AI Services

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Copyright © 2023 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 website 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 and word mark), “SailPoint,” (design and word mark), "Identity IQ,” “IdentityNow,” “SecurityIQ,” “Identity AI,” “Identity Cube,” and “SailPoint Predictive Identity” are registered trademarks of SailPoint Technologies, Inc. “Identity is Everything,” “The Power of Identity,” and “Identity University” 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.

SailPoint Technologies, Inc. makes no warranty of any kind regarding these materials 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

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. 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.

Access Request Recommendations

AI Services can be configured to give recommendations to people requesting access. With this option, users managing their own access are shown a set of access recommendations, based on information such as the user's manager, department, location, and colleagues. This can help reduce confusion on the user's part about what access to request, and save valuable time and effort in the request process.

See Enabling Recommendations for Access Requests for details on how to enable access request recommendations.

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 part of your AI Services integration. See Enabling Access Modeling.

Integrating SailPoint AI Services

> Note: 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 AI-Driven Identity Security for IdentityIQ*.

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. Select 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.

AI Services Limitations for Customizing Hibernate Files

IdentityIQ allows you to customize extended and searchable attributes by editing various `.hbm.xml` files (such as `IdentityExtended.hbm.xml` or `LinkExtended.hbm.xml`) when IdentityIQ is installed and configured. The AI Services feature requires that all the *default* values in IdentityIQ's `.hbm.xml` files are present.

The AI Services feature will not function properly if any default fields have been removed from any of the `.hbm.xml` files. Do not remove any default fields from the `.hbm.xml` files if you plan to implement the AI Services integration.

See the *IdentityIQ Installation Guide* for more details.

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.

> Note: **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 AI-Driven Identity Security for IdentityIQ*.

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.

Sharing IdentityIQ Data with AI Services

IdentityIQ connects to AI Services though a bespoke IdentityNow tenant. Customers deploy an AI Services Virtual Appliance for all communication, which requires configuration of a firewall to allow outbound HTTPS traffic.

For more information on the IdentityNow tenant and the AI Services Virtual Appliance, see *Getting Started with AI-Driven Identity Security for IdentityIQ*.

For each identity, customers can configure identity attributes collected during the provisioning of their tenant.

All data movements are done via encrypted channels, via Amazon Kinesis Data Firehose, which encrypts data using AWS Key Management Service, and AWS SQS.

IdentityIQ Data Collected for AI

Select data, as configured by each individual organization, is gathered by the AI Services Virtual Appliance and stored in both IdentityNow and AI Services repositories. All data movements are done via encrypted channels. Data, once transmitted, is stored according to the mechanisms of the final repository.

These are the objects and the associated information that is collected from IdentityIQ and stored in the AI Services repository:

Application

- ID
- Name
- Created
- Modified
- Extended attributes (as defined in the ObjectConfig attribute definitions)

- Connector
- Type
- isAuthoritative
- Features
- Owner

Bundle (Role)

- Id
- Name
- Created
- Modified
- Type
- Description
- displayableName
- Selector summary (getSelector().generateSummary()
- roleTypeDefinition (used to determine if the role is assignable)
- activationDate
- deactivationDate
- Owner
- Profiles
- Inheritance
- Requirements

- Permits

Certification

- Id
- Name
- Created
- Modified
- isComplete
- Phase
- isBulkReassignment
- Cert definition (used to calculate the due date)
- Signed date
- Finished date
- Expiration date
- Tags
- isElectronicallySigned
- isProcessRevokesImmediately
- Application
- certificationGroups
- Reviewers
- Signer
- Manager

- Parent certification (if there is one)

CertificationGroup

- Id
- Name
- Created
- Modified
- Certification definition (used to find the cert type)
- Status

CertificationItem

- Id
- Name
- Created
- Modified
- Use item type and Identity name (to calculate item name)
- Type
- summaryStatus
- hasDifferences
- Subtype
- Completed date
- Action object

  - action.approved
  - action.status
  - action.decisionDate
  - action.isBulkCertified
  - action.isRemediationCompleted
  - action.remediationAction
  - action.mitigationExpiration
- Certification
- Id (of the identity)
- Actor
- Certification definition (used to check showRecommnedations)
- Recommendation
- DataOwner
  - nativeIdentity
  - Instance
  - isAccountOnly
  - Application
  - Related Link objects
  - Managed attributes tied to the entitlement
- Type of Bundle (bundle id)
- Type of PolicyViolation

    - constraint name
    - policy name
    - status
    - mitigationExpiration
    - identity
    - revokedRoleIds
    - revokedEntitlementReferences

Identity

For the Identity object, a configurable list of identity attributes is collected. These additional attributes include details such as first name, last name, department, and other attributes. These attributes are at the customer's discretion and are configured during the provisioning of the customer's tenant.

