SailPoint® | IdentityIQ®

AI Services

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, 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.

Patents Notice. https://www.sailpoint.com/patents

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. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; 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.

Contents

About SailPoint AI Services

SailPoint's™ AI Services is a SaaS-delivered data analysis product designed to work with IdentityIQ and IdentityNow. The goal of AI Services is to improve your identity governance process through data analysis and machine learning.

Integrating AI Services with IdentityIQ helps your organization determine who should have access to what. AI Services uses peer group analysis and identity attributes to recommend access to your users, and to help certifiers decide when user access should be approved or denied. AI Services can also identify user access patterns to determine potential roles that accurately align with what users actually do in an organization.

Decision Recommendations

AI Services can be configured to give decision recommendations to the people performing access reviews and approving access requests. This can help them make more informed decisions about the access they are granting.

For example, an access reviewer may not be entirely familiar with what item in the access review is. The AI Services integration can provide recommendations to display in IdentityIQ about whether the access should be granted or not. AI Services can provide two types of recommendations - a thumbs up indicating Recommended, or a thumbs down indicating Not Recommended - or not provide any recommendation at all.

Users can also filter recommendations by type, making it easy to review all items with the same recommendation status, together.

Decision recommendations can be enabled both globally, and at the individual certification level. See Enabling Recommendations and Automatic Approvals Globally for Certifications for details on how to enable automatic approvals globally.

Automatic Approvals

You can use AI Services to automatically approve access based on recommendations. With this feature enabled, any access review item that has a recommendation of "thumbs up" is automatically moved from the reviewer's **Open** tab to the **Review** tab, with an "Approved" decision. Reviewers retain the option of changing the automated decision, as needed, before signing off on the review. Automated approvals help your reviewers process access reviews quickly and more efficiently by taking easy decisions out of the way so that they can focus on exceptional items.

Automated approvals can be enabled both globally, and at the individual certification level. See Enabling Recommendations and Automatic Approvals Globally for Certifications for details on how to enable automatic approvals globally.

Access Modeling

SailPoint's AI Services includes an Access Modeling service which uses patented machine learning algorithms to identify user access patterns and determine potential roles that accurately align with what users actually do in an organization.

In IdentityIQ, AI Services Access Modeling gives you the option to use this service for role discovery, to display potential roles based on the optimal role granularity derived from AI Services algorithms.

The Access Modeling feature is an optional integration that you can install as a plugin as part of your AI Services integration. For more information, see the Plugins documentation.

Integrating SailPoint AI Services

> Plugins must be enabled in IdentityIQ for AI Services to be installed. Ensure that `plugins.enabled=true` in the `identityiq_home/WEB-INF/classes/iiq.properties` file of your installation.

Prerequisites for Integrating AI Services

Because SailPoint's AI Services are a part of IdentityNow, you will need a connection to an IdentityNow tenant to integrate AI Services with IdentityIQ. You can read about AI Services prerequisites, the onboarding process, and deployment steps at Getting Started with SailPoint AI Services.

Importing the AI Services Integration File

Begin your implementation of SailPoint AI Services in IdentityIQ by importing the AI Services `init-ai.xml` file into IdentityIQ:

1. Log in to IdentityIQ as an administrator.
2. Click the **gear** icon > **Global Settings > Import from File**.
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**.

This process enables AI Services and installs the AI Services Recommender Plugin into your IdentityIQ instance.

Configuring AI Services

Use the AI Services Configuration page to connect IdentityIQ to AI Services. From the **gear** icon, select **Global Settings > AI Configuration**. Note that the AI Configuration option does not appear in the Global Settings page until you have completed the steps in Integrating SailPoint AI Services.

> **Websphere and IBM JDK**: Connections to AI Services using the IBM JDK require a JVM argument to support TLS version 1.2. If you deploy IdentityIQ on WebSphere, or other application servers using the IBM JDK, you must specify the JVM argument `-Dcom.ibm.jsse2.overrideDefaultTLS=true` for your Java process. To do this in WebSphere, add the JVM argument to the Generic JVM arguments at: **Servers > Java** and **Process Management > Process Definition > Java Virtual Machine > Generic JVM** arguments.

