



**SailPoint**

Version 7.3

# **Integration Guide**

**Copyright © 2018 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 © 2018 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,” “IdentityIQ,” “IdentityNow,” “AccessIQ,” “Identity Cube,” “Managing the Business of Identity” and the SailPoint logo are registered trademarks of SailPoint Technologies, Inc. “SecurityIQ,” “SailPoint,” “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

---

<b>Chapter 1: Overview</b>	<b>1</b>
What is SailPoint IdentityIQ?	1
SailPoint Integration Guide Overview	2
<b>Healthcare Integration Module</b>	<b>5</b>
<b>Chapter 2: SailPoint Epic Integration Module</b>	<b>7</b>
Overview	7
Important consideration	7
Supported features	8
Supported Managed System	8
Pre-requisites	8
Administrator permissions	9
Configuration parameters	9
Configuring WS-Security	10
Schema Attributes	11
Account attributes	11
Group attributes	15
Provisioning Policy attributes	16
Troubleshooting	19
<b>Chapter 3: SailPoint Cerner Integration Module</b>	<b>21</b>
Overview	21
Supported features	21
Pre-requisites	22
Configuration parameters	22
Additional configuration parameters	22
Schema attributes	23
Account attributes	23
Group attributes	24
Provisioning Policy attributes	24
Create Account	24
Update Account	25
Additional information	25
Troubleshooting	26
<b>IaaS Governance Modules</b>	<b>27</b>
<b>Chapter 4: SailPoint Amazon Web Services Governance Module</b>	<b>29</b>
Overview	29
Amazon Web Services Governance Module Setup 1.0	29
Supported features	29
Pre-requisites	31
Administrator permissions	32
Configuration parameters	34
Schema attributes	35
Provisioning Policy attributes	39
CloudTrail Logging Setup	40

Testing CloudTrail configurations .....	42
Federation Setup .....	42
Federation Server Setup .....	43
Additional information .....	44
Amazon Web Services Governance Module .....	44

## **Chapter 5: SailPoint SAP Governance Module .....51**

Overview .....	51
Supported features .....	51
Supported Managed Systems .....	53
Pre-requisites .....	53
Administrator permissions .....	53
Configuration parameters .....	57
Schema attributes .....	59
Account attributes .....	59
Group attributes .....	63
Schema extension and custom attributes .....	64
Upgrade considerations .....	65
Provisioning Policy attributes .....	65
Create account attributes .....	65
Additional information .....	65
Entitlement validity period .....	66
CUA support .....	66
Entitlement Data .....	66
Password Change .....	66
Logon and Communication Language attributes .....	67
Delta Aggregation .....	67
Partitioning Aggregation .....	70
Troubleshooting .....	70

## **Enterprise Resource Planning Integration Modules .....75**

## **Chapter 6: SailPoint Oracle E-Business Suite Integration Module .....77**

Overview .....	77
Supported features .....	77
Supported Managed Systems .....	78
Pre-requisites .....	78
Administrator permissions .....	78
Configuration parameters .....	81
Additional configuration parameter .....	83
Schema attributes .....	84
Account attributes .....	84
Group attributes .....	85
Provisioning Policy attributes .....	86
Create account attributes .....	86
Create group attributes .....	87
Additional information .....	87
Upgrade considerations .....	88
Support of provisioning of Start Date, End Date and Justification attributes .....	89
Troubleshooting .....	90

## **Chapter 7: SailPoint SAP Portal-User Management Web Service Integration Module**

### **91**

Overview .....	91
Supported features .....	92
Supported Managed Systems .....	92
Pre-requisite .....	92
Administrator permission .....	93
Configuration parameters .....	93
Schema attributes .....	94
Account attributes .....	94
Group attributes .....	95
Provisioning Policy attributes .....	95
Create account attributes .....	95
Create Group attributes .....	96
Additional information .....	97
Undeploy .sda file .....	97

## **Chapter 8: SailPoint PeopleSoft Integration Module .....**

### **99**

Overview .....	99
Supported features .....	99
Supported Managed Systems .....	100
Pre-requisites .....	100
Administrator permission .....	100
Configuration parameters .....	100
Schema attributes .....	102
Account attributes .....	102
Group attributes .....	103
Additional information .....	103
Creating the Component Interfaces .....	104
Partitioning Aggregation .....	104
Performance improvement .....	104
Creating the Component interface jar file .....	106
Configuring the Component Interface Security .....	107
Upgrade considerations .....	108
Troubleshooting .....	108

## **Chapter 9: SailPoint Siebel Integration Module .....**

### **111**

Overview .....	111
Supported features .....	111
Supported Managed Systems .....	112
Pre-requisites .....	112
Administrator permission .....	112
Configuration parameters .....	112
Schema attributes .....	114
Account attributes .....	114
Account Group attributes .....	114
Adding new custom attributes in schema .....	115
Provisioning policy attributes .....	115
Troubleshooting .....	116

## **Chapter 10: SailPoint NetSuite Integration Module .....**

### **117**

Overview .....	117
Supported features .....	117

Supported Managed Systems .....	118
Administrator permissions .....	118
Configuration parameters .....	118
Schema attributes .....	119
Account attributes .....	119
Group attributes .....	120
Schema extension and custom attributes .....	120
Provisioning Policy attributes .....	121
Additional information .....	122
NetSuite Application Program Interface (API) .....	122

## **Mainframe Integration Modules ..... 123**

### **Chapter 11: SailPoint RACF Integration Module ..... 125**

Overview .....	125
Supported features .....	125
Installing RACF Integration Module .....	125

### **Chapter 12: SailPoint CA-Top Secret Integration Module ..... 127**

Overview .....	127
Supported features .....	127
Installing CA-Top Secret Integration Module .....	127

### **Chapter 13: SailPoint CA-ACF2 Integration Module ..... 129**

Overview .....	129
Supported features .....	129
Installing CA-ACF2 Integration Module .....	129

### **Chapter 14: SailPoint RACF LDAP Integration Module ..... 131**

Overview .....	131
Supported features .....	131
Supported Managed Systems .....	132
Pre-requisites .....	132
Administrator permissions .....	133
Configuration parameters .....	133
Additional configuration parameter .....	134
Schema Attributes .....	134
Account attributes .....	134
Group attributes .....	136
Provisioning Policy Attributes .....	137
Additional information .....	138
Support for PassPhrase .....	138
Support for Connection Attributes .....	138
Implementing Secured Communication to RACF LDAP Server .....	138
Defining Search Scope .....	141
Troubleshooting .....	142

### **Chapter 15: SailPoint Top Secret LDAP Integration Module ..... 143**

Overview .....	143
Supported features .....	143
Supported Managed Systems .....	144
Administrator permissions .....	144
Configuration parameters .....	144

Schema Attributes .....	145
Account attributes .....	145
TopSecretProfile attributes .....	147
TopSecretGroup attributes .....	148
Provisioning Policy Attributes .....	148
Additional information .....	149
Support for PassPhrase .....	149
Implementing Secured Communication to Top Secret LDAP Server .....	149
Partitioning Aggregation .....	152

## **Service Desk Integration Modules ..... 155**

### **Chapter 16: SailPoint ServiceNow Service Integration Module ..... 157**

Overview .....	157
Supported features .....	157
Supported platforms .....	157
Pre-requisites .....	158
Service Request .....	158
Incident and Change Request .....	158
Basic configuration .....	159
Basic flow of Service Request .....	161
Basic configuration of Service Request .....	161
Configuring IdentityIQ to integrate with ServiceNow .....	162
IntegrationConfig XML files for Service Request, Incident and Change Request .....	165
Configuration procedure .....	166
Retryable mechanism .....	168
Sample scenario .....	168
Troubleshooting .....	169

### **Chapter 17: SailPoint HP Service Manager Service Integration Module ..... 173**

Overview .....	173
Supported features .....	173
Supported platforms .....	174
Pre-requisites .....	174
Configuring HP Service Manager for IdentityIQ Integration .....	177
Retryable mechanism .....	184
Additional information .....	184
Creating New Service Request Catalog Item .....	185
Exporting user details from HP Service Manager .....	185
Importing user details from HP Service Manager to IdentityIQ .....	185
Troubleshooting .....	186

### **Chapter 18: SailPoint BMC Remedy Service Desk Service Integration Module ... 189**

Overview .....	189
Supported features .....	189
Supported platforms .....	189
Pre-requisites .....	190
Basic configuration .....	190
Configuring BMC Remedy AR System for IdentityIQ Integration .....	191
Configuring IdentityIQ for BMC Remedy Action Request System Integration .....	193
BMC Remedy Action Request System Integration .....	193
Creating multiple tickets in Remedy System .....	197
Sample scenario .....	198

Troubleshooting .....	198
<b>GRC Integration Module .....</b>	<b>201</b>
<b>Chapter 19: SailPoint SAP GRC Integration Module .....</b>	<b>203</b>
Introduction .....	203
Supported features .....	204
<i>(Optional)</i> Support of additional feature .....	205
Supported platforms .....	205
Pre-requisites .....	205
SAP GRC Server Settings .....	205
SAP Connector changes for supporting SAP GRC integration .....	206
Creating IdentityIQ application of type SAP GRC .....	207
SAP GRC workflows .....	208
Minimum permissions required for SAP GRC user .....	211
Custom workflows provided for SAP GRC integration .....	212
SAP GRC Data Generator .....	212
SAP GRC Request Executor .....	213
Importing SAP GRC Application Rule .....	215
Viewing the reports .....	216
Upgrade considerations .....	216
Support proactive check and SAP CUA integration .....	216
Upgrade settings .....	216
Additional information .....	217
Creating a RFC Connection on SAP GRC system .....	217
Configuring cross system on SAP GRC .....	218
<i>(Optional)</i> Support for additional parameters .....	219
Support for provisioning start and end date for role assignment .....	221
Troubleshooting .....	222
<b>Service Management Integration Module (Service Catalog) .....</b>	<b>225</b>
<b>Chapter 20: SailPoint ServiceNow Service Catalog Integration .....</b>	<b>227</b>
Overview .....	227
Supported features .....	228
Supported platforms .....	229
Pre-requisites .....	229
Installation and configuration in ServiceNow .....	229
Installation .....	229
Configuration .....	231
Configuration in SailPoint IdentityIQ .....	233
Troubleshooting .....	233
<b>Chapter 21: SailPoint ServiceNow Service Catalog API Integration .....</b>	<b>235</b>
Overview .....	235
Supported features .....	236
Supported platforms .....	236
Pre-requisites .....	236
Installation and configuration in ServiceNow .....	236
Installation .....	236
Configuration .....	238
Configuration in SailPoint IdentityIQ .....	239
Status Maps .....	239



Troubleshooting .....	239
<b>Provisioning Integration Modules .....</b>	<b>241</b>
<b>Chapter 22: SailPoint Oracle Identity Manager Provisioning Integration Module</b>	<b>243</b>
Overview .....	243
Supported features .....	243
Supported platforms .....	244
Installing the OIM Integration Web Application .....	244
Authentication for Web Application .....	244
Testing the OIM Integration Web Application .....	245
Properties that can be defined in xellerate.properties .....	246
Configuration for OIM application .....	247
Testing the OIM Integration Client .....	247
Aggregating from OIM .....	248
Known/Open issues .....	248
<b>Chapter 23: SailPoint IBM Security Provisioning Integration Module .....</b>	<b>249</b>
Overview .....	249
Supported features .....	249
Supported platforms .....	249
General configuration .....	250
Configuration for Aggregation .....	250
Configuration for Provisioning .....	250
Troubleshooting .....	252
<b>Mobile Device Management Integration Modules .....</b>	<b>253</b>
<b>Chapter 24: SailPoint AirWatch Mobile Device Management Integration Module</b>	<b>255</b>
Overview .....	255
Supported features .....	255
Supported platforms .....	256
Pre-requisites .....	256
Configuration .....	256
Application configuration .....	257
Operation specific configuration .....	257
<b>Chapter 25: SailPoint MobileIron Mobile Device Management Integration Module ..</b>	<b>259</b>
Overview .....	259
Supported features .....	259
Supported platforms .....	260
Pre-requisites .....	260
Configuration .....	260
Application configuration .....	260
Operation specific configuration .....	261
<b>Chapter 26: SailPoint Good Technology Mobile Device Management Integration Mod- ule .....</b>	<b>263</b>
Overview .....	263
Supported features .....	263
Supported platform .....	264
Pre-requisites .....	264

Configuration .....	264
Application configuration .....	264
Operation specific configuration .....	265
<b>IT Security Integration Module .....</b>	<b>267</b>
<b>Chapter 27: SailPoint HP ArcSight Integration Module .....</b>	<b>269</b>
Overview .....	269
Common Event Format (CEF) .....	269
Supported features .....	270
Supported platforms .....	270
Pre-requisites .....	270
Configuration .....	270
Configuration to export IdentityIQ Data to ArcSight .....	270
Configuration to Import HP ArcSight CEF Flat File to SailPoint IdentityIQ .....	274
<b>Appendix .....</b>	<b>277</b>
<b>Appendix A: Common Identity Management Integration Configuration .....</b>	<b>279</b>
Overview .....	279
Creating the IntegrationConfig Object .....	279
Provisioning .....	284
<b>Appendix B: Component Interface .....</b>	<b>287</b>
Creating component interface for PeopleSoft .....	287
Basic structure of Custom Component (CI) from USERMAINT component for Users .....	287
Basic structure of Custom Component (CI) from ROLEMAINT component for Roles .....	293
Basic structure of Custom Component (CI) from RTE_CNTL_PROFILE component for Users .....	295
Basic structure of Custom Component (CI) from PURGE_USR_PROFILE component for Delete User .....	298
Basic structure of Component Interface (CI) from PURGE_ROLEDEFN component for Delete Role .....	300
Deleting the component interface .....	301

# 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:

- **"Healthcare Integration Module"**
  - SailPoint Epic Integration Module
  - SailPoint Cerner Integration Module
- **"IaaS Governance Modules"**
  - SailPoint Amazon Web Services Governance Module
  - SailPoint SAP Governance Module
- **"Enterprise Resource Planning Integration Modules"**
  - SailPoint Oracle E-Business Suite Integration Module
  - SailPoint SAP Portal-User Management Web Service Integration Module
  - SailPoint PeopleSoft Integration Module
  - SailPoint Siebel Integration Module
  - SailPoint NetSuite Integration Module
- **"Mainframe Integration Modules"**
  - SailPoint RACF Integration Module
  - SailPoint CA - Top Secret Integration Module
  - SailPoint CA - ACF2 Integration Module
  - SailPoint RACF LDAP Integration Module
  - SailPoint Top Secret LDAP Integration Module

- **“Service Desk Integration Modules”**
  - SailPoint ServiceNow Service Integration Module
  - SailPoint HP Service Manager Service Integration Module
  - SailPoint BMC Remedy Service Desk Service Integration Module
- **“GRC Integration Module”**
  - SailPoint SAP GRC Integration Module
- **“Service Management Integration Module (Service Catalog)”**
  - SailPoint ServiceNow Service Catalog Integration
  - SailPoint ServiceNow Service Catalog API Integration
- **“Provisioning Integration Modules”**
  - SailPoint Oracle Identity Manager Provisioning Integration Module
  - SailPoint IBM Security Provisioning Integration Module
- **“Mobile Device Management Integration Modules”**
  - SailPoint AirWatch Mobile Device Management Integration Module
  - SailPoint MobileIron Mobile Device Management Integration Module
  - SailPoint Good Technology Mobile Device Management Integration Module
- **“IT Security Integration Module”**
  - SailPoint HP ArcSight Integration Module

This document is intended for the above products and IdentityIQ System Administrators and assumes a high degree of technical knowledge.



# Healthcare Integration Module

This section contains information on the following section:

- "SailPoint Epic Integration Module" on page 7
- "SailPoint Cerner Integration Module" on page 21

**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 2: SailPoint Epic Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	7
Important consideration . . . . .	7
Supported features . . . . .	8
Supported Managed System . . . . .	8
Pre-requisites . . . . .	8
Administrator permissions . . . . .	9
Configuration parameters . . . . .	9
Configuring WS-Security . . . . .	10
Schema Attributes . . . . .	11
Account attributes . . . . .	11
Group attributes . . . . .	15
Provisioning Policy attributes . . . . .	16
Troubleshooting . . . . .	19

## 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

SailPoint Epic Integration Module supports managing Epic accounts (EMP records), linked templates, linked sub-templates, InBasketClassifications and LoginDepartmentFilterList.

## Important consideration

---

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
- the Epic connector uses Core Binding and Personnel Management 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 SailPoint Healthcare Integration Module.

## Supported features

---

SailPoint Epic Integration Module supports the following features:

- Account Management
  - Manage Epic EMP records as Accounts
  - Aggregation, Partitioning Aggregation, Refresh Account
  - Create, Update, Delete
  - Enable, Disable, Unlock, Change Password
  - 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

---

SailPoint Epic Integration Module supports Epic version 2018, 2017, 2015 and 2014.

## Pre-requisites

---

- **Epic Web Services:** Epic provides SOAP based Web-Services for connecting to various API's. All communication with the Epic Interconnect server should be done via these API's. For Epic Integration Module 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.

The **Core** and **Personnel Management** 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](http://[epic-webservices-server-name]/[epic-instancename]/StatusPage/Main.aspx)

For example, [http://example-epic-websrvr.acme.com/Interconnect-TST\\_POC2014/StatusPage/Main.aspx](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 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 and Personnel Management Web Service can be secured using WS-Security. The Epic Integration Module supports Username token based WS-Security for Core and Personnel Management 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 SailPoint Epic Integration Module, 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.

The Epic Integration Module uses the following connection attributes:

Attribute	Description
<b>Epic Connection Settings</b>	
Epic URL*	The host URL of Epic instance.
Username*	Specifies the administrator or the unique ID of the user which has administrative level privileges to perform aggregation and provisioning operation on Epic system.
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.
<b>WS-Security Settings</b>	
Enable WS-Security for Core Binding	Checkbox to enable WS-Security for Core Binding with Username token.
Username*	Enter Core Binding WS-Security Username.

## Configuration parameters

Attribute	Description
Password*	Enter Core Binding WS-Security Password.
Enable WS-Security for Personnel Management	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.

## Configuring WS-Security

Epic Connector uses the following methods for enabling the WS-Security:

- Core Binding
- Personnel Management

**Note:** When enabling WS-Security for Core Binding and Personnel Management, the WS-Security account must be configured for the Interconnect Web Service and need not be within the Epic application (EMP Record).

### Core Binding

To enable WS-Security for Core Binding, perform the following.

1. Ensure that the Enable WS-Security for Core Binding checkbox is selected.
2. Enter valid Username and Password.

### Personnel Management

EPIC Connector uses Apache Rampart module to implement WS-Security.

