IdentityIQ System Configuration

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

System Setup

Use System Setup to configure the different options for IdentityIQ. To access System setup options, click the gear icon on the Navigation menu bar and select from the list of options that can include:

> Caution: Do not open multiple tabs or browsers. Opening multiple tabs might overwrite changes made in the other.

> Note: Because configuration options are based on your deployment, your available options may vary from the set of options in this guide.

- IdentityIQ Global Settings
- Lifecycle Manager Setup in the **Lifecycle** documentation
- Compliance Manager

IdentityIQ Global Settings

From the Navigation bar, click the gear icon and then select **Global Settings**. Use the Global Setting index page to select the items you want to configure. The following table displays the available options.

> Note: You must be a System Administrator to access this page.

IdentityIQ Configuration

Set default values for use with notifications, work item policy, object expiration, user interface preferences, and identity history. See IdentityIQ Configuration.

Login Configuration

Set an application other than IdentityIQ for authentication verification and select the automatic identity creation rule. See Login Configuration.

Identity Mappings

Specify the applications, and application attributes, from which the identity data, is derived. See Identity Mappings.

Account Mappings

Specify the account attributes to be used in filters and searches throughout the application. See Account Mappings.

Rapid Setup

Configure global options for Rapid Setup in IdentityIQ for joiners, movers, leavers, immediate termination, and business processes in your organization. See Rapid Setup Configuration.

Application Attributes

Define application attributes in addition to those provided by the connectors. See Application Attributes.

Entitlement Catalog Attributes

Define custom extended entitlement attributes and role types. See Entitlement Catalog Attributes.

Quicklink Populations

Configure the quicklink populations for IdentityIQ. See Quicklink Populations.

Forms

Configure forms for workflows, role provisioning policies, and application provisioning policies in IdentityIQ. See Forms.

Role Configuration

Define custom extended role attributes and role type. See Role Configuration.

Scopes

Define scopes for use throughout your enterprise. See Scopes.

Time Periods

Define the time periods for use in activity searches. See Time Periods.

Audit Configuration

Specify the actions that are audited and stored in the audit logs. See Audit Configuration.

Electronic Signatures

Configure electronic signatures and their displayed meanings. See Electronic Signatures.

API Authentication

Import files into IdentityIQ. See API Authentication.

AI Services Configuration

> Note: This link is present only if you have purchased the AI Services product.

Connect IdentityIQ to the AI Services product. See AI Services Configuration.

File Access Manager Configuration

> Note: This link is present only if you have imported the File Access Manager module.

Configure IdentityIQ to connect to File Access Manager. See File Access Manager Configuration.

Cloud Access Management Configuration

> Note: This link is present only if you have purchased the Cloud Access Management module.

Configure IdentityIQ to use Cloud Access Management, including connection information, timeouts, and initiating data synchronization. See Cloud Access Management Configuration.

Import from File

Import files into IdentityIQ. See Import From File.

IdentityIQ Configuration

Use this page to set default values for use with notifications, work item policy, object expiration, user interface preferences, and identity history. This page contains the following tabs:

- Notification Settings
- Work Items
- Identities
- Roles
- Passwords
- Miscellaneous
- Privileged Account Management

Multi-language Description Files

Some escaped HTML characters are not recognized and do not display in descriptions if they are formatted using those characters. You must ensure that all files are formatted correctly before importing them into IdentityIQ and referencing them from the product. Use the following examples to format the HTML correctly:

```
test (to appear in bold) - <b>test</b>
<test> - &lt;test&gt;
<test> (to appear in bold) - <b>&lt;test&gt;<b\>
<<test>> - &lt;&lt;test&gt;&lt;
“test” - &quot;test&quot;
‘test’ - ‘test’
&test - &test
```

Using the Rule Editor

The Rule Editor lets you to edit any existing rule to your specifications. Click the “**...**” icon next to a rule drop-down list to access the rule editor throughout IdentityIQ. Choose to either create a new rule, or edit an existing rule structure.

The Rule Editor panel includes the following items:

Copy from an existing rule

Select an existing rule from the drop-down list. This option is available if you did not select a rule from the drop-down list on the previous page.

Code input area

Field where code is input. IdentityIQ recognizes BeanShell programing language. You can edit code from an existing rule or create a new one from scratch.

Description

Enter the description of your new rule.

Rule Name

Enter the name of your rule.

Rule Type

Non-editable field which displays the type of rule (for example, Violation).

Return Type

Non-editable field which displays the type of return (for example, PolicyViolation).

Arguments

Non-editable field which displays the arguments used in the rule (for example, log, context, state, etc.).

Returns

Non-editable field which displays the type of return the rule executes (for example, Violation).

When you have completed your rule edits, click **Save** to return to the previous page. The new rule is now available from the drop-down list.

Access Request Attachments

> Important: IdentityIQ does not perform file content validation or verification on attachments. It is your responsibility to ensure that only files that do not violate security policies within your environment are included as attachments.

> Note: Attachments are only allowed on single-user requests, and are only available for manual access requests.

The attachments feature enables users to add attachments to single user access requests. For example, you could attach training certificates or a notarized document of authorization.

By enabling attachments on the **Global Settings > IdentityIQ Configuration > Miscellaneous** tab, you are enabling, but not requiring, any user to add an attachment to any single user access request. When the feature is enabled, requests display the attachment icon, paper clip, on each item in a request, but the icon is only active if an attachment is allowed for that item. When you click the icon, the attachment overlay is displayed and you can add an attachment by dragging and dropping or uploading a file.

Attachments are controlled through AttachmentConfig rules. If there are no AttachmentConfig rules for an item, or they all have null or empty prompts, the attachment overlay contains no additional information.

Attachment Configuration

File attachment settings such as the maximum file size, maximum number of attachments per request, and the type(s) of files that can be attached to a request are configured on the Miscellaneous tab.

Attachments can be further configured through AttachmentConfig rules. When AttachmentConfig rules are set for file attachments, each of these rules is run with every request made. Use the AttachmentConfig rules to require attachments for specific access request scenarios and customize the prompts displayed on the attachment overlay. When an attachment is required, the word required is displayed with the attachment icon and an error is displayed if a request is submitted without an attachment.

Activate the attachment configuration rules to run with access requests by selecting them from the **Configuration Rules** list on the **Global Settings > IdentityIQ Configuration > Miscellaneous** tab under the gear icon.

You can import attachment configuration rules using the **Global Settings > Import from File** page under the gear icon.

To remove an attachment configuration rule from IdentityIQ, first de-select that rule from the **Configuration Rules** list and then delete the rule object.

These rules can be as simple or complex as the needs of your organization require.

These rules contain the following inputs:

- requestor – the user making the request
- requestee – the user for whom the request is being made

- requestItem – the item being requested
- action – the request action (add or remove)

Each attachment configuration rule is run once for each item being requested and returns a list of configuration objects.

The fields of an attachment configuration object are:

- required – boolean (true, false) where true means an attachment is required
- prompt – string – the prompt that is displayed in the attachment overlay when attaching files to this request item

Multiple attachment configuration objects can be associated with a single request item. In this case, the prompt strings are concatenated on the attachment overlay.

A file containing an example of attachment configuration rules is included in the IdentityIQ installation package. The `examplerules.xml` file is located in the *`IdentityIQ_HOME`*`/WEB-INF/config` directory.

Pruning Attachments

In rare cases attachments that are not associated with an access request might end up getting loaded into the database.The **System Maintenance** and **System Maintenance Object Pruner** tasks both include an option to prune those attachments and clean them out of your database. Use the Prune Attachments option in these tasks to delete any attachments that are more than 30 days old and and are not associated with an access request.

Files attached to abandoned access requests may also need to be cleared from your database. The **System Maintenance** and **System Maintenance Object Pruner** tasks both include an option to **Prune Pending Attachments**. When this option is selected, the task will delete any pending request attachments that are older than 12 hours. This timeframe can be overridden by adding an entry to the system configuration object called `pendingAttachmentPruneAge` with a value that represents a number of hours.

For auditing purposes, there is an audit event called **Prune Pending Attachments** which can be triggered during the cleanup in the System Maintenance Task. To enable auditing for attachment pruning, enable the **Prune Pending Attachments** option in IdentityIQ's Audit Configuration.

.

Notification Settings

Use this tab to set default values for how notifications are sent in IdentityIQ.

Email Settings

Email notifications can be sent using HTTP/OAuth authorization or SMTP/Basic authorization. You can also opt to redirect emails to a specific email address or to a file, which is useful for testing your email settings and templates.

Choose your **Email Notification Type**, then configure your email options as described below.

HTTP/OAuth

Choose this option to use the OAuth2 authentication protocol to send email notification via HTTP/HTTPS. This option is recommended for use with Microsoft Office 365, as an alternative to the SMTP/Basic method which has been deprecated by Microsoft.

> Note: IdentityIQ supports OAuth version 2.0

To use HTTP/OAuth with IdentityIQ, you need to register and configure IdentityIQ with your OAuth provider, and generate an access token to use for authenticating connection requests.

In addition, when working with Azure instances, you must set the Microsoft Graph **Mail.send** permission as an ***Application*** level permission; setting the permission type to *Delegated* does not provide sufficient access for this feature.

Email Service Endpoint

The email service endpoint for sending email notifications. Use the provided syntax as a guide, substituting your organization's preferred email address.

Token Endpoint

The token endpoint for the email notifier to use. Use the provided syntax as a guide, substituting your organization's tenant ID.

Refresh Token Endpoint

The refresh token endpoint for the email notifier to use. Use the provided syntax as a guide, substituting your organization's tenant ID.

Scope

The scope for the email notifier. The provided syntax enables the `/.default` scope, which is the least restrictive. You can edit this scope as needed.

Client ID and Client Secret

The OAuth Client ID and Client Secret for authenticating. For Azure Active Directory, these can be found in the Azure application registration page for your organization.

SMTP/Basic

Choose this option to use basic authentication for email notifications.

Encryption

Choose your email encryption type from the drop-down list: **NONE**, **SSL**, or **TLS**

Default SMTP Host

Your organization's default mail host.

Default SMTP Port

Your organization's default SMTP port.

Default From Address

The address to use as the **From** address for all notices automatically generated by IdentityIQ.

Username and Password

The username and password required to access the SMTP host.

Connection Timeout

The email socket connection timeout value in milliseconds.

If there are session properties defined in the notification template objects that are used to send the email, those will take precedence over this property.

Read Timeout

The email socket read timeout value, in milliseconds.

If there are session properties defined in the notification template objects that are used to send the email, those will take precedence over this property.

Redirect to Email

Choose this option to redirect all IdentityIQ emails to a specific email address. **The options you configure for this setting are the defined in the same way as the settings described above for SMTP/Basic**, with the addition of this option:

Redirection Email Address

The email address to which email should be redirected.

Redirect to File

Choose this option to redirect email to a file.

Redirection File Name

The name of the file to which email should be redirected.

Default From Address

The address to use as the **From** address for emails and notices generated by IdentityIQ.

Email Settings Common to All Notification Types

Every email notification type requires these configuration options:

Maximum Email Retries

Specify the maximum number of times to retry sending emails if a temporary error is returned. Set this to 0 to disable retries.

Suppress Duplicate Emails

Prevent the sending of multiple emails of the same type to the same recipient at one time. For example, if five work item reminders are generated for the same person at one time, they only receive an email for the first one. This option is used only for certification-related emails, and is enabled by default.

Notification Templates

Choose a template to use for each notification type. Notification templates are highly configurable; you can use IdentityIQ's provided defaults, or create your own. Detailed information about importing, customizing, and using IdentityIQ notification and email templates is in IdentityIQ Email Templates.

Email Task Alerts

You can configure IdentityIQ to send emails to users or groups with the status of tasks after completion. The settings defined here at the global level are typically used when the email notification configured at the task level is disabled. Note that email notification settings at the task level have priority over the global settings configured here. For example, if you set a global default to send task notifications to the Administrator, then configure "Task1" to send notifications to the IT Helpdesk and "Task2" without any notification settings, "Task1" will send notifications to the IT Helpdesk and "Task2" will send email notifications to the Administrator.

Refer to the **IdentityIQ Tasks** documentation for more information on choosing notification recipients and templates at the task level.

Email Notification

Select a frequency for email notification to be sent upon task completion:

- **Disabled** — no email notification sent on task completion
- **Warning** — send an email notification if the task results in a warning
- **Failure** — send an email notification if the task fails
- **Always** — always send an email notification upon task completion

Email Notification Template

Choose a notification email template from the drop-down list. The Task Status email template is provided out of the box as a default template for task notifications, but you can choose another template if you prefer. For details on creating your own custom email templates, see IdentityIQ Email Templates

This option is disabled if **Email Notification** field is disabled.

Email Recipients

Choose the users and/or groups to receive task completion notifications. You can use the drop-down arrow to display all identities, or type the first few letters of a name or group and select them from the list.

Microsoft Teams Notification Settings

Check **Enable Microsoft Teams Notification** to enable the Microsoft Teams Notification feature. This feature enables IdentityIQ to send notifications both to users' emails and to their Microsoft Teams application. When this option is checked, notifications are enabled on all Azure Active Directory applications on which Microsoft Teams are configured.

Work Items

Use this page to set default values for use with work item policy.

Certification Related Work Item Policy

Days before expiration

Specify the number of days after which a work item should expire.

Days before expiration to send first reminder

Specify the number of days, before a work item expires, that IdentityIQ should begin sending the owner of that work item reminder notices.

Days between expiration reminders

Specify the frequency with which reminder notices should be sent to the owners of certifications and work items.

Number of notices before escalation

Specify the number of reminder notices that should be sent before the first escalation notice is sent to the manager of the owner of the assess certification or work item.

Send notification email on work item assignment

Select this option to send an email notification when a work item is assigned.

Send notification email on work item assignment removal

Select this option to send an email notification when a work item assignment is removed.

Allow priority editing on work items

Select this option to give work item recipients the ability to adjust the priority level of work items.

Work Item Archives

Select one or more work item types to be archived. Press the **<Ctrl>** key to select multiple items.

Work Item Rules

You can use rules to customize work item processes and behavior. See **Using the Rule Editor** in IdentityIQ Configuration for more information on how to edit rules.

Inactive user work item escalation rule

Select the rule from the drop-down list for determining a new owner for work items from an inactive user.

Global work item forwarding rule

Use the drop-down list to select the rule used to determine general work item forwarding.

Self-certification work item forwarding rule

Use the drop-down list to select the rule used to determine work item forwarding in special cases. Allows for the specification of a fallback forwarding user in the case that configured automatic forwarding would cause self-certification.

This rule only applies if a user has configured a forwarding rule, the rule does not apply when a pre-delegation

rule causes self certification.

Identities

Use this page to set configuration values for identities.

Identity Risk

Use this section to categorize your organization's risk scores.

Number of Bands

Specify the number of colored bands, from 2 to 6, to display on all score card charts, graphs, and tables.

These bands are used to indicate various levels of risk associated with ranges of Identity risk scores. Specify a number that best meets the needs of your enterprise.

Label

Select the default labels or create your own text label associated with the colored risk bank.

Range

Input the numeric risk score range associated with each risk band. Risk scores are determined by multiple contributing factors defined on the Configure Risk Scoring page.

Refer to the system administration documentation for more information.

Indicator

The indication color associated with the risk level.

Identity Attributes

Number of Searchable Attributes

Specify the number of attributes that can be configured for use as searchable attributes on the Identity Attributes page. This can be any number between 1 and 20. The default is 10.

This number should match the number configured during the installation and deployment process. If no customization was performed during the installation and deployment process, the maximum number you can enter is 10.

Always Sync using workflow

Check this option if you want to always use the business process selected in the Business Processes section of this page for attribute synchronization. Leaving this option unchecked means that you can set the option to use the business process individually on each attribute in Identity Mappings. For more information see the **Provisioning** documentation.

Index History Granularity

IdentityIQ can save history about risk scorecards for identities and groups. Risk scorecards are calculated for identities and groups using the Identity Refresh task; scores are calculated based on the Identity Risk Model configured for your installation. Use this option to set the increments at which to store scorecard history for identities (using **Identity History**) and groups (using **Group History**). For example, if the Identity History is set to 'Week', scorecards are preserved on a weekly basis. This means that when a scorecard is updated, it overwrites any scorecard calculated within the previous week (7 days), and any scorecard that is older than 7 days is saved.

Identity Snapshots

Set the frequency with which identity snapshot should be taken. Identity snapshots are used to build the risk score card history that can be used to track trends and patterns for individual users, groups, departments, and your entire organization

Account Attributes

Specify the number of attributes that can be configured for use as searchable attributes. This can be any number between 1 and 20. The default is 5.

This number should match the number configured during the installation and deployment process. If no customization was performed during the installation and deployment process, the maximum number you can enter is 5.

Business Processes

You can configure IdentityIQ to run business processes when actions are taken on identities. See the **Business Processe**s documentation for more information.

Identity update

Select which business process is executed when an identity is edited in IdentityIQ. This can perform role assignment approvals and send provisioning requests.

Identity refresh

Select which business process is executed when an identity is refreshed in a background task. This might perform role assignment approvals and send provisioning requests.

Identity Correlation

Select which business process is executed when an manual correlation of accounts is done.

Attribute Sync

Using a business process with attribute synchronization lets you manage the synchronization of multiple attributes together, in a single request and approval process. To use this option, choose a business process to use for **Attribute Sync**. IdentityIQ provides a standard Attribute Sync business process that meets most use cases; you can edit this business process to tailor it to your needs, and you can also create and choose a custom business process if you prefer. See the **Business Processe**s documentation for more information.

Roles

Use this page to set default behavior for roles. Additional role configuration options are in Role Configuration.

Role Sunrise/Sunset Dates

Sunrise and sunset dates are used to make roles and entitlements temporary - they specify when a role (or an individual user's access to a role or an entitlement) becomes active, and when it becomes inactive. This feature offers an efficient, automated way to grant time-limited access to sensitive roles, roles that are seasonal or temporary, or access that for any reason is intended to have a limited duration, such as a short-term assignment to a different team or a special project.

IdentityIQ gives you two ways to use sunrise and sunset dates:

- On roles themselves, so that the role itself has a temporary duration.
- When a role or entitlement is granted to a specific user; in other words, the role itself may not have time limits, but a certain user's access to that role should have a limited duration.

