



IdentityIQ Rapid Setup

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

“SailPoint Technologies,” (design and word mark), “SailPoint,” (design and word mark), “Identity IQ,” “IdentityNow,” “SecurityIQ,” “Identity AI,” “Identity Cube,” and “SailPoint Predictive Identity” are registered trademarks of SailPoint Technologies, Inc. “Identity is Everything,” “The Power of Identity,” and “Identity University” are trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind regarding these materials or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

- About Rapid Setup 1**
 - Rapid Setup Joiner Overview 1
 - Rapid Setup Mover Overview 2
 - Rapid Setup Leaver Overview 3
- Rapid Setup Configuration 5**
 - General Information for Rapid Setup Configuration 5
 - Prerequisites for Configuring and Using Rapid Setup 6
 - Joiner Configuration 6
 - Mover Configuration 8
 - Leaver Configuration 10
 - Identity Operations Configuration 12
 - Miscellaneous Configuration 13
 - Defining Trigger Filters 15
 - Using Identity Processing Thresholds for Error Prevention 17
- Using Rapid Setup 18**
 - Aggregation in Rapid Setup 19
 - Joiner Processing in Rapid Setup 21
 - Mover Processing in Rapid Setup 23
 - Leaver Processing in Rapid Setup 23
- Terminating Identities with Rapid Setup 26**
- Rapid Setup Troubleshooting 27**

About Rapid Setup

Rapid Setup is a business-user-friendly interface that offers a streamlined way to onboard applications and handle common identity management scenarios such as joiner, mover, leaver, and terminating identities. It provides pre-configured processes that follow best practices for managing identities.

Rapid Setup lets you separate the technical and IT-centric steps of onboarding and configuring applications (such as defining connection parameters and schemas) from the business-centric steps of defining the business processes the application should follow. Rapid Setup removes the complexity of implementation by providing a guided experience for non-technical users.

Rapid Setup does not **replace** existing IdentityIQ functions for onboarding applications and managing identities. Instead, it provides an alternative way of defining application behavior and the events and processes for managing identities, in a configurable and guided way, and in a single, centralized UI.

Some of Rapid Setup's behavior and options are set **globally** and will apply to all applications that are onboarded with Rapid Setup. Other options can be set **at the application level**, so that you can customize processes for each application.

Applications that you want to onboard with Rapid Setup must have connection parameters and schemas already defined. To make application onboarding easier for your business users, it is helpful to also pre-define elements such as email templates, business processes, any rules you may want to use, and other event-specific drivers of identity processing. For more details, see [Prerequisites for Configuring and Using Rapid Setup](#).

For more overview information see:

- [Rapid Setup Joiner Overview](#)
- [Rapid Setup Mover Overview](#)
- [Rapid Setup Leaver Overview](#)

For information on configuring Rapid Setup's global options, see [Rapid Setup Configuration](#).

Rapid Setup comes included in Lifecycle Manager and does not need to be installed separately.

Rapid Setup Joiner Overview

The Joiner process defines the operations that are run when a new user joins your organization.

These can include:

- Building a provisioning plan which includes:
 - Assigning birthright roles. Birthright roles are any business roles that all employees have simply because they are employees, The Rapid Setup Joiner process uses assignment rules to determine how these roles are assigned to identities.
 - Creating a new account on each application that has account-only provisioning enabled (if no account exists yet). Account-only provisioning is used when there are no roles or entitlements that require the creation of accounts, but you want an empty account created on the application for the user anyway. Account-only creation will occur only if the identity meets the creation criteria that is configured in the Joiner process for that application.
- Executing the provisioning plan. The provisioning business process for Joiners is configured at a global level for Rapid Setup. See [Rapid Setup Configuration](#).
- Notifying the manager with results of provisioning.
- Optionally, notifying the manager when a temporary password is generated.
- Running an optional post-joiner rule.

The Joiner process must be enabled globally before users can configure and use it on a per-application basis. See [Rapid Setup Configuration](#) for details about global configuration.

