Cloud Access Management Integration

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

Getting Started

Cloud Access Management is a governance offering for multi-cloud environments. Use it quickly to discover who has access to what, how that access is being granted, and implement pre-configured policies that automate detection of compliance violations.

Within IdentityIQ, you can view additional detailed Cloud Access Management-based information about entitlements from identity warehouse, access requests, entitlement catalog, advanced analytics, and certifications. You can search for entitlements using Cloud Access Management-based values from entitlement catalog, manage access, advanced analytics, certifications, and targeted certification editor.

Whenever a summary of an entitlement is shown (e.g. in a table), there will be an easy, at a glance 'hint' to know if the entitlement has any cloud access.

When integrating Cloud Access Management with IdentityIQ, the following application types are supported:

- AWS
- Azure Active Directory

To install and configure Cloud Access Management with IdentityIQ, see Setup.

Setup

The Cloud Access Management integration feature will have to be installed and then configured to integrate with IdentityIQ.

For more information, see:

- Installation
- Configuration
- Operating Verification

Installation

Use the following information to activate your Cloud Access Management installation.

1. Log on to your instance of IdentityIQ as an administrator.
2. Click on **gear menu > Global Settings** and select **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-cam.xml file and click **Import**.
5. When the import is complete, click **Done**.

> Note: A restart of currently running application servers is required after init-cam.xml is installed.

Configuration

Use the Cloud Access Management configuration page to connect IdentityIQ to Cloud Access Management Services. To access this page, click **gear menu > Global Settings > Cloud Access Management Configuration**.

Enter your connection and configuration settings. Be sure to **Save** your changes.

Connection Information for Cloud Access Management Services

CAM Hostname

The hostname of the Cloud Access Management website for your organization. For example, `https://<org>.cam.sailpoint.com`.

OAuth Token Hostname

The hostname of your IdentityNow tenant, which is used to create the Cloud Access Management access token using the Client ID/Secret. For example, `https://<org>.api.identitynow.com`

Client ID / Client Secret

The Client ID is the identifier associated with the Cloud Access Management API service. The Client Secret is the OAuth secret associated with the Cloud Access Management API service.

To obtain a personal access token from IdentityNow, see Managing Personal Access Tokens. To obtain a personal access token from the API, see the API docs for details.

Advanced

Read Timeout

The maximum time in seconds to wait for a response from Cloud Access Management APIs before failing.

Connect Timeout

The maximum time in seconds to wait for a connection to succeed to Cloud Access Management APIs before failing.

Testing the Connection

Once your configuration details have been entered, you can click **Test Connection** to verify that the connection information is valid and that IdentityIQ can successfully connect to Cloud Access Management.

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

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

Event Properties

After Cloud Access Management has been installed and configured, it can start receiving events. By clicking this button, Cloud Access Management is notified to start sending data. After the data has initially been received, Initiate

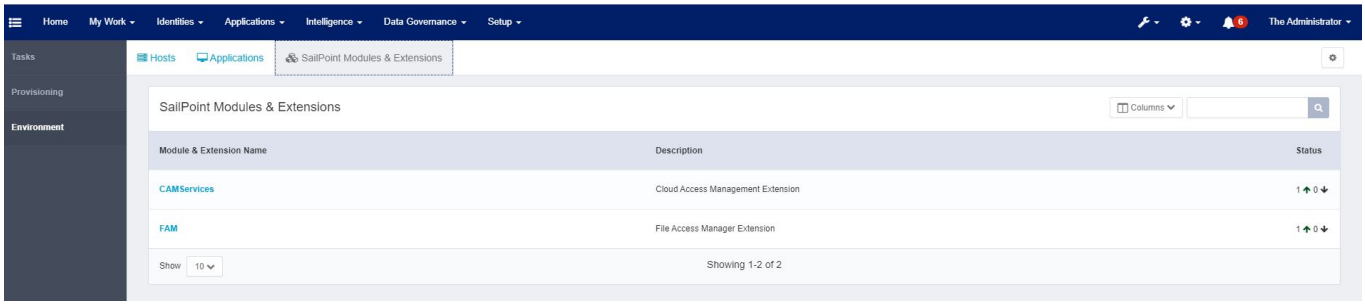
Events can be clicked again to request all data.

Operating Verification

To verify Cloud Access Management was installed and configured correctly, complete the following steps:

1. Navigate to the gear menu and click on **Administrator Console**.
2. Select **Environment**.
3. Click **SailPoint Modules & Extensions**.

   Here, all the integrated modules can be viewed along with their status, host name, and last ping to their server.

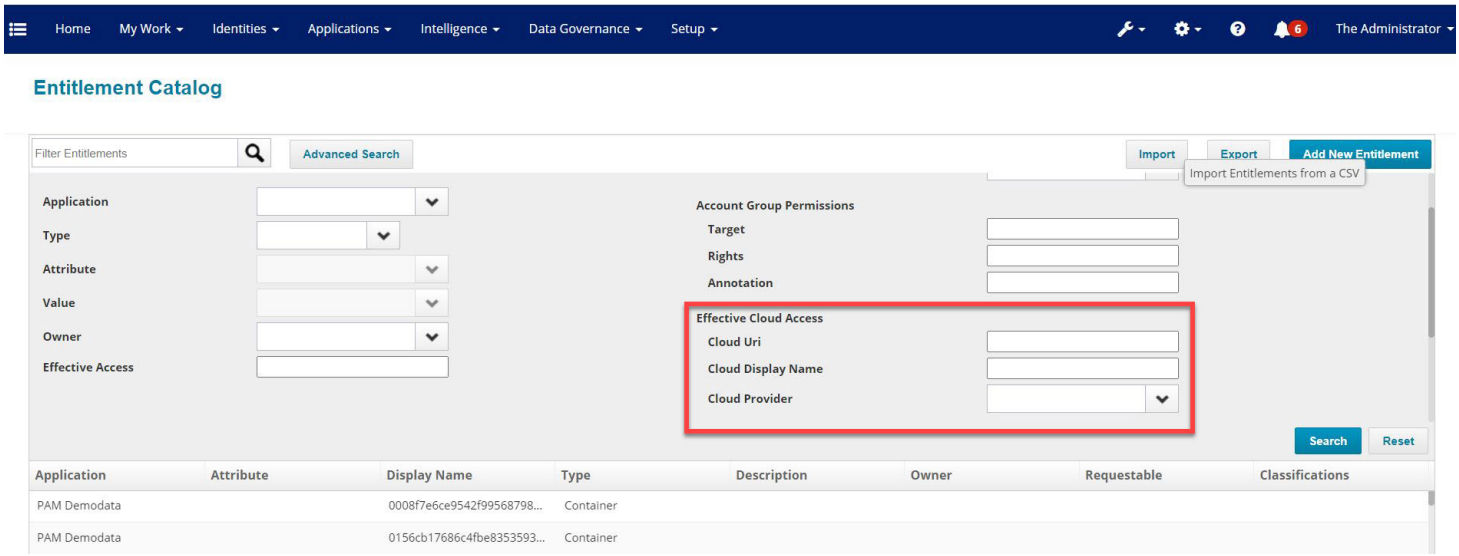


> Note: The default interval for the monitoring is five minutes.