To enable WS-Security for Personnel Management, perform the following:

1. Ensure that the **Enable WS-Security for Personnel Management** checkbox is selected.
2. Enter valid **Username** and **Password**.
3. Copy the **sailpoint\_epic\_connector\_axis2.xml** file from `integration\EPIC` folder to the `\WEB-INF\classes` directory.
4. 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-ut
ility-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/IncludeTok
en/AlwaysToRecipient" />
```

```

    </wsp:Policy>
  </sp:SupportingTokens>
  </wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>

```

## Schema Attributes

---

This section describes the different schema attributes.

### Account attributes

---

The following table lists the account 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	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	An NPI (National Provider Identifier), a pointer to the user's operating system login, or another ID created by third party.	Provider ID	17500

## Schema Attributes

Attribute Name	Description	Epic Name	Epic Item Number
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
AuthenticationConfiguration ID	A non-native authentication method (for example, LDAP) used to authenticate when user logs into Epic.	Authentication Record	48
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

Attribute Name	Description	Epic Name	Epic Item Number
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 <b>contact</b> for the User, meaning that previous values would be retained.		
EmployeeDemographics	This parameter is used to provide certain specific information about the user.		
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"><li><b>Yes:</b> the spouse's last name would appear first in the hyphenated last name</li><li><b>No</b></li></ul>		

## Schema Attributes

Attribute Name	Description	Epic Name	Epic Item Number
UserComplexName_Spouse Prefix	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.		
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.		



Attribute Name	Description	Epic Name	Epic Item Number
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.		
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**

## Group attributes

The following table lists the Group attributes:

Attribute name	Description
<b>Linked template attributes</b>	
LinkedTemplateID	The ID of the LinkedTemplate.
LinkedTemplateName	Name of the LinkedTemplate.
<b>Linked Subtemplates attributes</b>	
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.
<b>InBasketClassifications attributes</b>	
Number	ID of the InBasketClassifications.

## Provisioning Policy attributes

Attribute name	Description
Title	Description of the InBasketClassifications.
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, <b>INITIAL DEPARTMENT</b>
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.

Attribute name	Description
CustomUserDictionary_value_0	The string being stored at the indexed position.
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 <b>EmployeeDemographics</b> . 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
<b>Optional attributes</b>	
<i>After upgrading to IdentityIQ version 7.3, 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.

## Provisioning Policy attributes

Attribute name	Description
BlockReason	Reason why the user account is blocked.
BlockComment	Text comment about why the user is blocked. Maximum allowed length is 100 characters.

### 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 Epic Integration Module

When performing any operation, not able to generate SOAP Envelope logging in Epic Integration Module.

## Troubleshooting

**Resolution:** To enable advanced SOAP Envelope logging in Epic Integration Module 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 and WS-Security is enabled for EPIC connector, Test Connection fails with an error

When upgrading IdentityIQ to version 7.3 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.

# Chapter 3: SailPoint Cerner Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	21
Supported features . . . . .	21
Pre-requisites . . . . .	22
Configuration parameters . . . . .	22
Schema attributes . . . . .	23
Account attributes . . . . .	23
Group attributes . . . . .	24
Provisioning Policy attributes . . . . .	24
Additional information . . . . .	25
Troubleshooting . . . . .	26

## 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 SailPoint Cerner Integration Module is designed to provide automated way of provisioning through SailPoint IdentityIQ solution.

### Supported features

---

SailPoint Cerner Integration Module 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.
- For accessing provisioning adaptor, the target ID of the millennium and millennium domain is required.
- Permissions given to TargetID in Cerner millennium:

The Cerner provisioning adaptor 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://&lt;hostName&gt;/security-provisioning/ProvisioningServlet">http://&lt;hostName&gt;/security-provisioning/ProvisioningServlet</a>
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, " <b>millennium_XXXXXX</b> "
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"> <li>• True (LDAP user)</li> <li>• False (non-LDAP user)</li> </ul> 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.

## Provisioning Policy attributes

**Table 1—Account attributes (Continued)**

Attributes	Description
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 1—Account 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.

## Additional information

This section describes the additional information related to the Cerner Integration Module.

- **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
```

# 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**.

# IaaS Governance Modules

This section contains information on the following section:

- "SailPoint Amazon Web Services Governance Module" on page 29
- "SailPoint SAP Governance Module" on page 51



# Chapter 4: SailPoint Amazon Web Services Governance Module

---

The following topics are discussed in this chapter:

Amazon Web Services Governance Module Setup 1.0 .....	29
Supported features .....	29
Pre-requisites .....	31
Administrator permissions .....	32
Configuration parameters .....	34
Schema attributes .....	35
Provisioning Policy attributes .....	39
CloudTrail Logging Setup .....	40
Federation Setup .....	42
Additional information .....	44
Amazon Web Services Governance Module .....	44

## Overview

---

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. Amazon Web Services Governance Module 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.

## Amazon Web Services Governance Module Setup 1.0

---

The AWS Governance Module uses the AWS STS (Security Token Service) to setup cross-account access between AWS accounts.

### Supported features

---

SailPoint Amazon Web Services Governance Module 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

## Amazon Web Services Governance Module Setup 1.0

- 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 44.

- **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



Object Type	IdentityIQ Type	Aggregation	Re-fresh	Create	Update	Delete	Request-able	User Status
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 Id’s.
  - 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 44.

**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.

The following table lists the examples of policies for the respective policy names:

Policy Name	Policy Document
<b>For AWS Service IAM User</b>	
SPServiceAccount	<pre>{   "Version": "2012-10-17",   "Statement": [     {       "Sid": "VisualEditor0",       "Effect": "Allow",       "Action": [         "iam:GetUser",         "sts:AssumeRole"       ],       "Resource": "*"     }   ] }</pre>
<b>For Role</b>	
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"       ],       "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 45.

## 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>&lt;entry key="assumeRoleDurationInSeconds" value="3600" /&gt;</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>&lt;entry key="assumeRoleSessionName" value="SailPointUser" /&gt;</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.

## Group schema

The following table lists the group schema:

Attributes	Type	Description
<b>Object Type: Group</b>		
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.
CustomerManagedPolicies	CustomerManagedPolicy	Customer Managed Policies directly assigned to the group.
InlinePolicies	InlinePolicy	Inline Policies directly assigned to the group.

Attributes	Type	Description
<b>Object Type: AWSManagedPolicy</b>		
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.
<b>Object Type: Customer Managed Policy</b>		
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.
<b>Object Type: InlinePolicy</b>		
Name	String	The friendly name of the policy.
Id	String	The unique ID of the policy.
PolicyJSON	String	The JSON document for the policy.
<b>Object Type: Role</b>		
RoleName	String	The friendly name of the role.
RoleId	String	The unique ID of the role.
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.

Attributes	Type	Description
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.
<b>Object Type: SCP</b>		
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.
<b>Object Type: AWSAccount</b>		
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.
<b>Object Type: OrganizationUnit</b>		
OUPName	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.
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 Id*	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 <b>IAMUserChangePassword</b> policy to allow them to change their own password.
Programmatic Access	Create programmatic access for the IAM user.
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 th recent HTTPS credential.

### Group

- **Create:** The following table lists the attributes that are required for creating a group and customer managed policy.

Name	Description
<b>Group</b>	
Group Name*	Enter the group name for IAM group.
AWS Account Id*	Enter the Account Id or ARN of the AWS account under which the IAM user is to be created.
Path	Specify the path to the IAM group.
<b>CustomerManagedPolicy</b>	
Policy Name*	Enter the policy name.

## CloudTrail Logging Setup

Name	Description
AWS Account Id*	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
<b>UpdateGroup</b>	
Group Name	Enter the group name for the IAM group.
AWS Account Id	Enter the Account Id or ARN of the AWS account under which the IAM user is to be created.
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.
<b>UpdateRole</b>	
Role Name	Role name for the IAM role.
AWS Account Id	Enter the Account Id or ARN of the AWS account under which the IAM user is to be created.
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.

## CloudTrail Logging Setup

The AWS Governance Module has an optional feature that monitors AWS API Access Events and collects log information about individual policy access. This helps to make informed decisions when viewing entitlement

access in IdentityIQ. for this feature to work it requires enabling AWS CloudTrail in all AWS Accounts to be monitored.

**Note:** The CloudTrail templates provided can be modified by the AWS System Administrator as required.

1. Expand the AWS Governance Module plugin zip file and navigate to the **AWS** folder.
2. Copy the **cloudtrail.mainaccount.template.json** file and modify it if required.
3. Login to the AWS Account which would be used as a **logging hub**. This account would centralize all CloudTrail logging data from all accounts to one S3 bucket. This S3 bucket would contain sensitive information, hence it is recommended that the AWS Administrator reviews all permissions and scripts.
4. From the AWS Management Console, navigate to **CloudFormation** and **Create Stack** as follows:
  - a. Under **Choose a template** select the modified **cloudtrail.mainaccount.template.json** file from Step <\$elemparamonly2.
  - b. Under **Specify Details** add the following:
    - Select a stack name
    - Select a unique bucket name for the logs to be stored in
    - Select if global events are to be logged or no.
    - Select a SNS topic name where log file notification events would be sent
  - c. Run the stack.
5. If the stack deploys without errors, navigate to **SQS** from the AWS Management Console and perform the following:
  - a. Click on the **SailPointAssumeRoleQueue** and save the URL for later use.  
For example, <https://sqs.us-east-2.amazonaws.com/555555555/SailPointAssumeRoleQueue>
  - b. Navigate to the **Permissions** tab and ensure that there are permissions for the following:
    - permission that allows the SNS topic to post to the queue
    - permission that allows the AWS Governance Module user to read from the queue

**Note:** Modify the permissions as required by the organization.

1 SQS Queue selected

Effect	Principals	Actions	Conditions
Allow	• Everybody (*)	• sqs:SendMessage	• ArnEquals • aws:SourceArn: "arn:aws:sns:us-east-2:65-443:SailPointRoleAssumptionAudit"
Allow	• arn:aws:iam::65-443:root	• sqs:GetQueueAttributes • sqs:GetQueueList • sqs:ReceiveMessage	None

6. Add the following policy to the AWS Governance Module user profile:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
```

## Federation Setup

```
        "s3:List*",
        "s3:Get*"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
```

This policy would allow the AWS Governance Module to read the logging S3 bucket and receive SQS messages. The AWS Administrator can modify this policy to restrict the resources to be accessed.

7. Login to each account the organization wants to monitor and add a new CloudTrail service if it does not exist.
  - a. In the Trail configuration enter the SNS topic and S3 bucket from the global account setup in Step <\$elemparanumonly4 as follows:
  - b. All logging from this account would be forwarded to the S3 bucket and SNS topic in the central logging account.
  - c. Repeat this for each account the organization would want to monitor.

**Note:** Step c above can also be performed using CloudFormation and Stack Sets. AWS Administrator can help to automate this process.

8. Login to IdentityIQ and navigate to the plugin setup page and perform the following:
  - a. Click **Configure** on the AWS Governance Plugin.
  - b. Enter the application name for the AWS Governance Module setup in the “Amazon Web Services Governance Module Setup 1.0” on page 29.
  - c. Enter the AWS region, S3 bucket and SQS Queue that exist from Step <\$elemparanumonly4.
  - d. Enter the SQS URL noted from Step <\$elemparanumonly 5.
  - e. Change the value of **Enable AWS Cloud Trail Watcher** to **True**.

The CloudTrail monitoring is now enabled. Monitor the IdentityIQ log for errors. If errors are present, then it is due to improper configuration of permissions or incorrect login information from the AWS Governance Module configuration.

## Testing CloudTrail configurations

---

To test the CloudTrail configurations, login to AWS and perform an action with a user that has a policy with conditions present.

1. Wait ten minutes for the CloudTrail logging data to propagate.
2. Login to IdentityIQ and navigate to the Identity Warehouse and then the AWS IAM user.
3. Click on the user and navigate to AWS entitlement that has conditional policy.
4. Click on the **AWS** tab and navigate to the permission exercised (a user that has policy with conditions).
5. The user must view the CloudTrail data in the UI.

## Federation Setup

---

The AWS Governance Module allows an organization to map their AWS federated users to an IdentityIQ Governance Role which tracks what AWS roles a user has access to and what underlying entitlement grants access to said role. Most of the time the underlying entitlement is a group from an Enterprise Directory such as Active Directory.

1. After the AWS Governance Module Plugin is installed navigate to the IdentityIQ Tasks page.
2. Click on the **AWS Federation Role Sync** task.
  - a. Select the AWS Application name configured in the environment.
  - b. Select the Enterprise Directory Application used by your AWS federation solution.
  - c. If the organization follows a naming convention for group names that map to AWS Roles, enter the **regEx** pattern for said naming convention.  
  
 For example, **aws(.+ )role(.+ )** would parse all groups with names like **aws00000000roleFederationAdminAccess**  
  
 Where **00000000** is the AWS account number that contains the role and **FederationAdminAccess** is the role name.  
  
**Note:** **SailPoint recommends following the above mentioned naming convention as it simplifies the federation servers claims configuration.**
  - d. If the organization has complex claim rules or legacy configuration, a mapping can be defined between AWS Roles and directory groups.
  - e. Under **Federation Role Mapping** select the AWS Role and directory entitlement that grants access to said role and click **Add**.
3. Save and Execute the task.
4. Navigate to the Role page in IdentityIQ.
5. The user must be able to view several roles under **AWS Federation Roles** that represent all AWS federation roles defined in the **AWS Federation Role Sync**.

**Note:** **SailPoint recommends to periodically run this task in a Sequential task executor following Enterprise Directory and AWS aggregation.**

## Federation Server Setup

---

During Federation Server configuration ensure that the federated user sessions can be correlated back to identities in IdentityIQ. When configuring the **Relying Party Trusts** claim rules for AWS.

AWS requires the following attributes in the claim.

- **Named:** It is recommended that the Named is set to the native identity display name or native identity attribute configured in the IdentityIQ Enterprise Directory (Active Directory) Connector configuration. This allows IdentityIQ to correlate a federated user back to a IdentityIQ identity. Following is an example for claim rule for Active Directory Federation Server:  

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");
```
- **RoleSessionName:** In the AWS documentation, it is recommended that the user name must be used as the RoleSessionName. However, in order to tie API access events to a particular user session the RoleSessionName must be unique per session. It is recommended to concatenate a nonce or unique value to the end of the RoleSessionName. Following is an example for Active Directory Federation Server:

## Additional information

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",  
Issuer == "AD AUTHORITY"]  
&& c1:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant"]  
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/RoleSessionName", Value  
= RegExReplace(c.Value, "[\\]+", "-") + "-" + RegExReplace(c1.Value, "[:]+",  
"-"));
```

## Additional information

---

This section describes the additional information related to the AWS Governance Module setup.

### Amazon Web Services Governance Module

---

#### IAM User Status

Following are the IdentityIQ operations with the corresponding IAM User Status:

- **Enable**
  - Set Console Password
  - Activate Last Created Access Keys
  - Activate Last CreatedAWS CodeCommit HTTPS Credentials
  - Activate Last CreatedAWS CodeCommit SSH Keys
- **Disable**
  - Deletes Console Password
  - Inactive Both Access Keys
  - Inactive Both AWS CodeCommit HTTPS Credentials
  - Inactive All AWS CodeCommit SSH Keys

#### 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::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"> <li>• UpdateLoginProfile</li> <li>• CreateLoginProfile</li> </ul>
Group Create	CreateGroup
Group Update	<ul style="list-style-type: none"> <li>• UpdateGroup</li> <li>• AttachGroupPolicy</li> <li>• DetachGroupPolicy</li> </ul>
Create Customer Managed Policy	CreatePolicy
<b>Account Aggregation</b>	
<ul style="list-style-type: none"> <li>• Summary/Attributes (UserName, UserId, Path, ARN, CreateDate)</li> <li>• ConsoleAccess</li> <li>• Groups</li> <li>• AWSManagedPolicies and Custom-erManagedPolicies</li> <li>• InlinePolicies</li> <li>• Access Keys</li> <li>• AWS CodeCommit HTTPS Creden-tials</li> <li>• AWS CodeCommit SSH Keys</li> <li>• Signing Certificates</li> <li>• Multi-Factor Authentication (MFA) Device</li> </ul>	<ul style="list-style-type: none"> <li>• ListUsers</li> <li>• GetLoginProfile</li> <li>• ListGroupsForUser</li> <li>• ListUserPolicies</li> <li>• ListAttachedUserPolicies</li> <li>• ListAccessKeys</li> <li>• ListServiceSpecificCredentials</li> <li>• ListSSHPublicKeys</li> <li>• ListSigningCertificates</li> <li>• ListMFADevices</li> </ul>
<b>Account-Group Aggregation (Group)</b>	

## Additional information

IdentityIQ operation	IAM API (Action)
<ul style="list-style-type: none"> <li>Summary/Attributes (GroupName, GroupId, Path, ARN, CreateDate)</li> <li>AWSManagedPolicies and CustomerManagedPolicies</li> <li>InlinePolicies</li> </ul>	<ul style="list-style-type: none"> <li>ListGroups</li> <li>ListAttachedGroupPolicies</li> <li>ListGroupPolicies</li> </ul>
<b>Account-Group Aggregation (AWSManagedPolicy and CustomerManagedPolicy)</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (PolicyName, PolicyId, ARN, Path, CreateDate, UpdateDate, DefaultVersionId)</li> <li>Description</li> <li>PolicyJSON</li> </ul>	<ul style="list-style-type: none"> <li>ListPolicies</li> <li>GetPolicy</li> <li>GetPolicyVersion</li> </ul>
<b>Account-Group Aggregation (Role)</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (RoleName, RoleId, Path, ARN, Description, CreateDate, TrustPolicyJSON, MaxSessionDuration)</li> <li>AWSManagedPolicies and CustomerManagedPolicies</li> <li>InlinePolicies</li> </ul>	<ul style="list-style-type: none"> <li>ListRoles</li> <li>ListAttachedRolePolicies</li> <li>ListRolePolicies</li> </ul>
<b>Account-Group Aggregation (InlinePolicy)</b>	
<ul style="list-style-type: none"> <li>Id</li> <li>Name</li> <li>PolicyJSON</li> </ul>	<ul style="list-style-type: none"> <li>No API is called for this attribute, it is formatted as: <b>ARN of the entity:InlinePolicy:InlinePolicyName</b></li> <li>ListUserPolicies, ListGroupPolicies, ListRolePolicies</li> <li>GetUserPolicies, GetGroupPolicies, GetRolePolicies</li> </ul>
<b>Account Refresh</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (UserName, UserId, Path, ARN, CreateDate)</li> <li>Groups</li> <li>Access Keys</li> <li>Signing Certificates</li> <li>Password</li> <li>MFA Device</li> <li>AWS CodeCommit HTTPS Credentials and AWS CodeCommit SSH Keys: ListServiceSpecificCredentials</li> </ul>	<ul style="list-style-type: none"> <li>GetUser</li> <li>ListGroupsForUser</li> <li>ListAccessKeys</li> <li>ListSigningCertificates</li> <li>GetLoginProfile</li> <li>ListMFADevices</li> <li>ListServiceSpecificCredentials</li> </ul>



IdentityIQ operation	IAM API (Action)
<b>Refresh Operations</b>	
<ul style="list-style-type: none"> <li>• Refresh Group</li> <li>• Refresh Role</li> <li>• Refresh AWSManagedPolicy and CustomerManagedPolicy</li> <li>• Refresh Inline Policy associated with User</li> <li>• Refresh Inline Policy associated with Group</li> <li>• Refresh Inline Policy associated with Role</li> </ul>	<ul style="list-style-type: none"> <li>• GetGroup</li> <li>• GetRole</li> <li>• GetPolicy</li> <li>• GetUserPolicies</li> <li>• GetGroupPolicies</li> <li>• GetRolePolicies</li> </ul>
<b>Account Delete</b>	
<ul style="list-style-type: none"> <li>• Read Groups</li> <li>• Remove Groups</li> <li>• Read AWSManagedPolicy and CustomerManagedPolicy</li> <li>• Remove AWSManagedPolicy and CustomerManagedPolicy</li> <li>• Read InlinePolicy</li> <li>• Read Security Credentials <ul style="list-style-type: none"> <li>- Access Keys</li> <li>- Signing Certificates</li> <li>- Password</li> <li>- MFA Device</li> <li>- AWS CodeCommit HTTPS Credentials</li> <li>- AWS CodeCommit SSH Keys</li> </ul> </li> <li>• Remove Security Credentials <ul style="list-style-type: none"> <li>- Access Keys</li> <li>- Signing Certificates</li> <li>- Password</li> <li>- MFA Device</li> <li>- AWS CodeCommit HTTPS Credentials</li> <li>- AWS CodeCommit SSH Keys</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• DeleteUser</li> <li>• ListGroupsForUser</li> <li>• RemoveUserFromGroup</li> <li>• ListAttachedUserPolicies</li> <li>• DetachUserPolicy</li> <li>• ListUserPolicies</li> <li>• DeleteUserPolicy</li> <li>• ListAccessKeys</li> <li>• ListSigningCertificates</li> <li>• GetLoginProfile</li> <li>• ListMFADevices</li> <li>• ListServiceSpecificCredentials</li> <li>• ListSSHPublicKeys</li> <li>• DeleteAccessKey</li> <li>• DeleteSigningCertificate</li> <li>• DeleteLoginProfile</li> <li>• DeactivateMFADevice</li> <li>• DeleteServiceSpecificCredential</li> <li>• DeleteSSHPublicKey</li> </ul>
<b>Group Delete</b>	
<ul style="list-style-type: none"> <li>• Read Accounts in the Group</li> <li>• Remove Accounts from the Group</li> <li>• Read Group Policies</li> <li>• Remove Group Policies</li> </ul>	<ul style="list-style-type: none"> <li>• DeleteGroup</li> <li>• GetGroup</li> <li>• RemoveUserFromGroup</li> <li>• ListGroupPolicies</li> <li>• DeleteGroupPolicy</li> </ul>

## Additional information

IdentityIQ operation	IAM API (Action)
<b>Account Enable</b>	
<ul style="list-style-type: none"> <li>Set Password</li> <li>Activate Access Keys (Last created one)</li> <li>Activate AWS CodeCommit HTTPS Credentials (Last created one)</li> <li>Activate AWS CodeCommit SSH Keys (Last created one)</li> </ul>	<ul style="list-style-type: none"> <li>UpdateLoginProfile</li> <li>UpdateAccessKey</li> <li>UpdateServiceSpecificCredential</li> <li>UpdateSSHPublicKey</li> </ul>
<b>Account Disable</b>	
<ul style="list-style-type: none"> <li>Delete Password</li> <li>Deactivate Access Keys (All)</li> <li>Deactivate AWS CodeCommit HTTPS Credentials (All)</li> <li>Deactivate AWS CodeCommit SSH Keys (All)</li> </ul>	<ul style="list-style-type: none"> <li>DeleteLoginProfile</li> <li>UpdateAccessKey</li> <li>UpdateServiceSpecificCredential</li> <li>UpdateSSHPublicKey</li> </ul>
<b>Request Entitlement (Group and Managed Policies for User)</b>	
<ul style="list-style-type: none"> <li>Add group to user</li> <li>Add AWSManagedPolicy and CustomerManagedPolicy to user</li> </ul>	<ul style="list-style-type: none"> <li>AddUserToGroup</li> <li>AttachUserPolicy</li> </ul>
<b>Remove Entitlement (Group, Managed Policies, Inline Policies from User)</b>	
<ul style="list-style-type: none"> <li>Remove group from user</li> <li>Remove AWSManagedPolicy and CustomerManagedPolicy from user</li> <li>Remove Inline Policy from user</li> </ul>	<ul style="list-style-type: none"> <li>RemoveUserFromGroup</li> <li>DetachUserPolicy</li> <li>DeleteUserPolicy</li> </ul>
<b>Remove Inline Policy</b>	
<ul style="list-style-type: none"> <li>Read from User</li> <li>Delete from User</li> <li>Read from Group</li> <li>Delete from Group</li> <li>Read Role</li> <li>Delete from Role</li> </ul>	<ul style="list-style-type: none"> <li>GetUserPolicies</li> <li>DeleteUserPolicy</li> <li>GetGroupPolicies</li> <li>DeleteGroupPolicy</li> <li>GetRolePolicies</li> <li>DeleteRolePolicy</li> </ul>
<b>Update Role</b>	
<ul style="list-style-type: none"> <li>Attach AWSManagedPolicy and CustomerManagedPolicy</li> <li>Remove AWSManagedPolicy and CustomerManagedPolicy</li> </ul>	<ul style="list-style-type: none"> <li>AttachRolePolicy</li> <li>DetachRolePolicy</li> </ul>

### 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): <b>organizations:ListAccounts</b>

IdentityIQ operations	Organizations API (Actions)
<b>Account-Group Aggregation (OrganizationUnit)</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (OUName, OUIId, ARN, Parent)</li> <li>ServiceControlPolicies</li> <li>AWSAccounts</li> </ul>	<ul style="list-style-type: none"> <li>ListRoots, ListOrganizationalUnitsForParent</li> <li>ListPoliciesForTarget</li> <li>ListAccountsForParent</li> </ul>
<b>Account-Group Aggregation (SCP)</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (SCPName, SCPId, ARN, Description, AWSManaged)</li> <li>PolicyJSON</li> </ul>	<ul style="list-style-type: none"> <li>ListPolicies</li> <li>DescribePolicy</li> </ul>
<b>Account-Group Aggregation (AWSAccount)</b>	
<ul style="list-style-type: none"> <li>Summary/Attributes (AWSAccountName, AWSAccountId, ARN, EmailId, Status, JoinedType, JoinedTimestamp)</li> <li>OrganizationUnit</li> </ul>	<ul style="list-style-type: none"> <li>ListAccounts</li> <li>ListRoots, ListParents, DescribeOrganizationalUnit</li> </ul>
<b>Get Operations</b>	
<ul style="list-style-type: none"> <li>SCP</li> <li>AWS Accounts</li> <li>Organizational Unit</li> </ul>	<ul style="list-style-type: none"> <li>DescribePolicy</li> <li>DescribeAccount, ListRoots, ListParents, DescribeOrganizationalUnit</li> <li>DescribeOrganizationalUnit, ListRoots, ListParents, ListPoliciesForTarget, ListAccountsForParent</li> </ul>

## **Additional information**

# Chapter 5: SailPoint SAP Governance Module

---

The following topics are discussed in this chapter:

Overview . . . . .	51
Supported features . . . . .	51
Supported Managed Systems . . . . .	53
Pre-requisites . . . . .	53
Administrator permissions . . . . .	53
Configuration parameters . . . . .	57
Schema attributes . . . . .	59
Account attributes . . . . .	59
Group attributes . . . . .	63
Schema extension and custom attributes . . . . .	64
Upgrade considerations . . . . .	65
Provisioning Policy attributes . . . . .	65
Create account attributes . . . . .	65
Additional information . . . . .	65
Entitlement validity period . . . . .	66
CUA support . . . . .	66
Entitlement Data . . . . .	66
Password Change . . . . .	66
Logon and Communication Language attributes . . . . .	67
Delta Aggregation . . . . .	67
Partitioning Aggregation . . . . .	70
Troubleshooting . . . . .	70

## Overview

---

SAP Enterprise Resource Planning software solution is an integrated software solution that incorporates the key business functions of the organization.

The SAP Governance Module aggregates and provisions all the users along with their roles/profiles of the SAP system.

SailPoint SAP Governance Module supports provisioning to a standalone SAP system as well as SAP Central User Administration (CUA) system.

## Supported features

---

SailPoint SAP Governance Module 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 65.

- 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	SAP Governance Module aggregates Generated Profile associated to Role as a part of Account-Group Aggregation.
Change Password	<ul style="list-style-type: none"><li>• 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).</li><li>• 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"><li>- The log on session during which a productive password is set must be secured using Secure Network Communications (SNC).</li><li>- The user needs an additional authorization to set a productive password (authorization object: S_USER_GRP, activity: 'PP' - Set Productive)</li></ul></li></ul> <p>For more information, see SAP note <a href="https://service.sap.com/sap/support/notes/1287410">https://service.sap.com/sap/support/notes/1287410</a> (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 SAP_NEW contains a single profile SAP_NEW_<rel>, (for example, SAP_NEW_21D). This profiles holds its release status. Profiles like SAP_NEW_<rel> may not be aggregated.
Account - Group Aggregation	In Account-Group aggregation for SAP CUA landscape, SAP Governance Module 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

SailPoint SAP Governance Module 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

SailPoint SAP Governance Module supports the following modules of managed systems:

- SAP HR/HCM module
- SAP S/4HANA on-premise

**Note:** SailPoint SAP Governance Module manages ABAP users. For more information, see "Supported features" on page 51.

## 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 Governance 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
Account Aggregation	Test Connection and Account Aggregation  <b>Note:</b> For Account Aggregation of CUA systems, additional permissions must be executed as specified in the "Account Aggregation" section.

**Table 1— Operation specific required permissions**

Operation	Required permissions
Group Aggregation	Test Connection and Group Aggregation  <b>Note: For Group Aggregation of CUA systems, additional permissions must be executed as specified in the “ Group Aggregation” section.</b>
Delta Aggregation	Test Connection, Account Aggregation and Delta Aggregation
Create Account	Test Connection, Account Aggregation and Create Account  <b>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.</b>
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  <b>Note: For Change Password of SNC network, additional permissions must be executed as specified in the “ Add/Remove Entitlements and Change Password” section.</b>

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
S_TABU_NAM	TABLE Name	TABLE	AGR_FLAGS, AGR_PROF, AGR_TCODES, AGR_TEXTS (Roles), USR11, UST10C (Profiles)

## Overview

- 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"> <li>• (Profiles) USRSYSPRF, USRSYSPRFT</li> <li>• (Roles) USRSYSACTT, USRSYSACT</li> </ul>

## 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
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	02 - Change, 05 - Lock
S_RFC	RFC_NAME	Name of RFC object	SDIFRUNTIME
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.

- (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 SAP Governance Module:

Parameters	Description
SAP Host*	Host on which the SAP Server is running

## Configuration parameters

Parameters	Description
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
Unlock on Password Change	If checked, the account would be unlocked while changing password.  <b>Note: Account will be unlocked at the time of set password only if the account is locked by incorrect password attempts.</b>
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 <b>A-M</b> , then this specifies that all the users whose User ID's 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 70.
<b>Load Balance Configuration parameters</b>	
Load Balancer	Select this to configure and enable load balancing on this application.
Host	SAP message server host.  <b>Note: Required for a logon load balanced connection.</b>
Client Group	Logon group name of SAP application servers.
Port Number	SAP message server service or port number.
<b>SNC Configuration parameters</b>	
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

Parameters	Description
SNC Partner Name	Represents SNC partner.  For example, provide input as p:CN=R3, O=XYZ-INC, C=EN 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.
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"> <li>on Microsoft Windows: <code>C:/sapcryptolib/sapcrypto.dll</code> (the location of the cryptographic library)</li> <li>on UNIX: <code>/opt/sailpoint/lib/custom/libsapcrypto.so</code> (the location of the cryptographic library)</li> </ul>
<b>SAP GRC Settings parameters</b>	
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.
<b>Note: For more information on SAP GRC configuration, see <i>SailPoint IdentityIQ Integration Guide</i>.</b>	

**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.

## Schema attributes

Attributes	Description
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.
Code (Address)	Signature initials
Communication Language (Address)	Communication language of the user.  <b>Note:</b> The different values to be set for this attribute are mentioned in “Logon and Communication Language attributes” on page 67.
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.  <b>Note:</b> For more information, see “Upgrade considerations” on page 65.
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

Attributes	Description
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
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.  <b>Note:</b> The different values to be set for this attribute are mentioned in “Logon and Communication Language attributes” on page 67.
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

## Schema attributes

Attributes	Description
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
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



Attributes	Description
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
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.  <b>Note: The Account Aggregation fetches the active roles (composite /simple) assigned directly to the user.</b>
Profiles	Profiles for user.

## Group attributes

The following table lists the different group attributes:

Attributes	Description
<b>Group Object Type = Role</b>	
Name	Role name.
Type	Role type.
Description	Role description.

## Schema attributes

Attributes	Description
Child Roles	Sub Role list.  <b>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.</b>
Long Description	Role long description.
Subsystem	System name for CUA System Aggregation.
Generated Profile	System generated profile associated to Role which has authorizations.
TCodes	Transaction code list.
<b>Group Object Type = Profile</b>	
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, 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)
- 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"/>
```

**Note:** When upgrading IdentityIQ from version 6.x to 7.3, 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, 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 SAP Governance Module.

**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 SAP Governance Module.

### 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 SAP Governance Module 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

---

The different values for Logon and Communication Language fields are as follows:

- Serbian=0
- Chinese=1
- Thai=2
- Korean=3
- Romanian=4
- Slovenian=5
- Croatian=6
- Malay=7
- Ukrainian=8
- Estonian=9
- Afrikaans=a
- Icelandic=b
- Catalan=c
- Serbian (Latin)=d
- Indonesian=i
- Arabic=A
- Hebrew=B
- Czech=C
- German=D
- English=E
- French=F
- Greek=G
- Hungarian=H
- Italian=I
- Japanese=J
- Danish=K
- Polish=L
- Chinese traditional=M
- Dutch=N
- Norwegian=O
- Portugese=P
- Slovak=Q
- Russian=R
- Spanish=S
- Turkish=T
- Finnish=U
- Swedish=V
- Bulgarian=W
- Lithuanian=X
- Latvian=Y
- Customer reserve=Z

## 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 BAPI's

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.

### 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")

## Troubleshooting

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 SAP Governance Module 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.  
SAP Governance Module 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**.



**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

Few attributes are not working after upgrading from version 6.0 patch 7 and version 6.1 to version 7.3.

**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
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 passthrough is enabled

Login fails for non aggregated accounts when passthrough is enabled.

In SAP Governance Module the SAPICO 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.

## Troubleshooting

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:

```
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 53 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"/>
```



# Enterprise Resource Planning Integration Modules

This section contains information on the following sections:

- “SailPoint Oracle E-Business Suite Integration Module”
- “SailPoint SAP Portal-User Management Web Service Integration Module”
- “SailPoint PeopleSoft Integration Module”
- “SailPoint Siebel Integration Module”
- “SailPoint NetSuite Integration Module”



# Chapter 6: SailPoint Oracle E-Business Suite Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	77
Supported features . . . . .	77
Supported Managed Systems . . . . .	78
Pre-requisites . . . . .	78
Administrator permissions . . . . .	78
Configuration parameters . . . . .	81
Additional configuration parameter . . . . .	83
Schema attributes . . . . .	84
Account attributes . . . . .	84
Group attributes . . . . .	85
Provisioning Policy attributes . . . . .	86
Create account attributes . . . . .	86
Create group attributes . . . . .	87
Additional information . . . . .	87
Troubleshooting . . . . .	90

## 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.

SailPoint Oracle E-Business Suite Integration Module controls the activities related to account/groups by signing in managed system. SailPoint Oracle E-Business Suite Integration Module will manage the following entities of Oracle E-Business Suite:

- User
- Group (Responsibility, Role)

## Supported features

---

SailPoint Oracle E-Business Suite Integration Module 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

Oracle E-Business Integration Module 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 88.

- 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 Integration Module:

- Oracle E-Business Suite 12.2.x
- 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, 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 81.

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
<b>Definer</b>		
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;
<b>Invoker</b>		
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;
<b>Definer/Invoker</b>		
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, aggregation would fail for all the service accounts with older permissions.

## Configuration parameters

The following table lists the configuration parameters of Oracle E-Business Suite Integration Module:

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

Attributes	Type
<b>Oracle E-Business Connection Settings</b>	
Connection User*	The Oracle EBS Login name through which we want to connect Oracle EBS. For example, <b>APPS</b>
Password*	The authentication details of login.

## Configuration parameters

Attributes	Type	
Database URL*	<p>The url to connect to the database. The format is <code>jdbc:oracle:thin:@&lt;HOST&gt;:&lt;PORT&gt;:&lt;SID&gt;</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"><li>• <b>jdbc:oracle:thin:@</b>: This is common part which states that the connection is made using thin driver.</li><li>• <b>xxx.xx.xx.xx</b>: server Name or IP of the oracle server</li><li>• <b>1521</b>: The port number of the oracle server. This port number should be known by the oracle server administrator.</li><li>• <b>ORCL</b>: The SID of the oracle server.</li></ul>	
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><b>Note: Set the following permissions as mentioned in the "Administrator permissions" on page 78 when 'E-Business Proxy User' parameter is not set:</b></p> <ul style="list-style-type: none"><li>• <b>Under Grant Permissions:</b> <code>grant select on SYS.DBA_USERS to \${new role};</code></li><li>• <b>Creating the synonym:</b> <code>create synonym DBA_USERS for SYS.DBA_USERS</code></li></ul>	
Account Aggregation Settings		
<b>Note: To use the Account Aggregation Settings, see 'Account Aggregation Filters' under "Upgrade considerations" on page 88.</b>		
Account Aggregation Filters	Select the type of users to be aggregated: <b>Employees, Contractors, Employee and Contractors</b> , and <b>all users from FND_USER table</b> .	
	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.

Attributes	Type	
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>&lt;entry key="endDateUserEntitlements"&gt;   &lt;value&gt;     &lt;Boolean&gt;true&lt;/Boolean&gt;   &lt;/value&gt; &lt;/entry&gt;</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>&lt;entry key="useEffectiveDate"&gt;   &lt;value&gt;     &lt;Boolean&gt;false&lt;/Boolean&gt;   &lt;/value&gt; &lt;/entry&gt;</pre> <p><b>Note: For more information, see "Upgrade considerations" on page 88.</b></p>
skipFutureAssignedGroups	<p>To aggregate and provision future dated E-Business users, set the value of <code>skipFutureAssignedGroups</code> parameter to false as follows:</p> <pre>&lt;entry key="skipFutureAssignedGroups"&gt;   &lt;value&gt;     &lt;Boolean&gt;false&lt;/Boolean&gt;   &lt;/value&gt; &lt;/entry&gt;</pre> <p><b>Note: For more information, see "Upgrade considerations" on page 88.</b></p>
disableOldFNDAccounts	<p><i>(Applicable only for Create User)</i> To disable any existing active FND accounts, set the value of <code>disableOldFNDAccounts</code> parameter to true as follows:</p> <pre>&lt;entry key="disableOldFNDAccounts"&gt;   &lt;value&gt;     &lt;Boolean&gt;true&lt;/Boolean&gt;   &lt;/value&gt; &lt;/entry&gt;</pre> <p><b>Note: For more information, see "Upgrade considerations" on page 88.</b></p>

## Schema attributes

Parameter	Description
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>&lt;entry key="useResponsibilityWithApplication"&gt;   &lt;value&gt;     &lt;Boolean&gt;true&lt;/Boolean&gt;   &lt;/value&gt; &lt;/entry&gt;</pre> <p><b>Note:</b> For more information, see "Upgrade considerations" on page 88.</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.
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.

Attributes	Description
RESPONSIBILITIES	Responsibilities assigned to a user.
ROLES	Roles assigned to a user.

## Custom attributes

Perform the following to support the custom attributes in Oracle E-Business Suite Integration Module:

- 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

## Provisioning Policy attributes

Attributes	Description
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.
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 Oracle E-Business Suite Integration Module 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.



Attributes	Description
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.  <b>Note: Applicable to new application of Oracle E-Business Suite after upgrading IdentityIQ to version 7.3.</b>

## 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.
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 Oracle E-Business Suite Integration Module.

## Upgrade considerations

---

- (Optional) After upgrading to IdentityIQ version 7.3, 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, by adding the `useEffectiveDate` 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 83.
- **Assigning responsibilities to future dated E-Business users**

After upgrading to IdentityIQ version 7.3, 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, add the `skipFutureAssignedGroups` entry key to the application debug page. For more information, see "Additional configuration parameter" on page 83.
- **Disabling existing accounts during provisioning**

After upgrading to IdentityIQ version 7.3, 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, set the value of the `disableOldFNDAccounts` parameter to true in the application debug page. For more information, see "Additional configuration parameter" on page 83.
- **Identifying responsibility group uniquely**

After upgrading to IdentityIQ version 7.3, 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 83.

**Note:** After setting the value of `useResponsibilityWithApplication` attribute to true, previous entitlement data cannot be retrieved.
- After upgrading to IdentityIQ version 7.3, 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, 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 of provisioning of Start Date, End Date and Justification attributes

---

With IdentityIQ version 7.3, 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">
      <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

After upgrading IdentityIQ to version 7.3, 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, 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 Oracle E-Business Suite Integration Module 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 7: SailPoint SAP Portal-User Management Web Service Integration Module

---

The following topics are discussed in this chapter:

Overview .....	91
Supported features .....	92
Supported Managed Systems .....	92
Pre-requisite .....	92
Administrator permission .....	93
Configuration parameters .....	93
Schema attributes .....	94
Account attributes .....	94
Group attributes .....	95
Provisioning Policy attributes .....	95
Additional information .....	97

## 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. SAP Enterprise Portal Integration Module 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.

SailPoint SAP Portal-User Management Web Service Integration Module manages the following entities of SAP User Management Engine (UME):

- User
- Role (UME and Portal)

### Supported features

---

SailPoint SAP Portal-User Management Web Service Integration Module 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 SAP Portal-User Management Web Service Integration Module:

- SAP NetWeaver 7.5, 7.4, 7.3, 7.2 and 7.1

**Note:** SailPoint SAP Portal-User Management Web Service Integration Module manages SAP User Management Engine users. For more information, see "Supported features" on page 92.

### 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 97.

## 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 Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The SAP Portal UMWebService Integration Module uses the following connection attributes:

**Table 1—SAP Portal UMWebService Integration Module - 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><b>Note: When using https, the portal server's keystore and the application server's keystore must be configured.</b></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( &amp;quot;USER.R3_DATASOURCE.&amp;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>

**Table 1—SAP Portal UMWebservice Integration Module - Primary Attributes (Continued)**

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( &amp;quot;com.sap.pct&amp;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 SAP Portal-User Management WebService Integration Module.

**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"><li>• True: Does not sets the password as productive</li><li>• False: Sets the password as productive.</li></ul> <p><b>Note: User must add “changePasswordRequired” attribute in schema and create provisioning policy and set the required display name (for example, “Password Change Required”).</b></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 the SAP Portal-User Management Web Service Integration Module.