Enable Sunrise/Sunset Dates on Role Assignment

Enable the ability to set activation and deactivation dates on roles when they are assigned.
Activation and deactivation dates can be used to grant temporary access to sensitive roles.

A workflow to manage assignment and removal of roles or entitlements for this option can be set in **Scheduled role/entitlement assignment** in the Business Processes section below. A standard workflow ("Scheduled Assignment") is provided out of the box, but you can implement a custom workflow if your business needs require one.

Enable Sunrise/Sunset Dates on Role Activation

Enable the ability to insert activation and deactivation events into roles from the role modeler. Activation events are used to automatically activate or deactivate roles using business processes.

A workflow to manage activation/deactivation of roles or entitlements for this option can be set in **Scheduled role activation** in the Business Processes section below. A standard workflow ("Scheduled Role Activation") is provided out of the box, but you can implement a custom workflow if your business needs require one.

Days before Sunset expiration to send notification

Send a notification to both the requestor and the requestee of the role or entitlement, when access is about to expire. This value determines when the notification is sent. To disable notifications, enter 0. The email template to use for notifications is configured on the **Mail Settings** tab in the **For notice of deprovisioning of sunsetted roles and entitlements** field.

Business Process Editor

In this section you can set business processes to run with the sunrise and sunset options set in the previous section, and to run when roles are created, modified or deleted.

Role create, update, and delete

Select which business process is executed when roles are created, modified, or deleted in the role modeler.

Schedule role activation

Select which business process is executed when a scheduled role assignment becomes due. This assigns the role and can perform provisioning. Use this business process with **Enable Sunrise/Sunset Dates on Role Activation.**

Schedule role/entitlement assignment

Select which business process is executed when a scheduled role assignment or de-assignment becomes due. This de-assigns the role and can perform provisioning. Use this option with **Enable Sunrise/Sunset Dates on Role Assignment.**

Additional Role Options

Show user interface option to allow multiple application accounts

> Note: If this option is not enabled, required roles are assigned to the same account as the top-level role.

Enables an option on the Role Management page that enables a role to specify its own target account, or create a new account, during a role request, even if it is required by another role and included in that roles required roles list.

Show user interface option to allow multiple assignments

> Note: This option is only available on assignable role types.

Enable an option on the Role Management page that enables a role to be assigned to the same identity multiple times.

Allow multiple assignment for all assignable roles

> Note: This setting supersedes the settings on the individual role definitions.

Make all assignable role types available for multiple assignment to the same identity.

Allow propagation of role changes

Enables a role change to propagate to all identities that have the role assigned.

Retain assigned entitlements when detected roles are removed

Do not remove assigned entitlements from an identity when a detected role with which they are associated is removed from that identity.

Retain assigned entitlements when assigned roles are removed

Do not remove assigned entitlements from an identity when an assigned role with which they are associated is removed from that identity.

Require comments for all access items

Require comments in Access Requests. The comment requirement applies to both the addition and removal of roles and entitlements in the Access Requests UI.

Passwords

Use this tab to define the password policy for IdentityIQ. All of the users must set up their passwords based on the policy created on this tab.

Use the Define Character Types dialog to define a custom set of character that are allowed in passwords. These can be used to match password requirements for specific application types. Click **Define Character Types** to open the

dialog and enter character sets by category, such as **Digits**, **Uppercase Characters**, **Lowercase** or **Non-English Characters**, **Special Characters**. All characters are allowed if these fields are empty.

Configuration

Enable one-way hashing of secret values

You must run the Encrypt Sensitive Data Task after selecting this option to convert any saved values from encrypted to hashed.

> Note: When this option is selected, all values are hashed instead of encrypted.

These values include passwords, password history, and authentication questions. When this option is enabled, specific password policy options are disabled.

For more information, see Data Encryption.

Number of hashing iterations

The number of iterations performed in the hashing algorithm.

Password Policy

Minimum number of characters

The minimum number of characters, letters, or digits, required for a valid password.

Maximum number of characters

The maximum number of characters, letters, or digits, allowed in a valid password.

Minimum number of letters

The minimum number of letters required for a valid password.

Minimum number of character type constraints to meet

The minimum number of character types required for a valid password. Applicable character types are upper case, lower case, digits, and special characters. If no value is set, all of the character type constraints must be met.

Minimum number of digits

The minimum number of digits required for a valid password.

Minimum uppercase letters

The minimum number of uppercase letters required for a valid password.

Minimum lowercase letters

The minimum number of lowercase letters required for a valid password.

Minimum special characters

The minimum number of special characters required.

Number of repeated characters allowed

The maximum number of consecutive repeated characters allowed in a valid password. For example, if this option is set to 2, “cloudd” and “cclooud” are valid, but “clouddd”, “cloooud” and “cccloud” are invalid. This value also sets the maximum number of occurrences of repeated characters allowed in a valid password. For example, if this option is set to 2, “happy123” is valid, however, “happy22” and “happpy123” are not.

In this example, when “cclooudd” is an invalid password, the following error message is displayed: Password should not contain more than 2 occurrence(s) of the repeated characters. When “clouddd” is an invalid password, the following error message is displayed: Password should not contain more than 2 consecutive repeated characters.

Setting this value to zero has the same effect as leaving this field blank, allowing any number of repeated and consecutive characters.

To prevent the use of any **consecutive** repeated characters, set this value to 1. Setting the value to 1 does not prevent using a character more than once, as long as the characters are not consecutive. For example, with a value of 1, "kitkat" is valid but "kitten" is not.

Password history length

The number of previous passwords stored by IdentityIQ.

This number includes the current password so if the length is two, the history is the current password and one other. If the length is set to zero there is no history.

Triviality check against old password

Ensure that the shorter of the old and new password is not a substring of the other.

Both passwords are changed to upper case prior to the check.

Minimum number of characters by position

The minimum number of unique characters by position for the new password. Can be used to ensure that not just the first or last character is changed.

Select **Case sensitive check** to ensure that more than just the case is changing in the new password.

Days until expiration for manually set passwords

The number of days until a password set manually expires.

If the days are zero passwords do not expire.

Days until expiration for generated passwords

The number of days until a password set by the identity create rule during aggregation expires.

If zero the days are zero passwords do not expire.

Minimum Hours between password changes

The minimum number of hours that must past before a user's password can be changed again.

Validate passwords against the password dictionary

Ensures that the password to be created is unique.

Validate passwords against the identity's list of attributes

Check the new password for validity against the attributes assigned to the identity.

Require users to enter their current password when setting a new password

Require users to enter there current password before creating a new password.

Miscellaneous

Use this tab to set a variety of IdentityIQ configuration options.

Other Object Expirations

Days before snapshot deletion

Specify the number of days to keep an identity snapshot in the system before it is deleted. Identity snapshots are used to build history.

Days before task result deletion

Specify the number of days to keep task results on the Task Results page before removing them from the system.

Days before certifications are archived

Specify the number of days after which to archive certifications.
Leave the settings at zero (0) to never archive certifications.

> Caution: Certification archives are not recommended. Certification reports should be used to preserve certification information.

Days before certification archive deletion

Specify the number of days to maintain the certification archive before deleting certifications records.
Leave the settings at zero (0) to never delete certifications archives.

> Caution: Certification archives are not recommended. Certification reports should be used to preserve certification information.

Minutes before object locks are released

Specify the number of minutes to elapse before releasing an object lock.
Leave the settings at zero (0) to have no time delay when objects are released.

Days before provisioning request logs expire

Specify the number of days to maintain provisioning request logs before deleting them.
Leave the settings at zero (0) to never delete provisioning request logs.

UI Preferences

Disable Role Modeler Tree View

Disable the tree view on the Role Manager page. Disabling the tree view might enhance performance on that page.

Maximum Roles Page Size

The maximum number of roles to display per page on the **Role Management** page.

Show unsupported browser message

Display a message when an unsupported browser is used.

Accessibility: Color Contrast

Enable color contrast throughout the entire IdentityIQ instance.

Syslog Settings

Enable syslog

Enable the syslog.

Level at which syslog events will be stored

Select the lowest level of event which is stored in the syslog. Choose from FATAL, ERROR, and WARN.

Days before syslog event deletion

Input the number of days an event in the syslog must remain before becoming eligible for purging.

Provisioning Transaction Log Settings

Enable Provisioning Transaction Log

Enable the Provisioning Transaction table and begin logging some or all of the provisioning actions within IdentityIQ.

Maximum Log Level

The level at which transactions are logged based on their completion status.
Success — all transaction are logged
Retry — transactions that did not succeed and are in either the retry or failed state
Failure — only log transaction that have failed and are setup for retry

Days before provisioning transaction event deletion

The number of days before a provisioning transaction is removed from the table.

File Preferences

Temporary Directory

Input the path to a default temporary director for use by IdentityIQ. This is the directory where IdentityIQ stores temporary files, such as log files, during processing.

Maximum Upload Size (MB)

Limit the size of the files uploaded using import objects, batch requests, and entitlement imports.

System Help Settings

Help Contact Email Address

Input an email address of a user responsible for supporting IdentityIQ in your enterprise. The email account is accessible from an **Email Help** button displayed at the bottom of some pages.

Localized Object Attributes

Enable applications to be configured with multi-language descriptions

Enable applications to be configured with multi-language descriptions. See Multi-language Description Files.

Enable roles to be configured with multi-language descriptions

Enable roles to be configured with multi-language descriptions. See Multi-language Description Files

Enable policies to be configured with multi-language descriptions

Enable policies to be configured with multi-language descriptions. See Multi-language Description Files

Enable entitlements to be configured with multi-language descriptions

Enable entitlements to be configured with multi-language descriptions. See Multi-language Description Files.

Multi-Languages Descriptions

> Note: You must add all supported languages to the `<locale-configure>` section of the `faces-config.xml` file before the application can properly recognize the languages.

Default Language

Select the language to use as a default from the list of supported languages.

Supported Languages

Enter the languages that your instance of IdentityIQ supports.

Business Processes

Entitlement Update

Select the business process to execute when a managed entitlement or group is created or edited.

Password Intercept

Select the business process to execute when a password change interception event is received.

Caches

Enable asynchronous policy and role cache refresh

Disable the immediate cache refresh with each Lifecycle Manger request.

When you enable this option, IdentityIQ does not check for changes to policy and role objects. When a Lifecycle Manager request is submitted, the cache is refreshed immediately. Using this option can speed the request process. However, the effects of a recent policy or role change might not display for a few minutes.

Reports

CSV Delimiter

The character used as the CSV delimiter when exporting report results. Comma is used by default.

Filter searches by

Determines how users can search for report names in the Reports UI. Choose `startsWith` to let users find the input string only at the beginning of the report name, or `contains` to find the search string anywhere in the report name.

Plugin Settings

Prohibit scripts from accessing plugin-loaded classes

> Note: All BeanShell executions are referred to as scripts.

Restrict the access to classes loaded by plugins. Without this restriction, all class are available in IdentityIQ.

Relax strict declaration enforcement

Enable IdentityIQ to work fully with plugins that were created without explicitly declaring classes for export.

By default, for a fresh installation of IdentityIQ this option is not selected. For an upgraded installation of IdentityIQ, this option is selected if plugins exist.

Attachment Settings

For detailed information about configuring and using file attachments in access requests, see **Configuring File Attachments for Access Requests** .

> Caution: IdentityIQ does not perform file content validation or verification on attachments. It is your responsibility to ensure that only files that do not violate security policies within your environment are included as attachments.

> Note: Attachments are only allowed on single-user requests.

> Note: Attachments are only available for manual access requests.

Enable Attachments

Enable the attachments feature. Allow users to add attachments to access requests.

Attachments Per Item

The maximum number of attachments allowed for a request.

Maximum file size (MB)

Maximum file size for any single attachment. The default maximum value you can enter here is 20 MB, but the maximum attachment size limit can be adjusted by a system administrator using the `attachmentsMaxFileSizeLimit` key in the system configuration object.

Supported file types

Comma separated list of file types. The dot prefix is not required.

Supported characters

Special characters, in addition to Unicode alphanumeric characters, that are allowed in the filename.

Configuration Rules

> Note: Only the rules selected in this list are run during an access request.

This list contains all of the attachment configuration rules available in your installation of IdentityIQ. Use the Ctrl or Shift keys to select multiple rules.

Edit Preferences Settings

Enable edit for forwarding preferences

Enable users to change their forwarding preferences from the Edit Preferences page. See the **IdentityIQ Getting Started** documentation for more information.

Enable change password

Enable users to change their IdentityIQ password from the Edit Preferences page. See the **IdentityIQ Getting Started** documentation for more information.

Manage User Access Require Comments Settings

Require comments for all access items

Require comments on all Access Requests. The comment requirement applies to both the addition and removal of roles and entitlements in the Access Requests UI.

Complete the following to require user comments on access requests:

1. Navigate to the **gear icon > Global Settings > IdentityIQ Configuration**.
2. Select the **Miscellaneous** tab.
3. Select **Require comments for all access items** in the Manage User Access Require Comments section.
4. Select **Save**.

Configuration Rules

You can use rule logic to define specific requirements and behavior for requiring comments.

Select the rule(s) to run during access requests from this list. You can use the Ctrl or Shift keys to select multiple rules. Note that if the option to require comments for **all** access items is checked in the field above, the rules do not run.

A sample **Example Comment Config Rule** rule is included in the `examplerules.xml` file.

Privileged Account Management

The SailPoint IdentityIQ Privileged Account Management Module (PAM) extends identity governance processes and controls to highly privileged access, enabling you to centrally manage access to privileged and non-privileged accounts.

This tab appears only if you have implemented the Privileged Account Management feature. Use this tab to configure the Privileged Account Management feature.

For more information, see the **Privileged Account Management** documentation.

Login Configuration

Use the Login Configuration page to set an application for authentication verification. For example, if all of the users in your organization are set up with roles and authorization in an LDAP server, use that server to verify users logging into IdentityIQ. Login Configuration has the following tabs:

- Login Settings
- User Reset
- Multi-Factor Authentication
- SSO Configuration

Authentication Method Processing Order

IdentityIQ attempts to authenticate users by all enabled methods before reporting login failure. The methods are executed in this order, skipping any disabled methods:

1. Single Sign On (Rule-based or SAML)
2. Pass-Through Authentication
3. Internal IdentityIQ Authentication

> Note: If configured, Multi-Factor Authentication follows the initial user authentication through any of these means.

Login Settings

Use the Login Settings tab to configure general settings for login criteria.

> Note: Any user discovered by an aggregation task appears in the identities lists and can be assigned work items. Before a user can access IdentityIQ and the work item, they must be validated by an authentication verification server.

Use Auto create user rules when adding users to the application. The first time a user logs into the application, and is verified by the pass-through server, the **Auto create user rules** creates an IdentityIQ user based on specifications defined in this rule. Those rules are applied each time the user accesses product.

The following table describes the login settings.

Pass through application

Specify an application to use as the authentication verification server for all users logging into IdentityIQ.

Auto create user rule

Specify an auto create user rule to use when creating IdentityIQ identities based on account attributes discovered during aggregations.

Click the "..." icon to launch the Rule Editor to make changes to your rules if needed. See Using the Rule Editor

Login error style

If you select Simple and are using the Lockout feature, users that are locked out do not receive a message providing that information.

Select a login error message style.
Simple — shows an error with no information about what is incorrect.
Detailed — provides information about the incorrect part of the login. For example, Invalid password for user admin.

Login after timeout returns to

Specify how navigation is handled after a session times out and you log back in to that session.

If checked, the Home page is displayed. If not, the session returns to the page that was viewed at the time of the timeout.

Enable Authorization Lockout

> Note: This option is only associated with the IdentityIQ password. It does not apply to the pass through authentication application. For example, if a user is locked out of directly logging into IdentityIQ, but they enter the correct information on the pass through authentication server, they are allowed into the application.

Enable a lockout period for users who enter the wrong authorization information.

Use the options that display to set the lockout parameters.

Number of Unsuccessful Login Attempts before lockout

Specify the number of login attempt failures allowed before the user is locked out of IdentityIQ.

Number of minutes a user will be locked out due to unsuccessful login

Specify the number of minutes a user is locked out of IdentityIQ before they can attempt to login again.

Enable Protected User Lockout

Select this if you want users marked as "Protected" (such as the default **spadmin** user) to be treated the same as other users in authorization lockout. Leave it unchecked if you do not want protected users to be subject to lockout.

By default, only the **spadmin** user is marked as protected; if there are other users you want to protect from lock-out, you can make them protected by adding a `protected="true"` flag to the user's Identity object in the Debug Pages.

User Reset

On the User Reset tab, configure your system to let users reset forgotten passwords or unlock accounts. Navigate to **gear > Global Settings > Login Configuration** and use the following options:

- **Enable Forgot Password**—displays a Forgot Password link on the login page so users who have forgotten their password can reset it.
- **Enable Account Unlock**—displays an Account Unlock link on the login page so users who have been locked out can unlock their account.

Selecting either or both of these options brings up two additional options:

- **Enable Security Questions**—when enabled, security questions are used to confirm a user's identity if they have forgotten their password or become locked out.
- **Enable SMS Verification**—when enabled, a user is provided the option to have a reset code sent via SMS if they have forgotten their password or been locked out.

See **Password Recovery—Account Unlock.**

Security Question Configuration

> Note: Security questions and settings are associated with the password set on the pass through application. These are not associated with a direct logon to IdentityIQ.

Security questions display when you select the Forgot Password link on the login page during the authentication process. The questions list can contain tags from the properties file configured when your IdentityIQ instance was deployed, or when text is entered directly on this tab, or a combination of both. Mapping tags from a properties file is generally used for internationalization purposes.