For general information on getting started with AI Services, see Getting Started with SailPoint AI Services.

Connection Information for AI Services

AI Services Hostname

The host name of the AI Services recommendation API.
For example, `https://<org>.api.identitynow.com`

Client ID

OAuth client ID for the AI Services recommendation API. See Generating Client Credentials in Your IdentityNow Tenant for details on how to generate this credential.

Client Secret

OAuth client secret for the AI Services recommendation API. See Generating Client Credentials in Your IdentityNow Tenant for details on how to generate this credential.

Advanced

Read Timeout

The number of seconds IdentityIQ will wait to read recommendations from AI Services before reporting a failure.

Connect Timeout

The number of seconds IdentityIQ will wait to connect to AI Services before reporting a failure.

Testing Your Connection

Once your configuration details have been entered, you can click **Test Connection** to verify that the connection information is accurate and operating.

If you are using an HTTP or HTTPS proxy for IdentityIQ’s communications, and you want to make an exception for connecting to AI Services, you can configure your AI Services connection to bypass the proxy connection by adding this key to the **IdentityAIConfiguration** object:

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

Save your settings before leaving the page.

Enabling Recommendations for Access Request Approvals

> This option is not available until `init-ai.xml` is imported into IdentityIQ and a connection to AI Services is configured.

AI Services can make recommendations for decisions on access requests. This feature must be enabled in your Lifecycle Manager settings, in order to generate recommendations for access request approvals.

1. Log in as an IdentityIQ administrator.
2. Under the **gear** icon select **Lifecycle Manager**.
3. In the **AI Services Approval Recommendation** section of the Configure tab, check the **Enable the generation of AI Services recommendations for approvals** option.
4. **Save** your changes.

After this option is enabled, your access reviewers can see decision recommendations when they review access requests. See the **Lifecycle Manager** documentation for more information.

Enabling Recommendations and Automatic Approvals Globally for Certifications

> This option is not available until `init-ai.xml` is imported into IdentityIQ and a connection to AI Services is configured.

AI Services can provide decision recommendations during the access certification process, and can also make automatic approvals. Recommendations and automatic approvals can be enabled globally for *all* applicable certification types, or can be enabled at the individual certification level.

> Items automatically marked as approved still require a reviewer's sign-off to complete the certification. Reviewers retain the option of changing the automated decision, as needed, before signing off on the review.

To set a global default for all applicable certifications

1. Log in as an IdentityIQ administrator.
2. Under the **gear** icon select **Compliance Manager**.
3. In the **Decisions** section, check the **Show Recommendations** option.
4. If you want to automatically mark access review items as approved and move them from the Open to the Review tab of the access review, check the **Automatically Approve Recommended Items** option. When you enable automatic approvals, your reviewers will still have the opportunity to review and, if needed, change decisions before their final sign-off on the access review.
5. **Save** your changes.

To change the default setting on an individual certification, see the **Certifications and Access Reviews** documentation.

After this option is enabled, your certifiers can see decision recommendations when they perform access reviews.

Enabling Automatic Approvals in Individual Certifications

You can use automatic approvals in these types of certification:

- Targeted
- Manager
- Application Owner
- Advanced
- Role Membership

> **Important**: Exercise caution when **staging** certifications that have automatic approvals enabled. If you include a staging period with a certification that has automatic approvals enabled, then later disable either recommendations or automatic approvals, items that were flagged for automatic approval during staging will lose the starred automatically-approved icon, but will remain approved and will still show initially on the reviewer's Review tab rather than the Open tab.

