Classifications

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

Classifications

Classifications let you flag and categorize roles and entitlements, to help ensure the security and integrity of your access governance practices. Classifications can alert you when requesting, granting, or approving a user's access will give that user access to sensitive, protected, or otherwise significant data.

In IdentityIQ, classifications are typically used to flag access to sensitive data, such as financial, personal, or health-related information, but you can use classifications to identify any kind of access your business needs to pay special attention to.

Classifications can be used in certifications and policies, to help you monitor and control the access your users have to sensitive data. You can configure access requests, approvals, and access reviews to show a classification icon with any role or entitlement that grants access to sensitive data, so that the users responsible for making access decisions can quickly and easily see which entitlements allow potentially risky access.

This section includes:

Where Classification Data Comes From

IdentityIQ's classification functions are designed to integrate with SailPoint's File Access Manager module, to provide robust and seamless governance of sensitive data.

You can also implement classifications using data from sources other than File Access Manager, allowing you to tailor your classifications solution to your particular business needs.

File Access Manager Classifications

In File Access Manager, classification categories are assigned to Business Resources (folders). Classifications typically flag sensitive data, but can flag anything you configure File Access Manager to monitor. In many cases, access to classified data is granted through account groups - most typically, Active Directory Groups - such that users' membership in those groups indirectly grants access to that data. For example, a company's Human Resources group might have access to employees' personal data, or a hospital's group of doctors might have access to medical records. When you include File Access Manager's classification data in your IdentityIQ installation, you can see the implications of users' existing (and requested) group memberships, to better inform your access governance decisions in IdentityIQ.

For more information about how data is classified in File Access Manager, refer to the File Access Manager documentation.

Classifications from Other Sources

You can bring classification data into IdentityIQ from sources other than File Access Manager, or define your classification data independently in IdentityIQ, by importing the classification data as an XML object. To import an XML object, use the iiq console or the **gear menu > Global Settings > Import From File** feature.