Rapid Setup Mover Overview

The Mover process defines the operations that are launched when an identity moves within your organization. What constitutes a "move" can be defined according to your organization's needs, in the global settings for Rapid Setup. Some common examples of moves are change of manager and change of location.

Mover processes can include:

- Generating a certification for the identity that is moving, before mover processing begins. Settings at the application level can determine whether or not to certify additional entitlements. A global setting can be configured to bypass certifications during mover processing.
- Perform a joiner-type provisioning on the moving identity. When joiner processing is enabled, birthright roles will always be assigned or removed as appropriate. Settings at the application level can determine whether or not to perform account-only provisioning during mover processing. Global settings can be configured to bypass joiner-type provisioning.
- Running an optional post-mover rule.

The Mover process must be enabled globally before users can configure and use it on a per-application basis. See [Rapid Setup Configuration](#) for details about global configuration.

Rapid Setup Leaver Overview

The Leaver process defines the operations that are launched when someone leaves your organization. The criteria for how "leaving" is defined is configured according to your organization's needs, in Rapid Setup's global configuration.

Leaver processes can include:

- Reassigning ownership of artifacts (such as tasks, applications, and policies) currently owned by the leaving identity.
- Notifying the manager of the leaving identity about reassigned artifacts.
- Reassigning the administration of identities that are currently administered by the leaving identity. This option is typically used for service account or RPA type identities that the leaver is responsible for administering.
- Notifying the manager of the leaving identity about the reassigned identities.
- Auto-rejecting requests targeted for the leaving identity.
- Running an optional post-leaver rule.
- Updating links which may need updating due to a move.

The Leaver process can build an immediate provisioning plan to:

- Remove of the identity's assigned roles
- For each application on which identity has an account, and for which Leaver processing is enabled, determine which of these actions to perform, and whether to perform each one immediately or to defer the action:
 - Removal of the identity's entitlements (unless they are excluded from removal).
 - Scrambling the identity's password on the application.
 - Adding a comment to an account attribute.
 - Moving the account to a different OU on a container-based application.

- Disabling the account.
- Deleting the account.
- Execute the immediate provisioning plan.
- Notify the manager with results of the immediate provisioning.

The Leaver process must be enabled globally before users can configure and use it on a per-application basis. See [Rapid Setup Configuration](#) for details about global configuration.

You can also define processes for the **immediate termination** of identities, that can be distinct from your other leaver processes. Some of the termination behavior is configured globally as part of [Identity Operations Configuration](#); you can also define application-specific termination behavior as part of leaver processing.

Rapid Setup Configuration

Use the Rapid Setup configuration to set global options for Rapid Setup. Rapid Setup global configuration is accessed through the **Gear Icon > Global Settings > Rapid Setup Configuration**.

Configuring Rapid Setup includes defining:

- which processes are enabled system-wide
- how identities are selected for joiner, mover, and leaver processes
- which business processes to use for the joiner, mover, and leaver processes
- whether to use rules as part of processing identities, and which rules to use
- the email templates to use for notifying managers or workgroups about processing events
- other options that are specific to the various processes.

Each process is enabled and configured on its own tab:

- [Joiner Configuration](#)
- [Mover Configuration](#)
- [Leaver Configuration](#)
- [Identity Operations Configuration](#) - this is where options for immediate termination are configured. See [Terminating Identities with Rapid Setup](#) for more information.
- [Miscellaneous Configuration](#) - options for business processes and email message formatting and delivery

General Information for Rapid Setup Configuration

- Red asterisks indicate required fields or options.
- Be sure to save your changes as you configure each process. A solid dot on a tab title indicates that changes were made on the current tab and have not been saved. When you save your changes, a checkmark appears on the dot, to indicate that changes have been saved.

Prerequisites for Configuring and Using Rapid Setup

Rapid Setup is included with the Lifecycle Manager component of IdentityIQ. Its features are activated as part of activating Lifecycle Manager. See the **Lifecycle Manager Activation** guide for more information.

