handhelds
- Wipe Good for Enterprise app or entire device data
- Reset Good for Enterprise
- Set handheld policy
- View Policy Sets
- Manage policies (handheld and application)
- Manage roles

Configuration

This section describes the application and additional operation specific configurations.

Application configuration

To create an application in IdentityIQ for Good Technologies the following parameters are required:

Parameters	Description
Application Type	Good Technology EMM (Enterprise Mobility Management Infrastructure Module).
Good Technology Hostname	Provide computer name of the GMC server.
Good Technology Port	Provide port number of the GMC Web Service. For example, 19005
Good Technology Username	Administrator of GMC server.
Good Technology Password	Password of the administrator.
Page Size	Page size for aggregating devices.

Operation specific configuration

This section describes the various configurations required for the following operations:

- Aggregation
- Provisioning

Aggregation

Aggregation of devices: Good Technologies device aggregation retrieves all devices, their connected Policy Set and applications on the device. IdentityIQ manages Policy Set as entitlement.

Default aggregation without creating a correlation rule for the Good Technologies Enterprise Mobility Management application will create identity in IdentityIQ with Display Attribute (Device Model by default) of Good Technologies.

For example,

- Name: iPhone 4 (GSM, Rev. A) Account ID: phone 4 (GSM, Rev. A)

The correlation rule will display the effect only if identity is already created before account aggregation with same name as of correlation attribute of Identity.

- Name: "Demo User1" Account ID: iPhone 4 (GSM, Rev. A)

Import the following correlation xml which correlates devices to Identity based on name of a user in Good Technologies and display name of an Identity:

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE CorrelationConfig PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<CorrelationConfig name="Good Technology Device Correlation">
  <AttributeAssignments>
    <Filter operation="EQ" property="displayName" value="Name" />
  </AttributeAssignments>
</CorrelationConfig>
```

Provisioning

The following provisioning operations are available in IdentityIQ when integrating with Good Technologies:

- Add device
- Unlock device
- Delete device

Add device

While adding a device from IdentityIQ, default provisioning policy accepts the following fields:

- **User DN:** DN of a user present in Good Technologies User repository. This is a mandatory field.
- **Messaging Server:** Name of the Good Messaging server. If this field is left blank, IdentityIQ will locate a single GMM server if present. If multiple GMM servers exist, you must provide a value for this field else, the add operation will fail.

Unlock device

While Unlocking device from IdentityIQ, default provisioning policy accepts Unlock Code displayed on the device. Upon successful reset password, temporary unlock code is generated and it will be saved in **Provisioning Request ID** field in Unlock Access Request in IdentityIQ.

Configuration

Delete device

- **Delete Device operation from LCM:** In addition to delete device, you will be prompted to select **Entire Device** or **Enterprise Data Only** options before deleting the device.
- **Delete Device operation from Certification:** The default wipe operation will be the **Enterprise Data Only**. To change this default behavior to **Entire Device** add the following entry in the application debug of the device application:

```
<entry key="defaultWipeFromCertification" value="Entire Device"/>
```

Provisioning Infrastructure Modules

This section contains information on the following sections:

- “IdentityIQ for Oracle Identity Manager”
- “IdentityIQ for IBM Security Identity Manager”

Chapter 12: IdentityIQ for Oracle Identity Manager

The following topics are discussed in this chapter:

Overview	107
Supported features	107
Supported platforms	108
Installing the OIM Integration Web Application	108
Testing the OIM Integration Web Application.	109
Configuration for OIM application	111
Aggregating from OIM.	112
Known/Open issues	112

Overview

This chapter provides a guide to the integration between Oracle Identity Manager (OIM) and IdentityIQ. This chapter is intended for Oracle and IdentityIQ System Administrators and assumes a high degree of technical knowledge.

The integration is achieved by deploying a small web application in the application server that hosts OIM. IdentityIQ communicates with the web services contained in this application to read and write account information. Configuration of the OIM integration requires the username and password of the OIM administrator or another user with sufficient permissions.

Supported features

The IdentityIQ for Oracle Identity Manager supports the following functions:

- Account Management
 - Oracle Identity Manager user aggregation along with the connected child accounts and application
 - Create, Update, Delete
 - Enable, Disable, Unlock
 - Add/Remove Entitlements operations for Oracle Identity Manager connected child accounts
- User Management
 - Manages Oracle Identity Manager Users as Accounts
 - Create, Update, Delete
 - Enable, Disable, Unlock
 - Add/Remove Entitlements operations for Oracle Identity Manager Users

Supported platforms

IdentityIQ for Oracle Identity Manager supports the following versions of Oracle Identity Manager:

- Oracle Identity Manager 11g R2
- Oracle Identity Manager 11g R1

Installing the OIM Integration Web Application

You must first deploy the OIM Integration Servlet web application to the application server hosting the OIM application. The `iiq.war` file for this web application is contained in the IdentityIQ distribution as `$INSTALLDIR/integration/OIM/iiqIntegration-OIM.jar` or in the distribution for an IdentityIQ patch in a `.jar` file named `Integration-oim-<version>.jar`.

The `iiqIntegration-OIM.jar` file contains `iiq.war` file. You can customize the `iiq.war` file in many ways before being deployed into the application server hosting OIM.

Note: Ensure that if you are deploying web application as war file, it should be named as `iiq.war`. If you are deploying the web application from a directory, then directory must be named as `iiq`.

Following are the required customization steps:

1. Configure access to OIM by modifying `WEB-INF/classes/xellerate.properties` to set.
 - **XL.HomeDir:** the full path to the directory where OIM is installed
 - **userName:** the OIM administrator that has the appropriate permission to read and write user and account data
 - **password:** the password for the OIM administratorFor more information on the other properties that need to be set in `xellerate.properties` file, see “Properties that can be defined in `xellerate.properties`” on page 110.
2. Copy `OIM_ORACLE_HOME/designconsole/lib/oimclient.jar` API implementation file from the OIM installation into the `WEB-INF/lib` directory of the integration application.

Authentication for Web Application

Note: By default deployed Web application (`iiq.war`) in the application server (Weblogic) does not support authentication.

The Oracle Identity Manager application provides support for authenticating the IdentityIQ Web Application deployed on the Weblogic Server.

Following are the required customization steps for supporting authentication for Web Application:

1. Provide **Username** and **Password** in the Oracle Identity Manager application through debug page. The Username and Password must be one of the user configured in the Application server (Weblogic), where the Web Application (`iiq.war`) is deployed.
User can be found at Weblogic Application Server console: **Security Realms ==> myrealm ==>Users and Groups**.

For example:

```
<entry key="username" value="weblogic1"/>
<entry key="password" value="Sailpoint"/>
```

Note: The password would be encrypted once user saves the application.

2. Update the existing `xellerate.properties` file by providing the new parameters (**localUser** and **localPassword**) as follows:

```
#localUser=admin
#localPassword=Sailpoint
```

The **localUser** and **localPassword** properties are used for authentication:

- End User is expected to provide user and password of application server (Weblogic)
- User can be found at Weblogic Application Server console: **Security Realms ==> myrealm ==>Users and Groups**

3. For setting the authentication, update the `web.xml` file as follows:

```
<web-app>
  <display-name>OIM Service</display-name>
  <servlet>
    <servlet-name>OIM REST Servlet</servlet-name>
    <servlet-class>sailpoint.integration.oim.OIMRestServlet</servlet-class>
    <init-param>
      <param-name>handler</param-name>
      <param-value>sailpoint.integration.oim.OIMIntegration</param-value>
    </init-param>
    <init-param>
      <param-name>authenticator</param-name>
      <param-value>sailpoint.integration.oim.OIMBasicAuthenticator</param-value>
    </init-param>

    <!-- Add this if you want to no authentication
    <init-param>
      <param-name>noAuthentication</param-name>
      <param-value>true</param-value>
    </init-param> -->

  </servlet>
  <servlet-mapping>
    <servlet-name>OIM REST Servlet</servlet-name>
    <url-pattern>/resources/*</url-pattern>
  </servlet-mapping>
</web-app>
```

Testing the OIM Integration Web Application

Verify if the installation was successful using the following steps:

Note: For each test URL throughout this document, change the host name and port to match your OIM Server instance.

1. From any browser enter the following URL:
<http://localhost:8080/iiq/resources/ping>

The following response is displayed:

Testing the OIM Integration Web Application

OIM integration ready

Failure to get a ping response indicates a problem with the deployment of the Servlet.

2. Verify the integration Servlet can communicate with OIM by entering the following URL:

<http://localhost:8080/iiq/resources/users>

You should see a response containing the names of all OIM users. This might take a while to assemble depending on the number of users. To view details of a particular user, enter the following URL where <OIMUSER> is the name of a user in your OIM instance:

<http://localhost:8080/iiq/resources/user/<OIMUSER>>

To see additional diagnostic information for a particular user, enter the following URL where <OIMUSER> is the name of a user in your OIM instance:

<http://localhost:8080/iiq/resources/debug/<OIMUSER>>

If you are unable to request user information, there may be a problem with the credentials you entered in the `xellerate.properties` file. For more information, see “Properties that can be defined in `xellerate.properties`” on page 110.

Properties that can be defined in `xellerate.properties`

1. Add a ManagedResource definition in the ManagedResource list for an each OIM resource. For each resource, define a property prefix by adding a property whose name is the prefix and whose value is the OIM resource name.

For example:

AD=AD User

Oracle=Oracle DB User

This declares that any property that begins with ERP is related to the OIM resource named ERP Central Component.

2. For each ManagedResource, define the account attribute that represents the unique account identifier. The names used here must be the resource names used by OIM. The identityAttribute must have the internal form field name containing the account identifier. Use the OIM Design Console application to find the process form for each resource and view the field names. The example below gives two typical names, one used by the connector for Oracle database users and the other for the Active Directory connector.

`AD.id=UD_ADUSER_UID`

`Oracle.id=UD_DB_ORA_U_USERNAME`

3. Define the names of the child forms that support multiple attributes. The value is a CSV of the internal child form names:

`AD.childForms=UD_ADUSRC`

`Oracle.childForms=UD_DB_ORA_R`

In this example UD_ADUSRC is the internal name for the child form AD User Group Details and UD_DB_ORA_R is the internal name for the child form DBUM Grant/Revoke Roles.

4. Each child form name in the Oracle.childForms property there is another property whose value is a CSV of the child form fields to return and the order in which they will appear in IdentityIQ.

`Oracle.UD_DB_ORA_R=UD_DB_ORA_R_ROLE,UD_DB_ORA_R_ADMIN_OPTION`

In the previous example, we will return two fields from the child form UD_DB_ORA_R. The first field has the Role name and the second has the Role Admin option.

5. Following is the configuration for resource with child forms: ERP Central Component:

```

ERP=ERP Central Component
ERP.id=UD_ECC_USER_ID
ERP.childForms=UD_ECC_PRO,UD_ECCRL
ERP.UD_ECC_PRO=UD_ECC_PRO_SYSTEMNAME,UD_ECC_PRO_USERPROFILE
ERP.UD_ECCRL=UD_ECCRL_SYSTEMNAME,UD_ECCRL_USERROLE

```

Note: Before **IdentityIQ 6.0** there was a parameter in **xelerate.properties** file as **oldChildFormNames** which was used for the resources who have only one field in the childform, for example, Active Directory resource. For **IdentityIQ** version 6.0 onwards, the value must be set to true if the user wants to support **oldChildFormNames** where field returned would be form name + field name (For example, **UD_ADUSRC:UD_ADUSRC_GROUPNAME** field in Active directory).

6. To aggregate all the active and disabled OIM users in IdentityIQ, add a new parameter **OIM_USER_TYPE** in **xelerate.properties** file with the value as **ALL**. If **OIM_USER_TYPE** parameter is deleted from the **xelerate.properties** file then only the active OIM users will be aggregated. By default only active OIM user are aggregated.

Configuration for OIM application

Perform the following steps to create an IdentityIQ application for OIM:

1. Navigate to the IdentityIQ **Define=>Application** page.
2. Create a new application of type **Oracle Identity Manager**.
3. On the Attributes tab, enter the Oracle Identity Manager Host and Oracle Identity Manager Port.
4. Click **Test Connection** to verify the connection to OIM.

Note: You can make use of the “OIM Application creator” task to discover all the resources present in OIM environment. The input for this task would be an newly created application of type “Oracle Identity Manager” and executing this task would result in the creation of all multiplexed resources.

Testing the OIM Integration Client

While any IdentityIQ feature that generates a provisioning request such as a certification remediation, a role assignment, or a Lifecycle Manager request can be used to test the integration, it is sometimes useful to test at the provisioning layer using the IdentityIQ integration console.

Launch the console by using the IdentityIQ script in the `INSTALLDIR/WEB-INF/bin` directory of the IdentityIQ installation to run `iiq integration`.

From the console command prompt, use the **list** command to display the names of all Application objects created in the system. Using the example in the previous section, verify an Application object of type **Oracle Identity Manager** exists.

Use the following command:

```
use OIMApplicationName
```

Use the **ping** command to initiate a test connection message with OIM. A successful connection will return the following message:

```
Response: Connection test successful
```

Aggregating from OIM

If any problem occurs in the communication of this application with the OIM Integration Web Application, troubleshoot this application by viewing the application server logs for both the IdentityIQ and OIM application servers. You can enable `log4j` tracing on both sides by using the following:

```
log4j.logger.sailpoint.integration=debug
log4j.logger.sailpoint.connector=debug
```

This lets you see if the requests are transmitting over the network, and how they are processed.

If the OIM servlet is deployed on Weblogic 11g, tracing can be enabled on it by adding an entry to the logging file on the Weblogic server. Following is the logging file:

```
<DOMAIN_HOME>/config/fmwconfig/servers/oim_server1/logging.xml
```

Following is the entry that needs to be added:

```
<logger name="SailPoint.integration.oim" level="TRACE:32"/>
```

For more information on enabling system logging in OIM is included in the *Oracle Identity Manager Administrator Guide*.

Aggregating from OIM

To aggregate OIM users and resource accounts, create and execute an IdentityIQ Account Aggregation task. Include the OIM application in the applications to scan list.

When the aggregation is complete from the OIM application, a new application is created for every resource in OIM. The application schema includes attributes seen in the resource accounts. All users in OIM have an account created that is associated with the OIM application and includes all of the standard and extended user attributes of those users. Additionally, all of the resource accounts are aggregated and associated with the newly created applications.

Once the initial aggregation from the OIM application is completed, you can aggregate from it again to read in information for all managed systems.

Note: You can make use of the “OIM Application Creator task” to discover all of the Resources present in the OIM environment. The input for this task is an application of type Oracle Identity Manager. Executing this task results in the creation of all multiplexed Resource applications.

Known/Open issues

Following is the known/open issue of Oracle Identity Manager:

- You cannot perform provisioning operations simultaneously on the OIM server from IdentityIQ and the OIM console. This is a class loading issue observed with OIM 11g, after deploying `iiq` servlet (`iiq.war`) on Weblogic OIM Managed Server.

Workaround for this issue: Create another, empty WLS(Weblogic)Managed server next to the OIM Managed Server and only deploy the IIQ Servlet. Also, update the `Xellerate.properties` file by un-commenting the attribute `java.naming.provider.url`. This Url needs the host name of the host where OIM managed server is deployed and the listening port of the OIM managed server.

- Create OIM user and Update OIM user operations are not working with Oracle Identity Manager 11g R2.

Chapter 13: IdentityIQ for IBM Security Identity Manager

The following topics are discussed in this chapter:

Overview	113
Supported features	113
Supported platforms	114
General configuration	114
Configuration for Aggregation	114
Configuration for Provisioning	114
Troubleshooting	116

Overview

This chapter is designed to provide the necessary procedures, configuration steps, and general product guidelines to successfully integrate IBM Security® Identity Manager (ISIM) into your IdentityIQ production environment.

This chapter is intended for ISIM and IdentityIQ System Administrators and assumes a high degree of technical knowledge of these systems.

Note: Consider the terminologies ISIM and ITIM to be the same throughout the document.

Supported features

The IdentityIQ for IBM Security Identity Manager provides the ability to provision Target Application accounts from IdentityIQ.

The IdentityIQ for IBM Security Identity Manager supports the following functions:

- User Management
 - Manages IBM Security Identity Manager Users as Accounts
 - Aggregating Users
- Target Application Accounts Management
 - Manages Target Application Accounts as Accounts
 - Aggregating Target Accounts directly
 - Create, Update, Delete
 - Enable, Disable, Reset Password

Supported platforms

IdentityIQ for IBM Security Identity Manager supports version 6.0 of IBM Security Identity Manager.

General configuration

The installation steps for ISIM integrations vary based on the functions you wish to perform. IdentityIQ in conjunction with ISIM allows the following functionality:

- Aggregation
- Provisioning Entitlements in ISIM

Configuration for Aggregation

Aggregating from IBM Security Identity Manager involves configuring the ISIM application settings within the IdentityIQ user interface.

ISIM has two types of objects that can be aggregated; people and accounts. IdentityIQ refers to these as identities and accounts (or links). To aggregate from ISIM, perform the following:

1. **Create An ISIM Application:** Create a new application using the IBM Security Identity Manager connector and fill in the required parameters following the steps provided in the IdentityIQ User's Guide. Use the tenant DN search base. For example,
`erglobalid=00000000000000000000,ou=example,dc=com`

Leave the search filter blank. This is auto-generated correctly during aggregation. This application is used to aggregate ISIM person objects.
2. **Setup Correlation Attribute:** Create an identity attribute that is sourced from the `erglobalid` on the ISIM application and mark it as search-able. This is used to correlate ISIM accounts to this identity.
3. **Create ISIM Account Applications:** Run the ITIM Application Creator task to inspect ISIM and retrieve information about the ISIM services (applications). This task auto-generates an application for each service defined in ISIM.
4. **Setup Correlation on the ISIM Account Applications:** Set the correlation rule on the generated applications to Correlation - ISIM Account. This correlates the account to the identity using the `erglobalid`. If the rule is not listed by default, import it from the `$ISIM_INTEGRATION_PACKAGE/samples/ITIM-AccountCorrelationRule.xml` location.
5. **Aggregate:** Run aggregation for the ISIM application first and then for each ISIM account application.

Configuration for Provisioning

Provisioning entitlements and role assignments in ISIM requires the installation of IdentityIQ's ISIM integration web application in WebSphere with ISIM. This process varies slightly depending on the version of WebSphere.

IdentityIQ roles are queued and pushed in ISIM on a schedule. This is accomplished by using the Synchronize Roles task.

1. **Prepare the WAR:** The `iiqIntegration-ITIM.war` file contains a properties file named `itim.properties` with information about how to connect using ISIM. In order to execute, this must be edited to include appropriate information about the ISIM installation. Additionally, the `.war` file does not include any of the required jar files of ISIM files since these can change depending on the version and fixpack level of ISIM. These need to be copied out of the ISIM lib directory and added to the `.war` file.

- a. Expand the `iiqIntegration-ITIM.war` file in a temporary directory.
- b. Edit the `WEB-INF/classes/itim.properties` file and change the properties match your environment. Save the file with your changes. The following can be changed:

- **PLATFORM_URL:** URL to use to communicate with ISIM.
The format of the URL must be same as the value of `enrole.appServer.url` from `enRole.properties` located under `<ISIM-HOME>/data` directory.
- **PLATFORM_PRINCIPAL:** The administrator user who can login to the administrator Console of WAS.
- **PLATFORM_CREDENTIALS:** Password of the principal. Encrypting password is supported.
- **TENANT_DN:** The root DN of the ISIM tenant.

- c. Copy the required jar files of ISIM into the lib directory. These `.jar` files are located in the deployed ISIM ear directory.

(For ISIM 6.0): Example ISIM ear directory:

`$WAS_HOME/profiles/<app server>/installedApps/<cell>/ITIM.ear`

Following are the required files:

- `api_ejb.jar`
- `itim_api.jar`
- `itim_server_api.jar`

- d. Update the `iiqIntegration-ITIM.war` file to include the updated `itim.properties` and required jar files of ISIM.

For example,

```
jar uvf iiqIntegration-ISIM.war WEB-INF/classes/itim.properties \
WEB-INF/lib/api_ejb.jar WEB-INF/lib/itim_api.jar \
WEB-INF/lib/itim_common.jar WEB-INF/lib/itim_server_api.jar \
WEB-INF/lib/jlog.jar
```

2. **Install the IdentityIQ ISIM Integration Web Application:** In the WebSphere Administrative Console, navigate to Enterprise Applications and select **Install**.
 - a. Select **iiqIntegration-ITIM.war** as the application to install and type **iiqisim** as the context root.
 - b. Continue through the rest of the installation wizard accepting the defaults.
 - c. When completed, click **Save** to save the changes to the master configuration.
3. **Setup the Integration Config:** The **IntegrationConfig** object holds information about how to connect IdentityIQ to ISIM and all of the configuration requirements for various functions. ISIM supports dual role push mode, which means that both detectable and assignable roles can be used. An example can be found in the ISIM integration folder within your IdentityIQ installation directory in the `$INSTALLDIR/integration/ITIM/samples/exampleIntegration.xml` directory.

The main properties that need to be set are:

- **executor:** `sailpoint.integration.isim.ISIMIntegrationExecutor`
- **ApplicationRef:** The reference to the ISIM application
- **Attributes=> URL:** The URL to the IIQ web service on the ISIM server. For example, `https://myisim.example.com:9080/iiqisim/resources`

Note: SailPoint recommends that you use SSL when transmitting sensitive electronic information.

- **Attributes=> username:** ISIM user's credentials used for basic HTTP authentication.
- **Attributes=> password:** ISIM user's password used for basic HTTP authentication.
- **ManagedResources map:** Mappings of local IdentityIQ applications to ISIM services, including mappings of local IdentityIQ attribute names to ISIM service attribute names.

For more information, see [Appendix: A: Common Identity Management Integration Configuration](#).

4. **Verify:** Be certain that the integration has been installed correctly by using the ping command in the integration console. If successful, this should respond and list version information about the ISIM jar files that were put into the **iiqIntegration-ISIM.war** file. Compare this version information against the version of the ISIM server to ensure correct operation.
5. **Role Requests:** Set the **roleSyncStyle** to **dual** in the IntegrationConfig file as follows:

```
<IntegrationConfig executor="sailpoint.integration.isim.ISIMIntegrationExecutor"
name="ISIM 5.1 Integration" roleSyncStyle="dual">
```

Other than this, the role should be assignable (for example, a business role) and the name has to match the name of the role in ISIM.

Troubleshooting

1 - An error message appears when the url format in `itim.properties` is not valid

The following error messages appear when the url format in `itim.properties` is not valid:

- `java.lang.NoClassDefFoundError: com.ibm.cv.CVProxyException`
Workaround: Copy `com.ibm.cv.kmip.ext.jar` file to `<WAS-HOME>/profiles/<App server>/classes` directory and restart the application server.
- `java.util.MissingResourceException: Can't find resource for bundle tmsMessages`
Workaround: Copy `tmsMessages.properties` and `tmsMessages_en.properties` file from `<ISIM-HOME>/data` to `<WAS-HOME>/profiles/<App server>/classes` directory and restart the application server.

IaaS - Infrastructure-As-A-Service Module

This section contains information on the following section:

- “IdentityIQ for Amazon Web Services”

Chapter 14: IdentityIQ for Amazon Web Services

The following topics are discussed in this chapter:

IdentityIQ for Amazon Web Services Setup	119
IdentityIQ for Amazon Web Services	119
Supported features	120
Pre-requisites	121
Administrator permissions	122
Configuration parameters	125
Schema attributes	126
Provisioning Policy attributes	130
Additional information	132
(Optional) Upgrade Consideration	132
IdentityIQ for Amazon Web Services	132

IdentityIQ for Amazon Web Services Setup

The IdentityIQ for Amazon Web Services allows organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide a central point of visibility, administration, and governance across the entire enterprise. This includes policy discovery and user access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and improved federated access support.

The AWS Governance Module for IdentityIQ is a licensed module and includes the necessary connectivity components for operation.

For more information on installing the plug in for IdentityIQ for Amazon Web Services, see “[AWS Governance Module](#)” document on compass.

IdentityIQ for Amazon Web Services

Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow.

The SailPoint Amazon Web Services (AWS) Governance Module can be used to manage all the AWS Accounts in your organization or a subset of AWS Accounts. IdentityIQ for Amazon Web Services manages the AWS Organizations entities such as Service Control Policies, Organization Units and AWS Accounts. It also manages the IAM (Identity Access Management) entities such as Users, Groups, Roles, Inline policies, Managed policies (AWS and Customer managed) under each AWS Account.

The AWS Governance Module uses the AWS STS (Security Token Service) to setup cross-account access between AWS accounts.

Supported features

IdentityIQ for Amazon Web Services supports the following features:

- **Account Management**

- IAM Entities Management
 - Manages IAM Users under the AWS Account as Accounts
 - Aggregate, Refresh Accounts
 - Create, Update, Delete
 - Change Password
 - Add/Remove Entitlements (Groups, AWS Managed Policies, Customer Managed Policies)
 - Enable, Disable

For more information on enabling and disabling, see “IAM User Status” on page 132.

- **Group Management**

- IAM Entities Management
 - IAM Groups: Aggregate, Refresh Group, Create, Update, Delete
 - AWS Managed Policy Management: Aggregate, Refresh
 - Customer Managed Policy Management: Aggregate, Refresh, Create
 - Inline Policy Management: Aggregate, Refresh

Note: Inline Policy can be removed only through Certification.

- Role Management: Aggregate, Refresh, Update (Add/ Remove AWS Managed Policy or Customer Managed Policy from Role)
 - Organization Entities Management

The AWS Governance Module also supports following operation on Organization Entities (managed as group object only):

- AWS Accounts Management: Aggregate, Refresh
 - Organization Unit Management: Aggregate, Refresh
 - Service Control Policy Management: Aggregate, Refresh
- **Permissions Management:** AWS Governance Module supports JSON Policy for Permission Policy and Trust Policy as direct permission.

The Permission Policy for following AWS entities are represented as direct permission:

- AWS Managed Policies
- Customer Managed Policies
- Inline Policies
- Service Control Policies

The Trust Policy for following AWS entity is represented as direct permission:

- Roles

The supported features mentioned in this section can be represented in matrix form as follows:

Object Type	IdentityIQ Type	Aggregation	Re-fresh	Create	Update	Delete	Request-able	User Status
IAM User	Account	✓	✓	✓	✓	✓	NA	✓
Groups (Primary)	Entitlement	✓	✓	✓	✓	✓	✓	NA
AWS Managed Policy	Entitlement	✓	✓	NA	NA	NA	✓	NA
Customer Managed Policy	Entitlement	✓	✓	✓	NA	NA	✓	NA
Inline Policy	Group	✓	✓	NA	NA	✓	NA	NA
Service Control Policy	Group	✓	✓	NA	NA	NA	NA	NA
Roles*	Group	✓	✓	NA	✓	NA	NA	NA
Organization Unit	Group	✓	✓	NA	NA	NA	NA	NA
AWS Accounts	Group	✓	✓	NA	NA	NA	NA	NA

Note: * Role aggregation takes care of aggregating the trust policies (entities that can assume a role) as direct permission.

Pre-requisites

- Create service account as follows and assign the required permission to perform the operations (as mentioned in “Administrator permissions”):

Service User Requirement:

- Service User In Master AWS Account:
 - To manage the organization entities like SCPs, OUs and AWS Accounts, it is required to create service account in master AWS Account. Service account must be present in the master account with the required permissions. Additionally, all the organization related permissions must be given through the role present in master account.

- (If **Manage All Accounts** is selected in “Configuration parameters”) To manage all AWS accounts, the service user must be in the master account to get all the AWS Account IDs.
 - Service User In Member AWS Account:
 - (If **Include AWS Account IDs** is selected in “Configuration parameters”) To manage only IAM entities of various AWS Account, create service account in any of the AWS Account by deleting the schema objects of Organization Entities.
 - Ensure that you create **Cross Account Role** across the AWS Accounts with same name and assign the permissions as required.
- For more information on creating the Cross Account Role, see “Creating Cross Account Role” on page 132.

Note: The trust relationship must be established with the account explicitly in which the service IAM user belongs to, along with other AWS Accounts that are to be managed.

Administrator permissions

Customer Managed Policies must be created and attached to the AWS Service IAM User and Role respectively as mentioned in the table below.

Note: The AWS System Administrator can refine the Permission Policies as needed.

Note: If ‘Include AWS Account IDs’ list is specified and organization schema is not present in the application, then ‘iam:GetUser’ API permission is not required for AWS Service IAM User.

The following table lists the examples of policies for the respective policy names:

Policy Name	Policy Document
For AWS Service IAM User	
SPServiceAccount	<pre>{ "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["iam:GetUser", "sts:AssumeRole"], "Resource": "*" }] }</pre>

Policy Name	Policy Document
For Role	
SPOrganizationPolicy (Must be assigned to the Role which is in master AWS Account to manage Organization Entities)	<pre>{ "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["organizations:ListPoliciesForTarget", "organizations:ListAccountsForParent", "organizations:ListRoots", "organizations:ListAccounts", "organizations:ListTargetsForPolicy", "organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:DescribeAccount", "organizations:ListParents", "organizations:ListOrganizationalUnitsForParent", "organizations:DescribePolicy", "organizations:ListPolicies"], "Resource": "*" }] }</pre>

Policy Name	Policy Document
SPAggregationPolicy (Must be assigned to the Role of AWS Account which needs to be managed)	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["iam:GetPolicyVersion", "iam:ListServiceSpecificCredentials", "iam:ListMFADevices", "iam:ListSigningCertificates", "iam:GetGroup", "iam:ListSSHPublicKeys", "iam:ListAttachedRolePolicies", "iam:ListAttachedUserPolicies", "iam:ListAttachedGroupPolicies", "iam:ListRolePolicies", "iam:ListAccessKeys", "iam:ListPolicies", "iam:GetRole", "iam:GetPolicy", "iam:ListGroupPolicies", "iam:ListRoles", "iam:ListUserPolicies", "iam:GetUserPolicy", "iam:ListGroupsForUser", "iam:ListAccountAliases", "iam:ListUsers", "iam:ListGroups", "iam:GetGroupPolicy", "iam:GetUser", "iam:GetRolePolicy", "iam:GetLoginProfile", "iam:ListEntitiesForPolicy", "iam:GetAccessKeyLastUsed"], "Resource": "*" }] } </pre>

Policy Name	Policy Document
SPProvisioningPolicy (Must be assigned to the Role of AWS Account which needs to be managed)	<pre> { "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["iam:UpdateLoginProfile", "iam:CreateGroup", "iam:DeleteAccessKey", "iam:DeleteGroup", "iam:AttachUserPolicy", "iam:DeleteUserPolicy", "iam:UpdateAccessKey", "iam:AttachRolePolicy", "iam:DeleteUser", "iam:CreateUser", "iam:CreateAccessKey", "iam:CreatePolicy", "iam:CreateLoginProfile", "iam:RemoveUserFromGroup", "iam:AddUserToGroup", "iam:DetachRolePolicy", "iam:DeleteSigningCertificate", "iam:AttachGroupPolicy", "iam:DeleteRolePolicy", "iam:DetachGroupPolicy", "iam:DetachUserPolicy", "iam:DeleteGroupPolicy", "iam:DeleteLoginProfile"], "Resource": "*" }] }</pre>

Note: For all provisioning operations, in addition to the provisioning policy permissions listed for “SPProvisioningPolicy” the permissions for “Refresh Operations” are also required.

Note: For more information on operation specific administrator permissions required for IAM and Organization APIs, see “Operation specific administrator permissions” on page 133.

Configuration parameters

The following table lists the configuration parameters of AWS Governance Module:

Parameters	Description
Access Key ID*	Enter the Access Key ID of the Service Account.
Secret Access Key*	Enter the Secret Access Key of the Service Account.
Role Name	Enter the role name that is created in all the AWS Accounts that are to be aggregated.

Parameters	Description
Manage All Accounts	When checked, will manage IAM entities from all the accounts.
Exclude AWS Account IDs	Lists all the AWS Account IDs that are to be excluded.
Include AWS Account IDs	Lists all the AWS Account IDs that are to be included.
Page Size	The maximum size of each dataset when querying over large number of objects for IAM entities. Default: 100

Note: Parameters with * sign are mandatory parameters.

Additional configuration parameters

The following table describes the additional configuration parameters that can be set in the application debug page:

Parameters	Description
assumeRoleDurationInSeconds	<p>The duration, in seconds, of the role session. The value can range from 900 seconds (15 minutes) up to the maximum session duration setting for the role.</p> <p>Set the value of the <code>assumeRoleDurationInSeconds</code> parameter as follows:</p> <pre><entry key="assumeRoleDurationInSeconds" value="3600" /></pre> <p>Default value: 3600</p>
assumeRoleSessionName	<p>An identifier for the assumed role session. Use the role session name to uniquely identify a session when the same role is assumed by different principals or for different reasons. In cross-account scenarios, the role session name is visible to, and can be logged by the account that owns the role.</p> <p>Set the value of the <code>assumeRoleSessionName</code> parameter as follows:</p> <pre><entry key="assumeRoleSessionName" value="SailPointUser" /></pre> <p>Default value: SailPointUser</p>

Schema attributes

The following schema attributes are defined:

- Account schema
- Group schema

Account schema

The following table lists the account schema:

Attributes	Type	Description
UserName	String	The friendly name of the user.
UserId	String	The unique ID of the user.
Path	String	Path to the user.
ARN	String	Amazon Resource Name of the user.
CreateDate	String	Creation date of the user.
ConsoleAccess	String	Password status of the user.
Groups	Group	Groups the user is a part of.
AWSManagedPolicies	AWSManagedPolicy	AWS Managed Policies directly assigned to the user.
CustomerManagedPolicies	CustomerManagedPolicy	Customer Managed Policies directly assigned to the user.
InlinePolicies	InlinePolicy	Inline Policies directly assigned to the user.
Access Keys	String	Access keys associated with the user.
AWS CodeCommit HTTPS Credentials	String	AWS CodeCommit HTTPS Git credentials associated with the user.
AWS CodeCommit SSH Keys	String	AWS CodeCommit SSH public keys associated with the user.
Signing Certificates	String	Signing Certificates associated with the user.
Multi-Factor Authentication Device	String	Multi-Factor Authentication device associated with the user.
PasswordLastUsed	String	Password last used date of the user.
AccessKeyLastUsed	String	Access key last used details of the user.

Group schema

The following table lists the group schema:

Attributes	Type	Description
Object Type: Group		
GroupName	String	The friendly name of the group.
GroupId	String	The unique ID of the group.
Path	String	Path to the group.
ARN	String	Amazon Resource Name of the group.
Create	String	Creation date of the group.
AWSManagedPolicies	AWSManagedPolicy	AWS Managed Policies directly assigned to the group.

Attributes	Type	Description
CustomerManagedPolicies	CustomerManagedPolicy	Customer Managed Policies directly assigned to the group.
InlinePolicies	InlinePolicy	Inline Policies directly assigned to the group.
Object Type: AWSManagedPolicy		
PolicyName	String	The friendly name of the AWS managed policy.
PolicyId	String	The unique ID of the AWS managed policy.
Description	String	A friendly description of the AWS managed policy.
ARN	String	Amazon Resource Name of the AWS managed policy.
Path	String	The path to the AWS managed policy.
CreateDate	String	The creation date of the AWS managed policy.
UpdateDate	String	The last update date of the AWS managed policy.
DefaultVersionId	String	The currently enabled version ID of the AWS managed policy.
PolicyJSON	String	The JSON document for the AWS managed policy.
Object Type: Customer Managed Policy		
PolicyName	String	The friendly name of the customer managed policy.
PolicyId	String	The unique ID of the customer managed policy.
Description	String	A friendly description of the customer managed policy.
CreateDate	String	The creation date of the customer managed policy.
UpdateDate	String	The last update date of the customer managed policy.
ARN	String	Amazon Resource Name of the customer managed policy.
Path	String	The path to the customer managed policy.
DefaultVersionId	String	The currently enabled version ID of the customer managed policy.
PolicyJSON	String	The JSON document for the customer managed policy.
PolicyGroups	String	Groups attached to the customer managed policy.
PolicyRoles	String	Roles attached to the customer managed policy.
Object Type: InlinePolicy		
Name	String	The friendly name of the policy.
Id	String	The unique ID of the policy.
PolicyJSON	String	The JSON document for the policy.
Object Type: Role		
RoleName	String	The friendly name of the role.
RoleId	String	The unique ID of the role.

Attributes	Type	Description
Path	String	Path to the Role.
ARN	String	Amazon Resource Name of the role.
Description	String	Role Description.
CreateDate	String	Creation date of the role.
AWSManagedPolicies	AWSManagedPolicy	AWS Managed Policies directly assigned to the role.
CustomerManagedPolicies	CustomerManagedPolicy	Customer Managed Policies directly assigned to the role.
InlinePolicies	InlinePolicy	Inline Policies directly assigned to the role.
TrustPolicyJSON	String	Trust Relationship Policy JSON.
MaxSessionDuration	String	Maximum CLI/API session duration.
Object Type: SCP		
SCPName	String	The friendly name of the Service Control Policy.
SCPIId	String	The unique ID of the Service Control Policy.
ARN	String	Amazon Resource Name of the Service Control Policy.
Description	String	A friendly description of the Service Control Policy.
AWSManaged	String	A boolean value that indicates whether the Service Control Policy is an AWS managed policy.
PolicyJSON	String	The JSON document for the Service Control Policy.
Object Type: AWSAccount		
AWSAccountName	String	The friendly name of the AWS account.
AWSAccountId	String	The unique ID of the AWS account.
ARN	String	Amazon Resource Name of the AWS account.
Email	String	The email address associated with the AWS account.
Status	String	The status of the AWS account in the organization.
JoinedMethod	String	The method by which the AWS account joined the organization.
JoinedTimestamp	String	The date the AWS account became a part of the organization.
OrganizationUnit	OrganizationUnit	Organization unit holding the AWS Account.
Object Type: OrganizationUnit		
OUName	String	The friendly name of the Organization Unit.
OUIId	String	The unique ID of the Organization Unit.
ARN	String	Amazon Resource Name of the Organization Unit.

Attributes	Type	Description
ServiceControlPolicies	SCP	Service Control Policies attached to the Organization Unit.
Parent	OrganizationUnit	Parent Organization Unit.
AWSAccounts	AWSAccount	AWS Accounts attached to the Organization Unit.

Provisioning Policy attributes

The following default provisioning policies are defined for Account and Account-Group.

Account

- **Create:** The following table lists the attributes that are required for creating an account.

Name	Description
User Name*	Enter the user name for IAM user.
AWS Account*	Enter the Account ID or ARN of the AWS Account under which the IAM user is to be created.
Password	Enter the password for IAM user that allows users to sign-in to the AWS Management Console.
Require Password Reset	Users must create a new password at next sign-in. Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
Programmatic Access	Create an access key ID and secret access key for Programmatic Access.
Path	Specify the path to the IAM user.

- **Enable:** The following table lists the attributes that are required for enabling an account.

Name	Description
Password	Enter the password for IAM user that allows users to sign-in to the AWS Management Console.
Access Keys	Enables the recent access key.
AWS CodeCommit SSH Keys	Enables the recent SSH key.
AWS CodeCommit HTTPS Credentials	Enables the recent HTTPS credential.

Group

- **Create:** The following table lists the attributes that are required for creating a group and customer managed policy.

Name	Description
Group	

Name	Description
Group Name*	Enter the group name for IAM group.
AWS Account*	Enter the Account Id or ARN of the AWS account under which the IAM group is to be created.
Path	Specify the path to the IAM group.
CustomerManagedPolicy	
Policy Name*	Enter the policy name.
AWS Account*	Enter the Account Id of the AWS account under which the IAM Policy is to be created.
Policy Description	Enter the policy description.
Policy JSON*	Enter the policy document as a JSON string.
Path	Specify the path to the policy.

- **Update:** The following table lists the attributes that are required for updating group and role.

Name	Description
UpdateGroup	
Group Name	Enter the group name for the IAM group.
Path	Specify the path to the IAM group.
ARN	ARN of the group.
Creation Date	Creation date of the group.
AWS Managed Policies	Select the AWS managed policies name to be attached.
Customer Managed Policies	Select the Customer managed policies name to be attached.
Inline Policies	Associated inline policies.
UpdateRole	
Role Name	Role name for the IAM role.
Path	Path to the IAM role.
ARN	ARN of the role.
Creation Date	Creation date of the role.
MaxSessionDuration	Duration in seconds for which this role can be assumed.
Trust Policy JSON	Trust policy JSON attached to the Role.
AWS Managed Policies	Select the AWS managed policies name to be attached.
Customer Managed Policies	Select the Customer managed policies name to be attached.
Inline Policies	Associated inline policies.

Additional information

This section describes the additional information related to the AWS Governance Module setup.

(Optional) Upgrade Consideration

When upgrading IdentityIQ to version 7.3 Patch 3,

- to view the list of groups and roles that the customer managed policy is attached to, add the **PolicyGroups** and **PolicyRoles** attributes in schema of object type Customer Managed Policy.
- to get the information of password last used date and access key last used details of IAM User, add the **PasswordLastUsed** and **AccessKeyLastUsed** attributes in the account schema.
For more information on **PasswordLastUsed** and **AccessKeyLastUsed** attributes, see "Account schema" on page 126.

IdentityIQ for Amazon Web Services

IAM User Status

Following are the IdentityIQ operations with the corresponding IAM User Status:

- **Enable**
 - Set Console Password (This would also activate the Signing Certificate if it is associated with an IAM User.)
 - Activate Last Created Access Keys
 - Activate Last CreatedAWS CodeCommit HTTPS Credentials
 - Activate Last CreatedAWS CodeCommit SSH Keys
 - Activate Signing Certificates
- **Disable**
 - Deletes Console Password
 - Inactive Both Access Keys
 - Inactive Both AWS CodeCommit HTTPS Credentials
 - Inactive All AWS CodeCommit SSH Keys
 - Inactive Signing Certificates

Creating Cross Account Role

To aggregate the data present in AWS accounts in an organization, AWS Governance Module uses assume role functionality of AWS System. This functionality will help in getting data from different AWS accounts.

- Create cross account role to allow users from one AWS Account to access resources in another AWS Account.
- AWS Account Ids must be specified in the trust Relationship Policy in JSON format as follows:

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::123456789012:role/AWSRoleName"      },  
      "Action": "sts:AssumeRole"    }  
  ]  
}
```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::AccountId1:root",
        "arn:aws:iam::AccountId2:root",
        "arn:aws:iam::AccountId3:root"
      ]
    },
    "Action": "sts:AssumeRole",
    "Condition": {}
  }
]
}

```

Where AccountId1, AccountId2, and AccountId3 are the Account Ids that are to be managed.

Operation specific administrator permissions

This section lists the operation specific administrator permissions required for the following:

- IAM APIs
- Organization APIs

Identity and Access Management APIs

The following table lists the IdentityIQ operations along with the corresponding IAM API (Actions) used:

IdentityIQ operation	IAM API (Action)
Test Connection	GetUser
Account Update	CreateAccessKey
Reset Password	<ul style="list-style-type: none"> • UpdateLoginProfile • CreateLoginProfile
Group Create	CreateGroup
Group Update	<ul style="list-style-type: none"> • UpdateGroup • AttachGroupPolicy • DetachGroupPolicy
Create Customer Managed Policy	CreatePolicy
Account Aggregation	

Additional information

IdentityIQ operation	IAM API (Action)
<ul style="list-style-type: none"> Summary/Attributes (UserName, UserId, Path, ARN, CreateDate, PasswordLastUsed) ConsoleAccess Groups AWSManagedPolicies and CustomerManagedPolicies InlinePolicies Access Keys AWS CodeCommit HTTPS Credentials AWS CodeCommit SSH Keys Signing Certificates Multi-Factor Authentication (MFA) Device AccessKeyLastUsed 	<ul style="list-style-type: none"> ListUsers GetLoginProfile ListGroupsForUser ListUserPolicies ListAttachedUserPolicies ListAccessKeys ListServiceSpecificCredentials ListSSHPublicKeys ListSigningCertificates ListMFADevices GetAccessKeyLastUsed
Account-Group Aggregation (Group)	
<ul style="list-style-type: none"> Summary/Attributes (GroupName, GroupId, Path, ARN, CreateDate) AWSManagedPolicies and CustomerManagedPolicies InlinePolicies 	<ul style="list-style-type: none"> ListGroups ListAttachedGroupPolicies ListGroupPolicies
Account-Group Aggregation (AWSManagedPolicy and CustomerManagedPolicy)	
<ul style="list-style-type: none"> Summary/Attributes (PolicyName, PolicyId, ARN, Path, CreateDate, UpdateDate, DefaultVersionId) Description PolicyJSON (Only for CustomerManagedPolicy) PolicyGroups, PolicyRoles 	<ul style="list-style-type: none"> ListPolicies GetPolicy GetPolicyVersion (Only for CustomerManagedPolicy) ListEntitiesForPolicy
Account-Group Aggregation (Role)	
<ul style="list-style-type: none"> Summary/Attributes (RoleName, RoleId, Path, ARN, Description, CreateDate, TrustPolicyJSON, MaxSessionDuration) AWSManagedPolicies and CustomerManagedPolicies InlinePolicies 	<ul style="list-style-type: none"> ListRoles ListAttachedRolePolicies ListRolePolicies
Account-Group Aggregation (InlinePolicy)	
<ul style="list-style-type: none"> Id Name PolicyJSON 	<ul style="list-style-type: none"> No API is called for this attribute, it is formatted as: ARN of the entity:InlinePolicy:InlinePolicyName ListUserPolicies, ListGroupPolicies, ListRolePolicies GetUserPolicies, GetGroupPolicies, GetRolePolicies
Account Refresh	

IdentityIQ operation	IAM API (Action)
<ul style="list-style-type: none"> • Summary/Attributes (UserName, UserId, Path, ARN, CreateDate) • Groups • Access Keys • Signing Certificates • Password • MFA Device • AWS CodeCommit HTTPS Credentials and AWS CodeCommit SSH Keys: ListServiceSpecificCredentials 	<ul style="list-style-type: none"> • GetUser • ListGroupsForUser • ListAccessKeys • ListSigningCertificates • GetLoginProfile • ListMFADevices • ListServiceSpecificCredentials
Refresh Operations	
<ul style="list-style-type: none"> • Refresh Group • Refresh Role • Refresh AWSManagedPolicy and CustomerManagedPolicy • Refresh Inline Policy associated with User • Refresh Inline Policy associated with Group • Refresh Inline Policy associated with Role 	<ul style="list-style-type: none"> • GetGroup • GetRole • GetPolicy • GetUserPolicies • GetGroupPolicies • GetRolePolicies
Account Delete	
<ul style="list-style-type: none"> • Read Groups • Remove Groups • Read AWSManagedPolicy and CustomerManagedPolicy • Remove AWSManagedPolicy and CustomerManagedPolicy • Read InlinePolicy • Read Security Credentials <ul style="list-style-type: none"> - Access Keys - Signing Certificates - Password - MFA Device - AWS CodeCommit HTTPS Credentials - AWS CodeCommit SSH Keys • Remove Security Credentials <ul style="list-style-type: none"> - Access Keys - Signing Certificates - Password - MFA Device - AWS CodeCommit HTTPS Credentials - AWS CodeCommit SSH Keys 	<ul style="list-style-type: none"> • DeleteUser • ListGroupsForUser • RemoveUserFromGroup • ListAttachedUserPolicies • DetachUserPolicy • ListUserPolicies • DeleteUserPolicy • ListAccessKeys • ListSigningCertificates • GetLoginProfile • ListMFADevices • ListServiceSpecificCredentials • ListSSHPublicKeys • DeleteAccessKey • DeleteSigningCertificate • DeleteLoginProfile • DeactivateMFADevice • DeleteServiceSpecificCredential • DeleteSSHPublicKey

Additional information

IdentityIQ operation	IAM API (Action)
Group Delete	
<ul style="list-style-type: none"> Read Accounts in the Group Remove Accounts from the Group Read Group Policies Remove Group Policies 	<ul style="list-style-type: none"> DeleteGroup GetGroup RemoveUserFromGroup ListGroupPolicies DeleteGroupPolicy
Account Enable	
<ul style="list-style-type: none"> Set Password Activate Access Keys (Last created one) Activate AWS CodeCommit HTTPS Credentials (Last created one) Activate AWS CodeCommit SSH Keys (Last created one) 	<ul style="list-style-type: none"> UpdateLoginProfile UpdateAccessKey UpdateServiceSpecificCredential UpdateSSHPublicKey
Account Disable	
<ul style="list-style-type: none"> Delete Password Deactivate Access Keys (All) Deactivate AWS CodeCommit HTTPS Credentials (All) Deactivate AWS CodeCommit SSH Keys (All) 	<ul style="list-style-type: none"> DeleteLoginProfile UpdateAccessKey UpdateServiceSpecificCredential UpdateSSHPublicKey
Request Entitlement (Group and Managed Policies for User)	
<ul style="list-style-type: none"> Add group to user Add AWSManagedPolicy and CustomerManagedPolicy to user 	<ul style="list-style-type: none"> AddUserToGroup AttachUserPolicy
Remove Entitlement (Group, Managed Policies, Inline Policies from User)	
<ul style="list-style-type: none"> Remove group from user Remove AWSManagedPolicy and CustomerManagedPolicy from user Remove Inline Policy from user 	<ul style="list-style-type: none"> RemoveUserFromGroup DetachUserPolicy DeleteUserPolicy
Remove Inline Policy	
<ul style="list-style-type: none"> Read from User Delete from User Read from Group Delete from Group Read Role Delete from Role 	<ul style="list-style-type: none"> GetUserPolicies DeleteUserPolicy GetGroupPolicies DeleteGroupPolicy GetRolePolicies DeleteRolePolicy
Update Role	
<ul style="list-style-type: none"> Attach AWSManagedPolicy and CustomerManagedPolicy Remove AWSManagedPolicy and CustomerManagedPolicy 	<ul style="list-style-type: none"> AttachRolePolicy DetachRolePolicy

Organization APIs

The following table lists the IdentityIQ operations along with the corresponding IAM APIs used for managing organizational entities:

IdentityIQ operations	Organizations API (Actions)
Test Connections	Role (Master Account): organizations:ListAccounts
Account-Group Aggregation (OrganizationUnit)	
<ul style="list-style-type: none"> Summary/Attributes (OUName, OUIId, ARN, Parent) ServiceControlPolicies AWSAccounts 	<ul style="list-style-type: none"> ListRoots, ListOrganizationalUnitsForParent ListPoliciesForTarget ListAccountsForParent
Account-Group Aggregation (SCP)	
<ul style="list-style-type: none"> Summary/Attributes (SCPName, SCPId, ARN, Description, AWSManaged) PolicyJSON 	<ul style="list-style-type: none"> ListPolicies DescribePolicy
Account-Group Aggregation (AWSAccount)	
<ul style="list-style-type: none"> Summary/Attributes (AWSAccountName, AWSAccountId, ARN, EmailId, Status, JoinedType, JoinedTimestamp) OrganizationUnit 	<ul style="list-style-type: none"> ListAccounts ListRoots, ListParents, DescribeOrganizationalUnit
Get Operations	
<ul style="list-style-type: none"> SCP AWS Accounts Organizational Unit 	<ul style="list-style-type: none"> DescribePolicy DescribeAccount, ListRoots, ListParents, DescribeOrganizationalUnit DescribeOrganizationalUnit, ListRoots, ListParents, ListPoliciesForTarget, ListAccountsForParent

Additional information

Section II: SailPoint IdentityIQ Application Modules

The SailPoint IdentityIQ Application Modules section includes the following modules:

- “Enterprise Resource Planning Application Modules”
- “SAP Governance Modules”
- “SAP Governance Application Modules”
- “Healthcare Integration Modules”
- “Mainframe Integration Modules”

Enterprise Resource Planning Application Modules

This section contains information on the following sections:

- “IdentityIQ for SAP ERP - SAP Governance Module”
- “IdentityIQ for Oracle ERP – Oracle E-Business Suite”
- “IdentityIQ for SAP ERP – SAP Portal - User Management Web Service”
- “IdentityIQ for Oracle ERP – PeopleSoft”
- “IdentityIQ for Oracle ERP – Siebel”
- “IdentityIQ for NetSuite ERP”

Chapter 15: IdentityIQ for SAP ERP - SAP Governance Module

The following topics are discussed in this chapter:

Overview	143
Supported features	143
Supported Managed Systems	145
Pre-requisites	145
Administrator permissions	145
Configuration parameters	150
Schema attributes	152
Account attributes	152
Group attributes	156
Schema extension and custom attributes	157
Upgrade considerations	157
Provisioning Policy attributes	158
Create account attributes	158
Additional information	158
Entitlement validity period	158
CUA support	158
Entitlement Data	159
Password Change	159
Logon and Communication Language attributes	159
Delta Aggregation	160
Partitioning Aggregation	163
Troubleshooting	163

Overview

SAP Enterprise Resource Planning software solution is an integrated software solution that incorporates the key business functions of the organization.

The IdentityIQ for SAP ERP aggregates and provisions all the users along with their roles/profiles of the SAP system.

IdentityIQ for SAP ERP supports provisioning to a standalone SAP system as well as SAP Central User Administration (CUA) system.

Supported features

IdentityIQ for SAP ERP supports the following features:

- Account Management
 - Manages SAP users as Accounts
 - Aggregation, Partitioning Aggregation, Delta Aggregation, Refresh Accounts, Pass Through Authentication

Overview

For more information on Delta Aggregation and Partitioning Aggregation, see “Additional information” on page 158.

- Create, Update, Delete
- Enable, Disable, Unlock
- Change Password
- Add/Remove Entitlements

Entitlements are Roles (for user), Profiles (for user), UserGroup (User group of the user).

- Add /Remove Contractual User Type ID
- Account - Group Management
 - Manages SAP Roles as Account-Groups
 - Manages SAP Profiles as Account-Groups
 - Aggregation, Refresh Groups

Notes

The following table lists the notes of the respective supported features:

Supported features	Notes
Pass Through Authentication	If Pass Through authentication is enabled, user can login through IdentityIQ using user name and password without any authorization required.
Aggregation	IdentityIQ for SAP ERP aggregates Generated Profile associated to Role as a part of Account-Group Aggregation.
Change Password	<ul style="list-style-type: none">• For “Change password in Permanent Mode” ensure that the SNC is configured on SAP server. The log on session during which a productive password is set must be secured using Secure Network Communications (SNC).• SAP recommends that setting of productive passwords is more risky than setting an initial one, therefore additional security checks must be applied as follows:<ul style="list-style-type: none">- The log on session during which a productive password is set must be secured using Secure Network Communications (SNC).- The user needs an additional authorization to set a productive password (authorization object: S_USER_GRP, activity: 'PP' - Set Productive) <p>For more information, see SAP note https://service.sap.com/sap/support/notes/1287410 (SAP Service marketplace login required).</p>

Supported features	Notes
Manages SAP Profiles as Account-Groups	Few system composite profiles might have child profiles which are not present in SAP system. For example, for each release composite profile <code>SAP_NEW</code> contains a single profile <code>SAP_NEW_<rel></code> , (for example, <code>SAP_NEW_21D</code>). This profiles holds its release status. Profiles like <code>SAP_NEW_<rel></code> may not be aggregated.
Account - Group Aggregation	In Account-Group aggregation for SAP CUA landscape, IdentityIQ for SAP ERP will not fetch child roles, child profiles of any composite role and profile, as CUA system does not maintain child level roles and profile details for child subsystems. Same way it will not fetch TCodes and Generated Profile for group object type.

Supported Managed Systems

IdentityIQ for SAP ERP supports the following versions of managed systems:

- SAP Enterprise Resource Planning (ERP) Central Component (ECC) 6.0
- SAP NetWeaver 7.5, 7.4, 7.3, 7.2, 7.1 and 7.0

IdentityIQ for SAP ERP supports the following modules of managed systems:

- SAP HR/HCM module
- SAP S/4HANA on-premise
- SAP Business Warehouse
- SAP Customer Relationship Management (CRM)
- SAP Process Integration (PI)
- SAP GRC
- SAP Fiori

Note: IdentityIQ for SAP ERP manages ABAP users. For more information, see "Supported features" on page 143.

Pre-requisites

SAP JCO version 3.0.x libraries, along with `sapjco3.dll` (on Microsoft Windows) or `libsapjco3.so` (on UNIX), must be present in the `java.library.path` directory on the host. The JCO libraries (JCO Release 3.0.x) must be downloaded from the SAP website by navigating to the customer service marketplace and download the Java Integration Module.

Administrator permissions

The following table lists the required permissions for the specific operations mentioned below in this section:

Table 1— Operation specific required permissions

Operation	Required permissions
Test Connection	Test Connection

Table 1— Operation specific required permissions

Operation	Required permissions
Account Aggregation	Test Connection and Account Aggregation Note: For Account Aggregation of CUA systems, additional permissions must be executed as specified in the “ Account Aggregation” section.
Group Aggregation	Test Connection and Group Aggregation Note: For Group Aggregation of CUA systems, additional permissions must be executed as specified in the “ Group Aggregation” section.
Delta Aggregation	Test Connection, Account Aggregation and Delta Aggregation
Create Account	Test Connection, Account Aggregation and Create Account Note: For Create Account of CUA systems or SNC network, additional permissions must be executed as specified in the “ Create Account (Create user with assign role and profiles)” section.
Enable/Disable/Unlock Account	Test Connection, Account Aggregation and Enable/Disable/Unlock Account
Delete Account	Test Connection, Account Aggregation and Delete Account
Add/Remove Entitlement	Test Connection, Account Aggregation and Add/Remove Entitlement
Change Password	Test Connection, Account Aggregation and Change Password Note: For Change Password of SNC network, additional permissions must be executed as specified in the “ Add/Remove Entitlements and Change Password” section.

The role assigned to the SAP Administrative user must have the following Authorization Objects as mentioned in the tables below.

Test Connection

Authorization Objects	Field name	Field description	Field value
S_RFC	ACTVT	Activity	16 - Execute
	RFC_NAME	Name of RFC object	RFCPING
	RFC_TYPE	Type of RFC object	FUGR, FUNC

Account Aggregation

Authorization Objects	Field name	Field description	Field value
S_RFC	RFC_NAME	Name of RFC object	BAPI_USER_GETLIST, BAPI_USER_GET_DETAIL, DDIF_FIELDINFO_GET, MSS_GET_SY_DATE_TIME, RFC_GET_FUNCTION_INTERFACE, SDTX, SMSSDATA1, SU_USER
S_TABU_NAM	ACTVT	Activity	03 - Display
	TABLE Name	TABLE	USR11, USR06, USR02, TUTYP, TUTYPA
S_USER_GRP	ACTVT	Activity	03 - Display
	CLASS	User group in user master maintenance	* or specify the Group you want to assign for the user. For example, SUPER

- Additional permissions for CUA systems

Authorization Objects	Field name	Field description	Field value
S_RFC	RFC_NAME	Name of RFC object	BAPI_USER_LOCACTGROUPS_READ, BAPI_USER_LOCPROFILES_READ

Group Aggregation

Authorization Objects	Field name	Field description	Field value
S_RFC	ACTVT	Activity	16 - Execute
	RFC_NAME	Name of RFC object	BAPI_HELPVALUES_GET, PRGN_ACTIVITY_GROUPS_LOAD_RFC, PRGN_EXCHANGE, COLL_ACTGROUPS_GET_ACTGROUPS, DDIF_FIELDINFO_GET, MSS_GET_SY_DATE_TIME, PRGN_COLLECTIVE_ACTGROUPS, RFC_GET_FUNCTION_INTERFACE, SDTX, SMSSDATA1

Overview

Authorization Objects	Field name	Field description	Field value
S_TABU_NAM	TABLE Name	TABLE	<ul style="list-style-type: none"> (Roles) AGR_FLAGS, AGR_PROF, AGR_TCODES, AGR_TEXTS (Roles) (Profiles) AGR_DEFINE, USR11, UST10C (To aggregate Authorization Objects associated with role) AGR_1251, AGR_1252 <p>Note: If you do not want to aggregate the Authorization Objects (AGR_1251 and AGR_1252), then these permissions must not be provided and Authorization Objects must be removed from group schema also.</p>

Note: Group aggregation specific to Authorization Objects would not be supported for SAP CUA system.

- Additional permissions for CUA systems

Authorization Objects	Field name	Field description	Field value
S_TABU_NAM	TABLE Name	TABLE	<ul style="list-style-type: none"> (Profiles) USRSYSPRF, USRSYSPRFT (Roles) USRSYSACTT, USRSYSACT

Delta Aggregation

Authorization Objects	Field name	Field description	Field value
S_RFC	RFC_NAME	Name of RFC object	/SAILPOIN/USR_CHANGE_DOC_USERS , /SAILPOIN/IDENTITYIQ_FUGR, /SAILPOIN/USR_CHANGE_DOC_ROLES
S_TABU_NAM	TABLE Name	TABLE	USBAPILINK
S_USER_GRP	ACTVT	Activity	08 - Display change document

Create Account (Create user with assign role and profiles)

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	01 - Create or generate
S_RFC	RFC_NAME	Name of RFC object	SDIFRUNTIME

Authorization Objects	Field name	Field description	Field value
S_USER_SAS	ACTVT	Activity	22 - Enter, Include, Assign, 01 - Create
	ACT_GROUP	Role name	* or you can specify role name for which you have assigned
	CLASS	User group in user master maintenance	* or specify the Group you want to assign for the user. For example, SUPER
	PROFILE	Auth. profile in user master maintenance	* or you can specify Profile for which you have assigned
	SUBSYSTEM	Receiving system for central user administration	* or specify the system you are targeting.

- For SNC (Secure Network Communication)

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	PP – Set Productive

Enable/Disable/Unlock Account

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	05 - Lock

Delete Account

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	06 - Delete

Add/Remove Entitlements and Change Password

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	22 - Enter, Include, Assign, 02-Change
S_RFC	RFC_NAME	Name of RFC object	SDIFRUNTIME

Configuration parameters

Authorization Objects	Field name	Field description	Field value
S_USER_SAS	ACTVT	Activity	22 - Enter, Include, Assign
	ACT_GROUP	Role name	* or you can specify role name for which you have assigned
	CLASS	User group in user master maintenance	* or specify the Group you want to assign for the user. For example, SUPER
	PROFILE	Auth. profile in user master maintenance	* or you can specify Profile for which you have assigned
	SUBSYSTEM	Receiving system for central user administration	* or specify the system you are targeting.
S_USER_AGR	ACTVT	Activity	02 - Change
	ACT_GROUP	Role name	* or you can specify role name for which you want to provide access
S_USER_PRO	ACTVT	Activity	22 - Enter, Include, Assign
	PROFILE	Auth. profile	* or you can specify profile name for which you want to provide access.

- (For Change Password only) For SNC (Secure Network Communication)

Authorization Objects	Field name	Field description	Field value
S_USER_GRP	ACTVT	Activity	PP – Set Productive

Configuration parameters

The following table lists the configuration parameters of IdentityIQ for SAP ERP:

Parameters	Description
SAP Host*	Host on which the SAP Server is running
System Number*	2-digit SAP system number (Default: 00)
Client Number*	3-digit SAP client number (Default: 001)
Client Language*	2-letter SAP client language (Default: EN)
Username*	SAP Administrator user
Password*	SAP Administrator user password
CUA system	For CUA system detection
JCO RFC Trace	If checked, enables SAP JCO RFC trace

Parameters	Description
Unlock on Password Change	If checked, the account would be unlocked while changing password. Note: Account will be unlocked at the time of set password only if the account is locked by incorrect password attempts.
Partition Enabled	Check box to determine if partition aggregation is required.
Partition Statements	Criteria to specify the range of users to be downloaded. For example, If the range is specified as A-M , then this specifies that all the users whose User IDs are between A and M (including A and M) would be treated as one partition and downloaded. To specify more than one partition the entries should be separated using a new line character. For more information, see "Partitioning Aggregation" on page 163.
Load Balance Configuration parameters	
Load Balancer	Select this to configure and enable load balancing on this application.
Host	SAP message server host. Note: Required for a logon load balanced connection.
Client Group	Logon group name of SAP application servers.
Port Number	SAP message server service or port number.
SNC Configuration parameters	
SNC Mode	Represents Secure Network Connection which also internally signifies <code>jco.client.snc_mode</code> in SAP. SNC will be enabled if the mode is selected as ON whose value is 1. If SNC is off, the value will be 0.
SNC Level of Security	Represents the quality of protection level (QOP) which is defined as follows: 1 — Apply authentication only 2 — Apply integrity protection (authentication) 3 — Apply privacy protection (integrity and authentication) 8 — Apply the default protection 9 — Apply the maximum protection In SAP, it relates to <code>jco.client.snc_qop</code> . Default: 1
SNC Partner Name	Represents SNC partner. For example, provide input as <code>p:CN=R3, O=XYZ-INC, C=EN</code> in SAP. If SNC is configured, it relates to <code>jco.client.snc_partnername</code> .
SNC Name	Represent SNC name which internally signifies <code>jco.client.snc_myname</code> . It overrides default SNC partner.

Schema attributes

Parameters	Description
SNC Library	Path to library which provides SNC service. It internally signifies <code>jco.client.snc_lib</code> . For example, the value to be passed: <ul style="list-style-type: none">on Microsoft Windows: <code>C:/sapcryptolib/sapcrypto.dll</code> (the location of the cryptographic library)on UNIX: <code>/opt/sailpoint/lib/custom/libsapcrypto.so</code> (the location of the cryptographic library)
SAP GRC Settings parameters	
Enable SAP GRC	Enables the application for SAP GRC policy violation checks.
SAP GRC Connector Name	SAP GRC Connector name which is configured on GRC server for this application.
Note: For more information on SAP GRC configuration, see <i>SailPoint IdentityIQ Integration Guide</i>.	

Note: Attributes marked with * sign are the mandatory attributes.

Schema attributes

This section describes the different schema attributes.

Account attributes

The following table lists the account attributes:

Attributes	Description
Academic Title (Address)	Academic title of the user.
Academic Title 2 (Address)	2nd Academic title of the user.
Addr Number (Address)	Address number of the user.
Alias (Logon Data)	Alias name.
Birth Name (Address)	Name at birth.
Building (Address)	Name of the building.
Building 2 (Address)	Name 2 of the building.
Building Long (Address)	Long name of the building.
Care of (Address)	Care of name.
Check Status (Address)	Check status for the user.
City (Address)	Name of the city.
City Number (Address)	Number of the city.

Attributes	Description
Code (Address)	Signature initials
Communication Language (Address)	Communication language of the user. Note: The different values to be set for this attribute are mentioned in “Logon and Communication Language attributes” on page 159.
Communication type (Address)	Communication method for the user.
Company (Address)	Name of the company.
Company Address (Address)	Address of the company.
Company Address 2 (Address)	Address 2 of the company.
Company Address 3 (Address)	Address 3 of the company.
Company Address 4 (Address)	Address 4 of the company.
Contractual User Type ID	Contractual user types associated with user. Note: For more information, see “Upgrade considerations” on page 157.
Country (Address)	Name of the country.
Country ISO (Address)	ISO name of the country.
Delivery District (Address)	Delivery district name.
Department (Address)	Department name.
District (Address)	District name.
District Number (Address)	District number for the user.
E-Mail (Address)	E-mail address.
E-Mail List (Address)	E-mail address list.
Employee Number (Address)	Employee number of the user.
Fax (Address)	Fax number.
Fax Extension (Address)	Fax extension number
Fax List (Address)	Fax number list
First name (Address)	First name of the user
Floor (Address)	Floor number
Floor 2 (Address)	Floor 2 number
Format (Address)	Format name
Full Name (Address)	Full name of the user
Full Name 2 (Address)	Full name 2 of the user
Function (Address)	Function of the user
GUI Flag	Unsecured communication permitted.
House Number 2 (Address)	House number 2 of the user

Schema attributes

Attributes	Description
House Number (Address)	House number of the user
House Number 3 (Address)	House number 3 of the user
Inhouse ML (Address)	Inhouse mail of the user
Initials (Address)	Initials of the user
Language CR P (Address)	CR P language of the user
Language ISO (Address)	ISO language of the user
Language UCP ISO (Address)	CP ISO language of the user
Language UP ISO (Address)	P ISO language of the user
Last Name (Address)	Last name of the user
Location (Address)	Location name
Logon Language (Defaults)	Logon language for the user. Note: The different values to be set for this attribute are mentioned in “Logon and Communication Language attributes” on page 159.
Middle Name (Address)	Middle name of the user
Name Country (Address)	Name of the country
Nickname (Address)	Nickname of the user
Notes (Address)	Notes for the user
Other City (Address)	Name of the other city
Other City Number (Address)	Number of the other city
Pager/SMS List (Address)	Pager or SMS number list in the format pager_type#pager_number
Parameter List (Parameters)	Parameter list in the format parameter_ID=parameter_value
Pboxcity Number (Address)	Pbox number of the city
PCODE 1 Ext (Address)	Postal code 1 extension
PCODE 2 Ext (Address)	Postal code 2 extension
PCODE 3 Ext (Address)	Postal code 3 extension
PO Box (Address)	PO box number
PO Box City (Address)	PO box number of the city
PO Box City ISO (Address)	PO box number of the ISO city
PO Box Country (Address)	PO box number of the country
PO Box Region (Address)	PO box number of the region
PO Box Without Number (Address)	PO box without number
Postal Code (Address)	Postal code of the user
Postal Code 2 (Address)	2nd postal code of the user

Attributes	Description
Postal Code 3 (Address)	3rd postal code of the user
Prefix 1 (Address)	1st prefix
Prefix 2 (Address)	2nd prefix
Print Immediately (Defaults)	Print immediately flag for the user
Printer List (Address)	Print destination list
Region (Address)	Name of the region
Region Group (Address)	Group name of the region
Remote Communication List (Address)	Communication notes list
Remote Function Call List (Address)	Remote function call destination list
Remote Mail List (Address)	Remote mail list of the user
Room Number (Address)	Room number of the user
Room Number 2 (Address)	2nd room number of the user
Reference User	Reference user name.
Search Term 2 P (Address)	2nd search term P for the user
Search Term P (Address)	Search term P for the user
Search Term 1 (Address)	1st search term for the user
Search Term 2 (Address)	2nd search term for the user
Second Name (Address)	Second name of the user
Start Menu (Defaults)	Start menu for the user
Street Abbreviation (Address)	Street abbreviation for the user
Street Address (Address)	Street address of the user
Street Address 2 (Address)	Street address 2 of the user
Street Address 3 (Address)	Street address 3 of the user
Street Address 4 (Address)	Street address 4 of the user
Street Number (Address)	Street number of the user
SNC Name	SNC name.
Tax Jurisdiction Code (Address)	Tax jurisdiction code of the user
Telephone (Address)	Telephone number
Telephone Extension (Address)	Telephone extension number
Telephone List (Address)	Telephone number list
Teletex List (Address)	Teletex number list
Telex List (Address)	Telex number list
Time Format (Defaults)	Time format of the user

Schema attributes

Attributes	Description
Time Zone (Address)	System time zone.
Title (Address)	Title of the user
Title SPPL (Address)	Title SPPL of the user
Transportation Zone (Address)	Transportation zone of the user
TZone (Defaults)	Personal time zone.
URL (Homepage) List (Address)	URL (Homepage) address list in the format URI_type#URI_name
User Last Logon Time	User last log in time.
User Last Logon Date	User last log in date.
Productive Password	User password set in permanent mode.
User Name	User Name.
User Title (Address)	Title of the user
User Type (Logon Data)	Type of the user
User Valid From (Logon Data)	Valid from date for the user
User Valid To (Logon Data)	Valid to date for the user.
User Group (Groups)	User group of the user
X.400 List (Address)	Organization name list
Roles	Roles for user. Note: The Account Aggregation fetches the active roles (composite /simple) assigned directly to the user.
Profiles	Profiles for user.

Group attributes

The following table lists the different group attributes:

Attributes	Description
Group Object Type = Role	
Name	Role name.
Type	Role type.
Description	Role description.
Child Roles	Sub Role list. Note: The child roles will display the child roles of composite roles in the Group object properties of Entitlement Catalog. For existing applications which are getting upgraded, mark entitlement as true to display the child roles in Entitlement grid of Group object properties.
Long Description	Role long description.

Attributes	Description
Subsystem	System name for CUA System Aggregation.
Generated Profile	System generated profile associated to Role which has authorizations.
TCodes	Transaction code list.
Authorization Objects	Authorization objects associated with role.
Group Object Type = Profile	
ID	Profile name along with the description.
Name	Profile name.
Type	Profile type.
Description	Profile description.
Subsystem	System name for CUA System Aggregation.
Child Profiles	Sub profile list.

Schema extension and custom attributes

The schema can be extended up to the extent of the fields within the structures provisioned by the SAP standard BAPI. The fields in the following structures will be provisioned:

- ADDRESS
- ALIAS
- COMPANY
- DEFAULTS
- LOGONDATA
- PASSWORD

Note: No custom attributes will be supported during provisioning.

Upgrade considerations

While upgrading to IdentityIQ version 7.3 Patch 3, perform the following changes at schema level:

- Ensure that in **Role** schema, following attributes are added with appropriate properties:
 - Generated Profile
 - TCodes (Entitlement, Multi-Valued)
 - Authorization Objects
- In order to achieve the profile aggregation functionality for an existing application in previous releases it is recommended to perform the following procedure:
 - Add **Profile** schema under the Settings tab in the application page
 - In Account Schema the **schemaObjectType** attribute of Profiles must be changed to **profile**.
- To skip the inactive roles assignment during aggregation, add the following line in the application debug page:


```
<entry key="skipInactiveRoles" value="true"/>
```

Provisioning Policy attributes

Note: When upgrading IdentityIQ from version 6.x to 7.3 Patch 3, ensure that the 'Include Permissions' check box in Role schema is not selected.

- To fetch Contractual user types associated with user after upgrading IdentityIQ to version 7.3 Patch 3, add the **Contractual User Type ID** attribute to the application with:
 - Property: Multi-Valued
 - Data Type: string

Note: Only the active Contractual User ID assigned to the user would be aggregated.

Provisioning Policy attributes

This section lists the different policy attributes of IdentityIQ for SAP ERP.

Note: The attributes marked with * sign are the required attributes.

Create account attributes

The following table lists the provisioning policy attributes for Create Account:

Attributes	Description
User Name*	Name of the user to create.
password	Password for the user.
Last Name*	Last name of the user.

Additional information

This section describes the additional information related to the IdentityIQ for SAP ERP.

Entitlement validity period

The user can be assigned a SAP Role with Start Date and an End Date. The ability to select or specify the same, while requesting an entitlement for an account, is available in IdentityIQ by creating custom Provisioning Plan.

CUA support

By default the IdentityIQ for SAP ERP would not download data from CUA configured SAP System. In order to override this behavior, the **CUASystem** configuration parameter must be checked in configuration parameter list.

Entitlement Data

The aggregated entitlement data consists of the following:

- SAP Roles (Simple and Composite)
- SAP Profiles (Simple and Composite)

Password Change

The following change password policy must be added to set password as productive using administrative change password request.

```
<Form name="con_prov_policy_user_create_username" objectType="account "
type="ChangePassword">
  <Attributes>
    <Map>
      <entry key="IIQTemplateOwnerDefinition">
        <value>
          <DynamicValue value=""/>
        </value>
      </entry>
    </Map>
  </Attributes>
  <Field displayName="Productive Password" filterString=""
helpKey="ProductivePasswordFlag" name="Productive Password" required="true"
type="string" value="true">
    <AllowedValuesDefinition>
      <Value>
        <List>
          <String>true</String>
          <String>>false</String>
        </List>
      </Value>
    </AllowedValuesDefinition>
  </Field>
</Form>
```

Logon and Communication Language attributes

Following is a list of different Logon and Communication Language fields:

- Serbian
- Chinese
- Thai
- Korean
- Romanian
- Slovenian
- Croatian
- Malay
- Ukrainian
- Estonian
- Afrikaans
- Icelandic
- Catalan

Additional information

- Serbian (Latin)
- Indonesian
- Arabic
- Hebrew
- Czech
- German
- English
- French
- Greek
- Hungarian
- Italian
- Japanese
- Danish
- Polish
- Chinese traditional
- Dutch
- Norwegian
- Portugese
- Slovak
- Russian
- Spanish
- Turkish
- Finnish
- Swedish
- Bulgarian
- Lithuanian
- Latvian
- Customer reserve

Delta Aggregation

This section describes the procedure for configuring the SAP Connector for Delta Aggregation.

Supported attributes

The SAP Direct Connector supports Delta Aggregation for the following attributes:

- User created
- User deleted
- Password
- User Type
- Administrator lock set // IdentityIQ Disabled
- Administrator lock released // IdentityIQ Enabled
- Incorrect logon lock set // IdentityIQ Locked
- Incorrect logon lock released // IdentityIQ Unlocked
- Validity Period
- Account Number
- User Group
- SAP Profile(s) Assigned
- SAP Profile(s) Deleted
- Security Policy

Importing the BAPIs

This section describes how to import the transport request that contains the non - certified function modules used by SAP Connector to achieve the delta aggregation functionality.

Function modules are imported using one of the following methods:

- Using the Transport Control program manually
- Using the menu-driven administration of Transport Requests via SAP GUI

Pre-requisites

Copy the API Transport files to SAP. Use the following procedure to unpack and import the transport files function modules:

1. Copy the transport files.

Transport request is contained in the `ImportSAPDirect.TAR` compressed file.

The compressed file for each release contains the following files:

- `RrequestNumber.sapId`
- `KrequestNumber.sapId`

Using WinZip or a similar utility, uncompress and copy each file from the appropriate compressed file to the subdirectory of the local transport directory of the target SAP system as follows:

- Copy the `RrequestNumber.sapId` file to the `sapHomeDir\trans\data\RrequestNumber.sapId` directory.
- Copy the `KrequestNumber.sapId` file to the `sapHomeDir\trans\cofiles\KrequestNumber.sapId` directory.

Note: The values of *requestNumber* and *sapId*. These values are required later.

Additional information

Using the Transport Control Program manually

1. At the command prompt (for both Microsoft Windows or UNIX systems), enter the following command to register the transport with the buffer:
`os prompt> tp addtobuffer sapIdKrequestNumber yourSid`
In the preceding command line, *sapId* and *requestNumber* were determined in step 1 of “Pre-requisites”.
2. Enter the following command to import the above transport request in to your SAP Solutions system:
`os prompt>tp import sapIdKrequestNumber yourSid client=yourClient U126`
After executing the `tp import` command, the system issues a return code, indicating the status of the import. The most common return codes are described in the table below:

Table 2—Transport Request Import - Common Return Codes

Return Code	Description
0	Successful import. The Transport imported successfully.
4	Warning status. Minor version differences were detected. The Transport Imported successfully. (No action is required.)

Importing the Transport via SAP GUI

If you are running SAP GUI, use the following procedure for importing the function modules:

1. Log in to SAP GUI with administrator permissions.
2. Perform one of the following:
 - From the Command field, run transaction STMS
 - OR
 - From the menu, select **Tools => Administration => Transports => Transport management system**.
3. In the Transport Management System window, press **F5**.
4. In the Import Overview window, double-click your system queue.
The requests list for the system is displayed.
5. From the menu bar in the Import Queue window, select **Extras => Other requests => Add**.
6. Enter the request number and click **Yes**.
7. In the Attach to import queue message box, click **Yes**.
8. In the Import Queue window, click on the new line, and then press **Ctrl + F11** to import the request.
9. In the Import Transport Request dialog box, perform the following:
 - a. In the Target client field, enter the name of the SAP client to which you want to import the transport.
 - b. On the Date tab, under Start Date, set the values that you require.
 - c. On the Execution tab, under Import, ensure that **Synchronous** is selected.
 - d. On the Options tab, under Import options, ensure that all of the check boxes are selected.
10. In the Start Import dialog box, click **Yes**.

Verification

All non-validated function modules are transported as a function group whose name starts with SailPoint's unique namespace ("/SAILPOIN")

To verify that the required function modules have been imported in to the SAP system, perform the following:

1. In the SAP system, execute **SE37** transaction.
2. Enter: /SAILPOIN/* in the Function Module field.
3. Press the **F4** key.
This displays the Repository Info System window that lists all the imported functional modules currently available on the SAP system as follows:
 - SAILPOIN/USR_CHANGE_DOC_ROLES
 - SAILPOIN/USR_CHANGE_DOC_USERS

Partitioning Aggregation

To use the partitioning aggregation feature in IdentityIQ for SAP ERP perform the following:

1. Select the **Partition Enabled** check box.
2. Specify the criteria for partitioning in the **Partition Statements** textbox of the configuration parameter. IdentityIQ for SAP ERP accepts multiple characters in partition statement.
For example, **-AZ, -MZ, KA-RL, SA-SZ** and **ABG-ASHI**
The **AL-** and **K-** values are not accepted in the partition statement.
To specify more than one partition the entries must be separated using a newline character.

Troubleshooting

1 - Distribution of a user to SAP CUA Subsystem

In a SAP CUA landscape, a SAP role or profile requires a SUBSYSTEM to distribute the user to. The facility to select or specify the same, while requesting an entitlement for an account, is absent in IdentityIQ.

Workaround: The subsystem name is prepended to the Account-Group while aggregating account-groups from a SAP CUA system. As a result, only a limited subset of subsystem and account-group combinations will be available while requesting entitlements, and thus distributing users, in a SAP CUA landscape.

2 - Removed Entitlements are present in Current access page

Even after the execution of **Refresh Entitlement Correlation** the entitlements are not getting deleted from the current access page.

Workaround: Execute the **Perform Identity Request Maintenance** task to remove those entitlements. Ensure that the **Verify provisioning for requests** option is selected for this task.

3 - Password not set in permanent mode

After upgrade to the existing application, the password is not set in permanent mode, even when the user is created with the **Password in permanent mode** attribute selected.

This behavior occurs since the attribute name has changed from **Password in permanent mode** to **Productive Password**.

Troubleshooting

Workaround: In the debug page rename **Password in permanent mode** to **Productive Password** in schema and provisioning plan.

4 - Few attributes are not working after upgrading to version 7.3 Patch 3

Few attributes are not working after upgrading from version 6.0 patch 7 and version 6.1 to version 7.3 Patch 3.

Resolution: Open the application debug page of version 6.4 and use the following corresponding parameters:

Parameters used in version 6.0 patch 7/6.1	Parameters to be used in version 7.3 Patch 3
Password in permanent mode	Productive Password
Deactivate	Password Deactivated
LASTNAME	Last name
Reference User Name	Reference User
User Last Login	User Last Logon Time

5 - Login fails for non aggregated accounts when pass through is enabled

Login fails for non aggregated accounts when pass through is enabled.

In IdentityIQ for SAP ERP the SAPJCO libraries are used, which need permission to make connection with SAP Server. The user who does not have these permissions will not be able to log in and will not be a valid member of the authentication process.

Resolution: Perform the following to add the administrator permissions:

1. Run the **PFCG** transaction (Profile generator, maintain your roles, authorizations, and profiles) and enter the role name.
2. Click on **Single** and save the Role created.
3. Click on **Authorization Tab => Display Authorization Data**.
Template will appear, cancel the template.
4. Click on **Manual** tab and add the following:
 - S_RFC (All Activities)
 - S_USER_AGR (Activities: 02, 03, 22, 36, 78)
 - S_USER_GRP (Activities: 01, 02, 03, 05, 06, 22, 78)
 - S_USER_PRO (Activities: 01, 02, 03, 06, 07, 22)
 - S_USER_AUT (Activities : 03, 08)
 - S_USER_SAS (Activities : 01, 06, 22)
 - S_TABU_DIS (Activities: All Activities)(Additionally for SAP CUA System) S_USER_SYS (Activities: 03, 59, 68, 78)
 - Click on the **Generate (Shift+F5)** icon.
 - Click on the **Save (Ctrl+S)** icon.
 - Click on **Back (F3)** icon.

5. Click on the **Generate (Shift+F5)** icon and assign the above created role to a SAP user who must be an administrator.
6. Run the **PFCG** transaction.
7. Provide the role name which the customer has created.
8. Click on **USER tab => User Comparison**.

6 - When performing Delta Aggregation after upgrade, an error message appears

When performing Delta Aggregation after upgrade, the following error message appears:

Aggregation date needs to be set in configuration.

Resolution: Open the SAP-Direct application debug page and set the following parameters:

```
<entry key="lastAggregationDate" value="2014-06-21"/>
<entry key="lastAggregationTime" value="20:54:34"/>
```

In the above parameters the format of Date and Time are as follows:

- **Date:** yyyy-MM-dd (the date should be the current date of the SAP server)
- **Time:** HH:mm:ss (the time should be the current time of the SAP server)

7 - Change password feature is not working with SNC, when PRODUCITVE_PWD attribute is X

Change password feature is not working with SNC, when PRODUCITVE_PWD attribute is X.

Resolution: Define the **productivePasswordValue** attribute in debug pages as follows:

```
<entry key="productivePasswordValue" value="1">
```

By default the code would consider the value as x.

8 - Aggregation fails with error 'NOT AUTHORIZATION'

Aggregation fails with the following error due to not having proper authorization of authorization object 'S_TABU_DIS (Activities: All Activities)'.

Resolution: Provide the authorization of authorization object 'S_TABU_DIS (Activities: All Activities)'

Activities-All

Table Authorization Group-* (means all)

Or skip aggregation of license data of the user by adding the following entry key in debug pages of the application:

```
<entry key="skipLicenseData">
  <value>
    <Boolean>true</Boolean>
  </value>
</entry>
```

9 - Test connection fails with an error message

Test connection fails with the following error message:

Troubleshooting

```
com.sap.conn.rfc.driver.CpicDirver
```

Resolution: Download the latest SAPJCO.jar and SAPJCO.dll files from SAP Marketplace and then use that SAPJCO Jar file with the latest downloaded SAPJCO dll file.

10 - Role and Profile description in a language other than English

Resolution: In Account-Group Aggregation, if the Role and Profile Description is required in a language other than English language, add the **descriptionLanguage** parameter with the correct value.

For example, `<entry key="descriptionLanguage" value="D"/>`

In the above example, the value 'D' is the language code for Dutch language supported by SAP.

If the **descriptionLanguage** parameter is not provided, the descriptions displayed are in English language.

11 - Login to IdentityIQ fails for username and password with utf8 characters

The following error message appears when login to IdentityIQ for username and password with utf8 characters:

```
ERROR http-8080-1 sailpoint.server.Authenticator:323 -  
sailpoint.connector.AuthenticationFailedExcept  
com.sap.conn.jco.JCoException: (109) RFC_ERROR_CANCELLED: Handle close pending
```

Resolution: Add the following entry in the application debug page:

```
<entry key="jco.client.codepage" value="4110"/>
```

12 - Test connection/aggregation fails with an error message

Test connection / aggregation fails with the following error message:

```
Bad username or password. com.sap.conn.jco.JCoException: (109)  
RFC_ERROR_CANCELLED: Handle close pending
```

Resolution: Ensure that the administrator user specified in application has sufficient rights on the SAP systems as mentioned in the “Administrator permissions” on page 145 section.

13 - Test connection/aggregation fails if user name or password contain UTF-8 character

Resolution: Add the following entry in the application debug page:

```
<entry key="jco.client.pcs" value="2"/>
```

14 - Test Connection fails with an error even when all the required libraries are there in the required path

Test connection fails with the following error may be due to the libraries not getting loaded in Java even when all the required libraries are there in the required path:

```
[ConnectorException] [Error details] Destination Listener not initialized. Please  
make sure that all required libraries are in path.
```

Resolution: This issue can be resolved by performing the following procedure:

1. Create a folder/directory and place all the required libraries in it as mentioned in “Pre-requisites” on page 145.

2. Set the following environment variable:

- `LD_LIBRARY_PATH` => location of libraries in Linux
- `PATH` => location of libraries in Windows

For example, `LD_LIBRARY_PATH=/home/admin/lib`

Chapter 16: IdentityIQ for Oracle ERP – Oracle E-Business Suite

The following topics are discussed in this chapter:

Overview	167
Supported features	167
Supported Managed Systems	168
Pre-requisites	168
Administrator permissions	168
Configuration parameters	171
Additional configuration parameter	173
Schema attributes	174
Account attributes	174
Group attributes	176
Provisioning Policy attributes	177
Create account attributes	177
Create group attributes	177
Additional information	178
Troubleshooting	180

Overview

The Oracle E-Business Suite is an integrated suite of development, runtime, and system management tools. It also includes Forms, JDeveloper, Single Sign-On, Oracle Internet Directory, Portal, Discoverer, Web Cache, Integration, Oracle BPEL Process Manager.

IdentityIQ for Oracle ERP – Oracle E-Business Suite controls the activities related to account/groups by signing in managed system. IdentityIQ for Oracle ERP – Oracle E-Business Suite will manage the following entities of Oracle E-Business Suite:

- User
- Group (Responsibility, Role)

Supported features

IdentityIQ for Oracle ERP – Oracle E-Business Suite supports the following features:

- Account Management
 - Manages Oracle E-Business Suite users
 - Aggregation, Refresh Accounts, Discover Schema
 - Create, Update
 - Enable, Disable, Change Password
 - Add/Remove Entitlements

Overview

- Account - Group Management

Supports multiple group functionality.

- Manages Oracle E-Business Suite groups as RESPONSIBILITY

- Aggregation, Refresh Groups

The following versions represent the respective responsibilities:

- 4: Oracle Applications
- W: Oracle Self-Service Web Applications
- M: Oracle Mobile Applications

IdentityIQ for Oracle ERP – Oracle E-Business Suite aggregates responsibilities of only type '4' 'W' and 'M'. Hence Account-Group aggregation fetches only responsibilities of type 'Oracle Applications' 'Self-Service Web Applications' and 'Oracle Mobile Application'.

For more information on upgraded application of IdentityIQ, see "Upgrade considerations" on page 178.

- Create, Update
- Manages Oracle E-Business Suite groups as ROLE
- Aggregation, Refresh Groups

Supported Managed Systems

Following versions of Oracle E-Business Suite are supported by the IdentityIQ for Oracle ERP – Oracle E-Business Suite:

- Oracle E-Business Suite 12.2.1 to 12.2.6
- Oracle E-Business Suite 12.1.x

Pre-requisites

The compatible JDBC drivers must be used in the classpath of IdentityIQ for connecting to Oracle E-Business Server. For example, `ojdbc6.jar`.

Administrator permissions

Note: - *(For Invoker rights only)* After upgrading IdentityIQ to version 7.3 Patch 3, invoke the upgraded wrapper packages. For invoking the new wrapper package, additional permissions must be provided.
- Few additional permissions are required for definer rights also.
For more information on the additional permissions, see "Additional Administrator permissions" on page 171.

1. Rights present on Oracle packages:

Enter the following command to find the rights present on the Oracle packages:

```
SELECT dbo.object_name ,  
(DECODE(SIGN(bitand(options,16)),1,'INVOKER','DEFINER')) "authid"  
FROM dba_objects dbo, sys.PROCEDURE$ p
```



```
WHERE p.obj# = dbo.object_id
AND dbo.object_type = 'PACKAGE'
AND dbo.object_name = 'xxx'
AND dbo.owner = 'APPS';
```

Where **xxx** package is FND_USER_PKG, FND_RESPONSIBILITY_PKG, WF_LOCAL_SYNCH, FND_WEB_SEC, FND_GLOBAL, or FND_USER_RESP_GROUPS_API.

Sample example:

Enter the following command to find the rights present on the FND_USER_PKG:

```
SELECT dbo.object_name,
(DECODE(SIGN(bitand(options,16)),1,'INVOKER','DEFINER')) "authid"
FROM dba_objects dbo, sys.PROCEDURE$ p
WHERE p.obj# = dbo.object_id
AND dbo.object_type = 'PACKAGE'
AND dbo.object_name = 'FND_USER_PKG'
AND dbo.owner = 'APPS';
```

2. If **xxx** package has Invoker rights, perform the following:

Copy the package scripts from

identityiq\integration\OracleEBS\iiqIntegration-OracleEBS.zip directory to the OracleHome\bin directory and rename the type of scripts from *.txt to *.sql

Using SQL*Plus, log in to the Oracle database as APPS and run the following:

Run the @SP_xxx package script using SQL*Plus

Sample example: If FND_USER_PKG has invoker rights, run the @SP_FND_USER _PKG script using SQL*Plus
Perform this step for all **xxx** packages.

3. Log in to the Oracle database as database administrator for creating the new administrator user account using SQL*Plus as follows:

```
create role ${new role};
create user ${new user} identified by ${password};
grant create session to ${new user};
grant create synonym to ${new user};
grant ${new role} to ${new user};
```

Grant permissions to the new role created in the above step (\${new role}):

```
grant select on APPS.FND_PRODUCT_GROUPS to ${new role};
grant select on APPS.FND_USER to ${new role};
grant select on SYS.DBA_USERS to ${new role};
grant select on APPS.FND_RESPONSIBILITY_VL to ${new role};
grant select on APPS.FND_APPLICATION_VL to ${new role};
grant select on APPS.FND_DATA_GROUPS to ${new role};
grant select on APPS.FND_USER_RESP_GROUPS_ALL to ${new role};
grant select on DUAL to ${new role};
grant select on APPS.PER_ALL_PEOPLE_F to ${new role};
grant select on APPS.RA_CUSTOMERS to ${new role};
grant select on APPS.FND_MENUS to ${new role};
grant select on APPS.FND_REQUEST_GROUPS to ${new role};
grant select on APPS.FND_APPLICATION to ${new role};
grant select on APPS.FND_DATA_GROUP_UNITS to ${new role};
grant select on APPS.FND_APPLICATION_TL to ${new role};
grant select on APPS.FND_RESPONSIBILITY to ${new role};
```

```
grant select on APPS.WF_ROLES to ${new role};
grant select on APPS.WF_LOCAL_ROLES to ${new role};
grant select on APPS.WF_ALL_ROLES_VL to ${new role};
grant select on APPS.WF_ROLE_HIERARCHIES to ${new role};
grant select on APPS.FND_REQUEST_GROUP_UNITS to ${new role};
```

- If **xxx** package has Definer rights, perform the following:

```
grant execute on APPS.xxx to ${new role};
For example, grant execute on APPS.FND_USER_PKG to ${new role};
```

- If **xxx** package has Invoker rights, perform the following:

```
grant execute on APPS.SP_XXX to ${new role};
For example, grant execute on APPS.SP_FND_USER_PKG to ${new role};
```

Where **xxx** package is FND_USER_PKG, FND_RESPONSIBILITY_PKG, WF_LOCAL_SYNCH, FND_WEB_SEC, FND_GLOBAL, or FND_USER_RESP_GROUPS_API.

4. Login by the new user name \${new user} and create the following synonym:

```
create synonym FND_PRODUCT_GROUPS for APPS.FND_PRODUCT_GROUPS;
create synonym FND_USER for APPS.FND_USER;
create synonym DBA_USERS for SYS.DBA_USERS;
create synonym FND_RESPONSIBILITY_VL for APPS.FND_RESPONSIBILITY_VL;
create synonym FND_APPLICATION_VL for APPS.FND_APPLICATION_VL;
create synonym FND_DATA_GROUPS for APPS.FND_DATA_GROUPS;
create synonym FND_USER_RESP_GROUPS_ALL for APPS.FND_USER_RESP_GROUPS_ALL;
create synonym PER_ALL_PEOPLE_F for APPS.PER_ALL_PEOPLE_F;
create synonym RA_CUSTOMERS for APPS.RA_CUSTOMERS;
create synonym FND_MENUS for APPS.FND_MENUS;
create synonym FND_REQUEST_GROUPS for APPS.FND_REQUEST_GROUPS;
create synonym FND_APPLICATION for APPS.FND_APPLICATION;
create synonym FND_RESPONSIBILITY for APPS.FND_RESPONSIBILITY;
create synonym FND_APPLICATION_TL for APPS.FND_APPLICATION_TL;
create or replace synonym FND_DATA_GROUP_UNITS for APPS.FND_DATA_GROUP_UNITS;
create or replace synonym WF_ROLES for APPS.WF_ROLES;
create or replace synonym WF_LOCAL_ROLES for APPS.WF_LOCAL_ROLES;
create or replace synonym WF_ROLE_HIERARCHIES for APPS.WF_ROLE_HIERARCHIES;
create or replace synonym WF_ALL_ROLES_VL for APPS.WF_ALL_ROLES_VL;
create synonym FND_REQUEST_GROUP_UNITS for APPS.FND_REQUEST_GROUP_UNITS;
```

- If **xxx** package has Definer rights, perform the following:

```
create or replace synonym xxx for APPS.XXX;
For example, create or replace synonym FND_USER_PKG for APPS.FND_USER_PKG;
```

- If **xxx** package has Invoker rights, perform the following:

```
create or replace synonym xxx for APPS.SP_XXX;
For example, create or replace synonym FND_USER_PKG for APPS.SP_FND_USER_PKG;
```

Where **xxx** package is FND_USER_PKG, FND_RESPONSIBILITY_PKG, WF_LOCAL_SYNCH, FND_WEB_SEC, FND_GLOBAL, or FND_USER_RESP_GROUPS_API.

Note: If table ar_customers exist instead of ra_customer then provide the select permissions as follows:

```
grant select on APPS.AR_CUSTOMERS to ${new role};
```

Also the synonym must be as follows:

```
create synonym RA_CUSTOMERS for APPS.AR_CUSTOMERS;
```

Additional Administrator permissions

Sr.No	Permissions to Role	Synonyms
Definer		
1	grant execute on APPS.FND_USER_RESP_GROUPS_API TO \${new role};	create or replace synonym FND_USER_RESP_GROUPS_API for APPS.FND_USER_RESP_GROUPS_API;
Invoker		
2	grant execute on APPS.SP_FND_USER_RESP_GROUPS_API TO \${new role};	create or replace synonym FND_USER_RESP_GROUPS_API for APPS.SP_FND_USER_RESP_GROUPS_API;
Definer/Invoker		
3	grant select on APPS.WF_LOCAL_USER_ROLES TO \${new role};	create or replace synonym WF_LOCAL_USER_ROLES for APPS.WF_LOCAL_USER_ROLES;
4	grant select on APPS.FND_USER_RESP_GROUPS_DIRECT TO \${new role};	create or replace synonym FND_USER_RESP_GROUPS_DIRECT for APPS.FND_USER_RESP_GROUPS_DIRECT;
5	grant select on APPS.PER_PERIODS_OF_PLACEMENT TO \${new role};	create synonym PER_PERIODS_OF_PLACEMENT for APPS.PER_PERIODS_OF_PLACEMENT;
6	grant select on APPS.PER_PERIODS_OF_SERVICE TO \${new role};	create synonym PER_PERIODS_OF_SERVICE for APPS.PER_PERIODS_OF_SERVICE;

Note: After upgrading to the IdentityIQ version 7.3 Patch 3, aggregation would fail for all the service accounts with older permissions.

Configuration parameters

The following table lists the configuration parameters of IdentityIQ for Oracle ERP – Oracle E-Business Suite:

Note: Attributes marked with * sign are the mandatory attributes.

Attributes	Type	Description
Oracle E-Business Connection Settings		
Connection User*	The Oracle EBS Login name through which we want to connect Oracle EBS. For example, APPS	
Password*	The authentication details of login.	

Configuration parameters

Attributes	Type	Description
Database URL*		<p>The url to connect to the database. The format is <code>jdbc:oracle:thin:@<HOST>:<PORT>:<SID></code></p> <p>For example <code>jdbc:oracle:thin:@xxx.xx.xx.xx:1521:ORCL</code> url consist of</p> <ul style="list-style-type: none"> • jdbc:oracle:thin:@: This is common part which states that the connection is made using thin driver. • xxx.xx.xx.xx: server Name or IP of the oracle server • 1521: The port number of the oracle server. This port number should be known by the oracle server administrator. • ORCL: The SID of the oracle server.
JDBC Driver*		<p>It is the name of the Driver class supported by JDBC Type 4. For example, <code>oracle.jdbc.driver.OracleDriver</code></p>
E-Business Proxy User		<p>(Optional) E-Business Proxy User for Audit purpose. This user must be created in Oracle E-Business Suite Portal. Audit records would be created/updated with this user for all provisioning operations done for Oracle E-Business through IdentityIQ.</p> <p>If not provided an error would be displayed on Oracle E-Business Portal when user tries to view Record History for any user and his/her assigned entitlements.</p> <p>Note: Set the following permissions as mentioned in the "Administrator permissions" on page 168 when 'E-Business Proxy User' parameter is not set:</p> <ul style="list-style-type: none"> • Under Grant Permissions: <code>grant select on SYS.DBA_USERS to \${new role};</code> • Creating the synonym: <code>Create synonym DBA_USERS for SYS.DBA_USERS</code>
Additional Connection Parameters		<p>This text box can be used to specify the additional configuration parameters. These additional parameters must be passed in key value pairs. If multiple parameters must be specified, then they need to be passed in new line.</p> <p>For example,</p> <pre>oracle.net.encryption_client=ACCEPTED oracle.net.encryption_types_client=AES256</pre>
Account Aggregation Settings		
<p>Note: To use the Account Aggregation Settings, see 'Account Aggregation Filters' under "Upgrade considerations" on page 178.</p>		

Attributes	Type	Description
Account Aggregation Filters	Select the type of users to be aggregated: Employees, Contractors, Employee and Contractors , and all users from FND_USER table .	
	Aggregate only employees	Select to aggregate Oracle E-Business users that are associated with valid Employee records of Oracle HRMS system.
	Aggregate only contractors	Select to aggregate Oracle E-Business users that are associated with valid Contractor records of Oracle HRMS system.
	Aggregate employees and contractors	Select to aggregate Oracle E-Business users that are associated with valid Employee and Contractor records of Oracle HRMS system.
	Aggregate all users from FND_USER table in Oracle E-Business	Select to aggregate all the E-Business users that are there in the FND_USER table.
HRMS Person Records Effective From*	All the E-Business records associated with person records active after the date specified here would be aggregated in the connector. Format of the date entered is MM/DD/YYYY.	

Additional configuration parameter

The following table describes the additional configuration parameters that must be set in the application debug page:

Parameter	Description
endDateUserEntitlements	<p>To end date of the roles and responsibilities on disabling an Oracle E-Business Suite account, set the value of <code>endDateUserEntitlements</code> parameter to true as follows:</p> <pre><entry key="endDateUserEntitlements"> <value> <Boolean>true</Boolean> </value> </entry></pre>
useEffectiveDate	<p>To aggregate all the Oracle E-Business users without any aggregation filters, set the value of <code>useEffectiveDate</code> parameter to false as follows:</p> <pre><entry key="useEffectiveDate"> <value> <Boolean>>false</Boolean> </value> </entry></pre> <p>Note: For more information, see "Upgrade considerations" on page 178.</p>

Schema attributes

Parameter	Description
skipFutureAssignedGroups	<p>To aggregate and provision future dated E-Business users, set the value of skipFutureAssignedGroups parameter to false as follows:</p> <pre><entry key="skipFutureAssignedGroups"> <value> <Boolean>false</Boolean> </value> </entry></pre> <p>Note: For more information, see "Upgrade considerations" on page 178.</p>
disableOldFNDAccounts	<p>(Applicable only for Create User) To disable any existing active FND accounts, set the value of disableOldFNDAccounts parameter to true as follows:</p> <pre><entry key="disableOldFNDAccounts"> <value> <Boolean>true</Boolean> </value> </entry></pre> <p>Note: For more information, see "Upgrade considerations" on page 178.</p>
useResponsibilityWithApplication	<p>To identify responsibility group uniquely for new applications, use the combination of Responsibility_id and Application_id, set the value of useResponsibilityWithApplication parameter to true as follows:</p> <pre><entry key="useResponsibilityWithApplication"> <value> <Boolean>true</Boolean> </value> </entry></pre> <p>Note: For more information, see "Upgrade considerations" on page 178.</p>

Schema attributes

This section describes the different schema attributes.

Account attributes

The following table lists the account attributes:

Attributes	Description
USER_NAME	Application username (what a user types in at the Oracle Applications sign-on screen).
USER_ID	Application user identifier.
START_DATE	The date the user name becomes active.

Attributes	Description
END_DATE	The date the user name becomes inactive.
DESCRIPTION	Description.
PASSWORD_DATE	The date the current password was set.
PASSWORD_EXPR	The number of accesses left for the password.
PASSWORD_NO_OF_DAYS	The number of accesses allowed for the password.
EMAIL_ADDRESS	The electronic mail address for the user.
FAX	The fax number for the user.
EMPLOYEE_ID	Identifier of employee to whom the application username is assigned.
EMPLOYEE_NUMBER	Unique number of the employee.
FULL_NAME	Full name of the user.
CUSTOMER_ID	Customer contact identifier. If the AOL user is a customer contact, this value is a foreign key to the corresponding customer contact.
CUSTOMER_NAME	Customer name.
RESPONSIBILITIES	Responsibilities assigned to a user.
ROLES	Roles assigned to a user.

Custom attributes

Perform the following to support the custom attributes in IdentityIQ for Oracle ERP – Oracle E-Business Suite:

- Add the custom attribute name in the account schema by clicking **Add attribute** button.

Note: If custom attributes are required in the schema, a 'jdbcbuildmap' rule is required.

- Add the following lines in the application debug page:

```
<entry key = "customAttribute" >
  <value>
    <List>
      <String>custom1</String>
      <String>custom2</String>
    </List>
  </value>
</entry>
```

Discover Schema

Discover schema replaces the schema attributes by columns from the **FND_USER** table by deleting all the other schema attributes not present in **FND_USER** table (except the roles and responsibility attributes).

If there are any correlation rules using attributes other than the columns from **FND_USER** table, then they must be added again.

Group attributes

This section describes the different group attributes.

Responsibility GroupObjectType attributes

The following table lists the Responsibility GroupObjectType attributes:

Attributes	Description
RESPONSIBILITY_ID	Responsibility identifier.
RESPONSIBILITY_NAME	Name of the responsibility.
RESPONSIBILITY_KEY	Internal developer name for responsibility.
START_DATE	The date the responsibility becomes active.
END_DATE	The date the responsibility expires.
DESCRIPTION	Description
STATUS	Shows status of the responsibility.
VERSION	Version
WEB_HOST_NAME	IP address or alias of the computer where the Webserver is running. Defaults to the last agent.
WEB_AGENT_NAME	Name of Oracle Web Agent. Defaults to the last agent.
DATA_GROUP_APPL_NAME	Name of the data group application.
REQUEST_GROUP_APPL_NAME	Request Group Application name.
DATA_GROUP_ID	Identifier of data group.
DATA_GROUP_NAME	Name of the Data Group.
MENU_NAME	Name of the menu.
REQUEST_GROUP_NAME	Request group name.

Role GroupObjectType attributes

The following table lists the Role GroupObjectType attributes:

Attributes	Description
NAME	An internal name for the role.
DISPLAY_NAME	The display name of the role.
DESCRIPTION	Description
START_DATE	The date at which the role becomes valid.
EXPIRATION_DATE	The date at which the role is no longer valid in the directory service.
APPLICATION_NAME	Application that owns the information for the role.
STATUS	The availability of the Role to participate in a workflow process.

Attributes	Description
SUBORDINATE_ROLES	Subordinate roles for a role.
SUBORDINATE_RESPONSIBILITIES	Subordinate responsibilities for a role.

Provisioning Policy attributes

This section lists the single provisioning policy attributes of IdentityIQ for Oracle ERP – Oracle E-Business Suite that allows you to select the type of user/group to create.

Note: Attributes marked with * sign are the mandatory attributes.

Create account attributes

The following table lists the provisioning policy attributes for Create Accounts:

Attributes	Description
Name*	Name of the login user.
Password*	Password of the login user.
Description	Description.
Start Date*	The date from which login user becomes active.
End Date	The date from which login user becomes inactive.
Password Expiration Type	Type of the password to expire.
Number of Days	Days after which user password will expire.
Permanent Mode	In permanent mode change of password on first login is not required.
Employee ID	Person ID of the employee or contractor from the Oracle-HRMS system. Note: Applicable to new application of Oracle E-Business Suite after upgrading IdentityIQ to version 7.3 Patch 3.

Create group attributes

The following table lists the provisioning policy attributes for Create Group (Responsibility):

Attributes	Description
Responsibility Name*	Name of the responsibility.
Application Name	(Read only) Name of the application.
Description	Description
Responsibility Key*	Internal developer name for responsibility.
Start Date*	The date the responsibility becomes active.
End Date	The date the responsibility expires.

Additional information

Attributes	Description
Responsibility Version*	Responsibility version.
Data Group Name*	Name of the data group.
Data Group Application Name*	Name of the data group application.
Menu Name*	Name of the menu.
Request Group Name	Request group name.
Request Group Application Name	Request group application name.

Additional information

This section describes the additional information related to the IdentityIQ for Oracle ERP – Oracle E-Business Suite.

Upgrade considerations

- *(Optional)* After upgrading to IdentityIQ version 7.3 Patch 3, perform the following for provisioning of a responsibility of type other than 'Oracle Applications':
 - a. Navigate to **Provisioning Policies ==> Create Group**.
 - b. Click on **Edit** icon of **Responsibility Version** field and in **Edit Options ==> Settings**, modify the name from **PASSWORD_EXPR** to **VERSION**.
 - c. Click on **Edit Options ==> Value settings** in the Allowed Values field enter **Oracle Mobile Application** and click on + icon.
 - d. Click on **Apply** and **Save** the provisioning policy.
 - e. Click **Save** on the next screen and save the Application.
- **Account Aggregation Filters**

After upgrading to IdentityIQ version 7.3 Patch 3, by adding `<entry key="useEffectiveDate" value="true"/>` parameter in the application debug page users have the ability to select the type of users to be aggregated: **Employees**, **Contractors**, **Employees and Contractors** or **all users from FND_USER table**. For more information on adding the `useEffectiveDate` parameter, see "Additional configuration parameter" on page 173.
- **Assigning responsibilities to future dated E-Business users**

After upgrading to IdentityIQ version 7.3 Patch 3, the Oracle E-Business Suite connector would be able to provision and aggregate future E-Business users. If responsibilities are provided in the create request of future user, the connector would use user's start date for responsibility assignment's start date. For provisioning of future dated users for application created prior to IdentityIQ version 7.3 Patch 3, add the `skipFutureAssignedGroups` entry key to the application debug page. For more information, see "Additional configuration parameter" on page 173.
- **Disabling existing accounts during provisioning**

After upgrading to IdentityIQ version 7.3 Patch 3, the Oracle E-Business Suite connector would be able to disable any existing active FND accounts. For disabling any active FND accounts for application created prior to IdentityIQ version 7.3 Patch 3, set the value of the `disableOldFNDAccounts` parameter to true in the application debug page. For more information, see "Additional configuration parameter" on page 173.

- **Identifying responsibility group uniquely**

After upgrading to IdentityIQ version 7.3 Patch 3, the Oracle E-Business Suite connector can use combination of Responsibility_id and Application_id to identify responsibility group uniquely for new applications.

For existing application user can use this feature by setting the value of useResponsibilityWithApplication to true in the application debug page.

For more information, see "Additional configuration parameter" on page 173.

Note: After setting the value of useResponsibilityWithApplication attribute to true, previous entitlement data cannot be retrieved.

- After upgrading to IdentityIQ version 7.3 Patch 3, the Oracle E-Business Suite Connector would not aggregate indirect roles and responsibilities assigned to Oracle E-business users during account aggregation.
- After upgrading to IdentityIQ version 7.3 Patch 3, for aggregating disabled accounts on the previous application of Oracle E-Business Suite, set the value of the aggregateActiveAccounts parameter to false in the application debug page.

Support for Oracle Security Feature

Note: Oracle recommends the use of standard security feature (network encryption and Data integrity feature).

With this release of IdentityIQ, Oracle ERP – Oracle E-Business Suite is enhanced to support the network encryption and Data integrity feature for the Oracle Database target system.

This functionality can be leveraged by providing the required values for **Additional Connection Parameters** configuration parameter added under the "Configuration parameters" on page 171.

For example, oracle.net.encryption_client=REJECTED

User Editions

(Applicable only for Administrator User Account) For Oracle Database version 11g R2 and above which allow the Edition-based Redefinition, when creating new database user, enable editions on that user by using the following command on the database to avoid any errors while creating the synonyms:

```
alter user ${new user} enable editions;
```

For more information on Administrator User Account, see "Administrator permissions" on page 168.

Support of provisioning of Start Date, End Date and Justification attributes

With IdentityIQ version 7.3 Patch 3, Oracle E-Business connector supports provisioning of Start and End Date and the justification attributes when assigning a role or responsibility using the following sample Plan:

```
<!DOCTYPE ProvisioningPlan PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<ProvisioningPlan nativeIdentity="AccountName">
  <AccountRequest application="ApplicationName" nativeIdentity="AccountName"
    op="Modify">
    <AttributeRequest name="ROLES" op="Add" value="RoleCode">
```

Troubleshooting

```
<Attributes>
  <Map>
    <entry key="assignment" value="true" />
    <entry key="endDate">
      <value><String>YYYY/MM/DD</String></value>
    </entry>
    <entry key="startDate">
      <value><String>YYYY/MM/DD</String></value>
    </entry>
  </Map>
</Attributes>
</AttributeRequest>
<AttributeRequest name="RESPONSIBILITIES" op="Add" value="RESPONSIBILITIES_ID">
  <Attributes>
    <Map>
      <entry key="assignment" value="true"/>
      <entry key="endDate">
        <value><String>YYYY/MM/DD</String></value>
      </entry>
      <entry key="startDate">
        <value><String>YYYY/MM/DD</String>
      </value>
      </entry>
    </Map>
  </Attributes>
</AttributeRequest>
</AccountRequest>
</ProvisioningPlan>
```

Troubleshooting

1 - Provisioning and Aggregation would fail with the an error message on previous application of Oracle E-Business Suite after upgrading IdentityIQ to version 7.3 Patch 3

After upgrading IdentityIQ to version 7.3 Patch 3, provisioning and aggregation would fail with the following error message on previous application of Oracle E-Business Suite:

```
ORA-00942: table or view does not exist
```

Resolution: After upgrading IdentityIQ to version 7.3 Patch 3, for successful provisioning and aggregation operations on previous application of Oracle E-Business Suite, additional permissions from Sr.No 1 to 4 are required as mentioned in the table under the “Additional Administrator permissions” section.

2 - RA_Customers table not found when managing Oracle version 12c

If Customer is using IdentityIQ for Oracle ERP – Oracle E-Business Suite to manage Oracle version 12c, the Integration Module installation expects a table named **RA_Customers**. This table is renamed as **AR_Customers** in Oracle version 12c.

Resolution: Assign the following synonym to the new user,

```
create synonym ra_customers for apps.ar_customers;
```

3 - User must be re-hired who is disabled in native system

When a user must be re-hired who is disabled in native system, the following error message appears on native system:

```
User already exists
```

Resolution: To re-hire user who is disabled in native system, refresh the accounts from IdentityIQ using manage accounts. This corrects the status of the user in IdentityIQ and can be enabled manually from IdentityIQ or native system.

4 - A new user with an existing user name on native system is in disabled state must be newly hired

When a new user must be hired with an old user name on native system is in disabled state, the following error message appears on the native system:

```
User already exists
```

Resolution: IdentityIQ does not have the old user details which is disabled on the native system. The create user request would fail in IdentityIQ with the above error message. Therefore a new name must be entered for the new user.

Chapter 17: IdentityIQ for SAP ERP – SAP Portal - User Management Web Service

The following topics are discussed in this chapter:

Overview	183
Supported features	184
Supported Managed Systems	184
Pre-requisite	184
Administrator permission	185
Configuration parameters	185
Schema attributes	186
Account attributes	186
Group attributes	187
Provisioning Policy attributes	187
Additional information	189
Troubleshooting	189

Overview

SAP Enterprise Portal integrates information and applications across the enterprise to provide an integrated single point of access to information, enterprise applications, and services both inside and outside an organization. IdentityIQ for SAP ERP – SAP Portal - User Management Web Service uses the UME service to perform user management. The User Management Engine (UME) provides a centralized user management for all Java applications and can be configured to work with user management data from multiple data sources.

The UME can be configured to read and write user-related data from and to multiple data sources, such as Lightweight Directory Access Protocol (LDAP) directories, the system database of the AS Java, and user management of an AS ABAP.

IdentityIQ for SAP ERP – SAP Portal - User Management Web Service manages the following entities of SAP User Management Engine (UME):

- User
- Role (UME and Portal)

Supported features

IdentityIQ for SAP ERP – SAP Portal - User Management Web Service supports the following features:

- Account Management
 - Manages SAP Portal users as Accounts
 - Aggregation, Refresh Accounts, Pass Through Authentication
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements
- Account - Group Management
 - Create, Update, Delete
 - Manages SAP Roles as Account-Groups
 - Aggregation

Supported Managed Systems

Following versions of SAP NetWeaver versions are supported by the IdentityIQ for SAP ERP – SAP Portal - User Management Web Service:

- SAP NetWeaver 7.5, 7.4, 7.3, 7.2 and 7.1

Note: IdentityIQ for SAP ERP – SAP Portal - User Management Web Service manages SAP User Management Engine users. For more information, see "Supported features" on page 184.

Pre-requisite

The `sailpoint_ume.sda` file must be deployed on the SAP Enterprise Portal server which must be provisioned.

Perform the following steps to deploy the `sailpoint_ume.sda` file:

1. Copy the SDA file from `($build) / integration / sap / dist` directory to a temporary directory on the SAP server.
2. Navigate to the home directory of SAP Enterprise Portal server
`.. \usr \sap \ (ep_instance_name) \ J02 \ j2ee \ console` on SAP server and execute `textconsole.bat`.
3. Run the following command:
`>DEPLOY tmpDir\sailpoint_ume.sda(location of the sailpoint_ume.sda file)`
where `tmpDir` is the temporary directory where the SDA file is extracted.

For undeploying the `.sda` file, see "Undeploy .sda file" on page 189.

Administrator permission

The administrative account must have the following permissions for performing test connection, aggregation and provision operations:

- pcd:portal_content/administrator/user_admin/user_admin_role
- pcd:portal_content/administrator/system_admin/system_admin_role
- pcd:portal_content/administrator/super_admin/super_admin_role
- SAP_J2EE_ADMIN

Configuration parameters

This section contains the information that this Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for SAP ERP – SAP Portal - User Management Web Service uses the following connection attributes:

Table 1—IdentityIQ for SAP ERP – SAP Portal - User Management Web Service - Primary Attributes

Attribute	Description
UMWebService URL*	<p>The url for the UMWebService. For example:</p> <pre>http://HOST:PORT</pre> <p>In the above url, <i>HOST</i> refers to the instance where SAP Portal-User Management WebService is installed and <i>PORT</i> is the listening port of the server.</p> <p>This url can use either http or https.</p> <p>Note: When using https, the portal server's keystore and the application server's keystore must be configured.</p>
Username*	The SAP Portal user name used when connecting to the web service.
password*	Password for the user account specified in Username.
Account Filter	<p>Enter the string representation of an object filter. Any account object matching the filter is filtered out of the dataset. The following is an example of a filterString that filters out all objects where the uniqueId starts with USER.R3_DATASOURCE:</p> <pre>uniqueId.startsWith(&quot;USER.R3_DATASOURCE.&quot;)</pre> <p>If this property is non-empty, filtering happens on the IdentityIQ server side and does not filter on the SAP portal side.</p>

Schema attributes

Table 1—IdentityIQ for SAP ERP – SAP Portal - User Management Web Service - Primary Attributes

Attribute	Description
Group Filter	<p>Enter the string representation of an object filter. Any roles object matching the filter is filtered out of the dataset. The following is an example of a filterString that filters out all objects from the that have a displayName starting with com.sap.pct:</p> <pre>displayName.startsWith(&quot;com.sap.pct&quot;)</pre> <p>When this property is non-empty filtering happens on the IdentityIQ server side and does not filter on the SAP portal side</p>

Schema attributes

This section describes the different schema attributes.

Note: The attributes marked with * sign are the required attributes.

Account attributes

The following table lists the account attributes:

Attributes	Description
uniqueId	Users unique identification
firstName	Users first name
lastName	Users last name
displayName	Users display name
company	Users company name
title	Users title
uniqueName (Identity Name+ Display Name)	Users unique name
city	Users city
postalCode	Users postal address
email	Users email address
street	Users street
state	Users state
country	Users country
zip	Users postal zip code
fax	Users fax
telephone	Users telephone number
cellPhone	Users cell phone number

Attributes	Description
department	Users department assigned
salutation	Users salutation
jobTitle	Users job title
timeZone	Timezone of the user
language	Language of the user
securityType	Users's security type
lockStatus	User is locked or open
roles	Role assigned to the user
groups	Groups assigned to the user
validFrom	Valid from date
validTo	Valid to date

Group attributes

The following table lists the group attributes:

Attributes	Description
displayName is	Display name of the role
uniqueName identity Attribute	Unique name of the role
uniqueId	Unique ID of the role
description	Description of the role
userMembers	Users associated to the role
groupMembers	Groups associated to the role

Provisioning Policy attributes

This section lists the different policy attributes of IdentityIQ for SAP ERP – SAP Portal - User Management Web Service.

Note: The attributes marked with * sign are the required attributes.

Create account attributes

The following table lists the provisioning policy attributes for Create Account:

Attributes	Description
uniqueId	Users unique identification

Provisioning Policy attributes

Attributes	Description
First Name	Users first name
Last Name*	Users last name
Display Name	Users display name
company	Users company name
Department	Users department assigned
Unique Name*	Users unique name
Password*	Users password
City	Users city
Street	Users street
Email	Users email address
State	Users state
Country	Users country
Zip	Users postal zip code
Fax	Users fax
Tele Phone	Users telephone number
Cell Phone	Users cell phone number
Salutation	Users salutation
JobTitle	Users job title
Language	Language of the user
Security Type	Users's security type
Lock Status	User is locked or open
Password Change Required	<p>To create a new account in SAP Portal Server with productive password.</p> <p>Values are as follows:</p> <ul style="list-style-type: none">• True: Does not sets the password as productive• False: Sets the password as productive. <p>Note: User must add “changePasswordRequired” attribute in schema and create provisioning policy and set the required display name (for example, “Password Change Required”).</p>

Create Group attributes

The following table lists the provisioning policy attributes for Update Account:

Attributes	Description
Role Name*	Display name of the role
Description	Description of the role
User Members	Users associated to the role
Group Members	Groups associated to the role

Additional information

This section describes the additional information related to IdentityIQ for SAP ERP – SAP Portal - User Management Web Service.

Undeploy .sda file

Perform the following steps to undeploy the .sda file:

1. From the command prompt browse the following location:
`..\usr\sap\ (SAP ERP instance) \J02\j2ee\console`
2. Run the following file:
`textconsole.bat`
3. At the query prompt enter the following command:
`>UNDEPLOY name=SailpointSapEPArchive vendor=sailpoint.com`

Troubleshooting

1 - Aggregation fails with an error message

During aggregation when SAP Portal Server is connected to Active Directory/LDAP Server, the following error message appears:

Reason: `java.lang.NullPointerException`

Resolution: Undeploy the existing **sailpoint_ume.sda** file and deploy the new **sailpont_ume.sda** file. For more information, see “Undeploy .sda file” on page 189.

Chapter 18: IdentityIQ for Oracle ERP – PeopleSoft

The following topics are discussed in this chapter:

Overview	191
Supported features	191
Supported Managed Systems	192
Pre-requisites	192
Administrator permission	192
Configuration parameters	192
Schema attributes	194
Account attributes	194
Group attributes	195
Additional information	196
Creating the Component Interfaces	196
Partitioning Aggregation	196
Performance improvement	196
Creating the Component interface jar file	198
Configuring the Component Interface Security	199
Upgrade considerations	200
Troubleshooting	200

Overview

The IdentityIQ for Oracle ERP – PeopleSoft manages the administrative entities of PeopleSoft server (User Profiles and Roles). The IdentityIQ for Oracle ERP – PeopleSoft communicates to the PeopleSoft server through component interfaces.

Supported features

IdentityIQ for Oracle ERP – PeopleSoft supports the following features:

- Account Management
 - Manages PeopleSoft users as Accounts
 - Aggregation, Partitioning Aggregation, Refresh Accounts, Discover Schema

For more information on partitioning aggregation, see “Partitioning Aggregation” on page 196.
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements

Configuration parameters

- Account - Group Management
 - Manages PeopleSoft roles as Account-Groups
 - Manages PeopleSoft Roles with Route Controls attached to it as Account-Group
 - Aggregation, Refresh Groups

Note: With this release of IdentityIQ, SailPoint provides support for having two or more Connector application instances in the same IdentityIQ application through the Connector Classloader functionality which require different libraries. For more information on this, see “Appendix C: Connector Classloader”.

Supported Managed Systems

IdentityIQ for Oracle ERP – PeopleSoft supports the following managed systems:

- PeopleTools version 8.56, 8.55, 8.54, 8.53
- PeopleSoft Server version 9.2, 9.1

IdentityIQ for Oracle ERP – PeopleSoft supports the following modules of Managed System:

- PeopleSoft Financial and Supply Chain Management
- PeopleSoft Human Capital Management
- PeopleSoft Campus Solution

Pre-requisites

To use the IdentityIQ for Oracle ERP – PeopleSoft, you must first configure the component interfaces on PeopleSoft. This requires the following steps:

1. Creating the Component Interfaces
2. Creating the Component interface jar file
3. Configuring the Component Interface Security

The following files must be present on the computer where the IdentityIQ for Oracle ERP – PeopleSoft is installed:

- `psjoa.jar` (found on PeopleSoft server at `%PS_HOME%\class` where `%PS_HOME%` is the location where PeopleSoft is installed)
- `iiqPeopleSoftCompInt.jar` (See Creating the Component interface jar file)

Administrator permission

The PeopleSoft user who must act as an administrator for proper functioning of the IdentityIQ for Oracle ERP – PeopleSoft and must have access to the related Component Interfaces. For more information, see Configuring the Component Interface Security.

Configuration parameters

This section contains the information that IdentityIQ for Oracle ERP – PeopleSoft uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for Oracle ERP – PeopleSoft uses the following connection attributes:

Attribute	Description
Host*	The hostname of the PeopleSoft server.
Port*	<p>The Jolt port (Jolt Server Listener Port) on which the PeopleSoft server is listening. Default: 9000</p> <p>To determine the JOLT Server Listener (JSL) port of the application server, check the JOLTListener section in the psappsrv.cfg file. The file is located in <PS_CFG_HOME>\appserv\<DOMAIN_NAME>, where:</p> <ul style="list-style-type: none"> PS_CFG_HOME: Location of configuration file of PeopleSoft Server. DOMAIN_NAME: Name of the domain which is to be administered.
User*	The user name used to login to PeopleSoft.
Password*	The password to use to login to PeopleSoft.
User Component Interface*	The name of the PeopleSoft component interface to use to read PeopleSoft User Profile.
Group Component Interface*	<p>The name of the PeopleSoft component interface to use to read PeopleSoft Roles.</p> <p>For more information, see “Creating component interface for PeopleSoft” on page 319.</p>
Jar location	<p>If there are more than one PeopleSoft application of different PeopleTools versions running under the same instance of JVM, the location specified would be added in the classpath. (The psjoe.jar and iiqPeopleSoftCompInt.jar files). For more information, see Creating the Component interface jar file).</p> <p>Note: For single PeopleSoft application, the PeopleSoft jars can be located in WEB-INF\lib directory.</p>
Partition Enabled	Check box to determine if partition aggregation is required.
Partition Statements	<p>Criteria to specify the range of users to be downloaded. For example, if the range is specified as A-M, then this specifies that all the Users whose User IDs are between A and M (including A and M) would be treated as one partition and downloaded.</p> <p>To specify more than one partition the entries should be separated using a newline character. For more information, see “Partitioning Aggregation” on page 196</p>
Domain Connection Password Enabled	Determines if Domain connection Password is configured.
Domain Connection Password*	Password is required if Domain Connection Password Enabled attribute is selected.
Route Control Component Interface	<p>The name of the PeopleSoft component interface to use to read PeopleSoft RouteControls.</p> <p>For more information, see “Creating component interface for PeopleSoft” on page 319.</p>

Schema attributes

Note: All the parameters marked with the * sign in the above table are the mandatory parameters.

Note: While deleting a User, add Component Interface in debug as `deleteComponentInterface`.
For example, `<entry key="deleteComponentInterface" value="IIQ_DEL_USER"/>`

Schema attributes

This section describes the different schema attributes.

Account attributes

The following table lists the account attributes:

Attributes	Description
UserID	The PeopleSoft User ID.
AccountLocked	Status of Account if it is locked or not.
AlternateUserID	User ID Alias.
CurrencyCode	Currency code of the user.
DefaultMobilePage	Default mobile page.
EffectiveDateFrom	Workflow attribute - from date.
EffectiveDateTo	Workflow attribute - to date.
EmailAddresses	Email address of the user.
EmailUser	Routing preferences - email user. It is a multivalued attribute.
ExpertEntry	Enable expert entry.
FailedLogins	Number of failed logins.
IDTypes	User ID types and values.
LanguageCode	Language code.
LastUpdateDateTime	Last update date/time.
LastUpdateUserID	Last update user ID.
MultiLanguageEnabled	Multi-language enabled.
NavigatorHomePermissionList	Default navigator home page permission list.
Opertype	Use external authentication.
PasswordExpired	Is password expired.
PrimaryEmailAddress	Primary email address.
PrimaryPermissionList	Primary permission list.
ProcessProfilePermissionList	Process profile permission list.

Attributes	Description
roleNames	Roles and Roles along with Route Controls assigned to the user profile.
RowSecurityPermissionList	Row security permission list.
SymbolicID	Used to map the User Id to Access ID.
UserDescription	Description of the user.
Roles	Roles and Roles along with Route Controls assigned to the user - detailed.
Encrypted	Encrypted
ReassignWork	Reassign work to alternate user.
ReassignUserID	Reassigned user's UserID.
RowSecurityPermissionList	Row Security Permissions.
SupervisingUserID	Supervisor's User ID.
UserIDAlias	Alias of the user.
WorkListEntriesCount	Count of worklist entries.
WorklistUser	Displays user workflow.

Group attributes

The following table lists the group attributes:

Attributes	Description
ALLOWNOTIFY	Workflow routing - allow notifications.
ALLOWLOOKUP	Workflow routing - allow recipient lookup.
DESCR	Description of the role.
DESCRLONG	Long description.
LASTUPDDTTM	Last update date/time.
LASTUPDOPERID	Last update user ID.
RolePermissionLists	Permission List for the role.
ROLENAME	Name of the role.
ROLETYPE	Type of the role.
RouteControl	Route Control name.
RouteControlDescription	Route Control description.
Roles that can be granted	Roles that can be granted by this role.
Roles that can grant	Roles that can grant this role.

Additional information

This section describes the additional information related to the IdentityIQ for Oracle ERP – PeopleSoft.

Creating the Component Interfaces

For creating the component interfaces, see Appendix B: Component Interface.

Partitioning Aggregation

To use the partitioning aggregation feature in IdentityIQ for Oracle ERP – PeopleSoft, perform the following:

1. Select the **Partition Enabled** check box.
2. Specify the criteria for partitioning in the **Partition Statements** textbox of the configuration parameter.
For example, download all the PeopleSoft User Profiles from A to M (including A and M) (the statement A-M would be treated as one partition)

To specify more than one partition the entries must be separated using a newline character.

Performance improvement

For improving the performance of PeopleSoft, create views and add new people code in the component interfaces on the Managed system.

For more information, see “Creating Views and adding new People Code in Component Interface” on page 196.

Creating Views and adding new People Code in Component Interface

This section describes the procedure for creating views and adding new people code in component interface on Managed System.

Note: The following script is for PeopleSoft with Oracle as the backend server. For database other than Oracle, the script must be modified accordingly.
(Database tables might be created with schema prefix (for example, sysadm))

Creating Views

Login to database with sysdba permissions and execute the following commands:

1. //This script is for creation of View for getting User IDs

```
CREATE VIEW SP_PS_USERID_VIEW AS (SELECT OPRID FROM PSOPRDEFN);  
GRANT SELECT ON SP_PS_USERID_VIEW TO people;  
commit;
```

2. //This script is for creation of View for getting Role Names

```
CREATE VIEW SP_PS_ROLE_VIEW AS (SELECT ROLENAME FROM PSROLEDEFN);  
GRANT SELECT ON SP_PS_ROLE_VIEW TO people;
```

3. `commit;`
 //This script is for creation of View for getting Route controls and its description

```
CREATE VIEW SP_PS_RTE_CNTL_PROFILE_VIEW AS (select
RTE_CNTL_PROFILE,NVL(DESCRLONG,'NA') as DESCRLONG FROM PS_RTE_CNTL_PROF);
GRANT SELECT ON SP_PS_RTE_CNTL_PROFILE_VIEW TO people;
commit;
```

Adding new People Code

1. Adding new function getIds in user component interface

Note: The **IIQ_USERS** component interface must be available. To create **IIQ_USERS** or any other user, see **Appendix B: Component Interface**.

- a. Open the **IIQ_USERS** component interface.
- b. Right click on methods section and click on **View Peoplecode**.
- c. Copy and paste the following script in the blank space.