- Id
- Name
- Created
- Modified
- Attributes (certain attributes can be excluded)
- Score
- Links
- Manager
- assignedRoles
- detectedRoles
- Workgroups

- IdentityEntitlement objects
- policyViolations
- Type
- softwareVersion
- Administrator

For Workgroup Identities

- Id
- Name
- Created
- Modified
- All attributes
- Owner

IdentityRequest

Categorized as accessRequest, passwordRequest, identityChangeRequest, or identityRequest.

- Id
- Name
- Created
- Modified
- Type
- endDate
- executionStatus

- completitionStatus
- Priority
- requesterDisplayName
- targetIdentity
- Requester
- affectedAccounts
- affectedApplications
- affectedBundles
- affectedEntitlements
- Items

IdentityRequestItem

- Id
- Name
- Created
- Modified
- Application
- Instance
- nativeIdentity
- displayName
- Name
- Value

- Annotation
- Operation
- Startdate
- Enddate
- isApproved
- isRejected
- provisioningState
- compilationStatus
- expansionCause
- Retries
- provisioningEngine
- Owner
- Approver
- targetIdentity (to get affected accounts)
- affectedApplications
- affectedBundles
- affectedEntitlements
- Recommendation
- Number of attachments

Link

For the Link object, a configurable list of identity attributes is collected. These additional attributes include details such as first name, last name, department, and other attributes. These attributes are at the customer's discretion and are configured during the provisioning of the customer's tenant.

- Id
- Name
- Created
- Modified
- nativeIdentity
- isDisabled
- isLocked
- Application
- Attributes (certain attributes can be excluded)
- Identity

ManagedAttributes

- Id
- Name
- Created
- Modified
- displayableName
- Attribute
- Value
- Description
- isAggregated
- isRequestable

- Owner
- Application
- Permissions

PolicyViolation

- Id
- Name
- Created
- Modified
- constraintName
- policyName
- Status
- migrationExpiration
- Identity
- revokedRoleIds
- revokedEntitlements

Profile

- Id
- Name
- Created
- Modified
- accountType

- Owner
- Application
- Bundle
- Managed attributes (for entitlement references)

Enabling Recommendations for Access Request Approvals

> Note: 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 on 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 for Access Requests

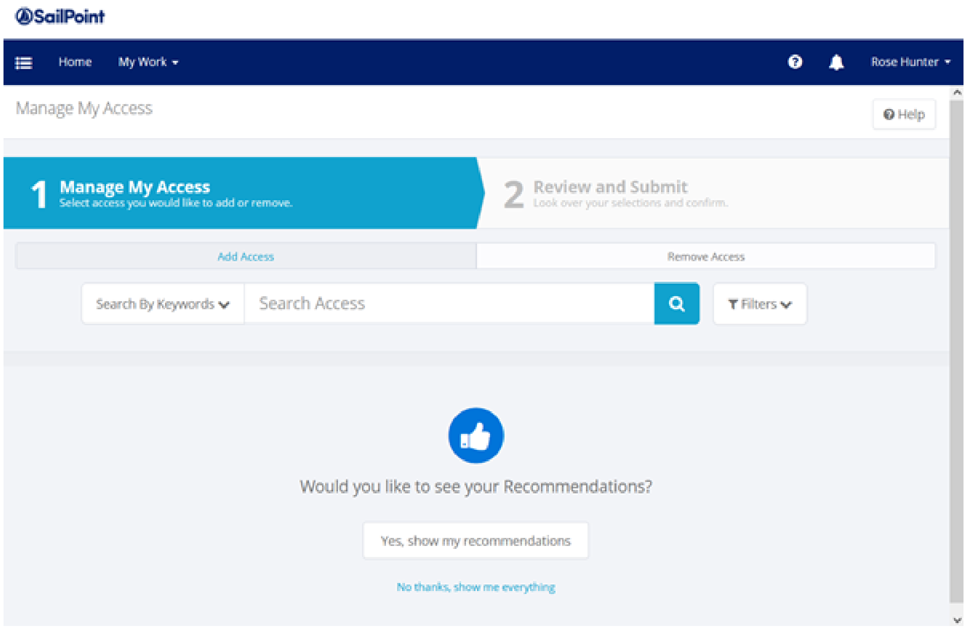
> Note: This option is not available until `init-ai.xml` is imported into IdentityIQ and a connection to AI Services is configured.