Configure security questions as follows:

1. In the Questions section, select your desired questions using the **+** option to add new questions and the **-** option to remove options from the list.
2. In the **Settings** section, adjust the default parameters as needed.
    - **Number of questions asked to authenticate an identity**—specifies the number of questions that must be answered correctly in order to reset the password.
    - **Number of questions a user must answer for authentication**—specifies the number of questions for which the user must provide answers in advance so they can be authenticated using these questions. Questions without known answers cannot be used for authentication because there is no correct answer to be matched.
    - **Prompt users for answers to unanswered security questions upon successful login**—causes IdentityIQ to check during login whether the user has the required number of authentication answers provided already and, if not, prompt the user for those answers. The required number of questions is defined on the Edit Preferences page.
    - **Maximum number of unsuccessful authentication attempts before IdentityIQ lockout**—specifies the number of failed authentication attempts before the user is locked out of IdentityIQ.
    - **Number of minutes a user will remain locked out due to unsuccessful authentication**—set how long a user is locked out after the specified number of unsuccessful login attempts before they can try again to sign into IdentityIQ.
3. Select **Save**.

When a user clicks the **Forgot Password** link and then selects and answers the authentication questions, by default the user's answers are shown in plain text as they are typed in the user interface. If you want to obscure the user's answers with asterisks as they are typed, use the Debug page to add this entry key to IdentityIQ's **SystemConfiguration** object.

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

Use the **Settings** section to configure behaviors for password attempts.

SMS Reset

Be sure to select the **Enable SMS Verification** checkbox. Additionally, before you set up SMS Reset, you need the following items from twilio.com:

- An active Twilio account
- Twilio ID
- Twilio credentials (authentication token)
- "From" phone number configured on account

SMS Verification Configuration

Set up SMS verification for your system by completing the form as follows:

- **Twilio Account ID**—enter the account ID you receive from Twilio when you set up your company Twilio account.
- **Twilio Authentication Token**—enter the authentication token you receive from Twilio when you set up your company Twilio account.
- **From Phone Number**—specify the phone number to be displayed in the From field on the SMS messages. This phone number must be configured as the From number on your Twilio account.
- **Phone Number Attribute on Identity**—from a dropdown list, select the identity attribute that represents the mobile phone number. To define a new identity attribute, see Account Mappings.

  > For a user to reset their password using the SMS Reset feature, the field associated with their mobile phone number must contain a complete number including the area code. Using E.164 number formatting for all phone numbers in the To and From fields is strongly encouraged. For more information, see SSO Configuration.

- **Verification Token Timeout (minutes)**—you may adjust the default as needed to specify how many minutes the user's password reset token is valid before it expires.
- **Throttle requests at a rate of 1 per N minute(s)**—specify the rate at which SMS requests can be made in a certain amount of time. For example, if you enter the number 5, your limit is 1 request every 5 minutes.
- **Maximum Failed Attempts**—after reaching the maximum failed attempts, a user cannot verify a reset token until that token expires and a new token is requested.

Multi-Factor Authentication

Multi Factor Authentication (MFA) adds an additional layer of security by requiring users to use multiple methods to authenticate their identity before they can log in to IdentityIQ. IdentityIQ supports the following MFA options:

- RSA Workflow
- Duo Workflow

To access MFA Login Configuration settings in IdentityIQ, click the **gear** icon in the menu bar and select **Global Settings > Login Configuration > Multi Factor Authentication** tab

This section includes the following topics:

MFA Prerequisites

> Note: To use Duo, you must follow the Duo Auth API instruction to enable the AuthAPI in the Duo Admin Panel. To locate the Duo API documentation, go to https://duo.com, search for Auth API documentation and then follow the steps for adding Duo two-factor authentication.

MFA User Process Flow Overview

The basic process flow for using MFA to log in to IdentityIQ includes the following steps:

1. The user enters a valid username and password at the IdentityIQ login screen.
2. The IdentityIQ MFA workflow begins and displays the MFA provider's login page or process for login. If a user is assigned to multiple providers, the user must select a provider from the provider list before proceeding to the provider’s login page.
3. The user completes the authentication process for their MFA provider.
4. The user is logged in to IdentityIQ and the Home page displays.

MFA Configuration Process Flow Overview

The basic process flow for configuring MFA for IdentityIQ includes the following steps:

1. Use a pre-defined MFA workflow or choose to create a custom workflow.
2. Install the workflow.

- Import the workflow.
- Configure the workflow as a business process.
- Enable the populations to use with MFA.

3. Save your MFA configuration.

For more information, see How to Install a Multi-Factor Authentication Workflow - DUO Example

Multi-Factor Authentication Workflows

Each MFA provider has its own flow and process. MFA Providers contain the populations and providers are configured from an existing list of DynamicScopes/Populations. Workflows of type **MultiFactorAuthentication** can enable Multi-Factor Authentication for a particular provider.

Pre-defined workflows are provided. These workflows use existing pre-configured applications to perform Multi-Factor Authentication

You can choose to create a custom workflow. See Custom Multi-Factor Authentication Workflows.

How to Install a Multi-Factor Authentication Workflow - DUO Example

The following workflows are provided, however they are not installed by default. These workflows use existing pre-configured applications to perform Multi-Factor Authentication. The provided workflows are located:

- `WEB-INF/config/workflow_MultiFactor_DUO.xml`
- `WEB-INF/config/workflow_MultiFactor_RSA.xml`

> Note: The following instruction are specific to using DUO as your MFA application. You can use these instructions to install RSA by changing the DUO-specific items to RSA. As noted in the instructions, you do not need to add API authentication credentials for RSA.

1. Review any prerequisites. See MFA Prerequisites.
2. To import the workflow, you can use the **Import From File** function in the **Global Settings** menu or use the IdentityIQ console. To use the IdentityIQ console, open the console and use the following command:

```
import workflow_MultiFactor_DUO.xml
```

3. Configure the workflow as a business process:

a. Login to IdentityIQ using an administrator account and navigate to **Setup > Business Processes**.

b. Click the workflow named **MFA DUO**

c. Click **Process Variables**

d. Select a pre-configured application, of type **Duo**, for the field **Duo Application Name**. The workflow reads new properties added to the application used to authenticate with the Duo cloud Authentication service.

e. Click **Save**.

4. Use the following steps to add Duo authentication API credentials:

> Note: These steps are not necessary for the MFA RSA workflow because RSA uses existing API credential information already configured in the RSA Application.

a. Navigate to **Applications > Application Definition**.

b. Select the Application of type Duo you configured in the previous step.

c. Click **Configuration**.

d. Complete the **Admin API Credentials** section using the credentials you obtained from the Duo Admin Panel.

The first time you set up a Duo application, you must enter the Admin API information received from Duo. If you are modifying a previously configured Duo application, the Admin API credentials should already be configured.

e. Click **Save**.

5. Next, enable a population of users that must use Multi-Factor Authentication to authenticate using the following steps:

a. Click the **gear** icon.

b. Navigate to **Global Settings >Quicklink Populations**.

c. Verify you have an existing population of users you want to authenticate using Multi-Factor Authentication.

6. The population you enabled can allow a user in the population to request access for other users. If you do not want a user have that capability, you can create a new QuickLink population. You must select **No one** in the

section **who can members request for?** when you create the new QuickLink population. This configuration separates Request Access type Quicklink Populations from Multi-Factor Authentication Populations.

7. Next, associate the population to the Multi-Factor Authentication workflow using the following steps:

   a. Click the **gear** icon and navigate to **Global Settings > Login Configuration > MFA tab**.

   b. Check the box for the MFA Workflow you want to enable.

   c. Add any populations to the multi-select list you want to enable for this MFA workflow.

   d. Click **Save**.

Custom Multi-Factor Authentication Workflows

Implementers can create custom Multi-Factor authentication workflows. Any workflow of type **MultiFactorAuthentication** displays in the MFA Configuration page. If you choose to create a custom workflow, review the following information:

- Adding an error message to the workflow case using:

  ```
  wfcase.addMessage(new Message(Type.Error, "An error has occurred that prevents Multi-Factor Authentication"))
  ```

  This adds an error to the workflow case and signals to the Multi-Factor framework the user should not be logged in.

- A workflow that was not marked **complete** will signal Multi-Factor authentication has failed. During normal workflow execution, if a workflow has not produced an error, the workflow is automatically marked complete.

SSO Configuration

IdentityIQ supports two different options for single sign-on (SSO) configuration, rule-based and SAML. SSO streamlines the login process for users even further than pass-through authentication by enabling the user to bypass signing in to each system, once they have completed the initial sign-on to the authenticating application.

SSO Configuration has the following options:

- Enable Rule-Based Single Sign-On (SSO) - uses rules for Single Sign-On and Validation
- Enable SAML Based Single Sign-On (SSO) - uses Security Assertion Markup Language (SAML) as an authentication protocol

> Note: To access the IdentityIQ Login page directly when Single Sign-On is configured, use a supported browser and enter `http://<iiq server>/spt/login.jsf?prompt=true`.

IdentityIQ supports specifying both types of SSO in the same installation's login configuration. The order in which they are consulted during user authentication will be determined as follows:

- If an ssoAuthenticators attribute is specified in the SystemConfiguration object, it will specify the configured SSO options in a CSV list, and the options will be checked in the order they are specified
- If that attribute is not present, SAML SSO will be used first and then rule-based SSO

Rule Based SSO

In rule-based Single Sign-On (SSO) configurations, when the user accesses the IdentityIQ web application, the authentication source recognizes it as a secure resource, requires the user to authenticate to it (if the user has not already done so), and passes a “token”, containing contextual information, in the HTTP header to IdentityIQ. The SSOAuthenticationRule validates that information and maps the user to the appropriate IdentityIQ Identity.

Single Sign-On Rule

Specify the rule to use when authorizing users through and single sign-on system, such as SiteMinder.

Click the “...” icon to launch the Rule Editor to make changes to your rules if needed.

See Using the Rule Editor.

Single Sign-On Validation Rule

Specify the rule to use to verify a single sign-on session to make sure a stale session is not actually a different user.

The rule type (SSOValidation) runs on every request. If the request is valid, it returns null. If it returns a string, that string is an indication of an error and is used in the error that is displayed in the logs. If the session is invalidated, the request is redirect to logoutUrl configured in web.xml.

This is designed to be used with the Single Sign-On Rule.

SAML Based SSO: Identity Provider Settings

In SAML-based SSO, the authorization request can be initiated with the Service Provider (the application itself - IdentityIQ) or with the SSO authentication application (known as the Identity Provider). In either case, the Identity Provider handles authentication of the user and provides a signed XML <Response>, or Assertion. This response contains information that IdentityIQ can match to an identity to determine the user's proper authorization to IdentityIQ

functionality.

Entity ID / Issuer

Unique identifier defining the organization (IdentityIQ) to the Identity Provider. This ID is usually the URL or domain name for the organization. For example, `https://identityiq-server.your-domain.-com:your-port/identityiq`

If you use the standard https port for communication, the `:your-port` is not necessary.

SSO Login URL

The URL of the Identity Provider SSO service provider (the SAML SSO service URL). You can obtain this address from your Identity Provider. If the Identity Provider Issuer is not set, the configuration defaults to Identity Provider Single Sign-On service URL.

Public X.509 Certificate

An encrypted string containing the public key of the X509 certificate of the Identity Provider.

This entry should include the header -----BEGIN CERTIFICATE----- and footer -----END CERTIFICATE-----

Identity Provider Issuer URL

The Unique Identifier that defines the Identity Provider to IdentityIQ. This identifier is often in the form of a URL, but does not have to be.

The Identity Provider Issuer URL field is only necessary if the SAML response does not contain an Issuer value that does not match the leading characters of the Identities Provider SSO Server URL field. For example,

Identity Provider SSO Server URL = `https://idp.your-domain.com/SSOApp/SSOLogin`

SAML Response Issuer field = `https://idp.your-domain.com/SSOApp`

SAML Based SSO: Service Provider Settings

Entity ID / Issuer

Unique identifier that represents the Service Provider.

SAML URL (Assertion Consumer Service)

Specify the IdentityIQ URL where the SAML is to be accepted. For example:

`https://identityiqserver.your-domain.com:your-port/identityiq/home.jsf`

SAML Binding

Select **HTTP POST** or **HTTP Redirect** for the communications scheme.

SAML Name ID Format

Select the name format from the list. The Identity Provider provides the formats listed in drop-down box.

SAML Correlation Rule

Select a rule to use to match a SailPoint identity with a SAML assertion from the Identity Provider results. IdentityIQ includes a sample SAML correlation rule, called IdentityNowSAML, that you can use as a model for developing a correlation rule that meets your business needs.

Identity Mappings

The Identity Mappings feature is where you configure the identities that are managed by IdentityIQ. This is where you specify the applications and application attributes from which the identity data is derived.

Use the Identity Attributes page to view and edit the identity attributes information for your configuration. These attributes are used throughout the product for certifications, searches, and to collect and correlate identity data from applications.

IdentityIQ also supports the use of Robotic Process Automation (RPA) or bot identities. A bot is an application that can perform automated tasks, especially simple, repetitive tasks such as requesting access and managing identities. See Robotic Process Automation (Bot) Identities for more information.

The Identity Attributes page lists any attributes that have been configured in your system, and shows the primary source mapping and any advanced options that have been configured for each attribute. For details on how to edit and further configure identity attributes, see Edit Identity Attributes Page.

Attribute

The Attribute column shows the display name of the identity attribute, which is derived from the attribute and its associated application in the Primary Source Mapping column.
The following attributes are required by IdentityIQ to perform correctly:

- ID
- manager
- email

- firstname
- lastname

Manager and **role** are system attributes that are configured for grouping. However, you can use any identity attribute or grouping by defining it as a group factory in the Advanced Options.

Primary Source Mapping

The Primary Source Mapping column lists the first of the the application/attribute pairs from which employee attributes are derived. If the required data is unavailable on this primary source, the collection process continues down the list of configured sources until the information is found.

Set up the list of sources on the Edit Identity Attributes page.

Setting the same application and attribute as the source and target for an identity attribute creates circular references.

Identity attributes with circular references between sources and targets can cause values to be continually changed on every attribute synchronization. This can be problematic when a transformation rule modifies a value without first checking the identity attribute value has already been transformed.

Advanced Options

The **Advanced Options** column shows some of the main options that are enabled for this attribute. Additional Advanced Options can be configured in the Edit Identity Attributes Page.

Editable — the attribute can be edited.

Group Factory — the attribute can be used to create groups that are used for analytical purpose throughout IdentityIQ.

Searchable — the attributes that are available for filtering in identity searches.

To add a new identity attributed, click **Add New Attribute**. For details on how to set up new identity attributes, see How to Add or Edit Identity Attributes and the Edit Identity Attributes Page.

To delete identity attributes, right-click the attribute and select **Delete**.

> Deleting an identity attribute also deletes any group factories that reference it. Review the group factory information in the Confirm Deletion of Attribute dialog before clicking Yes.

For additional information:

- Edit Identity Attributes Page
- How to Add or Edit Identity Attributes

Edit Identity Attributes Page

Use the Edit Identity Attribute page to create and edit identity attributes including the display name, advanced options and source mapping.

The maximum number of searchable attributes you can create is defined during the application installation and configuration process and controlled from the System Setup pages. The default number is ten (10). See Create Icons to Represent Specialized Account Attributes.

To support the governance of bots, IdentityIQ has three standard attributes in the identity object that enable you to do things like run a focused certification on just bots.

The attributes are:

- **Type**: an attribute to define the type of identity. The standard values for this attribute are:
    - Employee
    - Contractor
    - External / Partner
    - RPA / Bots
    - Service Account

However, you can define your own types in addition to these 5, via editing XML in debug

- **Version:** an attribute to indicate what version of software the bot is using. This attribute is intended to be used only for bots.
- **Administrator:** the owner, certifier, of the bot. This is used instead of manager for bots throughout IdentityIQ.

The Edit Identity Attribute page contains the following information:

Field	Description
Identity Attribute:	
Attribute Name	The name of the attribute as it is used throughout IdentityIQ. For example, this the name used to identify this attribute in rules.
Display Name	The IdentityIQ user assigned name.
Advanced Options:	
Attribute Type	Select from the following attribute types:

Field	Description
	String — creates a text-editable field. **Identity** — creates a drop-down list from which you choose an existing identity.
Edit Mode	Enable editing of this attribute from the Identity pages. **Read Only** — this attribute cannot be edited from the Identities pages. **Permanent** — changes made on the identities pages are not overwritten by refresh tasks. **Temporary** — changes made on the edit identities pages are overwritten when an aggregation task brings over a new (changed) value for the attribute.
Searchable	Enable this attribute for use in searches and filtering through IdentityIQ.
Multi-Valued	Specify attributes for which multiple values might be returned during aggregation. Attributes flagged as multi-valued are stored as a list. Even objects that have a single value for a multi-value attribute are stored as a single-item list. Multi-valued attributes are used for queries throughout the product.
Group Factory	Enable this attribute for use in creating groups used for analytical purpose throughout IdentityIQ.
Value Change Rule	Specify a rule to run every time a change is detected on this attribute during the aggregation process. For example, a rule can be written to send change notifications, request change approval or launch a certification. Click the "..." icon to launch the Rule Editor to make changes to your rules if needed. See Using the Rule Editor
Value Change Workflow	Specify a business process to run every time a change is detected on this attribute during the aggregation process. For example, a business process can be written to send change notifications, request change approval or launch a certification.
Sync with Workflow	To use a business process handling for attribute synchronization.

Field	Description
If you set the source and target mapping to the same application/attribute pair, it creates circular references and where the values continuously change with every attribute synchronization.	
Source Mappings: The list of application/attribute pairs from which employee attributes are derived. If the required data is unavailable on the primary source, the collection process continues down the list of configured sources until the information is found.	
Target Mappings (Only available for Identity attribute types): When creating or editing an Identity attribute, use the Target Attribute options to define targets that the basis for attribute synchronization. Click **Add Target** to display the Add a target to the AttributeName attribute dialog, and complete all of the information.	

How to Add or Edit Identity Attributes

> Note: When mapping to a named column, specify the name to match the `.hbm.xml` property name, not the database column name. With camel case, the database column name is translated to lower case with underscore separators. For example, costCenter in the Hibernate mapping file becomes cost_center in the database.

Begin by clicking **Add New Attribute** or clicking an existing attribute to display the Edit Identity Attribute page.

Enter or change the **Attribute Name** and an intuitive **Display Name**.

> Note: You cannot define an extended attribute with the same name as any existing identity attribute.

> Caution: Changing an attribute name might cause attributes that were previously aggregated to no longer be recognized.