```
REM This is an example of commenting PeopleCode;
/* ----- Logic for getting userIds from the view SP_PS_USERID_VIEW ----- */
Function getIds(&delimiter As string) Returns string;
    &finalString = "";
    &sql_text = "SELECT OPRID FROM SP_PS_USERID_VIEW ORDER BY OPRID";
    &userSql = CreateSQL(&sql_text);
    While &userSql.Fetch(&userId);
        &finalString = &finalString | &userId | &delimiter;
    End-While;
    &userSql.Close();
    Return &finalString;
End-Function;
```

- d. Save the script and component interface.
- e. Close the component interface and reopen to verify that a new method is available with name getIds.

2. Adding new function getIds in role component interface

Note: The **IIQ_ROLES** component interface must be available. To create **IIQ_Roles** or any other user, see **Appendix B: Component Interface**.

- a. Open the **IIQ_Roles** component interface.
- b. Right click on methods section and click on **View Peoplecode**.
- c. Copy and paste the following script in the blank space.

```
REM This is an example of commenting PeopleCode;
/* ----- Logic for getting roleIds from the view SP_PS_ROLE_VIEW ----- */

Function getIds(&delimiter As string) Returns string;
    &finalString = "";
    &sql_text = "SELECT ROLENAME FROM SP_PS_ROLE_VIEW ORDER BY ROLENAME";
    &userSql = CreateSQL(&sql_text);
    While &userSql.Fetch(&roleId);
        &finalString = &finalString | &roleId | &delimiter;
    End-While;
    &userSql.Close();
    Return &finalString;
```

Additional information

```
End-Function;
```

- d. Save the script and component interface.
 - e. Close the component interface and reopen to verify that a new method is available with new name getIds.
3. (Optional for Route Controls feature only) Adding new function getIds in route control component interface

Note: The **IIQ_ROUTECONTROL** component interface must be available. To create **IIQ_ROUTECONTROL** or any other user, see **Appendix B: Component Interface**.

- a. Open the **IIQ_ROUTECONTROL** component interface.
- b. Right click on methods section and click on **View Peoplecode**.
- c. Copy and paste the following script in the blank space.

```
REM This is an example of commenting PeopleCode;  
/* ----- Logic for getting route control name and description from the view  
SP_PS_RTE_CNTL_PROFILE_VIEW ----- */
```

```
Function getIds(&delimiter As string) Returns string;  
    Local Record &rtCntlId;  
    &finalString = "";  
    &rtCntlId = CreateRecord(Record.RTE_CNTL_PROF);  
    &sql_text = "SELECT RTE_CNTL_PROFILE,DESCRLONG FROM  
SP_PS_RTE_CNTL_PROFILE_VIEW ORDER BY RTE_CNTL_PROFILE";  
    &rtCntlSql = CreateSQL(&sql_text, &rtCntlId);  
    While &rtCntlSql.Fetch(&rtCntlId);  
        &finalString = &finalString | &rtCntlId.RTE_CNTL_PROFILE.Value |  
&delimiter | &rtCntlId.DESCRLONG.Value | &delimiter | &delimiter;  
    End-While;  
    &rtCntlSql.Close();  
    Return &finalString;  
End-Function;
```

- d. Save the script and component interface.
- e. Close the component interface and reopen to verify that a new method is available with new name getIds.

Creating the Component interface jar file

The `iiqPeopleSoftCompInt.jar` file contains the PeopleSoft Component Interface java classes. It must be generated from the respective PeopleSoft resource and then copied into the IdentityIQ classpath.

Perform the following steps to create the `iiqPeopleSoftCompInt.jar` file from the Component interface java files.

1. Logon to PeopleSoft Application Designer in two tier mode.
2. Open the Component Interface project and open all the component interfaces by double clicking each component interface. For example, **IIQ_USERS**
3. From the menu select **Build ==> PeopleSoft APIs**.
The **Build PeopleSoft API Bindings** window appears.
4. From the **Build PeopleSoft API Bindings** window, select the **Build** check box in the java Classes frame and clear the COM Type Library and C Header Files Build check boxes.

In the **Select APIs to Build** drop down menu, select the following options:

- `CompIntfc.CompIntfcPropertyInfo`
- `CompIntfc.CompIntfcPropertyInfoCollection`
- `PeopleSoft.*` (all Component Interfaces that begin with the prefix `PeopleSoft`)
- `CompIntfc.IIQ_*` (all Component Interfaces that begin with the prefix `CompIntfc.IIQ_`)

Note: If you need to generate Component Interface Java files for the entire group of Component Interfaces click **ALL**.

Create a directory to deploy the Java files. For example, if you specify `C:\CI` as the file path, then the Component Interface Java files are generated in `C:\CI\PeopleSoft\Generated\CompIntfc`.

6. Compile the JAVA files by performing the following steps:
 - a. Open the command prompt and change directories to the folder where the generated JAVA files are located. For example, `C:\CI`.
 - b. Navigate to the `PeopleSoft\Generated\CompIntfc\` directory.
 - c. Run the following command:

```
javac -classpath %PS_HOME%\class\psjoa.jar *.java
```

Where `%PS_HOME%` is the location that PeopleSoft is installed.

Important: Ensure that the JAVA compiler used for compiling the generated JAVA files is compatible with the JAVA provided with the PeopleSoft installation that needs to be managed.

- d. (Optional) You can delete all the generated java files from the existing directory, however, do not delete the `.class` files.
7. Perform the following steps to package the compiled files as the `iiqPeopleSoftCompInt.jar` file:
 - a. Open the Command prompt and navigate to the newly created directory. For example, `C:\CI`
 - b. Run the command: `jar -cvf iiqPeopleSoftCompInt.jar *`
8. Copy the generated `iiqPeopleSoftCompInt.jar` and `%PS_HOME%\class\psjoa.jar` files to the computer where IdentityIQ is running.

Configuring the Component Interface Security

Before using the IdentityIQ for Oracle ERP – PeopleSoft, you must allow the PeopleSoft user, for whom the Module is configured, to access the generated component interfaces.

To set security for the PeopleTools project, perform the following:

1. Log into the PeopleSoft web interface.
Default: `http://<server-name>:<port-number>/psp/ps`
2. Navigate to **PeopleTools ==> Security ==> Permissions & Roles ==> Permission Lists**.
3. Click **Add a New Value** to create a new permission list. Type **New_Name** as the name of the permission list, then click **Add**.
4. Click the Component Interfaces tab and add the created component interface.
For more information, see “Creating component interface for PeopleSoft” on page 319.

Troubleshooting

For example,

- IIQ_DEL_ROLE
- IIQ_DEL_USER
- IIQ_ROLES
- IIQ_USERS
- IIQ_ROUTECONTROL

5. For each added component interface, click **Edit ==> Full Access (All)**, then click **OK**.
6. Click **Save** to save the new permission list.
7. Navigate to **PeopleTools ==> Security ==> Permissions & Roles ==> Roles**.
8. Click **Add a New Value** to create a new role. Type **New_Name** as the name and then click **Add**. For example, **IIQ_ROLE**.
9. Enter the description as **IdentityIQ Role**.
10. Click the **Permission Lists** tab and add the permission list created in Step 3. Click **Save** to save the role.
11. Navigate to **PeopleTools ==> Security ==> User Profiles**, and select the user (for whom the permissions must be provided) that is being used in the IdentityIQ for Oracle ERP – PeopleSoft.
12. Click the **Roles** tab and add the role created in Step 10. Click **Save** to add the role to the user.

Upgrade considerations

(Optional) To use the Route Control functionality after upgrading IdentityIQ from any previous version to IdentityIQ version 7.3 Patch 3, manually add the following attributes in the Group Schema:

- RouteControl
- RouteControlDescription

For more information on the above attributes, see “Group attributes” on page 195.

Note: With this new implementation, there would be an impact on certification history. Certification history would be lost and would not be in synchronization with previous data.

Troubleshooting

1 - When the supported platform version is Java 1.6 an error message appears

When the supported platform version is Java version 1.6, the following error message appears:

```
java.lang.UnsupportedClassVersionError: psft/pt8/joa/API : Unsupported major.minor version 51.0 (unable to load class psft.pt8.joa.API)
```

Resolution: Ensure that the supported platform version is Java 1.7.

2 - (Only for PeopleTools version 8.54) Connection to Server not established

When testing the CI (Component Interface) Java APIs after upgrading to PeopleTools version 8.54, the connection to the application server fails with the following error message appears:

`openconnector.ConnectorException: Connection to server not established`

Resolution: Navigate to the location where PeopleSoft is installed. For example,
`C:\PS_CFG_HOME\webserv\peoplesoft\applications\peoplesoft\PORTAL.war\WEB-INF\classes`.

Copy all the files from this directory into the `WEB_INF\classes` directory of IdentityIQ.

Now you will be able to successfully connect to the server. This solution is documented in the following knowledge base article on the Oracle support site:

**E-CI: Java API Connection Fails With "java.lang.NoClassDefFoundError:
`com/peoplesoft/pt/management/runtime/pia/JoltSessionMXBean`" Error(1947124.1)**

Chapter 19: IdentityIQ for Oracle ERP – Siebel

The following topics are discussed in this chapter:

Overview	203
Supported features	203
Supported Managed Systems	204
Pre-requisites	204
Administrator permission	204
Configuration parameters	204
Schema attributes	206
Account attributes	206
Account Group attributes	206
Adding new custom attributes in schema	207
Provisioning policy attributes	207
Additional information	208
Troubleshooting	209

Overview

The IdentityIQ for Oracle ERP – Siebel manages entities in Oracle's Siebel CRM. Here **Employee** is managed as Accounts and **Position** as Account Groups. By default, the IdentityIQ for Oracle ERP – Siebel uses the Employee Siebel business component of the Employee Siebel business object for account provisioning. For Account Group provisioning Position business component of Position business object is used by Integration Module. However, the Integration Module can be configured to manage other Siebel Business Object/Component in the Account/Account Group provisioning. The Integration Module manages both single and multi-valued attributes of Siebel system. The Integration Module schema can be modified to manage attributes other than Schema that comes by default with Integration Module.

Supported features

IdentityIQ for Oracle ERP – Siebel provides support for the following features:

- Account Management
 - Manages Employee as Accounts
 - Aggregation, Refresh Accounts
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements

Note: Enable Account operation sets the Employment Status attribute to Active while it is set to Terminated for Disable Account operation.

Configuration parameters

- Account - Group Management
 - Manages Position as Account-Groups
 - Aggregation, Refresh Groups
 - Create, Update, Delete

Note: With this release of IdentityIQ, SailPoint provides support for having two or more Connector application instances in the same IdentityIQ application through the Connector Classloader functionality which require different libraries. For more information on this, see “Appendix C: Connector Classloader”.

Supported Managed Systems

IdentityIQ for Oracle ERP – Siebel supports the following versions of Siebel CRM Managed System:

- Siebel CRM version 16.0
- Siebel CRM version 8.2

Pre-requisites

Following Siebel JAR files are required in the `WEB-INF/lib` directory:

- **Siebel:** `Siebel.jar` and `SiebelJI_<<Language>>.jar`

For example, for Siebel CRM with English language: `Siebel.jar`, `SiebelJI_enu.jar`

The Siebel JAR files are available in the `SIEBEL_INSTALLATION_DIRECTORY/siebsrvr/CLASSES` directory.

Note: Do not copy JAR files for multiple versions of Siebel into the `WEB-INF/lib` directory; it may create conflicts at runtime.

Note: IdentityIQ for Oracle ERP – Siebel requires JRE 1.6 or above to manage Siebel CRM.

Administrator permission

The IdentityIQ for Oracle ERP – Siebel requires Siebel administrator credentials to accomplish provisioning tasks. The administrator user name and password configured for Oracle ERP – Siebel must be assigned sufficient privileges within Siebel to create new records and to update existing records for the specified business component.

For example, SADMIN user which is created during Siebel server installation is one of the example of administrator.

Note: A responsibility named “Siebel Administrator” assigned to this user gives access to all views.

Configuration parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for Oracle ERP – Siebel uses the connection parameters listed in the following table:

Table 1—Configuration parameters

Parameter	Description
Transport Protocol	Transport protocol while communicating with Siebel server. Select TCPIP or NONE. Default: TCPIP
Encryption	Data Encryption method. Select RSA or NONE. Default: NONE
Compression	Data Compression technique. Select ZLIB or NONE. Default: ZLIB
Siebel Server Host	Host Name where Siebel server is installed.
SCB Port	Listening port number for the Siebel Connection Broker (alias SCBroker). Sample value: 2321
Siebel Enterprise Name	Name of Siebel Enterprise. Sample value: SBA_82
Siebel Object Manager	Name of Siebel Application Object Manager. Sample value: SCCObjMgr
Admin User Name	User ID of the target system user account that you want to use for Integration Module operations. Sample value: SADMIN
Password	Password of the target system user account that you want to use for Integration Module operations. Sample value: sadmin
Language	Language in which the text on the UI is displayed. Specify any one of the following values: <ul style="list-style-type: none"> • For English: ENU • For Brazilian Portuguese: PTB • For French: FRA • For German: DEU • For Italian: ITA • For Japanese: JPN • For Korean: KOR • For Simplified Chinese: CHS • For Spanish: ESP • For Traditional Chinese: CHT
Account Business Object	Business Object for Account. Default value: Employee
Account Business Component	Business Component for Account. Default value: Employee
Entitlement Business Object	Business Object for Entitlement. Default value: Position
Entitlement Business Component	Business Component for Entitlement. Default value: Position
Siebel URL	Siebel server connection string. The server is connected using connection string. Specific parameters defined in the form are ignored. For example: <code>siebel.transport.encryption.compression://host:port/EnterpriseServer/AppObjMgr_lang" lang="lang_code"</code>

Schema attributes

By default the following mentioned set of attributes are managed:

Account attributes

The following table lists the account attributes (Siebel **Employee** attributes):

Attributes	Description
Login Name	Employee's login name.
First Name	Employee's first name.
Last Name	Employee's Last name.
Position	Multi-value attribute that contains a list of all positions assigned to employee.
Primary Position	Employee's primary position.
Responsibility	Multi-value attribute that contains a list of all responsibilities of employee.
Primary Responsibility Id	Employee's Primary responsibility ID.
Division	Division
Employment Status	Employment Status
Street Address	Street Address
Job Title	Job Title
Phone Number	Phone Number
Fax Number	Fax Number
Hire Date	Hire date
Alias	Alias
State	State
Availability Status	Availability status of employee.
ManagerLogin	Employee's Manager login.

Account Group attributes

The following table lists the Account Group attributes (Siebel **Position** attributes):

Attributes	Description
Id	Unique Id for Position Entity.
Name	Name of Position.
Last Name	Last Name of Employees having this Position.
Division	Division of Position.
Role	Role

Attributes	Description
Start Date	Start date for allocation of Position to Employee referred by Last Name.
Position Type	Position Type.
Parent Position Name	Parent Position's name.

Note: The search is made on *identityAttribute* while finding records. By default, "Login Name" for Account and "Id" for Account Group is set in the *identityAttribute*.

Adding new custom attributes in schema

Currently IdentityIQ for Oracle ERP – Siebel schema provides basic minimum attributes required to manage Employee and position. If you want to enhance schema, you can add more attributes to the existing schema. You can use Siebel Tools to get the details about attributes to be managed using schema. If you add any new multi value attribute, configure the following attribute in Application using the debug page:

```
<entry key="customMVGAttr">
  <value>
    <List>
      <!-- Format is <<Multi value attribute Name>>:<<MVG Business component>>:<<Business
Object for field>>:<<Business component for field>>:<<Search key for multi value
field>> -- >
      <String>Position:Position:Position:Position:Id</String>

      <String>Responsibility:Responsibility:Responsibility:Responsibility:Name</String>
    </List>
  </value>
</entry>
```

Note: As position and responsibility are main multi value field in Employee, if you do not configure it, IdentityIQ for Oracle ERP – Siebel will assume the default business components and objects. But for other Multi value attribute to work, you need to configure this attribute in Application.

Provisioning policy attributes

The following table lists the provisioning policy attributes for Create and Update of Accounts and Group:

Attributes	Description
Create Account	
Login Name	Employee's login name.
First Name	Employee's first name.
Last Name	Employee's last name.
Position	Multi-value attribute that contains a list of all positions assigned to employee.
Primary Position Id	Employee's primary position Id.
Responsibility	Multi-value attribute that contains a list of all responsibilities of employee.
Password	Employee account password.
Verify Password	Employee account password.

Additional information

Attributes	Description
Job Title	Job title.
Employee Type	Employee type.
Update Account	
First Name	Employee's first name.
Last Name	Employee's last name.
Responsibility	Multi-value attribute that contains a list of all responsibilities of employee.
Primary Position Id	Employee's primary position ID.
Create Group	
Position	Name of position.
Division	Division of position.
Position Type	Position type.
Parent Position Id	Parent position's ID.
Update Group	
Position	Name of the position.
Division	Division of position.
Position Type	Position type.
Parent Position Id	Parent position's ID.
Id	Unique Identifier for Position.
Last Name	Last Name of Employee that has this Position.
Role	Role
Start Date	The date when the position was assigned to Employee.
(Optional) Enable User	
Employment Status	Employee's employment Status.
(Optional) Disable User	
Employment Status	Employee's employment Status.

Note: For more information on Employment Status, see "Employment Status" below.

Additional information

This section describes the additional information related to the Siebel Connector.

Employment Status

The employment status is configurable for an employee. To configure the status as required, the following entry keys must be added in the application debug page:

- `<entry key="enableStatus" value="<provide value to be configured>" />`
- `<entry key="disableStatus" value="<provide value to be configured>" />`

Note: Default employment status for respective operations is as follows:

- **Enable:** Active
- **Disable:** Terminated

Supported values can be provided or configured in Siebel Server. For example, Leave Of Absence, Paid Leave Of Absence and so on.

To configure multiple employment status as **Enabled** in IdentityIQ, then all combination of status must be added in application debug page in the **activeStatusList** entry key along with **Enable Account** provisioning policy.

For example, if status of employee is **Active** or **Leave Of Absence** which must be considered as **Enabled** in IdentityIQ, add the following entries in the application debug page:

```
<entry key="activeStatusList">
  <value>
    <List>
      <String>Active</String>
      <String>Leave Of Absence</String>
    </List>
  </value>
</entry>
```

The status of the strings which are not provided in the **activeStatusList** entry key would be considered as **Disabled** in IdentityIQ.

Troubleshooting

1 - When Siebel JAR files are not copied correctly in the WEB-INF/lib directory error messages appear

When Siebel JAR files are not copied correctly in the WEB-INF/lib directory, the following errors are obtained:

- Test connection fails with the following error:
[ConnectorException] [Error details] com/siebel/data/SiebelException
- During add new entitlement the following error message is displayed:
The system has encountered a serious error while processing your request. Please report the following incident code.

Resolution: Copy the correct Siebel JAR files.

Chapter 20: IdentityIQ for NetSuite ERP

The following topics are discussed in this chapter:

Overview	211
Supported features	212
Supported Managed Systems	212
Administrator permissions	212
Configuration parameters	213
Schema attributes	213
Account attributes	213
Group attributes	214
Schema extension and custom attributes	214
Provisioning Policy attributes	215
Additional information	216
NetSuite Application Program Interface (API)	216
Troubleshooting	217

Overview

NetSuite is cloud-based Software-as-a-Service integrated business management software. NetSuite's cloud business management system includes ERP/accounting, order management/inventory, CRM, Professional Services Automation (PSA) and E-commerce.

Enterprise Resource Planning (ERP) in NetSuite encompasses several areas of your business, including accounting, inventory, order management, project management, and employee management.

For more information, see <http://www.netsuite.com/portal/products/main.shtml>

IdentityIQ for NetSuite ERP will manage the employee data in the NetSuite ERP system. This Integration Module is a write-capable Integration Module which manages the following entities:

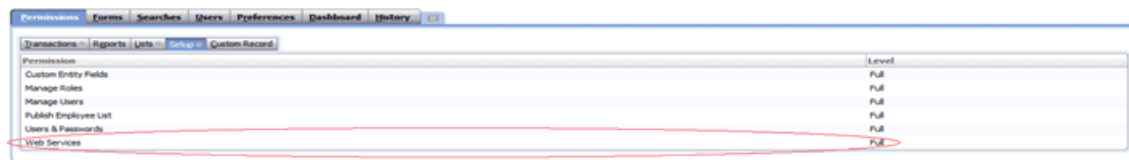
- Employee Account
- Employee Role
- Employee Entitlement

Supported features

IdentityIQ for NetSuite ERP support s the following features:

- Account Management
 - Manages NetSuite users as Accounts
 - Aggregation, Refresh Accounts, Pass Through Authentication
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements

Note: For Pass through Authentication, the account should have at least one role assigned with permissions required to perform the operation. Also this role needs to be Web Service enabled role as displayed in the following figure:



- Account - Group Management
 - Manages NetSuite groups as Account-Groups
 - Aggregation, Refresh Groups

Supported Managed Systems

IdentityIQ for NetSuite ERP supports the following managed system:

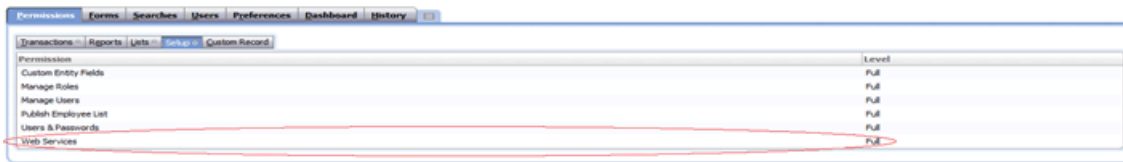
- NetSuite 2015.2
- Netsuite 2012_1

Administrator permissions

The IdentityIQ for NetSuite ERP administrator must be able to perform the following operations on NetSuite employee data:

- Search
- Create
- Update
- Delete
- Access Custom Attributes

Hence a role is required which has the permissions to the above operations. We need to create a role in NetSuite.



Configuration parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for NetSuite ERP uses the following connection parameters:

Parameters	Description
Account ID*	the account number assigned to an organization by NetSuite. This account number must be provided by each login request. This can be found by navigating to Setup => Integration => Web Services Preferences .
Role ID	When logging in using Web Services provide a role id along with your credentials. The role defined here must be a valid role contained in the Employee record of the given user. If no role id is provided, then the user's default role is used. If neither the request nor the Web Services default role is set, then the user's default UI role is used, provided it has the Web Services permission. For security reasons, it is recommended that you restrict permissions levels and access allowing only the most restricted permissions necessary to perform a given set of operations. For more information about the permissions, see "Administrator permissions" on page 212.
Administrator Email*	Email of the Account in Employee package having provisioning privileges.
Administrator Password*	Password of the employee Account.
Page Size	Limit to fetch number of accounts or groups per iteration through IdentityIQ for NetSuite ERP. If the value is not set then the default value is 50.

Schema attributes

The following schema attributes are defined:

- Account schema
- Group schema
- Custom attributes

Account attributes

The following table lists the account schema:

Schema attributes

Attribute Name	Description
EmpID (Display Attribute)	Employee ID
InternalID (Identity Attribute)	Auto generated Internal ID of the employee
EmployeeStatus	The status of employee
Email	Email ID of employee
Initial	The initials of first name and last name
OfficePhoneNumber	Office phone number of employee
HomePhoneNumber	Home phone number of employee
MobilePhoneNumber	Mobile number of employee
Department	Department of employee
Class	Class of employee
BillingClass	Billling class of employee
Groups (Entitlements)	Groups associated to the employee
GlobalSubscriptionStatus	Subscription status of employee
SocialSecurityNumber	Security number of employee
Supervisor	Supervisor of employee
DateOfHiring	Date of hiring of employee
Type	Working type of employee
JobTitle	Job title of employee
DateOfBirth	Date of birth of employee
JobDescription	Description of job of employee
TimeApprover	Approver of time for the employee (some one like supervisor or manager)

Group attributes

The following table lists the group schema:

Attribute Name	Description
GroupName (Display Attribute)	Name of the group
GroupInternalID (Identity Attribute)	Auto generated Internal id of the group

Schema extension and custom attributes

NetSuite system allows the support for extending the schema through custom entity fields. Custom entity fields are fields that you can add to your entity records to gather information specific to your business needs. Entity custom fields can be added to existing and custom sub tabs on the entry forms you use to enter entity records in your NetSuite account.

IdentityIQ for NetSuite ERP supports the read and write of custom attributes.

Following NetSuite Custom field type are supported in IdentityIQ

- Check Box
- Date
- Free-Form Text
- Email Address
- Phone Number
- HyperLink

Supporting of custom attributes

Perform the following to support the custom attributes from IdentityIQ:

- Add the custom attribute name in the schema by clicking **Add attribute** button.
- Add the following lines in the application debug page:

```
<entry key = "customAttribute" >
<value>
<List>
<String>custom1</String>
<String>custom2</String>
</List>
</value>
</entry>
```

Note: No code change would be required while adding new custom attributes in schema. This is applicable only for custom attributes.

Provisioning Policy attributes

The IdentityIQ for NetSuite ERP is pre-configured with an account creation provisioning policy that includes the commonly-used attributes that need to be set when creating an account. This field list can be modified as required.

The attributes listed in the following table are required for creating an user.

Attribute Name	Description
EmpID (Entity ID)*	Employee name
password	Password for the employee
Email*	Email of the employee
OfficePhoneNumber	Office phone number for the employee
Fax	Fax for the employee

In the above table, **EmpID** is the minimum parameter which is required to create a user on NetSuite server. But in IdentityIQ a user can only be created after assigning a role to it.

In NetSuite when a role is assigned to a user, the user requires UserName, Email and password as mandatory parameter for accessing the NetSuite server.

Additional information

Note: The field list can also be extended by adding custom attributes provided the attributes are defined in the application schema. For more information, see “Schema extension and custom attributes” on page 214.

Additional information

This section describes the additional information related to the IdentityIQ for NetSuite ERP.

NetSuite Application Program Interface (API)

SuiteTalk exposes NetSuite as a data source for programmatic access. The following operations supported in SuiteTalk would be used by IdentityIQ for NetSuite ERP:

Operation/API	Summary
add	Use to add record into the system. The system returns a NetSuite identifier (internalId) that is unique for each record created within a record type.
changePasswordOrEmail	Use to change a user’s email or password
get	Use to query the system for one record. You must provide either the internal or external ID and the record type for each query item.
getCustomizationId	Use to retrieve the internalIds, externalIds, and/or scriptIds of all custom objects of a specified type.
login	Use to login into NetSuite. This operation is similar to the NetSuite UI and requires you to provide a valid username, password, role, and account number.
logout	Use to logout from the system. The logout operation invalidates the current session.
search	Use to search for a set of records based on specific search criteria. This operation supports pagination, so that large result sets can be retrieved in smaller sets.
searchMore	Used to retrieve more records after an initial search operation is invoked.
update	Use to update existing record in the system by providing new values for the fields to be updated for each record. The records to be updated are identified by either the internal or external ID and the record type.
delete	Use to delete an existing record in the system by providing the internal id and record type.

Note: For more information, see *NetSuite SuiteTalk (Web Services) Platform Guide*.

Troubleshooting

1 - Test connection fails with an error message

Test connection fails with the following error message:

```
java.lang.IllegalArgumentException
```

This issue may occur if the value of WebService URL is different than the default value.

Resolution: Perform the following:

1. Access **<https://rest.netsuite.com/rest/datacenterurls?account=AccountID>** to find the WebService URL. It would be displayed as follows:

```
{ "webservicesDomain": "https://webservices.netsuite.com", "restDomain": "https://rest.netsuite.com", "systemDomain": "https://system.netsuite.com" }
```
2. Add an entry to the application XML with entry key as **NetsuitePortAddress** and value as **https://<webservicesDomain>/services/NetSuitePort_2012_1**.

For example,

```
<entry key="NetsuitePortAddress"  
value="https://abc123.api.netsuite.com/services/NetSuitePort_2012_1"/>
```


SAP Governance Modules

The SailPoint IdentityIQ SAP Governance Module improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ's lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities allow for more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as Transaction Codes.

The SAP Governance Module for IdentityIQ is a licensed module and includes the necessary connectivity components for operation.

Chapter 21: IdentityIQ for SAP ERP - SailPoint SAP Governance Module

The following topics are discussed in this chapter:

SAP Governance Module Setup	221
SAP Governance Module.	221

SAP Governance Module Setup

The SailPoint IdentityIQ SAP Governance Module improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ's lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities allow for more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as Transaction Codes.

The SAP Governance Module for IdentityIQ is a licensed module and includes the necessary connectivity components for operation.

Important features include:

- New visual hierarchy interface for improved user experience navigating, filtering, and selecting organizational data from SAP environments
- Granular support for defining Separation of Duty (SOD) policy violation rules that can include effective permissions within a SAP role, such as transaction codes (Tcodes).

For more information on installing the plug in for SAP Governance Module, see "[SAP Governance Module](#)" document on compass.

SAP Governance Module

SAP Governance Module includes the following:

- **SAP Direct Connector**

The SAP Integration Module aggregates and provisions all the users along with their roles/profiles of the SAP system.

SailPoint SAP Integration Module supports provisioning to a standalone SAP system as well as SAP Central User Administration (CUA) system.

For more information on the SAP Direct Connector, see "IdentityIQ for SAP ERP - SAP Governance Module" on page 143.

- **SAP HR/HCM Connector**

The SailPoint IdentityIQ SAP HR/HCM Connector aggregates and provisions the employee information from the SAP HR/HCM system.

For more information on the SAP HR/HCM Connector, see "SailPoint IdentityIQ SAP HR/HCM Connector" chapter of *SailPoint Direct Connectors Administration and Configuration Guide*.

SAP Governance Application Modules

This section contains information on the following section:

- “IdentityIQ for SAP GRC”

Note: A minority of SailPoint customers have deployed the Integration Modules in this section. SailPoint will provide assistance during the deployment of these integrations. Additional troubleshooting, diagnostic, and best practice information beyond what is contained in this document will be provided on Compass, SailPoint's Online customer portal. In some instances, SailPoint will guide the deployment team and actively participate in the design, configuration, and testing of the integration to the managed system. For more specific information, refer to the Connector and Integration Deployment Center on Compass.

Chapter 22: IdentityIQ for SAP GRC

The following topics are discussed in this chapter:

Introduction	225
Supported features	226
Supported platforms	227
Pre-requisites	227
SAP GRC Server Settings	227
SAP Connector changes for supporting SAP GRC integration	228
Creating IdentityIQ application of type SAP GRC	229
SAP GRC workflows	230
Minimum permissions required for SAP GRC user	233
Custom workflows provided for SAP GRC integration	234
SAP GRC Data Generator	234
SAP GRC Request Executor	235
Importing SAP GRC Application Rule	237
Viewing the reports	238
Upgrade considerations	238
Additional information	239
Creating a RFC Connection on SAP GRC system	239
Configuring cross system on SAP GRC	240
(Optional) Support for additional parameters	241
Support for provisioning start and end date for role assignment	243
Troubleshooting	244

Introduction

This chapter provides a guide to the integration between SAP GRC (Governance, Risk and Compliance) and IdentityIQ. This integration is used to leverage SAP GRC's ability to perform SOD (Separation of Duties) checks and take remediation or mitigation decisions within the SAP GRC. The mitigation decision must be taken in SAP GRC so that SAP GRC is aware of the mitigation controls which is applied on risks and would not report these risks till the time mitigation is applicable.

IdentityIQ for SAP GRC uses the SAP GRC Access Risk Analysis (ARA) and Access Request Management (ARM) web services which must be enabled before using the integration.

Supported features

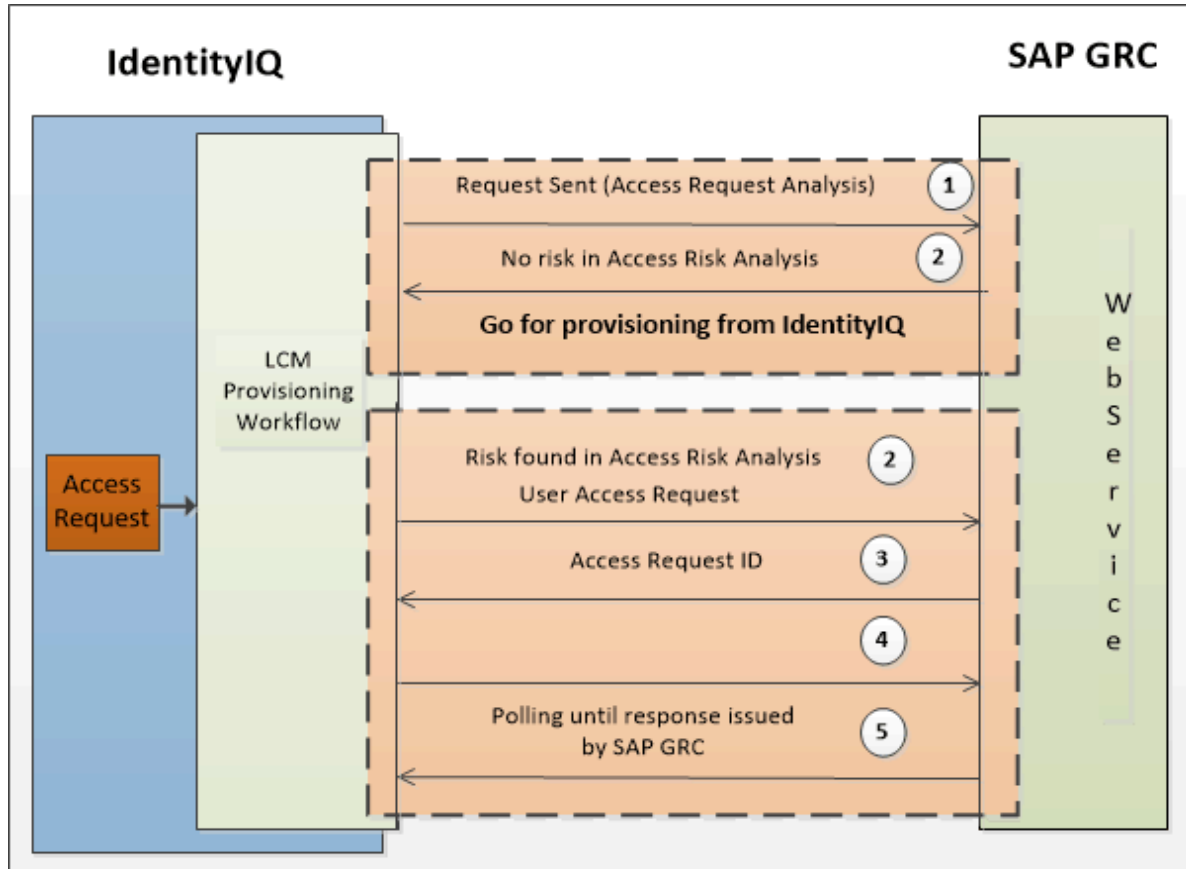


Figure 1—SAP GRC Integration Module with IdentityIQ

IdentityIQ for SAP GRC (Figure 1) enables checking for risk in the request placed in IdentityIQ (containing SAP Direct Roles and Profiles) in the following method:

1. Request will be sent to the SAP GRC for proactive check.
2. ARA Web Service will check for the risk present in the request, if no risk is returned then IdentityIQ will continue provisioning the request.
3. If ARA Web Service returns the risk in the request, then corresponding request is created in SAP GRC using the ARM Web Service.
4. IdentityIQ will continue with polling the request until response issued by SAP GRC.
5. On the basis of the response returned in step 4 above (approval or rejection by SAP GRC), IdentityIQ will continue with provisioning or rejection of the request.

Supported features

The IdentityIQ for SAP GRC performs Risk Analysis for new and change account requests using Lifecycle Compliance Manager (LCM).

Note: SAP GRC Integration supports Basic Authentication level with Transport Channel Authorization as User ID/Password.

(Optional) Support of additional feature

SAP GRC integration has been enhanced to provide support for provision start and end date for role assignment.

For more information, see “Support for provisioning start and end date for role assignment” on page 243.

Supported platforms

IdentityIQ for SAP GRC supports the following version of SAP GRC Access Control:


- SAP GRC Access Control 12.0
- SAP GRC Access Control 10.1
- SAP GRC Access Control 10.0

Pre-requisites


- SAP GRC Server Settings
- SAP Connector changes for supporting SAP GRC integration
- Creating IdentityIQ application of type SAP GRC
- SAP GRC workflows

Note: In addition to the above pre-requisites, Multi Step Multi Process (MSMP) workflow must be configured on the SAP GRC server.

SAP GRC Server Settings

- Perform the following settings on the SAP GRC Server using the administrator privileges:
 - a. Execute **SPRO** transaction code and click **SAP Reference IMG** button.
 - b. Expand **Governance, Risk and Compliance** ==> **Access Control** ==> **User Provisioning** option.
 - c. Click on  image to execute **Maintain Provisioning Settings** transaction.
 - d. In Dialog Structure double click on **Maintain Global Provisioning**.
 - e. In Provisioning options section, select **No Provisioning** from the drop down against label **Auto Provisioning**. The default value for this label is **Auto provisioning at end of request**.

Alternatively we can also maintain this settings at individual systems as follows:

- a. Execute **SPRO** transaction code and click **SAP Reference IMG** button.
- b. Expand **Governance, Risk and Compliance** ==> **Access Control** ==> **User Provisioning** option.
- c. Click on  image to execute **Maintain Provisioning Settings** transaction.
- d. In Dialog Structure double click on **Maintain System Provisioning** and select the required connector which is configured as defined in “Creating a RFC Connection on SAP GRC system” on page 239.
- e. In Provisioning options section, select **No Provisioning** from the drop down against label **Auto**


Pre-requisites

Provisioning. The default value for this label is **Auto provisioning at end of request**.

- A SAP ABAP type of connection must be defined in SM59 transaction, which would be used to indicate IdentityIQ connection virtually at SAP GRC server. This connection would be treated as Request Initiation System in SAP GRC application configuration. For more information, see “Creating IdentityIQ application of type SAP GRC ” on page 229.
- Status of requested Roles must be set to production on the SAP GRC Server.

Perform the following steps to obtain the SAP GRC URLs required when configuring the SAP GRC application in IdentityIQ

Note: Following steps are provided, considering that all required web services are set to active mode.

1. Execute **SOAMANAGER** transaction code on SAP GRC server.
2. Under Service Administration, select **Web Service Configuration**.
3. In Search criteria, select **Object Type** as Service Definition and Object Name contains **GRAC***.
4. Click on **Search**.
5. In search result, search (User Access web service) and click GRAC_USER_ACCESS_WS web service.
6. Perform the following for GRAC_USER_ACCESS_WS web service:
 - Click on  icon to open Service WSDL Generation.
 - Copy the URL from WSDL Generation section and open this URL in browser.
 - Locate the following string in the XML and copy the binding URL (in bold) mentioned in the string:

```
<wsdl:port name="Web_Service_BINDING_soap12"
binding="tns:Web_Service_WS_BINDING_soap12">