To enable automatic approvals in **Targeted** certifications:

1. Click **Setup > Certifications**
2. Click **New Certification > Targeted**
3. In the **Additional Settings** section, click **Advanced Options**
4. Select both the **Show Recommendations** and **Automatically Approve Recommended Items** boxes
5. Set the rest of your certification parameters as needed, and schedule the certification

To enable automatic approvals in all other supported certification types:

1. Click **Setup > Certifications**
2. Click **New Certification** and choose one of the certification types that supports automatic approvals (Manager, Advanced, Role Membership, or Application Owner)
3. On the **Behavior** tab, select both the **Show Recommendations** and **Automatically Approve Recommended Items** boxes
4. Set the rest of your certification parameters as needed, and schedule the certification

Enabling Access Modeling

SailPoint's AI Services includes an Access Modeling service which uses patented machine learning algorithms to identify user access patterns and determine potential roles that accurately align with what users actually do in an organization.

In IdentityIQ, AI Services Access Modeling gives you the option to use this service for role discovery, to display potential roles based on the optimal role granularity derived from AI Services algorithms.

The Access Modeling feature is an *optional* integration that you can install as a plugin as part of your AI Services integration.

For more information, see the **IdentityIQ Plugins** documentation.

Prerequisites for Access Modeling

To use Access Modeling for role discovery:

- AI Services must be integrated into your IdentityIQ instance. See Integrating SailPoint AI Services for details.
- Plugins must be enabled in your IdentityIQ instance. To enable plugins, ensure that the `<identityiq_home>/WEB-INF/classes/iiq.properties` file of your IdentityIQ installation includes the `plugins.enabled=true` setting.

You can read about AI Services prerequisites, the onboarding process, and deployment steps at Getting Started with SailPoint AI Services.

Installing the Access Modeling Plugin

Follow these steps to install the Access Modeling plugin. You can read more about Access Modeling prerequisites and features in Access Modeling.

1. Download the **Access Modeling** plugin from the IdentityIQ Plugins area of Compass.
2. Log in to IdentityIQ as an administrator.
3. From the IdentityIQ **gear** icon, select **Plugins**.
4. Click **New**, then browse to or drag and drop the plugin zip file to install the plugin.
5. Click the **Configure** button for the Access Modeling plugin and enter the URL for the IdentityNow tenant. For example: `https://<tenant>.identitynow.com`

Using Access Modeling for Role Discovery in Advanced Analytics

After the Access Modeling plugin is installed and configured, you can use it to explore potential roles based on users' current roles, and create new roles that align with the access users need.

1. Click **Intelligence > Advanced Analytics.**
2. In the **Search Type** field, make sure **Identity** is selected.
3. Enter search criteria as needed, to find the identities you want to discover roles for, and click **Run Search**.
4. Select the identity or identities to discover roles for.
5. Click **Role Discovery** to discover potential roles based on the optimal role granularity derived from our AI algorithms.
6. You will be redirected to the Access Modeling page in IdentityNow, using the URL that you configured in the Access Modeling plugin. If you are not already logged in to IdentityNow, you will have to enter admin credentials and authenticate.

7. For next steps on using IdentityNow for role discovery, see Access Modeling in the SailPoint Identity Services documentation.

Monitoring AI Services Status

You can use the SailPoint Modules and Extensions page of the Administrator Console to view the status of AI Services.

1. Log in as an IdentityIQ administrator
2. Under the **gear** icon select **Administrator Console**
3. Click the **Environment** item in the menu bar on the left
4. Click the **SailPoint Modules and Extensions** tab
5. On this tab you can view the current status of the AI Services connection, and can click on the module name to see the status of AI Services connections for each host