### Undeploy .sda file

---

Perform the following steps to undeploy the .sda file:

1. From the command prompt browse the following location:  
`..\usr\sap\ (SAP EP 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`

## **Additional information**

# Chapter 8: SailPoint PeopleSoft Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	99
Supported features . . . . .	99
Supported Managed Systems . . . . .	100
Pre-requisites . . . . .	100
Administrator permission . . . . .	100
Configuration parameters . . . . .	100
Schema attributes . . . . .	102
Account attributes . . . . .	102
Group attributes . . . . .	103
Additional information . . . . .	103
Creating the Component Interfaces . . . . .	104
Partitioning Aggregation . . . . .	104
Performance improvement . . . . .	104
Creating the Component interface jar file . . . . .	106
Configuring the Component Interface Security . . . . .	107
Upgrade considerations . . . . .	108
Troubleshooting . . . . .	108

## Overview

---

The SailPoint PeopleSoft Integration Module manages the administrative entities of PeopleSoft server (User Profiles and Roles). The PeopleSoft Integration Module communicates to the PeopleSoft server through component interfaces.

## Supported features

---

SailPoint PeopleSoft Integration Module 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 104.
  - 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

## Supported Managed Systems

---

SailPoint PeopleSoft Integration Module supports the following managed systems:

- PeopleTools version 8.56, 8.55, 8.54, 8.53
- PeopleSoft Server version 9.2, 9.1

SailPoint PeopleSoft Integration Module 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 PeopleSoft Integration Module, 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 Integration Module 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 Integration Module 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 this Integration Module uses to connect and interact with the application. Each application type requires different information to create and maintain a connection.

The PeopleSoft Integration Module uses the following connection attributes:

Attribute	Description
Host*	The hostname of the PeopleSoft server.
Port*	The Jolt port (Jolt Server Listener Port) on which the PeopleSoft server is listening. Default: 9000
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*	The name of the PeopleSoft component interface to use to read PeopleSoft Roles.  For more information, see “Creating component interface for PeopleSoft” on page 287.
Jar location	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 <code>psjoe.jar</code> and <code>iiqPeopleSoftCompInt.jar</code> files). For more information, see Creating the Component interface jar file).  <b>Note:</b> For single PeopleSoft application, the PeopleSoft jars can be located in <code>WEB-INF\lib</code> directory.
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 ID's are between <b>A</b> and <b>M</b> (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 newline character. For more information, see “Partitioning Aggregation” on page 104
Domain Connection Password Enabled	Determines if Domain connection Password is configured.
Domain Connection Password*	Password is required if <b>Domain Connection Password Enabled</b> attribute is selected.
Route Control Component Interface	The name of the PeopleSoft component interface to use to read PeopleSoft RouteControls.  For more information, see “Creating component interface for PeopleSoft” on page 287.

**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.
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.



Attributes	Description
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 PeopleSoft Integration Module.

## Creating the Component Interfaces

---

For creating the component interfaces, see Appendix B: Component Interface.

## Partitioning Aggregation

---

To use the partitioning aggregation feature in ERP Integration Module, 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 104.

## 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 ROLENAM 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;
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

## Additional information

**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 Integration Module, you must allow the PeopleSoft user, for whom the Integration 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 287.

## 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 Integration Module.
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, manually add the following attributes in the Group Schema:

- RouteControl
- RouteControlDescription

For more information on the above attributes, see “Group attributes” on page 103.

**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 9: SailPoint Siebel Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	111
Supported features . . . . .	111
Supported Managed Systems . . . . .	112
Pre-requisites . . . . .	112
Administrator permission . . . . .	112
Configuration parameters . . . . .	112
Schema attributes . . . . .	114
Account attributes . . . . .	114
Account Group attributes . . . . .	114
Adding new custom attributes in schema . . . . .	115
Provisioning policy attributes . . . . .	115
Troubleshooting . . . . .	116

## Overview

---

The SailPoint Siebel Integration Module manages entities in Oracle's Siebel CRM. Here **Employee** is managed as Accounts and **Position** as Account Groups. By default, the Siebel Integration Module 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

---

SailPoint Siebel Integration Module 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

## Supported Managed Systems

---

SailPoint Siebel Integration Module 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:** Siebel Integration Module requires JRE 1.6 or above to manage Siebel CRM.

## Administrator permission

---

The Siebel Integration Module requires Siebel administrator credentials to accomplish provisioning tasks. The administrator user name and password configured for the Siebel Integration Module 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 Siebel Integration Module 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"> <li>• For English: ENU</li> <li>• For Brazilian Portuguese: PTB</li> <li>• For French: FRA</li> <li>• For German: DEU</li> <li>• For Italian: ITA</li> <li>• For Japanese: JPN</li> <li>• For Korean: KOR</li> <li>• For Simplified Chinese: CHS</li> <li>• For Spanish: ESP</li> <li>• For Traditional Chinese: CHT</li> </ul>
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 Siebel Integration Module 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, Siebel Integration Module 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
<b>Create Account</b>	
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.

## Troubleshooting

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 Type	Position type.
Parent Position Id	Parent position's Id.

## 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 10: SailPoint NetSuite Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	117
Supported features . . . . .	117
Supported Managed Systems . . . . .	118
Administrator permissions . . . . .	118
Configuration parameters . . . . .	118
Schema attributes . . . . .	119
Account attributes . . . . .	119
Group attributes . . . . .	120
Schema extension and custom attributes . . . . .	120
Provisioning Policy attributes . . . . .	121
Additional information . . . . .	122
NetSuite Application Program Interface (API) . . . . .	122

## 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>

NetSuite Integration Module 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

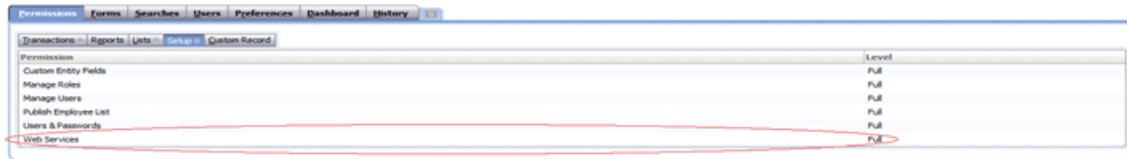
---

SailPoint NetSuite Integration Module supports 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

## Configuration parameters

**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

SailPoint NetSuite Integration Module supports the following managed system:

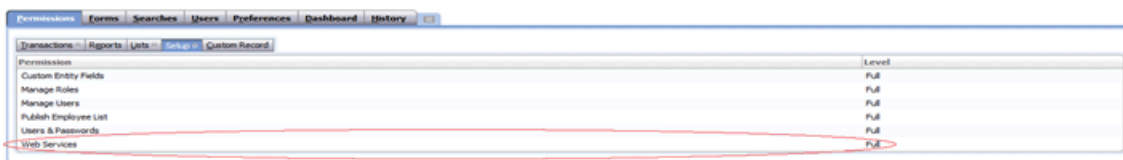
- NetSuite 2015.2
- Netsuite 2012\_1

## Administrator permissions

The NetSuite Integration Module 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 NetSuite Integration Module 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 <b>Setup =&gt; Integration =&gt; Web Services Preferences</b> .
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 <a href="#">"Administrator permissions" on page 118</a> .
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 NetSuite Integration Module. 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:

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

## Schema attributes

Department	Department of employee
Class	Class of employee
BillingClass	Billing 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.

NetSuite Integration Module 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 NetSuite Integration Module 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.

**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 120.

## Additional information

This section describes the additional information related to the NetSuite Integration Module.

### 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 NetSuite Integration Module

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*.

# Mainframe Integration Modules

This section contains information on the following sections:

- "SailPoint RACF Integration Module"
- "SailPoint CA-Top Secret Integration Module"
- "SailPoint CA-ACF2 Integration Module"
- "SailPoint RACF LDAP Integration Module"
- "SailPoint Top Secret LDAP Integration Module"



# Chapter 11: SailPoint RACF Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	125
Supported features . . . . .	125
Installing RACF Integration Module . . . . .	125

## Overview

---

The SailPoint RACF Integration Module manages IBM RACF User Profiles and Group Profiles.

## Supported features

---

SailPoint RACF Integration Module 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 RACF Integration Module

---

For installing RACF Integration Module, perform the following:

1. Install the Connector Gateway.  
For more information on installing the Connector Gateway, see *SailPoint Quick Reference Guide for Gateway Connectors*.
2. Install SailPoint Connector for RACF  
For more information on installing the Connector Gateway, see *SailPoint Connector for RACF Administration Guide*.





# Chapter 12: SailPoint CA-Top Secret Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	127
Supported features . . . . .	127
Installing CA-Top Secret Integration Module . . . . .	127

## Overview

---

The SailPoint CA-Top Secret Integration Module manages CA-Top Secret User ACIDs and Profile/Group ACIDs.

## Supported features

---

SailPoint CA-Top Secret Integration Module 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 CA-Top Secret Integration Module

---

For installing CA-Top Secret Integration Module, perform the following:

1. Install the Connector Gateway.  
For more information on installing the Connector Gateway, see *SailPoint Quick Reference Guide for Gateway Connectors*.
2. Install SailPoint Connector for CA-Top Secret  
For more information on installing the Connector Gateway, see *SailPoint Connector for CA-Top Secret Administration Guide*.

## Installing CA-Top Secret Integration Module

# Chapter 13: SailPoint CA-ACF2 Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	129
Supported features . . . . .	129
Installing CA-ACF2 Integration Module . . . . .	129

## Overview

---

The SailPoint CA-ACF2 Integration Module manages users and UIDs (implemented as Groups) in CA-ACF2.

## Supported features

---

SailPoint CA-ACF2 Integration Module 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 CA-ACF2 Integration Module

---

For installing CA-ACF2 Integration Module, perform the following:

1. Install the Connector Gateway.  
For more information on installing the Connector Gateway, see *SailPoint Quick Reference Guide for Gateway Connectors*.
2. Install SailPoint Connector for CA-ACF2  
For more information on installing the Connector Gateway, see *SailPoint Connector for CA-ACF2 Administration Guide*.

## Installing CA-ACF2 Integration Module

# Chapter 14: SailPoint RACF LDAP Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	131
Supported features . . . . .	131
Supported Managed Systems . . . . .	132
Pre-requisites . . . . .	132
Administrator permissions . . . . .	133
Configuration parameters . . . . .	133
Schema Attributes . . . . .	134
Account attributes . . . . .	134
Group attributes . . . . .	136
Provisioning Policy Attributes . . . . .	137
Account attributes . . . . .	134
Additional information . . . . .	138
Support for PassPhrase . . . . .	138
Support for Connection Attributes . . . . .	138
Implementing Secured Communication to RACF LDAP Server . . . . .	138
Defining Search Scope . . . . .	141
Troubleshooting . . . . .	142

## Overview

---

The SailPoint RACF LDAP Integration Module mainly uses the LDAP interfaces to communicate with z/OS LDAP server. The RACF LDAP Integration Module supports reading and provisioning of RACF LDAP users and entitlements.

## Supported features

---

SailPoint RACF LDAP Integration Module 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 141.

## Supported Managed Systems

---

SailPoint RACF LDAP Integration Module supports the following managed systems:

- 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

- 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 138.
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 141.

## Administrator permissions

The service account configured for SailPoint RACF LDAP Integration Module 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 RACF LDAP Integration Module uses the following configuration parameters:

Parameters	Description
<b>RACF LDAP Configuration Parameters</b>	
<code>useSSL</code>	Specifies if the connection is over TLS.
<code>authorizationType</code>	The authorization type to use when connecting to the server.
<code>user*</code>	User to connect as a DN string such as Administrator.
<code>password</code>	Password for the administrator account.
<code>port*</code>	Port number through which the server is listening.
<code>host*</code>	Host of the LDAP server.
<code>racfConnectProfileDN*</code>	Connect Profile type DN used during group membership provisioning.
<code>provisionPropertiesToAllConnections</code>	Sets the RACF connection properties defined in Provisioning Policy to all the RACF connections when multiple RACF Groups are requested in single operation.

## Schema Attributes

Parameters	Description
<b>Account Settings</b>	
searchScope	Depth to search the LDAP tree. <ul style="list-style-type: none"><li>• <b>OBJECT_SCOPE</b>: Limits the search to the base object or named object.</li><li>• <b>ONELEVEL_SCOPE</b>: Search is restricted to the immediate children of a base object, but excludes the base object itself.</li><li>• <b>SUBTREE_SCOPE</b>: 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.</li></ul>
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.



Attribute	Description
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 <b>top</b> or <b>alias</b> .
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 <b>ADSP GRPACC NOPASSWORD</b> or modify a RACF user entry with <b>NOGRPACC SPECIAL NOEXPIRED RESUME NOOMVS</b> .
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.
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.

## Schema Attributes

Attribute	Description
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
<b>Create Account</b>	
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.
connection_racfconnectowner	Distinguished name of the connection owner.
connection_racfConnectRevokeDate	Connection Revoke Date. For example, mm/dd/yy

## Additional information

Attributes	Description
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 RACF LDAP Integration Module.

### Support for PassPhrase

---

SailPoint RACF LDAP Integration Module 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

---

SailPoint RACF LDAP Integration Module 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
#####
TTLRule LDAP
{
  LocalAddr ALL
  RemoteAddr ALL
  LocalPortRange 389
  Direction Inbound
  Priority 255 # highest priority rule
  Userid GLDSRV
  TTLSTGroupActionRef GrpAct_LDAP
  TTLSEnvironmentActionRef GrpEnv_LDAP
  TLSSTConnectionActionRef GrpCon_LDAP
}

TTLSTGroupAction GrpAct_LDAP
{
  TTLSSTEnabled On
```

## Additional information

```
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
    TTLSCipherParmsRef 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
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
}
TTLSTKeyringParms PrmKeyRing_LDAP
{
    Keyring GLDRING
}

```

## Defining Search Scope

**Note:** RACF LDAP Integration Module 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 RACF LDAP Integration Module, objects can be retrieved by means of a **searchDN**, **searchFilter** and **searchScope**. RACF LDAP Integration Module 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 "/>
        <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>
    </List>
  </value>
</entry>

```

## Troubleshooting

```

    </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 15: SailPoint Top Secret LDAP Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	143
Supported features . . . . .	143
Supported Managed Systems . . . . .	144
Administrator permissions . . . . .	144
Configuration parameters . . . . .	144
Schema Attributes . . . . .	145
Account attributes . . . . .	145
TopSecretProfile attributes . . . . .	147
TopSecretGroup attributes . . . . .	148
Provisioning Policy Attributes . . . . .	148
Account attributes . . . . .	145
Additional information . . . . .	149
Support for PassPhrase . . . . .	149
Implementing Secured Communication to Top Secret LDAP Server . . . . .	149
Partitioning Aggregation . . . . .	152

## Overview

---

The SailPoint Top Secret LDAP Integration Module mainly uses the LDAP interfaces to communicate with CA LDAP server. The Top Secret LDAP Integration Module supports reading and provisioning of Top Secret LDAP users and entitlements.

## Supported features

---

SailPoint Top Secret LDAP Integration Module 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 152.

### Supported Managed Systems

---

SailPoint Top Secret LDAP Integration Module 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 149.
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 SailPoint Top Secret LDAP Integration Module 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 Top Secret LDAP Integration Module 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 Top Secret LDAP Integration Module.

### Support for PassPhrase

SailPoint Top Secret LDAP Integration Module supports PassPhrase feature as follows:

For password change operation on Top Secret LDAP 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
#####
TTLSPRule 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

---

Top Secret LDAP Integration Module supports Partitioning Aggregation feature to enable faster retrieval of Top Secret data.

In Top Secret LDAP Integration Module, objects can be retrieved by means of a **searchDN** and **searchFilter**. Top Secret LDAP Integration Module 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**

# Service Desk Integration Modules

This section contains information on the following sections:

- "SailPoint ServiceNow Service Integration Module"
- "SailPoint HP Service Manager Service Integration Module"
- "SailPoint BMC Remedy Service Desk Service Integration Module"



# Chapter 16: SailPoint ServiceNow Service Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	157
Supported features . . . . .	157
Supported platforms . . . . .	157
Pre-requisites . . . . .	158
Service Request . . . . .	158
Incident and Change Request . . . . .	158
Basic configuration . . . . .	159
Basic flow of Service Request . . . . .	161
Basic configuration of Service Request. . . . .	161
Configuring IdentityIQ to integrate with ServiceNow. . . . .	162
IntegrationConfig XML files for Service Request, Incident and Change Request . . . . .	165
Configuration procedure . . . . .	166
Retryable mechanism . . . . .	168
Sample scenario . . . . .	168
Troubleshooting . . . . .	169

## 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 ServiceNow Service Integration Module eliminates the need to build and maintain a custom integration, and reduces time-to-deployment.

## Supported features

---

SailPoint ServiceNow Service Integration Module 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

---

SailPoint ServiceNow Service Integration Module supports the following ServiceNow versions:

- Kingston
- Jakarta
- Istanbul

## 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 ServiceNow Service Integration Module Administrator must be assigned the `x_sap_iiq_sim.admin` role.
- Apply the ServiceNow Service Integration Module update set:
  - a. 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 version	Update Sets
Istanbul or Later	IdentityIQServiceNowServiceIntegrationModule.v2.1.3.xml SailPointServiceRequestGenerator.v1.1.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/>
- c. 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](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 ServiceNow Service Integration Module Administrator must be assigned the `x_sapo_iiq_sim.admin` role.
- Apply the ServiceNow Service Integration Module update set:
  - a. 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 version	Update Sets
Istanbul or Later	IdentityIQServiceNowServiceIntegrationModuleForIncidentAndChange.v1.2.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 Istanbul or later uncomment the following entry in the statusMap:

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

- for Change Request: #CHANGE REQUEST
  - a. For Istanbul or later, replace `<state>1</state>` with `<state>-5</state>` in the soap-message.
  - b. For Istanbul 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 162.

**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 SailPoint ServiceNow Service Integration Module 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.

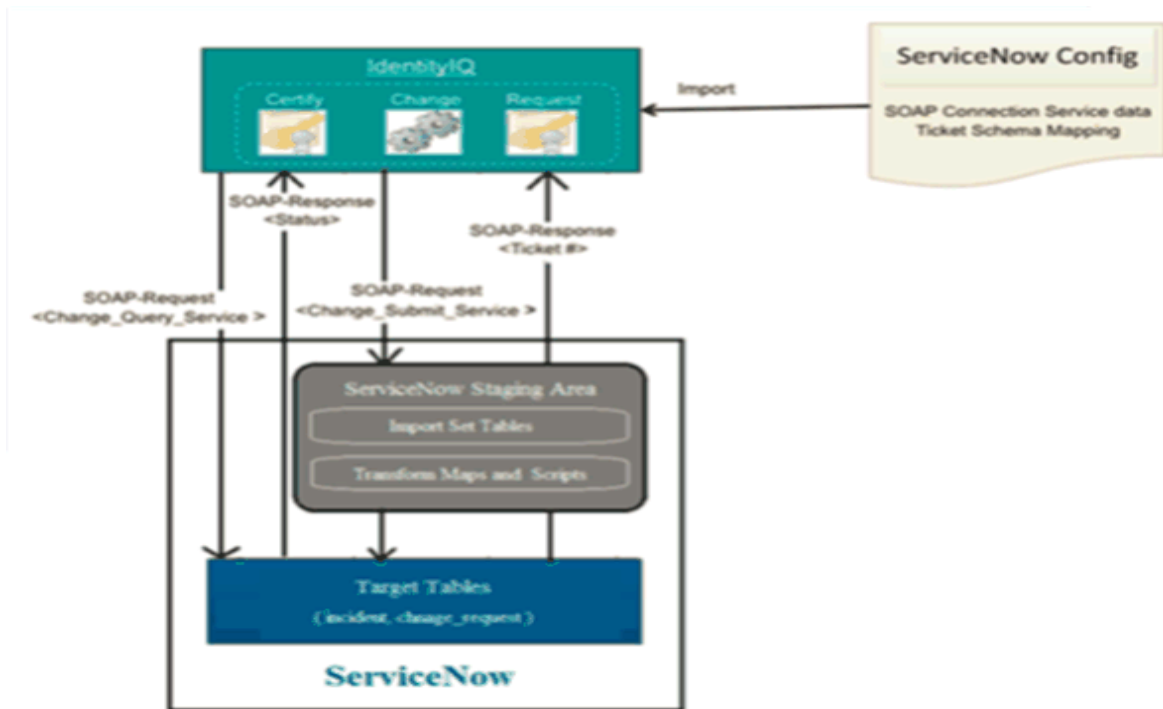


Figure 1—Basic configuration

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 ServiceNow Service Integration Module. The name must contain “IdentityIQ” to filter and display in SailPoint Service Integration Module 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](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](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"/>
```

## Configuring IdentityIQ to integrate with ServiceNow

**Note:** The Catalog item name is case sensitive.

- 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 SailPoint Service Integration Module 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](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](http://wiki.servicenow.com/index.php?title=Using_Access_Control_Rules#Creating_ACL_Rules)

## 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	Istanbul or Later
ServiceNow endpoint to create a ticket	Service Request	<a href="https://demo.service-now.com/ScRequestGenerator.do?SOAP">https://demo.service-now.com/ScRequestGenerator.do?SOAP</a>
	Incident	<a href="https://demo.service-now.com/x_sapo_iiq_sim_incident.do?SOAP">https://demo.service-now.com/x_sapo_iiq_sim_incident.do?SOAP</a>
	Change Request	<a href="https://demo.service-now.com/x_sapo_iiq_sim_change_request.do?SOAP">https://demo.service-now.com/x_sapo_iiq_sim_change_request.do?SOAP</a>
ServiceNow endpoint to get ticket status	Service Request	<a href="https://demo.service-now.com/sc_req_item.do?SOAP">https://demo.service-now.com/sc_req_item.do?SOAP</a>
	Incident	<a href="https://demo.service-now.com/incident.do?SOAP">https://demo.service-now.com/incident.do?SOAP</a>
	Change Request	<a href="https://demo.service-now.com/change_request.do?SOAP">https://demo.service-now.com/change_request.do?SOAP</a>

- **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 167](#).