Here is an example of what a classification object might look like. This example includes a name, display name, source of origin for the data, and localized descriptions for the classification.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Classification PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<Classification id="" name="PHI" displayName="Protected Health Information" ori-
gin="MyIndependentDataSource">
  <Attributes>
    <Map>
      <entry key="sysDescriptions">
        <value>
          <Map>
           <entry key="en_US" value="Allows access to Protected Health Information"/>
           <entry key="fr_FR" value="Permet l’accès aux informations de santé
protégées"/>
          </Map>
        </value>
      </entry>
    </Map>
  </Attributes>
</Classification>
```

Working with Classifications in IdentityIQ

Classifications in IdentityIQ are managed as attributes on entitlements; if you are integrating with File Access Manager, these entitlements will most typically be group entitlements. For example, a Human Resources group is aggregated into IdentityIQ as a group entitlement; if this group is categorized in File Access Manager (or some other source) as having access to sensitive information, an attribute that flags the Human Resources group entitlement as having this access is added to the group entitlement. Once you have defined classifications in IdentityIQ, you can apply classification attributes to any entitlement, not just group entitlements.

Entitlements are managed in IdentityIQ, using IdentityIQ's range of compliance and lifecycle management features, such as access requests, certifications and access reviews, policies, and reporting.

You can view and manage classifications in these areas of IdentityIQ:

Lifecycle Manager Global Setting for Access Requests and Approvals

A global setting in Lifecycle Manager determines whether classification data is shown with the access items (such as roles or entitlements) that you can request for users in the Manage Access feature. This global setting is provided so that you can choose whether or not to alert requesters to the fact that certain roles or entitlements may allow access to sensitive or protected data.

To enable the display of classifications in Access Requests:

1. Click the **gear menu > Lifecycle Manager**.
2. On the **Configure** tab, scroll to the **Manage Classifications Options** section.
3. Check the **Display classifications in Access Request** box.
4. **Save** your change.

If this setting is enabled in Lifecycle Manager, roles and entitlements are flagged with relevant classification information in the Access Requests pages. You can click the Details button for flagged roles and entitlements, to see more information about the classifications.

Classification data also appears in the Approvals page for access requests. Classification flags always appear in the Approvals page, regardless of the setting in the Lifecycle Manager's **Manage Classifications Options** section, since reviewers will always need to know when granting access will allow access to sensitive or protected data.

Adding Classifications to Roles and Entitlements

For File Access Manager integrations, classifications can be added to entitlements by running a task. This process is described in more detail in Integrating with File Access Manager for Classifications.

For classifications that come from a source other than File Access Manager, classifications can be added manually to roles and entitlements.

To add classifications to a role:

1. Click **Setup > Roles**.
2. To add classifications to existing roles, find the role you want to edit in the Role Viewer, then click **Edit Role**; for new roles, click **New Role > Role.**
3. In the **Role Editor**, select the classifications you want to add from the drop-down list.
4. **Save** your changes.

You can also include classifications as criteria in “Match List” **Assignment Rules** for the role. Assignment Rules are used to automatically assign roles to identities during a correlation process.

In the **Role Search** tab you can include classifications as search criteria.

To add classifications to an entitlement:

1. Click **Applications > Entitlement Catalog**.
2. To add classifications to existing entitlements, use the **Filter** field or **Advanced Search** to find the entitlement you want to edit; for new entitlements, click **Add New Entitlement**.
3. On the **Classifications** tab, select the classifications you want to assign from the drop-down list, then click **Add** to assign the classification.
4. **Save** your changes.

In the **Advanced Search** feature of the Entitlement Catalog, you can include classifications as search criteria.

Classifications in Certifications and Access Reviews

When scheduling a certification campaign, you can opt to show classification data in the campaign's access reviews. Classifications can be shown in Manager, Application Owner, Advanced, Role Membership, and Targeted certifications. You can also use classifications as a criterion for what to certify, in Targeted certifications.

You can set a global default to show classifications for all your certification campaigns, and modify the default setting in any individual certifications you schedule.

To set the global default for showing classifications in your certification campaigns:

1. Click the **gear menu > Compliance Manager**.
2. In the **Behavior** section, use the **Show Classifications** checkbox to enable or disable showing classifications by default.

Classifications in Policies and Policy Violations

In **Advanced** policies, you can use classifications as criteria for your policy rules.

To add classifications to an Advanced policy rule:

1. Click **Setup > Policies**.
2. To add classifications to an existing policy, use the **Filter** field or **Advanced Search** to find the policy you want to edit; for new policies, click **New Policy** > **Advanced Policy.**
3. Click **Create New Rule**, or double-click an existing rule you want to edit. Classifications can be used as rule criteria in Match List, Rule, Script and Filter rules.
   Rules and scripts are written in BeanShell, and Filters are an XML specification.
4. For Match List rules:
   a. Under **Selection Method**, choose **Match List**.
   b. Click **Add Role Attribute** or **Add Entitlement Attribute**.
   c. In the **Name** field choose **Classification**.
   d. Choose an operator: **Equals**, **Not Equals**, or **Is Null**.
   e. In **Value**, type the name of the classification to use. (To find the name of a classification, you can use the Debug pages to open the classification object and find the name value.)
5. When you have added all the classification criteria you want to use, you can run a simulation of the rule, or click **Done** to save your changes and exit.

Classifications in Advanced Analytics

In the Advanced Analytics page, you can search for roles and entitlements using classifications as search criteria.

1. Click **Intelligence > Advanced Analytics**.
2. Choose **Role** or **Entitlement** as the **Search Type**.