Advanced Options

Advanced options are optional. The Advanced Options you can set are described on the Edit Identity Attributes Page.

Source Mappings

Click **Add Source** to display the Add a source dialog, then specify a source for the new attribute. You can use more than one source for the attribute.

Map directly to an attribute on an application.

For Application Attributes you have the option to also make this source a target for attribute synchronization. If there are multiple source applications on which a user might have accounts, you would likely want to push the most authoritative value to the rest of the accounts.

1. Select **Application Attribute**.
2. Select an application from the **Application** drop-down list.
3. Select an attribute from the **Attribute** drop-down list.
4. Click **Add**.

Map to an application rule.

This rule only applies to the application specified.

1. Select **Application Rule**.
2. Select an application from the **Application** drop-down list.
3. Select a rule from the **Rule** drop-down list.
4. Click **Add**.

Map to a global rule.

This rule applies to all applications that contain this attribute.

1. Select **Global rule (all apps)**.
2. Select a rule from the **Rule** drop-down list.
3. Click **Add**.

When you have added your sources for the attribute, use the arrows to the right of the sources list to arrange the search order for the attribute sources. When aggregation tasks are run, they search the source at the top of the list, or the primary source, first and then work down the list.

Target Mappings

For Identity attribute types only, add targets for attribute synchronization

1. Select **Add Target** to display the Add a target to the attribute dialog.
2. Select the application to receive the value.
3. Select the attribute to receive the value.
4. **Optional:** Select a transformation rule to transform the value before it is set on the destination.
5. **Optional:** Select Provision All Accounts to provision all of the identities accounts on the targeted application. If you disable this option you are asked to select the accounts to provision manually.

Click **Save** to create the new attribute and return to the Identity Attribute page.

Account Mappings

> Note: Extended attribute names must be unique. Extended attributes cannot share a name with any other attribute in any other application schema.

Use the Account Mapping page to setup and map specialized accounts. Specialized accounts can be any accounts that justify special handling throughout your enterprise. For example privileged accounts such as Root, Administrator, or Super User, and service accounts that access a specific service or function on an application. Any attribute extended on this page is available for searching on the Identity Search page.

You can assign icons to extended attributes to highlight these accounts in certifications and the detailed identity pages. See Create Icons to Represent Specialized Account Attributes.

Specialized account attributes can be modeled to handle any concept using simple one-to-one mapping and rules. This section describes two of the most common scenarios.

Use the Account Attributes page to view the extended account attribute information for your configuration. Use this page to set up specialized account attributes such as Privileged and Service, and any other extended attributes for use in certifications and searches.

The Account Attributes page contains the following information:

Attribute

The display name of an account attribute derived from the attribute and its associated application in the Primary Source Mapping column.

Primary Source Mapping

The first of the list of attribute/application pairs or rules from which account attributes are derived. If the required data is unavailable on this primary source, the collection process continues down the list of configured sources

until the information is found.

Set up the list of sources on the Edit Account Attribute page.

To work with the attributes and sources, see Edit Account Attributes Page.

To delete account attributes, right-click the attribute and select **Delete**.

To edit account attributes, right-click the attribute and select **Edit**.

Additional Information:

- Edit Account Attributes Page
- How to Add or Edit Account Attributes

Edit Account Attributes Page

Use the Edit Account Attribute page to create and edit account attributes including the display name, attribute type and source mapping. You can also use this page to create specialized account attributes. See Create Icons to Represent Specialized Account Attributes.

The maximum number of searchable attributes that can be created is defined during the installation and configuration process. By default you can set five searchable account attributes. See System Setup.

The Edit Account Attribute page contains the following information:

Account Attribute:

Attribute Name

The name of the attribute as it appears in the application.

Changing an attribute name might cause attributes that were previously aggregated to no longer be recognized.

Display Name

The IdentityIQ user assigned name for use throughout IdentityIQ.

Advanced Options:

Edit Mode

Enable editing of this attribute.

Read Only — this attribute cannot be edited.

Permanent — changes made to this attribute manually are not overwritten by refresh tasks.

Temporary — changes made to this attribute manually are overwritten by the first refresh task that detects a value different than the original value.

For example, if the original value is A and it is manually changed to B, the value is not overwritten by a refresh task until the newly aggregated value is not A. When an aggregation detects a value that is not A, it refreshes the manually-changed value and the value is updated with each subsequent refresh.

Attribute Type

The attribute type to be linked, for example string, boolean or date.

Searchable

Account attributes are existing link values and are always searchable. This field is displayed as selected and read only so that identity and account attribute configuration pages are consistent in appearance.

Multi-Valued

Specify attributes for which multiple values might be returned during aggregation.
Attributes flagged as multi-valued are stored as a list. Even objects that have a single value for a multi-value attribute are stored as a single-item list. Multi-valued attributes are used for queries throughout the product.

Source Mappings:

The list of attribute/application pairs or rules from which account attributes are derived. If the required data is unavailable on this primary source, the collection process continues down the list of configured sources until the information is found. This feature is unlikely to be used for Account Attribute mapping.

See How to Add or Edit Account Attributes

How to Add or Edit Account Attributes

> Note: When mapping to a named column, specify the name to match the `.hbm.xml` property name, not the database column name. With camel case the database column name is translated to lower case with underscore separators. For example, costCenter in the Hibernate mapping file becomes cost_center in the database.

1. Click **Add New Attribute** or click an existing attribute to display the Edit Account Attribute page.
2. Enter or change the attribute name and an intuitive display name.

> Note: You cannot define an extended attribute with the same name as any application attribute that is provided by a connector.

3. Edit the Advance Options as required.
4. Click **Add Source** to display the Add a source dialog and specify a source for the new attribute.
   a. Map directly to an attribute on an application .
      i. Select **Application Attribute**.
      ii. Select an application from the **Application** drop-down list.
      iii. Select an attribute from the **Attribute** drop-down list.
   b. Map to an application rule. This rule only applies to the application specified.
      i. Select **Application Rule**.
      ii. Select an application from the **Application** drop-down list.
      iii. Select a rule from the **Rule** drop-down list.
   c. Map to a global rule. This rule applies to all applications that contain this attribute.
      i. Select **Global rule (all applications)**.
      ii. Select a rule from the **Rule** drop-down list.
5. Click **Add** to add the new source.
6. Use the arrows to the right of the sources list to rearrange the search order for the attribute sources. When aggregation tasks are run they search the source at the top of the list, or the primary source, first and then work down the list.
7. Click **Save** to create the new attribute and return to the Account Attribute page.

Account Attributes

Create a Service Account Using Simple Mapping

In this example, if IdentityIQ finds an attribute named Service that has a value of true on the application DB Application it is marked as a service account. For this case the database connector has already provided an attribute value to

reflect the service state, so a simple mapping is all that is required.

> Note: After configuring these attributes you must re-aggregate or refresh the identity cubes to set the values.

To configure the mapping:

1. Access the Account Attributes page.
   Select the System Setup tab and select **Account Mappings** from the table.
2. Click **Add New Attribute** to display the Edit Account Attribute page.
3. Specify the following values:
   - **Attribute Name** — service
   - **Display Name** — Service Account
   - **Edit Mode** — Read Only
   - **Attribute Type** — boolean
   - **Searchable** — Read Only
   - **Multi-Valued** — this is not a multi-valued attribute so do not select this field.
4. Click **Add Source Mapping** to display the Add a source to the attribute dialog.
5. Map the attribute:
   a. Select **Application Attribute**.
   b. Select **DB Application** from the Application drop-down list.
   c. Select **Service** from the Attribute drop-down list.
6. Click **Add**.

Create a Privileged Account Using a Rule

In this example, if IdentityIQ finds an account that is a member of the group **Domain Admins** on any AD application, that account should be marked as a privileged account.

1. Write the rule to define the logic.
   This rule checks each account on every AD application and looks for the Domain Admins group. If the Domain Admins group is found, the rule returns true, and the account is considered privileged.

Example rule:

```
<Rule language="beanshell" name="Example privileged promotion rule"
        type="LinkAttribute">
    <Source>
        <![CDATA[
Boolean privileged = null;
            If ( link.getApplication().getName().contains(“AD”) ) {
                privileged = new Boolean(false);
                List groups = (List)link.getAttribute("memberOf");
                if ( groups != null ) {
                    for ( String group : groups ) {
                        if ( ( group != null ) &&
    ( group.startsWith("cn=Domain Admins") ) ) {
    privileged = new Boolean(true);
}
    }
    }
    )
    return privileged;
    ]]>
    </Source>
</Rule>
```

1. Access the Account Attributes page.
   Go to the Global Settings and select **Account Mappings**.
2. Click **Add New Attribute** to display the Edit Account Attribute page.
3. Specify the following values:
   - **Attribute Name** — service
   - **Display Name** — Service Account
   - **Edit Mode** — Read Only
   - **Attribute Type** — boolean

- **Searchable** — Read Only
- **Multi-Valued** — this is not a multi-valued attribute so do not select this field.

4. Click **Add Source** to display the Add a source to the attribute dialog.
5. Map the attribute:
   Select **Global Rule (all applications)**.
   Select **Example privileged promotion rule** from the Application drop-down list.
6. Click **Save**.

Create Icons to Represent Specialized Account Attributes

Assign icons to extended attributes to highlight these accounts in certifications and the detailed identity pages. To assign icons you must modify the UIConfig file and add AccountIconConfig entries for any value that should be recognized.

The following example references the attributes defined in this section.

```
<ImportAction name='merge'>
    <UIConfig name='UIConfig'>
        <Attributes>
            <Map>
                <entry key='accountIconConfig'>
                    <value>
                        <List>
                            <!–This indicates that when we are displaying accounts and we
see
                                    the value “true” for the extended account attribute
named
                                privileged we should display the icon listed in the
“source”
                                attribute. The title will be used in hover-over help.
                                ->
                            <AccountIconConfig attribute="privileged"
                                        value="true"
                                        source="/images/icons/privilege_16.png"
                                        title="This is a privileged account"/>
                            <!–This indicates that when we are displaying accounts and we
see
                                the value “true” for the extended account attribute
named
                                service we should display the icon listed in the
“source”
                                attribute. The title will be used in hover-over help.
                                ->
                            <AccountIconConfig attribute="service"
```

```
                                        value="true"
                                        source="/images/icons/service.png"
                                        title="This is a service account"/>
                        </List>
                    </value>
                </entry>
            </Map>
        </Attributes>
    </UIConfig>
</ImportAction>
```

Use the IdentityIQ console to import the modifications.

Application Attributes

Use the Edit Application Configuration page to define extended application attributes not provided by the application connectors during aggregation. These extended attributes are displayed on the Attributes tab of the Application Configuration page below the connection attributes provided by the connector. Because the additional attributes are stored with those provided by the connector, if you define an extended attribute with a name that matches any connector attribute, the values of the extended attribute overwrite the values of the connector attribute.

You can use these extended attributes inside rules and custom reports and queries.

The Edit Application Configuration page contains the following information:

Name

The display name of the application attribute assigned when it was added.

Category

The category defined when the attribute was created.
If no category was defined this column is blank.

Description

A short description of the extended application attribute.

Click **New Attribute** to add additional attributes to the applications.

To edit or delete an existing attribute from the list, right-click the attribute and select the corresponding option from the menu. If you are deleting an attribute you must confirm the deletion in the pop-up dialog.

Additional Information

- Edit Extended Attributes
- How to Add or Edit Extended Attributes

Edit Extended Attributes

Use the Edit Extended Attribute page to create and edit additional application attributes including the display name, attribute type and description.

The fields displayed on the Edit Extended Attribute page are dependent on the attribute type selected.

> **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a standard prefix or naming convention that ensures that your extended attribute names are unique.

The Edit Extended Attribute page contains the following information:

Attribute Name

The name of the attribute as it appears in the application.

> **Caution:** Changing an attribute name might cause attributes that were previously aggregated to no longer be recognized.

Display Name

The IdentityIQ user assigned name for use throughout IdentityIQ.

Type

The attribute type to be linked, for example string, boolean, date, rule, or identity.

Description

A brief description of the application attribute.

Category Name

An optional category used to separate the attributes into categories on the Application Configuration page. Enter a category name or select an existing one from the drop-down list.

Searchable

Enable this application attribute for use in searches throughout the product.

Editable

Enable editing of this attribute from other pages in the product.

Required

For String type attributes only.
Required attributes must have a value before you can save an application.

Allowed Values

For String type attributes only.
Enter the values that are allowed for this attribute. The values entered in this list are used to populate the drop-down value list on the Application Configuration page.

Default Value

Enter a default value for the attribute or select a value from the drop-down list, depending on the attribute type you are working with.

How to Add or Edit Extended Attributes

> **Note**: When mapping to a named column, specify the name to match the `.hbm.xml` property name, not the database column name. With camel case the database column name is translated to lower case with underscore separators. For example, costCenter in the Hibernate mapping file becomes cost_center in the database.

1. Click **New Attribute** or click an existing attribute to display the Edit Extended Attribute page.
2. Enter or change the attribute name and an intuitive display name.

> **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a

standard prefix or naming convention that ensures that your extended attribute names are unique.

Caution: If you define an extended attribute with the same name as an application attribute, the value of the extended attribute overwrites the value of the connector attribute.

3. Select the attribute type from the drop-down list, String, Integer, Boolean, Date, Rule, or Identity.
4. **Optional**: add more information for the extended attribute, as needed.
   - Enter a description of the additional attribute.
   - Select a category for the attribute.
   - Activate the Searchable option to enable this attribute for searching throughout the product.
   - Activate the Editable option to enable this attribute for editing from other pages within the product.
   - Mark the attribute as required. For string type attributes only.
   - Enter allowed values for the attribute. For string type attributes only.
   - Specify a default value.
5. Click **Save** to save your changes and return to the Edit Application Configuration page.

Entitlement Catalog Attributes

Use the Edit Entitlement Catalog Configuration page to define custom extended entitlement attributes. The extended attributes are displayed with the rest of the entitlement information throughout the product. An example of a extended entitlement attribute might be Time Zone.

The Edit Entitlement Catalog Configuration page contains the following information:

Name

The display name of the extended entitlement attribute assigned when it was added.

Category Name

The category defined when the attribute was created.
If no category was defined this column is blank.

Description

A short description of the extended entitlement attribute.

Click **New Attribute** to add additional extended entitlement attributes.

To edit or delete an existing attribute or type from the list, right-click the item and select the corresponding option from the menu. If you are deleting, you must confirm the deletion in the pop-up dialog.

Additional Information

- Extended Attributes
- How to Add or Edit Extended Entitlement Attributes

Extended Attributes

Use the Edit Extended Attribute page to create and edit additional role attributes including the display name, attribute type and description.

The Edit Extended Attribute page contains the following information:

Attribute Name

The name of the attribute as it appears in the application.

> **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a standard prefix or naming convention that ensures that your extended attribute names are unique.

> **Caution**: Changing an attribute name might cause attributes that were previously aggregated to no longer be recognized.

Display Name

The name for use throughout the product.

Type

The attribute type to be linked, for example string, boolean, date, rule, or identity.

Description

A brief description of the entitlement attribute.

Category Name

An optional category used to separate the attributes into categories on the Application Configuration page. Enter a category name or select an existing one from the drop-down list.

Searchable

Enable this entitlement attribute for use in queries.

Editable

Enable editing of this attribute from other pages in the product.

Required

For String type attributes only. Required attributes must have a value before you can save an entitlement.

Allowed Values

For String type attributes only. Enter the values that are allowed for this attribute. The values entered in this list are used to populate the drop-down value list on the Roles page.

Default Value

Enter a default value for the attribute or select a value from the drop-down list, depending on the attribute type you are working with.

How to Add or Edit Extended Entitlement Attributes

> **Note**: When mapping to a named column, specify the name to match the `.hbm.xml` property name, not the database column name. With camel case the database column name is translated to lower case with underscore separators. For example, costCenter in the Hibernate mapping file becomes cost_center in the database.

1. Click **New Attribute** or click an existing attribute to display the Edit Extended Attribute page.
2. Enter or change the attribute name and an intuitive display name.

> **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a standard prefix or naming convention that ensures that your extended attribute names are unique.

> **Caution**: If you define an extended attribute with the same name as an application attribute, the value of the extended attribute overwrites the value of the connector attribute.

3. Select the attribute type from the drop-down list, String, Integer, Boolean, Date, Rule, or Identity.
4. Optional Selections:
   - **Optional:** Enter a description of the additional attribute.
   - **Optional:** Select a category for the attribute.
   - **Optional:** Activate the Searchable option to enable this attribute for searching throughout the product.
   - **Optional:** Activate the Editable option to enable this attribute for editing from other pages within the product.
   - **Optional:** Mark the attribute as required. For string type attributes only.
   - **Optional:** Enter allowed values for the attribute. For string type attributes only.
   - **Optional:** Specify a default value.
6. Click **Save** to save your changes and return to the Edit Entitlement Catalog Configuration page.

Quicklink Populations

Quicklinks are tasked-based links to frequently-used areas of IdentityIQ. Quicklinks are displayed as cards on the IdentityIQ Home page and as links in the Quicklink Menu, which is available throughout the product.

Use the Quicklinks Populations page to associate quicklinks, that are created and imported into IdentityIQ by your administrators, with quicklink populations, sometimes referred to as dynamic scopes.

Quicklink populations grant access to specific areas of IdentityIQ to predetermined populations of users. These populations can be defined based on capabilities, identity attributes, work groups, or by selecting individual identities.

One predefined population, Everyone, is in the list by default. If you have purchased IdentityIQ Lifecycle Manager you also see Help Desk, Manager, and Self Service in the Populations list.

Select a population from the list or click **New** to open the Configuration and Quicklinks tabs.

The Configuration tab contains the following:

Details

Name

Name of the population.

Description

Description of the population.

Membership

Membership Rule

Select a membership rule to define the population.

None — only the identities specified in the **Included Identities** list are in the population.

All — include all identities in the population.

Match List — only identities whose criteria match that specified in the list. Add identity attributes, application attributes and application permissions. Customize further by creating attribute groups to which this assignment rule applies.

If Is Null is selected, the associated value text box is disabled. When the is null match is processed, the term matches users on the chosen application who have a null value for that attribute/permission.