Rapid Setup can be used with applications that have basic connection and schema parameters already defined. These are set in the application definition (**Applications > Application Definition**), on the application's **Configuration** tab. For more details, see the **Application Configuration** documentation.

Rapid Setup administrators and users can choose drivers of application behavior such as rules, email templates, provisioning policies, business processes, roles, and populations, as part of onboarding an application. Rapid Setup provides some out-of-the-box business processes and email templates that are designed for use with Rapid Setup, but your organization can define any of these items according to your own requirements.

Although it is not a requirement to have all these artifacts developed before implementing Rapid Setup, it will speed up the implementation process and make Rapid Setup easier and more powerful for your business users to work with if they are already defined.

Sample Rules for Rapid Setup

Rapid Setup can use BeanShell rules to provide custom business logic. Joiner, mover, leaver, and aggregation operations can all use rules to drive specific behavior.

A set of sample rules is provided with Rapid Setup. You can use these sample rules as templates for developing your own Rapid Setup rules. The sample rules file, `rsexamplerules.xml`, is located in the `\WEB-INF\config\rapidsetup` directory of your IdentityIQ installation.

Joiner Configuration

The Joiner process defines the operations that are run when a new user joins your organization.

Move the slider to enable **Joiner Processing**. Then configure global behavior for joiner processing.

Note: See [Sample Rules for Rapid Setup](#) for information about sample rules included with Rapid Setup.

Option	Description
Generate Approvals	Enable this option if the joiner process should include approvals. The approval path is defined in the Joiner Business Process you specify below. Note that the default RapidSetup - Joiner business process delegates approvals to the LCM Provisioning business process.
Automatically	Enable this option to include new identities that have no accounts in joiner pro-

Option	Description
Join New Empty Identities	<p>cessing. When this option is enabled, any Trigger Filters you set below for selecting identities are bypassed for new identities.</p> <p>See Defining Trigger Filters for more information.</p>
Exclude Uncorrelated Identities	<p>Exclude uncorrelated identities from joiner processing. A <i>correlated</i> identity is an identity that has an account on an authoritative application.</p>
Alternative Workgroup for Joiner Completed Notification Email	<p>If you want to send email notifications to a workgroup rather than the manager of the joining identity, choose the workgroup here.</p> <p>The workgroup you choose here will also be the recipient of the Temporary Password email, if you opt to send one.</p>
Joiner Completed Notification Email Template	<p>Choose an email template to use for notification emails.</p> <p>For more information on email templates, see the System Configuration documentation.</p>
Send Temporary Password Email	<p>Enable this option to send an email notification with temporary password info to whoever is responsible for managing the new identity's access.</p> <p>By default this is the identity's manager, but if you choose an Alternative Workgroup (above) for notification emails, the email will go to that group.</p> <p>If neither a manager or an alternative workgroup is defined for an identity, this email will go to a workgroup that is responsible for identities with no manager. You can choose a "no manager" workgroup specifically for Rapid Setup operations in Miscellaneous Configuration.</p>
Post Joiner Rule	<p>Rules can drive custom actions outside of the standard joiner processes. If you want to run a rule as the final step of the joiner process, choose the rule here. Rules of type <code>PostLifecycle</code> are available to select for this option.</p>
Threshold Type	<p>Identity Processing Thresholds stop lifecycle events before they are fully processed, in case of accidentally-triggered workflows. To enable an Identity Processing Threshold, choose from Fixed or Percentage.</p> <p>For more information, see Using Identity Processing Thresholds for Error Prevention.</p>
Threshold	<p>Enter a value to use in conjunction with the Threshold Type, for Identity Processing Thresholds.</p>
Joiner Business	<p>Choose a business process for the joiner processing.</p>

Option	Description
Process	
Trigger Filters	<p>You can set a Trigger Filter to identify which identities are considered joiners if you have a specific attribute (or set of attributes) that identify new identities in your system. If not, use the Automatically Join New Empty Identities option to run joiner processing on all new identities.</p> <p>See Defining Trigger Filters for more information.</p>

Mover Configuration

The Mover process defines the operations that are launched when an identity moves within your organization.