IdentityIQ can make recommendations for self-service requests for roles, using AI Services. AI Services uses peer group analysis, based on information such as the user's manager, department, location, and colleagues, to make recommendations about what access a particular user should have. The recommendations and the final decision are captured in reports, supplying important information about access decisions for auditors.

This feature must be enabled in your Lifecycle Manager settings, in order to generate recommendations for access requests.

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 on access requests** option.
4. **Save** your changes.

After this option is enabled, your users have the option to see recommendations when they request access.



Would you like to see your Recommendations?

See the **Lifecycle Manager** documentation for more information.

Enabling Recommendations and Automatic Approvals Globally for Certifications

> Note: 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.

> Note: 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 part of the AI Services integration. For more information, see **Configuring IdentityIQ for Access Modeling** in the *AI-Driven Identity Security Guide*.

> Note: AI service modules may be licensed separately. Please direct questions to your account manager to clarify your agreement.

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.

You can read about AI Services prerequisites, the onboarding process, and deployment steps at *Getting Started with AI-Driven Identity Security for IdentityIQ*.

Configuring Access Modeling Discover Common Access Functionality

Discover Common Access functionality is only available to organizations using IdentityIQ's AI functionality.

> Note: Configuration settings automatically copy over for those running the AI Services Access Modeling plugin prior to IdentityIQ version 8.4.

Begin by enabling AI – see Configuring AI Services – then configure Discover Common Access and Role Discovery:

1. Log in to IdentityIQ as an administrator.
2. Navigate to **gear > Global Settings > AI Services Configuration** and enter:
   - Connection information, including AI Services Hostname, Client ID, and Client Secret.
   - IdentityNow URL. This is specific to each customer.
   - Minimum number of identities on which to model roles. The default is 20.

> Note: Selecting fewer identities on which to model roles yields more potential role options. Using a higher minimum number of identities avoids yielding many highly-specific roles.

3. Select **Save**.

Using Access Modeling for Role Discovery in Advanced Analytics

After the Access Modeling is enabled 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.

See Common Access Roles Discovery and Specialized Roles Discovery.

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.

Disabling AI Services

If you no longer want to use the AI Services features, AI Services can be disabled.

1. Log in as an IdentityIQ administrator.

2. Disable the AI Services feature in the Debug pages:

   a. Navigate to the Debug pages through the Debug URL: `https://<hostname>/identityiq/debug` (for example, *http://localhost:8080/identityiq/debug*).

   b. From the **Configuration Objects** dropdown list, choose **System Configuration**.

   c. Locate the **identityAIEnabled key** and change the value from true to false:
   `<entry key="identityAIEnabled" value="false"/>`

   d. **Save** your change to the System Configuration object.

3. Disable the AI Services plugins:

   a. Click the **gear icon > Plugins**.

   b. Disable the **AI Services Recommender Plugin** by clicking the power button icon to enable or disable plugins, and confirming your decision.

