



Cloud Access Management Integration

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

- Getting Started** **1**
- Setup** **2**
 - Installation 2
 - Configuration 2
 - Operating Verification 4
- Cloud Based Search Options** **5**
- Cloud Based Locations** **8**
 - Cloud Tab Locations 8
 - Cloud Classifications 14
- Associations** **15**
- Targeted Certifications Cloud Filtering** **16**
- Updating the CAMSync Service** **18**
 - CAMSync Service 18
- Troubleshooting** **19**
 - Wrong Hostname 19
 - Wrong Client ID 19
 - Additional Configuration Details 20
 - Logging 21
 - Module Status 22

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.

Module & Extension Name	Description	Status
CAMServices	Cloud Access Management Extension	1 ↕
FAM	File Access Manager Extension	1 ↕

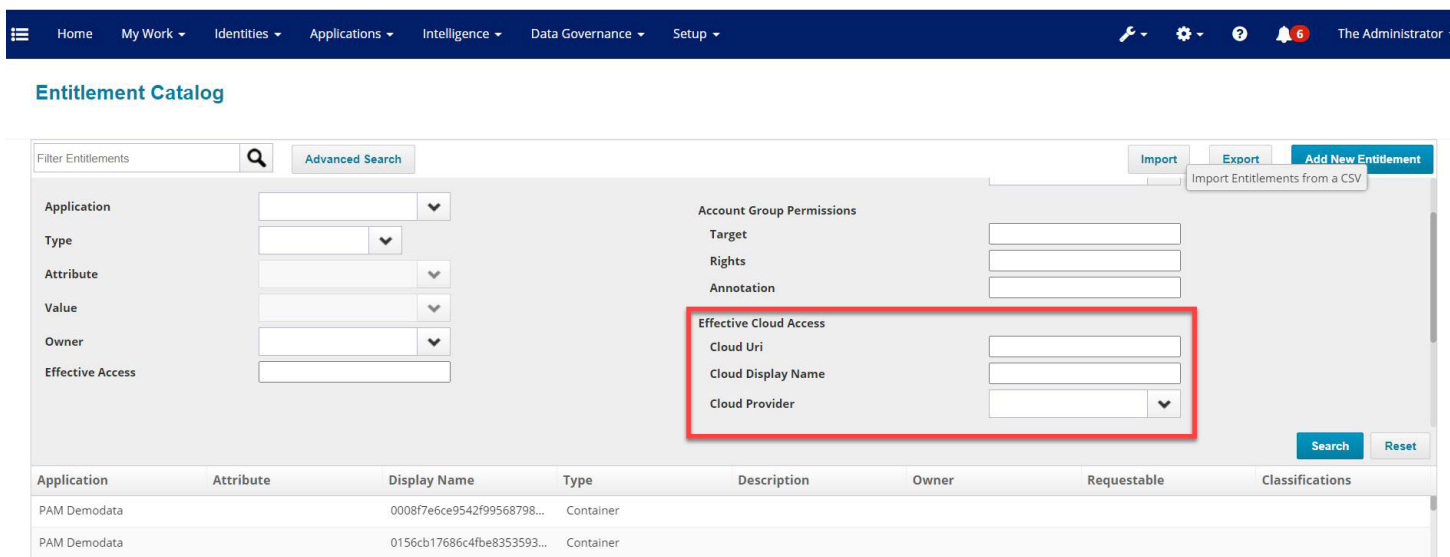
Showing 1-2 of 2

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.

Cloud Based Search Options

1 Select Users
Find and select users for whom you want to manage access.

2 Manage Access
Add access for the users you've selected.

3 Review and Submit
Look over your selections and confirm.

Add Access Remove Access

Search By Keywords Search Access

Identities Selected: Aaron Nichols

Filter Access

Role Type

Entitlement Owner

Entitlement Rank

Role Classifications

Entitlement Classifications

Entitlement Application

Entitlement Authorization

Entitlement Attribute

Entitlement Email

Previous Next

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.