<soap12:address location="http://XXXX" />

</wsdl:port>
```
7. Perform the above steps for the following respective web services:
 - Risk Analysis: GRAC_RISK_ANALYSIS_WOUT_NO_WS
 - Request Details: GRAC_REQUEST_DETAILS_WS
 - Audit Log: GRAC_AUDIT_LOGS_WS

These URLs would be used for User Request, Request Details, Risk Analysis, and Audit Log respectively in SAP GRC application configuration in IdentityIQ. For more information, see “Creating IdentityIQ application of type SAP GRC ” on page 229.

SAP Connector changes for supporting SAP GRC integration

For supporting the SAP GRC integration, create a SAP GRC RFC (ABAP) connection on the SAP GRC system. For more information on creating the connector on SAP GRC system, see “Creating a RFC Connection on SAP GRC system” on page 239.

On SAP Direct application configuration page, the following checkbox and field have been introduced:

- **Enable SAP GRC:** Select this checkbox for the SAP GRC application to be sent to SAP GRC server for risk analysis.
- **SAP GRC Connector Name:** The value of this field would be the name of the SAP GRC Connector created in “Creating a RFC Connection on SAP GRC system” section.

In case of single SAP Direct application, user can add connector name manually. For multiple SAP Direct applications, a rule is provided to avoid the manual work. For more information, see “Importing SAP GRC Application Rule” on page 237.

Creating IdentityIQ application of type SAP GRC

Note: When you create your SAP GRC application you can configure it and perform a test connection from the Application Definition page; however, once you have saved the SAP GRC application, you must use the Debug page to view or edit it. It will not appear in your list of applications in the Application Definition page.

IdentityIQ application holds the connection parameters to communicate with SAP GRC server. Following are the connection parameters required by SAP GRC Server:

Field names	Description
SAP GRC Connection Settings	
Username*	User Name from SAP GRC Server which have minimum permissions. For more information on minimum permissions required by the SAP GRC user, see “Minimum permissions required for SAP GRC user” on page 233.
Password*	Login Password.
Request Initiation System *	Name of the connector configured in SAP GRC server which is treated as Request Initiation System . This connector is configured in SPRO define connectors or in SM59 transaction code. For more information, see “Creating a RFC Connection on SAP GRC system” on page 239.
Polling interval	Polling interval in minutes (Range 1 to 360).
Web Service URL Details	
User Access *	End Point URL for SAP GRC User Access Web Service. Format of URL would be as follows: http://<SAP GRC Host Name>/sap/bc/srt/rfc/sap/GRAC_user_acces_ws<WebService Binding URL>

Pre-requisites

Field names	Description
Risk Analysis*	End Point URL for SAP GRC Access Risk Analysis Web Service. Format of URL would be as follows: http://<SAP GRC Host Name>/sap/bc/srt/rfc/sap/GRAC_risk_analysis_wout_no_ws<WebService Binding URL>
Request Details *	End Point URL for SAP GRC Request Detail Web Service. Format of URL would be as follows: http://<SAP GRC Host Name>/sap/bc/srt/rfc/sap/GRAC_request_details_ws<WebService Binding URL>
Audit Log	End Point URL for SAP GRC Audit Log Web Service. To get Mitigation details in IdentityIQ, audit log URL can be provided. This detail can be viewed in Interaction section of Access Request Page. Format of URL would be as follows: http://<SAP GRC Host Name>/sap/bc/srt/rfc/sap/GRAC_audit_logs_ws<WebService Binding URL>
Note: For more information, see “Perform the following steps to obtain the SAP GRC URLs required when configuring the SAP GRC application in IdentityIQ” on page 228.	

Additional configuration parameter

Setting GRC Connection Timeout parameter: Along with the default **connectionTimeout** parameter set in the **SAP GRC Executor workflow**, add the following entry key to the SAP GRC application debug page:

```
<entry key="grc_connection_timeout" value="timeout Value"/>
```

The **timeout Value** is a value in minutes. For example, the **timeout Value** of **10** would set the **grc_connection_timeout** to **10** minutes.

SAP GRC workflows

The standard LCM provisioning workflow does not support the SAP GRC integration. Custom workflows are shipped with IdentityIQ to support this integration.

Integration workflows

Following are the custom workflows to interact with SAP GRC:

- SAP GRC Data Generator
 - Gathers all provisioning request from IdentityIQ.
 - Filter the plans which contain roles from SAP Direct application which has SAP GRC check box enabled.

For more information, see “Custom workflows provided for SAP GRC integration” on page 234.

- Creates a map of all the requested items which are required by SAP GRC Request Executor.

Note: The step to create map from the plan can be customized as required.

- SAP GRC Request Executor

For a proactive check performed on Access Request, if there is no risk found for particular Access Request then request will be provisioned, else perform the following:

- a. Creates a request on SAP GRC Server.
- b. Polling is done for the request till it is in pending status.
- c. Receives the response back from SAP GRC Server.
- d. Based on the response, this workflow takes decision whether to provision the request on SAP Server or not.

For more information, see “Custom workflows provided for SAP GRC integration” on page 234.

Note: Proactive check on Access request displays the risks even if they are mitigated earlier. Therefore each time mitigated risks get calculated, request would be created on SAP GRC for approval.

Importing integration workflows

Import `Workflow_SAPGRC_Integration.xml` which contains **SAP GRC Data Generator** and **SAP GRC Request Executor** workflows located at `../WEB-INF/config` file.

These workflow must be integrated in LCM provisioning workflow in **Provisioning Approval Subprocess** sub-process as mentioned below:

1. Change **Provisioning Approval Subprocess** as mentioned below:

- Navigate to process designer and click on **Add A Step**.
- Select **Stop**.
- Drag and drop the **Stop** step (in Auto Layout) after the **end** step.
- Right click on **end** step and select **Change Icon**.
- Select **Generic** and click on Save.
- Right click on **end** and click **Edit Step**.

Provide the following values in the Details section:

- **Name:** Invoke SAP GRC Data Generator
- **Subprocess:** (select under Action section) SAP GRC Data Generator.

Pre-requisites

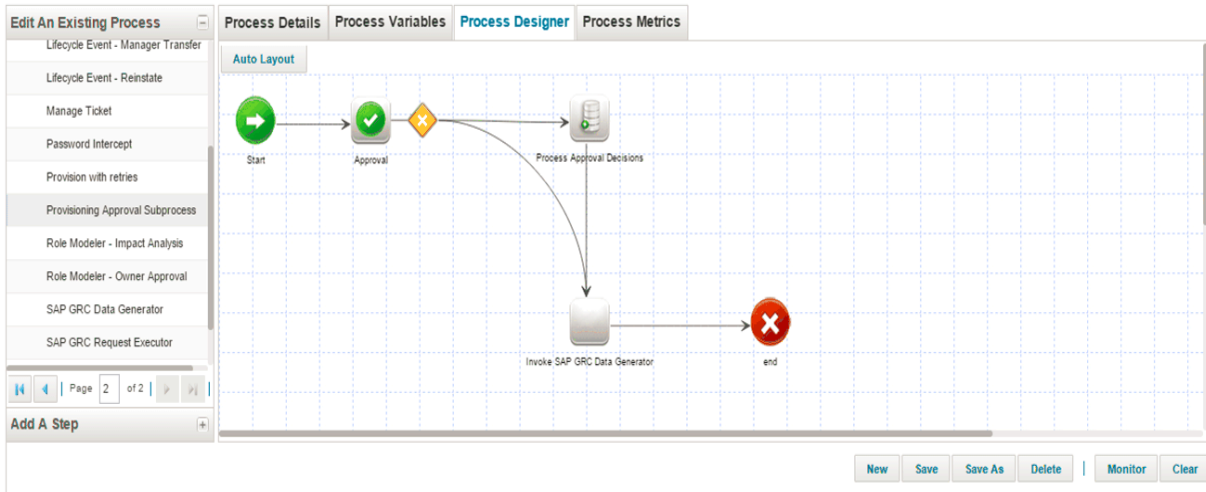
Save the form.

- Right click on **Stop** step, click **Edit Step** and in Details section provide the name as **end**.

Save and close the workflow.

- Right click on **Invoke SAP GRC Data Generator** step and perform the following:
 - a. Start the transition and end that transition on **end** step.
 - b. Save the changes.

Business Process Editor



- Open the **Provisioning Approval Subprocess** and right click on **Invoke SAP GRC Data Generator** and edit the step.

In Arguments section of this step search for `identityName`, `identityDisplayName`, `project`, `approvalSet` and enter the values as `identityName`, `identityDisplayName`, `project` and `approvalSet` respectively for Reference fields. Save the changes.

- Save the changes.
- Navigate to debug page and search the following in **Provisioning Approval Subprocess** workflow:

```
<Step icon="Default" name="Invoke SAP GRC Data Generator"
```

Perform the following change:

```
<Step icon="Default" name="Invoke SAP GRC Data Generator" posX="320" posY="196"
resultVariable="approvalSet">
```

After all the `<Arg>` tags add the following before invoking the SAP GRC Data Generator workflow:

```
<Return name="approvalSet" to="approvalSet"/>
```

```
<Return name="project" to="project"/>
```

2. Open **SAP GRC Data Generator** process and perform the following:
In Process Variable section open **applicationNameSAPGRC** variable and in Initial value section select String and provide value as the name of application of type SAP GRC configured in IdentityIQ.

(Optional) Life cycle event workflows

1. Import `Workflow_SAPGRC_LifeCycle_Events.xml` located at `../WEB-INF/config` which includes **New Account - Joiner** and **Mover - Process** workflows.
2. These Lifecycle events are triggered in case of joiner and change attribute events respectively.

Note: These are sample workflows which can be customized as required.

Minimum permissions required for SAP GRC user

The minimum permissions required for the SAP GRC account must have the following Authorization Objects assigned to it:

Authorization Objects	Field names
S_SERVICE	<ol style="list-style-type: none"> 1. SRV_NAME (Select * or select Technical names of following web service configured in SAP GRC) <ul style="list-style-type: none"> • Risk analysis Webservice: • User access Webservice • Request details Webservice • Audit log Webservice: 2. SRV_TYPE: WS
GRAC_RA	<ul style="list-style-type: none"> • Activity: Administrator • Object types for Authorization: User, Role, Profile • Risk Analysis Mode: All values or provide the required value • Report Type: All values or provide the required value
GRAC_SYS	<ul style="list-style-type: none"> • Activity: 01 • Application Type: 001 (SAP) • SYSTEM Environment: Select the environment in use, that is, Development, Production, Test • Connector ID: * or select the connector id configured on SAP GRC
GRAC_REQ	<ul style="list-style-type: none"> • Activity: 01 • Request Type: 001,002 • Business Process: * or provide the required values • Functional Area: * or provide the required functional areas • Request for single or multiple: All values or provide the required value • Request Information: All values or provide the required value

Authorization Objects	Field names
GRAC_ROLED	<ul style="list-style-type: none"> Activity: 03 Business Process: * or provide the required values Connector Group: * or select the connector group configured on SAP GRC Role Sensitivity: 000 Role Type: BUS, COM, CUA, PRF, SIN Role Name: * or provide the required value

Custom workflows provided for SAP GRC integration

SAP GRC Data Generator

This workflow fetches following information from IdentityIQ:

- Details of user for whom access is requested.
- Details of user who is requesting for access.
- Details of access which are requested.

SAP GRC Data Generator subprocess has a custom script to fetch the values which can be changed by user as per his requirements.

Inputs to SAP GRC Data Generator workflow

Field names	Description
identityName	Name of the identity object being modified.
plan	A master provisioning plan object required for building transient approval set for SAP GRC response.
project	A ProvisioningProject object describing the modifications to the identity. This may include a list of Question objects which will cause the generation of a Form and a WorkItem to solicit additional information necessary for provisioning.
identityDisplayName	Display name for identity.
applicationNameSAPGRC	Name of the application created of type SAPGRC.
approvalSet	These attributes are set during the Build Approval Set step, which builds this list by going through the ProvisioningPlan to build the line items that must be approved. This variable includes all ApprovalItems that are part of the request process and is updated during the AfterScript of the approval process by assimilating the decisions and comments from the Approvals copy of the ApprovalItem.
trace	Used for debugging this workflow and when set to true, trace will be sent to stdout .
requester	Requester who initiated the request.

Field names	Description
Support for additional parameters	
reportType	A comma separated string of Report Types used for SAP GRC Proactive checks.
riskLevel	A comma separated string of Risk Level numbers for SAP GRC Proactive check.
ruleSetId	A Rule Set Id for SAP GRC Proactive check.
Note: For more information about the support for additional parameters, see (Optional) Support for additional parameters 241.	

Output of SAP GRC Data Generator workflow

Table 1— Output of SAP GRC Data Generator workflow

Field names	Description
completeDetailMap	Map used to keep all other maps required by SAP GRC Request Executor.
userInfoMap	Map used to provide details for the link to whom access request is created.
requestedLineItemMap	A map with details of roles which are requested for a link.
credentialsMap	Map containing values of credential to connect to SAP GRC server.
requestHeaderDataMap	Map containing values of requester.
userGroupsMap	Map containing user group details.
accountRequestSAPGRC	A list of SAP Direct AccountRequest which are qualified for SAP GRC violation check.
customFieldsValMap	Map containing custom values of requester.
parameterMap	Map containing parameter values to be set.
language	Language used by requester. Default: English.

The **Invoke SAP GRC Request Executor** step of SAP GRC Data Generator workflow invokes the SAP GRC Request Executor workflow.

SAP GRC Request Executor

The SAP GRC Request Executor workflow pro-actively checks for Access Request Risk with SAP GRC, if risk is found then it creates the request on SAP GRC server and regularly checks the status of the request in asynchronous manner. As this workflow checks status of the response at regular interval, variables related to such polling are defined here. User can change those variables as per requirement.

Inputs to SAP GRC Request Executor workflow

Field names	Description
numberOfRetries	The number of retries that will be attempted before failure of the provisioning activities.

Custom workflows provided for SAP GRC integration

Field names	Description
retrievableErrors	A comma separated string that specifies errors which will be retried while getting the status of the request.
approvalSet	This attribute is set during the Build Approval Set step, which builds this list by going through the ProvisioningPlan to build the line items that must be approved. This variable includes all ApprovalItems that are part of the request process and are updated during the AfterScript of the approval process by assimilating the decisions and comments from the Approvals copy of the ApprovalItem.
plan	A master provisioning plan object required for building transient approval set for SAP GRC response.
identityDisplayName	Display name for identity.
userGroupsMap	The map containing UserGroup data required as an input for SAP GRC User Access Web service.
customFieldsValMap	The map containing CustomFieldsVal data required as an input for SAP GRC User Access Web service.
parameterMap	A list containing Parameter data required as an input for SAP GRC User Access Web service.
requestHeaderDataMap	A map containing RequestHeaderData required as an input for SAP GRC User Access Web service.
credentialsMap	A map to store credential information which is gathered from SAP GRC application.
requestedLineItemMap	A list containing RequestedLineItem data required as an input for SAP GRC User Access Web service.
userInfoMap	A list containing UserInfo data required as an input for SAP GRC User Access Web service.
language	SAP System Language.
requestStatusMap	The request status map containing the status information of the request received from the Request Detail Web service.
connectionTimeout	The Axis2 timeout for the Web service connection timeout. This field accepts the value in minutes.
requestNumber	The request number received after successful execution of the User Access Web service. This Request number is used by Request Detail Web service for polling.
pollingInterval	The polling interval in minutes to check the status of the request.
trace	Used for debugging this workflow and when set to true, trace will be sent to stdout.
requestStubDetailsMap	Holding user information and headerinfo to generate request detail stub.
project	ProvisioningProject which is a compiled version of the ProvisioningPlan.

Output of SAP GRC Request Executor workflow

Field names	Description
approvalSet	This attribute is set during the Build Approval Set step, which builds this list by going through the ProvisioningPlan to build the line items that must be approved. This variable includes all ApprovalItems that are part of the request process and is updated during the AfterScript of the approval process by assimilating the decisions and comments from the Approvals copy of the ApprovalItem.
requestStatusMap	The request status map containing the status information of the request received from the Request Detail Web service.
auditLog	Audit Log for the particular request.

Importing SAP GRC Application Rule

The IdentityIQ Rule is required for populating IdentityIQ SAP application configuration parameter with SAP GRC Connector name.

Perform the following steps to import and execute the SAP GRC application rule:

1. Create `sapGrcApplications.csv` file which contains the following columns separated by comma:
 - IdentityIQ Application name
 - Respective SAP GRC Server side Connector name

For example:

SAPAPPLICATION1, SAPGRCCONNECTOR

Note: Comments can be provided in the `sapGrcApplications.csv` file using # symbol at the beginning of the line. For example column headers.

Note: If second column name is not provided than IdentityIQ application name would be treated as SAP GRC Connector name.

2. Create `sapGrcRuleParameters.xml` file which will contain the following map of arguments that are required to pass externally to the rule:

- **path:** path of the `sapGrcApplications.csv` file
- **separator:** separator used in `sapGrcApplications.csv` file, to separate the IdentityIQ application name and respective SAP GRC Server side Connector name.

For example,

```
<Map>
  <entry key='path' value='E://SAPGRCAApplications.csv' />
  <entry key='separator' value=', ' />
</Map>
```

3. Import `sapGrcApplicationsRule.xml` IdentityIQ Rule which populates IdentityIQ SAP application configuration parameter with SAP GRC Connector name.

- The `sapGrcApplicationsRule.xml` file is present in `WEB-INF/config` folder.
- From console run the following commands:

```
import sapGrcApplicationsRule.xml
rule "Mapping GRC Connector Name to SAP based Application" <path of
sapGrcRuleParameters.xml file>
```

Viewing the reports

For example, rule "Mapping GRC Connector Name to SAP based application"
"E://sapGreRuleParameters.xml"

Following figure displays the output of the above performed steps:



Logging for the Rule -

Enter the following line to set logging for the rule in log4j.properties file:

```
log4j.logger.SAPGRC.sapGrcApplicationsRule=debug
```

Viewing the reports

SAP GRC related transaction in access request status report will be displayed against Comments with **External GRC System-SAP GRC** string, which is located at **Intelligence => Reports => Category:Lifecycle Manager Reports => Access Request Status Report**.

Upgrade considerations

Note: Any customizations done on SAP GRC before upgrading to IdentityIQ version 7.1 will not be reflected in SAP GRC after upgrading to IdentityIQ version 7.3 Patch 3.

Support proactive check and SAP CUA integration

To support proactive check and SAP CUA integration in SAP GRC, import Workflow_SAPGRC_Integration.xml file while upgrading to IdentityIQ version 7.3 Patch 3.

Note: Perform Step 2. of "Importing integration workflows" section.

Upgrade settings

For user upgrading to IdentityIQ version 7.3 Patch 3, perform the following changes:

1. SAP GRC Data Generator workflow to pass value of modified provisioning project.
For **Invoke SAP GRC Request Executor** add the following changes in the application debug page:

```
<Arg name="project" value="ref:project"/>
```


Add the following after all the <arg> tags:

```
<Return name="project" to="project"/>
```
2. For SAP GRC Request Executor workflow, add a process variable project as follows:

```
<Variable input="true" name="project">
```



```
<Description>
```

```

        ProvisioningProject which is a compiled version of the ProvisioningPlan.
    </Description>
</Variable>
For updateGRCResponse, add the following changes in the application debug page:
<Arg name="project" value="ref:project" />
Add the following after all the <arg> tags:
<Return name="project" to="project" />

```

Additional information

This section describes the additional information related to the SAP GRC integration.

Creating a RFC Connection on SAP GRC system

The following steps are used to create RFC connection which can be used as Request Initiation System to indicate IdentityIQ connection virtually at SAP GRC server:

1. Execute **TCODE SM59** or navigate to **SPRO ==> SAP Reference IMG ==>Governance Risk and Compliance ==> Common Component Settings ==> Integration Framework ==> Create Connectors** and execute it. The Configuration of RFC Connections page is displayed.
2. Navigate to **ABAP Connections** and click on the create icon.
3. Give a name to the RFC Destination in new screen and provide connection type as 3 means ABAP connection.
4. Enter the details on **Technical Settings, Logon & Security** tabs accordingly and click on Test connection and save the changes.
5. Navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Common Component Settings ==> Integration Framework ==> Maintain Connectors and Connection Types** and execute it.
6. In new screen click on **Define Connectors**. In right hand section with name **Connection type definition** click on **SAP** and double click on **Define Connectors** again in the left hand side section.
7. In new screen click on **New Entries**.
8. Select the **Target Connector** from the drop down box which is defined in Step 3. The name of the **Source Connector** and **Logical Port** must be same as that of **Target Connector**. Select the **Connection Type** as **SAP**.
9. Select the created new entry and click on **Define Connector Groups** in the left hand section. Click on **New Entries**.
10. Provide name for new connector group in column **Conn Group** in the screen at left side.
11. Provide any **Connector Group Text** and **Con. Type** as **SAP** and save it.
12. Select the created Define Connector Group and double click on **Assign Connector Group to Group Types** in the left side of the same screen.
13. In the new screen, click on **New Entries** and provide the **Connector Group Type** as **Logical Group** on the right hand side of the screen.
14. Select the created **Connector Group Type** and double click on **Assign Connectors to Connector Group** section in left side of the screen.
15. In the new screen, click on **New Entries** and provide same name which was defined in Step 3. under column **Target Connector** in right side screen. Provide **Connection Type** as **SAP** in the same screen and save it.

Additional information

16. Navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Common Component Settings ==> Integration Framework ==> Maintain Connection Setting** and execute it.
17. A new window (Determine Work Area Entry) will be displayed. In this window select the **Integration Scenario** as **Auth** and click on **Continue (Enter)**.
18. Select Sub-Scenario as **AUTH** and double click on **Scenario-Connector Link** in the left hand side screen.
19. Click on **New Entries**. In the new screen on right side, select **Target Connector** name which is same as that mentioned in Step 3.
20. In Same Screen, select **Conn. Type** as **SAP**.
21. Repeat Step 16. to Step 20. for selecting the different Integration Scenario types as **PROV, ROLMG, SUPMG**.
22. Navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Access Control ==> Maintain Connection Settings** and execute it.
23. Select **Maintain Connector Settings** select **New Entries**.
24. In right hand side screen select **Target Connector** as the name defined in Step 3. and select **App Type** as **1**. Select the Environment as required and **PATH ID** as **B012**.
25. Navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Access Control ==> Maintain Mapping for Actions and Connector Groups** and execute it.
26. Select **Maintain Connector Group Status** and click on **New Entries** in left side screen.
27. In new screen in right side provide **Conn. Group** as the same name defined in Step 10. Select **Appl Type** as **001** and enable the Active check box for the respective **Conn.Group**.
28. In left hand screen double click on **Assign Default Connector To Connector Group** and click on **New Entries**.
29. Select **Conn.Group** as defined in Step 10. Select the **Target Connector** as defined in Step 3. Enable the Default check box.
Note: Perform the above step for all the actions and save it.
30. To verify whether connector is added successfully or not, navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Access Control ==> Synchronization Job ==> Authorization Sync** and see whether this new connector is listed in the drop-down of connector or not.

Configuring cross system on SAP GRC

SAP GRC integration can be used to verify the risk for the request placed for cross system configuration containing SAP Role for multiple SAP Direct applications.

Perform the following steps to configure cross system on SAP GRC:

1. Create connectors for all the SAP Direct applications as mentioned in the “Creating a RFC Connection on SAP GRC system” on page 239.
2. Navigate to **SPRO ==> SAP Reference IMG ==> Governance Risk and Compliance ==> Common Component Settings ==> Integration Framework ==> Maintain Connector and Connection Types** and execute it.
3. In new screen click on **Define Connectors**. In right hand section with name Connection type definition click on **SAP**.
4. In new screen click on **New Entries** and enter the value of **Conn.Group** as **CROSS_SYST** and **Connector Group Text** as **Cross_System_Group**. Save it.
5. Select **Cross System** and on the left hand side double click **Assign Connector Group to Group Types**.

6. Click on **New Entries** and in the New screen select **Connector Group Type** as **Cross_System_Group**.
7. Select **CROSS_SYST** group and double click on **Assign Connectors To Connector Groups**.
8. Click on **New Entries** and add the connector Names configured in Step 1.

(Optional) Support for additional parameters

SAP GRC Integration has been enhanced to provide support of the following additional parameters in the SAP GRC Data Generator workflow:

- RiskLevel
- RuleSetId
- ReportType
- simulationRiskOnly

Displays results of risks or violations which would be obtained from the combination of user's existing and new assignments. Possible values for **simulationRiskOnly** are as follows:

- **X**: displays the new violation result obtained from combination of new assignment
- **Blank**: displays all the violations of old and new assignments (a consolidated violation result)

Perform the following steps to specify the value of the above parameters:

1. Navigate to Menu ==> Setup ==> Business Processes and click and open **SAP GRC Data Generator** workflow.
2. Navigate to **Process Variables** tab.
3. Expand the required Variable (that is, RiskLevel, RuleSetId or ReportType) and initialize the values by selecting type as **String** and add single/multiple values separated by comma in textbox.

Upgrade settings

For the user upgrading to IdentityIQ version 7.3 Patch 3, perform the following changes in **SAP GRC Data Generator** workflow to specify the values for:

- riskLevel, reportType and ruleSetId
 - a. In between the following lines add the following workflow process variables marked in **bold**:


```
"<Variable initializer="false" name="trace">
<Description>Used for debugging this workflow and when set to true trace
will be sent to stdout.</Description>
</Variable>"
<Variable input="true" name="reportType">
<Description>A comma separated string of Report Type values used for SAP GRC Proactive
checks.</Description>
</Variable>
<Variable input="true" name="riskLevel">
<Description>A comma separated string of Risk Level values used for SAP GRC Proactive
check.</Description>
</Variable>
```

Additional information

```
<Variable input="true" name="ruleSetId">
```

```
<Description>A comma separated string of Rule Set Id values used for SAP GRC Proactive check.</Description>
```

```
</Variable>
```

```
"<Description> This subprocess is used in "Provision and Approval " subprocess."
```

- b. At **Invoke SAP GRC Request Executor** step, add the following arguments and return structures:

```
<Arg name="reportType"/>
```

```
<Arg name="riskLevel"/>
```

```
<Arg name="ruleSetId"/>
```

```
<Return name="riskLevel" to="riskLevel"/>
```

```
<Return name="ruleSetId" to="ruleSetId"/>
```

```
<Return name="reportType" to="reportType"/>
```

- c. Perform the following steps to add initial values to variables:

Navigate to **Menu ==> Setup ==> Business Processes** and open **SAP GRC Data Generator** workflow and navigate to **Process Variables** tab and perform the following:

- expand the **reportType** and initialize the values by selecting type as String and add values in textbox as comma separated. For example, 02,05
- expand the **riskLevel** and initialize the values by selecting type as String and add single numeric value in textbox. For example, - 1
- expand the **ruleSetId** and initialize the values by selecting type as String and add single text value. For example, - CLIENT_RULESETID

Note the following:

- Performance of SAP GRC is impacted if multiple **riskLevel** and **ruleSetIds** are set together.
- If risk is detected for any value of **riskLevels** and **ruleSetIds** then it creates SAP GRC Request immediately and rest all **riskLevel** and **ruleSetId** values would be ignored.
- Setting multiple values for **riskLevel**, **reportType** and **ruleSetId** with leading or trailing spaces are not allowed.

- **simulationRiskOnly**

- a. In between the following lines add the following workflow process variables marked in **bold**:

```
<Variable input="true" name="ruleSetId">
```

```
<Description>A comma separated string of Rule Set Id values used for SAP GRC Proactive check.</Description>
```

```
</Variable>
```

```
*<Variable input="true" name="simulationRiskOnly">
```

```
<Description>A String value of Simulation Risk Only used for SAP GRC check.
```

```
</Description>
```

```
</Variable>*
```

"<Description> This subprocess is used in "Provision and Approval" subprocess.

- b. At **Invoke SAP GRC Request Executor** step, add the following arguments and return structures:

```
<Arg name="simulationRiskOnly" />

<Return name="simulationRiskOnly" to="simulationRiskOnly" />
```

Support for provisioning start and end date for role assignment

SAP GRC integration has been enhanced to provide support for provisioning start and end date for role assignment. The start and end dates are the values set for the **startDate** and **endDate** variables in SAP DATA Generator workflow. These dates are passed to the SAP GRC integration and then to the SAP Direct for provisioning.

If sunset/sunrise dates in IdentityIQ are used for role assignment, then these dates have to be passed to the SAP DATA Generator workflow and set to the **startDate** and **endDate** variables using additional customizations.

Note: The same start and end date would be applied to all the roles requested.

Perform the following changes on IdentityIQ workflows to support start and end date for role assignment:

1. Open **Provisioning Approval Subprocess** workflow and add the following:

- **Workflow variables:**

```
<Variable name="endDate" output="true">
  <Description>End date of the role assignment.</Description>
</Variable>
<Variable name="startDate" output="true">
  <Description>Start date of the role assignment.</Description>
</Variable>
```

- Search for **SAP GRC Data Generator** and add the following entries before **<Workflowref>** **<Step>** section:

```
<Return name="endDate" to="endDate" />
<Return name="startDate" to="startDate" />
```

2. Open **Approve and Provision Subprocess** workflow and add the following:

- **Workflow variables:**

```
<Variable name="endDate" output="true">
  <Description>End date of the role assignment.</Description>
</Variable>
<Variable name="startDate" output="true">
  <Description>Start date of the role assignment.</Description>
</Variable>
```

- Search for **Provisioning Approval Subprocess** workflow and add the following entries before **<Workflowref>**:

```
<Return name="endDate" to="endDate" />
<Return name="startDate" to="startDate" />
```

- Search for **Identity Request Provision** entry and add the following arguments to the existing list of arguments in **<Step>** with name **Provision**:

```
<Arg name="endDate" value="ref:endDate" />
<Arg name="startDate" value="ref:startDate" />
```

3. Open **Identity Request Provision** workflow and add the following:

- **Workflow variables:**

```
<Variable name="endDate" output="true">
  <Description>End date of the role assignment.</Description>
</Variable>
<Variable name="startDate" output="true">
  <Description>Start date of the role assignment.</Description>
</Variable>
```

- Search for **Provision with retries** entry and add the following arguments to the existing list of arguments in <Step> with name **Provision**:

```
<Arg name="endDate" value="ref:endDate"/>
<Arg name="startDate" value="ref:startDate"/>
```

4. Open **Provision with retries** workflow and add the following:

- **Workflow variables:**

```
<Variable name="endDate" output="true">
  <Description>End date of the role assignment.</Description>
</Variable>
<Variable name="startDate" output="true">
  <Description>Start date of the role assignment.</Description>
</Variable>
```

- Search for **Initialize Retries** and add the following entries in **start** <Step> section:

```
<Arg name="endDate" value="ref:endDate"/>
  <Arg name="startDate" value="ref:startDate"/>
  <Transition to="Set Dates for SAP Roles" when="script:(endDate != null ||
startDate != null )"/>
```

- Add the following step:

```
<Step action="rule:xxxx" name="Set Dates for SAP Roles">
  <Arg name="endDate" value="ref:endDate"/>
  <Arg name="startDate" value="ref:startDate"/>
  <Arg name="project" value="ref:project"/>
  <Return name="project" to="project"/>
  <Transition to="Initialize Retries"/>
</Step>
```

where xxx is name of the workflow rule written to set dates as arguments to the plan.

5. Import **Set Date SAP GRC Role Assignment** rule from **examplerules.xml**, which is used to add date arguments to the provisioning project.

Troubleshooting

1 - IdentityIQ Rule displays an error message when '&' is used as a separator

The IdentityIQ Rule displays the following error message when '&' is used as a separator in .csv file:

```
java.lang.RuntimeException
```

Resolution: Add the separator in the `sapGrcRuleParameters.xml` file in the following format:

```
<Map>
  <entry key='path' value='<path of .csv file>'>
  <entry key='separator' value='&amp' />
</Map>
```

3 - After IdentityIQ is upgraded, when performing Provisioning operation, an error message is displayed

The following error message is displayed when performing the provisioning operation after upgrading IdentityIQ to version 7.3 Patch 3:

An unexpected error occurred: Execution of the Access Request Web service resulted in error. Message Type: ERROR, Message Reason: Role Type is mandatory

Resolution: Perform Account-Group Aggregation task.

4 - While requesting an access for an identity from IdentityIQ an error message appears

While requesting an access for an identity from IdentityIQ, the following error message appears:

RABAX in SAP GRC Integration

Resolution: Roles which are requested, must have provisioning status set as **Production** on SAP GRC Server.

To set the status of role as **Production**, the Role maintenance quick link from the section Role Management can be used in NWBC user interface.

5 - Request gets provisioned even if there is a risk in the request

Request gets provisioned even if there is a risk in the request which may occur due to the following reasons:

1. **GRAC_RISK_ANALYSIS_WOUT_NO_WS** web service was not returning an error message if correct permissions were not given to the service account.

Resolution: To resolve this issue implement the following SAP Note in the SAP GRC Server:

2187803 - GRAC_RISK_ANALYSIS_WOUT_NO_WS does not return correct error message

2. **GRAC_RISK_ANALYSIS_WOUT_NO_WS** web service not returning risk as the report format value input is different as per different SP level of SAP GRC.

Resolution:

- **For user on SAP GRC 10.1 SP level SP-Level 0010 or lower:** initialize the value of REPORT_FORMAT to DETAILED in the SAP GRC DATA generator workflow under 'Initialize Detail Map' step as follows:

```
private static final String REPORT_FORMAT = "DETAILED";
```

- **For user on SAP GRC 10.1 SP level SP-Level 0011 or above:** initialize the value of REPORT_FORMAT to 2 in the SAP GRC DATA generator workflow under 'Initialize Detail Map' step as follows:

```
private static final String REPORT_FORMAT = "2";
```

Add requestLineDataMap.put ("ReportFormat", REPORT_FORMAT); statement for the location specified below:

- Search for requestLineDataMap.put ("ProvItemType", PROVISIONING_ITEM_TYPE_ROL); and add the following line:
requestLineDataMap.put ("ReportFormat", REPORT_FORMAT);

Troubleshooting

Perform the above for all occurrences of `requestLineDataMap.put("ProvItemType", PROVISIONING_ITEM_TYPE_ROL);` line.

The final code view would be as follows:

```
requestLineDataMap.put("ProvItemType", PROVISIONING_ITEM_TYPE_ROL);  
requestLineDataMap.put("ReportFormat", REPORT_FORMAT);
```

- Search for `requestLineDataMap.put("ProvItemType", PROVISIONING_ITEM_TYPE_PRF);` and add the following line:

```
requestLineDataMap.put("ReportFormat", REPORT_FORMAT);
```

Perform the above for all occurrences of `requestLineDataMap.put("ProvItemType", PROVISIONING_ITEM_TYPE_PRF);` line.

The final code view would be as follows:

```
requestLineDataMap.put("ProvItemType", PROVISIONING_ITEM_TYPE_PRF);  
requestLineDataMap.put("ReportFormat", REPORT_FORMAT);
```

3. **GRAC_RISK_ANALYSIS_WOUT_NO_WS** web service not returning risk for the Critical roles /profiles

Resolution: Implement the following SAP Note in the SAP GRC Server:

2409002 - Critical role/profile shows no result for GRAC_RISK_ANALYSIS_WOUT_NO_WS

6 - Mitigation comments are not displayed in Access Request Status report

When the Account name for the identity is in lower case, mitigation comments are not displayed in Access Request Status report.

Resolution: Account Name (User Name) should always be in upper case letters

7 - Unable to request SAP direct profiles through GRC Integration

While requesting the profile, the following error message is displayed:

An unexpected error occurred: Undefined argument: startDate: at Line: 166

Resolution: Implement the following SAP Note in the SAP GRC server:

2194063 - UAM: Request status IDM service doesn't return reqstatus and reqstatus_txt and request detail service doesn't return comment, approvers and correct

8 - Incorrect SAP GRC Connector name

If incorrect SAP GRC Connector name is provided, request gets provisioned even if there is a risk in the request.

Resolution: Implement the following SAP Note in the SAP GRC Server:

2399698 - Validation changes in GRAC_RISK_ANALYSIS_WOUT_NO_WS webservice

9 - Risk is not detected for Critical role/profile

If Critical role/profile gets provisioned even if there is a risk in the request.

Resolution: Implement the following SAP Note in the SAP GRC Server:

2409002 - Critical role/profile shows no result for GRAC_RISK_ANALYSIS_WOUT_NO_WS

10 - Request gets rejected in IdentityIQ even if its is approved on SAP GRC 12.0

Resolution: Implement the following SAP Note in the SAP GRC Server:

2698051 - AC12 - GET_REQUEST_DETAILS is returning empty line items

11 - Request for Create account fails with an error message

Request for create account fails with the following error message:

Risk Analysis failed with error

One of the reasons for the above error message could be due to the value of the '**enable user ID validation in access request against search data sources**' parameter not being set properly for SAP GRC.

Resolution: Perform the following to set the correct value for '**enable user ID validation in access request against search data sources**' parameter:

1. Navigate to **SPRO ==> Governance, Risk and Compliance ==> Access Control ==> Maintain Configuration Settings**.
2. Set the value of the parameter **2051 (enable user ID validation in access request against search data sources)** to **No**.

Healthcare Integration Modules

This section contains information on the following section:

- “IdentityIQ for Epic Healthcare”
- “IdentityIQ for Cerner Healthcare”

Note: For customers entitled to the SailPoint Healthcare Integration Module, the following requirements must be met:

- access to the API of the Electronic Medical Record (EMR) system so that SailPoint Connector can connect to the EMR system
- access to the EMR system's user interface or console to view results of any action performed by the SailPoint Connector through user interface or console

This EMR access is required to support ongoing development, test and maintenance of SailPoint Healthcare Integration Module.

Chapter 23: IdentityIQ for Epic Healthcare

The following topics are discussed in this chapter:

Overview	251
Important consideration	251
Supported features	252
Supported Managed System	252
Pre-requisites	252
Administrator permissions	253
Configuration parameters	253
Additional configurations for WS-Security	255
Schema Attributes	255
Account attributes	255
Group attributes	260
Provisioning Policy attributes	261
Troubleshooting	264

Overview

Epic is a privately held health care software company. Epic offers an integrated suite of health care software centered on a MUMPS database. Their applications support functions related to patient care such as follows:

- including registration and scheduling
- clinical systems for doctors, nurses, emergency personnel, and other care providers
- systems for lab technicians, pharmacists, and radiologists
- billing systems for insurers

IdentityIQ for Epic Healthcare supports managing Epic accounts (EMP records), linked templates, linked sub-templates, InBasketClassifications and LoginDepartmentFilterList.

Important consideration

For customers entitled to the IdentityIQ for Epic Healthcare Integration Module, the following requirements must be met:

- access to the API of the Electronic Medical Record (EMR) system so that SailPoint Connector can connect to the EMR system
- the Epic connector uses Core Binding, Personnel Management and Common SOAP Web-Services which must be licensed from Epic.

Note: The license information can be obtained from Epic by emailing to 'open@epic.com'.

This EMR access is required to support ongoing development, test and maintenance of IdentityIQ Healthcare Integration Module.

Supported features

IdentityIQ for Epic Healthcare supports the following features:

- Account Management
 - Manage Epic EMP records as Accounts
 - Aggregation, Partitioning Aggregation, Refresh Account
 - Create, Update, Delete
 - Enable, Disable, Unlock
 - Add/Remove Entitlements

Entitlements are supported for Epic Linked Template, Linked Sub-templates, InBasketClassifications and LoginDepartmentFilterList.
- Account - Group Management
 - Manage Epic Linked Template as Account - Groups
 - Manage Epic Linked Subtemplates as Account - Groups
 - Manage Epic InBasketClassifications as Account - Groups
 - Manage Epic Login Department as Account - Groups
 - Aggregation

Note: Due to api limitations on the Epic interconnect side, only templates and subtemplates that are associated with a user record would be aggregated.

Supported Managed System

IdentityIQ for Epic Healthcare supports Epic version 2019, 2018, 2017, 2015 and 2014.

Pre-requisites

- **Epic Web Services:** Epic provides SOAP based Web-Services for connecting to various APIs. All communication with the Epic Interconnect server should be done via these APIs. For Epic Healthcare to work, following web services must be enabled on Interconnect server:
 - **Core:** The Core WCF service fetches all the records matching specified filters. The Integration Module uses this service to:
 - read all records with INI type as EMP (for user records) and DEP (for login departments)
 - get categories for Epic items 55 (BlockStatus) and 450 (InBasketClassifications)
 - **Personnel Management:** The personnel management is a web service that implements all the provisioning related API's used by the Integration Module. In addition, it provides interface to read details about each of the EMP record that the Core service returns.
 - **Common:** The common Web Services used to update **UserDemographics** related attributes.

The **Core**, **Personnel Management** and **Common** Module of the Epic Web Services must be enabled for access. A debugging interface available on the Epic Web Services server, displays the enabled and disabled status of various Epic Web Services. This debugging interface must be used to view and verify that the

required Web Services are enabled when integrating with IdentityIQ. The format of the URL for the diagnostic service is as follows:

http://[epic-webservices-server-name]/[epic-instancename]/StatusPage/Main.aspx

For example, **http://example-epic-websrvr.acme.com/Interconnect-TST_POC2014/StatusPage/Main.aspx**

- **Configuring the truststore:** For configuring the trust store, server root certificate should be imported into the keystore for the remote API calls. Ensure that the following java system property is set to the path of the imported root certificate for SSL SOAP connections:

```
Djavax.net.ssl.trustStore2 = <Path of the imported root certificate>
```
- For customers using SOAP version 1.2, add the following entry in the application debug page and perform the supported operations:

```
<entry key="soapVersion" value="1.2"/>
```
- The Core, Personnel Management and Common Web Service can be secured using WS-Security. The Epic Healthcare supports Username token based WS-Security for Core, Personnel Management and Common Web Service. It is recommended to provide Transport Layer Security (TLS) in conjunction with Username token based approach for WS-Security. This ensures that the underlying communication channel keeps the data encrypted.

Administrator permissions

To manage IdentityIQ for Epic Healthcare, ensure that Web Services mentioned in the “Pre-requisites” section must be enabled on Interconnect server.

Configuration parameters

This section contains the information that this Integration Module uses to connect and interact with the application.

IdentityIQ for Epic Healthcare uses the following methods for enabling the WS-Security:

- Core
- Personnel Management
- Common

Note: When enabling WS-Security for Core Binding and Personnel Management, the WS-Security account must be configured for the Interconnect Web Service. If the account being configured is a local account that is, it exists only on the Interconnect server, then the WS-Security Username must be prefixed by 'local:'. If the account being configured is an EMP account that is, it exists as an EMP record in EPIC, then the WS-Security Username must be prefixed by 'emp:'.

The IdentityIQ for Epic Healthcare uses the following configuration attributes:

Attribute	Description
Epic Configuration	
Epic URL*	The host URL of Epic instance.

Configuration parameters

Attribute	Description
Admin UserID*	Specifies the administrator or the unique ID of the user which has administrative level privileges to perform aggregation and provisioning operation on Epic system.
Admin User Type	The type of the ID specified in Admin UserID.
Manage Active Accounts Only	<i>(Applicable to Account aggregation only)</i> By default this is selected and will aggregate only active accounts during account aggregation.
Page Size	Number of records to fetch during account or group aggregation in a single call to Interconnect server. Default: 500
Number of Partitions	Define number of partitions to subdivide the aggregation data.This overrides system suggested number of partitions.
Core Web Services Configuration	
UserID	UserID to connect core Web Services.
Enable WS-Security	Checkbox to enable WS-Security for Core Binding with Username token.
Username*	Enter Core Binding WS-Security Username.
Password*	Enter Core Binding WS-Security Password.
Personnel Management Web Services Configuration	
Enable WS-Security	Checkbox to enable WS-Security for Personnel Management with username token.
Username*	Enter Personnel Management WS-Security Username.
Password*	Enter Personnel Management WS-Security Password.
Note: For more information on additional configurations of WS-Security for Personnel Management, see “ Additional configurations for WS-Security”.	
Enable Auditing	Enable auditing information.
Audit UserID	The identifier of the person who is creating the new User record. This ID must correspond to the AuditUserIDType.
Audit User Password	The Epic password of the Audit User.
Audit User Type	The type of the ID specified in AuditUserID.
Common Web Services Configuration	
Enable WS-Security	Select this checkbox to enable WS-Security for Common Web Services with username token
Username*	Enter Common Web Services WS-Security Username.
Password*	Enter Common Web Services WS-Security Password.
Note: For more information on additional configurations of WS-Security for Common, see “ Additional configurations for WS-Security”.	

Additional configurations for WS-Security

- **Personnel Management Web Services Configuration**

Note: EPIC Connector uses Apache Rampart module to implement WS-Security for Personnel Management.

- After enabling the **Enable WS-Security** checkbox, enter the valid **Username** and **Password**.
- Copy the **sailpoint_epic_connector_axis2.xml** file from `integration\EPIC` folder to the `\WEB-INF\classes` directory.
- The WS-Security policy file must be present in `\WEB-INF\classes\` directory. Name of the policy file must be **epic_security_policy.xml**.

Following is the sample security policy file:

```
<?xml version="1.0" encoding="UTF-8"?>

<wsp:Policy wsu:Id="UTOverTransport"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">