Filter — a custom database query.

Script — a custom script.

Rule — select an existing rule from the drop-down list.

Click **Edit Rule** to launch the Rule Editor. See Using the Rule Editor.

Population — select an existing population.

Included Identities

Manually select identities to include in the population.

Excluded Identities

Manually select identities that should not be included in the population. For example, Administrator.

Who can members request for?

Identities for whom the members of this population can make access requests.

Everyone

Can create access request for anyone.

Specific Users

Can only create access requests for identities based on the selected criteria.
Use the drop down list to specify if they must match all of the criteria or just any of the criteria.

Share attributes with the requester

Can make requests for identities that share the attributes specified.

Report to the requester

Enable managers to make requests for their subordinates.
Specify if this applies to direct reports or all subordinates. If all subordinates, specify a **Maximum Hierarchical Depth**.

Match custom criteria

The filter is the context of the identity object and is parsed as a Velocity template with a parameter called `requester.spa`
For example for an identity whose manager's name is the same as the manager's name for the `requester: manger.name == "$requester.manager.name"`

Match filter rule

Select the IdentityFilterGenerator rule that generates the filter that specifies for whom users can make requests.

> Note: You must have the ManageRules SPRight to create or edit an Identity Filter Generator rule from this page.

When this rule is executed, the resulting filter value is added to the list of filters used to query the list of accessible identities.

For example, the following Beanshell in a rule could be used to return only identities that have the same manager as the requester.

```
import sailpoint.object.Filter;
import sailpoint.object.Identity;
log.warn("Executing on behalf of " + requester.getFullName());
if (requester.getManager() != null)
{
  return Filter.eq("manager.id", requester.getManager().getId());
```

```
}
return null;
```

Ignore scoping

Disregard IdentityIQ scopes when determining for whom request can be made.

What can members request?

Click **Edit Rule** to launch the Rule Editor for any of the following. See Using the Rule Editor.

Roles

Select a rule that defines the set of roles that this population can request.

Applications

Select a rule that defines the set of applications from which this population can request entitlements.

Entitlements

Select a rule that defines the set of entitlements that this population can request.

What can members remove?

Click **Edit Rule** to launch the Rule Editor for any of the following. See Using the Rule Editor.

Roles

Select a rule that defines the set of roles that this population can remove.

Applications

Select a rule that defines the set of applications from which this population can remove entitlements.

Entitlements

Select a rule that defines the set of entitlements that this population can remove.

Sync with Request

The selections from **What members can request** is copied to **What members can remove**.

Once you have selected a population, you can click The Quicklinks Tab to define Quicklinks for this population.

The Quicklinks Tab

This tab contains all of the quicklinks that are available in your environment.

You cannot add quicklinks within IdentityIQ. The **New** button opens the Configuration tab to create a new population.

Enabled

Specify which quicklinks to associate with this population.

Name

Name of the quicklink as it appears on cards on the IdentityIQ Home page and as links in the Quicklink Menu.

Description

Description of the quicklink.

Category

The category in which this quicklink displays in the Quicklink Menu.

Options

When available, use **Configure** to specify quicklink settings.

Forms

Form Editors are used for configuring forms for Workflows, Role Provisioning Policies, and Application Provisioning Policies in IdentityIQ. Forms are referred in two ways, Centralized Forms and Reference Forms.

Centralized Forms

Centralized Form location is a single location within the system, where an Administrator would be able to view all the forms. All of the forms can be created, edited, managed, and maintained as one object.

The Forms page displays all the standalone forms. The form grid displays Workflow, Role and Application types of forms.

Create and Edit Forms

To create a new form, click the **Create Form** button. On the **Create New Form** window, select one of the following type of the form to be created:

- Application Provisioning Policy Form
- Role Provisioning Policy Form

- Workflow Form

On saving the newly created forms, the form grid would be updated.

To edit an existing form, click the **Edit** button provided next to each form in the grid to display the Form Editor page.

Search Forms

Forms are searched by their names. To search the required form, enter any name word of the Form Name. The search results is displayed by refreshing the list to display the searched form.

Reference Forms

Reference Forms provide a means to create a single form that can be reused and referenced as standalone forms for Application Provisioning Policy Form, Role Provisioning Policy Form, and Workflow Form.

Create Forms

To create a new policy form, click **Add Policy** under the Provisioning Policies tab to display the Forms window. Click **Create Policy Form** to display the Provisioning Policy Editor page.

On saving the newly created policy, the provisioning policies are updated.

Referencing Forms

> Note: The Existing Forms lists only contain the reference forms of the type associated with the policy type you are viewing, application, role, or workflow. If you are not seeing forms in the list, ensure that the forms you are looking for have the correct type set on the **gear > Global Settings > Forms** page.

Form referencing is done by using the form name. To reference a form, click **Add Policy** under the Account Provisioning Policies tab to display the Forms window. Click **Reference Policy Form** to display the list of application provisioning policy forms from the central location on the Existing Forms page.

Edit Reference Forms

Click the policy name to display an option to **Create a Form** or **Change Reference Policy Form** button to edit an existing reference form.

- Click **Create Policy Form** to display the Provisioning Policy Editor page. On saving the newly created policy, the reference provisioning policies are removed and policy is updated with newly created form.
- Click **Change Reference Policy Form** to display a list of application provisioning forms.

Role Configuration

Use the Edit Role Configuration page to define custom extended role attributes and role types. The extended attributes are displayed with the rest of the role information throughout the product. An example of a extended role attribute might be role status. Role type is used to configure roles to perform different functions within your business model. For example, type might be used to control inheritance or automatic assignment of roles.

The Edit Role Configuration page contains the following information:

Role Attributes:

Name

The display name of the role attribute assigned when it was added.

Category

The category defined when the attribute was created.
If no category was defined this column is blank.

Description

A short description of the role attribute.

Role Types:

Name

The display name of the role type.

Description

A short description of the role type.

Click **New Attribute** to add additional role attributes. See Edit Extended Role Attributes.

Click **New Type** to add or edit a role type. See Edit Role Types.

To edit or delete an existing attribute or type from the list, right-click the item and select the corresponding option from the menu. If you are deleting, you must confirm the deletion in the pop-up dialog.

Edit Extended Role Attributes

Use the Edit Extended Attribute page to create and edit additional role attributes including the display name, attribute type and description.

> **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a standard prefix or naming convention that ensures that your extended attribute names are unique.

The Edit Extended Attribute page contains the following information:

Attribute Name

The name of the attribute as it appears in the application.

> Caution: Changing an attribute name might cause attributes that were previously aggregated to no longer be recognized.

Display Name

The name for use throughout the product.

Type

The attribute type to be linked, for example string, boolean, date, rule, or identity.

Description

A brief description of the role attribute.

Category Name

An optional category used to separate the attributes into categories on the Application Configuration page. Enter a category name or select an existing one from the drop-down list.

Searchable

Enable this role attribute for use in queries.

Editable

Enable editing of this attribute from other pages in the product.

Required

For String type attributes only.
Required attributes must have a value before you can save a role.

Allowed Values

For String type attributes only.
Enter the values that are allowed for this attribute. The values entered in this list are used to populate the drop-down value list on the Roles page.

Default Value

Enter a default value for the attribute or select a value from the drop-down list, depending on the attribute type you are working with.

How to Add or Edit Extended Attributes

How to Add or Edit Extended Attributes

1. Click **New Attribute** or click an existing attribute to display the Edit Extended Attribute page.
2. Enter or change the attribute name and an intuitive display name.

   > **Important:** Extended attributes must use unique attribute names that will not be duplicated in other parts of your IdentityIQ environment. For example, an extended attribute name must not duplicate any attribute names in any of your application schema(s). A best practice is to use a standard prefix or naming convention that ensures that your extended attribute names are unique.

3. Select the attribute type from the drop-down list, String, Integer, Boolean, Date, Rule, or Identity.
4. **Optional**: add more information for the extended attribute, as needed.
   - Enter a description of the additional attribute.
   - Select a category for the attribute.
   - Activate the Searchable option to enable this attribute for searching throughout the product.
   - Activate the Editable option to enable this attribute for editing from other pages within the product.
   - Mark the attribute as required. For string type attributes only.
   - Enter allowed values for the attribute. For string type attributes only.
   - Specify a default value.

5. Click **Save** to save your changes and return to the Edit Role Configuration page.

Edit Role Types

Use the Edit Role Type Definition page to create and edit types to use with roles. Role type is used to configure roles to perform different functions within your business model. For example, type might be used to control inheritance or automatic assignment of roles.

Role modeling also uses the concept of permission to enable you to grant users permission to specific roles without assigning them the role or incorporating it in their role hierarchy. For example, while a non-IT user with a business-type role might need access to the entitlements contained within an IT-type role, they probably do not need to have that role assigned to them or included as part of their hierarchal role structure.

The Edit Role Type Definition page contains the following information:

Type Name

The name of the role type.

Display Name

The display name of the role type used throughout the product.

Description

A brief description of the role type.

Icon Path

The path to the iconic representation of this role type.
See How to Add or Edit Role Types

Disallow inheritance of other roles

Do not allow roles of this type to inherit other defined roles.

Disallow other roles from inheriting this role

Do no allow roles of this type to be inherited.

No automatic detection with profiles

Do not automatically detect and assign this role to identities during aggregation and correlation.

No automatic detection with profiles unless assigned

Do not automatically detect and assign a role during aggregation and correlation unless it is required or permitted by an identity's assigned roles.

No entitlement profiles

Do not enable the direct assignment of profiles to this role type.
For example, a roles used to create hierarchy in your business model might only gain access to entitlement profiles through permitted IT roles.

No automatic assignment with rule

Do not allow a rule to automatically assign roles of this type to identities.

No assignment rule

Do not display the Assignment Rule panel in the Role Modeler for rules of this type.

No manual assignment

Do not allow roles of this type to be assigned manually from the Identities User Rights tab.

No permitted roles list

Do not display the Permitted Roles panel in the Role Modeler for rules of this type.

Disallow this role from being on a permitted roles list

Do not display roles of this type on the select list of the Permitted Roles panel of any other role.

No required roles list

Do not display the Required Roles panel in the Role Modeler for rules of this type.

Disallow this role from being on a required roles list

Do not display roles of this type on the select list of the Required Roles panel of any other role.

Disallow Granting of IdentityIQ User Rights

Do not allow the granting of IdentityIQ capabilities or scopes based on role assignment. If this option is selected, the Granted IdentityIQ User Rights table is not displayed on the Role Editor page.

How to Add or Edit Role Types

How to Add or Edit Role Types

1. Click **New Type** or click an existing type to display the Edit Role Type Definition page.
2. Enter or change the name and display name.
3. Enter an icon path to link to the iconic image associated with roles of this type in the Role Modeler.

   To assign an icon to a role type, do the following:

   a. Add two icon images to *iiq_home*/images/icons folder of your IdentityIQ installation, one for the role and one for the role as it is undergoing analysis or approval. For example:

```
.itIcon {
 background-image: url("../images/icons/modeler_application_16.png")
!important;
 background-repeat: no-repeat;
}
.itIconPendingbusiness process {
 background-image: url("../images/icons/modeler_application_approval_16.png")
!important;
 background-repeat: no-repeat;
}
```

   b. Reference the images from the `iiq-custom.css` file in the `iiq_home/css` directory.

3. **Optional:** Select configuration options for the role type.
4. Click **Save** to save your changes and return to the Edit Role Configuration page.

Scopes

Scope is used to determine the objects to which a user has access. If scoping is active, identities can only see objects that they created or that are within the scopes they control. IdentityIQ capabilities control the components within the product to which a user has access. Scope controls access to the individual objects within those components. For example, a user might be able to access the Identity Search page, however, the Application and Role drop-down lists only display application and roles that are contained within a scope they control.

Scope is referred to in two ways, Controlled Scope and Assigned Scope. Assigned scope is the scope assigned to an identity or object manually, automatically, or through aggregation and correlation. Controlled scopes refer to the scopes to which an identity has access. You can only see objects that are within your controlled scopes, that you created, or possibly that have no scope assigned. Controlled scope is hierarchical. If you control a parent scope, you control any child scopes contained within.

Use the Configure Scoping page to create new scopes, edit existing scopes, and configure scoping for your enterprise.

> Note: If you manually create scopes they should be associated with existing identity attributes or be defined in a scope correlation rule.

Create and Edit Scopes

To create a new scope, right-click **Scopes** and select **New** to display the Create Scope page. Enter the scope name and click **Create** to return to the Scope page. Use the Scope Correlation Rule to correlate identities with the correct scopes.

To edit an existing scope, right-click the scope and select **Edit** to display the Edit Scope page. You can only edit the display name.

Drag and drop existing scopes to create a scope hierarchy.

Delete Scopes

To delete a scope, right-click the scope and select **Delete** to display the Delete Scope page. The Delete Scope page contains the following:

Assigned Scope Replacement

Reassign objects to a different scope upon deletion.

Authorized Scope Replacement

Assign an authorized scope to replace the one to be deleted.

Delete Child Scopes

Delete all child scopes in the scope hierarchy.

Configure Scoping

Use the Configure Scoping page to configure scope assignment and correlation. The Configure Scoping page contains the following:

> Note: You must run an identity refresh task with the refresh scope option enabled before scope configuration changes are visible.

Enable Scoping

> Note: De-selecting this option is useful in troubleshooting performance issues.

When checked, scoping mechanisms are enabled. Scopes do not take effect until this is enabled, even if the scopes are already defined and assigned.

Scope Identity Attribute

Select an identity attribute from the drop-down list to use for scoping.

A scope is created for each value of the selected attribute aggregated during the identity refresh task. This attribute is used to correlate identities to assigned scope.

Scope Correlation Rule

Select a rule to use to correlated scopes and identities during aggregation and refresh task. If a scope is not found that correlates to the value returned by an attribute, one is created.

Scope correlation rules enable more flexibility in scope assignment than specifying a single identity attribute.

Click the **...** icon to launch the Rule Editor to make changes to your rules if needed.

See Using the Rule Editor

Scope Selection Rule

Select a selection rule to use if the identity attribute or scope correlation rule return more then one value for the assigned scope of an identity.

For example, if department is specified as the scope identity attribute and the identity aggregation task returns more then on value for department for an identity, this rule determines which value to use as the assigned scope.

Click the **...** icon to launch the Rule Editor to make changes to your rules if needed.

See Using the Rule Editor

Unsloped Objects Globally Accessible

When selected, all objects that do not have an assigned scope are available to all users.
When cleared, all objects that do not have an assigned scope are only available to system administrators.

Identity Controls Assigned Scope

When selected, identities automatically control the scope to which they are assigned.

Time Periods

Use the Configure Time Periods page to specify the time periods used for activity searching. Setting time periods for your enterprise enables you to track who is accessing your sensitive applications and when they are accessing it.

Access at unusual times can indicate a security issue that requires investigation. Time periods include things such as office hours, holidays, and weekends. Because each time period is set individually, you can customize the setting to meet the needs of your enterprise.

The following are the available time periods:

- Date ranges — a range of specific dates that define things such as fiscal quarters.
- Time ranges — a range of hours, or times, that define office hours and non-office hours.
- Date lists — a list of dates that define enterprise holidays.
- Day lists — a list of days that define week days and weekends.

To edit a time period, click a time period in the Time Periods column to access the Configure Time Period page and make the required changes.

Configure Time Period

The configuration options on the Configure Time Period page are based on the type of time period to be edited.

Date Ranges:

For date ranges, specify the Begins on and Ends on dates for the time period to be defined. For these date ranges you can enter dates manually of click the... icon and select a date from the calendar.

Time Ranges:

For time ranges, specify the starting at and ending at times. Time ranges are used to define working and non-working hours.

Date Lists:

Use the date list to specify a list of holidays, or regularly schedule dates on which your enterprise business would not normally conduct business. This list does not include weekends. Weekends are defined separately from a day list. You can enter dates manually of click the "..." icon and select a date from the calendar. Use the Add and Delete buttons to add or remove dates from the list.

Day Lists:

Use the day lists to specify week days from weekend days. Select the correct days using the selection boxes on the right of the table and deselect, or DE-activate, the days that should not be included.

Audit Configuration

Use the Audit Configuration page to specify the actions that are collected for audit logs. Since collecting event information and storing it in the audit logs affects performance, a system administrator must specify the actions that are audited. Before any data is collected by the audit logs for use in an audit search, IdentityIQ must be configured for auditing.

The Audit Configuration page contains the following types of actions:

- General Actions — typical action performed while using IdentityIQ. For example, running a task and signing off on a certification are general actions.
- Link Attribute Changes — changes made to any assigned link attributes.
- Identity Attribute Changes — changes to assigned roles, capabilities, authorized scopes, and controlled scopes, and changes to the password. This list might also include extended identity attributes.
- Class Actions — action taken on the underlying classes used to configure the way in which IdentityIQ operates. For example, editing a role, creating a policy, specifying the default email template, and adding attachments are class actions.
- SCIM Resource Actions — action taken on any SCIM resource, for example, create, read, update, and delete.

Electronic Signatures

Electronic signatures provide proof of a decision. You can set up electronic signatures to be used for Certifications, Policy Violations, and Approvals. Use the Electronic Signatures page to set the meaning or text that is displayed to the end user when they perform an electronic signature.

> Warning: Electronic Signatures have legal implications. They should explicitly state each action and consequence, to ensure that end users understand what they are signing.

Electronic Signature Meanings

The Electronic Signature Meanings page displays a table of configured meanings. Click **New Meaning** to open the New Electronic Signature Meaning window. Provide a **Name**, **Display Name**, and **Meaning**. The **Meaning** is the text of the electronic signature that the user will agree to when signing. Then click **Save**.

If your IdentityIQ instance is configured to support Multi-Language Descriptions, you can supply Meanings for the electronic signatures in any of the languages IdentityIQ is configured to support. For more information see the **Multi-Languages Descriptions** section in the Miscellaneous tab.

Electronic Signature Authentication

The method that end users will use for authenticating when they perform an electronic signature is determined by IdentityIQ's login configuration (under the **gear** menu > **Global Settings** > **Login Configuration**).