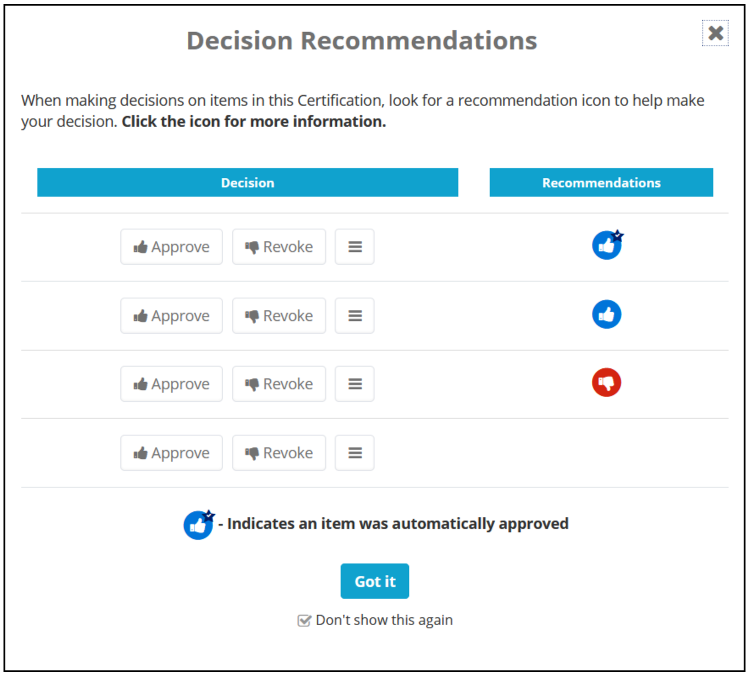
Using Automatic Approvals

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

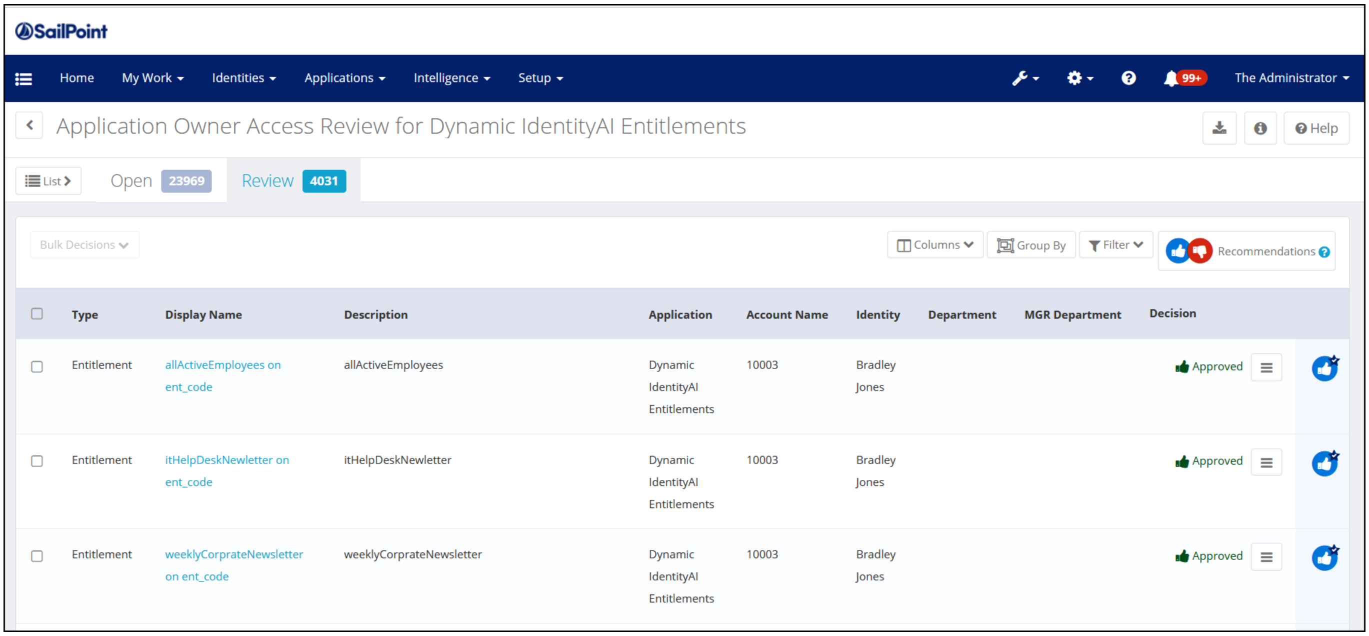
When making decisions on items in this Certification, look for a recommendation icon to help make your decision. **Click the icon for more information.**

Decision	Recommendations
Approve Revoke ≡	👍★
Approve Revoke ≡	👍
Approve Revoke ≡	👎
Approve Revoke ≡	

👍★ **- 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

Discovering Common Access

The AI Access Modeling – Discover Common Access feature uses AI analytics and scoring methodologies to evaluate access for a given population, then presents a recommended role that includes the entitlements that are common across those identities. You can create and assign the common access role to large populations of employees to provide broad-based access from the first day an employee joins your organization. Once entitlements are labeled as part of a common access role, they are excluded from future access modeling role mining, role insights, and access request recommendations, which helps simplify your AI model.