Cloud Based Search Options

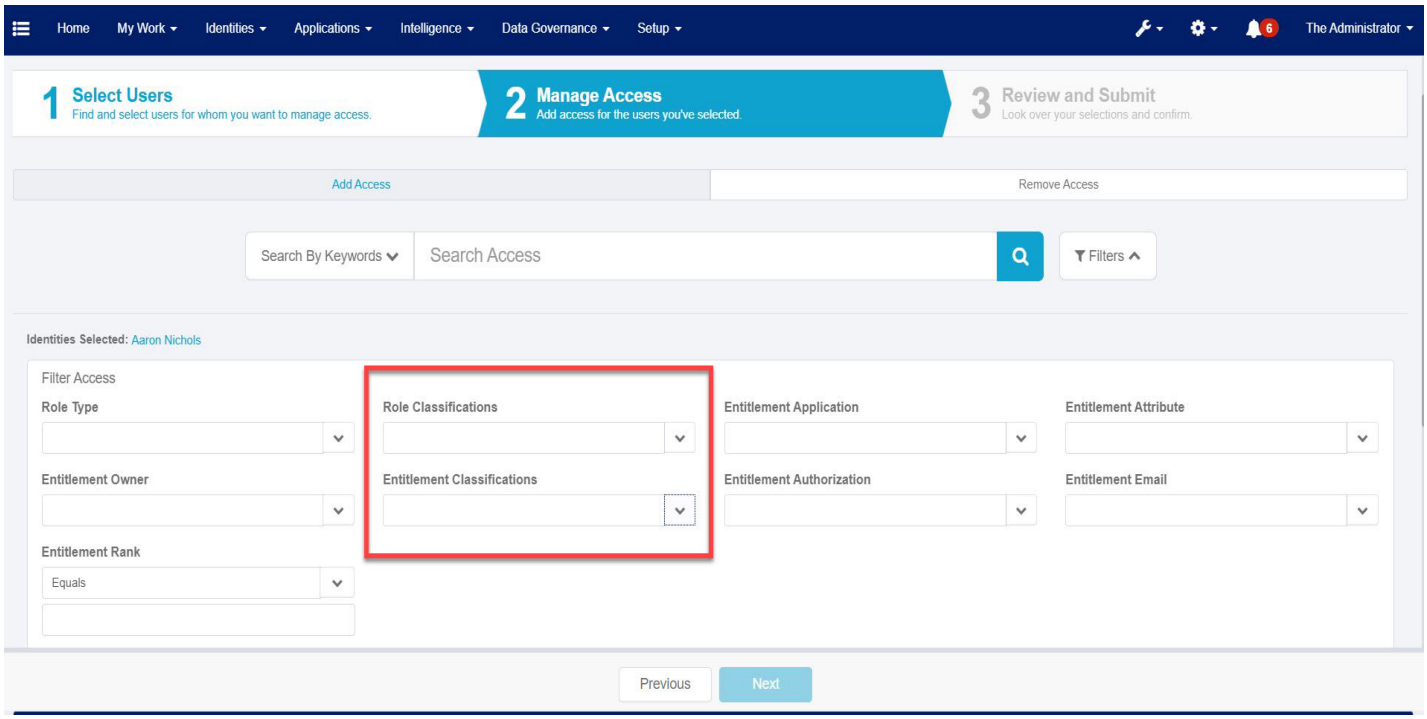
When Cloud Access Management is enabled, additional fields will be present in the Entitlement Catalog Advanced Search, the Manage Access Page, and the Advanced Analytics page.

For the Entitlement Catalog, the new fields under Effective Cloud Access are Cloud URI, Cloud Display Name, and Cloud Provider. These fields will search for data stored in IdentityIQ through Cloud Access Management Events.

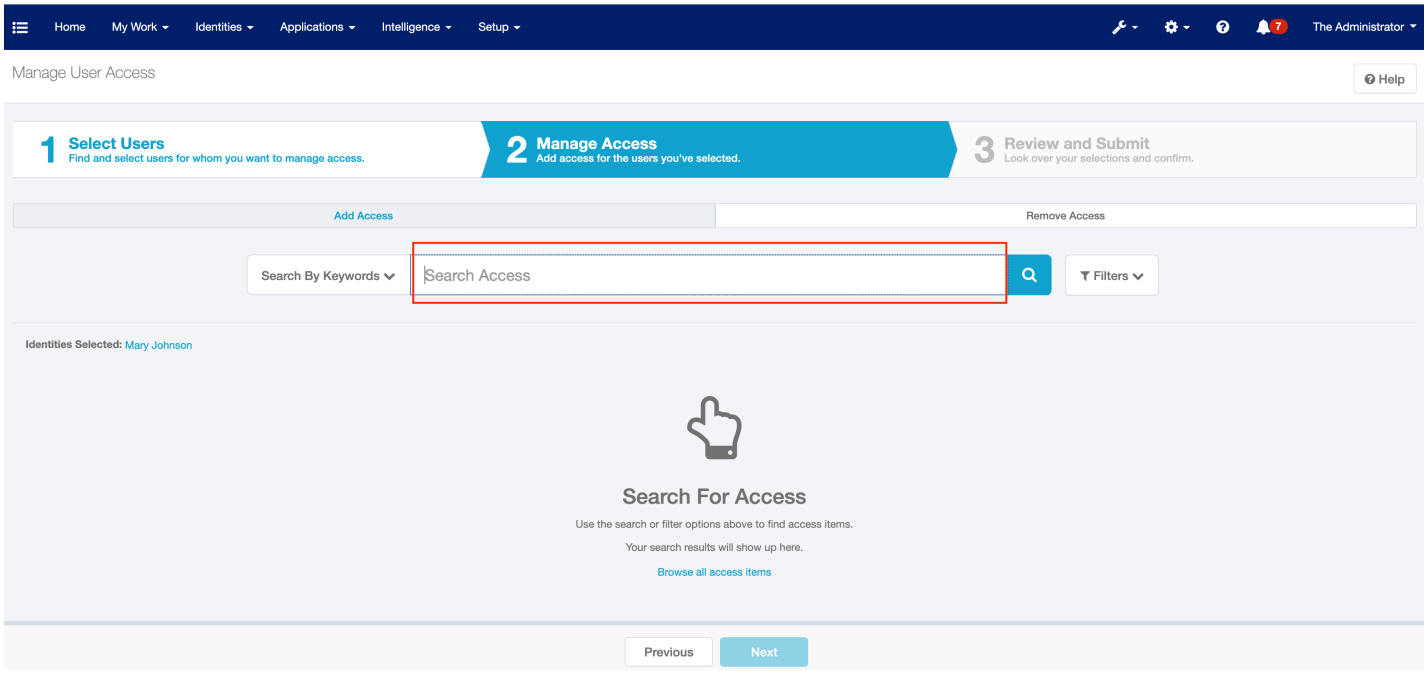


For Manage Access, new filters are added for the Manage Access Page to search for managed attributes which are cloud based by classifications. This filter is multi-valued and lists the different clouds (AWS, Azure, etc). The two new fields are Role Classifications and Entitlement Classifications.

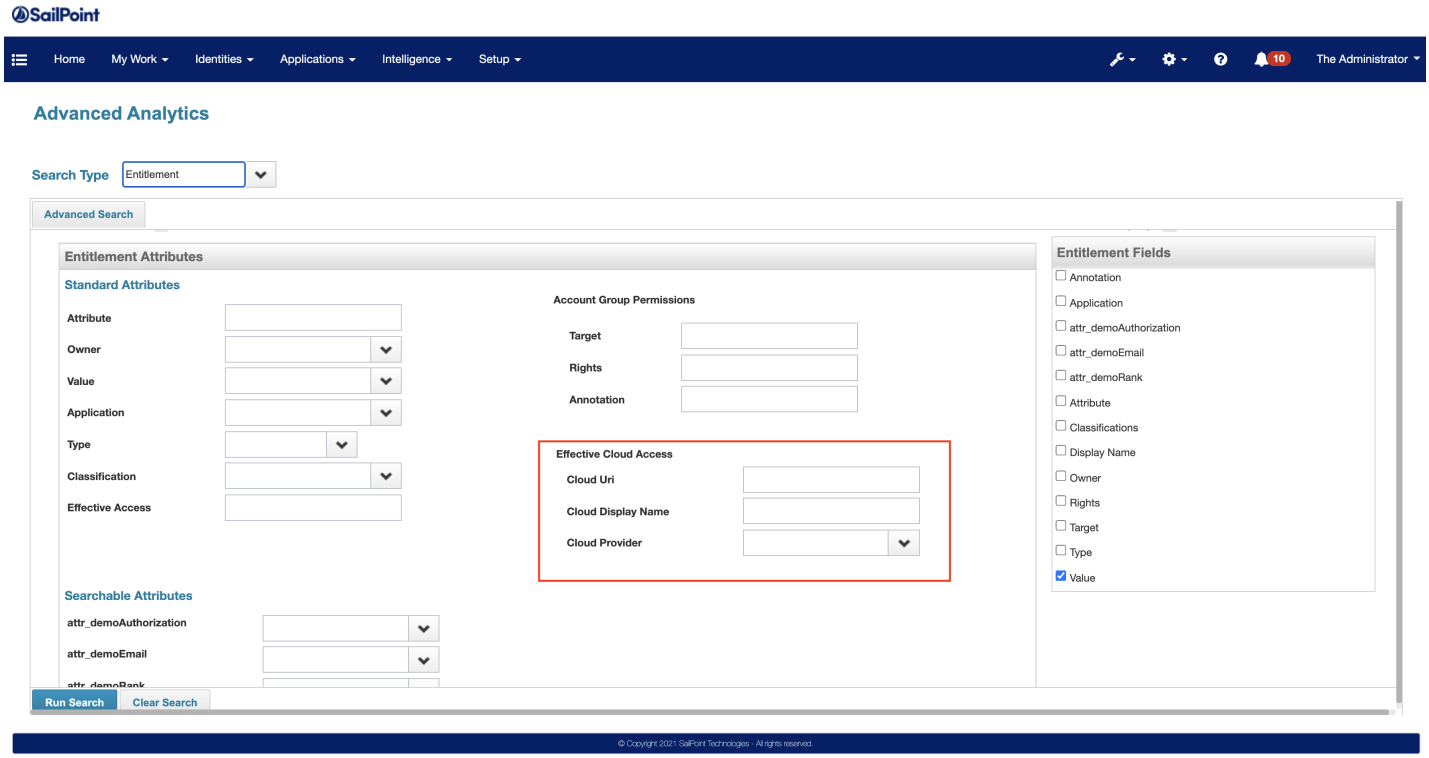
> Note: There is an additional field titled Entitlement Cloud Provider.