Home My Work Identities Applications Intelligence Setup

Manage User Access

1 Select Users
Find and select users for whom you want to manage access.

2 Manage Access
Add access for the users you've selected.

3 Review and Submit
Look over your selections and confirm.

Add Access Remove Access

Search By Keywords Search Access

Identities Selected: Mary Johnson

Search For Access

Use the search or filter options above to find access items.
Your search results will show up here.

[Browse all access items](#)

Previous Next

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.

SailPoint

Home My Work Identities Applications Intelligence Setup

Advanced Analytics

Search Type: Entitlement

Advanced Search

Entitlement Attributes

Standard Attributes

Attribute: [Text Field]
Owner: [Dropdown]
Value: [Dropdown]
Application: [Dropdown]
Type: [Dropdown]
Classification: [Dropdown]
Effective Access: [Text Field]

Searchable Attributes

attr_demoAuthorization: [Dropdown]
attr_demoEmail: [Dropdown]
attr_demoRank: [Dropdown]

Account Group Permissions

Target: [Text Field]
Rights: [Text Field]
Annotation: [Text Field]

Effective Cloud Access

Cloud Uri: [Text Field]
Cloud Display Name: [Text Field]
Cloud Provider: [Dropdown]

Entitlement Fields

Annotation
 Application
 attr_demoAuthorization
 attr_demoEmail
 attr_demoRank
 Attribute
 Classifications
 Display Name
 Owner
 Rights
 Target
 Type
 Value

Run Search Clear Search

© Copyright 2021 SailPoint Technologies. All rights reserved.

Cloud Based Locations

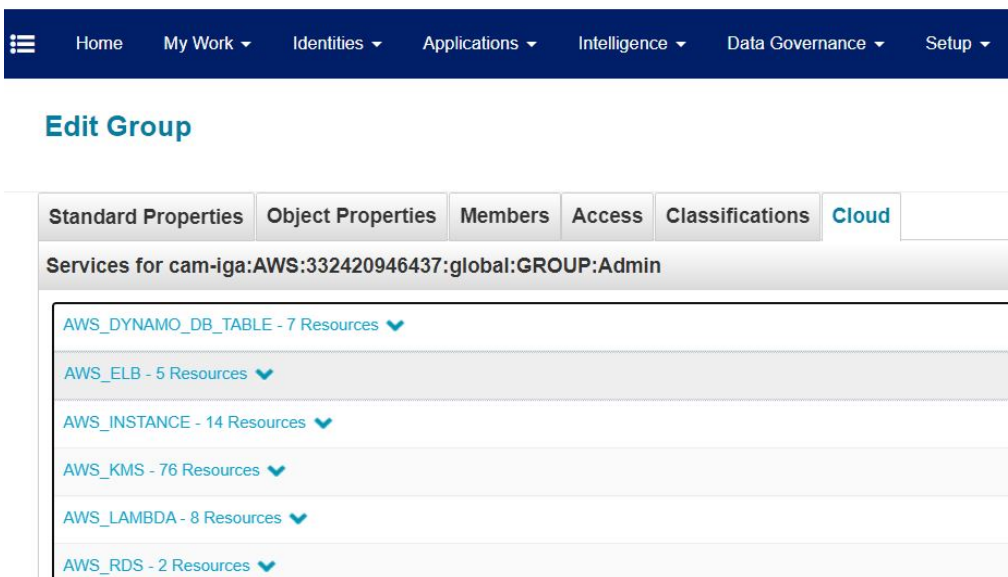
After the Cloud Access Management module is integrated, IdentityIQ will retrieve at display time additional entitlement details from Cloud Access Management and display them in a new Cloud tab.

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.

Attributes Entitlements Application Accounts Policy History Risk Activity User Rights Events

Oleg was last refreshed on 4/8/21 at 4:48:05 AM Direct Effective

Roles

Filter by role name

Name	Description	Classifications	Assigned By	Allowed By	Acquired	Application	Account Name
No data to display							

Page 0 of 0

Entitlements

Filter by attribute Filter by application Show only additional entitlements

Attribute	Entitlement	Classifications	Application	Account Name
CustomerManagedPolicies	AzureUserPolicy		AWS - CAM	Oleg
Groups	Admin			
AWSManagedPolicies	AdministratorAcc			
CustomerManagedPolicies	Amit-to-Travis			
InlinePolicies	OlegAssumeRole			
AWSManagedPolicies	AdministratorAcc			
CustomerManagedPolicies	SecurityAuditPol			
Groups	Developer			
Groups	Arch			
InlinePolicies	OlegAssumeRole			
groups	Support			
servicePrincipals	AAD Request Ve			
groups	Oleg-24-07			
groups	Oleg-17-06			
groups	DEMO-AWS-Der			
servicePrincipals	OrkusTest			
servicePrincipals	AWS Oleg			
groups	OUI			

qa-oleg-aws Object Details

Roles

Services

owner - AZURE

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.