  <wsp:ExactlyOne>

    <wsp:All>

      <sp:SupportingTokens
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">

        <wsp:Policy>

          <sp:UsernameToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient" />

        </wsp:Policy>

      </sp:SupportingTokens>

    </wsp:All>

  </wsp:ExactlyOne>

</wsp:Policy>
```

- **Common Web Services Configuration**

- After enabling the **Enable WS-Security** checkbox, enter valid **Username** and **Password**.
- Copy the **sailpoint_epic_connector_axis2.xml** file from `integration\EPIC` folder to the `\WEB-INF\classes` directory.
- The WS-Security policy file must be present in `\WEB-INF\classes\` directory. Name of the policy file must be **epic_security_policy.xml**.

Schema Attributes

This section describes the different schema attributes.

Account attributes

The following table lists the account attributes:

Schema Attributes

Attribute Name	Description	Epic Name	Epic Item Number
UserID	Unique ID of the Epic user.	User ID, ".1"	0.1
Name	The Epic user's name, in LastName, FirstName MI format.	UserName	0.2
SystemLoginID	The user's operating system login. The name must be unique.	System Login	45
UserAlias	Another name by which this user is known. Typically used for maiden names or other name changes. In Last, First format.	User Alias	180
StartDate	The date the user started at the organization.	Start Date	720
IsPasswordChangeRequired	Password change required Flag	Force Password Change	46
EndDate	The date the user was terminated or left the organization.	End Date	730
DefaultLoginDepartmentID	By default, when the user logs into Epic, he is presented with this department.	Default login Department	17325
DefaultLinkedTemplateID	The default linkable template for this user.	Default linked template	1101
LinkedProviderID	Stores the user's Provider ID. EpicCare uses this number to enable this user to receive provider messages. Cadence uses this to link a provider's schedule to a user. Note: A record for the provider in the Provider master file must be created.	Provider ID	17500
LinkedSubtemplateIDs	Sub-templates are used to provide modular configuration for many users and are highly configurable. Sub-templates with a lower index have priority.	Subtemplate ID	1110
LinkedTemplateID	The list of templates the user is allowed to select from Epic. Templates are used to provide modular configuration for many users and are highly configurable.	Linked Template ID	198
AuthenticationConfigurationID	A non-native authentication method (for example, LDAP) used to authenticate when user logs into Epic.	Authentication Record	48

Attribute Name	Description	Epic Name	Epic Item Number
UserRoles	User Roles combine to produce the look, feel, and behavior of Epic for a given user.	Default User Role	14300
ExternalIdentifiers	Manage user identity in multiple systems.	External ID	2402
CustomUserDictionaries	User's dictionary file to maintain their own spell check corrections.	Custom Dictionary	17460
InBasketClassifications	Determines the messages the user receives in Epic.	In Basket	450
Notes	Text notes about the user.	Notes	14100
ContactComment	Comment associated with the creation of this user.	Contact Comment	23
ContactDate	Last modified date. Defaults to current date if not provided.	Contact Date	10
UserDictionaryPath	File path at which the custom user dictionary files can be found.	User Dictionary Path	17465
LDAPOverrideID	A string that can be provided to identify the user to the LDAP server in place of the SystemLogin.	LDAP Override ID	51
IsActive	Indicates whether the user is allowed to log into Epic.	Record Status	50
IsBlocked	Indicates whether the user is blocked from logging into Epic.	Login Blocked	55
BlockReason	Reason why the user account is blocked.	Block Reason	55
BlockComment	Text comment about why the user is blocked. Maximum allowed length is 100 characters.	Block Comment	55
ReportGrouper1	Report groupers are used to segregate users for highly specific reporting and statistics needs.	Report Group 1	280
ReportGrouper2		Report Group 2	281
ReportGrouper3		Report Group 3	282
UserPhotoPath	A URL or file path to a picture of this user.		
Sex	The Users legal sex, typically. Valid values include the Male, Female, Unknown.		
ProviderAtLoginOption	Prompted to choose an associated provider upon login.		
ForceContactCreation	If true, the provided values would be filed to a new contact for the User, meaning that previous values would be retained.		
EmployeeDemographics	This parameter is used to provide certain specific information about the user.		

Schema Attributes

Attribute Name	Description	Epic Name	Epic Item Number
CategoryReportGrouper1	Report groupers are used to segregate Users for highly specific reporting and statistics needs.		
CategoryReportGrouper2			
CategoryReportGrouper3			
CategoryReportGrouper4			
CategoryReportGrouper5			
CategoryReportGrouper6			
UserComplexName_AcademicTitle	Academic title of the User. For example, Phd, MD, Dr, DDS,DD and so on.		
UserComplexName_FatherName	The Users father's name, typically used for constructing Arabic names.		
UserComplexName_FirstName	The first or given name of the User.		
UserComplexName_GivenNameInitials	Initials for the first name.		
UserComplexName_GrandfatherName	The Users grandfathers name, typically used for constructing Arabic names.		
UserComplexName_LastName	The Users last or family name.		
UserComplexName_LastNamePrefix	The Users last name prefix.		
UserComplexName_PrimaryTitle	Primary title of the User. For example, Mr., Miss, Dr., Ms.		
UserComplexName_SpouseLastName	The last or family name of the Users spouse.		
UserComplexName_SpouseLastNameFirst	<ul style="list-style-type: none"> Yes: the spouse's last name would appear first in the hyphenated last name No 		
UserComplexName_SpousePrefix	The Users spouse prefix.		
UserComplexName_Suffix	Suffix of user. For example, Sr., Jr., I, II, III.		
CommunityUser_WebExternalIdentifier	The external system Login ID.		
CommunityUser_ReceiveExternalEmail	This controls whether users receive notification emails from EpicCare link.		
CommunityUser_ReceiveGroupNotifications	This controls whether users receive group notification emails from EpicCare link.		
CommunityUser_Deactivated	Signifies a user should no longer have access to the application.		

Attribute Name	Description	Epic Name	Epic Item Number
CommunityUser_SiteManagerContexts	This links users to EpicCare Link user context groups for the purposes of site management.		
CommunityUser_UserContexts	This links users to EpicCare Link user context groups.		
UserGroups	The current list of User Groups for the selected user.		
BIDefaultUser	The BI default user name for the Hyperspace user, which is used by Hyperspace to connect to BI applications.		
EmailAddress	Email address of the user.		
PhoneNumber	Phone number of the user.		
FaxNumber	Fax number of the user.		
UpdateLinkedProviderRecord	Provides UpdateLinkedProviderRecord.		
Address_City	City of the user.		
Address_Country	Country of the user.		
Address_County	County of the user.		
Address_District	District of the user.		
Address_HouseNumber	House number of the user.		
Address_Lines	Lines of the user.		
Address_State	State of the user.		
Address_ZipCode	Zip code of the user.		
PreferredLoginDepartments	The departments on the user's preferred list.		
LoginDepartmentFilterList	The list of departments to use when limiting access for the user.		
LoginDepartmentFilterSetting	Whether the Department Filter List is Inclusive or Exclusive.		
ReportAuthorizedServiceAreas	A list of service areas for which the user has access.		
ReportAuthorizedLocations	A list of locations for which the user has access.		
ReportAuthorizedDepartments	A list of Departments for which the user has access.		
ReportAuthorizedDepartmentGroups	A list of department groups for which the user has access.		
ReportAuthorizedUsers	A list of users for which the user has access.		
ReportAuthorizedProviders	A list of providers for which the user has access.		

Schema Attributes

Attribute Name	Description	Epic Name	Epic Item Number
LinkedTemplateConfig	<p>List of LinkedTemplateConfig object points to the template setup for the User. The LinkedTemplateConfig attribute is multi valued.</p> <p>After aggregation LinkedTemplateConfig properties is displayed in the following format:</p> <pre>Id = 123; Name = ADMINISTRATOR TEMPLATE; StartDate = 11/16/15; EndDate = 11/16/22; LoginTypes = [Clarity Console, Rover, Home Health]</pre> <p>For provisioning user must use the following format:</p> <pre>TemplateID#StartDate#EndDate#Login types</pre>		

Note:

- Following attributes support only write operations:
EmailAddress, PhoneNumber, FaxNumber, UpdateLinkedProviderRecord, Address_City, Address_Country, Address_County, Address_District, Address_HouseNumber, Address_Lines, Address_State, Address_ZipCode
- IdentityIQ for Epic Healthcare provides support for all types of UserID's. For example, External, Internal, SytemLogin and so on. User must manually add the new schema attribute in account schema in the following specified format:
`UserID_userIDType`
For example, UserID_Internal, UserID_SytemLogin, UserID_External and so on.
The suffix in schema attribute must be the same as the type of userID received in viewUser response, for example, for Internal UserID the schema attribute name must be UserID_Internal)

Group attributes

The following table lists the Group attributes:

Attribute name	Description
Linked template attributes	
LinkedTemplateID	The ID of the LinkedTemplate.
LinkedTemplateName	Name of the LinkedTemplate.
Linked Subtemplates attributes	
LinkedSubtemplateIDs	<p>ID of the Linked Sub-template.</p> <p>Sub-templates are used to provide modular configuration for many users and are highly configurable. Sub-templates with a lower index have priority.</p>
LinkedSubTemplateName	Name of the Linked Sub-template.
InBasketClassifications attributes	
Number	ID of the InBasketClassifications.
Title	Description of the InBasketClassifications.

Attribute name	Description
Abbreviation	Abbreviation of the InBasketClassifications.
Department attributes	
ExternalID	The external ID of department.
Name	Name of the department.
Location	Location of the department.
Service Area	Service Area of the department.
Center	Center of the department.
Specialty	Specialty of the department.

Provisioning Policy attributes

The following table lists the provisioning policy attributes for Create and Update Account:

Attribute name	Description
Name	The Epic user's name in LastName, FirstName, MI format.
User ID	User ID for the newly created user. If provided, it will create user with specified ID else Epic will assign the ID automatically. User can pass * as value to allow Epic system create User ID automatically.
Password	Password of the user to be created.
DefaultLoginDepartment	Represents the department of the user. For example, INITIAL DEPARTMENT
DefaultLinkedTemplateID	The default linkable template for the user.
StartDate	Defaults to the initial start date.
EndDate	End date of the user account.
SystemLoginID	Unique name of the users operating system login. The maximum length is 254 characters.
Notes	Free text notes about the user.
ContactComment	A comment associated with the creation of the user.
LDAPOverrideID	A string that can be provided to identify the user to the LDAP server in place of the SystemLogin.
UserDictionaryPath	File path at which custom user dictionary files can be found.
AuthenticationConfigurationID	If a non-native authentication method is used authenticate user when he logs into Epic.
CustomUserDictionary_index_0	A number that indicates the priority of the value. Lower order numbers are given more priority.
CustomUserDictionary_value_0	The string being stored at the indexed position.

Provisioning Policy attributes

Attribute name	Description
CustomUserDictionary_index_1	A number that indicates the priority of the value. Lower order numbers are given more priority.
CustomUserDictionary_value_1	The string being stored at the indexed position.
ExternalIdentifier_id_0	The external ID to be set for this user.
ExternalIdentifier_type_0	Type of this ID - that is, for what kind of system it is valid.
ExternalIdentifier_password_0	Password to set for specific external ID.
ExternalIdentifier_isActive_0	Value must be set to true in case this ID must be marked as active, that is, if the user can use it in the external system; else false.
ExternalIdentifier_id_1	External ID to be set for this user.
ExternalIdentifier_type_1	Type of this ID - that is, for what kind of system it is valid.
ExternalIdentifier_password_1	Password to set for this external ID.
ExternalIdentifier_isActive_1	Value must be set to true in case this ID must be marked as active, that is, if the user can use it in the external system; else false.
EmployeeDemographics_Index_0	A number that indicates the priority of the EmployeeDemographics . Smaller numbers override larger ones.
	EmployeeDemographics_EmployeeDemographic1_0: The value for EmployeeDemographic1
	EmployeeDemographics_EmployeeDemographic2_0: The value for EmployeeDemographic2
	EmployeeDemographics_EmployeeDemographic3_0: The value for EmployeeDemographic3
EmployeeDemographics_Index_1	A number that indicates the priority of the EmployeeDemographics. Smaller numbers override larger ones .
	EmployeeDemographics_EmployeeDemographic1_1: The value for EmployeeDemographic1
	EmployeeDemographics_EmployeeDemographic2_1: The value for EmployeeDemographic2
	EmployeeDemographics_EmployeeDemographic3_1: The value for EmployeeDemographic3
Optional attributes	
<i>After upgrading to IdentityIQ version 7.3 Patch 3, if required user can add the following attributes manually to Provisioning Policy</i>	
IsActive	Indicates whether the user is allowed to log into Epic.
IsBlocked	Indicates whether the user is blocked from logging into Epic.
BlockReason	Reason why the user account is blocked.

Attribute name	Description
BlockComment	Text comment about why the user is blocked. Maximum allowed length is 100 characters.

Note: IdentityIQ for Epic Healthcare provides provisioning support for other types of UserID's (for example, External, Internal, SytemLogin and so on) supported by the managed system. Respective attributes must be added in the provisioning policy.

Examples for Provisioning Complex Attributes

- To provide multiple values for **CustomUserDictionary** and **ExternalIdentifier**, provisioning policy can be updated to include multiple attribute to accept multiple values.
For example, to provide three custom user dictionaries, following attributes can be added in Provisioning Policy:

- CustomUserDictionary_index_2
- CustomUserDictionary_value_2
- CustomUserDictionary_index_3
- CustomUserDictionary_value_3

The last characters of these values keep incrementing for any additional attributes added.

- To provide multiple values for **EmployeeDemographics**, provisioning policy can be updated to include multiple attribute to accept multiple values.

For example, to provide two **EmployeeDemographics** values, following attributes can be added in Provisioning Policy:

- EmployeeDemographics_Index_0 :
- EmployeeDemographics_EmployeeDemographic1_0
- EmployeeDemographics_EmployeeDemographic2_0
- EmployeeDemographics_EmployeeDemographic3_0
- EmployeeDemographics_Index_1
- EmployeeDemographics_EmployeeDemographic1_1
- EmployeeDemographics_EmployeeDemographic2_1
- EmployeeDemographics_EmployeeDemographic3_1

- Update use cases for **LinkedTemplateConfig** object: (While provisioning of LinkedTemplateConfig character '#' is considered as delimiter used for separating values and character '*' is used as wild cards.

- If '*' is specified instead of LinkedTemplateID then connector would assign same StartDate, EndDate and LoginTypes for all those LinkedTemplates for which StartDate, EndDate and LoginTypes are not provided.
- If '*' is specified instead of any connection property then connector would preserve exiting values of StartDate and EndDate for T1 LinkedTemplate while updating.

To provide multiple LoginTypes, values can be provided separated by the ',' delimiter.

Following is the provisioning policy format for LinkedTemplateConfig:

LinkedTemplateConfig = LinkedTemplateID#StartDate#EndDate#LoginTypes

Examples:

- To update Template T1 with values provided: **T1#01/01/11#12/31/21#Hover,Home Health**
- To update Template T1 is updated with values provided and remove StarDate, EndDate as it is not provided: **T1####Hover,Home Health**
- To update Template T1 is updated with values provided, existing values of StarDate, EndDate is preserved: **T1*##*#Hover,Home Health**
- Assign same StartDate, EndDate and LoginTypes for all those LinkedTemplates for which StartDate, EndDate and LoginTypes is not provided: ***#01/01/11#12/31/21#Hover,Home Health**

Troubleshooting

1 - While executing any operations in IdentityIQ error messages are displayed

While executing any operations in IdentityIQ, either of the following error messages are displayed:

```
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be non-empty
```

OR

```
sun.security.validator.ValidatorException: PKIX path building failed:  
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid  
certification path to requested target
```

Resolution: Configure the certificates correctly.

2 - An error message appears if the core service is not enabled

If the Core service is not enabled the following error message appears in the interface or log file:

```
ApplicationFault:<Type>FacadeServiceDisabled</Type>
```

The requested business service is disabled.

Resolution: Enable the Core web services on the Epic web services server.

3 - For JBoss EAP server, test connection fails with an error message

The following error message appears when the test connection fails for JBoss EAP Server:

```
Exception while connecting to Personnel service
```

Resolution: Copy the addressing-1.6.1.mar file from \\WEB-INF\\lib\\ directory to deployment directory of JBoss (for example, jboss-eap-6.2\\standalone\\deployments) in order to work with certificate based authentication on JBoss.

Provide the path to MAR files as a parameter while starting JBOSS EAP server (for example, standalone.bat -Daxis2.repo=\\jboss-eap6.2\\standalone\\deployments\\addressing-1.6.1.mar)

4 - Not able to generate SOAP Envelope logging in IdentityIQ for Epic Healthcare

When performing any operation, not able to generate SOAP Envelope logging in IdentityIQ for Epic Healthcare.

Resolution: To enable advanced SOAP Envelope logging in IdentityIQ for Epic Healthcare configure the following attribute in xml application schema:

```
<entry key="logSOAPEnvelop" value="true"/>
```

Note: Download the `sailpoint_epic_connector_axis2.xml` file from `IdentityIQ.zip/integration` directory and copy it into `identityiq\WEB-INF\classes` directory in order to generate SOAP logs.

5 - Account Aggregation Task enters into an endless loop

Account Aggregation Task enters into an endless loop when GetRecords API enters into endless loop.

Resolution: To avoid the **GetRecords API** call getting into an endless loop, a **GetRecordsCallsthreshold** parameter is used. The default value of **GetRecordsCallsthreshold** is 5000. To increase the count of **GetRecordsCallsthreshold**, enter the following key in Epic application xml:

```
<entry key="getRecordsCallsThreshold" value="value"/>
```

where, value is the maximum number of calls that would be made to Interconnect server.

6 - Unable to perform Test Connection/Account Aggregation for trailing backslash

The following message appears when unable to perform the Test Connection/Account Aggregation for trailing backslash:

```
ERROR http-nio-8080-exec-8 apache.axis2.engine.AxisEngine:219 - The [action] cannot be processed at the receiver
```

Resolution: Provide a link as follows without the trailing backslash at the end:

`http://example-epic-websrvr.acme.com/Interconnect-TST_POC2014`

7- When upgrading IdentityIQ to version 7.3 Patch 3 and WS-Security is enabled for EPIC connector, Test Connection fails with an error

When upgrading IdentityIQ to version 7.3 Patch 3 and WS-Security is enabled for EPIC connector, Test Connection fails with the following error message:

```
Test [ConnectionFailedException] [Possible suggestions] Ensure the Epic system host is reachable and there is a smooth connectivity between Identity Server and Epic host. [Error details] Failed to connect to Epic System. At least one security token in the message could not be validated.
```

Resolution: Perform the following:

1. Add the following entry key in the upgraded application debug page:

```
<entry key="encrypted" value="authUserPassword,coreWSSecurityPassword"/>
```
2. Perform the Test Connection and proceed.

8 - Test Connection fails when user has different end points

Resolution: To configure EPIC Web Service endpoint, update the following entries in the application debug page:

```
<entry key="CoreStubUrl" value="/httplistener.ashx" />
<entry key="EpicSOAP1.1EndpointsMap">
  <value>
    <Map>
```

Troubleshooting

```
        <entry key="CommonUser2011"
value="wcf/Epic.Common.GeneratedServices/User.svc/basic" />
        <entry key="PersonnelManagement2012"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/basic" />
        <entry key="PersonnelManagement2014"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/basic_2014" />
        <entry key="PersonnelManagement2015"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/basic_2015" />
        <entry key="PersonnelManagement2016"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/basic_2016" />
        <entry key="PersonnelManagement2017"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/basic_2017" />
    </Map>
</value>
</entry>
    <entry key="EpicSOAP1.2EndpointsMap">
        <value>
            <Map>
                <entry key="CommonUser2011"
value="wcf/Epic.Common.GeneratedServices/User.svc" />
                <entry key="PersonnelManagement2012"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/" />
                <entry key="PersonnelManagement2014"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/2014" />
                <entry key="PersonnelManagement2015"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/2015" />
                <entry key="PersonnelManagement2016"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/2016" />
                <entry key="PersonnelManagement2017"
value="wcf/Epic.Security.GeneratedServices/PersonnelManagement.svc/2017" />
            </Map>
        </value>
    </entry>
```

Note: Modify the endpoint URL's as required.

Chapter 24: IdentityIQ for Cerner Healthcare

The following topics are discussed in this chapter:

Overview	267
Supported features	267
Pre-requisites	267
Configuration parameters	268
Schema attributes	268
Account attributes	268
Group attributes	270
Provisioning Policy attributes	270
Troubleshooting	272

Overview

Cerner Corporation is a global supplier of health care information technology (HCIT) solutions, services, devices and hardware. Cerner solutions optimize processes for health care organizations. The IdentityIQ for Cerner Healthcare is designed to provide automated way of provisioning through SailPoint IdentityIQ solution.

Supported features

IdentityIQ for Cerner Healthcare supports the following features:

- Account Management
 - Aggregation, Refresh Account
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements (position and organization groups)
- Account - Group Management
 - Aggregation

Pre-requisites

- The Cerner Enterprise Provisioning Service exposes the provisioning mechanism to external requests and responses using the SPML (Service Provisioning Markup Language) standard Cerner Millennium provisioning language. The Service allows external provisioning solutions to create and maintain users. The Cerner connector accesses the enterprise provisioning service to perform all the requests. For accessing enterprise provisioning service, the target ID of the millennium and millennium domain is required.

Configuration parameters

- For accessing provisioning adapter, the target ID of the millennium and millennium domain is required.
- Permissions given to TargetID in Cerner millennium:

The Cerner provisioning adapter requires one Millennium account having Manage Accounts privilege, which modifies the users within Millennium. The service account is mapped to TargetID which is required in order to make calls to the provisioning adapter. The IdentityIQ requires targetID to connect to the Cerner provisioning adapter (through Cerner API's access). This is necessary, since Cerner has no way of defining users to have the authority to send requests.

Configuration parameters

Parameters	Description
Cerner URL	URL to connect to Cerner Server. URL of the Provisioning Servlet and the Provisioning Servlet allows SailPoint Cerner connector to communicate with Cerner through SPML calls. For example, <a href="http://<hostName>/security-provisioning/ProvisioningServlet">http://<hostName>/security-provisioning/ProvisioningServlet
Target ID	ID with required permission to get the data and to perform provisioning on Cerner. Enter Valid Target ID. Target ID is referred to as the Millennium ID that must be created and considered to be a service account used by the Cerner connector. Users must get the Millennium ID created from the Cerner through some form of Service Request. For example, "millennium_XXXXXX"
Include end-dated Personnel Records	Disable this option to prevent aggregating INACTIVE Personnel in Cerner.

Additional configuration parameters

- Time out setting is required if the response is getting delayed from the Cerner system. By default, timeout is set to 1 minute. The timeout settings can be configured from the application debug page as follows:
`<entry key="timeout" value="1"/>`
- Cerner API's require version while executing the operations. Currently version 1.0 is supported. Version can be configured from the application debug page as follows:
`<entry key="version" value="1.0"/>`

Schema attributes

Account attributes

The following table lists the account attributes ([Table 1—Account attributes](#)):

Table 1—Account attributes

Attributes	Description
ID	Identifies an object that exists on a target that is exposed by a provider
username	The user name associated with the account. The value of the user name field must be unique within the target Cerner Millennium domain. Any value between 1 and 48 characters
directoryIndicator	<ul style="list-style-type: none"> • True (LDAP user) • False (non-LDAP user) Contains an indicator if the user is an LDAP directory user or not.
birthdate	Birthdate of the personnel.
firstname	First name for the personnel.
lastname	Surname (last name) for the personnel.
middleName	Middle name of the personnel.
displayName	Display name for the personnel.
suffix	Suffix of the personnel.
privilege	Privileges assigned to the Cerner account.
gender	A coded value representing the gender of the personnel.
restriction	A restriction to be assigned to or unassigned from the account.
title	Title (or list of titles) for the personnel. For example, Dr. Mr. and so on.
physicianInd	An indicator if the personnel is a physician or not.
position	A coded value representing the position assigned to the personnel which is treated as Group entity.
beginEffectiveDateT ime	Date/time at which the personnel becomes/became effective.
endEffectiveDateTi me	Date/time at which the personnel ceases/ceased to be effective.
organization Group	When a personnel record is unassigned from an organization group, all organizations in the group will also be unassigned from the personnel record, unless they are associated to another organization group that is still assigned to the personnel. It will be read-only field and data will be displayed during account aggregation.
confidentialityLevel	A coded value representing the confidentiality code that applies to the relationship.
personnelAlias	Personnel alias information.
personnelGroup	It contains personnel group information.
credential	Credentials are used to highlight the level of education and specialty of a care provider.

Group attributes

The following table lists the group attributes ([Table 2—Group attributes](#)):

Table 2—Group attributes

Attributes	Description
Id	The Id of the group.
Display	Display name of the group.

Provisioning Policy attributes

This section describes the provisioning policy attributes for Create and Update Account.

Create Account

The following table lists the provisioning policy attributes for Create Account:

Attributes	Description
username	The user name associated with the account. The value of the user name field must be unique within target Cerner Millennium domain [1- 48 characters]
password	The password for the user account. Any value, assuming that value meets all criteria defined in the Cerner Millennium password policy maintained in AuthView. The password is only required when the user being provisioned is a non-LDAP user (when the user will authenticate against the Cerner Millennium user directory).
first name	Given (first) name for the personnel.
lastname	Surname (last name) for the personnel.
confidentialityLevel	The confidentiality level set for organization or organization groups.

Update Account

The following table lists the provisioning policy attributes for Update Account:

Attributes	Description
confidentialityLevel	The confidentiality level set for organization or organization groups.

Dormant Account support

IdentityIQ for Cerner Healthcare now provides support for an additional functionality of removing an username or disassociating an account which can be achieved by adding a new checkbox with name as **removeUserName** in Provisioning Policy.

Note: If the newly added 'removeUserName' checkbox is checked, then the Cerner Connector would by default remove the Username and disassociate the account from Personnel. This disassociated Username can be assigned to any other account.

If user wants to only remove the Username and not disassociate an account, then add the **disassociateAccount** attribute in the application debug page as follows:

```
<entry key="disassociateAccount" value="false" />
```

- **personnelAlias**

- To provision **personnelAlias** through update account provisioning policy, enter the input format for attribute as follows:

```
alias-id:XXXX#alias-type:<AliasType>#alias-pool:<AliasPool>
```

For example, alias-id:SP#alias-type:DOCUPIN#alias-pool:UPIN

- To provision the **personnelAlias** with StartDate and EndDate, add the **aliasFormat** entry key in the application debug page as follows:

```
<entry key="aliasFormat"
value="alias-id#alias-type#alias-pool#alias-startdate#alias-enddate" />
```

For example,

```
alias-id:SP#alias-type:DOCUPIN#alias-pool:UPIN#alias-startdate:2017/12/5#alias-enddate:2100/12/5
```

- **credential**

- To provision **credential** through update account provisioning policy, enter the input format for attribute as follows:

```
cred-name:<credName><#cred-type:<credType>#cred-state:<credState>#cred-AddToNameIndicator:<true/false>
```

For example,

```
cred-name:MD#cred-type:License#cred-state:AK#cred-AddToNameIndicator:true
```

- To provision the **credential** with displaySequence, beginEffectiveDateTime, endEffectiveDatetime, RenewalDateTime and idNumber, add the credential entry key in the application debug page as follows:

```
<entry key="credFormat"
value="cred-name#cred-type#cred-state#cred-AddToNameIndicator#cred-displaySequence#cred-beginEffectiveDateTime#cred-endEffectiveDatetime#cred-RenewalDateTime#cred-idNumber" />
```

For example,

```
cred-name:MD#cred-type:License#cred-state:AK#cred-AddToNameIndicator:false#cred-idNumber:IDNumber101#cred-displaySequence:101#cred-beginEffectiveDateTime:2015/06/23#cred-endEffectiveDatetime:2100/12/31#cred-RenewalDateTime:2100/09/30
```

- **address**

- To provision **address** through update account provisioning policy, enter the input format for attribute as follows:

```
addr-type$addr-street1$addr-street2$addr-street3$addr-street4$addr-city$addr-state$addr-zipcode$addr-country
```

For example,

Troubleshooting

```
addr-type:Ship To$addr-street1:Street 1$addr-street2:Street
2$addr-street3:Street 3$addr-street4:Street
4$addr-city:Citrus$addr-state:Alberta$addr-zipcode:585546$addr-country:Australia
```

- To provision **address** attributes with additional attributes like addr-begindate and addr-enddate, entry key **addressFormat** must be added in the application debug page as follows:

```
<entry key="addressFormat"
value="addr-type$addr-street1$addr-street2$addr-street3$addr-street4$addr-city$addr-state$addr-zipcode$addr-country $addr-begindate$addr-enddate"/>
```

For example,

```
addr-type:Billing$addr-street1:Street 1$addr-street2:Street
2$addr-street3:Street 3$addr-street4:Street
4$addr-city:Alger$addr-state:Ontario$addr-zipcode:452245$addr-country:Denmark$addr-begindate:2018/10/10$addr-enddate:2018/10/30
```

Note: Default delimiter for address is considered as "\$". In order to change the delimiter, add the following entry in application debug page and change the value:

```
<entry key="addressColumnDelimiter" value="<<delimiter as
required>>"/>
```

The entry key **addressFormat** must be updated with the required delimiter.

- **phone**

- To provision **phone** through update account provisioning policy, enter the input format for attribute as follows:

```
phone-number:<PhoneNumber>#phone-type:<TypeOfPhone>#phone-extension:<PhoneExtension>
```

For example,

```
phone-number:60548567#phone-type:Billing#phone-extension:0015
```

- To provision the **phone** attribute with additional attributes like phone-begindate and phone-enddate, entry key **phoneFormat** must be added in the application debug page as follows:

```
<entry key="phoneFormat"
value="phone-number#phone-type#phone-extension#phone-format#phone-desc#phone-instruction#phone-begindate#phone-enddate"/>
```

For example,

```
phone-number:9885628655#phone-type:Home#phone-extension:12052#phone-format:Default#phone-desc:Description for Phone#phone-instruction:Any specific instruction#phone-begindate:2018/10/10#phone-enddate:2018/12/31
```

Troubleshooting

1 - An error message is displayed while performing the operations

The following error message is displayed while performing the operations:

```
xml.soap.SOAPException: Read timed out" OR "call: Connection Refused: connect
```

Resolution: Ensure that the Cerner server is up and running.

2 - Aggregation task fails with an error message

The Aggregation task fails with the following error message even when the test connection is successful:

An error has occurred retrieving user: XXXXXXXX

Resolution: Verify the read and Write privileges for the respective account.

3 - Insufficient privileges displayed in the Managed System

If insufficient privileges are displayed in the Managed System for a particular account and the domain server is not available, then the permissions of the account are disabled.

This issue is related to the Authorize server not running in the domain. This is caused by an issue with the server controller service.

Resolution: Perform the following to cycle the Millennium domain and resolve the issue:

- Run an **mbt -ctrl**, to verify if there were no orphaned processes
- Run an **mbs -ctrl** to restart

4 - An error message appears during aggregation

During group aggregation the following error message may appear:

```
"Exception during aggregation of Object Type Group on Application CernerOLD. Reason:
sailpoint.connector.ConnectorException: Group Aggregation failed : [Unable to
unmarshall request, error: Unexpected end of element
{urn:cerner:xmlns:security-provisioning:refData}:refData]"
```

Resolution: Ensure that the **position** account schema attribute must be **group** instead of **string**.

Mainframe Integration Modules

This section contains information on the following sections:

- “IdentityIQ for RACF Mainframe”
- “IdentityIQ for TopSecret Mainframe”
- “IdentityIQ for ACF2 Mainframe”
- “IdentityIQ for RACF LDAP Mainframe”
- “IdentityIQ for TopSecret LDAP Mainframe”

Chapter 25: IdentityIQ for RACF Mainframe

The following topics are discussed in this chapter:

Overview	277
Supported features	277
Installing IdentityIQ for RACF Mainframe	277

Overview

The IdentityIQ for RACF Mainframe manages IBM RACF User Profiles and Group Profiles.

Supported features

IdentityIQ for RACF Mainframe supports the following features:

- Create RACF User Profile
- Update RACF User Profile
- Update RACF Group Profile
- Add a RACF Group Profile to a RACF User Profile
- Remove a RACF Group Profile from a RACF User Profile
- Change password of a RACF User Profile
- Enable/Disable a RACF Profile

Installing IdentityIQ for RACF Mainframe

For installing IdentityIQ for RACF Mainframe, perform the following:

1. Install the Connector Gateway.
For more information on installing the Connector Gateway, see [Installing and Configuring Connector Gateway](#) page on compass.
2. Install SailPoint Connector for RACF
For more information on installing the Connector, see *SailPoint Connector for RACF Administration Guide*.

Chapter 26: IdentityIQ for TopSecret Mainframe

The following topics are discussed in this chapter:

Overview	279
Supported features	279
Installing IdentityIQ for TopSecret Mainframe	279

Overview

The IdentityIQ for Top Secret Mainframe manages CA-Top Secret User ACIDs and Profile/Group ACIDs.

Supported features

IdentityIQ for TopSecret Mainframe supports the following features:

- Create ACID for CA-Top Secret User
- Update CA-Top Secret User ACID (for example, update Department, Division, Zone to ACID of a CA-Top Secret User)
- Update CA-Top Secret User ACID to add/remove a CA-Top Secret Profile/Group
- Change password of a CA-Top Secret User
- Enable/Disable a CA-Top Secret User
- Add a CA-Top Secret ACID of a Profile/Group

Installing IdentityIQ for TopSecret Mainframe

For installing IdentityIQ for TopSecret Mainframe, perform the following:

1. Install the Connector Gateway.
For more information on installing the Connector Gateway, see [Installing and Configuring Connector Gateway](#) page on compass.
2. Install SailPoint Connector for CA-Top Secret
For more information on installing the Connector, see *SailPoint Connector for CA-Top Secret Administration Guide*.

Chapter 27: IdentityIQ for ACF2 Mainframe

The following topics are discussed in this chapter:

Overview	281
Supported features	281
Installing IdentityIQ for ACF2 Mainframe	281

Overview

The IdentityIQ for ACF2 Mainframe manages users and UIDs (implemented as Groups) in CA-ACF2.

Supported features

IdentityIQ for ACF2 Mainframe supports the following features:

- Create Users in CA-ACF2
- Update Users in CA-ACF2
- Connect User to Group by updating the UID string of user in CA-ACF2
- Disconnect User from Group by updating the UID string of user in CA-ACF2
- Create and update groups in IdentityIQ for the CA-ACF2 Users
- Change password of a CA-ACF2 User

Installing IdentityIQ for ACF2 Mainframe

For installing IdentityIQ for ACF2 Mainframe, perform the following:

1. Install the Connector Gateway.
For more information on installing the Connector Gateway, see [Installing and Configuring Connector Gateway](#) page on compass.
2. Install SailPoint Connector for CA-ACF2
For more information on installing the Connector, see *SailPoint Connector for CA-ACF2 Administration Guide*.

Chapter 28: IdentityIQ for RACF LDAP Mainframe

The following topics are discussed in this chapter:

Overview	283
Supported features	283
Supported Managed Systems	284
Pre-requisites	285
Administrator permissions	285
Configuration parameters	285
Schema Attributes	286
Account attributes	287
Group attributes	289
Provisioning Policy Attributes	289
Account attributes	287
Additional information	290
Support for PassPhrase	290
Support for Connection Attributes	290
Implementing Secured Communication to RACF LDAP Server	290
Defining Search Scope	293
Troubleshooting	294

Overview

The IdentityIQ for RACF LDAP Mainframe mainly uses the LDAP interfaces to communicate with z/OS LDAP server. The IdentityIQ for RACF LDAP Mainframe supports reading and provisioning of RACF LDAP users and entitlements.

Supported features

IdentityIQ for RACF LDAP Mainframe supports the following features:

- Account Management
 - Manages RACF LDAP Users as Account
 - Aggregate, Refresh Accounts, Partitioning Aggregation
 - Create, Update, Delete
 - Enable, Disable, Change Password
 - Add/Remove Entitlements
- Group Management
 - Aggregation

For more information on partitioning aggregation, see “Defining Search Scope” on page 293.

Supported Managed Systems

IdentityIQ for RACF LDAP Mainframe supports the following managed systems:

- IBM Tivoli Directory Server for z/OS 2.3 with SDBM LDAP back end
- IBM Tivoli Directory Server for z/OS 2.2 with SDBM LDAP back end
- IBM Tivoli Directory Server for z/OS 2.1 with SDBM LDAP back end

TLS communication between IdentityIQ and RACF LDAP Server

If you want secure TLS connection for RACF LDAP, TLS communication must be enabled between IdentityIQ and RACF LDAP Server. For a Java client to connect using TLS and self-signed certificates, install the certificate into the JVM keystore.

System requirements

- The following respective components for z/OS versions must be installed for TLS communication:

z/OS version	Cryptographic Services	z/OS Security Level 3
z/OS 2.1	System SSL Base: FMID HCPT410	System SSL Security Level: FMID: JCPT411
z/OS 2.2	System SSL Base: FMID HCPT420	System SSL Security Level: FMID JCPT421
z/OS 2.3	System SSL Base: FMID HCPT430	System SSL Security Level: FMID JCPT431

- The CSF started task must be active.

Creating TLS communication between IdentityIQ and RACF LDAP Server

To create TLS communication between IdentityIQ and RACF LDAP Server, perform the following:

1. Implement z/OS Secured Communication to RACF LDAP Server.
For more information on implementing the secured communication to RACF LDAP Server, see “Implementing Secured Communication to RACF LDAP Server” on page 290.
2. Export server CA certificate and copy the exported `.cer` file to the Java client computer (IdentityIQ computer).
3. At the client computer execute the following command from the bin directory of JDK:

```
keytool -importcerts -trustcacert -alias aliasName -file <absolute path of certificate> -keystore <JAVA_HOME>/jre/lib/security/cacerts
```

 In the preceding command line, *aliasName* is the name of the alias.
4. Login to IdentityIQ.
5. Create the application for RACF LDAP, use TLS and provide all the required values.
6. Click on **Test Connection** and save the application.

Pre-requisites

Ensure that the following pre-requisites are satisfied for the directory servers:

- **Set the value of the LDAP_COMPAT_FLAGS environment variable to 1**

The SDBM attributes which are in DN format are by default returned in Uppercase format. This causes duplicate entry of entitlement in IdentityIQ due to the difference in the cases of group DN fetched while aggregation and group DN fetched while group membership provisioning operation.

To avoid the mentioned issue, the LDAP_COMPAT_FLAGS environment variable is set to 1 which would return the values for the mentioned attributes in mixed case format that is in the same format as of group DN returned during aggregation.

The LDAP_COMPAT_FLAGS environment variable value can be specified in LDAP server environment variables file. By default, the file name is `/etc/ldap/ds.envvars`.

- **RACF restriction on amount of output**

When processing certain LDAP search requests, SDBM uses the RACF **R_admin** run command interface to issue RACF search commands. The **R_admin** run command interface limits the number of records in its output to 4096. This means that the RACF search command output might be incomplete if you have many users, groups, connections, or resources.

To avoid the mentioned search limit issue, Partition must be defined to retrieve all requested objects. Partitions must be created in such a way that each Partition must not exceed the default or specified search limit. For more information on defining Partitions, see “Defining Search Scope” on page 293.

Administrator permissions

The service account configured for IdentityIQ for RACF LDAP Mainframe must have the read/write privileges over the RACF directory information tree in order to manage the RACF data, that is, the administrator user must have SPECIAL attribute to be able to manage all RACF entries. In order to limit the scope of service account, group-SPECIAL user can be created as per the requirement. Administrator user must not be a PROTECTED user that is, administrator user must have password.

Configuration parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for RACF LDAP Mainframe uses the following configuration parameters:

Parameters	Description
RACF LDAP Configuration Parameters	
useSSL	Specifies if the connection is over TLS.
authorizationType	The authorization type to use when connecting to the server.
user*	User to connect as a DN string such as Administrator.
password	Password for the administrator account.
port*	Port number through which the server is listening.
host*	Host of the LDAP server.

Schema Attributes

Parameters	Description
racfConnectProfileDN*	Connect Profile type DN used during group membership provisioning.
provisionPropertiesToAllConnections	Sets the RACF connection properties defined in Provisioning Policy to all the RACF connections when multiple RACF Groups are requested in single operation.
Account Settings	
searchScope	Depth to search the LDAP tree. <ul style="list-style-type: none">• OBJECT_SCOPE: Limits the search to the base object or named object.• ONELEVEL_SCOPE: Search is restricted to the immediate children of a base object, but excludes the base object itself.• SUBTREE_SCOPE: A subtree search (or a deep search) includes all child objects as well as the base object. When referrals are followed (by default, Integration Module follow referrals) then the scope will also include child domains of the base object (when it is a parent domain) in a forest.
searchDN*	Distinguished name of the container.
iterateSearchFilter	LDAP filter that defines scope for accounts/groups from this container.
filterString	Used to filter object as they are returned for an underlying application. Derived attributes can also be included in the filter.

Note: Attributes marked with * sign are the mandatory attributes.

Additional configuration parameter

When default group is updated from account, to retain the old default group in **racfConnectGroupName** attribute, add the following attribute in the application debug page:

```
<entry key="dropDefaultGroupConnection">
  <value>
    <Boolean>true</Boolean>
  </value>
</entry>
```

Schema Attributes

The application schema is used to configure the objects returned from a Integration Module. When an Integration Module is called, the schema is supplied to the methods on the Integration Module interface. This Integration Module currently supports two types of objects, account and group.

Account attributes

Account objects are used when building identities Link objects.

Attribute	Description
dn	Distinguished name by which the user is known.
racfid	ID for an user on RACF.
objectClass	Describes the kind of object which an entry represents. This attribute is present in every entry, with at least two values. One of the value is top or alias .
racfAttributes	Multi-valued attribute which list keywords that describes more about the user account. For example, racfAttributes can be used to add a RACF user entry with ADSP GRPACC NOPASSWORD or modify a RACF user entry with NOGRPACC SPECIAL NOEXPIRED RESUME NOOMVS .
racfClassName	Multi-valued attribute used to specify the classes in which the new user is allowed to define profiles to RACF for protection. Classes that can be specified are USER, and any resource classes defined in the class descriptor table.
racfDefaultGroup	Represents the default group associated with the user.
racfConnectGroupName	List of groups of which this person is a member. Example: "Sales" or "Engineering"
racfLastAccess	Information about last date-time user logged in to system.
racfProgrammerName	Users name associated with the user ID.
racfPasswordChangeDate	Last date the user changed his password.
racfPasswordInterval	Number of days during which a user's password and password phrase (if set) remain valid.
racfHavePasswordEnvelope	Information whether users password is enveloped.
racfPassPhraseChangeDate	Last date the user changed his password phrase.
racfHavePassPhraseEnvelope	Information whether users password phrase is enveloped.
racfResumeDate	Starting date when user will be allowed to access the system again.
racfRevokeDate	Starting date when user will be disallowed to access the system.
racfSecurityLabel	Users default security label.
racfSecrityLevel	Users default security level.
racfSecurityCategoryList	Multi-valued attribute contains one or more names of installation-defined security categories.
racfLogonDays	A multi-valued attribute which specifies the days of the week when the user is allowed to access the system from a terminal.
racfLogonTime	Hours in the day when the user is allowed to access the system from a terminal.
racfAuthorizationDate	Date when user was defined to RACF system.

Schema Attributes

Attribute	Description
racfInstallationData	Installation data associated the user.
racfDatasetModel	Discrete data set profile name that is used as a model when new data set profiles are created that have userid as the high-level qualifier.
racfOwner	Distinguished name of the owner of the user.
racfOperatorClass	Multi-valued attribute contains classes assigned to this operator to which BMS (basic mapping support) messages are to be routed - CICS segment.
racfOperatorIdentification	Operator ID for use by BMS - CICS segment.
racfOperatorPriority	Number from 0 - 255 that represents the priority of the operator - CICS segment.
racfTerminaltimeout	Time, in hours and minutes, that the operator is allowed to be idle before being signed off - CICS segment.
racfOperatorReSignon	Specifies whether the user is signed off by CICS when an XRF takeover occurs - CICS segment.
SAFAccountNumber	Users default TSO account number when logging on through the TSO/E logon panel - TSO segment.
SAFDefaultCommand	Specifies the command run during TSO logon - TSO segment.
SAFDestination	Specifies the default destination to which the system routes dynamically-allocated SYSOUT data sets - TSO segment.
SAFHoldClass	Specifies the users default hold class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.
SAFJobClass	Specifies the users default job class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.
SAFMessageClass	Specifies the users default message class. The specified value must be 1 alphanumeric character, excluding national characters - TSO segment.
SAFTsoSecurityLabel	Specifies the users Security label entered or used during TSO LOGON - TSO segment.
SAFDefaultSysoutClass	Specifies the users default SYSOUT class - TSO segment.
SAFDefaultUnit	Specifies the default name of a device or group of devices that a procedure uses for allocations - TSO segment.
SAFDefaultLoginProc	Specifies the name of the users default logon procedure when logging on through the TSO/E logon panel - TSO segment.
SAFLogonSize	Specifies the default or requested region size during TSO logon - TSO segment.
SAFMaximumRegionSize	Specifies the maximum region size the user can request at logon - TSO segment.
SAFUserdata	Specifies the optional installation data defined for the user. The specified value must be 4 EBCDIC characters. Valid characters are 0 - 9 and A - F - TSO segment

Group attributes

The group schema is used when building AccountGroup objects which are used to hold entitlements shared across identities.

Attribute	Description
dn	Distinguished name by which the Group is known.
racfid	ID for group on RACF.
objectClass	The values of the objectClass attribute describe the kind of object which an entry represents. The objectClass attribute is present in every entry, with at least two values. One of the values is either “top” or “alias”.
racfAuthorizationDate	Date when group was defined to RACF system.
racfInstallationData	Installation data associated the group.
racfOwner	Distinguished names of objects that have ownership responsibility for the object that is owned.
racfGroupNoTermUAC	Specifies that during terminal authorization checking, RACF is to allow the use of the universal access authority for a terminal when it checks whether a user in the group is authorized to access a terminal.
racfSuperiorGroup	Distinguished name of the superior group of the associated group.
racfSubGroupName	Distinguished name of the groups to which the associated group is superior group.
racfGroupUniversal	Specifies that this is a universal group that allows an effectively unlimited number of users to be connected to it for the purpose of resource access.
racfGroupUserids	Distinguished names of the users which are member of the group.
racfDatasetModel	Discrete data set profile name that is used as a model when new data set profiles are created that have group name as the high-level qualifier.

Provisioning Policy Attributes

The following table lists the provisioning policy attributes for create and update Account:

Attributes	Description
Create Account	
dn*	Distinguished name of the user to be created.
password*	Password of the user to be created.
racfDefaultGroup	Default group of the user to be created. Value for this field will be the DN of the group.
racfOwner	The owner of the user to be created. Value for this field will be the DN of the group or user.

Additional information

Attributes	Description
connection_racfconnectowner	Distinguished name of the connection owner.
connection_racfConnectRevokeDate	Connection Revoke Date. For example, mm/dd/yy
Update Account	
connection_racfconnectowner	Distinguished name of the connection owner.
connection_racfConnectRevokeDate	Connection Revoke Date. For example, mm/dd/yy

Note: The attributes marked with * sign are required attributes.

Additional information

This section describes the additional information related to the IdentityIQ for RACF LDAP Mainframe.

Support for PassPhrase

IdentityIQ for RACF LDAP Mainframe supports PassPhrase feature as follows:

For password change operation on RACF managed system, `racfPassword` or `racfPassPhrase` is supported. If the length of password provided is less than or equal to 8 characters then password attribute used would be `racfPassword` and if the length of password provided is greater than 8 characters then password attribute used would be `racfPassPhrase`.

Support for Connection Attributes

IdentityIQ for RACF LDAP Mainframe supports provisioning of **racfConnectionOwner** and **racfConnectRevokeDate** while provisioning entitlements. For a single entitlement request along with connection attribute values, the values of the attributes are assigned to the connection.

Provision Properties to All Connections: Select to provision same set of connection attributes values to all requested entitlements.

Implementing Secured Communication to RACF LDAP Server

Secured communication to RACF LDAP Server must be implemented using one of the following methods:

- **LDAP SSL:** Communication must be implemented on a port defined to LDAP as secured (ldaps). For more information, see “Implementing LDAP TLS”.
- **AT-TLS policy:** Communication must be implemented on a port defined to LDAP as non-secured (ldap). The TLS processing is done by TCPIP and is transparent to RACF LDAP Server. For more information, see “Implementing AT-TLS policy for RACF LDAP communication”.

The secured communication is implemented using server authentication.

Common implementation procedure

1. A valid server certificate with its associated server private key must be defined. This certificate must be signed by a trusted Certificate Authority's (CA).
2. The server certificate and the CA certificate must be connected to a key ring.
3. The CA certificate must be exported to a file, transferred (using FTP with ASCII mode) to the client and installed there to be used for certificate verification by the TLS handshake process.

Note: For testing purposes, a local CA can be defined for signing the server certificate.

Implementing LDAP TLS

For detailed information about implementing LDAP TLS, see “Setting up for SSL/TLS” chapter of *z/OS IBM Tivoli Directory Server Administration and Use for z/OS IBM manual*.

Note: RACF LDAP server must be granted with permission to access the key ring containing the RACF LDAP server certificate and the CA certificate.

Implementing AT-TLS policy for RACF LDAP communication

For detailed information about implementing AT-TLS policy, see “Application Transparent Transport Layer Security data protection” chapter of *z/OS Communications Server IP Configuration Guide*.

The required policy attributes for AT-TLS policy are:

- Local Port Range – ports defined in LDAP as non-secured
- Direction = Inbound
- TLS Enabled = On
- TLS v1.1 = On
- TLS v1.2 = On
- Handshake Role = Server
- Client Authorization Type = PassThru
- Application Controlled = Off
- Secondary Map = Off
- The name of the certificate created for the secured communication and the name of the key ring to which the server certificate and the CA certificate are connected, should be specified.

Note: TCPIP must be granted permission to access the key ring to which the RACF LDAP server certificate and the CA certificate are connected.

Sample file for AT-TLS policy

```
# RULE for LDAP GLDSRV
#####
TTLSRule LDAP
{
  LocalAddr ALL
  RemoteAddr ALL
  LocalPortRange 389
  Direction Inbound
  Priority 255 # highest priority rule
  Userid GLDSRV
  TTLSGroupActionRef GrpAct_LDAP
  TTLSEnvironmentActionRef GrpEnv_LDAP
```

Additional information

```
TTLSTConnectionActionRef GrpCon_LDAP
}

TTLSTGroupAction GrpAct_LDAP
{
    TTLS-enabled On
    Trace 7
}

TTLSTEnvironmentAction GrpEnv_LDAP
{
    Trace 7
    HandshakeRole Server
    EnvironmentUserInstance 0
    TTLSKeyringParmsRef PrmKeyRing_LDAP
    TTLSEnvironmentAdvancedParmsRef PrmEnvAdv_LDAP
}

TTLSTEnvironmentAdvancedParms PrmEnvAdv_LDAP
{
    TLSv1.1 On
    TLSv1.2 On
    ClientAuthType PassThru
}

TTLSTConnectionAction GrpCon_LDAP
{
    HandshakeRole Server
    TTLS-CipherParmsRef PrmCipher_LDAP
    TTLSConnectionAdvancedParmsRef PrmConAdv_LDAP
    CtraceClearText Off
    Trace 7
}

TTLSTConnectionAdvancedParms PrmConAdv_LDAP
{
    ApplicationControlled Off
    CertificateLabel GLDSRV
    SecondaryMap Off
}

TTLSTCipherParms PrmCipher_LDAP
{
    # supported cipher suites - we used a wide list, that should be decreased according
    # to specific needs
    V3CipherSuites TLS_DH_DSS_WITH_DES_CBC_SHA
    V3CipherSuites TLS_DH_RSA_WITH_DES_CBC_SHA
    V3CipherSuites TLS_NULL_WITH_NULL_NULL
    V3CipherSuites TLS_RSA_WITH_NULL_MD5
    V3CipherSuites TLS_RSA_WITH_NULL_SHA
    V3CipherSuites TLS_RSA_EXPORT_WITH_RC4_40_MD5
    V3CipherSuites TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
    V3CipherSuites TLS_RSA_WITH_DES_CBC_SHA
    V3CipherSuites TLS_DHE_DSS_WITH_DES_CBC_SHA
    V3CipherSuites TLS_DHE_RSA_WITH_DES_CBC_SHA
    V3CipherSuites TLS_RSA_WITH_AES_256_CBC_SHA256
    V3CipherSuites TLS_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
}
```

```

V3CipherSuites      TLS_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
V3CipherSuites      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_CBC_SHA
V3CipherSuites      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
V3CipherSuites      TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
}
TTLSKeyringParms PrmKeyRing_LDAP
{
    Keyring GLDRING
}

```

Defining Search Scope

Note: IdentityIQ for RACF LDAP Mainframe supports Partitioning Aggregation feature to enable faster retrieval of RACF data. In order to define search scope, enabling Partitioning Aggregation on aggregation task is not required.

In IdentityIQ for RACF LDAP Mainframe, objects can be retrieved by means of a **searchDN**, **searchFilter** and **searchScope**. IdentityIQ for RACF LDAP Mainframe partition entries are the application configuration searchDNs list with each entry of the list treated as a single partition.

Typically, the partitions can be defined as the searchDNs list as follows:

```

<entry key="searchDNs">
  <value>
    <List>
      <Map>
        <entry key="iterateSearchFilter" value="(racfid=a*)"/>
        <entry key="searchDN" value="profiletype=USER,cn=SDBM"/>
        <entry key="searchScope" value="SUBTREE"/>
      </Map>
      <Map>
        <entry key="iterateSearchFilter" value="(racfid=b*)"/>
        <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
        <entry key="searchScope" value="SUBTREE"/>
      </Map>
      <Map>
        <entry key="iterateSearchFilter" value="(racfid=c*)"/>
        <entry key="searchDN" value="profiletype=USER,cn= SDBM "/>
      </Map>
    </List>
  </value>
</entry>

```

Troubleshooting

```
        <entry key="searchScope" value="ONELEVEL_SCOPE" />
      </Map>
    <Map>
      <entry key="iterateSearchFilter" value="(racfid=d*)" />
      <entry key="searchDN" value="profiletype=USER,cn= SDBM " />
      <entry key="searchScope" value="SUBTREE" />
    </Map>
.....
...
...
.....

    <Map>
      <entry key="iterateSearchFilter" value="(racfid=z*)" />
      <entry key="searchDN" value="profiletype=USER,cn= SDBM " />
      <entry key="searchScope" value="SUBTREE" />
    </Map>
  </List>
</value>
</entry>
```

Note: Each specified partition has to be unique by way of the iterateSearchFilter value. If not, the first partition would get aggregated skipping the subsequent duplicate ones. Partitions must be created in such a way that each partition must not exceed the default or specified search limit.

Troubleshooting

1 - When setting password/passphrase with 9 - 13 characters an error message is displayed

When setting password/passphrase with 9 - 13 characters, the following error message is displayed:

```
Invalid Password
```

Resolution: Passphrase can be 9 - 100 characters if KDFAES or ICHPWX11 encryption algorithm is present on the server. If KDFAES or ICHPWX11 encryption algorithm is not present on the server then the allowed number of characters for passphrase are 14 - 100.

2 - Change Password operation fails with an error

When performing a self change password operation for an account and if any one of the connection is revoked, the following error message is displayed:

```
[LDAP:error code 1 - R000208 Unexpected racroute error safRC=8 racfRC=36
racfReason=0(srv_authenticate_native_password:3567)]
```

Resolution: For change password operation, connections of the accounts must not be revoked.

3 - Create account request fails with an error

When create account request has multiple groups and default group is not mentioned then create account request would fail with the following error message:

```
Failed to create account. Specifying default group is mandatory when more than one
groups are requested.
```

Resolution: Ensure that the default group is specified. If Owner of the user account is not specified then default group of the user would be the owner of the user account.

Chapter 29: IdentityIQ for TopSecret LDAP Mainframe

The following topics are discussed in this chapter:

Overview	297
Supported features	297
Supported Managed Systems	298
Administrator permissions	298
Configuration parameters	298
Schema Attributes	299
Account attributes	299
TopSecretProfile attributes	301
TopSecretGroup attributes	302
Provisioning Policy Attributes	302
Account attributes	299
Additional information	303
Support for PassPhrase	303
Implementing Secured Communication to Top Secret LDAP Server	303
Partitioning Aggregation	306

Overview

The IdentityIQ for TopSecret LDAP Mainframe mainly uses the LDAP interfaces to communicate with CA LDAP server. The IdentityIQ for TopSecret LDAP Mainframe supports reading and provisioning of Top Secret LDAP users and entitlements.

Supported features

IdentityIQ for TopSecret LDAP Mainframe supports the following features:

- Account Management
 - Manages Top Secret LDAP Users as Account
 - Aggregate, Refresh Accounts, Partitioning Aggregation
 - Create, Update
 - Enable, Disable, Unlock, Change Password
 - Add/Remove Entitlements
- Group Management
 - Aggregation

For more information on partitioning aggregation, see “Partitioning Aggregation” on page 306.

Supported Managed Systems

IdentityIQ for TopSecret LDAP Mainframe supports the following managed system:

- CA LDAP Server for z/OS Release 15.1.00 with CATSS_UTF back end

TLS communication between IdentityIQ and Top Secret LDAP Server

If you want secure TLS connection for Top Secret LDAP, TLS communication must be enabled between IdentityIQ and Top Secret LDAP Server. For a Java client to connect using TLS and self-signed certificates, install the certificate into the JVM keystore.

Creating TLS communication between IdentityIQ and Top Secret LDAP Server

To create TLS communication between IdentityIQ and Top Secret LDAP Server, perform the following:

1. Implement z/OS Secured Communication to Top Secret LDAP Server.
For more information on implementing the secured communication to Top Secret LDAP, see “Implementing Secured Communication to Top Secret LDAP Server” on page 303.
2. Export server CA certificate and copy the exported `.cer` file to the Java client computer (IdentityIQ computer).
3. At the client computer execute the following command from the bin directory of JDK:
`keytool -importcerts -trustcacert -alias aliasName -file <absolute path of certificate> -keystore <JAVA_HOME>/jre/lib/security/cacerts`
In the preceding command line, *aliasName* is the name of the alias.
4. Login to IdentityIQ.
5. Create the application for Top Secret LDAP, use TLS and provide all the required values.
6. Click on **Test Connection** and save the application.

Administrator permissions

The service account configured for IdentityIQ for TopSecret LDAP Mainframe must have the read/write privileges over the Top Secret directory information tree in order to manage the Top Secret data.

Configuration parameters

This section contains the information that this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The IdentityIQ for TopSecret LDAP Mainframe uses the following configuration parameters:

Parameters	Description
Host*	Host of the LDAP server.
Port*	Port number through which the server is listening.
Use TLS	Specifies if the connection is over TLS.
User*	User to connect as a DN string such as Administrator.

Parameters	Description
Password	Password for the administrator account.
Suffix*	Distinguished name of the container.
Account Filter	LDAP filter that defines scope for accounts from this container.

Note: Attributes marked with * sign are the mandatory attributes.

Schema Attributes

The application schema is used to configure the objects returned from a Integration Module. When an Integration Module is called, the schema is supplied to the methods on the Integration Module interface. This Integration Module currently supports three types of objects account, TopSecretProfile and TopSecretGroup.

Account attributes

Account objects are used when building identities Link objects.

Attribute	Description
dn	Distinguished name of the Top Secret User.
ACCESSORID	Top Secret User ID.
objectClass	Top Secret User Object Classes.
AACID	Authority levels at which ACID can manage ACIDs within scope.
AdminListData	Authority to list Security File information
Misc1	Authority to perform one or more administrative functions (LCF, INSTDATA, USER, LTIME, SUSPEND, NOATS, RDT, TSSSIM, ALL)
Misc2	Authority to perform one or more administrative functions (ALL, SMS, TSO, NDT, DLF, APPCLU, WOR)
Misc3	Authority to perform one or more administrative functions (ALL, SDT, PTOK)
Misc8	Authority to list the contents of the RDT, FDT or STC or to use the ASUSPEND administrative function (LISTRDT, LISTSTC, LISTAPLU, LISTSDT, MCS, NOMVSDF, PWMAINT, REMASUSP, ALL)
Misc9	Authority to perform one or more high-level administrative functions (BYPASS, TRACE, CONSOLE, MASTFAC, MODE, STC, GLOBAL, GENERIC, ALL)
ASUSPEND	Account is suspended due to administrator action.
NODSNCHK	CA Top Secret bypasses all data set access security checks for this ACID.
SITRAN	CICS transaction CA Top Secret automatically executes after an ACID successfully signs on to a facility.
OPCLASS	CICS operator classes.
OPIDENT	CICS operator identification value equal to the ACID OPIDENT entry in the CICS SNT (Signon Table).

Schema Attributes

Attribute	Description
OPPRTY	CICS operator priority of associated ACID.
SCTYKEY	CICS security keys an ACID may use.
CONSOLE	Ability to modify control options by ACID.
CREATED	Date ACID was created.
DEPT	Department ACID.
DIVISION	Division ACID.
EXPIRE	Expiration date of ACID.
GROUPS	List of Groups a TSS User is a member.
XSUSPEND	Account is suspended due to CA-Top Secret Installation exit.
LAST-COUNT	Number of times the ACID has been used (logon times since user was defined).
MASTFAC	Multi-user facility name.
MCSAUTH	Authorize the operator commands that can be entered from the console.
PROFILES	List of Profiles a Top Secret User is a member.
MODIFIED	Last date and time when ACID was updated.
NAME	Name of ACID.
NOPWCHG	Prevent ACID from changing passwords at signon or initiation.
OIDCARD	Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.
DFLTGRP	Default group to an ACID operating under OpenEdition MVS.
HOME	Subdirectory of ACID under OMVS.
UID	Numeric UID value for security within USS.
PSUSPEND	Account is suspended due to password violation.
PHYSKEY	Physical security key to support external authentication devices.
TSOHCLASS	Default hold class for TSO-generated JCL for TSO users.
TSOJCLASS	Job class for TSO generated job cards from TSO users.
TSOLACCT	TSO Default account number.
TSOCOMMAND	Default command issued at TSO logon.
TSOLPROC	Default procedure used for TSO logon.
TSOMSIZE	Maximum region size (in kilobytes) that a TSO user may specify at logon.
TSOMCLASS	Default message class for TSO generated JCL for TSO users.
TSOMPW	Support multiple TSO UADS passwords, on a user-by-user basis.
TSOOPT	Default options that a TSO user may specify at logon
TSODEST	Default destination identifier for TSO generated JCL for TSO users.
TSODEFPRFG	Default TSO performance group.

Attribute	Description
TSOLSIZE	Default region size (in kilobytes) for TSO.
TSOSCLASS	Default SYSOUT class for TSO generated JCL for TSO users.
TSOUNIT	Default unit name for dynamic allocations under TSO.
TSOUDATA	Site-defined data field to a TSO user.
USER	User defined classes and resources.
PASSEXPD	Expiration date of password.
PASSINTV	Number of days during which password remains valid.
TYPE	ACID type (MSCA,LSCA,SCA,ZCA,VCA,MCA,USER).
VSUSPEND	Account is suspended due to access violation.
ZONE	Zone ACID.

TopSecretProfile attributes

The following table lists the profile attributes.

Attribute	Description
dn	Distinguished name of Top Secret Profile.
ACCESSORID	Top Secret Profile Id.
objectClass	Top Secret Profile Object Classes.
AUDIT	Allow an audit of ACID activity.
CREATED	Date ACID was created.
DEPT	DEPT ACID.
DIVISION	Division ACID.
GAP	Globally administered profile.
MODIFIED	Last date and time when ACID was updated.
NAME	Name of ACID.
NOPWCHG	Prevent ACID from changing passwords at signon or initiation.
OIDCARD	Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.
GID	Group identification for OMVS.
SOURCE	Source reader or terminal prefixes through which the associated ACID may enter the system.
LTIME	How long (in minutes) until terminal of ACID locks if CA Top Secret does not detect activity at that terminal.
TYPE	ACID type.
ZONE	Zone ACID.

TopSecretGroup attributes

The following table lists the group attributes.

Attribute	Description
dn	Distinguished name of Top Secret Profile.
ACCESSORID	Top Secret Group Id.
objectClass	Top Secret Group Object Classes.
AUDIT	Allow an audit of ACID activity.
CREATED	Date ACID was created.
DEPT	DEPT ACID.
DIVISION	Division ACID.
GAP	Globally administered profile.
MODIFIED	Last date and time when ACID was updated.
NAME	Name of ACID.
NOPWCHG	Prevent ACID from changing passwords at signon or initiation.
OIDCARD	Prompt ACID to insert identification cards into a batch reader whenever signing on to TSO.
GID	Group identification for OMVS.
SOURCE	Source reader or terminal prefixes through which the associated ACID may enter the system.
LTIME	How long (in minutes) until terminal of ACID locks if CA Top Secret does not detect activity at that terminal.
TYPE	ACID type.
ZONE	Zone ACID.

Provisioning Policy Attributes

The following table lists the provisioning policy attributes for create Account:

Attributes	Description
USER DN*	Distinguished name of the user to be created.
Password*	Password of the user to be created.
Full Name*	Name of the Top Secret user to be created
Department*	DEPT of which the user would be a part.
Facilities	Permit an ACID to have access to a resource through the specified facility.
TSOLPROC	Default procedure used for TSO logon.

Attributes	Description
CONSOLE	Ability to modify control options by ACID.

Note: The attributes marked with * sign are required attributes.

Additional information

This section describes the additional information related to the IdentityIQ for TopSecret LDAP Mainframe.

Support for PassPhrase

IdentityIQ for TopSecret LDAP Mainframe supports PassPhrase feature as follows:

For password change operation on TopSecret LDAP Mainframe managed system, `userPassword` or `PassPhrase` is supported. If the length of password provided is less than or equal to 8 characters then password attribute used would be `userPassword` and if the length of password provided is greater than 8 characters then password attribute used would be `PassPhrase`. To support self change password or passphrase on Top Secret, then appropriate logon option must be specified that is., only password or only passphrase or both.

Implementing Secured Communication to Top Secret LDAP Server

Secured communication to Top Secret LDAP Server must be implemented using one of the following methods:

- **LDAP SSL:** Communication must be implemented on a port defined to LDAP as secured (ldaps).
For more information, see “Implementing LDAP TLS”.
- **AT-TLS policy:** Communication must be implemented on a port defined to LDAP as non-secured (ldap).
The TLS processing is done by TCPIP and is transparent to Top Secret LDAP Server.
For more information, see “Implementing AT-TLS policy for Top Secret LDAP communication”.

The secured communication is implemented using server authentication.

Common implementation procedure

1. A valid server certificate with its associated server private key must be defined. This certificate must be signed by a trusted Certificate Authority's (CA).
2. The server certificate and the CA certificate must be connected to a key ring.
3. The CA certificate must be exported to a file, transferred (using FTP with ASCII mode) to the client and installed there to be used for certificate verification by the TLS handshake process.

Note: For testing purposes, a local CA can be defined for signing the server certificate.

Implementing LDAP TLS

For detailed information about implementing LDAP TLS, see *CA LDAP Server for z/OS Product Guide*.

Note: Top Secret LDAP Server must be granted with permission to access the key ring containing the Top Secret LDAP Server certificate and the CA certificate.

Implementing AT-TLS policy for Top Secret LDAP communication

For detailed information about implementing AT-TLS policy, see “Application Transparent Transport Layer Security data protection” chapter of *z/OS Communications Server IP Configuration Guide*.

The required policy attributes for AT-TLS policy are:

- Local Port Range – ports defined in LDAP as non-secured
- Direction = Inbound
- TLS Enabled = On
- TLS v1.1 = On
- TLS v1.2 = On
- Handshake Role = Server
- Client Authorization Type = PassThru
- Application Controlled = Off
- Secondary Map = Off
- The name of the certificate created for the secured communication and the name of the key ring to which the server certificate and the CA certificate are connected, should be specified.

Note: TCPIP must be granted permission to access the key ring to which the Top Secret LDAP Server certificate and the CA certificate are connected.

Sample file for AT-TLS policy

```
# RULE for LDAP GLDSRV
#####
TTLRule LDAP
{
    LocalAddr ALL
    RemoteAddr ALL
    LocalPortRange 389
    Direction Inbound
    Priority 255 # highest priority rule
    Userid GLDSRV
    TTLSGroupActionRef GrpAct_LDAP
    TTLSEnvironmentActionRef GrpEnv_LDAP
    TTLSConnectionActionRef GrpCon_LDAP
}

TTLSGroupAction GrpAct_LDAP
{
    TTLSEnabled On
    Trace 7
}

TTLSEnvironmentAction GrpEnv_LDAP
{
    Trace 7
    HandshakeRole Server
    EnvironmentUserInstance 0
    TTLSKeyringParmsRef PrmKeyRing_LDAP
    TTLSEnvironmentAdvancedParmsRef PrmEnvAdv_LDAP
}

TTLSEnvironmentAdvancedParms PrmEnvAdv_LDAP
```



```

{
    TLSv1.1 On
    TLSv1.2 On
    ClientAuthType PassThru
}

TTLSConnectionAction GrpCon_LDAP
{
    HandshakeRole Server
    TTLS cipherParmsRef PrmCipher_LDAP
    TTLSConnectionAdvancedParmsRef PrmConAdv_LDAP
    CtraceClearText Off
    Trace 7
}
TTLSConnectionAdvancedParms PrmConAdv_LDAP
{
    ApplicationControlled Off
    CertificateLabel GLDSRV
    SecondaryMap Off
}
TTLSCipherParms PrmCipher_LDAP
{
    # supported cipher suites - we used a wide list, that should be decreased according
    # to specific needs
    V3CipherSuites      TLS_DH_DSS_WITH_DES_CBC_SHA
    V3CipherSuites      TLS_DH_RSA_WITH_DES_CBC_SHA
    V3CipherSuites      TLS_NULL_WITH_NULL_NULL
    V3CipherSuites      TLS_RSA_WITH_NULL_MD5
    V3CipherSuites      TLS_RSA_WITH_NULL_SHA
    V3CipherSuites      TLS_RSA_EXPORT_WITH_RC4_40_MD5
    V3CipherSuites      TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
    V3CipherSuites      TLS_RSA_WITH_DES_CBC_SHA
    V3CipherSuites      TLS_DHE_DSS_WITH_DES_CBC_SHA
    V3CipherSuites      TLS_DHE_RSA_WITH_DES_CBC_SHA
    V3CipherSuites      TLS_RSA_WITH_AES_256_CBC_SHA256
    V3CipherSuites      TLS_RSA_WITH_AES_256_CBC_SHA
    V3CipherSuites      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_RSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
    V3CipherSuites      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_CBC_SHA
    V3CipherSuites      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_RSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
    V3CipherSuites      TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA

```

Additional information

```
V3CipherSuites      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
V3CipherSuites      TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
}
TTLSKeyringParams PrmKeyRing_LDAP
{
    Keyring GLDRING
}
```

Partitioning Aggregation

IdentityIQ for TopSecret LDAP Mainframe supports Partitioning Aggregation feature to enable faster retrieval of Top Secret data.

In IdentityIQ for TopSecret LDAP Mainframe, objects can be retrieved by means of a **searchDN** and **searchFilter**. IdentityIQ for TopSecret LDAP Mainframe partition entries are the application configuration searchDNs list with each entry of the list treated as a single partition.

Typically, the partitions can be defined as the searchDNs list as follows:

```
<entry key="searchDNs">
  <value>
    <List>
      <Map>
        <entry key="iterateSearchFilter" value="(tssacid=a*)" />
        <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us" />
      </Map>
      <Map>
        <entry key="iterateSearchFilter" value="(tssacid=b*)" />
        <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us" />
      </Map>
      <Map>
        <entry key="iterateSearchFilter" value="(tssacid=c*)" />
        <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us" />
      </Map>
      <Map>
        <entry key="iterateSearchFilter" value="(tssacid=d*)" />
        <entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us" />
      </Map>
      .....
      ...
      ...
      .....
    </Map>
```

```
<entry key="iterateSearchFilter" value="(tssacid=z*)" />
<entry key="searchDN" value="host=SYSB,o=SAILPOINT,c=us " />
</Map>
</List>
</value>
</entry>
```

Additional information

Appendix

This section contains information on the following:

- "A: Common Identity Management Integration Configuration" on page 311
- "B: Component Interface" on page 319
- "C: Connector Classloader" on page 335

Appendix A: Common Identity Management Integration Configuration

This appendix describes the following information.

Overview	311
Creating the IntegrationConfig Object	311
Provisioning	316

Overview

This appendix describes configuration process for integrations with identity management (IDM) systems and the places in IdentityIQ that use the integrations. It does not describe the details of a specific integration only the general framework common to all integrations.

Creating the IntegrationConfig Object

The first step in configuring an integration is designing an instance of the IntegrationConfig object. There is currently no user interface for editing these objects, you must write them in XML and import them. The IntegrationConfig defines the following things:

- Java class that handles communication with the IDM system
- Connection parameters such as host name, user name, and password
- IdentityIQ Application object that represents the IDM system in aggregations
- List of the applications that are managed by the IDM system
- Resource and attribute name mappings
- Role synchronization style
- Methods for selecting roles to synchronize

Here is an example of IntegrationConfig file that has all of the options:

```
<IntegrationConfig name='Example Integration'
  executor='sailpoint.integration.ExampleIntegration'
  roleSyncStyle='it'>

  <!--
    Application representing the IDM system in IIQ
  -->
  <ApplicationRef>
    <Reference class='Application' name='Example Integration' />
  </ApplicationRef>

  <!--
    Connection parameters needed by the executor.
  -->

  <Attributes>
    <Map>
```

Creating the IntegrationConfig Object

```
<entry key='url' value='http://somehost:8080/rest/iiq' />
<entry key='username' value='jlarson' />
<entry key='password' value='1:987zxd9872970293874' />
</Map>
</Attributes>

<!--
  Definitions of managed resources and name mappings.
-->
<ManagedResources>
  <ManagedResource name='LDAP 42'>
    <ApplicationRef>
      <Reference class='Application' name='Corporate Directory' />
    </ApplicationRef>
    <ResourceAttributes>
      <ResourceAttribute name='memberOf' localName='groups' />
    </ResourceAttributes>
  </ManagedResource>
</ManagedResources>

<!--
  Synchronized role list.
  In practice you will never have a SynchronizedRoles with
  the RoleSyncFilter or RoleSyncContainer elements. All three
  are shown only as an example.
-->
<SynchronizedRoles>
  <Reference class='Bundle' name='role1' />
  <Reference class='Bundle' name='role2' />
</SynchronizedRoles>
```

The executor attribute has the name of a class that implements the `sailpoint.object.IntegrationExecutor` interface. This class is conceptually similar to a Connector class in that it does the work specific to a particular integration. Each integration package will come with an example `IntegrationConfig` that contains the executor class name.

The `roleSyncStyle` attribute defines how roles are synchronized between IdentityIQ and the IDM system. The possible values are:

- **none**: roles are not synchronized
- **detectable**: detectable (IT) roles are synchronized
- **assignable**: assignable (business) roles are synchronized
- **dual**: both detectable and assignable roles are synchronized

If this attribute has no value the default is none. More information on the role synchronization process is found in the Role Synchronization section.

ApplicationRef

Some integrations support identity aggregation. In these cases there is a **sailpoint.object.Application** object defined to represent the IDM system and an implementation of the **sailpoint.connector.Connector** interface that handles communication with the IDM system. This is normally a multiplexed connector that returns objects representing the IDM system account as well as accounts on managed resources. Links in the identity cube are created for the managed resource accounts as well as the IDM system account.

```
<ApplicationRef>
  <Reference class='Application' name='Example Integration' />
```



```
</ApplicationRef>
```

The documentation of each integration must describe the supported configuration attributes.

The following attributes are reserved and can only be used for the purposes defined here.

- **roleSyncHistory**: list of objects containing a history of previous synchronizations
- **universalManager**: enables the integration as a manager of all applications

The **roleSyncHistory** attribute contains a list of **sailpoint.object.IntegrationConfig.RoleSyncHistory** objects that have information about roles previously synchronized with this integration. This includes the name of the role and the date it was synchronized. This list can be used by the role synchronization task to optimize communication with the IDM system by sending only the roles that have changed since the last synchronization.

The **universalManager** attribute is set to the string true to enable this integration as a manager for all IdentityIQ applications without a ManagedResources list. This can be helpful in test environments to validate deployment configuration as well as environments where all provisioning must be fulfilled by a single integration.

ManagedResources

If the integration supports provisioning, it must define a list of managed resources that corresponding to applications defined in IdentityIQ. This determines how provisioning plans created during certification or role assignment are divided and sent to each integration.

```
<!--
  Definitions of managed resources and name mappings.
-->
<ManagedResources>
  <ManagedResource name='LDAP 42'>
    <ApplicationRef>
      <Reference class='Application' name='Corporate Directory' />
    </ApplicationRef>
    <ResourceAttributes>
      <ResourceAttribute name='memberOf' localName='groups' />
    </ResourceAttributes>
  </ManagedResource>
</ManagedResources>
```

The ManagedResources element contains a list of ManagedResource elements. A ManagedResource element must contain an ApplicationRef that defines the associated IdentityIQ application. The ManagedResource element might have an optional name attribute that defines the name of the resource within the IDM system. If the name is not specified it is assumed that the resource name is the same as the IdentityIQ application name.

The ManagedResource element might also contain a ResourceAttributes element that contains one or more ResourceAttribute elements. ResourceAttribute is used to define mappings between attribute names in the IDM system and IdentityIQ. ResourceAttribute has the following XML attributes.

- **name**: attribute name in the IDM system
- **localName**: attribute name in the IdentityIQ application schema

If a provisioning plan is sent to this integration with attributes that are not in the ResourceAttributes list it is assumed that the name in IdentityIQ is the same as the name in the IDM system.

The ResourceAttributes list does not define a filter for attributes sent to the IDM system it only defines name mappings. When an integration has an IdentityIQ application in the ManagedResource list it is assumed that all attribute requests for that application are sent to that integration. You cannot have more than one integration managing different sets of attributes for the same application.

Creating the IntegrationConfig Object

There is a special attribute that can be defined in Attributes that declares the integration as the manager of all applications in IdentityIQ regardless of the content of the ManagedResources element. You can still use ManagedResources to define name mappings for certain applications when necessary.

SynchronizedRoles

The SynchronizedRoles element is used to define a concrete list of roles to consider when roles are synchronized. When this is included in an IntegrationConfig object it has priority over both RoleSyncFilter and RoleSyncContainer elements if they are also included.

```
<SynchronizedRoles>
  <Reference class='Bundle' name='role1' />
  <Reference class='Bundle' name='role2' />
</SynchronizedRoles>
```

This can be used to synchronize simple integrations with a small set of roles that does not change often. If the set of roles is large or frequently changing, it is better to use RoleSyncFilter or RoleSyncContainer.

RoleSyncFilter

The RoleSyncFilter element contains a filter that is used to identify the roles to consider for synchronization.

```
<RoleSyncFilter>
  <Filter property='syncFlag' operation='EQ' value='true' />
</RoleSyncFilter>
```

```
<RoleSyncFilter>
  <Filter property='name' operation='LIKE' matchMode='START'
value='Sync' />
</RoleSyncFilter>
```

Synchronization filters typically used extended role attributes. In the first example an extended attribute syncFlag must be configured and have a value of true for the role to be synchronized.

Naming conventions can also be used to identify synchronized roles. In the second example any role whose name starts with Sync is synchronized.

A RoleSyncFilter can be combined with a RoleSyncContainer. If both are specified the intersection of the two role sets is considered for synchronization.

RoleSyncContainer

The RoleSyncContainer element defines the set of roles to be considered for synchronization by identifying an inherited role.

In this example, any role that directly or indirectly inherits the role named Roles To Synchronize is synchronized. This is typically a container role that has no function other than organizing other roles.

Specifying roles with inheritance has the advantage of creating a node in the modeler tree for Roles To Synchronize that you can expand to quickly see all of the synchronized roles.

A RoleSyncContainer can be combined with a RoleSyncFilter. If both are specified the intersection of the two role sets are synchronized.

Note: If an IntegrationConfig does not have any SynchronizedRoles, RoleSyncFilter, or RoleSyncContainer elements and the roleSyncStyle element has a value other than none, it is assumed that all roles are considered for synchronization.

Aggregation

Some integrations support feeds of identity information through the normal aggregation process. In these cases the integration package will have a `SailPoint.connector.Connector` implementation class and an example `SailPoint.object.Application` object in XML.

IDM connectors are usually multiplexed connectors that return objects representing the IDM system account as well as accounts on all managed resources.

When an aggregation application is defined a reference to it should be placed in the `IntegrationConfig`. This enables provisioning operations to obtain the account name in the IDM system that corresponds to an identity in IdentityIQ.

Role Synchronization

Role synchronization is performed by running the standard system task named Synchronize Roles. This task is defined in the file `tasksRunnable.xml` and is created during the normal initialization and upgrade processes.

The task normally attempts synchronization with every **IntegrationConfig** stored in the repository. The task has one hidden input argument, `integrations`, that can be set to a CSV of names of `IntegrationConfig` objects. Use this to restrict the synchronization to a particular set of integrations.

Each **IntegrationConfig** has a **roleSyncStyle** attribute that determines how roles are synchronized. If this attribute is missing or set to `none`, role synchronization is disabled.

When synchronization is enabled, the task first determines the set of candidate roles by evaluating the filtering options defined in the `IntegrationConfig`. If there is a `SynchronizedRoles` element it defines the concrete list of candidate roles. Otherwise the `RoleSyncFilter` and `RoleSyncContainer` are evaluated and intersected to produce the set of candidate roles.

Note: Candidate roles are not necessarily the ones that are sent to the IDM system. The roles sent are further constrained by the synchronization style.

roleSyncStyle=detectable

When the synchronization style is `detectable` the candidate role list is filtered to contain only detectable roles as defined by the role type.

For each candidate role a simplified representation of the role is built using the `SailPoint.integration.RoleDefinition` class, this is called the target role.

Entitlements for the target role are extracted from the candidate in one of two ways. If the candidate role has a provisioning plan, the plan defines the resources and attribute values that are included in the target role. If the candidate role has no provisioning plan, a set of resource attributes is derived by analyzing the profile filters in the candidate role.

To give a role a provisioning plan, design an instance of the `SailPoint.object.ProvisioningPlan` as an XML and place it inside the XML for the `SailPoint.object.Bundle` object representing the role.

Using provisioning plans gives you more control over the contents of the target role. Profile filters might be ambiguous or result in more attribute values for the role than are necessary, but for relatively simple filters it can be easier than defining provisioning plans.

To derive target roles, first build a list of candidate profiles. If the role option `or Profiles` is `false`, then all profiles defined in the role become candidates. If the `or Profiles` option is `true`, then only the first profile in the role is a candidate. Then iterate over each filter in each candidate profile applying this algorithm:

```
if the filter is EQ or CONTAINS_ALL
```

Provisioning

```
    add the values for this attribute comparison to the role
  if the filter is OR
    recurs for the first child filter term
  if the filter is AND
    recurs for all child filter terms
```

If the role inherits other roles, the hierarchy is flattened and inherited entitlements are merged into the target role. The same process described above is applied to every role in the inheritance hierarchy.

roleSyncStyle=assignable

When the synchronization style is assignable the candidate role list is filtered to contain only assignable roles as defined by the role type.

For each candidate role, build a simplified representation of the role using the `SailPoint.integration.RoleDefinition` class, this is called the target role.

Entitlements for the target role are extracted from the candidate by first applying the process described in `roleSyncStyle=detectable` to the candidate role. This might not have any effect since assignable roles do not normally have provisioning plans or profiles.

Next the `roleSyncStyle=detectable` process is applied to each of the required roles referenced by the candidate role. This is typically where most of the entitlements are found.

roleSyncStyle=dual

This is a hybrid of the assignable and detectable styles used only by the IBM Security Provisioning Integration Module.

First detectable roles are synchronized as defined in the “`roleSyncStyle=detectable`” on page 315 section.

Next assignable roles are synchronized. Instead of entitlements the roles have an extended attribute containing the names of all roles that were on the required list. The integration executor might further annotate the role definition with rules for automated assignment.

Provisioning

Provisioning can be performed in several ways.

- After role assignment from the IdentityIQ identity edit page
- After role assignment from the Access Request Manager
- During certification to handle revocations and role completions
- In a background reconciliation task
- During aggregation

Both IdentityIQ and the Access Request Manager (ARM) launch workflows with provisioning being done at the end. This provides the opportunity to insert an approval step before provisioning. The default workflow for IdentityIQ identity edits is named Identity Update. By default it has no approvals but does attempt provisioning. The example workflow for ARM requests is named ARM Role Approval Example.

Certifications can do provisioning to remove entitlements and roles that were revoked as well as add missing entitlements that are necessary to satisfy a role assignment.

A reconciliation task is an instance of the Identity Refresh task template with the provisioning argument set to true. This argument is visible in the configuration page for the refresh task. Reconciliation compares the assigned

roles with the detected entitlements and automatically provisioning any missing entitlements. Entitlements might be missing due to either changes in role assignments for an identity, or changes to the definition of roles already assigned to an identity.

Reconciliation is intended to replace the IdentityIQ Provisioning. The old provisioning page was role oriented, monitored changes to roles, and sent provisioning requests for users assigned to modified roles. It did not detect changes to the assigned roles list of identities, however. The reconciliation task is identity oriented and calculates all changes necessary to make an identity's entitlements match the currently assigned roles.

Since reconciliation is now part of the core set of identity refresh options, it can also be done during aggregation. This is less common, but aggregation could change account attributes that are used by role assignment rules resulting in changes to the assigned and detected role lists. With provisioning enabled, the aggregation could trigger the provisioning of missing entitlements for the assigned roles. A common use case for this would be aggregating from an application representing a HR system with HR attributes determining assigned business roles.

Note: Automated provisioning done by the reconciliation task or within workflows typically does not remove entitlements, it only adds missing entitlements. Removal of unnecessary entitlements is expected to be done in a certification where a user has more control. While it is possible to enable removals during automated provisioning, it is potentially dangerous and should not be done without careful consideration.

Provisioning with Synchronized Roles

The provisioning sub-system works with the role synchronization sub-system to determine how role assignments are provisioned. If roles are not being synchronized, the raw entitlements needed by that role are compiled and sent to the integration executors. If an integration supports role synchronization, requests are compiled to the IDM system itself to add or remove native role assignments.

There might be median cases where an integration does role synchronization, but only manages a subset of the possible applications. In these cases plans are compile with both IDM system role assignments and as raw entitlements for the entitlements that are not covered by a native role assignment.

Appendix B: Component Interface

This appendix describes the following information.

Creating component interface for PeopleSoft	319
Basic structure of Custom Component (CI) from USERMAINT component for Users	319
Basic structure of Custom Component (CI) from ROLEMAINT component for Roles.	325
Basic structure of Custom Component (CI) from RTE_CNTL_PROFILE component for Users	327
Basic structure of Custom Component (CI) from PURGE_USR_PROFILE component for Delete User ..	329
Basic structure of Component Interface (CI) from PURGE_ROLEDEFN component for Delete Role ...	331
Deleting the component interface	332

Creating component interface for PeopleSoft

This section describes the procedure for creating the basic structure of a new Component Interface (CI) for PeopleSoft financial from USERMAINT and ROLEMAINT components.

Basic structure of Custom Component (CI) from USERMAINT component for Users

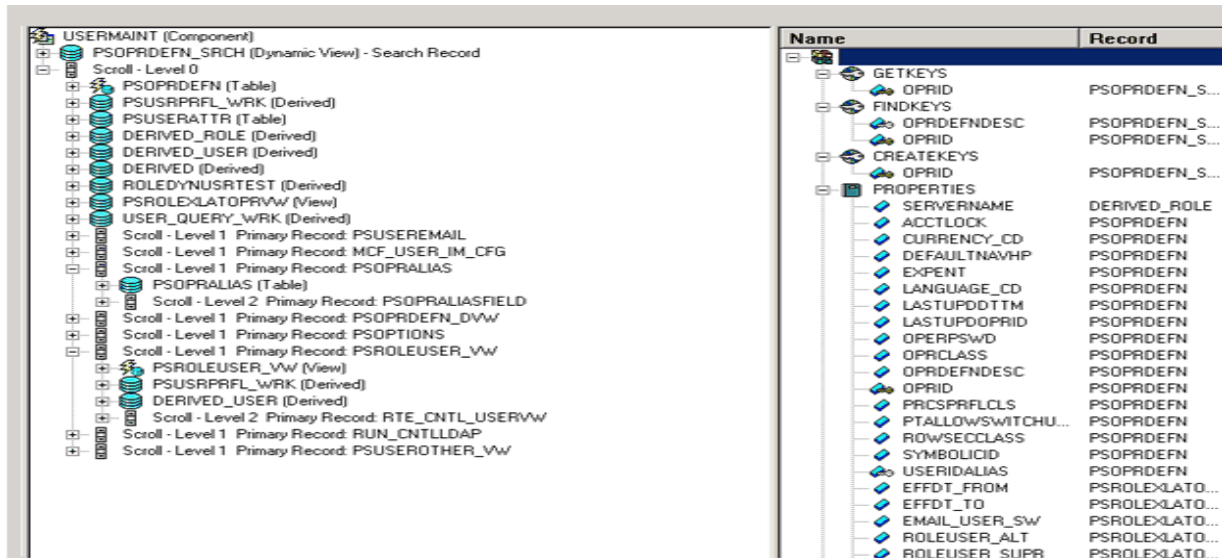
This section describes the creation of basic structure of CI from USERMAINT component, changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CIs, and verification of the newly created CI.

Creating CI

1. Log on to Application Designer and click on **File => New**.
A new dialog box named New Definition is displayed.
2. Select **Component Interface => OK**.
A new dialog box named Select source Component for Component Interface is opened.
3. Enter the name as **USERMAINT** under the **Selection Criteria** tab and click **Select**.
A dialog box appears with the following message:
Do you want to default the properties based on the underlying component definition
4. Click **Yes**.

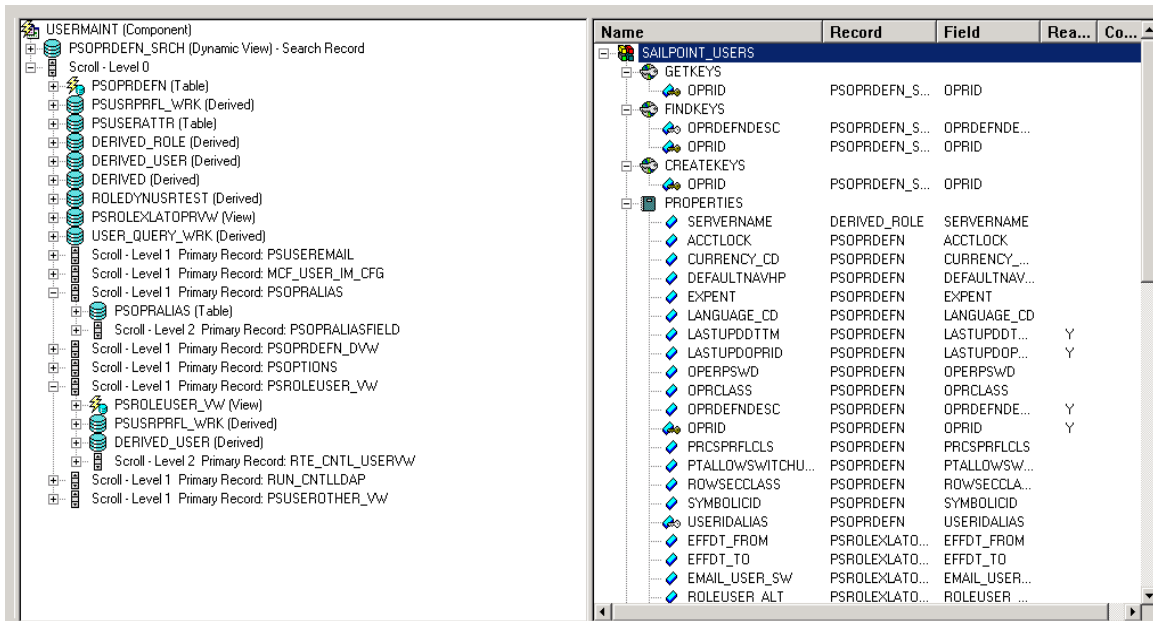
Creating component interface for PeopleSoft

Following screen shot appears:



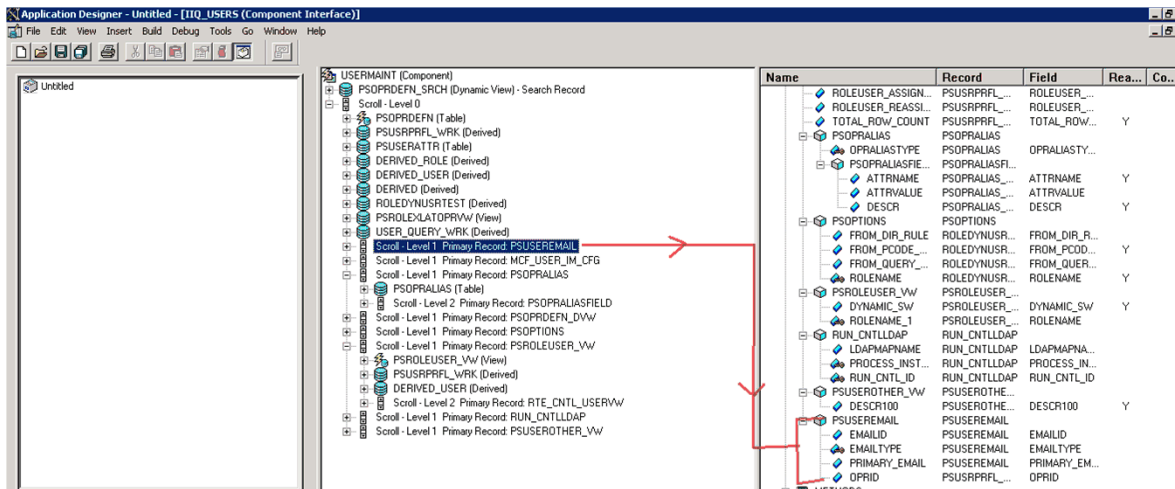
- Click on **File => Save As**.

A new dialog box appears requesting for the name of the CI as follows:

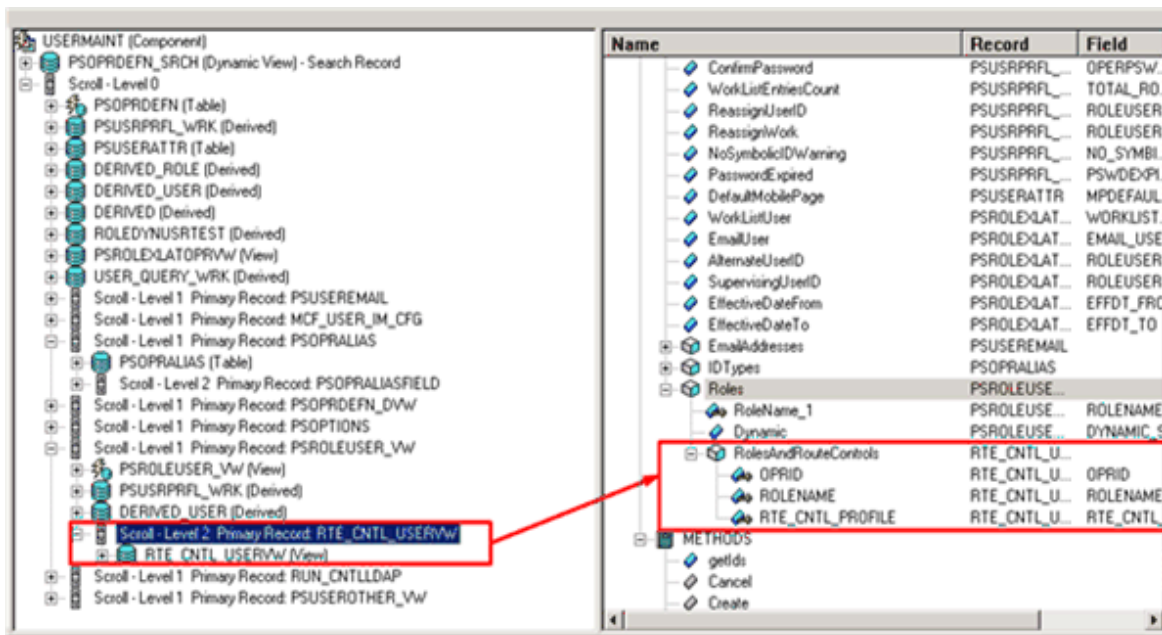


- Enter the name of the CI as **{NEW_Name}**. For example, **SAILPOINT_USERS**.
- Drag the **Scroll-Level1 Primary Record: PSUSERMAIL** from source component (USERMAINT) to the properties of the newly created CI **{NEW_Name}**. For example, **SAILPOINT_USERS**.

After dragging and dropping the Scroll-Level1 Primary Record: PSUSERMAIL attribute, a new property is listed in the PROPERTIES of the newly created CI.



8. Drag the **Scroll-level 2 Primary Record: RTE_CNTL_USERVW** from source component (USERMAINT) to the properties of the newly created CI {NEW_NAME}. for Example, **SAILPOINT_USERS**. After dragging & dropping the Scroll-Level 2 Primary Record: **RTE_CNTL_USERVW** attribute, a new property is listed in the PROPERTIES of the newly created CI and rename it to **RolesAndRouteControls**



Changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI

1. Expand **FINDKEYS** and click on **OPRID**. Right click on **OPRID** and select **Edit Name** to change the attribute name to **UserID**. Similarly change the name of **OPRDEFNDESC** attribute to **UserDescription**.
2. Expand **GETKEYS** and change the name of **OPRID** to **UserID**.

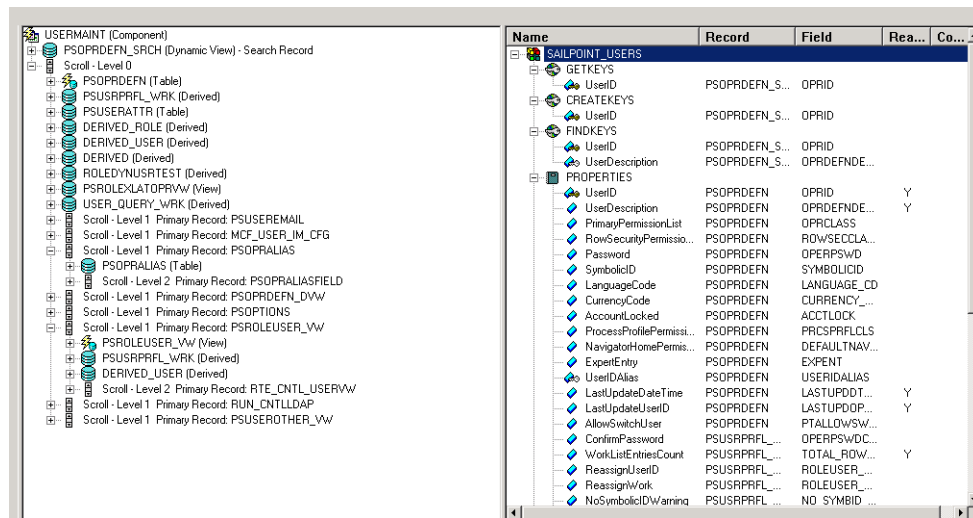
Creating component interface for PeopleSoft

3. Expand **CREATEKEYS** and change the name of **OPRID** to **UserID**.
4. After changing the keys for **GETKEYS**, **FINDKEYS** and **CREATEKEYS**, change the **PROPERTIES**.
 - Changing Single attribute
 - a. Expand **PROPERTIES**.
 - b. Select the attribute and right click on **Edit Name** to change the name of the attribute. Provide the names mentioned in the following table for the respective attributes:

Original attribute name	Changed attribute name
OPRID	UserID
OPRDEFNDESC	UserDescription
OPRCLASS	PrimaryPermissionList
ROWSECCLASS	RowSecurityPermissionList
OPERPSWD	Password
SYMBOLICID	SymbolicID
LANGUAGE_CD	LanguageCode
CURRENCY_CD	CurrencyCode
ACCTLOCK	AccountLocked
PRCSPRFLCLS	ProcessProfilePermissionList
DEFAULTNAVHP	NavigatorHomePermissionList
EXPENT	ExpertEntry
USERIDALIAS	UserIDAlias
LASTUPDDTTM	LastUpdateDateTime
PTALLOWSWITCHUSER	AllowSwitchUser
OPERPSWDCONF	ConfirmPassword
TOTAL_ROW_COUNT	WorkListEntriesCount
ROLEUSER_REASSIGN	ReassignUserID
ROLEUSER_ASSIGN_SW	ReassignWork
NO_SYMBID_WARN	NoSymbolicIDWarning
PSWDEXPIRED	PasswordExpired
MPDEFAULMP	DefaultMobilePage
WORKLIST_USER_SW	WorkListUser
EMAIL_USER_SW	EmailUser
LASTUPDOPRID	LastUpdateUserID
ROLEUSER_ALT	AlternateUserID
ROLEUSER_SUPR	SupervisingUserID
EFFDT_FROM	EffectiveDateFrom
EFFDT_TO	EffectiveDateTo

Original attribute name	Changed attribute name
CHANGE_PWD_BTN	ChangePassword
Note: This attribute is applicable only for PeopleTools version 8.55 and above.	

- c. Delete the **SERVERNAME** property attribute.



- Changing collection attribute
 - a. Some attributes when expanded, have other attributes under them. Such attributes are called as collection attributes.

PSUSEREMAIL	PSUSEREMAIL	
EMAILID	PSUSEREMAIL	EMAILID
EMAILTYPE	PSUSEREMAIL	EMAILTYPE
PRIMARY_EMAIL	PSUSEREMAIL	PRIMARY_EM...
OPRID	PSUSRPRFL_...	OPRID

- b. Select the collection attribute name => right click on the attribute => click on **Edit Name** and change the name of that attribute.
 - c. Expand the Attribute. Change the internal Attribute names also in similar manner. The following table mentions the attribute names to be modified:

Original collection attribute name	Changed collection attribute name	Original child attribute name	Changed child attribute name
PSUSEREMAIL	EmailAddresses	EMAILID	EmailAddress
		EMAILTYPE	EmailType
		PRIMARY_EMAIL	PrimaryEmail
		OPRID	OPRID

Creating component interface for PeopleSoft

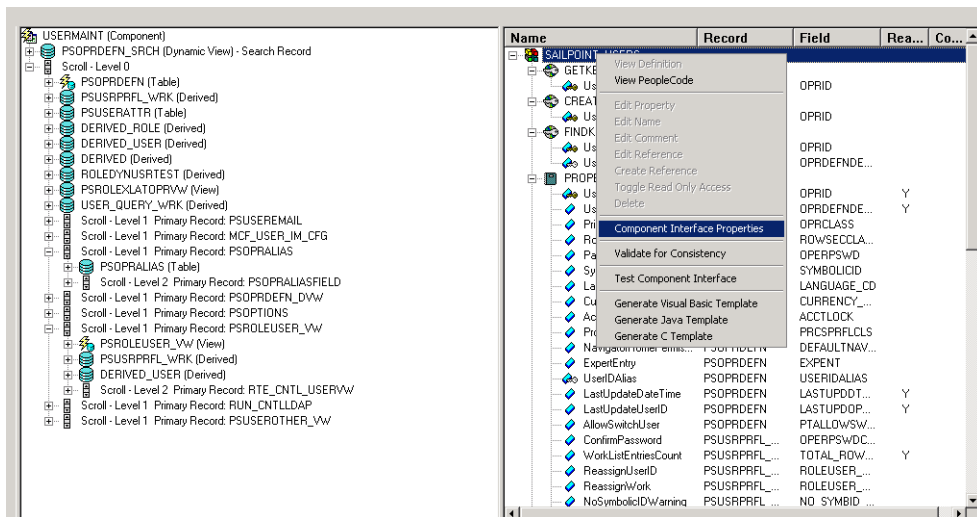
Original collection attribute name	Changed collection attribute name	Original child attribute name	Changed child attribute name
PSOPRALIAS	IDTypes	OPRALIASTYPE	IDType
		PSOPRALIASFIELD	Attributes
		ATTRNAME	AttributeName
		ATTRVALUE	AttributeValue
		DESCR	DESCR
PSROLEUSER_VW	Roles	DYNAMIC_SW	Dynamic
		ROLENAME_1	RoleName_1

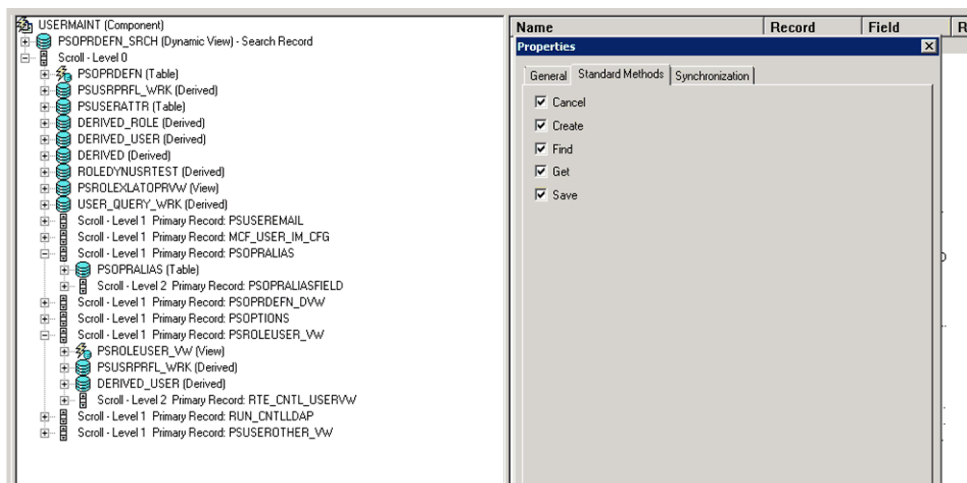
d. After renaming property attributes as mentioned in the above table, delete the following attributes:

- PSOPTIONS
- RUN_CNTLLDAP
- PSUSEROTHER_VW

Verification of the standard methods for the newly created CI

1. Right click on the name of the **CI** => click on **Component Interface Properties** => Click on **Standard Methods**.
where CI is the Component Interface created as mentioned in “Creating component interface for PeopleSoft” on page 319.
2. Verify all properties (**cancel, create, find, get, save**) are selected.





The new CI is ready to be used. For example, **SAILPOINT_USERS**

Basic structure of Custom Component (CI) from ROLEMAINT component for Roles

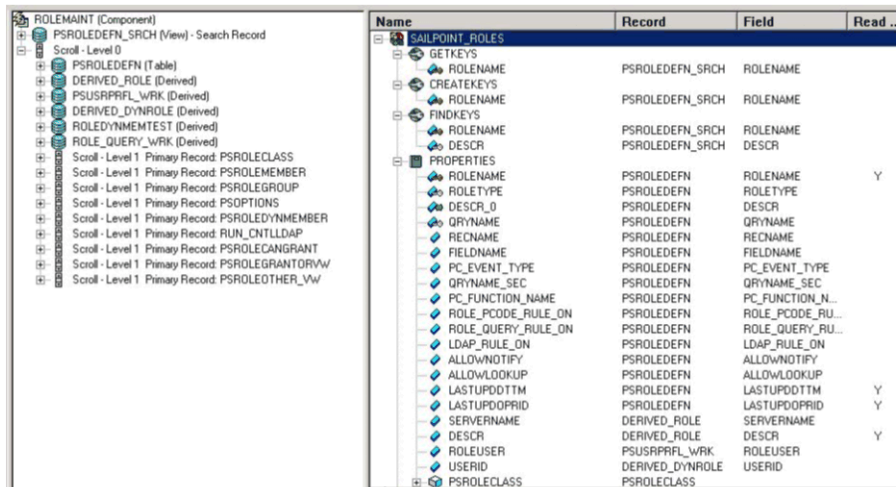
This section describes the creation of basic structure of CI from ROLEMAINT component.

Creating CI

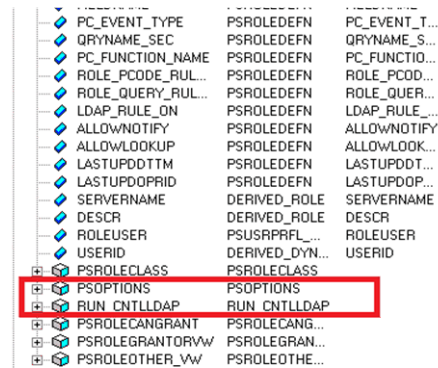
1. Log on to Application Designer and click on **File => New**.
A new dialog box named New Definition is displayed.
2. Select **Component Interface => OK**.
A new dialog box named Select Source Component for Component Interface is opened.
3. Enter the name as **ROLEMAINT** under the **Selection Criteria** tab and click **Select**.
A dialog box appears with the following message:
Do you want to default the properties based on the underlying component definition
4. Click **Yes**.

Creating component interface for PeopleSoft

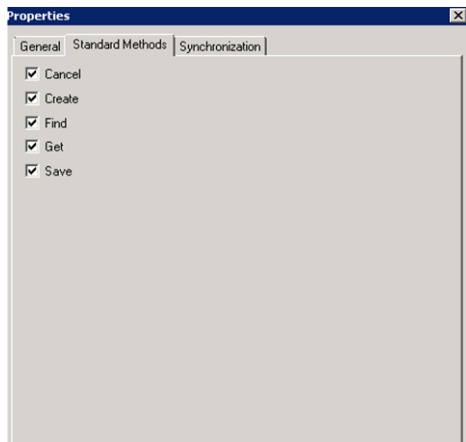
Following screen shot appears:



- Click on **File => Save As**.
A new dialog box appears requesting for the name of the CI.
- Enter the name of the CI as **{NEW_NAME}**. For example, **SAILPOINT_ROLES**.
- Delete the following collective attributes:
 - PSOPTIONS
 - RUN_CNTLLDAP

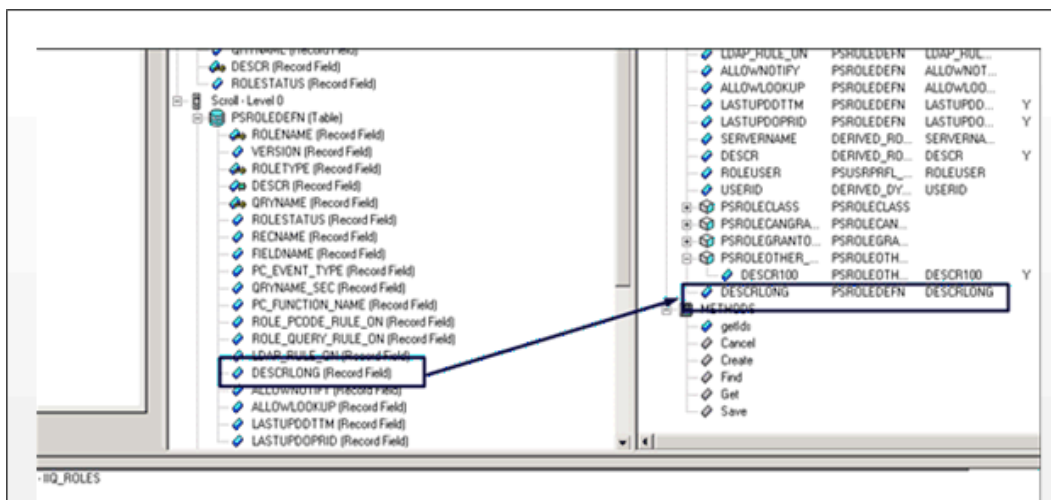


- Verification of the standard methods are selected for this newly created component Interface. For example, **SAILPOINT_ROLES**.



The newly created component interface is ready to be used. For example, **SAILPOINT_ROLES**.

In order to reflect the description for the Role in IdentityIQ, user must drag the following component in Roles component interface as displayed below:



Basic structure of Custom Component (CI) from RTE_CNTL_PROFILE component for Users

This section describes the creation of basic structure of CI from RTE_CNTL_PROFILE component, changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI, and verification of the newly created CI's.

Creating CI

1. Log on to Application Designer and click on **File => New**.
A new dialog box named New Definition is displayed.
2. Select **Component Interface => OK**.
A new dialog box named Select Source Component for Component Interface is opened.
3. Enter the name as **RTE CNTL PROFILE** under the **Selection Criteria** tab and click **Select**.

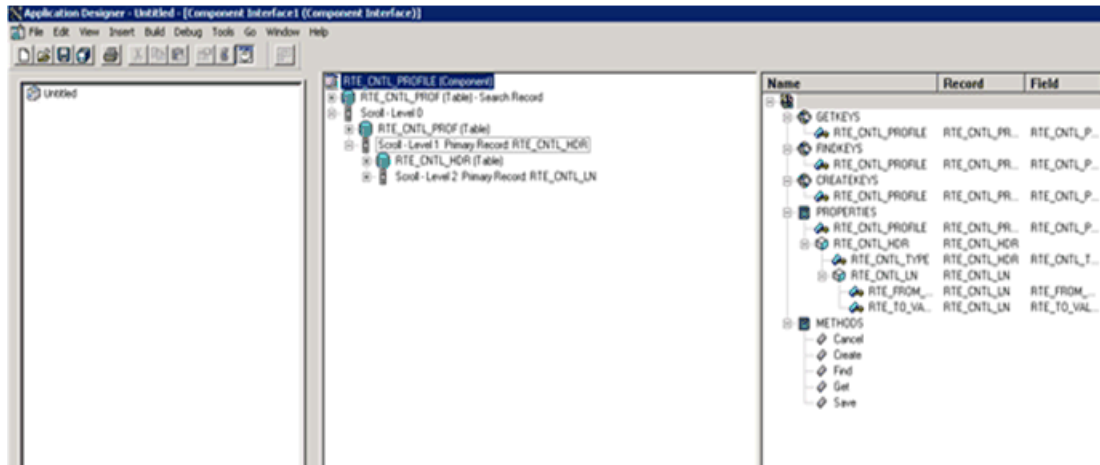
Creating component interface for PeopleSoft

A dialog box appears with the following message:

Do you want to default the properties based on the underlying component definition

4. Click **Yes**.

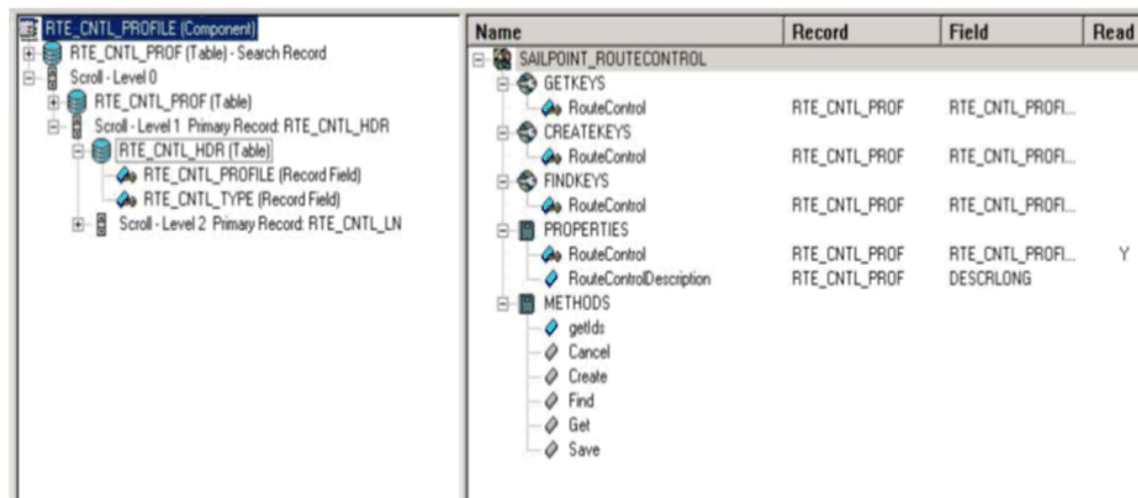
Following screen shot appears:



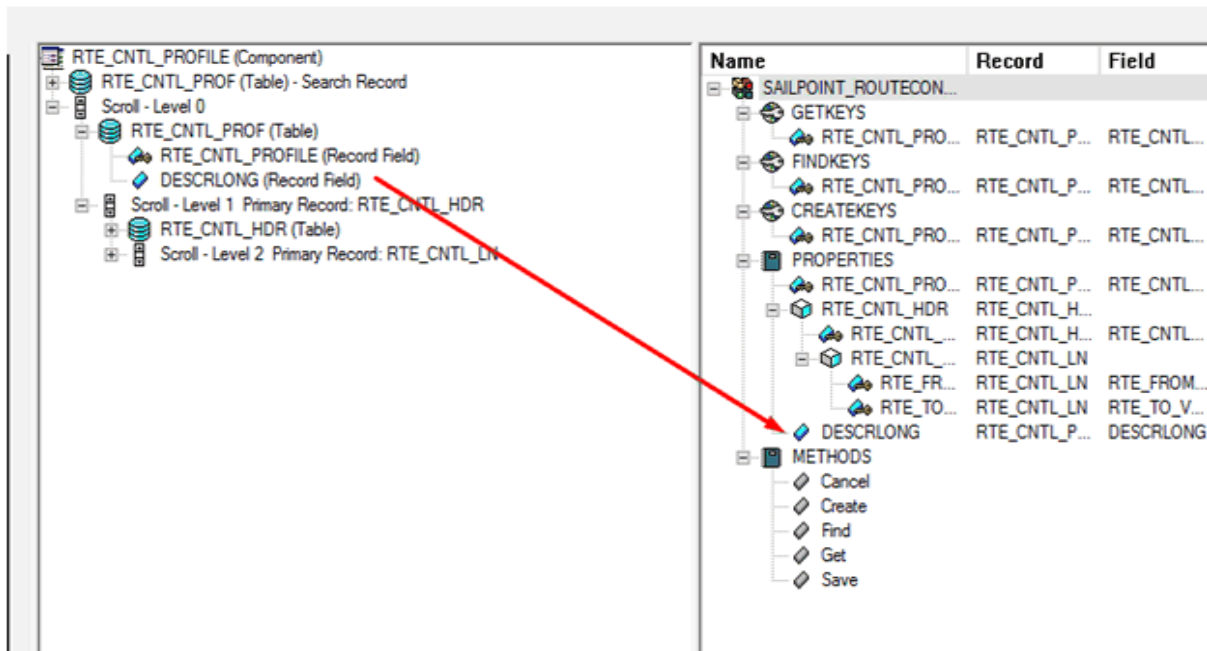
5. Click on **File => Save As**.

A new dialog box appears requesting for the name of the CI.

6. Enter the name of the CI as **{NEW_NAME}**. For example, **SAILPOINT_ROUTECONTROL**.



7. Drag the **Scroll-Level 0 : DESCRLONG (Record Field)** from source component (RTE_CNTL_PROFILE) to the properties of the newly created CI **{NEW_Name}**. For example, **SAILPOINT_ROUTECONTROL**.



Changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI

1. Expand **FINDKEYS** and click on **RTE_CNTL_PROFILE**. Right click on **RTE_CNTL_PROFILE** and select **Edit Name** to change the attribute name to **RouteControl**.
2. Expand **GETKEYS** and change the name of **RTE_CNTL_PROFILE** to **RouteControl**.
3. Expand **CREATEKEYS** and change the name of **RTE_CNTL_PROFILE** to **RouteControl**.
4. After changing the keys for **GETKEYS** and **FINDKEYS** change the **PROPERTIES**.
 - Changing Single attribute
 - a. Expand **PROPERTIES**.
 - b. Select the attribute and right click on **Edit Name** to change the name of the attribute. Provide the names mentioned in the following table for the respective attributes:

Original attribute name	Changed attribute name
OPRID	UserID
OPRDEFNDESC	UserDescription
RTE_CNTL_PROFILE	RouteControl
DESCRLONG	RouteControlDescription

- c. Delete the **RTE_CNTL_HDR** collection.

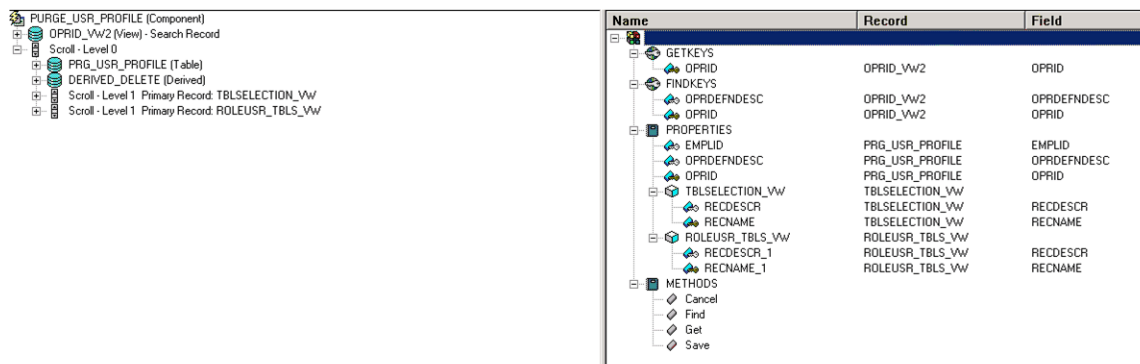
Basic structure of Custom Component (CI) from PURGE_USR_PROFILE component for Delete User

This section describes the creation of basic structure of CI from Delete User component. For example, **SAILPOINT_DEL_USER**

Creating component interface for PeopleSoft

Creating CI

1. Log on to Application Designer and click on **File => New**.
A new dialog box named New Definition is displayed.
2. Select **Component Interface => OK**.
A new dialog box named Select Source Component for Component Interface is opened.
3. Enter the name as **PURGE_USR_PROFILE** under the **Selection Criteria** tab and click **Select**.
A dialog box appears with the following message:
Do you want to default the properties based on the underlying component definition
4. Click **Yes**.
Following screen shot appears:



5. Click on **File => Save As**.
A new dialog box appears requesting for the name of the CI.
6. Enter the name of the CI as **{NEW_NAME}**. For example, **SAILPOINT_DEL_USER**.
Delete the following collective attributes:
 - TBLSELECTION_VW
 - ROLEUSR_TBLS_VW

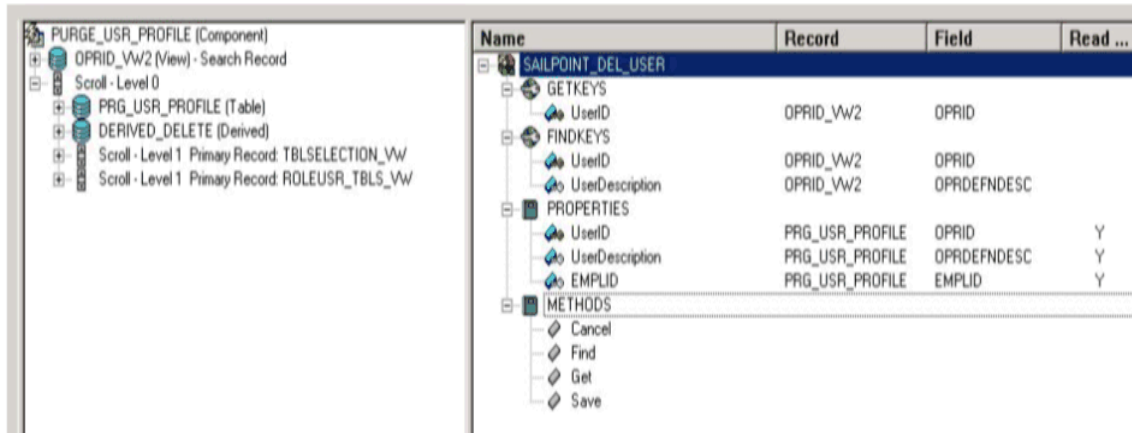
Changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI

1. Expand **FINDKEYS** and click on **OPRID**. Right click on **OPRID** and select **Edit Name** to change the attribute name to **UserID**.
Similarly change the name of **OPRDEFNDESC** attribute to **UserDescription**.
2. Expand **GETKEYS** and change the name of **OPRID** to **UserID**.
3. After changing the keys for **GETKEYS** and **FINDKEYS** change the **PROPERTIES**.
 - Changing Single attribute
 - a. Expand **PROPERTIES**.
 - b. Select the attribute and right click on **Edit Name** to change the name of the attribute. Provide the names mentioned in the following table for the respective attributes:

Original attribute name	Changed attribute name
OPRID	UserID

Original attribute name	Changed attribute name
OPRDEFNDESC	UserDescription

After the changes the CI would appear as follows:

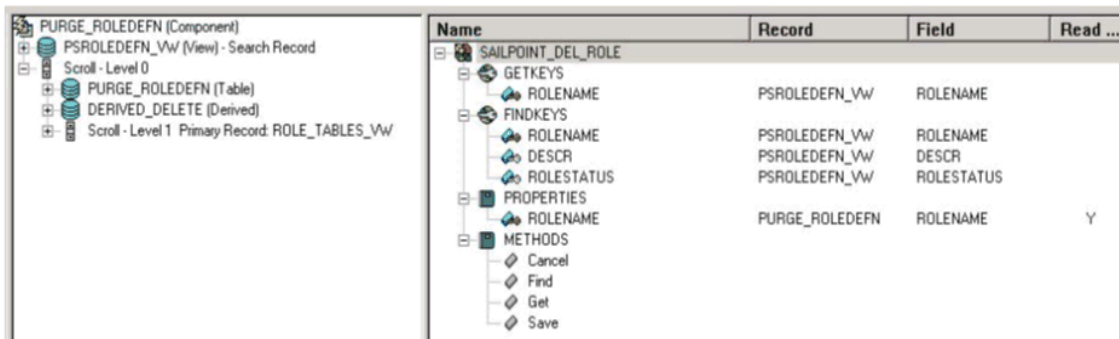


Basic structure of Component Interface (CI) from PURGE_ROLEDEFN component for Delete Role

This section describes the creation of basic structure of CI from Delete Role component. For example, **SAILPOINT_DEL_ROLE**

Creating CI

1. Log on to Application Designer and click on **File => New**.
A new dialog box named New Definition is displayed.
2. Select **Component Interface => OK**.
A new dialog box named Select Source Component for Component Interface is opened.
3. Enter the name as **PURGE_ROLEDEFN** under the **Selection Criteria** tab and click **Select**.
A dialog box appears with the following message:
Do you want to default the properties based on the underlying component definition
4. Click **Yes**.
Following screen shot appears:



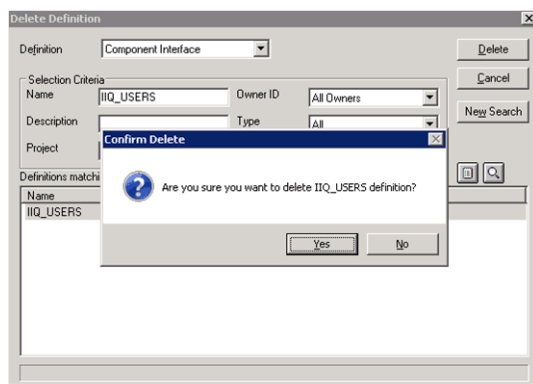
Deleting the component interface

5. Click on **File => Save As**.
A new dialog box appears requesting for the name of the CI.
6. Enter the name of the CI as **{NEW_NAME}**. For example, **SAILPOINT_DEL_ROLE**.
Delete the **ROLE_TABLES_VW** collective attribute.
7. Click **Save**.

Deleting the component interface

Perform the following procedure to delete the Component interface:

1. Open **Application Developer => Files => Delete**.
The Delete Definition window appears. as follows:



2. Select **Definition** as the name of the CI you want to delete and click on **Delete**.
The required Component Interface is deleted.

Appendix C: Connector Classloader

The Java classloader dynamically loads the Java classes into the Java Virtual Machine. While loading a class, all the corresponding dependencies are loaded. The classloader that loads a class is associated with that class. The classloader that loads a class, also loads all its dependencies and hence it is recommended that the same class must not be loaded by different Classloaders.

This appendix describes about two different version of same Connectors requiring different libraries.

To create two applications instances of a connector, where each instance is connecting to different type of target system or different version of target system which requires different set of third-party jars. This can be achieved by performing the following configurations with the help of Connector Classloader:

1. Create two separate directories under `WEB-INF/lib-connectors` directory with the specific versions or types of directories and add respective set of third-party libs to these directories.
2. Add the **connector-classpath** attribute to the application attribute map.

The following attribute application map displays the possibility of adding a single jar to Connector Classloader's classpath or by adding the directory location which would add all the jars under that to classpath:

```
<!-- IIQ filePathPrefix = Directory Path including /WEB-INF -->
<entry key="connector-classpath">
  <value>
    <List>
      <String>\lib-connectors\JDBCCustom\commons-codec-1.9.jar</String> <!--
path of single jar -->
      <String>\lib-connectors\ JDBCCustom \</String> <!-- path of folder, all
jars under the folder will be added to classpath -->
    </List>
  </value>
</entry>
```

For example, PeopleSoft Direct Connector's two instances can be created on the same IdentityIQ and both the instances are connecting to separate target systems.

Assuming that one application instance is connecting to 8.X and another to 7.X, create two separate directories under the `web-inf/lib-connectors` directory as follows:

- **PPLSFT7.0**
- **PPLSFT8.0**

Add the required set of libraries under the specific directories by adding the configuration to respective applications classpath as follows:

- **For PeopleSoft 7.0**

```
<!-- IIQ filePathPrefix = Directory Path including /WEB-INF -->
<entry key="connector-classpath">
  <value>
    <List>
      <String>\lib-connectors\PPLSFT7.0\</String>
```

```
        </List>
      </value>
    </entry>
```

- For PeopleSoft 8.0

```
<!-- IIQ filePathPrefix = Directory Path including /WEB-INF -->
<entry key="connector-classpath">
  <value>
    <List>
      <String>\lib-connectors\PPLSFT8.0\</String>
    </List>
  </value>
</entry>
```

Upgrade considerations

After upgrading IdentityIQ, custom connectors and customization rules can be impacted if connectors are initiated directly without using Connector Factory.

For example, `connector = ConnectorFactory.getConnector(application, null);`