Also for Manage Access, the Search Access has a powerful searching capability. When Cloud Access Management is enabled, searches that match the Cloud Display Name or Cloud URI (mentioned above) with any of the three cloud access types, will result in all roles and groups within that hierarchy.



For Advanced Analytics, the new fields under Effective Cloud Access are Cloud URI, Cloud Display Name, and Cloud Provider. These fields will search for data stored in IdentityIQ through Cloud Access Management Events.



Cloud Based Locations

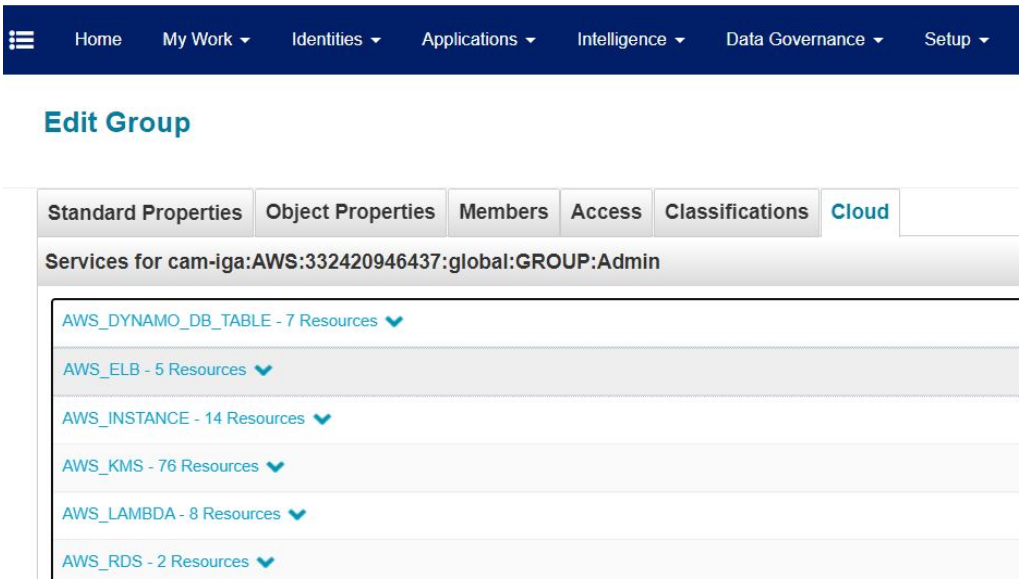
After the Cloud Access Management module is integrated, IdentityIQ will retrieve at display time additional entitlement details from Cloud Access Management and display them in a new Cloud tab.

Cloud Tab Locations

This section highlights all the locations of IdentityIQ where the new cloud tab will display when dealing with entitlements.

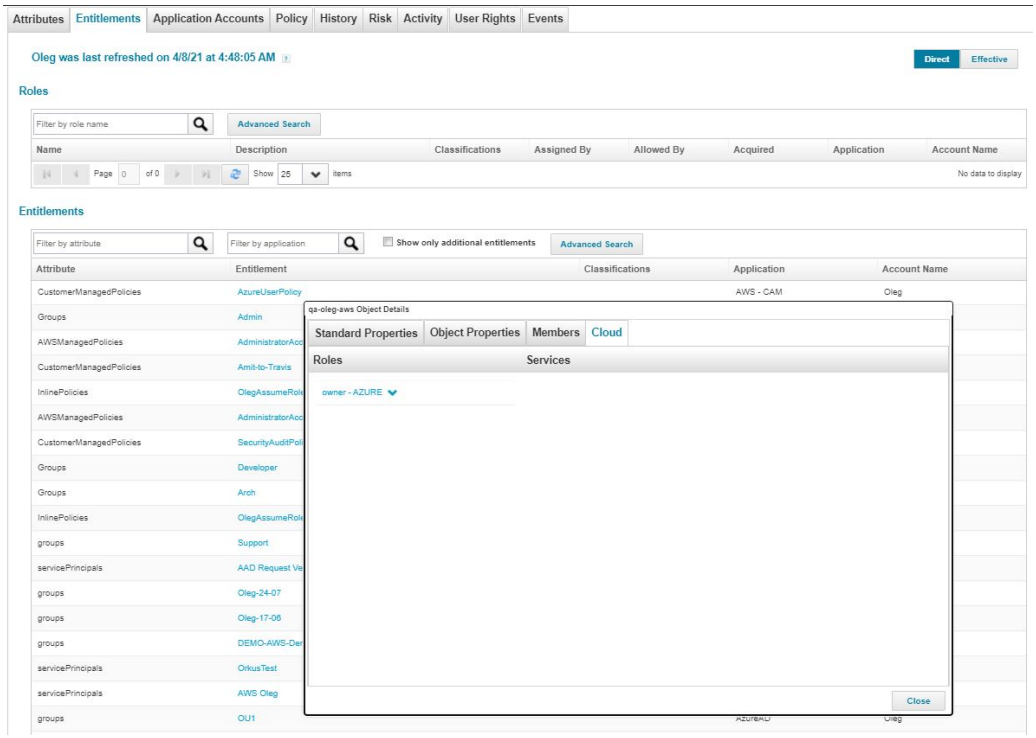
Entitlement Catalog

When searching for entitlements within the Entitlement Catalog, select the desired cloud enabled entitlement. Next, select the Cloud tab.



Identity Warehouse

After selecting an identity within the Identity Warehouse, navigate to the Entitlements tab and select a cloud enabled entitlement. The Cloud tab will show similar data as the Cloud tab for the Entitlement Catalog.