The screenshot displays the 'Accounts' tab in a management interface. At the top, there are navigation tabs: Details, Configuration, Correlation, Accounts (selected), Risk, Activity Data Sources, Rules, and Password Policy. Below the tabs is a search bar labeled 'Filter by Name'. A table lists accounts with columns: Account ID, Account Name, Status, and Last Refresh. The table contains several entries, including 'MS', 'Test Denys Volkov', 'OlegDenys', 'Manoj Guglani', and 'Oleg'. A modal window titled 'Oleg-17-06 Object Details' is open over the 'Oleg' account. This modal has tabs for 'Standard Properties', 'Object Properties', 'Members', and 'Cloud'. The 'Roles' section lists 'contributor - AZURE', 'proper-access - AZURE', and 'reader - AZURE'. The 'Members' section shows 'CrayonAdmin'. The 'Cloud' section is currently empty. A 'Close' button is at the bottom right of the modal.

Delegated Work Items

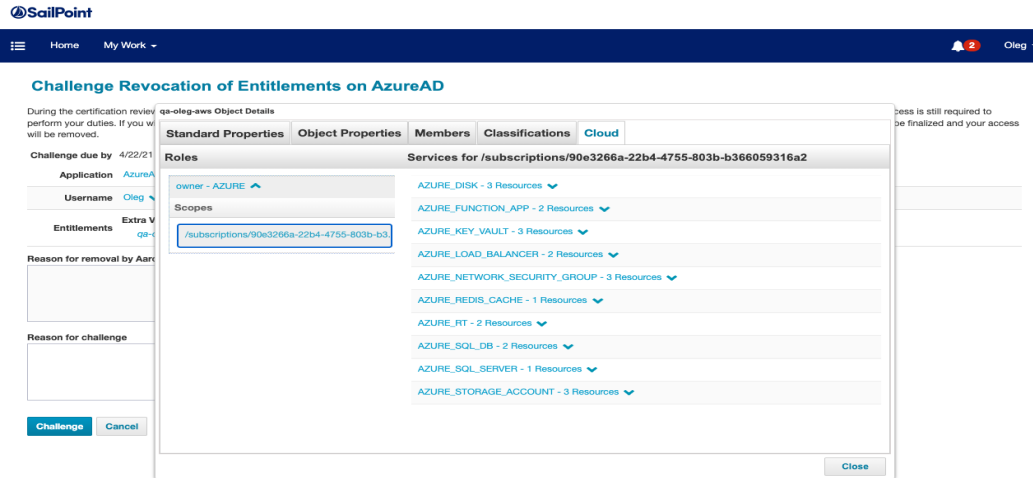
After selecting a work item, click on the entitlement. The same dialog as the Identity Warehouse will display.

View Work Item 207

The screenshot shows the 'View Work Item 207' dialog. It has a 'Summary' section with the following details: Work Item ID: 207, Requester: The Administrator, Owner: Alan Bradley, Description: Certify the 'AzureAD' entitlement on 'CrayonAdmin', Created: Mar 9, 2021 10:49:42 AM, Expiration: Mar 8, 2021 7:08:58 PM, Priority: Normal, History: None. Below the summary is a 'Send Comment to Requester' section with an 'Add Comment' button. At the bottom, there are tabs for 'Decisions', 'Recent Changes', 'Employee Data', and 'Risk Data'. The 'Decisions' tab is active, showing a table of 'Additional Entitlements' with columns for Decision, Account Name, Attribute, and Entitlements. The table shows one entry for 'CrayonAdmin' with attribute 'groups' and entitlement 'Ous6'. A legend at the top of the Decisions tab includes icons for Approve, Revoke, Allow Exception, Delegate, and Action Required.