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 <a href="#">“IntegrationConfig XML files for Service Request, Incident and Change Request”</a> on page 165.
<code>username</code>	Can be blank if <b>Require basic authorization for incoming SOAP requests</b> is not selected on ServiceNow side.
<code>password</code>	Can be blank if <b>Require basic authorization for incoming SOAP requests</b> 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

Entry key (ServiceNow)	Values (IdentityIQ)
<b>statusMap</b>	
1	inProcess
2	inProcess
3	inProcess
4	inProcess
5	inProcess
6	committed
7	committed
8 (For Istanbul or later)	failure
<b>statusMapCloserCode</b>	
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 &amp;

- 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.

## Sample scenario

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.

## Retryable mechanism

---

By default ServiceNow Service Integration Module 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 Service Integration Module. 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 Service Integration Module, then IdentityIQ will not attempt a retry.

For example,

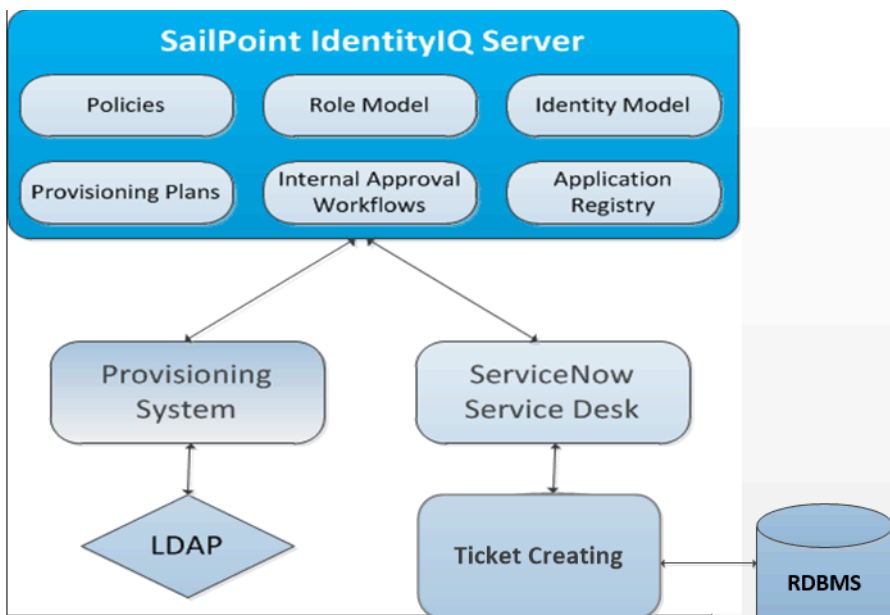
```
<entry key="retryableErrors">
  <value>
    <List>
      <String>Connection reset</String>
    </List>
  </value>
</entry>
```

**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 SailPoint 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.
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 ServiceNow Service Integration Module.
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 ServiceNow Service integration Module.

**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 166.

### 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.saaj.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 GUID's

**Resolution:** Ensure that the Cart GUID's 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](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=""/>
```



# Chapter 17: SailPoint HP Service Manager Service Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	173
Supported features . . . . .	173
Supported platforms . . . . .	174
Pre-requisites . . . . .	174
Configuring HP Service Manager for IdentityIQ Integration . . . . .	177
Retryable mechanism . . . . .	184
Additional information . . . . .	184
Troubleshooting . . . . .	186

## 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

---

HP Service Manager Service Integration Module supports the following features:

- Creates the following types of tickets in HP Service Manager 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

---

SailPoint HP Service Manager Service Integration Module supports the following version of Service Manager:

- 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 185.
  - 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” on page 185 and “Importing user details from HP Service Manager to IdentityIQ” on page 185.

### 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 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	HPServiceManagerIntegrationConfigForRequest.xml
Incident Request	HPServiceManagerIntegrationConfigForIncident.xml
Change Request	HPServiceManagerIntegrationConfigForChange.xml

For more information, refer to the “Sample XML files for Service, Incident and Change Request” on page 179 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 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 for IdentityIQ Integration

### *Service Request*

Entry Key	Values
<b>statusMap</b>	
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
<b>Status Map Closure Codes</b>	
<i>Incident Closure Codes</i>	
Automatically Closed	committed
Cancelled	failure
Fulfilled	committed

Entry Key	Values
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
<b>statusMap</b>	
Closed	committed
Pending Other	inProcess

## Configuring HP Service Manager for IdentityIQ Integration

Entry key	Values
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
<b>Status Map Closure Codes</b>	
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
<b>statusMap</b>	
initial	inProcess
waiting	inProcess
reopened	inProcess
closed	committed
<b>Status Map Closure Codes</b>	
1 - Successful	committed



Entry Key	Values
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 **&amp;**;
    - 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.
    - 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

## Additional information

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.

## Retryable mechanism

---

By default HP Service Manager Service Integration Module 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 Service Integration Module. 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 Service Integration Module, 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 HP Service Manager Integration Module.

## 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**.
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**.

## Exporting user details from HP Service Manager

---

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 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 HP Service Manager Service Integration Module.

## 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 183.

## 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.saaj.SOAPConnectionFactoryImpl
- -Djavax.xml.soap.MessageFactory=org.apache.axis2.saaj.MessageFactoryImpl
- -Djavax.xml.soap.SOAPFactory=org.apache.axis2.saaj.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:  
`threadspersprocess: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.hp servicemanager.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 for IdentityIQ Integration” on page 177 for Incident and Change Requests are performed appropriately.



# Chapter 18: SailPoint BMC Remedy Service Desk Service Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	189
Supported features . . . . .	189
Supported platforms . . . . .	189
Pre-requisites . . . . .	190
Basic configuration . . . . .	190
Configuring BMC Remedy AR System for IdentityIQ Integration . . . . .	191
Configuring IdentityIQ for BMC Remedy Action Request System Integration . . . . .	193
Sample scenario . . . . .	198
Troubleshooting . . . . .	198

## 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 Service 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 Integration

**Module component:**

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

## Supported features

---

BMC Remedy Service Integration Module 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

---

SailPoint BMC Remedy Service Desk Service Integration Module supports the following versions of BMC Remedy AR System:

- 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](#)).



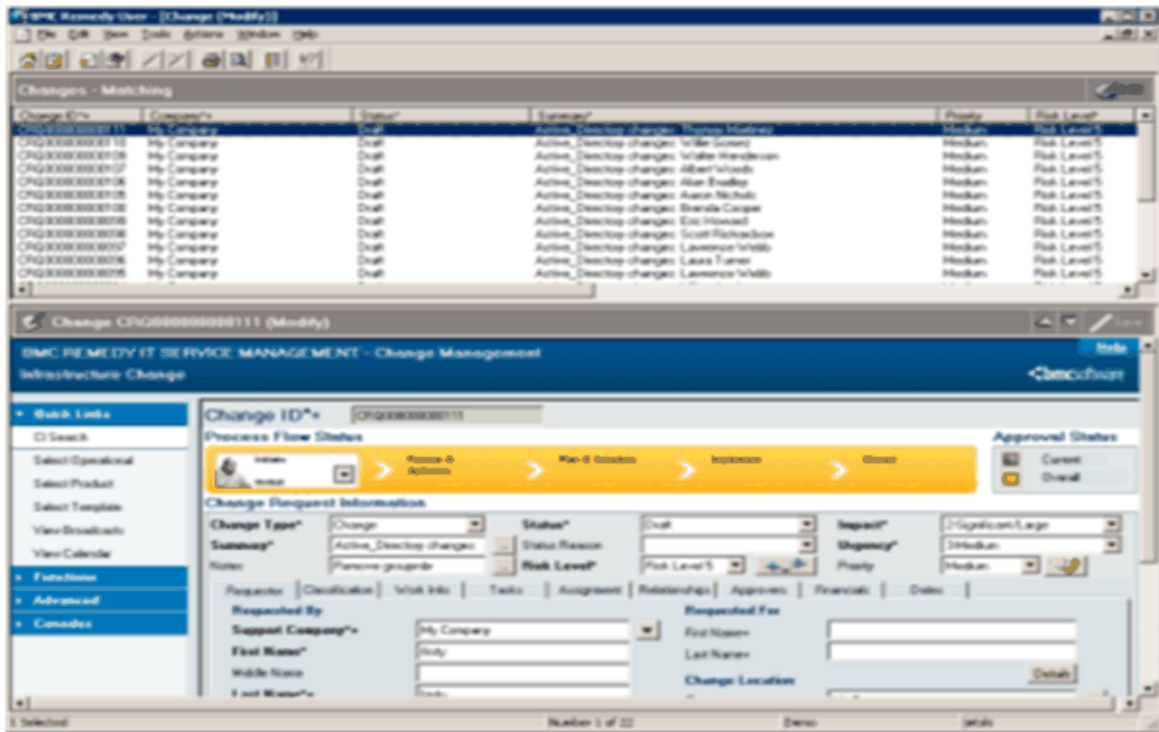


Figure 1—Change request

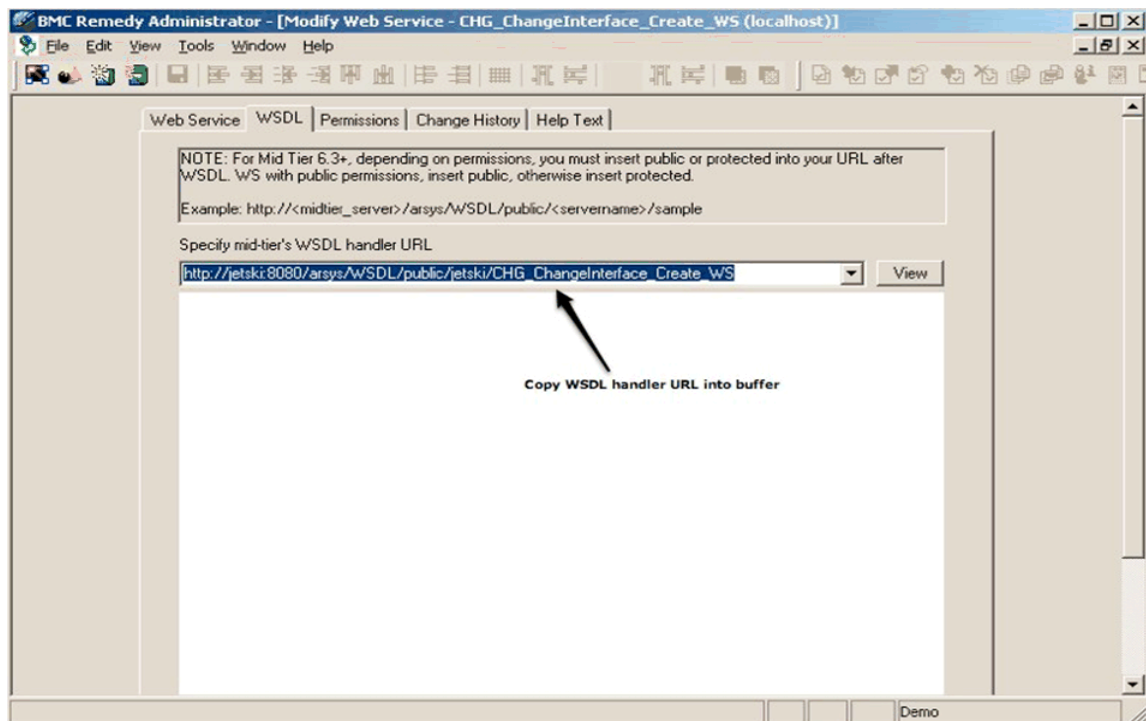
## Configuring BMC Remedy AR System for IdentityIQ Integration

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 &amp;

- 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 195 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">

```

## Sample scenario

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

## Sample scenario

---

The sample integration scenario is built around a sample system. In the sample scenario SailPoint (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.
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.



# GRC Integration Module

This section contains information on the following section:

- "SailPoint SAP GRC Integration Module"

**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 19: SailPoint SAP GRC Integration Module

---

The following topics are discussed in this chapter:

Introduction .....	203
Supported features .....	204
Supported platforms .....	205
Pre-requisites .....	205
SAP GRC Server Settings .....	205
SAP Connector changes for supporting SAP GRC integration. ....	206
Creating IdentityIQ application of type SAP GRC .....	207
SAP GRC workflows .....	208
Minimum permissions required for SAP GRC user .....	211
Custom workflows provided for SAP GRC integration .....	212
SAP GRC Data Generator .....	212
SAP GRC Request Executor .....	213
Importing SAP GRC Application Rule .....	215
Viewing the reports .....	216
Upgrade considerations .....	216
Additional information .....	217
Creating a RFC Connection on SAP GRC system .....	217
Configuring cross system on SAP GRC .....	218
(Optional) Support for additional parameters .....	219
Support for provisioning start and end date for role assignment .....	221
Troubleshooting .....	222

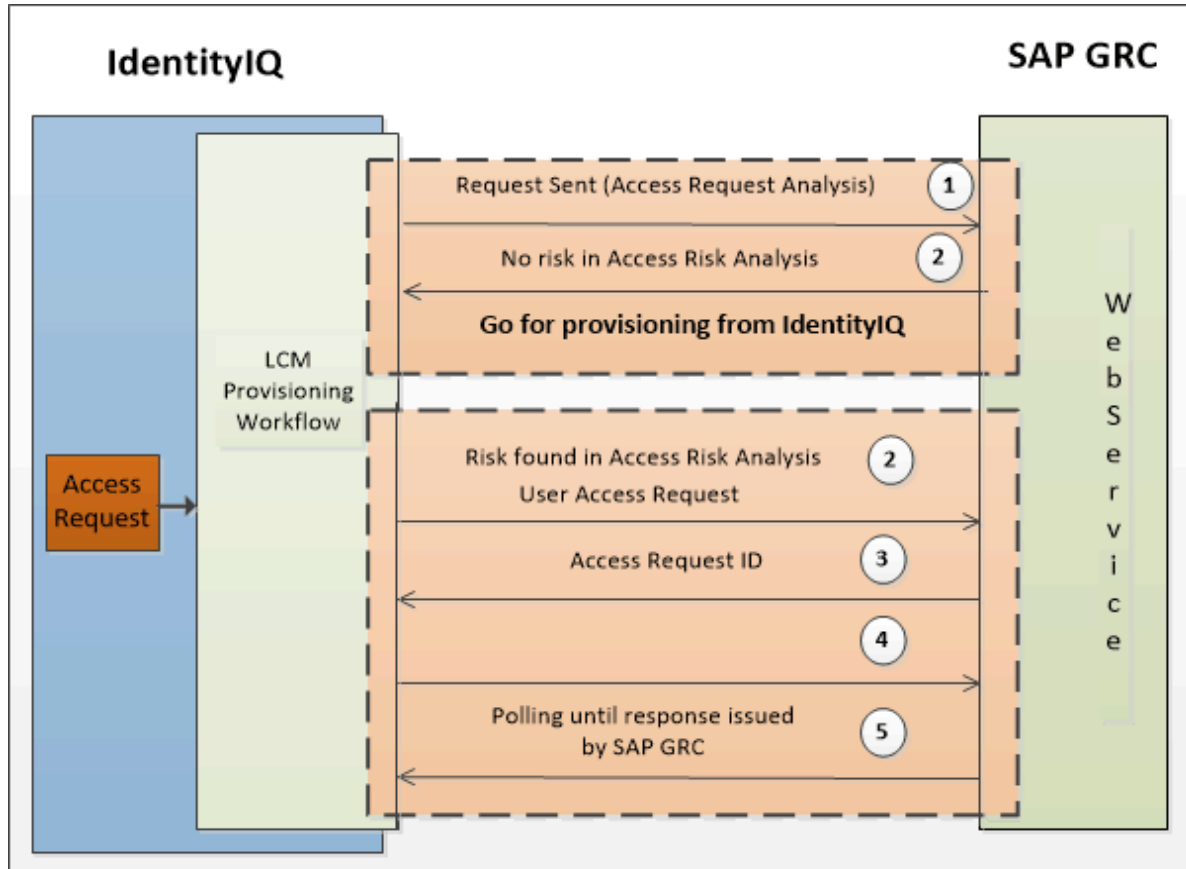
## Introduction

---

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.

SailPoint SAP GRC Integration Module 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**

SailPoint SAP GRC Integration Module (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 SAP GRC Integration Module 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 221.

## Supported platforms

---

SailPoint SAP GRC Integration Module supports the following version of SAP GRC Access Control:

- 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:
  - Execute **SPRO** transaction code and click **SAP Reference IMG** button.
  - Expand **Governance, Risk and Compliance** ==> **Access Control** ==> **User Provisioning** option.
  - Click on  image to execute **Maintain Provisioning Settings** transaction.
  - In Dialog Structure double click on **Maintain Global Provisioning**.
  - 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:


- Execute **SPRO** transaction code and click **SAP Reference IMG** button.
- Expand **Governance, Risk and Compliance** ==> **Access Control** ==> **User Provisioning** option.
- Click on  image to execute **Maintain Provisioning Settings** transaction.
- 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 217.
- 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**.

## Pre-requisites

- 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 207.
- 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 207.

## 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 217.



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 215.

## 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
<b>SAP GRC Connection Settings</b>	
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 211.
Password*	Login Password.
Request Initiation System *	Name of the connector configured in SAP GRC server which is treated as <b>Request Initiation System</b> . 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 217.
Polling interval	Polling interval in minutes (Range 1 to 360).
<b>Web Service URL Details</b>	
User Access *	End Point URL for SAP GRC User Access Web Service.  Format of URL would be as follows:  <b>http://&lt;SAP GRC Host Name&gt;/sap/bc/srt/rfc/sap/GRAC_user_acces_ws&lt;WebService Binding URL&gt;</b>

## 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:  <b>http://&lt;SAP GRC Host Name&gt;/sap/bc/srt/rfc/sap/GRAC_risk_analysis_wout_no_ws&lt;WebService Binding URL&gt;</b>
Request Details *	End Point URL for SAP GRC Request Detail Web Service.  Format of URL would be as follows:  <b>http://&lt;SAP GRC Host Name&gt;/sap/bc/srt/rfc/sap/GRAC_request_details_ws&lt;WebService Binding URL&gt;</b>
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:  <b>http://&lt;SAP GRC Host Name&gt;/sap/bc/srt/rfc/sap/GRAC_audit_logs_ws&lt;WebService Binding URL&gt;</b>
<b>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 206.</b>	

## 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 212.

- 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 212.

**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.

Save the form.

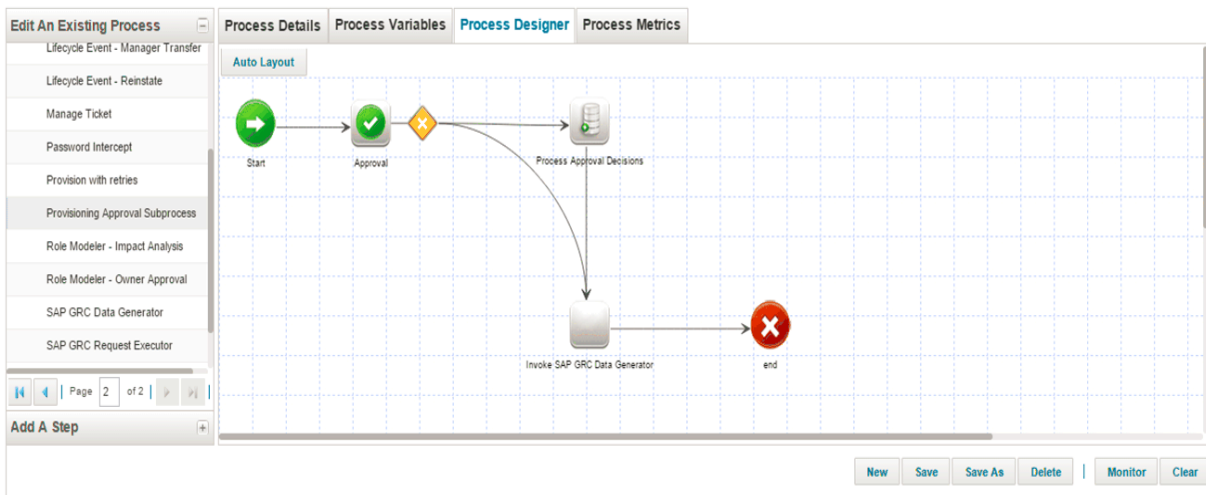
- Right click on **Stop** step, click **Edit Step** and in Details section provide the name as **end**.