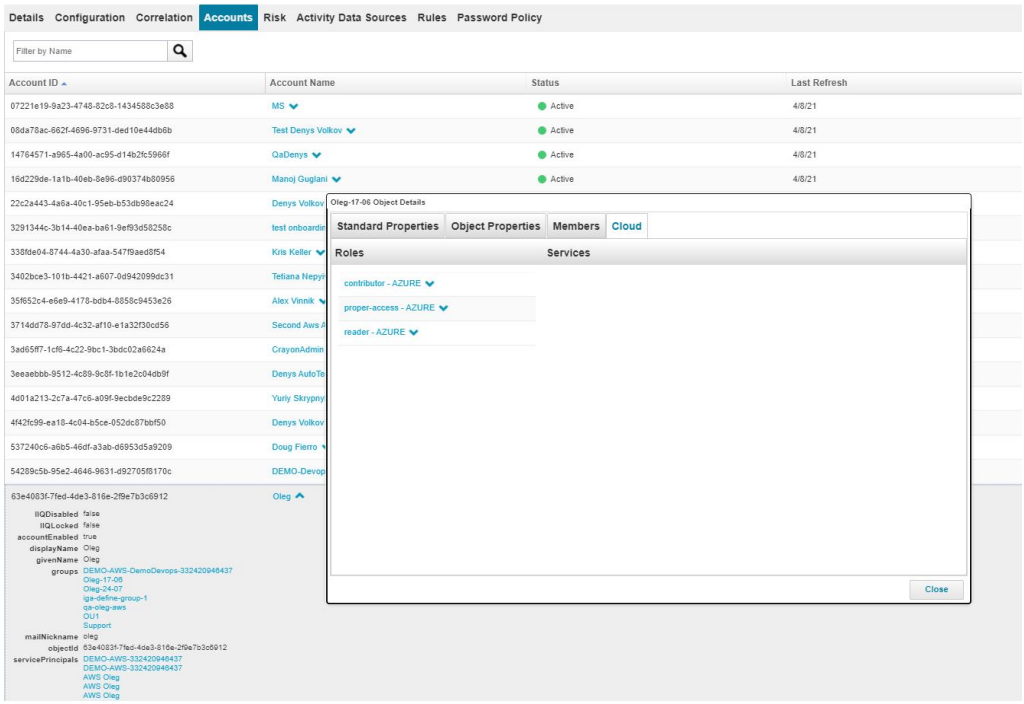


Application Definition

When selecting an application within Application definition, navigate to the Accounts tab. Expand the user details having the cloud enabled entitlement.

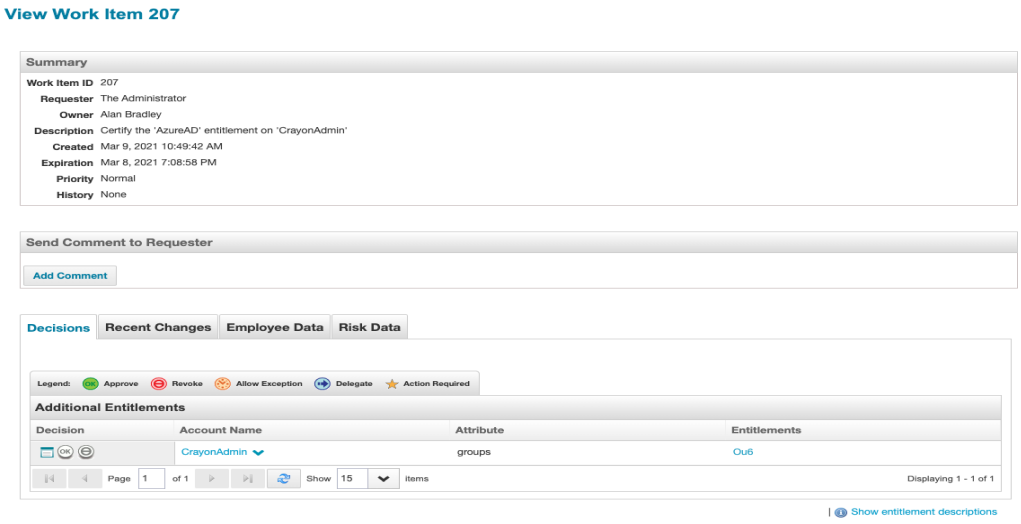
Select the desired group for an identity.

The Object Details dialog will display. Click the Cloud tab.



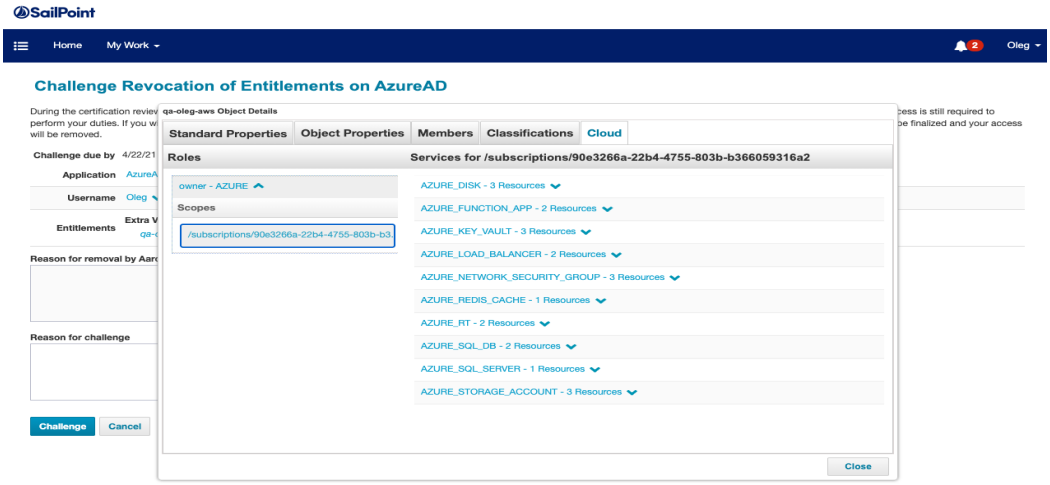
Delegated Work Items

After selecting a work item, click on the entitlement. The same dialog as the Identity Warehouse will display.



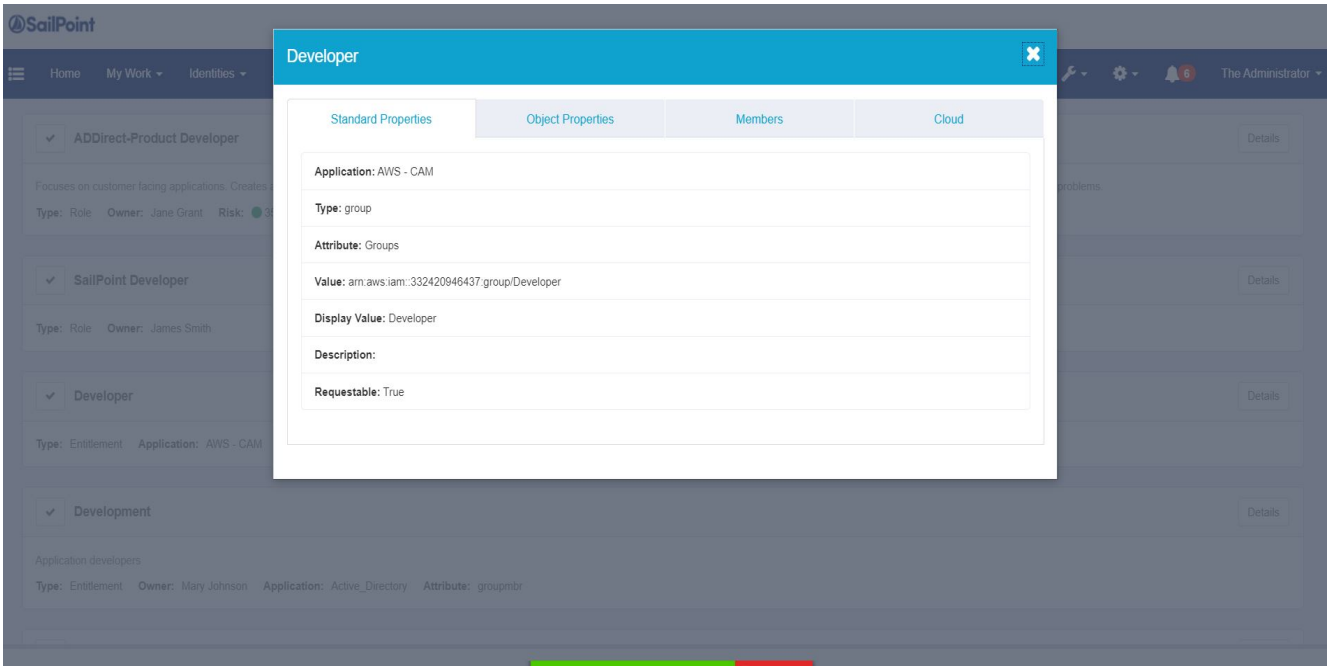
Challenge Work Items

When a challenge phase is enabled, the cloud can be viewed on the particular entitlement in the Challenge Work Item.