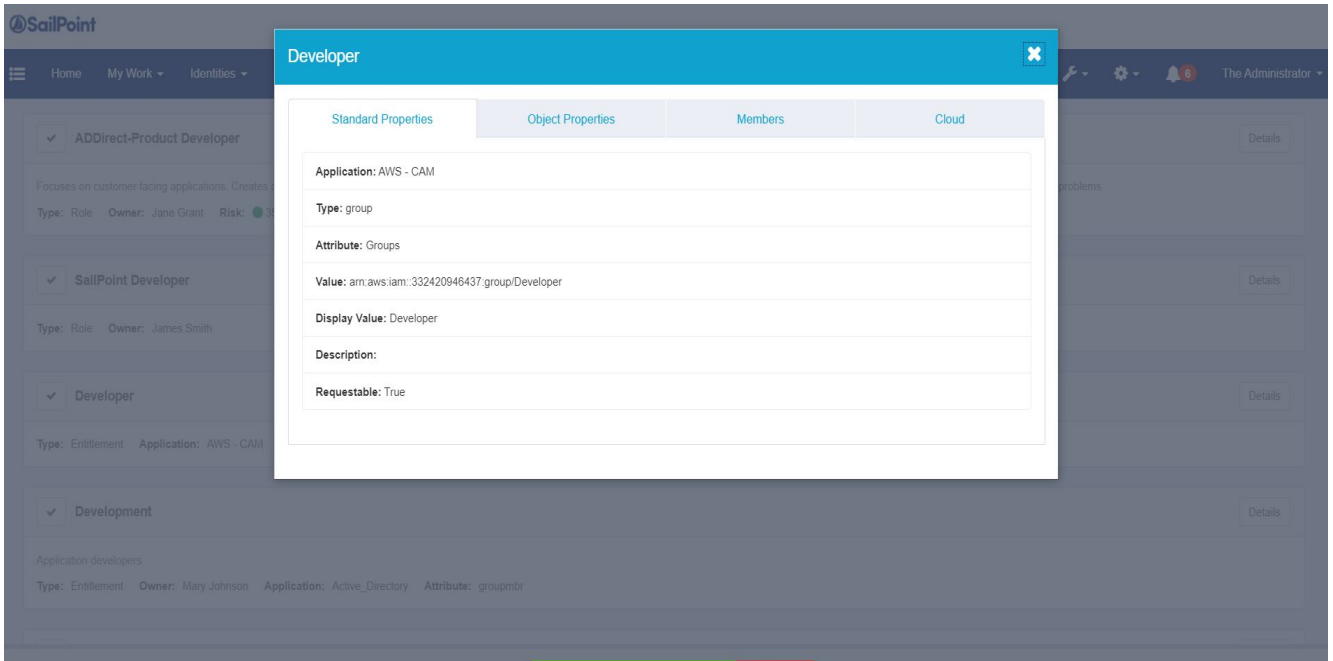
Challenge Work Items

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



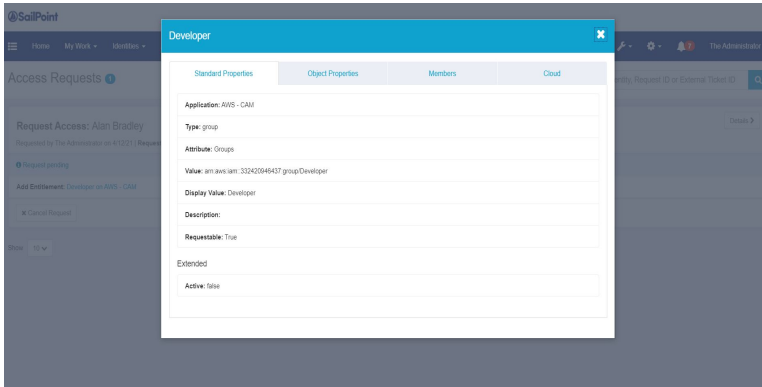
Manage User Access

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.



