SailPoint IdentityIQ

SailPoint IdentityAI Implementation Guide

This document and the information contained herein is SailPoint Confidential Information.

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

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

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

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

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

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

"SailPoint Technologies & Design," "SailPoint," "IdentityIQ," "IdentityNow," "SecurityIQ," "AccessIQ," "Identity Cube" and "Managing the Business of Identity" are registered trademarks of SailPoint Technologies, Inc. "IdentityAI," "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.

Implement SailPoint IdentityAI

IdentityAI is a SaaS-delivered data analysis product designed to work with SailPoint products, IdentityIQ, IdentityNow, and SecurityIQ. 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 1, “Enable IdentityAI for Access Request Approvals” on page 2, and "Enable IdentityAI for Certifications" on page 2.

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

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
4. **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

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.

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

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