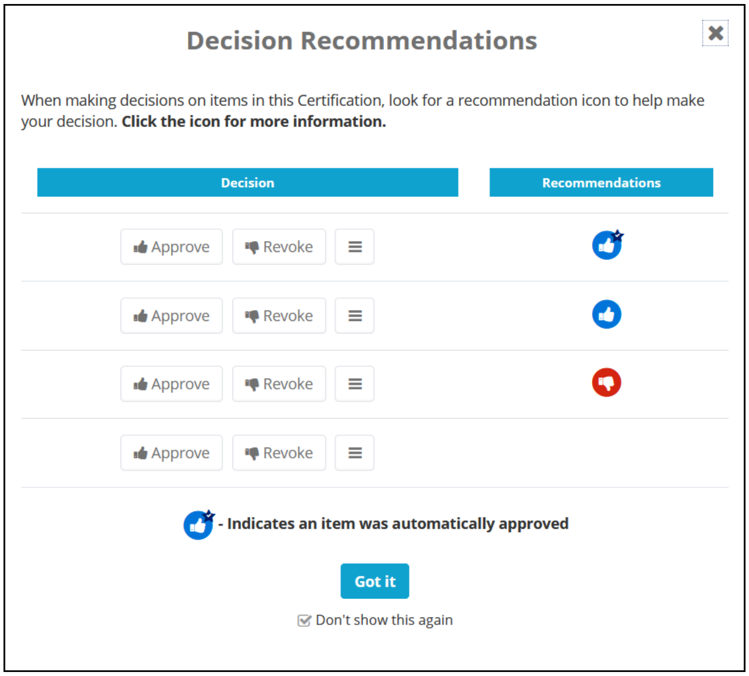
Using Automatic Approvals

You can use AI Services to automatically approve access based on recommendations. With this feature enabled, any access review item that has a recommendation of "thumbs up" is automatically moved from the reviewer's **Open** tab to the **Review** tab, with an "Approved" decision. Reviewers retain the option of changing the automated decision, as needed, before signing off on the review. Automated approvals help your reviewers process access reviews quickly and more efficiently by taking easy decisions out of the way so that they can focus on exceptional items.

Automated approvals can be enabled both globally, and at the individual certification level. See Enabling Recommendations and Automatic Approvals Globally for Certifications for details on how to enable automatic approvals globally.

How Automatic Approvals Work

The icon for Auto Approved Recommendations is the standard "thumbs up" icon, with a star.