If **SAML Based SSO** is enabled and configured, the user performing an electronic signature will be routed to your SAML provider for authentication, then returned to the IdentityIQ UI to complete the signature. If you are using **rule-based SSO** for authentication to IdentityIQ, electronic signature uses an SSO rule to complete the electronic signature process. In other cases, **basic authentication** with the user's IdentityIQ credentials is used. See SSO Configuration.

Auditing SAML-Based Electronic Signatures

If SAML is enabled, SAML details for electronic signatures can be included in auditing. To enable this, check the **Login** option in the Audit Configuration. You can use Advanced Analytics to search for and view details about SAML authentication for electronic signatures, including the SAML Assertion ID, SAML Issue Instant, SAML Issuer, SAML NameID and Sign-Off Validity.

For more information about Advanced Analytics, see the **IdentityIQ Advanced Analytics** documentation.

API Authentication

IdentityIQ supports the use of OAuth 2.0 (client credentials) as a token-based protocol for API authentication. Use this feature to create and manage OAuth clients that you use with the IdentityIQ API.

> Note: You can set up a proxy user that connects on behalf of the user to avoid exposing sensitive user data. In order for the proxy user to have correct rights to make API calls, you must assign capabilities to that proxy user.

OAuth Client Management

The **OAuth Client Management** tab is where you create and edit OAuth clients.

How To Create An OAuth Client

1. From the top menu, navigate to the **Gear icon > Global Settings > API Authentication**.
2. On the OAuth Client Management tab, click **Create**.
3. In the OAuth Client dialog enter a unique name for **Client Name** and then enter a user name or select a user from the drop-down list for the **Proxy User**.
4. Click **Save** to save your new OAuth client.

After your create an OAuth client, you can use it with the associated secret to log in and access the token for that proxy user.

The OAuth Client Management tab also gives you these controls for editing the OAuth client and displaying the secret:

- **Secret Details** icon: click to display the secret for the OAuth client.
- **Edit** icon: click to edit the Client Name or Proxy User.
- **Delete** icon: click to delete the OAuth client. You will be prompted to confirm the deletion.
- **Regenerate** icon: click to generate a new secret for the OAuth client. Generating a new secret will prevent new tokens from being issued using the existing secret.

General Settings

- **Access Token Expiration in Seconds**: set the number of seconds that the OAuth token is valid for.

Token Settings

- **Access Token Authentication Scope**: The expected scope of the API access token issuer; for example, `GetToken`.
- **Access Token Authentication Audience**: A suffix that identifies the service or system to which the call is directed; for example `/iiq/api`. The validator will ensure the SSO audience claim ends with this value.
- **Access Token Authentication Issuers**: Identification of the SSO token provider; for example, `https://sts.windows.net/{{tid}}/`.
- **Correlation Variable**: The SSO claim used match the requesting user with an existing IdentityIQ user; for example `oid`.

If you want to remove any required data from these fields, use the **Clear and Exit** option. This allows you to reset your identity authorization token settings by removing them even though they are required.

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.

File Access Manager Configuration

IdentityIQ can integrate with File Access Manager to bring key data governance features to the IdentityIQ business user. A Data Governance menu in IdentityIQ provides direct access to the File Access Manager website, and dashboard widgets provide the context needed to make informed access decisions.

You can also use the File Access Manager Configuration settings to configure correlation logic for mapping File Access Manager objects to IdentityIQ identities.

To install and configure the File Access Manager integration:

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

Connection Information for File Access Manager:

File Access Manager Hostname

The host name of the File Access Manager server. This is the host where the File Access Manager website is installed.

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

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

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, enter the username for an identity that has the API User privilege in File Access Manager.

Password

For Basic authentication, enter the password for an identity that has the API User privilege in File Access Manager.

Client ID

For OAuth authentication, enter the OAuth client ID for File Access Manager

Client Secret

For OAuth authentication, enter the OAuth client secret for File Access Manager

Correlation Information for File Access Manager:

SCIM Correlation Rule

If the correlation logic in your configured applications does not meet your needs for correlating File Access Manager groups and accounts to 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 drop-down.

SCIM Correlation Applications

Select the application(s) to use for correlating File Access Manager objects to IdentityIQ identities. Selecting an application here means that the correlation logic defined for the application will determine how File Access Manager objects are correlated to identities.

Use **Test Connection** to verify that the connection information is accurate and functional.

Data Governance Menu

Once the File Access Manager integration is configured, a Data Governance menu is available in IdentityIQ. The Data Governance menu provides direct access to features in the File Access Manager website.

The Data Governance menu is available only to users who have the IdentityIQ FAM Administrator capability, or any capability that includes the ViewFAMNavigationMenu SPright.

For more information about Data Governance in File Access Manager, refer to the IdentityIQ File Access Manager documentation.

Dashboard Widgets

Once the File Access Manager integration is configured, widgets that show data about Sensitive Data Exposure and Sensitive Resources Missing Owners are available on the IdentityIQ home page.

The widgets display read-only information about sensitive data that is monitored in File Access Manager. Each widget shows counts for resources, and an overall compliance score. The compliance score is color-coded to indicate risk, 0-5 is considered high risk, 5.1-7.5 medium risk, and 7.6-10 low risk.

The widgets do not provide direct access to the File Access Manager website; in other words, users cannot click the widgets for more detailed information, or to access the File Access Manager website.

These widgets are available to users who have the IdentityIQ FAM Administrator capability, or any capability that includes the ViewFAMAdminWidgets SPright.

Users can click **Edit** on the home page to add, remove, or move these widgets.

For more information about Sensitive Data Exposure and Data Ownership in File Access Manager, refer to the **File Access Manager** documentation.

Import From File

Use the Import From File page to import files into IdentityIQ. For example, use this page to import custom rules or scoring pages.

> Note: Imported files might not be immediately available. Some file contents might require an application restart.

> Note: Any include directives in the import file include files from the application server file system and not that of the client browser.

Use the Browse button to navigate to a file or enter the path manually and click **Import** to begin the download process.

Select **No role events generated for role propagation** to avoid event generation during role propagation.

When the import is complete the results are displayed on the Import from File Results page. Click **Import Another File** to go back to the Import from File page, or **Done** to return to the **Global Settings** page.

Compliance Manager

> Note: Most of the fields on this page enable you to configure default settings that a user can change on certifications they are reviewing or scheduling. Those fields that behave differently are described as such.

From the Navigation bar, click the gear icon and then select **Compliance Manager**. Use the Compliance Manager page to configure control and default settings for certifications.

- Select to enable email notifications to users that have items revoked.
- Input the number of selected items which require additional confirmation for bulk revocations.
- Enable the certifier to provision missing role requirements from within an access review.
- Select the actions to enable from the Worksheet/Identity view and the Detail view. The actions include the following:
- Exclude entitlements on tier application accounts from the access review.This only applies to logical applications. Tier applications are those application that make up a logical application.
- Notification Templates

Lifecycle

Notify Users of Revocations

Select to enable email notifications to users that have items revoked.

Certification Escalation Rule

Select a rule from the drop-down list as the default rule that the system uses when an access review is escalated.

When Exceptions Expire

Select the action performed on a mitigation when it expires

Active Period Duration

Input the number of units and unit type (hours, days, weeks or months) to use as the default active period duration.

Enable Challenge Period

Select to enable default challenge period and its default duration.
The challenge period enables users to challenge requests from certifiers to remove access privileges.

Enable Revocation Period

> Note: Select to enable the default revocation period and its default duration. The revocation period places a limit on the amount of time a revoker has to act on a revocation request before that request work item is escalated.

If the revocation period is disabled, the certification is not scanned for completed revocations and revocation status might not be accurately reflected throughout the product.

Default Revoker

Select the user to whom all bulk remediation requests are to be sent.
Bulk revocation requests are made during the certification process. You can select an item from the **Select Bulk Action** drop-down list on the Certification Report worksheet view or click **Revoke All** on the Certifications Decision tab.
If this field is left blank, the remediator is specified as part of the request process.

Enable Automatic Closing

Specifies that the remediation period should be enabled, during which IdentityIQ periodically scans users to determine whether the requested remediations have been carried out. Use the following options to configure the details of this process.

Time After Certification Expiration — Select the amount of time following this access review expiration date that IdentityIQ should wait before attempting to automatically close it.

Closing Rule — Select the rule that IdentityIQ runs at the beginning of the automatic closing process.

Action Taken On Undecided Items — The action that IdentityIQ assigns to any undecided items when automatically closing this access review. Choose from Approve, Revoke, or Allow Exception.

Comments — Input the comments that IdentityIQ adds to any undecided items when automatically closing this access review.

Signer — Select the identity who signs off on automatically closed access reviews. This setting is only configurable at the system setup level. Individuals who are scheduling certifications cannot define the signer.

Behavior

Selection Count Requiring Bulk Revoke Confirmation

Input the number of selected items which require additional confirmation for bulk revocations.

Prompt for Sign Off

Select to display a pop-up window when an access review is complete and ready for sign off.

Require Electronic Signature

Select to require that, by default, all certifications require an electronic signature.

Require Subordinate Completion

Require that, by default, all subordinate access reviews be completed before the parent access review can be completed.

Automatically Sign Off When Nothing to Certify

Automatically sign off the certification when assignee has nothing to certify.

Suppress Notification When Nothing to Certify

Suppress notification of certification when assignee has nothing to certify.

Require Reassignment Completion

Require that, by default, all reassigned access review items be completed before the parent access review can be completed.

Return Reassignments to Original Access Review

Specify that, by default, the content of reassigned access reviews be returned to the parent access review upon sign off.
Use this option to ensure that the original content of an access review request is preserved for tracking and reporting purposes.

Automatically Sign Off When All Items Are Reassigned

> Note: This item is not available if the Required Reassignment Completion or the Return Reassignments to Original Access Review options are selected.

Specify that an access review be automatically signed off on when all items in that access review are reassigned.

Require Comments for Approval

Require that all certifiers enter comments for each item they approve in an access review request.

Require Comments When Allowing Exceptions

Require certifier to include comments when a certification decision is made.

Require Comments For Revocation

Require certifier to include comments when a certification decision is made.

Require a review on delegated certification items

Select to require that all access review approvers review the decision made on any user, role, entitlement, or policy violation that they delegated to another approver before they can complete the access review containing that delegation.

Require delegated certification items to be completed

Select to require that all items in a delegation work item have a decision associated with them before the work item can be marked as complete. This setting is only configurable at the system setup level. Individuals cannot change the value of this setting for a single certification.

Disable Delegation Forwarding

Select to disallow the forwarding of a work item that a different user delegated.

Allow Self Certification For

Choose which users may self-certify - that is, be the certifier for their own access, either by forwarding or reassigning an access review: All certifiers, Certification and System Administrators, System Administrators only.

Self Certification Violation Owner

For users that are not allowed to self-certify, this is the identity or workgroup that will receive any items that would require a self-certification - that is, when the reviewer and the user whose access is under review are the same person. If a Self Certification Violation Owner is not specified, any items that require self-certification will be read-only to the reviewer.

Limit Reassignments

The limit reassignment feature allows you to limit the number of times the users within the certification campaign can reassign a certificatation item.

Reassignment Limit

> Note: Certification is not forwarded or reassigned when the reassignment limit is reached.

Set the number of reassignments allowed.

Show Classifications

Set the global default to show classification data in certification access reviews. Classifications can be shown in Manager, Application Owner, Advanced, Role Membership, and Targeted certifications. This setting also determines whether classification information is shown in Separation of Duties (SOD) policy violations, in the dialog for correcting violations by revoking access.

Decisions

Enable Provisioning Of Missing Role Requirements

Enable the certifier to provision missing role requirements from within an access review.

Enable Line Item Delegation

Enables certifiers to delegate individual access review items, such as a single role or entitlement, rather than the entire identity to be reviewed.

This option also enables the delegation of policy violations, either from inside an access certification or from the Manage -> Policy Violations page.

Enable Account Revocation

Allow users to bulk revoke all entitlements for a given account.

Enable Identity Delegation

Enable certifiers to delegate entire identities from a certification request.

Enable Allow Exceptions (applies only to non-policy violation items)

Enables certifiers to allow exceptions on access review items such as roles or entitlements, that are not policy violations. Allowing an exception means the user should not have access indefinitely, but can retain access for a specified period of time.

Deprovision Items When Exception Expires (applies only to non-policy violation items)

Enables automatic deprovisioning of access when the allowed exception period has expired. This setting applies only to items such as roles or entitlements, that are not policy violations.

Enable Allow Exception Popup

Enables certifiers to view the Allow Exception pop-up and manually set expiration dates.

Default Duration for Exceptions

Set the time period during which exceptions should be allowed. Input the number of units and unit type (hours, days, weeks or months) to use as the exception duration.

Default Operation for Remediation Modifiable Attributes

Set the default operation shown on the revocation dialog for remediation-modifiable attributes.

Show Recommendations

> Note: This option is only visible if you have purchased and activated the SailPoint AI Services product.

Enable recommendations from AI Services to display in access reviews.

Automatically Approve Recommended Items

> Note: This option is only visible if you have purchased and activated the SailPoint AI Services product.

Enable access review items to be automatically marked as approved by AI Services and move to the Access Certification Review tab for final approval.

Bulk Actions

Select the actions to enable from the Worksheet/Identity view and the Detail view. The actions include the following:

- Enable Bulk Approve
- Enable Bulk Revocation
- Enable Bulk Allow Exceptions

- Enable Bulk Reassignment
- Enable Bulk Account Revocation
- Enable Bulk Clear Decisions

Certification Contents

Exclude Logical Tier Entitlements

Exclude entitlements on tier application accounts from the access review.
This only applies to logical applications. Tier applications are those application that make up a logical application.

Generate Certification(s)

Specify whether, by default, access review requests should generate an access review request for the specified managers, or for the specified managers and all employees below them in the reporting hierarchy.
If you select **For the specified manager(s) only**, the **Flatten Hierarchy** option is displayed. Select the **Flatten Hierarchy** option to include all of the employees that report directory to the selected managers and the employees that report to their subordinate managers on the access review request.

Notification Templates

Much of the communication performed during the access review process is done through notifications that are sent automatically by IdentityIQ as an access review proceeds through its lifecycle. Notifications can be sent as emails, or as notifications in Microsoft Teams.

Use this section to choose the template to use for each certification-related notification.

Define Home Page Quicklinks

Quicklinks are objects in IdentityIQ that enable you to place customized links on the IdentityIQ Home page and in the Quicklinks menu available on every page. Quicklinks are defined when IdentityIQ is deployed and are based on the needs of your enterprise. You can determine the behavior and availability of these links for different users. For example, IdentityIQ can be set up to limit access based on the user capabilities, rights, or workgroup membership.

Three objects control links. QuickLink objects define the links, the DynamicScope object controls who can view those links, and the QuickLinkOption object references the first two to create the Quicklinks within the product.

QuickLinkOption

The **QuickLinkOption** object is created when a quicklink population, or DynamicScope object, is created on the Quicklink Populations page and associated with one or more **QuickLink** objects. The **QuickLinkObjects** objects do not control quicklink populations, nor the targets of the **QuickLink** objects, they are containers holding references to both.

```
<QuickLinkOptions allowSelf="true" created="1443970828183"
id="2c90900950335ce70150335e4797010e">

  <DynamicScopeRef>

    <Reference class="sailpoint.object.DynamicScope"
id="2c90900950335ce70150335e4783010c" name="Everyone"/>

  </DynamicScopeRef>

  <QuickLinkRef>

    <Reference class="sailpoint.object.QuickLink"
id="2c90900950335ce70150335e478a010d" name="Access Reviews"/>

  </QuickLinkRef>

</QuickLinkOptions>
```

DynamicScope

The DynamicScope object define groups of users, quicklink populations, based on capability, rights, indirect capabilities and rights granted by a workgroup, population, or any attribute of the identity. These objects are defined on the Quicklinks Populations page. Refer to the system administration documentation for more information.

DynamicScope objects are referenced by name or ID in a **QuickLinkOption** object. If the quicklink population applies to an identity, the Quicklink is visible to that identity. Only System Administrators can view Quicklinks with no scopes.

> DynamicScope objects are used to define the population of people who can view and run the Quicklink. DynamicScope objects are not the group of identities or objects that the Quicklink interacts with after the link is clicked.

Examples

The product ships with a DynamicScope that represents the **allowAll** option. The name of the DynamicScope is named **Everyone**. You can associate this option with any Quicklinks you want to enable the entire user population to view or use. The following **QuickLinkOptions** reference this DynamicScope by default:

- Access Reviews
- Approvals
- Signoffs
- Work Items
- Policy Violations

```
<DynamicScope allowAll="true" created="1443970828163"
id="2c90900950335ce70150335e4783010c" name="Everyone"/>
```

The following XML example of a DynamicScope restricts visibility to a specified Quicklink. Visibility is enabled for users in the IT department or who have the Help Desk Personnel capability. Visibility is also enabled for identities in the Inclusion list. Because Barbara.Wilson is in the Inclusions list, she can always see the Quicklink regardless of her capabilities or department.

```
<DynamicScope created="1443973952475" id="2c90900950335ed60150338df3db000a" name-
e="MyDynamicScope">
  <Description></Description>
  <Inclusions>
    <Reference class="iiq.object.Identity" id="2c90900950336e720150336f0797010d" name-
e="Barbara.Wilson"/>
  </Inclusions>
  <PopulationRequestAuthority allowAll="true"/>
  <Selector>
    <IdentitySelector>
      <MatchExpression>
        <MatchTerm name="capabilities" value="Help Desk Personel"/>
        <MatchTerm name="Department" value="IT"/>
      </MatchExpression>
    </IdentitySelector>
  </Selector>
</DynamicScope>
```

By default, IdentityIQ assumes that any link defined as a top-level **QuickLink** object is for a non-Lifecycle Manager action which does not operate on a target identity, so no user selection options are presented.

EmailTemplate Nested Elements

The components listed are generally expressed as nested elements due to their complexity and length.

<subject>

Subject line for the email message

<body>

Body, or main content, of the email message

<signature>

Hashmap of arguments to the email template
The signature for each template cannot be changed through the XML. Arguments to each template vary based on the associated system activity to which they apply. Properties and methods belonging to any object passed as an argument are available to include in the message, but other objects that are not part of the template signature cannot be retrieved to use in the email message.