Move the slider to enable **Mover Processing**. Then configure global behavior for mover processing.

Note: see [Sample Rules for Rapid Setup](#) for information about sample rules included with Rapid Setup.

Option	Description
Generate Approvals	<p>Enable this option if the mover process should include approvals. The approval path is defined in the Mover Business Process you specify below.</p> <p>Note that the default RapidSetup - Mover business process delegates approvals to the LCM Provisioning business process.</p>
Exclude Uncorrelated Identities	<p>Exclude uncorrelated identities from mover processing. A <i>correlated</i> identity is an identity that has an account on an authoritative application.</p>
Launch a Targeted Certification	<p>Launch a targeted certification campaign as part of mover processing. By default, the approver for this certification is the identity's manager; in cases where the move results in a change of manager for the identity, the new manager is the approver. You can add the identity's current (that is, pre-move) manager to the approval process by enabling the Include Previous Manager as a Certifier option, below.</p> <p>If you are enabling joiner processing as part of the mover process, this certification campaign must reach completion before joiner processing will begin.</p>
Stage the Certification	<p>Staging is an optional phase you can use to test or validate a certification before sending it to reviewers.</p> <p>See the Phases of a Certification information in the Certifications and</p>

Option	Description
	Access Reviews documentation for more information.
Include Birthright Roles	Include any birthright roles that were previously assigned to this user in the certification.
Certification Owner	The identity or group responsible for the certification campaign.
Backup Certifier	The identity or workgroup that will be responsible for access reviews, if the primary certifier is unable to certify or cannot be identified.
Include Previous Manager as a Certifier	If the move includes a change of manager, add the identity's previous manager as an additional approver in the certification process.
Joiner Processing	Run the joiner process as part of mover processing, in order to perform basic access assignment such as the addition or removal of birthright roles and, if enabled at the application level, performing account-only provisioning if no account exists for the identity.
Post Mover Rule	Rules can drive custom actions outside of the standard mover processes. If you want to run a rule as the final step of the mover process, choose the rule here. Rules of type <code>PostLifecycle</code> are available to select for this option.
Threshold Type	Identity Processing Thresholds stop lifecycle events before they are fully processed, in case of accidentally-triggered workflows. To enable an Identity Processing Threshold, choose from Fixed or Percentage . For more information, see Using Identity Processing Thresholds for Error Prevention .
Threshold	Enter a value to use in conjunction with the Threshold Type, for Identity Processing Thresholds.
Mover Business Process	Choose the business process for mover processing.
Trigger Filter	Trigger filters define what is considered a "mover" in your organization. For example, if a change to an identity's manager should trigger mover processing, you can set a Trigger Filter using the "Manager" attribute with the operator "Changed" to select identities. You can use attributes, populations, or a combination of both to define your moving identities. You can use "And" and "Or" conditions for filtering, and the gear icon to the right of your criteria lets you move, duplicate, or delete rows. For more information, see Defining Trigger Filters .

Leaver Configuration

The Leaver process defines the operations that are launched when someone leaves your organization.

Move the slider to enable **Leaver Processing**. Then configure global behavior for leaver processing.

Note: see [Sample Rules for Rapid Setup](#) for information about sample rules included with Rapid Setup.

