SailPoint IdentityAI

Implementation Guide

IdentityIQ Introduction

SailPoint IdentityIQ 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.

IdentityAI – Integrating IdentityAI within IdentityIQ enables the delivery of Predictive Identity. IdentityAI is a rule based machine learning engine using identity graph technology to provide recommendations for access review and access request decisions. With IdentityAI enabled, you can also review access history for identity cubes, create dashboards that can be customized from an administrative perspective, and view peer groups within the IdentityAI user interface.

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 IdentityIQ 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.

Implement SailPoint IdentityAI

IdentityAI is a SaaS-delivered data analysis product designed to work with SailPoint products, IdentityIQ and IdentityNow. The goal is to improve your identity governance process through data analysis and machine learning.

Use this document to integrate with IdentityIQ.

Integrate SailPoint IdentityAI

Note: Plugins must be enabled in IdentityIQ for IdentityAI to install. Ensure that plugins.enabled=true in the WEB-INF/classes/iiq.properties file of your installation.

Use the following information to integrate SailPoint IdentityAI with IdentityIQ.

1. Log on to your instance of IdentityIQ as an administrator.
2. Click on Global Settings under the gear icon and select the Import from File Page.
3. Click **Browse** and browse to the following directory:
   identityiq_home`\WEB-INF\config`
   where *identityiq_home* is the directory in which you extracted the identityiq`.war` file during the IdentityIQ installation procedure.
4. Select the `init-ai.xml` file and click **Import**.
5. When the import is complete, click **Done**.

The IdentityAI Recommender Plugin is now installed and the SailPoint IdentityAI features are available in the IdentityIQ product. To configure and enable IdentityAI and its features, see “IdentityAI Configuration” on page 3, “Enable IdentityAI for Access Request Approvals” on page 4, and "Enable IdentityAI for Certifications" on page 4.

IdentityAI Configuration

Use the IdentityAI Configuration page to connect IdentityIQ to the IdentityAI product. From the gear icon, select **Global Settings -> IdentityIA Configuration**.

Table 1— IdentityAI Congiguration Page Field Descriptions

Field	Description
Connection Information for IdentityAI:	
IdentityAI Hostname	The host name of the IdentityAI recommendation API
Client ID	OAuth client ID for the IdentityAI recommendation API
Client Secret	OAuth client secret for the IdentityAI recommendation API
Advanced:	
Read Timeout	The number of seconds IdentityIQ will wait to read recommendations from IdentityAI before reporting a failure

Table 1— IdentityAI Congiguration Page Field Descriptions

Field	Description
Connect Timeout	The number of seconds IdentityIQ will wait to connect to IdentityAI before reporting a failure

Use **Test Connection** to ensure the connection information is accurate and operating.

Save your settings before leaving the page.

Enable IdentityAI for Access Request Approvals

Note: This option is not available before init-ai.xml is imported into IdentityIQ.

Note: IdentityAI is enabled by default when init-ai.xml is imported

IdentityAI must be enabled to work with Lifecycle Manager in order to generate recommendations for access request approvals.

1. Login as an IdentityIQ administrator
2. Under the gear icon select **Lifecycle Manager**
3. **Enable the generation of IdentityAI recommendations for approvals** in the IdentityAI Approval Recommendation section of the Configure tab
4. **Save** your changes

Enable IdentityAI for Certifications

Note: This option is not available before init-ai.xml is imported into IdentityIQ.

Note: IdentityAI is enabled by default when init-ai.xml is imported

Note: Items automatically marked as approved still require a physical sign off to complete the certification

IdentityAI must be enabled to work with certifications in IdentityIQ. Recommendations can be applied to all applicable certification types, or to an individual certification as required.

To set the default for all applicable certifications.

1. Login as an IdentityIQ administrator
2. Under the gear icon select **Compliance Manager**
3. Select **Show Recommendation** in the Decisions section of access reviews
4. Select **Automatically Approve Recommended Items** to automatically mark access review items as approved and move them from the Open to the Review tab of the access review
5. **Save** your changes

To change the default setting on an individual certification, refer to the *SailPoint IdentityIQ User's Guide* for information on scheduling specific certification types.

IdentityAI Status

Use the SailPoint Modules and Extensions page of the Administrator Console to view the status of IdentityAI.

1. Login as an IdentityIQ administrator
2. Under the gear icon select **Administrator Console**
3. From the Environment table, open the SailPoint Modules and Extensions tab
4. View the current status of the IdentityAI connection or click on the module name to see the status of IdentityAI connections for each host

IdentityAI Reports

IdentityAI recommendation information is included in the following IdentityIQ reports:

- Access Review Decision Report — the Roles table for this report intentionally does not contain the recommendation columns
- Manager Access Review Live Report
- Application Owner Access Review Live Report
- Advanced Access Review Live Report
- Role Membership Access Review Live Report
- Targeted Access Review Live Report
- Certification Activity by Application Live Report

The following columns are included in these access review and certification reports. In live reports, the columns function the same as the other IdentityIQ columns on the Report Layout tab.

Note: These columns are always blank on Policy Violation tables, recommendations are not evaluated for policy violations

- Recommended Decision
- Recommendation Timestamp
- Recommendation Reasons
- Auto Decision Generated
- Auto Decision Accepted

For request types that are not supported by recommendation, the reports return the following:

- **Recommendation** — Not Consulted
- **Recommendation Timestamp** — blank column
- **Recommendation Reasons** — The recommender in use does not support recommendations for this work item type
- **Auto Decision Generated** — False
- **Auto Decision Accepted** — False

If a recommendation is not found for a line item, the report returns the following:

- **Recommendation** — Not Found
- **Recommendation Reasons** — We do not have a recommendation for this access because the identity was not found within IdentityAI
- **Recommendation timestamp** — the timestamp
- **Auto Decision Generated** — False
- **Auto Decision Accepted** — False

IdentityAI IdentityIQ Console Commands

Use the IdentityIQ console to view the status of your recommender or disable recommendations for this IdentityIQ installation.

The following commands are available in the IdentityIQ console after `init-ai.xml` is imported:

- **reco list** — a list of all recommender definitions and their status, In Use, Available, or Unavailable
- **reco use <Recommender_Name>** — the name of the recommender to use. If the recommender name contains white spaces, include quotation marks, “Recommender Name”
- **reco use --** — disable and clear the recommender selection