<Inputs>

Nested element within Signature, signifying the input arguments to the template

<Argument>

> HTML cannot be passed into a template as an argument value. All HTML must be included as part of the base template.

Nested element within Signature and Inputs. This element names and specifies the type of each input argument to the template

<Description>

Indicates descriptive information for the reader of the XML. Describes the element in which it is nested
For example:
`<Description>` within `<Argument>` describes the argument usage.
`<Description>` within the `<EmailTemplate>` describes the purpose and usage of the template

At the most basic level, the contents of these elements and attributes can be written as straight text values with no variable substitutions. However, the real flexibility and usefulness of these templates is found when custom text is substituted into the message body, subject, and other attributes. This substitution is managed by the Apache Velocity Engine.

IdentityIQ Email Templates

Many events in IdentityIQ generate email notifications to notify users of actions required by them or actions taken that directly affects them. These email messages are created based on email templates. Basic templates are provided with the product to construct messages corresponding to each of the email-generating events, and these messages can be customized to meet your specific needs.

> Note: The default email templates should not be modified directly because they might be over-written during the IdentityIQ release upgrade process.

To customize any of these templates, copy and rename the template using a unique name.

1. Copy and rename the template using a unique name.
2. Associate the customized template to the email-generating event through the IdentityIQ user interface or configuration XML. See Importing Email Templates into IdentityIQ.

Accessing the Templates

The default email templates that ship with the product are located in the following area:

- Directory — *`iiq_installation_directory`*`/WEB-INF/config directory`
  where *`iiq_installation_directory`* is the location where you expanded the IdentityIQ installation media
- Files — `emailtemplates.xml` and `lcmemailtemplates.xml`

A third file, named `emailtemplatesSample.xml`, contains additional example templates that are not loaded into IdentityIQ during the initial load process. These templates describe how to create HTML email messages. Any of the templates in these files can be cloned to create custom templates.

After the email templates are loaded into IdentityIQ, either during the initial load or using the console or user interface import option, the templates are stored as XML objects. The templates can be viewed or modified through the IdentityIQ Debug pages. The default templates should not be modified from here because the template are overwritten during any IdentityIQ version update. However, customized templates can be edited directly through the Debug pages, if the organization's source code control procedures allows.

To view the list of email templates from the Debug pages, select **EmailTemplate** from the object list and click **List**. Select the desired template to view or edit its XML representation.

Importing Email Templates into IdentityIQ

When email templates are edited outside of IdentityIQ, they must be imported into the system before they can be used for any notifications. Email templates can be imported through the IdentityIQ user interface or console.

To import a template through the user interface, navigate to the **Gear** icon **-> Global Settings -> IdentityIQ Configuration -> Import from File**. Click **Browse** to select the email template's XML file from the file system and click **Import**. IdentityIQ parses the XML during the import process and recognizes the file's contents as an EmailTemplate object. The import fails if the XML is invalid.

> Note: Import files can contain one or more EmailTemplate objects. However, if a file contains more than one object, the import methods expect the set of objects to be wrapped in a `<sailpoint></sailpoint>` block.

To import the email template through the IdentityIQ console:

1. Navigate to the `IdentityIQ_Installation/WEB-INF/bin` directory.
2. Start the console and use the console import command to import the file. The import is successful only if the XML is valid. Any errors encountered are reported to the console.

Associating Templates with Events

Email templates are associated to their respective email-generating events in several places in the IdentityIQ user interface and configuration XML. The information below shows the notification type, the default template name, and their association location. To use a custom template for any of these notifications, specify the custom template name in place of the default template in that notification configuration.

For details about the arguments which are provided by default to all instances of email messages sent as part of IdentityIQ's core processes, see the Email Template Arguments technical white paper on Compass.

> Note: HTML cannot be passed into a template as an argument value. All HTML must be included as part of the base template.

> Note: Different email templates accept and use different arguments. The selection lists in the user interface for each notification lists all email templates, no matter what arguments they require. Because IdentityIQ provides a fixed set of arguments for each notification type, only templates whose arguments list matches the provided arguments work correctly to create a useful event notification. Refer to the default template XML to see the arguments (names and variable types) for each notification, and ensure that the selected template's argument list matches the default template's arguments.

IdentityIQ Global Notification Templates

The following templates can be configured in the **Gear icon > Global Settings > IdentityIQ Configuration > Notification Settings > NotificationsTemplates** section.

Server Root Path

The root path of the server, including the scheme, server name [port], and root directory. For example, if the value was set to 'https://localhost:80/iiq', then the expected URL would look like <serverrootpath>/example.jsf or https://-localhost:80/iiq/example.jsf

Templates

For reminder notices

Work Item Reminder

For escalation notices

Work Item Escalation

For work item comment notices

Work Item Comment

For work item forwarding notices

Work Item Forward

For policy violation notices

Policy Violation

For task and report signoff notices

Task Result Signoff

For work item assignment notices

Work Item Assignment

For work item assignment removal notices

Work Item Assignment Removal

For remediation item assignment notices

Remediation Item Assignment

For remediation item assignment removal notices

Remediation Item Assignment Removal

For delegation notices

Delegation

For delegation finished notices

Delegation Finished

For delegation revocation notices

Delegation Revocation

For remediation work item notices

Remediation Work Item

For certification reminder notices

Certification Reminder

For policy violation delegation notices

Policy Violation Delegation

For open certifications notices

Open Certifications

For access request reminder notices

Access Request Reminder

For notice of deprovisioning of sunsetted roles and entitlements

Sunset Expiration Reminder

Compliance Notification Email Templates

These notifications are used with Certifications. Navigate to **gear icon > Compliance Manager** and scroll down to the **Notification Templates** section.

> Note: When the challenge period is enabled, Challenge-related notification email templates can be overwritten for individual certifications on the Lifecycle page in each certification configuration.

> Note: Initial Notification and Bulk Reassignment notices can be overwritten for each certification on the Notifications page in each certification configuration.

Suppress Initial Notifications

Check this option if you do not want to send initial notification emails to certifiers. This sets the default initial notification behavior at a global level, but you can still change it for an individual certification campaign as needed.

Templates

Initial Notification Email Template

Certification

Exceptions Expiration Notices

Mitigation Expiration

Bulk Reassignment Modification notices

Bulk Reassignment

Challenge Period Start Notices to Challengers

Challenge Period Start

Challenge Period End Notices to Certifiers

Challenge Period End

Challenge Creation Notices to Challengers

Challenge Creation Notification

Challenged Decision Notices to Certifiers

Certification Decision Challenged Notification

Challenge Expiration Notices to Challengers

Challenge Expiration

Challenge Decision Expiration Notices to Challengers and Certifiers

Challenge Decision Expiration

Challenge Accepted Notices to Challengers

Challenge Accepted

Challenge Rejected Notices to Challengers

Challenge Rejected

Sign-off Approval Notices to Approvers

Certification Sign-off Approval

Reminder or Escalation Email Templates

These are set in the Notifications step in each certification configuration when the associated reminder or escalation option is enabled.

Reminder Email Template

Work Item Reminder

Escalation Email Template

Work Item Escalation

(Revocation) Reminder Email Template

Work Item Reminder

(Revocation) Escalation Email Template

Work Item Escalation

Report Sign-off Email Template

> Note: Because this is cumbersome, you might choose to edit the Default Report Template directly rather than cloning it. This customization must be reapplied after any IdentityIQ version upgrade, as it is overwritten during the upgrade process.

Not specified in the user interface. When a report is defined, its XML can be edited to add an emailTemplateId argument to change the email message template.

Configured in report specification if **Require Signoff** is selected when the report is defined.

Report signoff initial notification

Task Result Signoff

Report signoff reminder notice

No default in UI but argument list matches Work Item Reminder

Report signoff escalation notice

No default in UI but argument list matches Work Item Escalation

Send PDF of report to someone

Default Report Template

Workflow Email Templates

Email templates may be specified within workflow definitions in **Setup >Business Processes** as a process variable, step argument, or work item configuration email notification template.

> Note: For templates referenced from a workflow, all workflow variables, and all steps arguments and approval arguments defined for the step that invokes the email template are also available for use in the email message (subject, body, cc, etc.)

Various Process Variables and Step Arguments

LCM Requester Notification

LCM Manager Notification

LCM User Notification

Approval Work Item Configuration Email Notification Template

LCM Identity Update Approval

The following workflows (including sub-processes) use these templates:

- Identity Correlation
- Do Manual Actions
- Do Provisioning Forms
- Assimilate Provisioning Form
- Provisioning Approval Subprocess
- Identity Request Notify
- Identity Request Provision
- LCM Create and Update
- LCM Manage Passwords
- LCM Provisioning
- Lifecycle Event - Leaver
- Lifecycle Event Reinstate
- Role Modeler - Impact Analysis
- Role Modeler - Owner Approval

The following templates do not include a Type in their XML definitions, so they may be used in various workflows:

- LCM Pending Manual Changes
- LCM Password Change Notification
- Pending Manual Changes
- Account Selection Notification
- Provisioning Form Notification

- Role Modeler - Approval
- Role Modeler - Impact Analysis Review

XML Email Templates

XML email templates cannot be configured through the user interface, they can only be edited through the email template's XML

From IdentityIQ **Debug Pages > Object Browser**, select the **EmailTemplate** object, then select the individual template to edit.

> Important: There is no rollback mechanism for edits to objects that are saved in the Debug pages. Although objects can be viewed and edited in the Debug pages, it is a best practice to export or check out the object, edit the XML as needed outside of IdentityIQ, and then import the updated object to a test environment for validation before importing into your production instance. This also allows you to manage your changes in a source control system, to facilitate rollback. Use caution when editing objects in the Debug pages, as there is no mechanism in the Debug pages for rolling back changes once they have been saved.

To edit a template's value in your implementation, select the **Configuration** object, then **System Configuratio**n and search the XML for these email template names or key values:

key=delegationEmailTemplate

Delegation

key=delegationRevocationEmailTemplate

Delegation Revocation

key=delegationFinishedEmailTemplate

Delegation Finished

key=remediationEmailTemplate

Remediation Work Item

key=remediationNotificationEmailTemplate

Remediation Notification

Sent when Notify Users of Revocations is selected in a certification configuration.

key= certificationReminderEmailTemplate

Certification Reminder

Sent on demand from certification.

key= policyViolationDelegationEmailTemplate

Policy Violation Delegation

key= AccountGroupPermissions. challengeGenerationEmailTemplate

Account Group Challenge Creation Notification

Specialized form of the Challenge Creation Notification email

key= accessRequestReminderEmailTemplate

Access Request Reminder

Sent on demand from the Access Requests page

key=openCertsEmailTemplate

Open Certifications

Email Template XML

The Email Template XML consists of an <EmailTemplate> element with a set of attributes and nested elements that specify the basic components of an email message, such as sender, subject, message body, etc.

These sections describe the attributes and nested elements.

- Email Template Attributes
- EmailTemplate Nested Elements

Email Template Attributes

The following lists the components that are generally expressed as attributes on the Email Template.

Example:

```
<EmailTemplate name="Work Item Reminder" cc="$identity.Manager.email" >
<From>administrator@XYZCorp.com</From>
<Body>
```

```
....
```

name

Short but descriptive name for template that uniquely identifies email template

cc, bcc

> Note: The **to** attribute is not specified in the email template because it is determined programmatically as the email is sent and would be overridden

Carbon Copy and Blind Carbon Copy recipients for the email

from

Sender email address. If this entry is not specified in template, the default sender specified on the **Global Settings > IdentityIQ Configuration > Notification Settings > Default From Address** is used.

Apache Velocity Engine

IdentityIQ email templates are processed through an open-source engine called Apache Velocity. Velocity is a Java-based template engine that allows web page designers to reference methods defined in Java code. IdentityIQ email templates make use of the Velocity Template Language to dynamically specify the email messages' contents and generate custom email messages specific to the recipient, work item, and action involved.

The Velocity Template Language (VTL) is a fairly simple to use. Highlights are included below, and full documentation on the syntax is available in the Apache Velocity User Guide or Reference Guide.

References

Directives (Commands)

VTL vs. $(variableName) Notation

References

As IdentityIQ prepares to send an email notification, the appropriate email template is loaded and its argument variables are passed into the VelocityContext where they can be accessed through VTL reference syntax. The contents of different variable types can be accessed through the syntax described in below.

Variables

$identityName${identityName}$!identityName

These three syntaxes are generally interchangeable in VTL. Shorthand notation (the first example) is the most commonly used, but each of the other two is required in special cases. Refer to the Velocity User Guide for more information.

Hash table values

$customer.Address

Returns the value corresponding to the Address key in a customer hash table

Object properties

$identity.DisplayName

Invokes the getDisplayName() method on the identity object

> Note: Property notation resolves to the getter method corresponding to the property name, not to an instance variable.Nested object properties can also be retrieved with this notation.
> **Example:** $item.Certification.Name invokes the getName() method on the Certification object retrieved through the getCertification() method on the item object

Object methods

$identity.getBundles($application)$identity.hasRole($role,'true')

Used for all non-getter methods and for any methods that require arguments

Directives (Commands)

These are the key commands of the Velocity Template Language that are most frequently used in IdentityIQ email templates to dynamically determine the text that is printed in each email message.

#If… #elseif… #else… #end

Conditional evaluation

```
#if($requester) requested by $requester.displayableName. #{end}
```

#foreach… #end

Loop through a list of objects

```
#foreach ($attrReq in $acctReq.attributeRequests) Operation: $attrReq.operation
Attribute:$attrReq.name Value(s): $attrReq.value#end
```

#set

Establish the value of a reference

```
 #set ($identityName = "John.Smith")#set ($book.Title = "War and Peace")
```

Refer to the Velocity User Guide for additional information on the language, including the syntax for less commonly used directives.

VTL vs. $(variableName) Notation

The VTL reference syntax must not be confused with the $(variableName) notation used for variable referencing in other IdentityIQ XML objects, such as Workflows. Velocity does not recognize this syntax and is unable to parse text that uses it. When IdentityIQ detects this syntax in any element of an email template, that portion of the message is not passed to Velocity for rendering at all. Instead, its contents are rendered by a simpler mechanism that is capable of doing the variable substitution based on the template's arguments. However, none of the Velocity directives are interpreted. Any Velocity commands included in the same element with a variable that uses the $(variableName) notation is treated as normal text and printed as-is in the final message.

Incorporating VTL in Email Template XML

All input arguments in the template signature are automatically loaded into the VelocityContext and are therefore accessible through the VTL reference notation for inclusion in the message text. Additionally, Velocity commands can be used in determining the text to print in the messages. Excerpts from the default email templates in IdentityIQ are used as examples throughout the rest of this section to illustrate how reference variables and various command syntaxes can be used.

Where to Use VTL

The Velocity Template Language syntax can be specified in any attribute or element that is used to build the email message. Most commonly, this means the <Subject> and <Body> elements of the message, but the cc and bcc recipients (as well as the from email address) are often dynamically specified through reference variables as well.

Reference Variables

> Note: For HTML contained within variables, refer to HTML Escaping.

When a variable name is referenced within the text for any of the message elements, its value is substituted into the text in its place.

Example:

```
<Body>$certifierName has accepted the challenge for '$challengeItem' and will change the
decision.
</Body>
```

Variable substitution results in the email message content:

John Smith has accepted the challenge for 'Entitlements on Financials' and will change the decision. Velocity can also access data values in fields within objects passed as arguments and replace the variable notation with those values. Consider the <subject> and <body> elements shown below. The argument list for this email template includes a Certification object (named certification) and an Identity object (named certifier).

```
<Subject>$certification.name requires approval</Subject>
<Body>$certification.name was signed by $certifier.displayableName and requires your
approval.
Login and view your work item inbox to complete this request.
</Body>
```

To resolve these variable references, Velocity calls the getName() method on the certification object and the getDisplayableName() method on the certifier's identity object. When the substitutions are made, the final email message looks like this:

Subject: Manager Access Review for Catherine Simmons requires approval

Manager Access Review for Catherine Simmons was signed by Catherine Simmons and requires your approval.

Login and view your work item inbox to complete this request.

Any attribute or method on any of a template's input arguments can be accessed through the reference variables.

Extended attributes on IdentityIQ objects can be accessed through the attributes hash map or by providing the attribute name as an argument to the appropriate getter method. Identity extended attributes, for example, are accessible through the Identity's attributes hash map or through the getAttribute() method on the Identity object (e.g. $certifier.attributes.region and $certifier.getAttribute("region") both return the value in the "region" extended attribute).

> Note: The list of available methods for IdentityIQ objects (Identity, Certification, ProvisioningPlan, etc.) can be found in the SailPoint JavaDocs that ship with the IdentityIQ product. These can be viewed through a browser at URL: [IdentityIQ base URL]/doc/javadoc/.

HTML Escaping

> Note: HTML escaping is applied to HTML that is passed into a HTML email template using a variable.

HTML escaping, or encoding, is the process of replacing any HTML reserved characters in a string, such as < or >, with their non-interpretable HTML entity representation. This is done to prevent unvalidated data from being included in a template and distributed through an email.

For example this:

```
<a href=”http://www.sailpoint.com” onclick=”steal_passwords();return false”>Click here to approve</a>
```

is transformed into this when HTML-escaped :

```
&lt;a href=&rdquo;http://www.sailpoint.com&rdquo;onclick=&rdquo;steal_passwords();return false&rdquo;&gt;Click here to approve&lt;/a&gt;
```

HTML content that is part of the template body itself is not escaped, it is rendered by any HTML email client correctly.

For security reasons, all HTML strings passed into a HTML email template using variables have their HTML escaped.

Re-factoring HTML Email Templates

If you have already defined email templates to use HTML supplied by variables, they must be re-factored so that all HMTL is contained within the email template itself.

For example if you have the following email template:

```
<html>
<body>
$header

You have a pending work item that requires attention. Work Item: $workItemDescription

--------------------------------------------------------------------------------
$!comment
</body>
</html>
```

Where the `$header` is a variable containing HTML, such as `<h2>Hello, $identityname</h2>`, the HTML part of the string needs to be moved directly into the email template.

For example:

```
<html>
<body>

<h2>Hello, $identityName</h2>

You have a pending work item that requires attention. Work Item: $workItemDescription

--------------------------------------------------------------------------------
$!comment
</body>
</html>
```

Where `$header` is an `$identityName` variable which contains only the name.