Option	Description
Generate Approvals	Enable this option if the leaver process should include approvals. The approval path is defined in the Leaver Business Process you specify below. Note that the default RapidSetup - Leaver business process delegates approvals to the LCM Provisioning business process.
Exclude Uncorrelated Identities	Exclude uncorrelated identities from joiner processing. A <i>correlated</i> identity is an identity that has an account on an authoritative application.
Remove Assigned Roles	Remove assigned roles from an identity during leaver processing.
Reassign Artifacts	Reassign objects, such as applications, workgroups, or policies, that are owned by a leaving user.
Reassignment Artifacts Types	Choose which types of object should be reassigned, if the current owner is the leaving identity.
Reassign Artifacts to Manager	Reassign the objects selected above to the manager of the leaving identity.
Reassign Artifacts Rule	Handle reassignment of object using a rule. If the Reassign Artifacts to Manager option is also enabled, the leaver process will first attempt to assign objects to the manager, then will use the rule chosen here, if no manager can be determined.
Reassign Artifacts Alternate	Reassign objects to this identity if none were discovered for manager or by the reassignment rule.
Reassign Identities	If the leaving identity is the owner or administrator of other identities, such as service accounts or RPA/bot identities, enable this option to reassign those identities to another identity or workgroup.
Reassign Identities to Manager	Reassign the identities to the manager of the leaving identity.

Option	Description
Reassign Identities Rule	Handle reassignment of managed identities using this rule, if a manager cannot be determined, or if the Reassign Identities to Manager option is not enabled.
Reassign Identities Alternate	Reassign managed identities to this identity, if no identity was discovered as a manager or by the reassignment rule.
Send Leaver Notification to this Workgroup	Select a workgroup to receive leaver notification emails, rather than a manager.
Ownership Reassignment Notification Email Template	Email template to compose the email notification regarding reassignments (used for both artifact and identity reassignment). For more information on email templates, see the System Configuration documentation.
Leaver Completed Notification Email Template	The template to use for notification emails. For more information on email templates, see the System Configuration documentation.
Post Leaver Rule	Rules can drive custom actions outside of the standard leaver processes. If you want to run a rule as the final step of the leaver process, choose the rule here. Rules of type <code>LeaverReassignment</code> are available to select here.
Threshold Type	Identity Processing Thresholds stop lifecycle events before they are fully processed, in case of accidentally-triggered workflows, To enable an Identity Processing Threshold, choose from Fixed or Percentage . For more information, see Using Identity Processing Thresholds for Error Prevention .
Threshold	Enter a value to use in conjunction with the Threshold Type, for Identity Processing Thresholds.
Leaver Business Process	Choose the business process for leaver processing.
Trigger Filter	Trigger filters define what is considered a "leaver" in your organization. For example, if change in an identity's status from "active" to "inactive" should trigger leaver processing, you can set a Trigger Filter using the "Inactive" attribute with the operator "Changed To" set to a value of "True" to select leaver identities. You can use attributes, populations, or a combination of both to define your

Option	Description
	<p>leaving identities. You can use "And" and "Or" conditions for filtering, and the gear icon to the right of your criteria lets you move, duplicate, or delete rows.</p> <p>For more information, see Defining Trigger Filters.</p>

Identity Operations Configuration

The Identity Operations process defines how to process operations such as immediate termination.

Move the slider to enable **Terminate Processing**. Then configure global behavior for termination processing.

Options	Description
Generate Approvals	<p>Enable this option if the terminate process should include approvals. The approval path is defined in the Terminate Business Process you specify below.</p> <p>Note that the default RapidSetup - Leaver business process delegates approvals to the LCM Provisioning business process.</p>
Remove Assigned Roles	Remove assigned roles from an identity during terminate processing.
Reassign Artifacts	Reassign objects, such as applications, workgroups, or policies, that are owned by a terminated user.
Reassignment Artifacts Types	Choose which types of object should be reassigned, if the current owner is the terminated identity.
Reassign Artifacts to Manager	Reassign the objects selected above to the manager of the terminated identity.
Reassign Artifacts Rule	Handle reassignment of object using a rule. If the Reassign Artifacts to Manager option is also enabled, the terminate process will first attempt to assign objects to the manager, then will use the rule chosen here, if no manager can be determined.
Reassign Artifacts Alternative	Reassign objects to this identity, if no identity was discovered as a manager or by the reassignment rule.
Reassign Identities	If the terminated identity is the owner or administrator of other identities, such as service accounts or RPA/bot identities, enable this option to reassign those identities to another identity or workgroup.
Reassign Identities to Manager	Reassign the identities to the manager of the terminated identity.