3. Choose a classification to search on, from the drop-down.
4. If you want to see classification details in your search results, select **Classifications** in the **Fields to Display** panel.
5. Click **Run Search**.

Classifications in the Identity Warehouse

To see which entitlements a user has that are flagged with classifications, in the Identity Warehouse:

1. Click **Identities > Identity Warehouse**.
2. Select an identity.
3. Click the **Entitlements** tab. Any entitlement or role with a classification assigned to it is flagged with the classifications icon.

Classifications in the Edit/View Identity Page

The Manage Identity feature shows classifications for entitlements on identities.

1. In the Quicklinks menu, click **Manage Identity**
2. Choose **Edit Identity** or **View identity**.
3. Click on the identity; the **Access** panel for the identity shows a classification icon for any entitlements with classifications assigned. Click the classification icon for more details.

Integrating with File Access Manager for Classifications

For integration with File Access Manager's classification feature, the initial installation and configuration involves two steps:

1. Import the `init-fam.xml` file into IdentityIQ, using the iiq console or the **gear menu > Global Settings > Import From File** feature.
2. Click **gear menu > Global Settings > File Access Manager Configuration**.

Field Name	Description
File Access Manager Hostname	The hostname of the File Access Manager website. For example, `https://web-client.mydomain.com`
Basic/OAuth	Choose your method of authenticating with the File Access Manager website. **Basic** uses a username and password. **OAuth** uses a client ID and client secret. Basic authentication can be used for identities that are configured in the File Access Manager Administrative Client as having the API User privilege. OAuth credentials can be retrieved from the File Manager website, through the **Settings > General > API Authorization** menu.
Username	For Basic authentication: the username for logging in to the File Access Manager web client. This identity must have the API User privilege in File Access Manager.
Password	For Basic authentication: the password for logging in to the File Access Manager web client.
Client ID	For OAuth authentication: the Client ID for logging in to the File Access Manager website. This value is stored in the File Access Manager website in **Settings > General > API Authorization**.
Client Secret	For OAuth authentication: the Client Secret for logging in to the File Access Manager website. This value can be copied from the File Access Manager website in **Settings > General > API Authorization**.
SCIM Correlation Rule	If the correlation logic in your configured applications does not meet your needs for correlating File Access Manager groups and accounts against IdentityIQ groups, you can use a custom rule to manage correlation. The rule must have a rule type of `Correlation` in order to appear in this dropdown.
SCIM Correlation Applications	Select the applications to correlate File Access Manager groups and accounts against. Typically these will be Active Directory applications.

If you are implementing classifications that come from a source other than File Access Manager, you do not need to take any special steps to configure the feature. You can import your classification objects directly into IdentityIQ and manage classifications as described in the sections above.

File Access Manager Classification Process

Bringing classification data from File Access Manager into IdentityIQ, and including classifications in your lifecycle and data governance practices, is a multi-step process. An overview of these processes is provided here.

This section assumes you have already completed the configuration in File Access Manager to classify resources and identify which groups have access to those resources. It also assumes that you have applications configured in IdentityIQ for aggregating group and account data.

When you work with classifications that originate in File Access Manager, the assumption is that both the IdentityIQ instance and the File Access Manager instance use the same group data. If this is not the case, you may need to configure rule-based logic to correlate your File Access Manager accounts and groups with your IdentityIQ accounts and groups. You can specify a custom correlation rule for this aggregation in **Global Settings > File Access Manager Configuration**, in the **SCIM Correlation Rule** field.

At a high level, these are the steps for aggregating and managing classifications from File Access Manager.

Application Configuration

1. Configure the IdentityIQ application(s) that aggregate group data. As part of this configuration, you must specify a correlation key in each application's group schema, to correlate groups in IdentityIQ to groups in File Access Manager.
   For Active Directory applications, the group schema attribute to set as the correlation key is MsDs-PrincipalName.
2. In the **File Access Manager Configuration** (under the **gear menu > Global Settings**), add each of the applications that aggregate group data to the **SCIM Correlation Application** field.

Run Tasks to Aggregate and Process Classification Data

IdentityIQ uses tasks to aggregate accounts, groups, and File Access Manager classification data. If you do not already have tasks set up to aggregate accounts and groups, you will need to set these tasks up as part of implementing this feature. You must also create and configure a File Access Manager Classification task.

For more information see the **Tasks** documentation.

These tasks should be run on a recurring basis, to keep your classification data in IdentityIQ current.

1. Run a task to aggregate groups. Typically these will be Active Directory groups.
2. Run a **File Access Manager Classification** task. See the **Tasks** documentation for more information.
3. *Optional*: Run an **Effective Access Indexing** task. You only need to run this task if you are tracking classification data for effective access items. These options are important for managing classifications on effective access items:

Index classifications

Use this option to add an entitlement's classifications to the target association that is created when the entitlement target is indexed; in the UI, this means that an entitlement's classifications will be displayed whenever that entitlement occurs as Effective Access. For example, if an IT role contains EntitlementA, and EntitlementA has a classification, the indexing option will make EntitlementA's classification also appear on that role.

Promote classifications

Promote is used with applications such as Active Directory that can have "nested" entitlements, to ensure that classifications are adorned to all entitlements along the effective access chain. For example, if EntitlementA grants you effective access to EntitlementB, and EntitlementB has a classification assigned to it, then with the Promote Classifications option enabled, the classification assigned to EntitlementB will also be displayed in the UI for EntitlementA.