$(…) Variable Syntax

The `$(…)` variable syntax pre-dates the use of Velocity VTL templates. If you have templates that contain the `$(…)` variable syntax, two changes in IdentityIQ might affect you:

- HTML passed to a template using `$(…)` syntax is escaped just like VTL.
- VTL and the `$(…)` syntax can not co-exist in the same template. If the `$(…)` syntax is found anywhere in the template, the entire template string is passed to IdentityIQ's non-Velocity resolver and any VTL scripting code or velocity reference variables are not be processed. SailPoint-provided context variables are still resolved as expected.

For example, if your email template contains VTL as follows:

```
#if (
!$workItem.get("fromSource").equalsIgnoreCase("QuickLink"))
$workflow.get("launcherDisplayName")
#else
$(managerName)
#end
```

The VTL `if/else` statements is not processed because of the existence of `$(managerName)`, but instead rendered as literal strings.

In VTL, you should change any of the `$(variableName)` syntax to use the VTL `$variableName` syntax.

Conditional Statements

Conditional statements can be used to determine whether text should be included in the message or to choose alternate wording based on attribute values.

Whole paragraphs can be included or omitted based on conditional tests.

```
#if ($remindersRemaining > 0)
This work item will escalate after $remindersRemaining more reminder(s).
#end
```

Additionally, parts of a paragraph or sentence can be suppressed or altered based on conditional evaluations. In this example, if $requester is null, the portion of the text “requested by $requester.displayableName, and” is suppressed. Specifying the #if statement in-line with the rest of the text prevents extra line breaks in the middle of the sentence in the resulting email message.

```
<Body>This is your $ordinalNumReminders reminder that the work item $workItemName #if($re-
quester)requested by $requester.displayableName, and #{end}created on
…
```

Attribute values can also be evaluated to determine which of multiple text selections to include in a message:

```
#if ( $launcher != $identityName )
$launcher requested the following password changes be made to your account(s).
#else
The following password changes were made to your account(s) at your request.
#end
```

Method Calls

Methods within object arguments can be accessed directly through the method reference syntax.

```
#if($expiration)
#if($expiration.getTime() > $nowDate.getTime())
is due on $spTools.formatDate($expiration,3,1).
#{else}
was due on $spTools.formatDate($expiration,3,1).
#{end}
#{else}
was due on $spTools.formatDate($oldDueDate,3,1).
#{end}

#if ( $item.level )
           Priority: $item.level
#else
           Priority: Normal
#end
```

This block checks to see if $expiration is null. If it is not null, it prints “is due on…” or “was due on…” based on whether the expiration date/time is before or after the current date/time. If $expiration is null, this is an older expired work Item so the message uses the $oldDueDate field as work item due date in the message. It also checks to see if the priority was set in. If the $item.level is null, the priority is set to Normal.

Throughout this example, the printed date/time is formatted with the spTools.formatDate() method. The spTools reference variable is discussed in the next section.

> Note: This example was altered from its original format in the default Work Item Reminder email template. In the template, this #if statement was specified in-line to prevent unwanted line breaks in the message. Line breaks have been inserted here for readability and should not be included in the message body unless they are desired in the resulting message text.

SpTools Function Library

Immediately before any template is submitted for evaluation by the Velocity engine, the `spTools` argument is added to the VelocityContext so the template can access its methods. SpTools is a function library that contains a few localization utility methods to help with message formatting -- primarily date formatting. The methods available within spTools are listed below:

String formatDate(Object date)

Formats the passed-in date object to a string representation using the IIQ default date and time styles (both the java.util.dateformat SHORT formats), formatted per the norms of the server's default locale and timezone

String formatDate(Object date, Integer dateStyle, Integer timeStyle)

Formats the passed-in date object to a string representation using the specified date and time styles, formatted per the norms of the server's default locale and timezone

NOTE: The styles are represented by constant values:
SHORT = 3
MEDIUM = 2
LONG = 1
FULL = 0
dateStyle and timeStyle correspond to java.text.DateFormat constants. See the Sun Javadocs for details

String formatDate(Object date, String formatString)

Formats the date according to the specified formatString (uses the java.text.SimpleDateFormat method)

String getMessage(String key)

Returns an internationalized message from the message catalog corresponding to the provided key

String escapeHtml(String string)

Converts HTML special characters to their entity equivalents

Example:

```
escapeHtml('<div class="article">This is an article</div>')
```

Returns:

```
 &lt;div class="article"&gt;This is an article&lt;/div&gt;
```

In the out-of-the-box email templates, the most commonly used method from this library is the `formatDate()` method that takes a date object and two integers as arguments:

```
$spTools.formatDate($expiration,3,1)
```

After the reference shown above is resolved by Velocity, the date/time value in the expiration argument is printed in the email message in MM/dd/yy hh:mm:ssPM format (or the appropriate equivalent for the server's locale).

CDATA Blocks

When any component of the email message (body, subject, cc, etc.) contains characters that are illegal in XML text (e.g. characters like < and & that are interpreted by the parser as the start of an XML element or character entity, respectively), the entire component must be expressed in a CDATA block to prevent it from being parsed. For example, any message body written as HTML must be contained within a CDATA section.

```
<Body><![CDATA[
<html>
<body style="background:#FFF;margin:0;padding:0;text-align:left;">
<p style="margin:20px 0 0;padding:0;color:#333;font:bold 10pt
Arial;line-height:15pt;">$!{workItem.owner.firstname},</p>
<p style="margin:0 0 20px;padding:0;color:#333;font:normal 10pt
Arial;line-height:15pt;">As part of our periodic compliance efforts, you are
responsible for certifying the access your employees have to enterprise applications.
</p>
<p style="margin:0;padding:0;color:#333;font:normal 10pt Arial;line-height:15pt;">A
specific access certification is named <b>$!{workItemName}</b> has been created for
you, and is due on <strong>$spTools.formatDate(
$certification.expiration,3,3)</strong>. <a
href="http://localhost:8080/iiq/manage/certification/entityList.jsf?certificationId
=$!{certification.id}">Click here to get started on this task.</a></p>
</body>
</html>
]]> </Body>
```

The marked up text can then be passed to Velocity for variable substitution and can be rendered as an HTML email message.

Sending an Email from a Rule

Some installations may require notifications to be sent based on events that are not covered by the automated system notifications. Rules can often be used to drive these notifications. The example below shows how to send an email from a rule.

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE sailpoint PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<sailpoint>
<Rule language="beanshell" name="Test Email Sending" type="BuildMap">
  <Description>Debugging Tool - Sends a sample email out via the email serv-
er.</Description>
  <Signature returnType="Map">
    <Inputs>
      <Argument name="log">
        <Description>
          The log object associated with the SailPointContext.
        </Description>
      </Argument>
      <Argument name="context">
        <Description>
          A sailpoint.api.SailPointContext object that can be used to query the database
if necessary.
        </Description>
      </Argument>
    </Inputs>
   </Signature>
   <Source>
       // Library inclusions for BeanShell
import sailpoint.api.*;
import sailpoint.object.*;
import sailpoint.tools.*;

import java.util.*;
import java.lang.*;
import java.text.*;

// Point this to the "To" email address
String emailDest = "adam.hampton@example.com";

// Specify the email template name in tplName
String tplName = "SailPoint - Test Email Sending";
EmailTemplate template = context.getObjectByName(EmailTemplate.class, tplName);
if (null == template) {
   log.error("ERROR: could not find email template [ " + tplName + "]");
   return;
}
template = (EmailTemplate) template.deepCopy(context);
if (null == template) {
   log.error("ERROR: failed to deepCopy template [ " + tplName + "]");
   return;
}
Map args = new HashMap();
// Add all args needed by the template like this
args.put("testField1", "This is a test of template parameters.");

EmailOptions ops = new EmailOptions(emailDest, args);
context.sendEmailNotification(template, ops);

return;
```

```
 </Source>
 </Rule>
</sailpoint>
```

The BeanShell from this example rule can be used as a template for sending an email from any defined rule. Simply change the email template name, recipient, and template arguments to create the desired notification.

Using a Rule to Test Templates and Email Configuration

For an overview of developing and using rules in IdentityIQ, see the *IdentityIQ System Administration* guide.

Using a Rule to Test Templates and Email Configuration

This example rule can also be used to test the email server configuration or to test any email template. Complete these steps to use the rule for testing purposes:

> Note: To test email templates independently from the email server configuration without actually sending emails through the server, choose Email Notification Type: Redirect to File. This writes the email text to the specified file.

1. Set up an email server on **Gear icon > Global Settings > IdentityIQ Configuration > Notification Settings**.
2. Edit an email template to contain the desired message and import it.
3. Edit the “Test Email Sending” rule to include the desired “To” email address, email template, and arguments, and import the rule. (Rules are imported the same way as templates, as described in Importing Email Templates into IdentityIQ.)
4. Run the “Test Email Sending” rule from the IdentityIQ console to send the email.

   ```
   > rule “Test Email Sending”
   ```

5. Examine the resultant email (either in the recipient's inbox or the redirect email file) to verify that the message appears as expected.

For an overview of developing and using rules in IdentityIQ, see the *IdentityIQ System Administration* guide.

Data Encryption

Data encryptions is done using four basic concepts: the keystore, master password, encrypted data synchronization, and the keystore console.

- KeyStore — the location where the encryption keys used by IdentityIQ are persisted.
- Master Password — the entire keystore can be encrypted with an ascii password. This is the keystore or master password. You can change the keystore password using the keystore console command. Only one master password can exist. When the master password changes the entire keystore and master password file are re-encrypted and rewritten.
- Encryped Data Synchronization — the process of re-encrypting existing data with the newest key in the keystore.
- Keystore Console — the tool (spt keystore) used to manage the keystore and master password.

The keystore and master password are file based and secured by the file system. They are stored in two separate files. The files can be located in the IdentityIQ deployment directory or placed in an alternative directory during configuration. By default the files are stored in the following location:

```
keystorePassword = WEB-INF/classes/iiq.cfg
keystore = WEB-INF/classes/iiq.dat
```

An alternate keystore file location, password file, or just password in clear text can be specified in the `iiq.properties` file under these keys:

```
keyStore.file
keyStore.passwordFile
```

spt KeyStore Console Commands

Encrypted Data Synchronization

Using IdentityIQ KeyStore

spt KeyStore Console Commands

The **iiq keystore** command is the interface to update the keystore and keystore password. A master password can to be entered into the console or generated when it is being updated.

The keyStore console supports the following commands:

`use` *KeyStoreFilemasterFile*

> Note: If you do not call the use command, the changes are positioned in the configured paths.

Specify the keystore and master file to use when interacting with an alternate keystore.

The `keyStoreFile` argument in position 1 specifies the path to the file to be used when creating/updating the keystore. If this argument is not specified the command uses `$SPHOME/WEB-INF/classes/iiq.dat.`

The `masterFile` argument in position 2 specifies the path and filename used to store the master file.

The **use** command gives you the ability to build the keystores outside your operating running environment and merge them in when scheduled.

addKey [-q]

> If no argument is included, you are prompted for confirmation before the key is generated.

Generate a new encryption key, the key is securely generated and random.

`-q` as argument in position 1 generatesa new key without prompting for confirmation.

list

List the contents of the keystore.

master [newPasswordnewPasswordConfirmation]

> Note: Passwords must be at least 8 characters.

Change the master password and re-encrypt the keystore using the new password.

> Note: If no argument is included, you are prompted for confirmation.

If `newPassword` and `newPasswordConfirmation` are in argument position 1 and 2, you are not prompted for confirmation.

`-g` is in argument position 1 a new password is generated without confirmation.

about

Specifies the two files that being modified.

Encrypted Data Synchronization

The Encrypted Data Synchronization task goes over the objects re-encrypting the values using the newest key.

> Note: The Encrypted Data Synchronization task is not enabled upon installation, you must create the task from the New Task drop-down menu.

The task encrypts the following attributes/types by default:

- Application secret configuration attributes
- User passwords
- Password history
- Users challenge questions
- Activity/Target source configurations
- Integration configuration password attributes

In cases such as integration configuration and unstructured target sources the task looks for encrypted values with the password in the name. You can also add a configuration attribute, `IIQSecretAttributes`, to either type names to define which attributes are targeted during a re-synchronization.

```
<entry key="IIQSecretAttributes">
 <value>
 <List>
 <String>mySecret1</String>
 <String>mySecret2</String>
 <String>password</String>
 </List>
 </value>
 </entry>
```

The task enables you do disable the following three categories of objects:

- Applications — which enabled application, activity and target source updates
- Identity
- Integration configuration

Using IdentityIQ KeyStore

> Note: Make sure to store copies of the iiq.dat and iiq.cfg files in a safe place. When you upgrade or reinstall IdentityIQ, the files are readily available to be restored.

> Note: Make sure that the file permissions are set to allow access only by the application server that runs IdentityIQ.

In a standard installation of IdentityIQ, passwords are all encrypted using the same encryption secret. Encrypted passwords used in one installation can be reused (decrypted) by any other installation ofIdentityIQ. The keystore feature enables the use of a site specific key. With the keystore feature enabled, a password used on one site cannot be decrypted on another site without having the site specific encryption keys.

Configuration

The keystore is stored in `WEB-INF/classes/iiq.dat` with an accompanying configuration file `WEB-INF/-classes/iiq.cfg`.

The `iiq.properties` file provides two options to specify an alternative location for `iiq.dat` and `iiq.cfg`. In the default `iiq.properties`, these options (`keyStore.file` and `keyStore.passwordFile`) are commented out.

```
# IIQ Keystore and Master Password properties
#

# file location of the IIQ keystore
# (override of the default $SPHOME/WEB-INF/classes/iiq.dat )
#
#keyStore.file = /example/path/filename

# file location of the IIQ master password file
# (override of the default $SPHOME/WEB-INF/classes/iiq.cfg )
#
#keyStore.passwordFile = /example/path/filename
```

To put the files in an alternative location, for example `/etc/identityiq`, enable and change these options as follows.

> You may need to modify your application server or Java sandbox security settings to allow access to the key files outside the application server installation directories.

```
# IIQ Keystore and Master Password properties
#

# file location of the IIQ keystore
# (override of the default $SPHOME/WEB-INF/classes/iiq.dat )
```

```
#
 keyStore.file = /etc/access governance suite/iiq.dat

# file location of the IIQ master password file
# (override of the default $SPHOME/WEB-INF/classes/iiq.cfg )
#
 keyStore.passwordFile = /etc/access governance suite/iiq.cfg
```

Key Creation

To create or manage the keystore: navigate to the `WEB-INF/bin` folder and start the IdentityIQ KeyStore console with the **keystore** command:

1. Navigate to the `WEB-INF/bin` folder and start the IdentityIQ Keystore console with the keystore command.

   ```
   iiq keystore
   ```

2. The console displays a prompt similar to the IdentityIQ console. Use the **help** to list all accepted KeyStore Console commands. For example, use the **addKey** command to create a new key and the **list** command to view the contents of the keystore.

   ```
   > addKey
   Generate a new encryption key (y/n)?
   y
   Generating a new encryption key for keystore
   [/var/tomcat/webapps/identityiq/WEB-INF/classes/spt.dat].
   New encrpytion key successfully saved to keystore.
   All application servers must be restarted for changes to take effect.
   >
   ```

   > Note: If the keystore file does not exist, it is created and a new, randomly generated key is added.

3. The **list** command displays the newly created key:

   ```
   > list
   Listing contents for keystore
   [/var/tomcat/webapps/iiq6/WEB-INF/classes/iiq.dat].
   KeyAlias Algorithm Format Object

   2 AES RAW javax.crypto.spec.SecretKeySpec@fffe81cd
   >
   ```

4. Use the **exit** command to leave the console.

5. Restart your application server.
   After you restart the application server, any newly set password is encrypted using the new encryption key.

Without the files `iiq.dat` and `iiq.cfg`, passwords cannot be decrypted by IdentityIQ.
If you run more than one instance of `IdentityIQ`, you must place the following files in the `WEB-INF/-classes` folder of each instance, or in the location specified in `iiq.properties`.

Re-Encrypt Passwords

The new encryption key is used for newly encrypted passwords. However, because existing passwords can also be decrypted using the default method on any system, you must re-encrypt existing passwords. Ro re-encrypt existing password, you must create a new Encrypted Data Synchronization Task in IdentityIQ.

1. From the Navigation menu bar, select **Intelligence -> Tasks**.
2. From the **New Task** drop-down list select **Encrypted Data Synchronization Task** from the drop-down list.
3. Enter a name for the new task.
4. OPTIONAL: If needed, you can exclude types such as applications, identities or integration configurations from processing.
5. **Save and Execute** to immediately run the task.

After the task has completed, all selected encrypted data is changed. A password encrypted with the default key is pre-fixed with 1. Items encrypted with the new encryption key are prefixed with 2 or another number if multiple encryption keys are stored.

For example, when you look up the Administrator's password in the console, the displays is similar to the following:

```
> search identity password where name admin
2:WpTZ2hmNaInTAJzeK9Swcw==
```

Using the Different Encryption Keys

After a new key is added to the keystore, the key is used as the default encryption key. Everything encrypted inside IdentityIQ then uses the new key. For example:

```
$ ./iiq console
> encrypt test
2:bt7YJA6iovzF5Uu6RIjueg==
>
```

There is one exception. The command **iiq encrypt**, continues to use the original default encryption key:

```
$ ./iiq encrypt test
1:8zJwAXqvK5/b92JbPXLLKw==
$
```

Although the syntax reported by the bare command does not indicates this, the command accepts an extra parameter to select the encryption key to use. For example:

```
iiq encrypt string [key]
```

> Note: The encrypt command in the iiq console does NOT accept this extra parameter.

The *key* is the number that displays in the list command and used as prefix for the keys.

- To select the newly created key, use 2. If multiple keys are in the keystore, use any available higher number.
- To select the original default key use 1 or nothing.

For example:

```
$ ./iiq encrypt test 1
1:8zJwAXqvK5/b92JbPXLLKw==
$ ./iiq encrypt test 2
2:bt7YJA6iovzF5Uu6RIjueg==
```