This feature is available to organizations using AI Access Modeling. You need the ManageIAICommonAccessDiscovery SPRight, which is part of the AIAccessModelingAdministrator and AIServicesAdministrator capabilities. Your system configuration needs to have AI enabled. See About SailPoint AI Services .

> Note: Access Modeling, available prior to version 8.4 as an IdentityIQ plugin, may be part of your AI subscription as of version 8.4. You will no longer need to download a separate plugin, and you will no longer see it listed with your Installed Plugins.

> Note: AI service modules may be licensed separately. Please direct questions to your account manager to clarify your agreement.

Common Access Roles Discovery

IdentityIQ Administrators can use this functionality to determine which access should be common to nearly all identities in an organization. Common access roles are not tied to specific job functions.

> Note: Only roles created using Discover Common Access will be designated as common access in AI, and only these roles will have their entitlements excluded from future Access Modeling mining sessions.

To discover a common access role:

1. Navigate to **Intelligence > Advanced Analytics**.

2. In the Search Type field, make sure **Identity** is selected.

3. Enter and apply search criteria.

4. Select the identity or identities to discover roles for.

5. Select the **Discover Common Access Roles** button.

6. You will be redirected to the Access Modeling page in IdentityNow, using the URL that you configured in Enabling Access Modeling. If you are not already logged in to IdentityNow, you will have to enter admin credentials and authenticate.

   AI displays the potential role.

   > Note: Once you are in a role mining session, you can select the Settings button at the right side of the screen to adjust settings and use the granularity slider to adjust the minimum number of identities in a group.

7. The Potential Role page includes the following tabs:

   - On the Composition tab, use the slider to exclude entitlements beyond your chosen popularity threshold, then select **Apply**.
   - On the Exclusions tab, indicate exclusions.
   - On the Identity Overview tab, use the Show Chart dropdown to view the Identity Attributes. A list of identities shows those that would be included in this role, listed by display name, department, job title, and location.

8. Select the **Create a Role** button. Alternately, you may select **Save Draft** if it needs additional work.

9. On the Create a Role page, enter a name, owner, and description to create it. This role will be excluded from future Access Modeling role mining, role insights, and Access Request recommendations.

   Select the **Include Identities** checkbox to indicate that you want the identities listed in the Identity Overview tab to be included in the new role when it is created.

10. Select the **Create a Role** button.

Specialized Roles Discovery

Specialized Roles Discovery, part of Access Modeling, identifies user access patterns and determines potential roles, or bundles of access, that accurately align with what users actually do in an organization. IdentityIQ Administrators can use this functionality to generate roles for specific job functions, such as Accounting or Sales.

To discover specialized roles:

1. Navigate to **Intelligence > Advanced Analytics**.

2. In the Search Type field, make sure **Identity** is selected.

3. Enter and apply search criteria.

4. Select the identity or identities to discover roles for.

   > Note: AI Access Modeling limits the number of identities to 10,000 per population to be mined.

5. Select the **Discover Specialized Roles** button.

6. You will be redirected to the Access Modeling page in IdentityNow, using the URL that you configured in Enabling Access Modeling. If you are not already logged in to IdentityNow, you will have to enter admin credentials and authenticate.

   AI displays a list of potential roles.

   > Note: Once you are in a role mining session, you can select the **Settings** button at the right side of the screen to adjust settings and use the granularity slider to adjust the minimum number of identities in a group.

7. Select a role from the list.

8. The Potential Role page includes the following tabs:

   - On the Composition tab, use the slider to exclude entitlements beyond your chosen popularity threshold, then select **Apply**.
   - On the Exclusions tab, indicate exclusions.
   - On the Identity Overview tab, use the **Show Chart** dropdown to view the Identity Attributes. A list of identities shows those that would be included in this role, listed by display name, department, job title, and location.

9. Select the **Create a Role** button. Alternately, you may select **Save Draft** if it needs additional work.

10. On the Create a Role page, enter a name, owner, and description to create it. This role will be excluded from future Access Modeling role mining, role insights, and Access Request recommendations.

    - Select the **Include Identities** checkbox to indicate that you want the identities listed in the Identity Overview tab to be included in the new role when it is created.

11. Select the **Create a Role** button.

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.

> 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 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.