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.

## Pre-requisites

### 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"> <li>SRV_NAME (Select * or select Technical names of following web service configured in SAP GRC) <ul style="list-style-type: none"> <li>Risk analysis Webservice:</li> <li>User access Webservice</li> <li>Request details Webservice</li> <li>Audit log Webservice:</li> </ul> </li> <li>SRV_TYPE: WS</li> </ol>
GRAC_RA	<ul style="list-style-type: none"> <li>Activity: Administrator</li> <li>Object types for Authorization: User, Role, Profile</li> <li>Risk Analysis Mode: All values or provide the required value</li> <li>Report Type: All values or provide the required value</li> </ul>
GRAC_SYS	<ul style="list-style-type: none"> <li>Activity: 01</li> <li>Application Type: 001 (SAP)</li> <li>SYSTEM Environment: Select the environment in use, that is, Development, Production, Test</li> <li>Connector ID: * or select the connector id configured on SAP GRC</li> </ul>
GRAC_REQ	<ul style="list-style-type: none"> <li>Activity: 01</li> <li>Request Type: 001,002</li> <li>Business Process: * or provide the required values</li> <li>Functional Area: * or provide the required functional areas</li> <li>Request for single or multiple: All values or provide the required value</li> <li>Request Information: All values or provide the required value</li> </ul>
GRAC_ROLED	<ul style="list-style-type: none"> <li>Activity: 03</li> <li>Business Process: * or provide the required values</li> <li>Connector Group: * or select the connector group configured on SAP GRC</li> <li>Role Sensitivity: 000</li> <li>Role Type: BUS, COM, CUA, PRF, SIN</li> <li>Role Name: * or provide the required value</li> </ul>

## 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 <b>Build Approval Set</b> 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 <b>stdout</b> .
requester	Requester who initiated the request.
<b>Support for additional parameters</b>	
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.
<b>Note: For more information about the support for additional parameters, see (Optional) Support for additional parameters 219.</b>	

## 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.
retriableErrors	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.

## Custom workflows provided for SAP GRC integration

Field names	Description
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://SAPGRCAplications.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>
```

**For example,** rule "Mapping GRC Connector Name to SAP based application"  
"E://sapGrcRuleParameters.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:

## Viewing the reports

```
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.

### 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.

**Note:** Perform Step 2. of “Importing integration workflows” section.

### Upgrade settings

---

For user upgrading to IdentityIQ version 7.2 Patch 2, 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.
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.

## Additional information

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 217.
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, 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>
<Variable input="true" name="ruleSetId">
<Description>A comma separated string of Rule Set Id values used for SAP GRC Proactive
check.</Description>
</Variable>
```

## Additional information

```
"<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.

**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"/>
```

## Troubleshooting

```
<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:



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);
```

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);
```

## Troubleshooting

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**

# Service Management Integration Module (Service Catalog)

The Service Management Integration Module helps to perform effective and efficient service management for IdentityIQ services offered to the organization in the ServiceNow Service Catalog. The information contained within the Service Catalog 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. 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 section:

- "SailPoint ServiceNow Service Catalog Integration"  
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.
- "SailPoint ServiceNow Service Catalog API Integration"  
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 20: SailPoint ServiceNow Service Catalog Integration

---

The following topics are discussed in this chapter:

Overview . . . . .	227
Supported features . . . . .	228
Supported platforms . . . . .	229
Pre-requisites . . . . .	229
Installation and configuration in ServiceNow . . . . .	229
Configuration in SailPoint IdentityIQ . . . . .	233
Troubleshooting . . . . .	233

## Overview

---

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.

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 SailPoint Service Catalog Integration in ServiceNow. The following information enables administrators to deploy and maintain the integration.

The flow of SailPoint Service Catalog Integration in ServiceNow is as follows:

- User logs in to ServiceNow.
- The **SailPoint Service Catalog Integration** application is available to the logged in user.
- Click on any of the links mentioned in the request section of SailPoint Service Catalog Integration 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 Service Catalog Integration with SailPoint IdentityIQ:

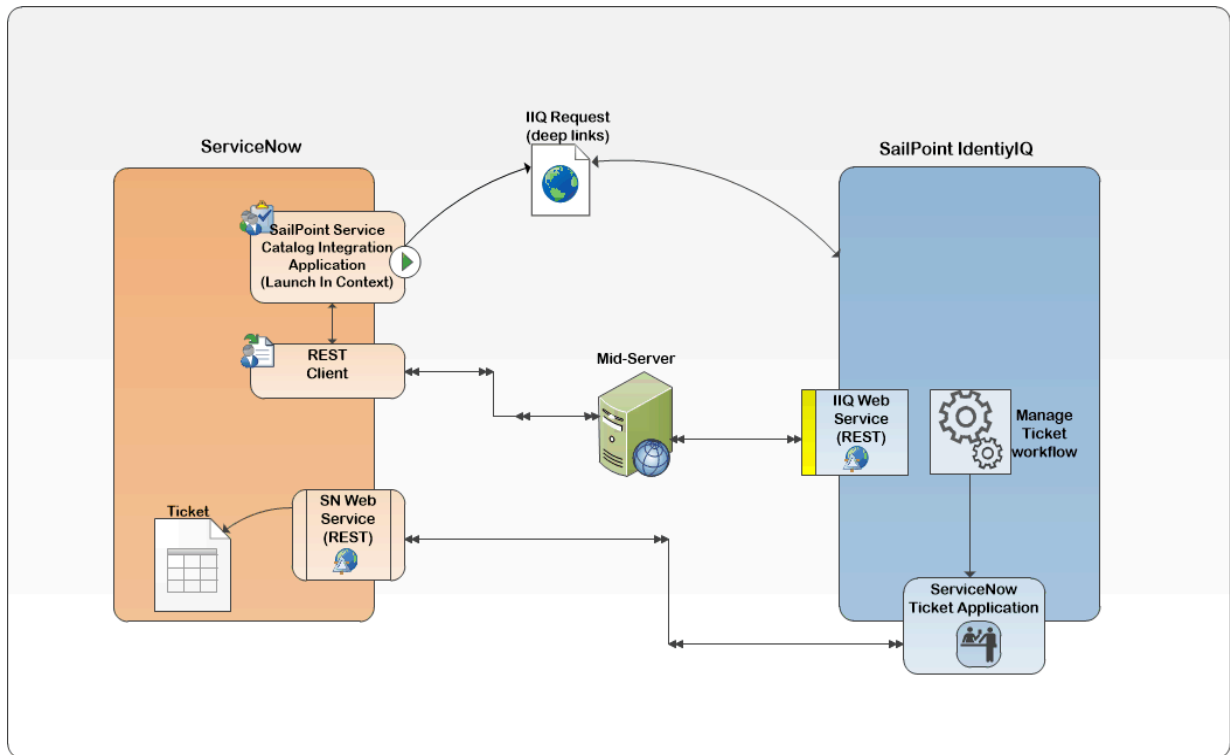


Figure 1—Basic Configuration

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 SailPoint Service Catalog Integration enables the use of IdentityIQ Lifecycle Manager within ServiceNow user interfaces. The inclusion of the SailPoint Service Catalog Integration 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

---

SailPoint Service Catalog Integration supports the following ServiceNow instance versions:

- Kingston
- Jakarta
- Istanbul

## 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 231.

**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:** SailPoint Service Catalog Integration Administrator Role. The user with this role can access all the modules of the application.
- **x\_sapo\_iiq\_catalog.spnt\_manager:** SailPoint Service Catalog Integration Manager Role. The user with this role can access all modules except Setup.
- **x\_sapo\_iiq\_catalog.spnt\_user:** SailPoint Service Catalog Integration 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 Service 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
Istanbul 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](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 **SailPoint Service Catalog Integration** application is created.
3. After committing the update set for SailPoint Service Catalog Integration, add read operation ACL's 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 Service Catalog Integration" Application

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

**Note:** The **SailPoint Service Catalog Integration** 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 Istanbul 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](http://wiki.servicenow.com/index.php?title=MID_Server)

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

<https://docs.servicenow.com/bundle/Istanbul-it-operations-management/page/product/mid-server/task/t ValidateAMIDServer.html>

## Configuration

---

### Set “SailPoint Service Catalog Integration” Application properties in ServiceNow to point to the SailPoint IdentityIQ instance

Open the **Properties** module from **SailPoint Service Catalog Integration** Application and modify the following properties:

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

## Installation and configuration 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 SailPoint Service Catalog Integration 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 SailPoint Service Catalog Integration application in ServiceNow

**Resolution:** To enable the traces in SailPoint Service Catalog Integration 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 Service Catalog Integration application parameters to enable logging. This enables any IdentityIQ provisioning actions traceable.



# Chapter 21: SailPoint ServiceNow Service Catalog API Integration

---

The following topics are discussed in this chapter:

Overview . . . . .	235
Supported features . . . . .	236
Supported platforms . . . . .	236
Pre-requisites . . . . .	236
Installation and configuration in ServiceNow . . . . .	236
Configuration in SailPoint IdentityIQ . . . . .	239
Troubleshooting . . . . .	239

## Overview

---

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.

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 SailPoint ServiceNow Service Catalog API Integration in ServiceNow. The following information enables administrators to deploy and maintain the integration.

The flow of SailPoint ServiceNow Service Catalog API Integration in ServiceNow is as follows:

- User logs in to ServiceNow Service Portal.
- 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 SailPoint ServiceNow Service Catalog API Integration enables the use of IdentityIQ Lifecycle Manager within ServiceNow user interfaces. The inclusion of the SailPoint ServiceNow Service Catalog API Integration 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

---

SailPoint ServiceNow Service Catalog API Integration supports the following ServiceNow instance versions:

- Kingston
- Jakarta
- Istanbul

## 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 237.

**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 SailPoint ServiceNow Service 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.v1.0.0.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/jakarta-application-development/page/build/system-update-sets/task/t\\_SaveAnUpdateSetAsAnXMLFile.html?title=Saving\\_Customizations\\_in\\_a\\_Single\\_XML\\_File#ari-aid-title2](https://docs.servicenow.com/bundle/jakarta-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 **SailPoint ServiceNow Service Catalog API Integration** application is created.
3. After committing the update set for SailPoint ServiceNow Service Catalog API Integration, add read operation ACL's 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 “SailPoint ServiceNow Service Catalog API Integration” Application

The SailPoint ServiceNow Service Catalog API Integration provides easy access to Role Access Requests.

**Note:** The **SailPoint ServiceNow Service Catalog API Integration** 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](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 “SailPoint ServiceNow Service Catalog API Integration” Application properties in ServiceNow to point to the SailPoint IdentityIQ instance

Open the **Properties** module from **SailPoint ServiceNow Service Catalog API Integration** application and modify the following properties:

**Note:** The properties module from **SailPoint ServiceNow Service Catalog API Integration** application is available only to those user who have the `x_sap_servcat_api.admin` role in ServiceNow.

Properties	Description
URL to connect to SailPoint instance	URL specifying the SailPoint IdentityIQ endpoint.
User to login to the SailPoint instance	Username for authentication during REST Requests to SailPoint IdentityIQ.  <b>Note: This user must have SCIM Executor Permission in IdentityIQ.</b>
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.
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.
Involved SailPoint Roles	Role type to request.  <b>Default:</b> it, business
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.  <b>Default:</b> 1000
Name of the application in the SailPoint instance that handles ticket requests	Name of the application in the SailPoint instance that handles ticket requests.  <b>Default:</b> servicenow-ticket-management-app
SailPoint Request Access business process name	SailPoint Request Access business process name.  <b>Default:</b> LCM Provisioning
Use SailPoint approval model	<b>Default:</b> Yes
Logging Level	<b>Default:</b> 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.
provisioningStateMap	Mapping between Access Request Provisioning state in IdentityIQ and Provisioning State of Requested Item (RITM) in ServiceNow.

## Troubleshooting

### 1 - Enable Traces for SailPoint ServiceNow Service Catalog API Integration application in ServiceNow

**Resolution:** To enable the traces in SailPoint ServiceNow Service Catalog API Integration 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 SailPoint ServiceNow Service Catalog API Integration 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 categories. Provide the required configuration on the OOTB item.

### 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).

# Provisioning Integration Modules

This section contains information on the following sections:

- "SailPoint Oracle Identity Manager Provisioning Integration Module"
- "SailPoint IBM Security Provisioning Integration Module" on page 249



# Chapter 22: SailPoint Oracle Identity Manager Provisioning Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	243
Supported features . . . . .	243
Supported platforms . . . . .	244
Installing the OIM Integration Web Application . . . . .	244
Testing the OIM Integration Web Application. . . . .	245
Configuration for OIM application . . . . .	247
Aggregating from OIM . . . . .	248
Known/Open issues . . . . .	248

## 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 Oracle Identity Manager Provisioning Integration Module 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

---

SailPoint Oracle Identity Manager Provisioning Integration Module 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 246.
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>

## Testing the OIM Integration Web Application

The following response is displayed:

```
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 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/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 246.

## 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 23: SailPoint IBM Security Provisioning Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	249
Supported features . . . . .	249
Supported platforms . . . . .	249
General configuration . . . . .	250
Configuration for Aggregation . . . . .	250
Configuration for Provisioning . . . . .	250
Troubleshooting . . . . .	252

## 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 SailPoint production environment.

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

## Supported features

---

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

The Security Provisioning Integration Module 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

---

SailPoint IBM Security Provisioning Integration Module 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 searchable. 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-Account-CorrelationRule.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`
- `isim_api.jar`
- `isim_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/isim_api.jar \
WEB-INF/lib/isim_common.jar WEB-INF/lib/isim_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

---

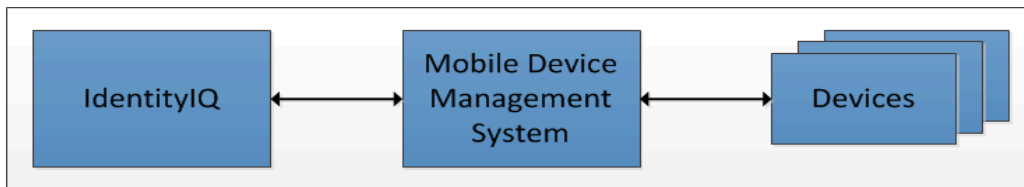
### 1 - An error message appears when the url format in itim.properties is not valid

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.

# Mobile Device Management Integration Modules

Mobile Device Management Integration Module (MIM) manages Devices enrolled in Mobile Device Management (MDM) System. MIM also manages Users/Administrators of MDM System. Following is an architecture diagram of MIM:



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. MIM does not communicate with the devices directly.

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

This section contains information on the following:

- "SailPoint AirWatch Mobile Device Management Integration Module" on page 255
- "SailPoint MobileIron Mobile Device Management Integration Module" on page 259
- "SailPoint Good Technology Mobile Device Management Integration Module" on page 263





# Chapter 24: SailPoint AirWatch Mobile Device Management Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	255
Supported features . . . . .	255
Supported platforms . . . . .	256
Pre-requisites . . . . .	256
Configuration . . . . .	256
Application configuration . . . . .	257
Operation specific configuration . . . . .	257

## Overview

---

This document provides a guide to the AirWatch Mobile Device Management (AirWatch) 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 Mobile Device Management (MDM) 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 MDM Integration 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 MDM
  - Delete, Unlock devices

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

## 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 MDM are retrieved into IdentityIQ.
Delete account for AirWatch device application	Enterprise/Device Wipe and Delete device is triggered on the device via AirWatch MDM system. For more information, see “Operation specific configuration” on page 257.
Unlock account for AirWatch device application	Unlock device is triggered on the device via AirWatch MDM 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

---

SailPoint AirWatch Mobile Device Management Integration Module supports the following version of AirWatch:

- AirWatch Platform Services 8.4.7.0

## Pre-requisites

---

Administrator user configured for AirWatch MDM 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 MDM 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 MIM (Mobile Device Management Integration Module).
AirWatch Server	AirWatch server URL where it's REST API are accessible. For example, <a href="https://apidev-as.awmdm.com">https://apidev-as.awmdm.com</a> .
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 MDM 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 MDM 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 25: SailPoint MobileIron Mobile Device Management Integration Module

The following topics are discussed in this chapter:

Overview . . . . .	259
Supported features . . . . .	259
Supported platforms . . . . .	260
Pre-requisites . . . . .	260
Configuration . . . . .	260
Application configuration . . . . .	260
Operation specific configuration . . . . .	261

## 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 Mobile Device Management (MDM) Application.

## Supported features

The SailPoint MobileIron MDM Connector provides the ability to provision MobileIron devices from IdentityIQ.

The MobileIron MDM Connector supports the following functions:

- Account Management
  - Device aggregation which include device Attribute, Group Attribute - Labels and Entitlements - Apps, Labels.
  - MobileIron MIM 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 MDM:

IdentityIQ operation	Resulting change on MobileIron
Account aggregation on MobileIron application	The devices that are managed by the MobileIron MDM 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 MDM are retrieved into IdentityIQ.
Create account of MobileIron application	Registering a device on MobileIron system. For more information, see “Operation specific configuration” on page 261.
Delete account of MobileIron application	Wipe/Retire device is triggered on the device via MobileIron MDM System. For more information, see “Operation specific configuration” on page 261.
Unlock account for MobileIron application	Unlock device is triggered on the device via MobileIron MDM system.
Adding entitlements to account	Adding labels to device from MobileIron MDM system.
Deleting entitlements from account	Removing device labels from MobileIron MDM system.

## Supported platforms

SailPoint IdentityIQ MobileIron Mobile Device Management Integration Module supports the following version of MobileIron WebService

- API version for MobileIron WebService 5.7.1

## Pre-requisites

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

**Note:** If MobileIron MDM 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 MIM (Mobile Device Management Integration 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 26: SailPoint Good Technology Mobile Device Management Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	263
Supported features . . . . .	263
Supported platform . . . . .	264
Pre-requisites . . . . .	264
Configuration . . . . .	264
Application configuration . . . . .	264
Operation specific configuration . . . . .	265

## Overview

---

This document provides a guide to the Good Technology Mobile Device Management (MDM) integration and configuration for your enterprise.

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

- Good Technology MDM Application (referred to as User Application in this document) for managing Good Technology 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 Technology MDM Integration Module supports the following features:

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

## Supported platform

---

SailPoint IdentityIQ Good Technology Mobile Device Management Integration Module supports the following version of Good Mobile:

- Good Mobile Control version 2.6.4.972

## Pre-requisites

---

Administrator user configured for Good Technology MDM 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 Technology the following parameters are required:

Parameters	Description
Application Type	Good Technology MIM (Mobile Device Management Integration 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 Technology 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 Technology Mobile Device Management Integration Module (MIM) application will create identity in IdentityIQ with Display Attribute (Device Model by default) of Good Technology.

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 Technology 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 Technology:

- 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 Technology 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"/>
```

# IT Security Integration Module

This section contains information on the following section:

- "SailPoint HP ArcSight Integration Module"



# Chapter 27: SailPoint HP ArcSight Integration Module

---

The following topics are discussed in this chapter:

Overview . . . . .	269
Supported features . . . . .	270
Supported platforms . . . . .	270
Pre-requisites . . . . .	270
Configuration . . . . .	270
Configuration to export IdentityIQ Data to ArcSight. . . . .	270
Configuration to Import HP ArcSight CEF Flat File to SailPoint IdentityIQ. . . . .	274

## Overview

---

HP ArcSight ESM 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 HP ArcSight 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 platforms

---

SailPoint HP ArcSight Integration Module supports the following versions of HP ArcSight Enterprise Security Manager:

- HP ArcSight Enterprise Security Manager version 6.9
- HP ArcSight Enterprise Security Manager version 6.8

## 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 HP ArcSight Integration Module

### 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
<b>Datasource Parameters</b>	
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"> <li>• <b>Full</b>: Exports all the records irrespective if they were exported earlier.</li> <li>• <b>Incremental</b>: 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 <b>Full</b> option.</li> </ul>

## 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"><li>• <b>Full</b>: Exports all the records irrespective if they were exported earlier.</li><li>• <b>Incremental</b>: 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 <b>Full</b> option.</li></ul>

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 sptr\_arcsight\_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 272.
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 sptr\_arcsight\_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.
application	Describes the name of application the target belongs to.