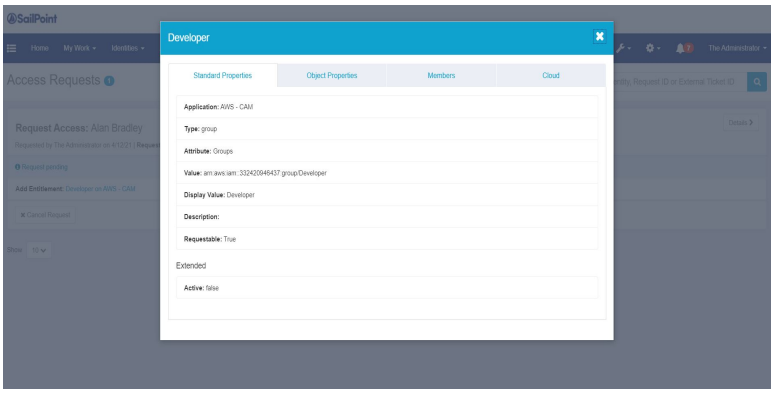
Manage User Access

When selecting an identity to add or remove access from, scroll to the desired entitlement and click the Details option. The Cloud tab will display in this window.



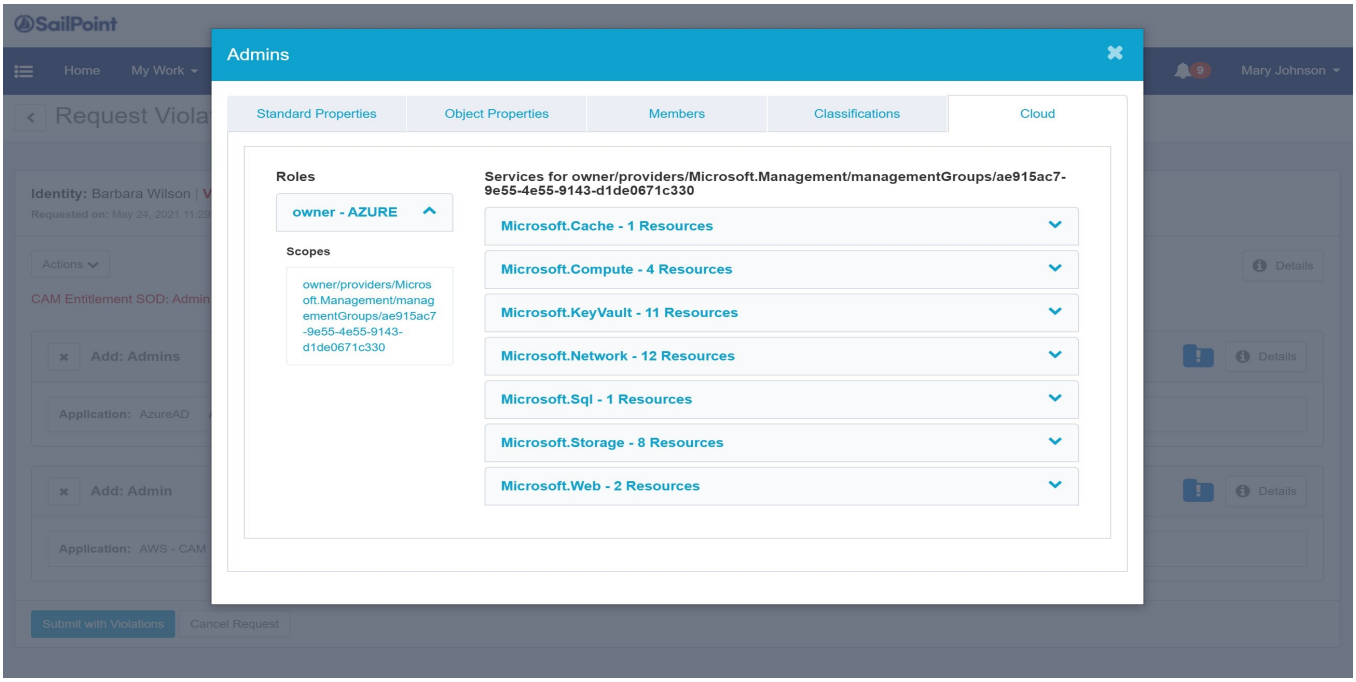
Access Request

When adding an entitlement, this Cloud tab can be seen within Track My Requests.



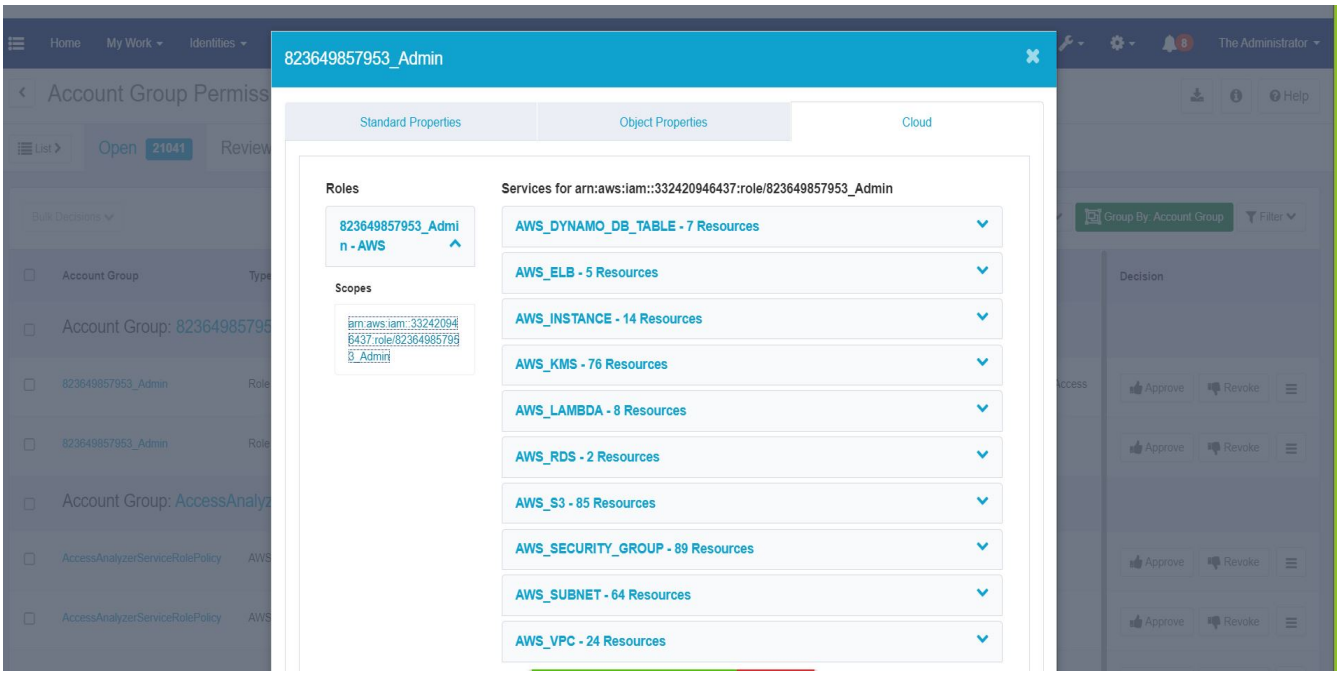
Request Violation

This Cloud tab will display when viewing a request violation work item. If a created policy conflicts between two cloud entitlements, this tab will display.