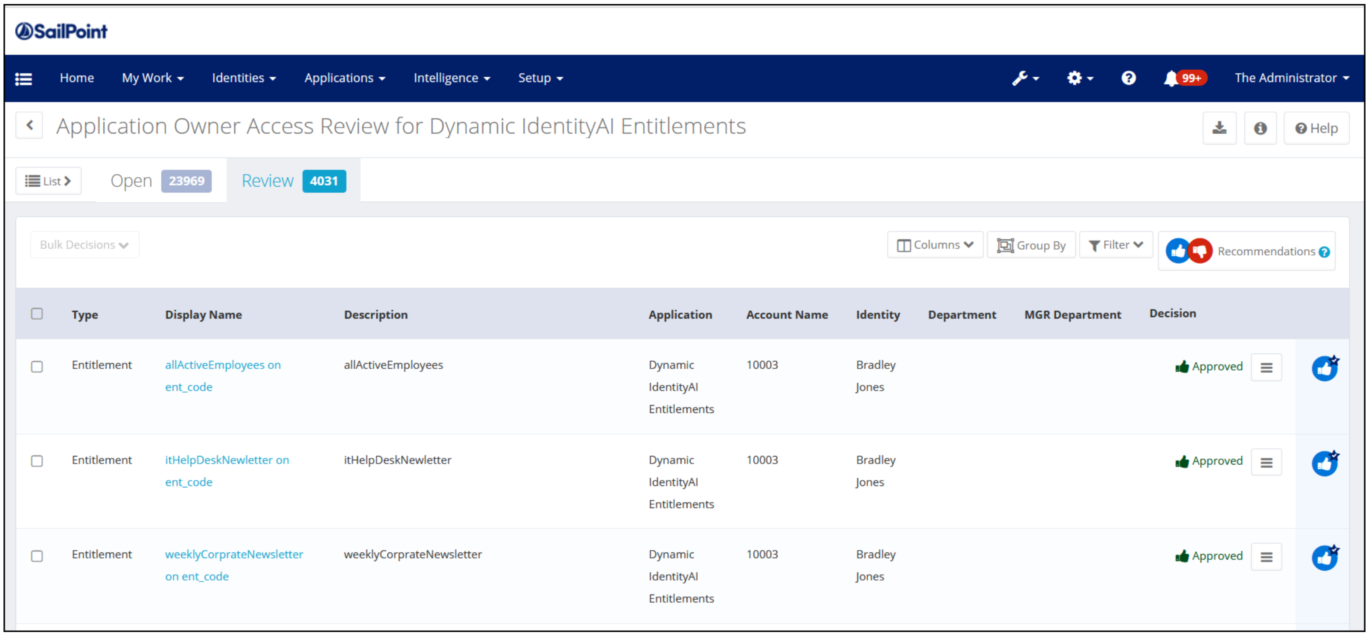
Decision Recommendations

When making decisions on items in this Certification, look for a recommendation icon to help make your decision. **Click the icon for more information.**

- Indicates an item was automatically approved

☑ Don't show this again

Any access review item that has a recommendation of "thumbs up" is automatically moved from the reviewer's **Open** tab to the **Review** tab, with an "Approved" decision.



Application Owner Access Review for Dynamic IdentityAI Entitlements

□	Type	Display Name	Description	Application	Account Name	Identity	Department	MGR Department	Decision
□	Entitlement	allActiveEmployees on ent_code	allActiveEmployees	Dynamic IdentityAI Entitlements	10003	Bradley Jones			Approved
□	Entitlement	itHelpDeskNewletter on ent_code	itHelpDeskNewletter	Dynamic IdentityAI Entitlements	10003	Bradley Jones			Approved
□	Entitlement	weeklyCorprateNewsletter on ent_code	weeklyCorprateNewsletter	Dynamic IdentityAI Entitlements	10003	Bradley Jones			Approved

Reviewers retain the option of changing the automated decision, as needed, before signing off on the review.

Users still have to sign off on automatically approved items in the Review tab. If the user reverses an automatic approval, the item is moved back to the user's Open tab for further review as needed.

Finding Automatically Approved Items

For quick viewing of all automatically approved items, you can Filter the items in your Access Review:

1. In the Access Review, click **Filter**.
2. Click **Add Filter** and select **Auto Approved**.
3. Choose a value of **True** to find automatically approved items; you can choose **False** if you want to filter items to show those that are not automatically approved.
4. Click **Apply**.

Reporting on Automatic Approvals

You can include automated approval information in reports, to help track and monitor items that have been automatically approved.

To report on automatically-approved items:

1. Click **Intelligence > Reports**
2. From the **Access Reviews and Certifications** reports section, choose a "live report" option for one of the certification types (Manager, Targeted, Application Owner, Advanced, or Role Membership) that supports automatic approvals.
3. In the **Report Layout** section, choose the columns related to automatic approvals that you want to display, such as:

- Decision Maker
- Decision Maker Comments
- Recommendation
- Recommendation Reasons
- Recommendation Timestamp
- Auto Decision Generated
- Auto Decision Accepted

AI Services Reports

AI Services recommendation information is included in the following IdentityIQ reports. For more information see the **Reports** documentation.

- Access Review Decision Report - note that the Roles table for this report intentionally does not contain the recommendation columns
- Access Request Status Report
- Advanced Access Review Live Report
- Application Owner Access Review Live Report
- Certification Activity by Application Report
- Manager Access Review Live Report
- Role Membership Access Review Live Report
- Targeted Access Review Live Report
- Work Item Archive 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.

> 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 recommendations, the reports return the following:

- **Recommendation** — Not Consulted
- **Recommendation Timestamp** — Blank
- **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 AI Services
- **Recommendation Timestamp** — Blank
- **Auto Decision Generated** — False
- **Auto Decision Accepted** — False

AI Services IdentityIQ Console Commands

You can use the IdentityIQ console to view the status of your recommender or to disable recommendations for this IdentityIQ instance.

These 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, put quotation marks around the name (“Recommender Name”)
- **reco use --** — disable and clear the recommender selection

For more information see the **IdentityIQ Console** documentation.