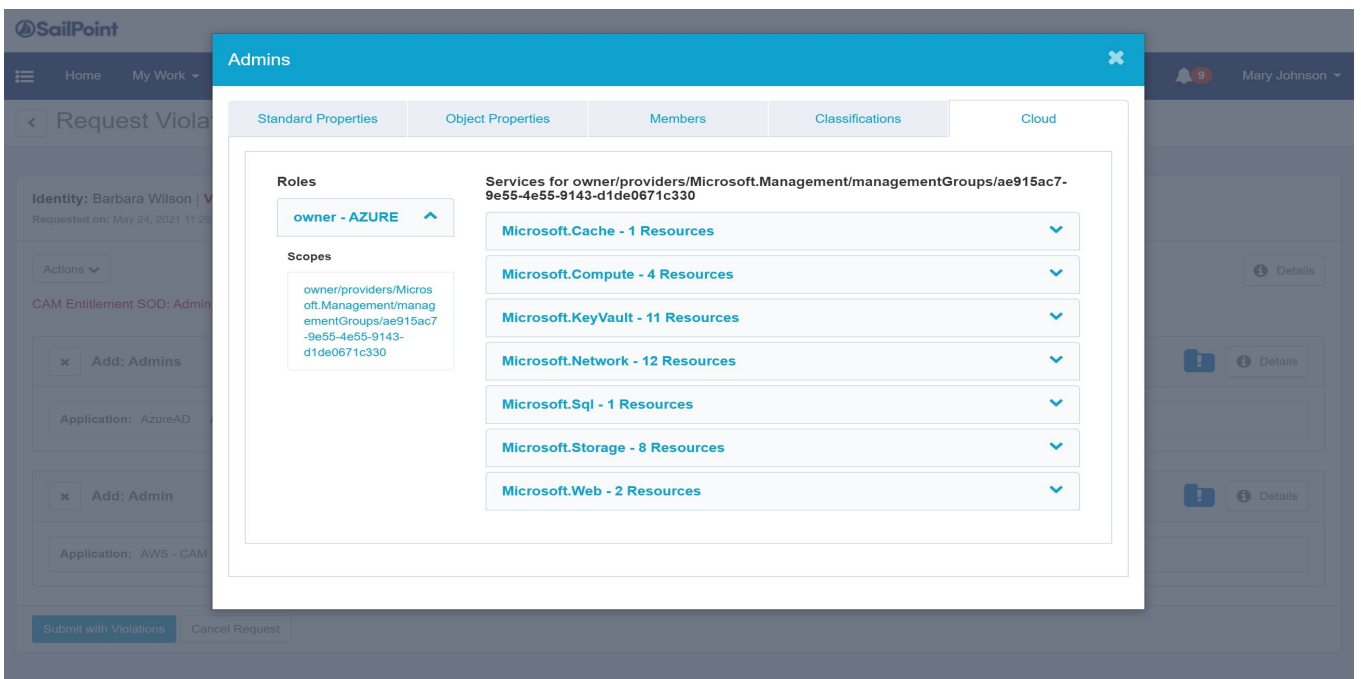
Access Request

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



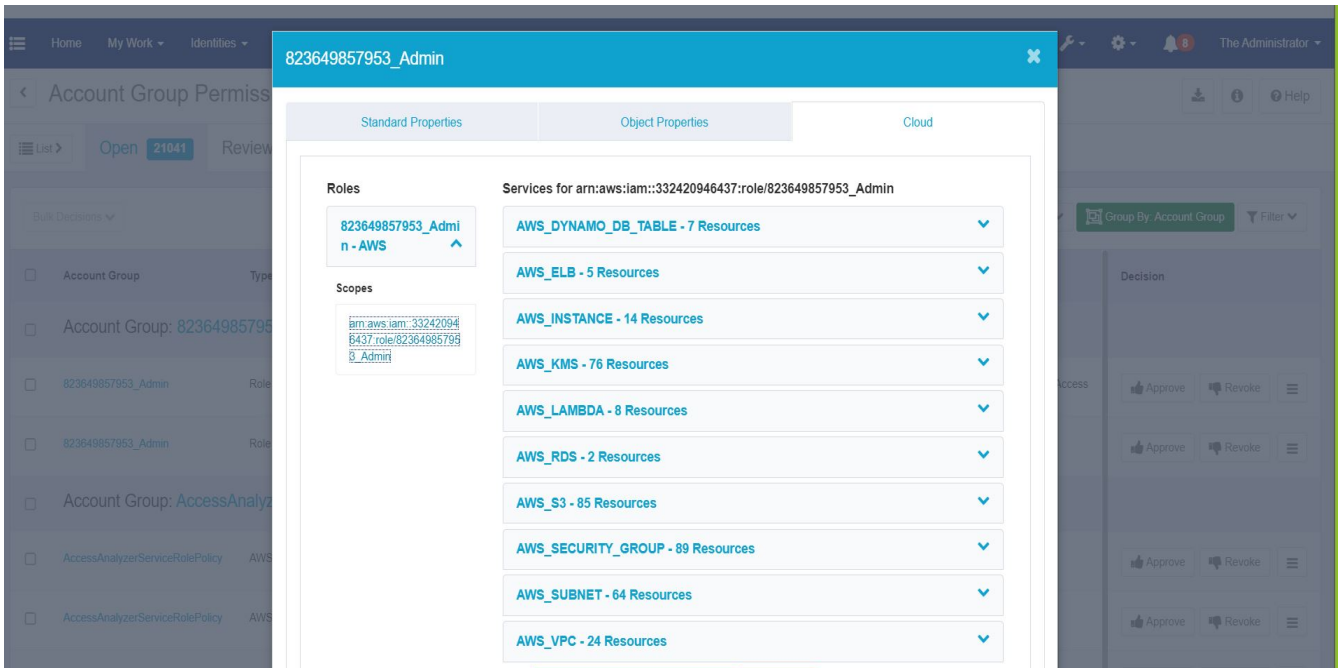
Request Violation

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