Access Review

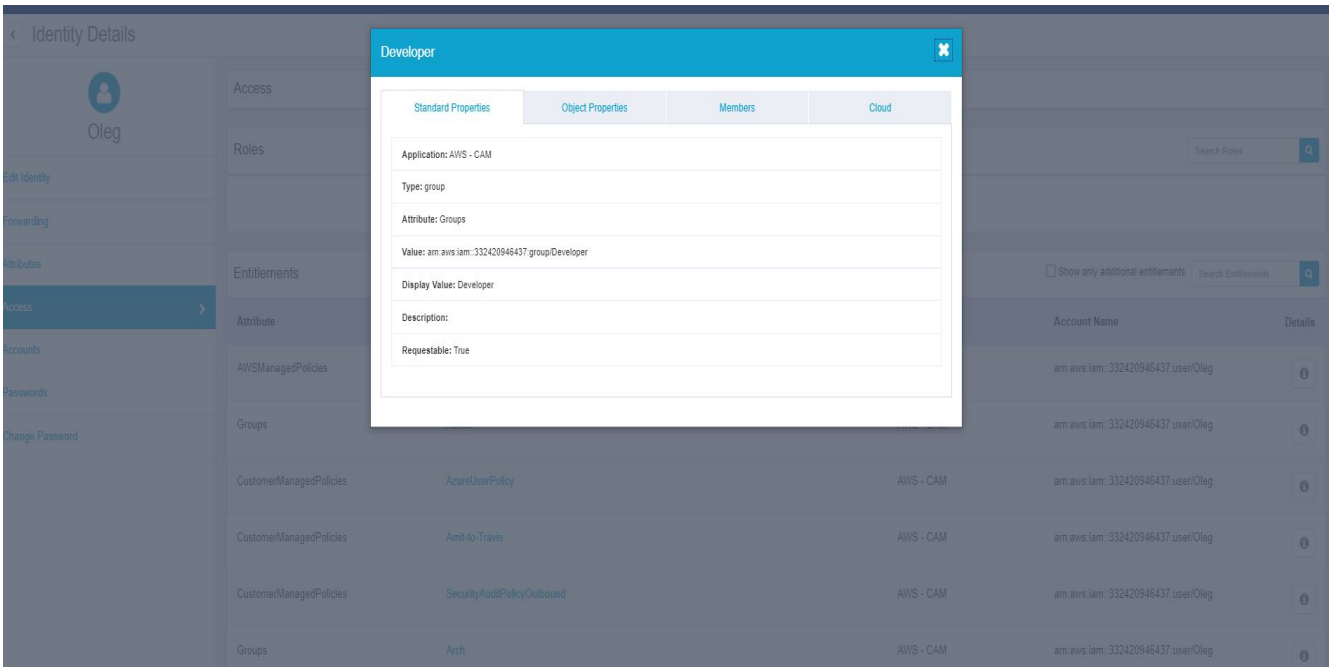
This Cloud tab will display when scheduling a certification. Choose the desired cloud application, then click on Account to view the Cloud tab.



Identity Details Access Page

Navigate to the Manage Identity dropdown and choose either **View Identity** or **Edit Identity**. Then, click on the **Access** tab to see the list of entitlements.

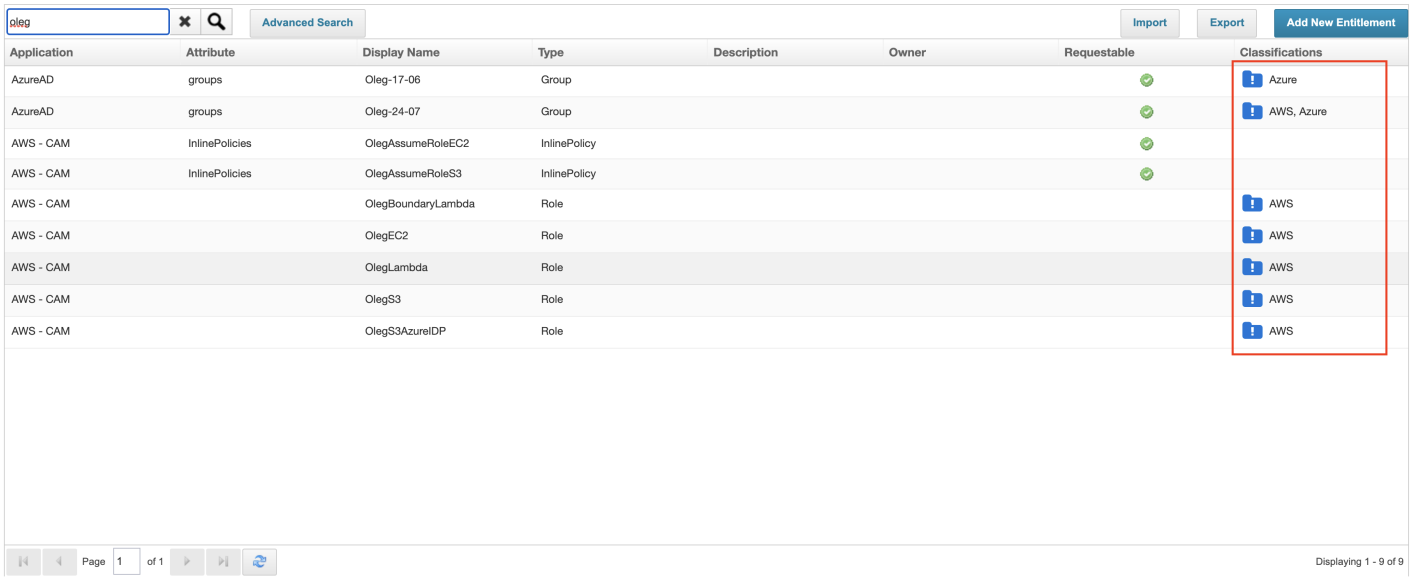
> Note: The cloud tab will only be visible in the Details dialog if it's a cloud supported managed attribute / entitlement.



Cloud Classifications

Cloud Access Management classifications will be visible for cloud based entitlements. The classifications correspond to the cloud provider for which the entitlements are associated. The classifications for a cloud access group entitlement will also include the classifications of its cloud access roles. These classifications will display in the Classification column within the Entitlement Catalog (and other tables within IdentityIQ) as shown below.

Entitlement Catalog



Associations

Click the Cloud tab to retrieve information from the Cloud API. The following associations can be determined from the information retrieved from Cloud Access Management:

- Federated Group – a Cloud Access Management group that has associated Cloud Access Management role (s)
- Native Group – a Cloud Access Management group having no Cloud Access Management roles but is associated with Cloud Access Management services
- Cloud Access Management Role association

Federated Groups

For federated and hybrid groups, two panels will display when looking at the Cloud Access Management details.

The left panel will display all associated role in an accordion style. When opened, the associated scope(s) with that role will listed under.

When a scope is selected, the right panel will populate with the associated Cloud Access Management service(s). These services are also listed in an accordion style. When a service is selected, the associated CAM resource(s) will be listed.