Options	Description
ager	
Reassign Identities Rule	Handle reassignment of managed identities using this rule.
Reassign Identities Alternative	Handle reassignment of managed identities using this rule, if a manager cannot be determined, or if the Reassign Identities to Manager option is not enabled.
Send Terminate Notification to this Workgroup	Select a workgroup to receive termination notification emails, rather than a manager.
Ownership Reassignment Notification Email Template	Email template for the email notification regarding reassignments of artifacts and identities. For more information on email templates, see the System Configuration documentation.
Terminate Completed Notification Email Template	The template to use for notification emails. For more information on email templates, see the System Configuration documentation.
Post Terminate Rule	Rules can drive custom actions outside of the standard terminate processes. If you want to run a rule as the final step of the terminate process, choose the rule here. Rules of type <code>LeaverReassignment</code> are available to select here.
Terminate Business Process	Choose the business process for termination processing.

Miscellaneous Configuration

Use the **Miscellaneous** tab to configure Rapid Setup options for business processes and email message formatting and delivery.

Identity Selection	Description
Business Process Requester	Select an identity to use as the requester for RapidSetup lifecycle business processes. This is the workgroup or identity who is responsible for the overall Rapid Setup processes and is used primarily for informational and auditing purposes.
Alternative Workgroup	Select a workgroup to receive notification emails in cases where an identity does not have a manager.

Identity Selection	Description
for Rapid Setup Notification	<p>The default workgroup, RapidSetup No Manager, is an empty workgroup. You can add people to this workgroup, or select a different one.</p> <p>For information on how to add people to a workgroup, see the Role, Group, and Population Management documentation.</p>
Workgroup to Receive Error Notifications Email	<p>Select a workgroup to be notified of Rapid Setup errors by email. The default group, Rapid Setup Error Notification, is an empty workgroup. You can add people to this workgroup, or select a different one.</p> <p>For information on how to add people to a workgroup, see the Role, Group, and Population Management documentation.</p>
Notification Style Sheet Email Template	<p>Select a style sheet for notification emails.</p> <p>Style sheets can be edited in the Debug pages.</p>
Notification Header Email Template	<p>Select a template to use for the header of notification emails.</p> <p>Style sheets can be edited in the Debug pages.</p>
Notification Footer Email Template	<p>Select a template to use for the footer of notification emails.</p> <p>Style sheets can be edited in the Debug pages.</p>
Role Types to Treat as Rapid Setup Birthright Roles	<p>Rapid Setup lets you use a specific role type to identify birthright roles. Roles designated as birthrights are automatically assigned, through Rapid Setup joiner and mover processes, to identities that match the trigger criteria in the joiner and mover processes.</p> <p>IdentityIQ provides a default role type, <code>rapidSetupBirthright</code>, to identify these roles.</p> <p>A role's type is set in the Role Editor (under the Setup > Roles menu). To designate a role as a Rapid Setup birthright role, set the role's type to the type you have chosen here. You can edit existing roles to change their type to birthright, but if you are working with an established role model, it is a good practice to create new roles to handle birthright access.</p> <p>For information on editing a role's type, see the Role, Group, and Population Management documentation.</p>