**Table 2—IdentityIQ sptr\_arcsight\_audit\_event export table**

Fields	Description
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.



# Appendix

This section contains information on the following:

- "A: Common Identity Management Integration Configuration" on page 279
- "B: Component Interface" on page 287





# Appendix A: Common Identity Management Integration Configuration

---

This appendix describes the following information.

Overview .....	279
Creating the IntegrationConfig Object .....	279
Provisioning .....	284

## 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 283 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 .....	287
Basic structure of Custom Component (CI) from USERMAINT component for Users .....	287
Basic structure of Custom Component (CI) from ROLEMAINT component for Roles. ....	293
Basic structure of Custom Component (CI) from RTE_CNTL_PROFILE component for Users .....	295
Basic structure of Custom Component (CI) from PURGE_USR_PROFILE component for Delete User ..	298
Basic structure of Component Interface (CI) from PURGE_ROLEDEFN component for Delete Role ...	300
Deleting the component interface .....	301

## 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

---

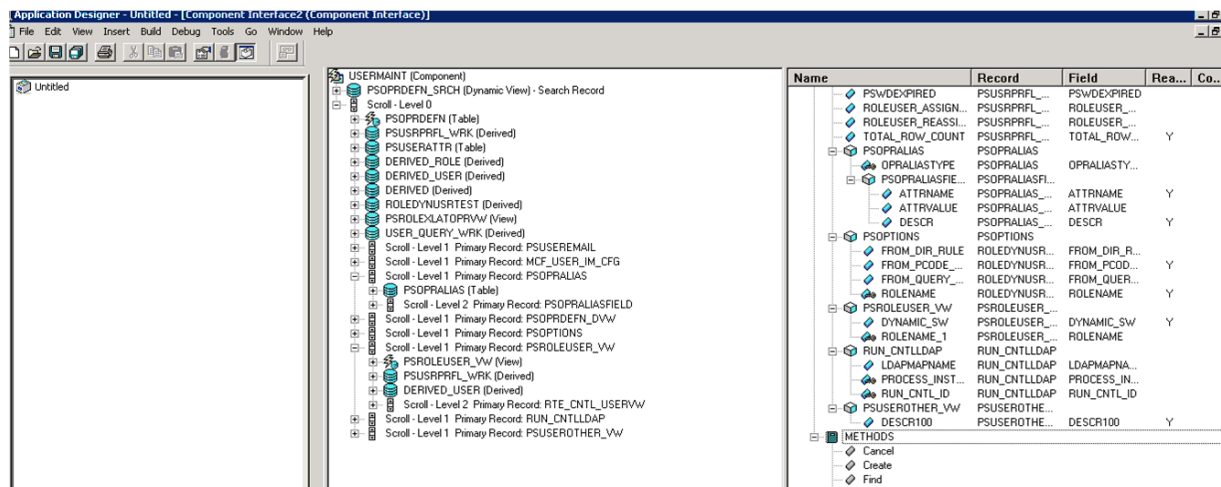
This section describes the creation of basic structure of CI from USERMAINT component, changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI, and verification of the newly created CI's.

#### 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 **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**.

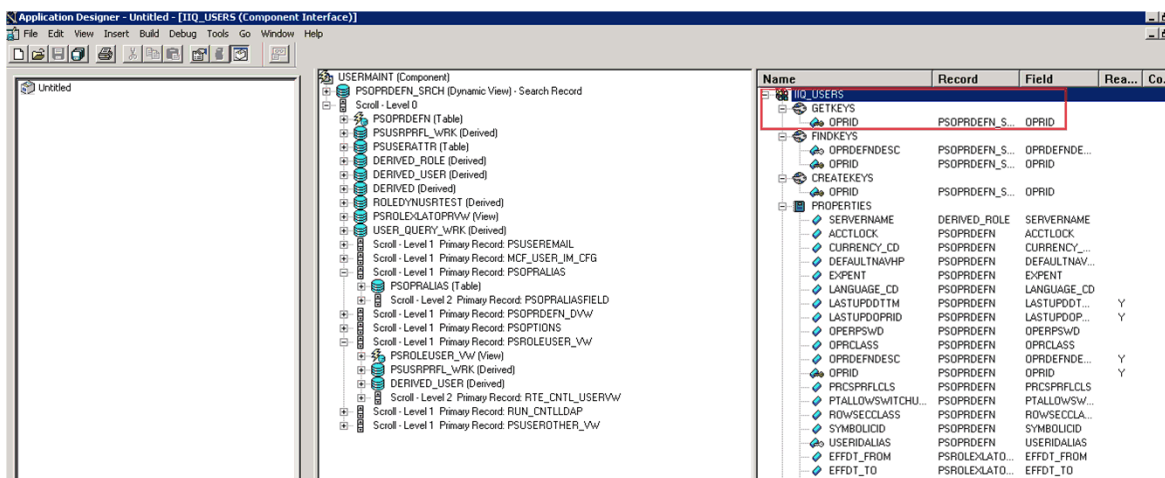
## Creating component interface for PeopleSoft

Following screen shot appears:



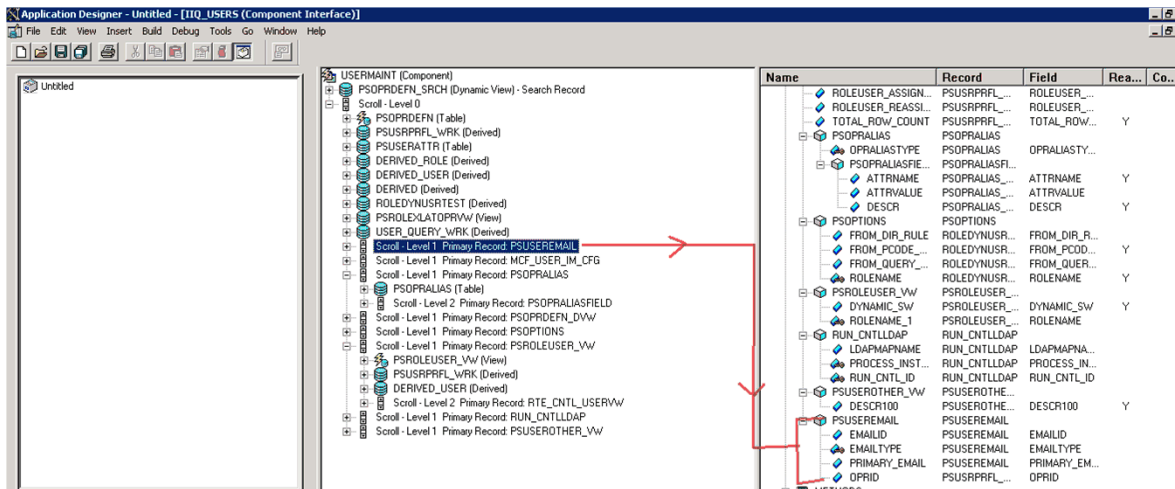
- Click on **File => Save As**.

A new dialog box appears requesting for the name of the CI as follows:

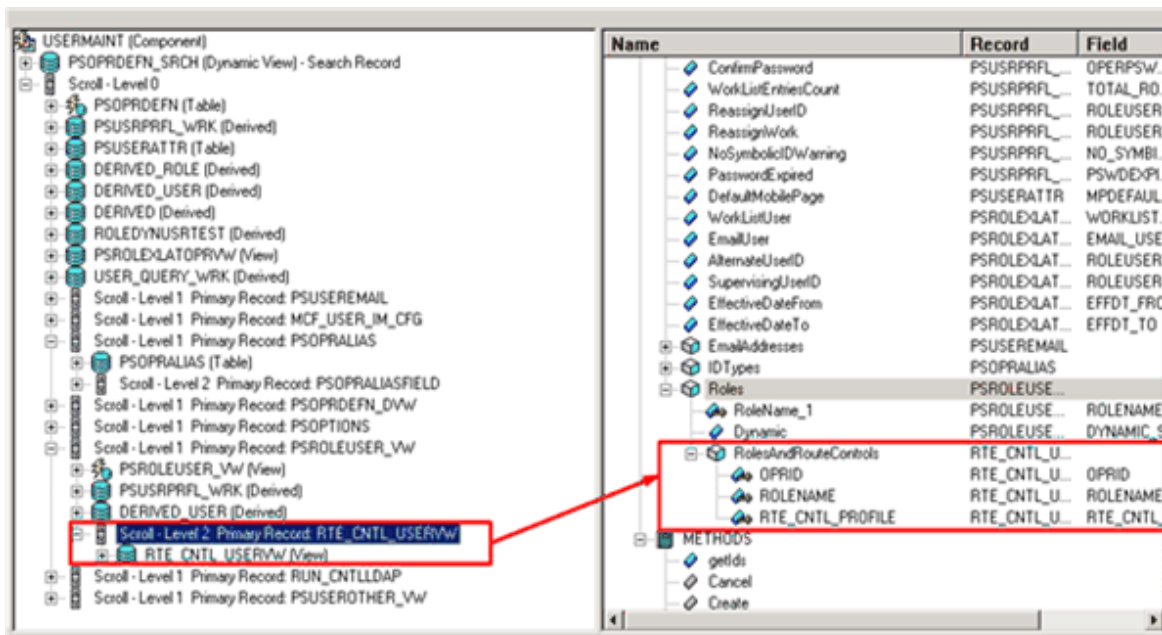


- Enter the name of the CI as **{NEW\_Name}**. For example, **IIQ\_USERS**.
- Drag the **Scroll-Level1 Primary Record: PSUSERMAIL** from source component (USERMAINT) to the properties of the newly created CI **{NEW\_Name}**. For example, **IIQ\_USERS**.

After dragging and dropping the Scroll-Level1 Primary Record: PSUSERMAIL attribute, a new property is listed in the PROPERTIES of the newly created CI.



- 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, IIQ\_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

- Expand **FINDKEYS** and click on **OPRID**. Right click on **OPRID** and select **Edit Name** to change the attribute name to **UserID**.

## Creating component interface for PeopleSoft

Name	Record	Field	Rea...	Co...
IQ_USERS				
FINDKEYS				
OPRID	PSOPRDEFN_S...	OPRID		
OPRDEFNDESC	PSOPRDEFN_S...	OPRDEFNDE...		
CREATEKEYS				
OPRID	PSOPRDEFN_S...	OPRID		
GETKEYS				
OPRID	PSOPRDEFN_S...	OPRID		
PROPERTIES				
OPRID	PSOPRDEFN	OPRID		Y
OPRDEFNDESC	PSOPRDEFN	OPRDEFNDE...		Y
OPRCLASS	PSOPRDEFN	OPRCLASS		
ROWSECCLASS	PSOPRDEFN	ROWSECCLA...		
OPERPSWD	PSOPRDEFN	OPERPSWD		
SYMBOLICID	PSOPRDEFN	SYMBOLICID		
LANGUAGE_CD	PSOPRDEFN	LANGUAGE_CD		
CURRENCY_CD	PSOPRDEFN	CURRENCY_...		
ACCTLOCK	PSOPRDEFN	ACCTLOCK		
PRCSPRFLCLS	PSOPRDEFN	PRCSPRFLCLS		
DEFAULTNAVHP	PSOPRDEFN	DEFAULTNAV...		
EXPENT	PSOPRDEFN	EXPENT		
USERIDALIAS	PSOPRDEFN	USERIDALIAS		
LASTUPDDTTM	PSOPRDEFN	LASTUPDDT...		Y
LASTUPDOPRID	PSOPRDEFN	LASTUPDOP...		Y
PTALLOWSWITCHU...	PSOPRDEFN	PTALLOWSW...		
OPERPSWDCONF	PSUSRPRFL...	OPERPSWDC...		
TOTAL_ROW_COUNT	PSUSRPRFL...	TOTAL_ROW...		Y
ROLEUSER_REASSI...	PSUSRPRFL...	ROLEUSER_...		

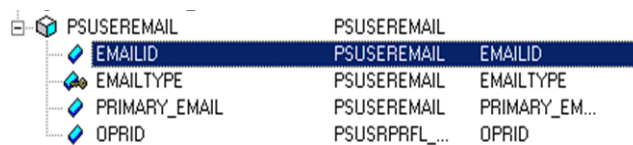
Similarly change the name of OPRDEFNDESC attribute to UserDescription.

- Expand **GETKEYS** and change the name of **OPRID** to **UserID**.
- Expand **CREATEKEYS** and change the name of **OPRID** to **UserID**.
- After changing the keys for **GETKEYS**, **FINDKEYS** and **CREATEKEYS**, change the **PROPERTIES**.
  - Changing Single attribute
    - Expand **PROPERTIES**.
    - 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

Original attribute name	Changed attribute name
TOTAL_ROW_COUNT	WorkListEntriesCount
ROLEUSER_REASSIGN	ReassignUserID
ROLEUSER_ASSIGN_SW	ReassignWork
NO_SYMBID_WARN	NoSymbolicIDWarning
PSWDEXPIRED	PasswordExpired
MPDEFAULTMP	DefaultMobilePage
WORKLIST_USER_SW	WorkListUser
EMAIL_USER_SW	EmailUser
LASTUPDOPRID	LastUpdateUserID
ROLEUSER_ALT	AlternateUserID
ROLEUSER_SUPR	SupervisingUserID
EFFDT_FROM	EffectiveDateFrom
EFFDT_TO	EffectiveDateTo
CHANGE_PWD_BTN	ChangePassword
	<b>Note: This attribute is applicable only for PeopleTools version 8.55 and above.</b>

- 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.



- 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

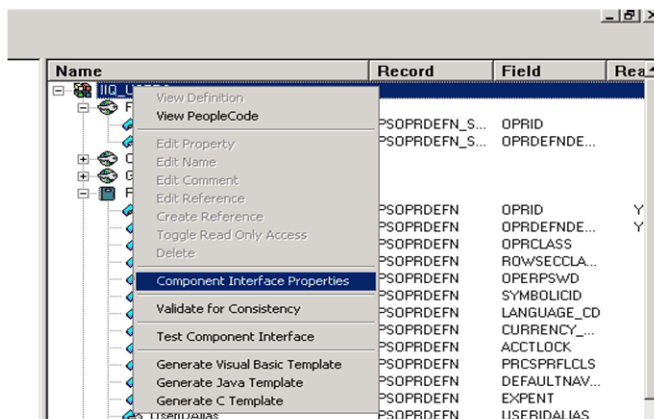
Original collection attribute name	Changed collection attribute name	Original child attribute name	Changed child attribute name
PSOPRALIAS	IDTypes	OPRALIASTYPE	IDType
		PSOPRALIASFIELD	Attributes
		ATTRNAME	AttributeName
		ATTRVALUE	AttributeValue
		DESCR	DESCR
PSROLEUSER_VW	Roles	DYNAMIC_SW	Dynamic
		ROLENAME_1	RoleName_1

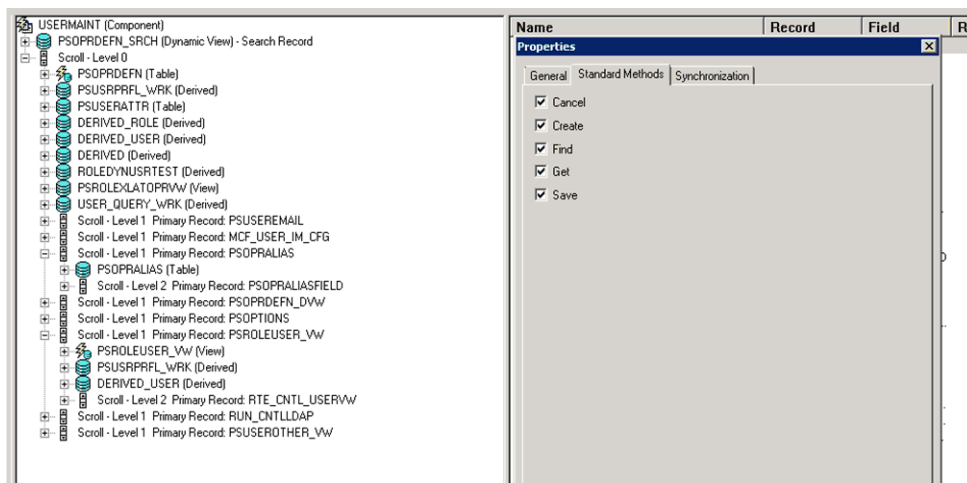
d. After renaming property attributes as mentioned in the above table, delete the following attributes:

- 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 287.
2. Verify all properties (**cancel**, **create**, **find**, **get**, **save**) are selected.





The new CI is ready to be used. For example, **IIQ\_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:

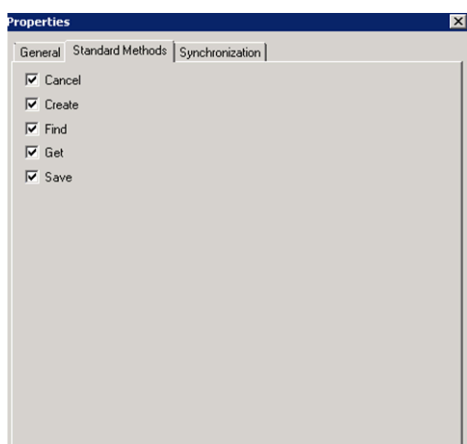
Name	Record	Field	Rea...	Co...
GETKEYS	PSROLEDEFN...	ROLENAME		
FINDKEYS	PSROLEDEFN...	DESCR		
CREATEKEYS	PSROLEDEFN...	ROLENAME		
PROPERTIES	PSROLEDEFN...	ROLENAME		
USERID	DERIVED_DYN...	USERID		
DESCR	DERIVED_ROLE	DESCR	Y	
SERVERNAME	DERIVED_ROLE	SERVERNAME		
ALLOWLOOKUP	PSROLEDEFN	ALLOWLOOK...		
ALLOWNOTIFY	PSROLEDEFN	ALLOWNOTIFY		
DESCR_0	PSROLEDEFN	DESCR		
FIELDNAME	PSROLEDEFN	FIELDNAME		
LASTUPDDTTM	PSROLEDEFN	LASTUPDDT...	Y	
LASTUPDOPRID	PSROLEDEFN	LASTUPDOP...	Y	
LDAP_RULE_ON	PSROLEDEFN	LDAP_RULE...		
PC_EVENT_TYPE	PSROLEDEFN	PC_EVENT_T...		
PC_FUNCTION_NAME	PSROLEDEFN	PC_FUNCTION...		
QRYNAME	PSROLEDEFN	QRYNAME		
QRYNAME_SEC	PSROLEDEFN	QRYNAME_S...		
RECNAM	PSROLEDEFN	RECNAM		
ROLENAME	PSROLEDEFN	ROLENAME	Y	
ROLETYPE	PSROLEDEFN	ROLETYPE		
ROLE_PCODE_RUL...	PSROLEDEFN	ROLE_PCOD...		
ROLE_QUERY_RUL...	PSROLEDEFN	ROLE_QUER...		
ROLEUSER	PSUSRPRFL...	ROLEUSER		

- 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, **IIQ\_ROLES**.
- Delete the following collective attributes:
  - PSOPTIONS
  - RUN\_CNTLLDAP

PC_EVENT_TYPE	PSROLEDEFN	PC_EVENT_T...
QRYNAME_SEC	PSROLEDEFN	QRYNAME_S...
PC_FUNCTION_NAME	PSROLEDEFN	PC_FUNCTION...
ROLE_PCODE_RUL...	PSROLEDEFN	ROLE_PCOD...
ROLE_QUERY_RUL...	PSROLEDEFN	ROLE_QUER...
LDAP_RULE_ON	PSROLEDEFN	LDAP_RULE...
ALLOWNOTIFY	PSROLEDEFN	ALLOWNOTIFY
ALLOWLOOKUP	PSROLEDEFN	ALLOWLOOK...
LASTUPDDTTM	PSROLEDEFN	LASTUPDDT...
LASTUPDOPRID	PSROLEDEFN	LASTUPDOP...
SERVERNAME	DERIVED_ROLE	SERVERNAME
DESCR	DERIVED_ROLE	DESCR
ROLEUSER	PSUSRPRFL...	ROLEUSER
USERID	DERIVED_DYN...	USERID
PSROLECLASS	PSROLECLASS	
PSOPTIONS	PSOPTIONS	
RUN_CNTLLDAP	RUN_CNTLLDAP	
PSROLECANGRANT	PSROLECAN...	
PSROLEGRANTORVW	PSROLEGRAN...	
PSROLEOTHER_VW	PSROLEOTHE...	