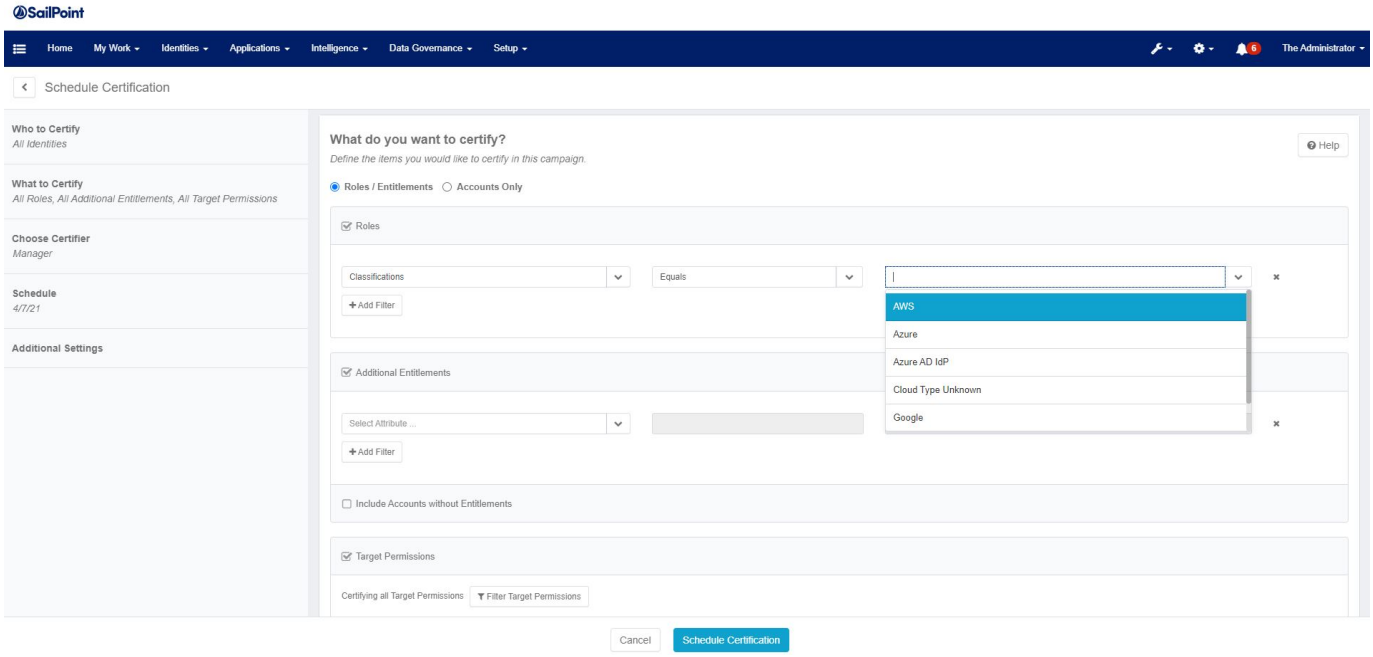
Native Groups

Only services are listed in one panel.

Targeted Certifications Cloud Filtering

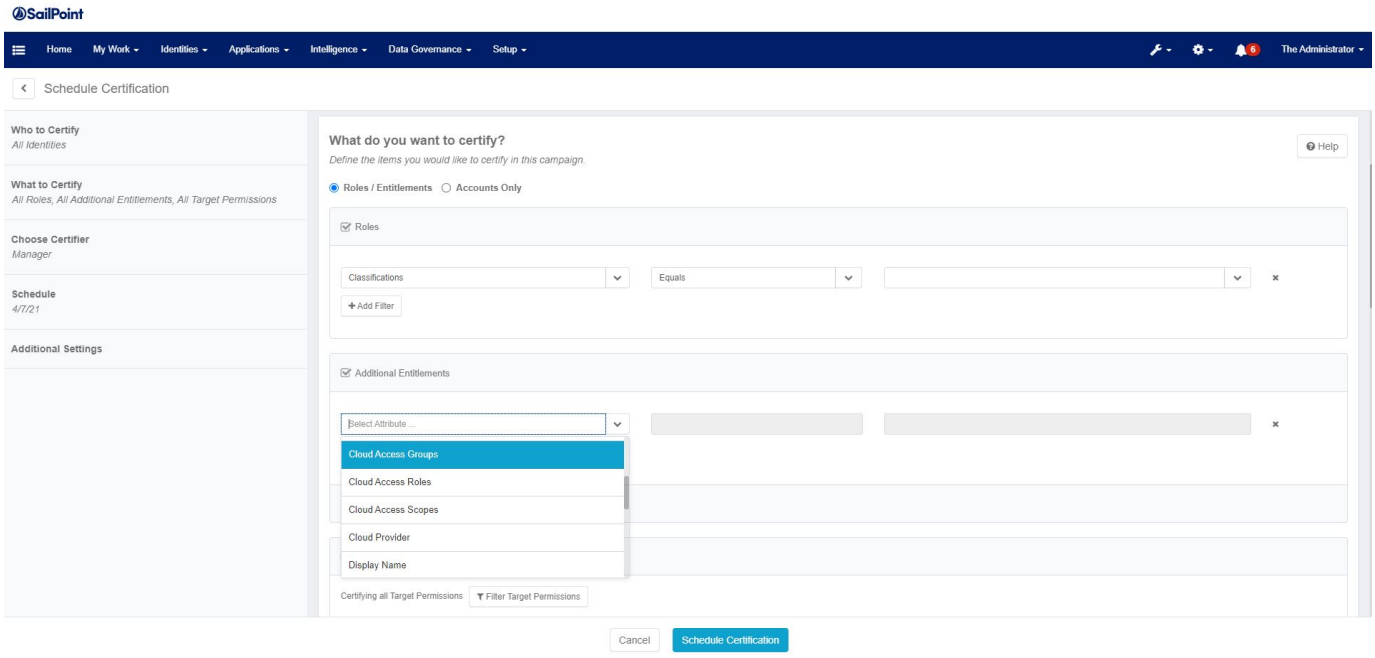
When integrated with IdentityIQ, Cloud Access Management allows the user to define a Targeted Certification to specify cloud specific selection criteria for Roles and Additional Entitlements.

The selection criteria for Targeted Certifications is used to decide which entitlements and / or roles will be included as certifiables when the certification is generated.



> Note: New search criteria have been added for Additional Entitlements. All new search criteria will appear as a pull-down option. They will only appear if Cloud Access Management is enabled.

- Cloud Access Scopes – matches ManagedAttributes which have *any* of the given scopes indirectly from their Cloud Access Manager groups or roles.
- Cloud Access Roles – matches ManagedAttributes which map to *any* of the given roles directly or indirectly from their Cloud Access Manager groups.
- Cloud Access Groups – matches ManagedAttributes which map to *any* of the given groups.
- Cloud Provider – matches ManagedAttributes which have a Cloud Access Manager group or (indirectly) a Cloud Access Manager role with *any* of the given clouds set directly.


SailPoint
Home
My Work
Identities
Applications
Intelligence
Data Governance
Setup
The Administrator
Schedule Certification
Who to Certify
All Identities
What to Certify
All Roles, All Additional Entitlements, All Target Permissions
Choose Certifier
Manager
Schedule
4/7/21
Additional Settings
What do you want to certify?
Define the items you would like to certify in this campaign.
Help
Roles / Entitlements
Accounts Only
Roles
Classifications
Equals
Add Filter
Additional Entitlements
Select Attribute ...
Cloud Access Groups
Cloud Access Roles
Cloud Access Scopes
Cloud Provider
Display Name
Certifying all Target Permissions
Filter Target Permissions
Cancel
Schedule Certification

Updating the CAMSync Service

This section provides information about the CAMSync service and the cloud access hints.

CAMSync Service

The cloud based search capability and cloud classifications rely on the new service CAMSync. The CAMSync service is responsible for synchronizing Cloud Access Management data into IIQ to enhance searching and classifications.

In a multi-server deployment, synchronization with the Cloud Access Management will only occur from the CAMSync service on one of the hosts. The active CAMSync service host will be chosen automatically, and automatic failover is supported.