Defining Trigger Filters

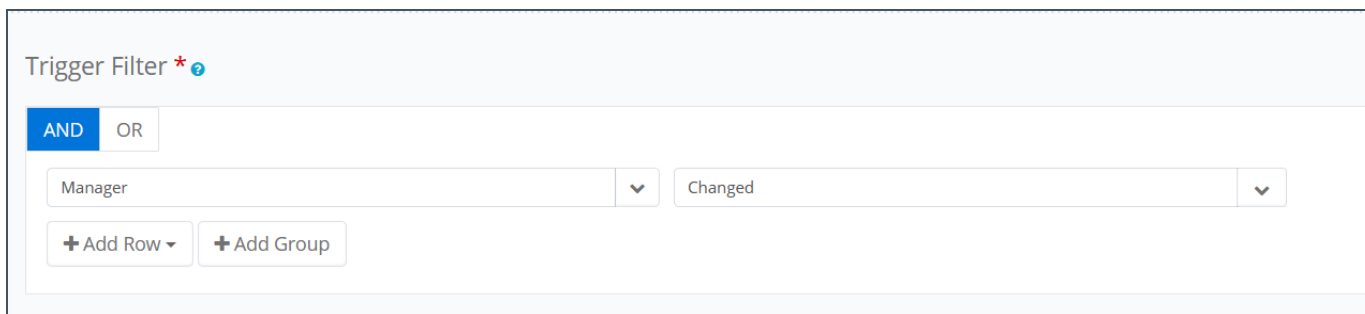
Trigger filters are the core of what drives joiner, mover, and leaver processes within Rapid Setup. Trigger filters are the constraint logic that determines which identities are subject to joiner, mover, and leaver business processes. Trigger filters use identity attributes or populations, coupled with operators and values, to choose identities to act on.

Important: These filters are called "trigger" filters because they define what should trigger each process. When setting up a trigger filter for movers or leavers, it's important to include criteria that identifies a **change** in an identity's status or condition; otherwise you risk running mover or leaver processes repeatedly on identities that have not changed.

Important: For example, you might want to trigger a leaver process any time an identity changes from "Active" to "Inactive" status. If you create a filter using the logic "Inactive Equals True" you will select all inactive identities every time the leaver process runs, regardless of whether they became inactive today or have been inactive for weeks. A better filter in this case would be "Inactive *Changed to* True"

Trigger filters are defined globally through a query builder in the Rapid Setup configuration pages for joiner, mover, and leaver processes. The filters you set in the configuration page for each type of process will apply to all applications that use Rapid Setup.

Here is an example of a simple trigger filter that will select all identities whose manager has changed:



Trigger Filter *

AND OR

Manager Changed

+ Add Row + Add Group

You can build filters using multiple criteria, choosing "AND" or "OR" processing. For example, to select all identities with a change in *either* Manager *or* in Location, your query could look like this. Note that the OR operator is selected; if the AND operator had been selected, the filter would select only those identities who have changes to *both* Manager *and* Location.

The screenshot shows a 'Trigger Filter' configuration interface. At the top, there are two radio buttons for 'AND' and 'OR', with 'OR' selected. Below this, there are two rows of criteria. The first row has a dropdown for 'Manager' and a dropdown for 'Changed'. The second row has a dropdown for 'Location', a dropdown for 'String', and a dropdown for 'Changed'. At the bottom left, there are two buttons: '+ Add Row' and '+ Add Group'.

You can also **group** sets of criteria, to allow for more complex filtering, by clicking **Add Group**. For example, if you wanted to select all identities that have a type of "Contractor" who have had a change to *either* Manager or Location, you would add a group to contain the Manager and Location filters, and your filter might look like this. Note that the AND condition applies to the Contractor type and to the group below it; within the grouping, an OR condition applies to the Manager and Location criteria.

The screenshot shows a 'Trigger Filter' configuration interface. At the top, there are two radio buttons for 'AND' and 'OR', with 'AND' selected. Below this, there is a row of criteria: a dropdown for 'Type', a dropdown for 'String', a dropdown for 'Equals', and a dropdown for 'Contractor'. Below this row is a shaded area representing a group. Inside the group, there are two radio buttons for 'AND' and 'OR', with 'OR' selected. Below these are two rows of criteria: the first row has a dropdown for 'Manager' and a dropdown for 'Changed'; the second row has a dropdown for 'Location', a dropdown for 'String', and a dropdown for 'Changed'. At the bottom left of the group, there are two buttons: '+ Add Row' and '+ Add Group'. At the bottom left of the entire interface, there are two buttons: '+ Add Row' and '+ Add Group'.