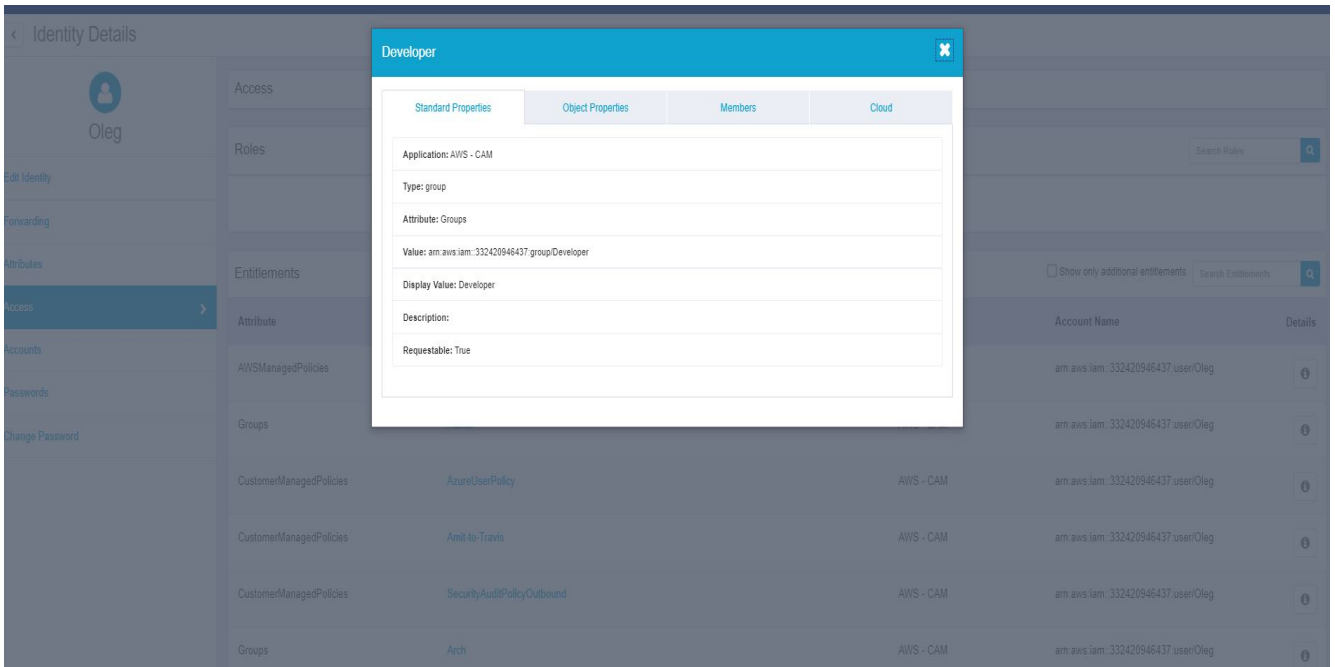
This Cloud tab will display when scheduling a certification. Choose the desired cloud application, then click on Account to view the Cloud tab.