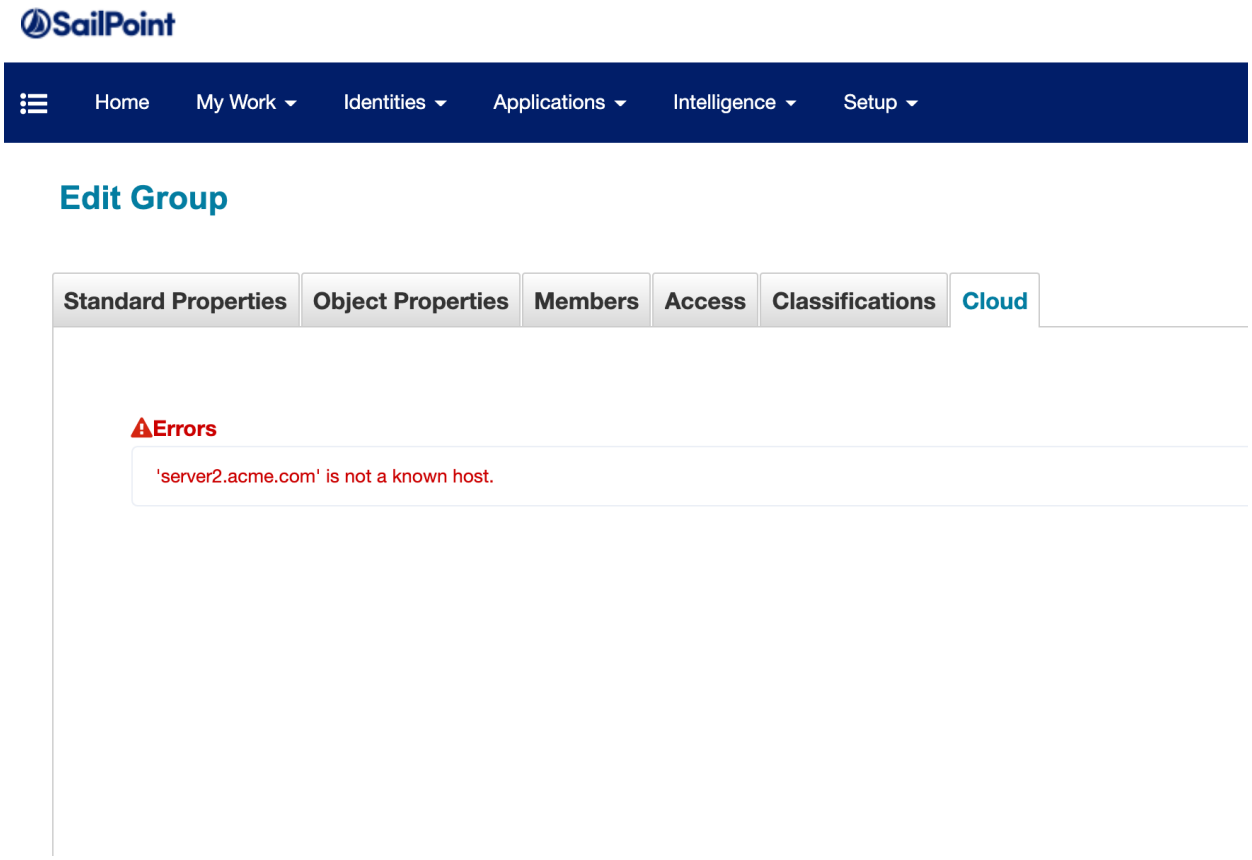
As described in Configuration, the Initiate Events button under **Gear menu > Global Settings > Cloud Access Management Configuration** must be clicked once to initiate the flow from Cloud Access Management into IdentityIQ via the CAMSync service. All data from Cloud Access Management will be received, and future changes to the data will then arrive upon occurrence. However, for unusual circumstances, an additional click on the Inititate Events button can be done to force a full refresh of all data from Cloud Access Management again.

Troubleshooting

The following are a couple of errors that may appear depending on if information was entered correctly.

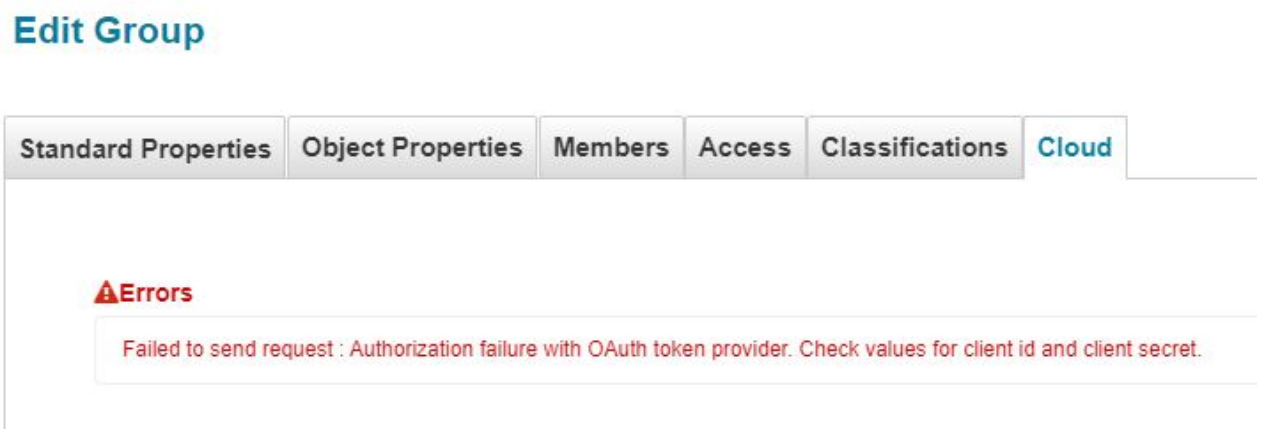
Wrong Hostname

When configuring Cloud Access Management within Global Settings, if the Cloud Access Management hostname was entered incorrectly, the following error will display when clicking the cloud tab within Edit Group.



Wrong Client ID

When configuring Cloud Access Management within Global Settings, if the Cloud Access Management Client ID was entered incorrectly, the following error will display when clicking the cloud tab within Edit Group.



Additional Configuration Details

The SystemConfiguration Configuration object contains the following key when Cloud Access Management is installed:

- <entry key="camEnabled" value="true"/>

The CAMConfiguration Configuration object contains the following keys:

Key	String	Description
clientId	string	OAuth client id
clientSecret	string	OAuth client secret (encrypted)
hostname	string	Cloud Access Management hostname
oauthHostname	string	OAuth access token hostname
connectTimeoutSeconds	integer	Maximum time in seconds to wait for a connection to succeed to Cloud Access Management APIs before failing. default = 10
readTimeoutSeconds	integer	Maximum time in seconds to wait for a response from Cloud Access Management APIs before failing default = 60
eventAcknowledgeEndpoint	string	default = /tqr/v1/messages/acknowledge
groupsEndpoint	string	default = /v1/resources/groups
messagesEndpoint	string	default = /tqr/v1/messages

Key	String	Description
rolesEndpoint	string	default = /v1/resources/roles
scopesEndpoint	string	default = /v1/resources/scopes
servicesEndpoint	string	default = /v1/resources/services
subscribersEndpoint	string	default = /tqr/v1/subscribers
subscriptionsEndpoint	string	default = /tqr/v1/subscriptions
supportedAppTypes	map	By default, AWS and Azure applications are supported.
doInitialization	boolean	Default of false. Upon clicking the Event Initialization button, this is set to true. When true, a CAMSync iteration will request an event initialization (getting all data). When the event initialization request has completed (whether success or failure), this is set back to false.
eventGroupId	string	Default of null. The first time the CAMConfigBean is instantiated (i.e. - whenever the CAMConfiguration is queried or modified the first time in Identity IQ), this is set to iiq_<uuid>, where uuid is generated.
initializationError	string	Default of null. If an error occurs during the initialization request, it is set in this field. A non-null initializationError will display on the CAM Configuration UI page.
initializationHost	string	Default of null. This is set to be the host that requests an event initialization.
initializedDate	date	Default of null. This is set to the date of an event initialization.

Logging

The following logs can be helpful to troubleshoot the Cloud Access Management integration:

 # CAMSync service top-level

logger.camsyncservice.name=sailpoint.server.CAMSyncService

logger.camsyncservice.level=debug

 # Calls to Cloud Access Management APIs

logger.camservice.name=sailpoint.cam.CAMService

logger.camservice.level=info

 # CAMSync service event director

logger.cameventdir.name=sailpoint.cam.CAMEventDirector

logger.cameventdir.level=debug

 # CAMSync service event persistence

logger.cloudaccessorizer.name=sailpoint.cam.CloudAccessorizer

logger.cloudaccessorizer.level=debug

 # CAMSync service event listening

logger.camsynch.name=sailpoint.server.CAMSynchronizer

logger.camsynch.level=debug

 # Request CAM event data when creating new entitlements

logger.camstats.name=sailpoint.api.aggregation.CAMStatisticsCommand

logger.camstats.level=DEBUG

 # Filters to search for Cloud Access Management based entitlements

logger.camurisearch.name=sailpoint.search.CloudAccessUriFilterBuilder

logger.camurisearch.level=debug

logger.camdnsearch.name=sailpoint.search.CloudAccessDisplayNameFilterBuilder

logger.camdnsearch.level=debug

Module Status

The status of the Cloud Access Management integration can be viewed under Gear icon > **Administrator Console > Environment > SailPoint Modules & Extensions**, and then click on the CAMServices name in the list.