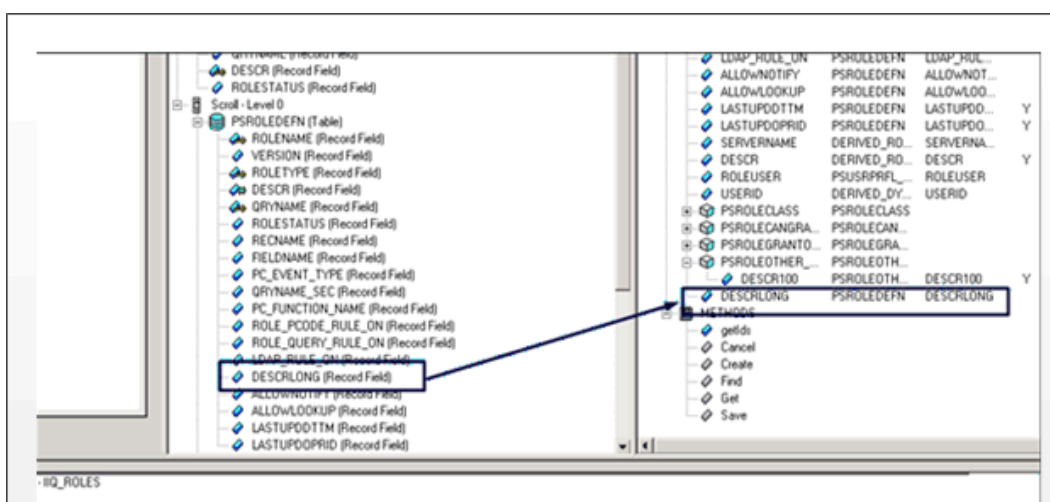
- Verification of the standard methods are selected for this newly created component Interface. For example, **IIQ\_ROLES**.





The newly created component interface is ready to be used. For example, **IIQ\_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**.

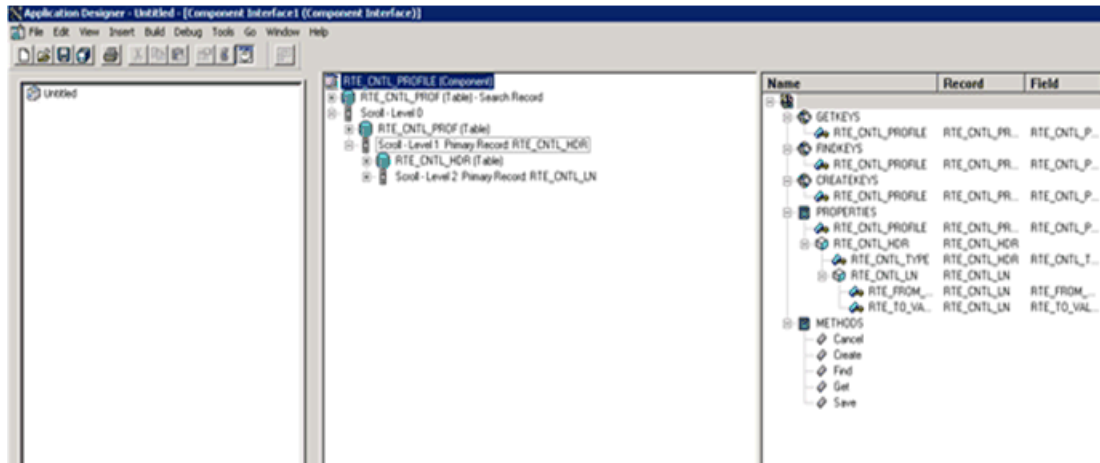
## Creating component interface for PeopleSoft

A dialog box appears with the following message:

Do you want to default the properties based on the underlying component definition

4. Click **Yes**.

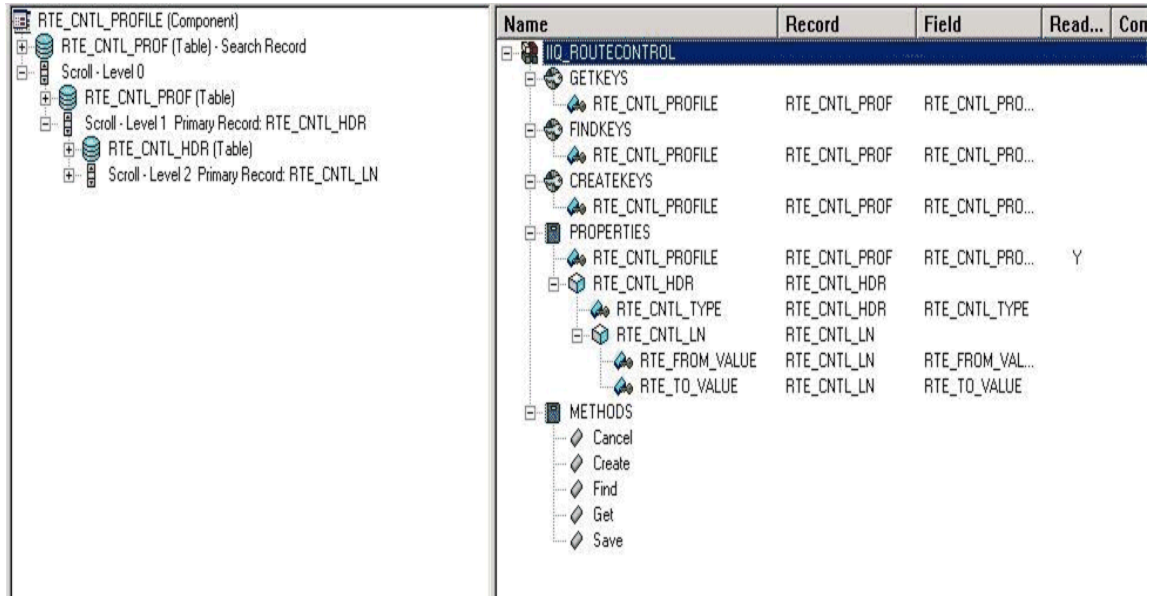
Following screen shot appears:



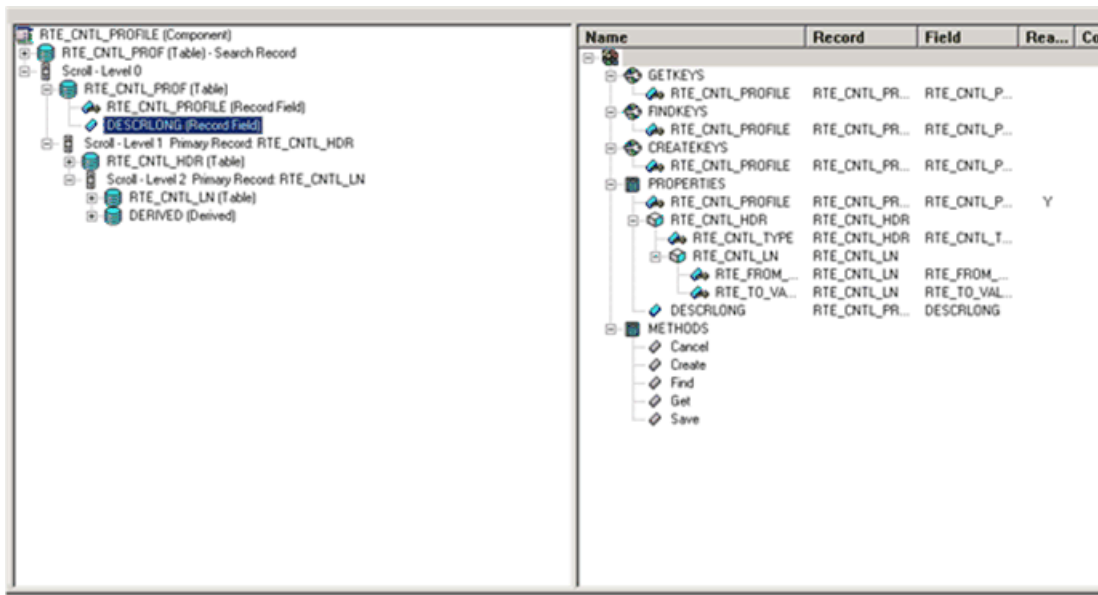
5. Click on **File => Save As**.

A new dialog box appears requesting for the name of the CI.

6. Enter the name of the CI as **{NEW\_NAME}**. For example, **IIQ\_ROUTECONTROL**.

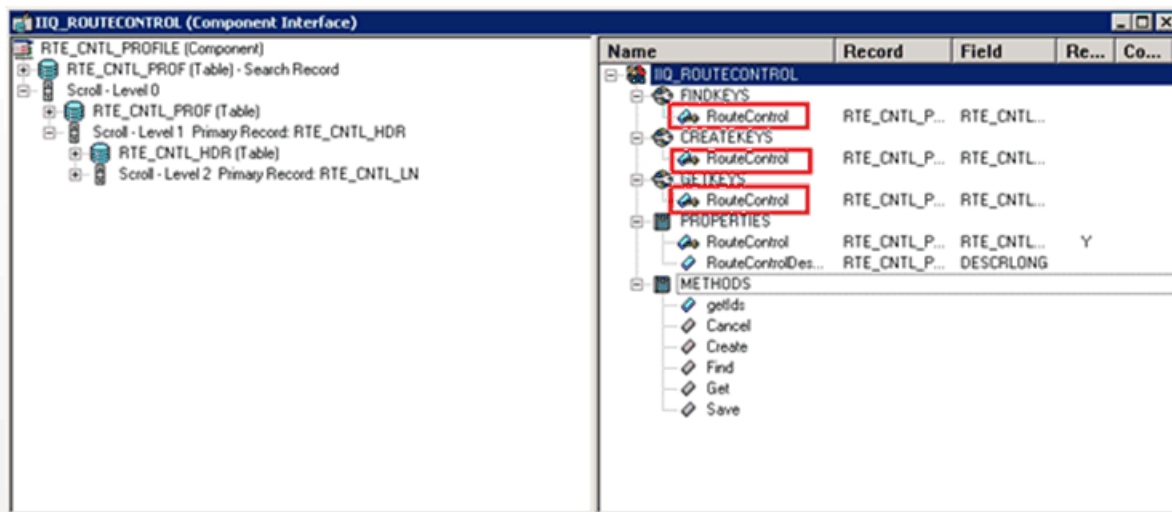


7. Drag the **Scroll-Level 0 : DESCRLONG (Record Field)** from source component (IIQ\_RTE\_CNTL\_PRF\_CI) to the properties of the newly created CI **{NEW\_Name}**. For example, **IIQ\_ROUTECONTROL**.



## 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**.



Similarly change the name of **DESCRLONG** attribute to **RouteControlDescription**.

2. Expand **GETKEYS** and click on **RTE\_CNTL\_PROFILE**. Right click on **RTE\_CNTL\_PROFILE** and select edit name to change the attribute name to **RouteControl**.
3. Expand **CREATEKEYS** and click on **RTE\_CNTL\_PROFILE**. Right click on **RTE\_CNTL\_PROFILE** and select edit name to change the attribute name to **RouteControl**.

## Creating component interface for PeopleSoft

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:

Key	Original attribute name	Changed attribute name
GETKEYS	RTE_CNTL_PROFILE	RouteControl
FINDKEYS	RTE_CNTL_PROFILE	RouteControl
CREATEKEYS	RTE_CNTL_PROFILE	RouteControl
PROPERTIES	RTE_CNTL_PROFILE	RouteControl

- c. Delete the **RTE\_CNTL\_HDR** collection.

The screenshot displays the PeopleSoft Application Designer interface. On the left, the component structure for **RTE\_CNTL\_PROFILE (Component)** is shown, including tables like **RTE\_CNTL\_PROF**, **RTE\_CNTL\_PROFILE**, **RTE\_CNTL\_HDR**, and **RTE\_CNTL\_LN**. On the right, a table lists the attributes for the **IIQ\_ROUTECONTROL** component. The **RTE\_CNTL\_HDR** attribute is highlighted in blue.

Name	Record	Field	Read...	Com...
IIQ_ROUTECONTROL				
GETKEYS	RTE_CNTL_PROF	RTE_CNTL_PROF...		
FINDKEYS	RTE_CNTL_PROF	RTE_CNTL_PROF...		
CREATEKEYS	RTE_CNTL_PROF	RTE_CNTL_PROF...		
PROPERTIES	RTE_CNTL_PROF	RTE_CNTL_PROF...	Y	
<b>RTE_CNTL_HDR</b>	<b>RTE_CNTL_HDR</b>			
RTE_CNTL_TYPE	RTE_CNTL_HDR	RTE_CNTL_TYPE		
RTE_CNTL_LN	RTE_CNTL_LN			
RTE_FROM_VALUE	RTE_CNTL_LN	RTE_FROM_VALUE		
RTE_TO_VALUE	RTE_CNTL_LN	RTE_TO_VALUE		
RouteControlDescription	RTE_CNTL_PROF	DESCRLONG		
METHODS				
Cancel				
Create				
Find				
Get				
Save				

## 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, **IIQ\_DEL\_USER**

### 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.

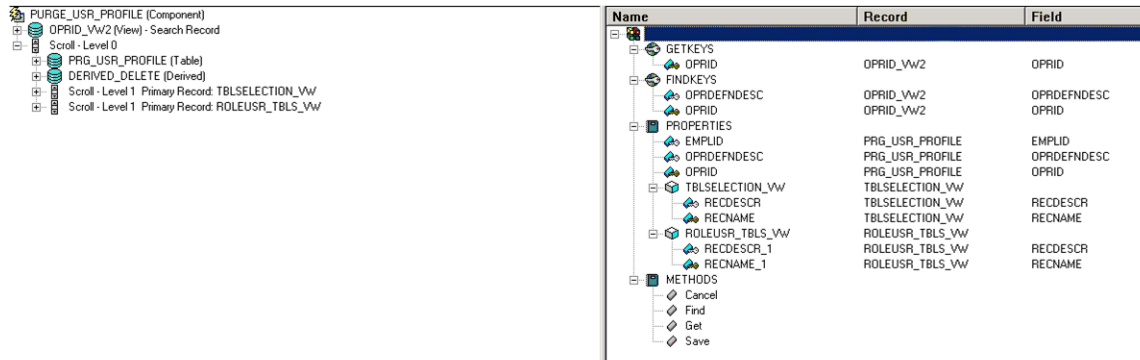
- Enter the name as **PURGE\_USR\_PROFILE** under the **Selection Criteria** tab and click **Select**.

A dialog box appears with the following message:

Do you want to default the properties based on the underlying component definition

- Click **Yes**.

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, **IIQ\_DEL\_USER**.

Delete the following collective attributes:

- TBLSELECTION\_VW
- ROLEUSR\_TBLS\_VW

## Changing GETKEYS, FINDKEYS and CREATEKEYS for the newly created CI

- 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**.

- Expand **GETKEYS** and change the name of **OPRID** to **UserID**.

- After changing the keys for **GETKEYS** and **FINDKEYS** change the **PROPERTIES**.

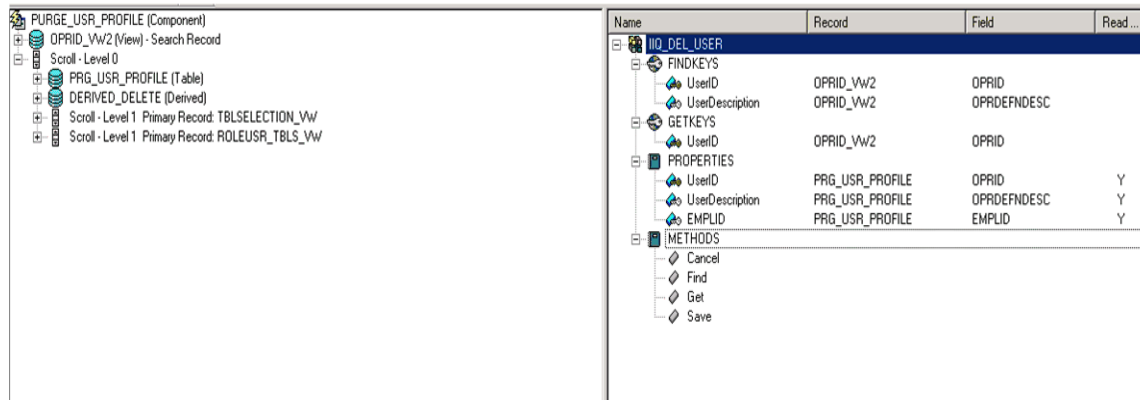
- Changing Single attribute

- Expand **PROPERTIES**.
- 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

## Creating component interface for PeopleSoft

After the changes the CI would appear as follows:



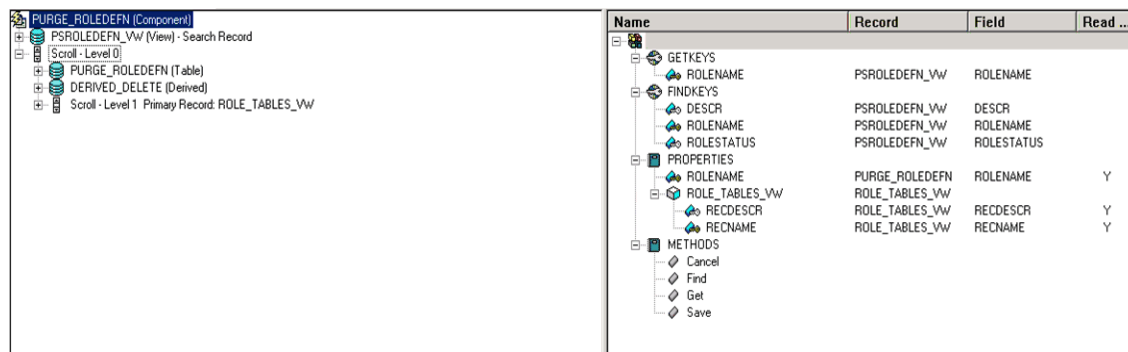
Name	Record	Field	Read...
<b>IIQ_DEL_USER</b>			
FINDKEYS			
UserID	OPRID_VW2	OPRID	
UserDescription	OPRID_VW2	OPRDEFNDESC	
GETKEYS			
UserID	OPRID_VW2	OPRID	
PROPERTIES			
UserID	PURGE_USR_PROFILE	OPRID	Y
UserDescription	PURGE_USR_PROFILE	OPRDEFNDESC	Y
EMPLID	PURGE_USR_PROFILE	EMPLID	Y
METHODS			
Cancel			
Find			
Get			
Save			

## 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, **IIQ\_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:



Name	Record	Field	Read...
<b>PURGE_ROLEDEFN</b>			
GETKEYS			
ROLENAME	PSROLEDEFN_VW	ROLENAME	
FINDKEYS			
DESCR	PSROLEDEFN_VW	DESCR	
ROLENAME	PSROLEDEFN_VW	ROLENAME	
ROLESTATUS	PSROLEDEFN_VW	ROLESTATUS	
PROPERTIES			
ROLENAME	PURGE_ROLEDEFN	ROLENAME	Y
METHODS			
ROLE_TABLES_VW	ROLE_TABLES_VW	RECDESCR	Y
RECNAME	ROLE_TABLES_VW	RECNAME	Y
Cancel			
Find			
Get			
Save			

5. Click on **File => Save As**.

A new dialog box appears requesting for the name of the CI.

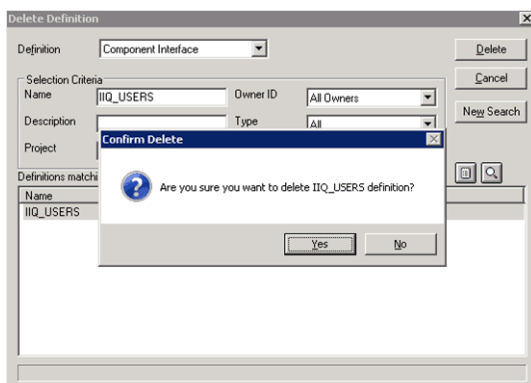
6. Enter the name of the CI as **{NEW\_NAME}**. For example, **IIQ\_DEL\_ROLE**.  
Delete the **ROLE\_TABLES\_VW** collective attribute.
7. Click **Save**.

## 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.

## Deleting the component interface