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

Application	Attribute	Display Name	Type	Description	Owner	Requestable	Classifications
AzureAD	groups	Oleg-17-06	Group			✔	Azure
AzureAD	groups	Oleg-24-07	Group			✔	AWS, Azure
AWS - CAM	InlinePolicies	OlegAssumeRoleEC2	InlinePolicy			✔	
AWS - CAM	InlinePolicies	OlegAssumeRoleS3	InlinePolicy			✔	
AWS - CAM		OlegBoundaryLambda	Role				AWS
AWS - CAM		OlegEC2	Role				AWS
AWS - CAM		OlegLambda	Role				AWS
AWS - CAM		OlegS3	Role				AWS
AWS - CAM		OlegS3AzureDP	Role				AWS

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.

Targeted Certifications Cloud Filtering

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.

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

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 Initiate Events button can be done to force a full refresh of all data from Cloud Access Management again.

Troubleshooting

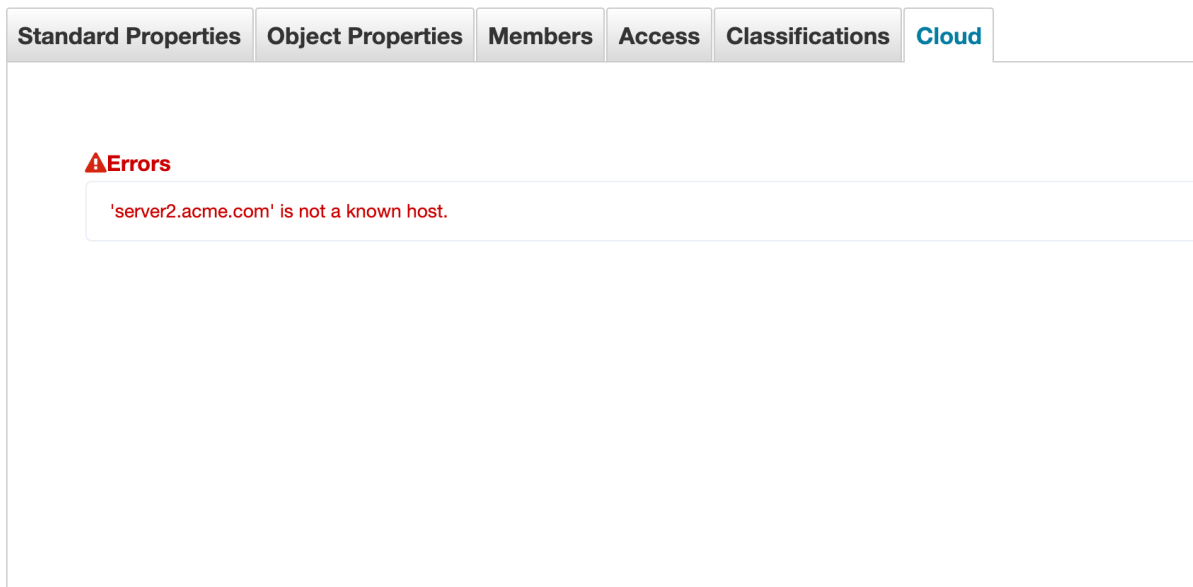
The following are a couple of errors that may appear depending on if information was entered correctly.

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.



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.

Edit Group

Standard Properties

Object Properties

Members

Access

Classifications

Cloud

Errors

Failed to send request : Authorization failure with OAuth token provider. Check values for client id and client secret.

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.