For more complex filtering, you may wish to create **populations** to use as filtering criteria. Populations are created using the **Intelligence > Advanced Analytics** feature to search for identities using a wide variety of criteria, which can include things like roles and risk scores in addition to attributes. You can save the results of these searches as populations, which are then available to use as trigger filters in Rapid Setup. When you use a population as a filter, you can choose whether you want to select identities that *are* included in this population, or that *are not*.

For example, suppose you wanted to exempt both your senior executives and your Unix system administrators from standard mover processing. In this case you could use Advanced Analytics to create and save populations that filter on job title or department to identify your executives, and on role assignments to identify your Unix administrators. Then you can use those populations as filter criteria to exclude the identities in either of those populations from a standard mover process that is based on a change in manager.

The screenshot shows a 'Trigger Filter' configuration interface. At the top, there are two radio buttons for 'AND' and 'OR', with 'AND' selected. Below this, there is a row of criteria: a dropdown for 'Manager' and a dropdown for 'Changed'. Below this row is a shaded area representing a group. Inside the group, there are two radio buttons for 'AND' and 'OR', with 'OR' selected. Below these are two rows of criteria: the first row has a dropdown for 'Chief Executives - Global' and a dropdown for 'Doesn't Contain Identity'; the second row has a dropdown for 'Unix Sysadmins' and a dropdown for 'Doesn't Contain Identity'. At the bottom left of the group, there are two buttons: '+ Add Row' and '+ Add Group'. At the bottom left of the entire interface, there are two buttons: '+ Add Row' and '+ Add Group'.

To move criteria up or down, duplicate criteria rows, or delete groups or rows, use the **gear** icons at the right of each row and group of your criteria.

Note: If you are using date fields as part of your filter criteria, you can enter day, month, and year; actions that are triggered by date criteria will take place on midnight (local time) of the date specified.

Using Identity Processing Thresholds for Error Prevention

Identity processing thresholds let you stop lifecycle events (such as joiner, mover, and leaver) before they are fully processed, to protect against dangerous or accidentally-triggered workflows from completing. For example, if someone makes a change in the Human Resources database that accidentally changes the status of an entire department's employees to "terminated", the identity processing threshold can stop IdentityIQ from running a Leaver workflow for hundreds of employees.

Thresholds can be set either as a fixed number, or as a percentage of identities. When a threshold is set, the **Identity Refresh** task will terminate when the threshold is met, without updating any identities.

Identity processing thresholds can be configured in Rapid Setup (as global setting), and in Lifecycle Events for specific workflows.

In the Identity Refresh task, the **Process events** option must be enabled in order for identity processing threshold option to take effect. If you want to process events for other purposes but disable the identity processing threshold feature, you can check the **Disable identity processing threshold** option.

If the processing threshold is triggered, the task result will include a notification that the task has failed, and a localized message provides feedback.

If you are using partitioning in the Identity Refresh task, the threshold works as a cumulative value of all events triggered across all of the partitions.

For more information, see the **Tasks, Certifications and Access Reviews**, and **Lifecycle Manager** documentation.

Using Rapid Setup

Users can configure Aggregation, Joiner, Mover, and Leaver processes for applications from **Applications > Rapid Setup**. Note that business users can only access the Rapid Setup processes that have been enabled and configured in [Rapid Setup Configuration](#)

Note: If you enabled **Terminate Processing** in your [Rapid Setup Configuration](#), that process is accessed through the **Identities > Identity Operations** menu. See [Identity Operations Configuration](#) and [Terminating Identities with Rapid Setup](#) for more details.

Choose an Application

Choose the application you want to configure for Rapid Setup processes. The applications you can choose from the drop-down list are applications that have been defined in your IdentityIQ instance through the **Applications > Application Definition** option. Before you begin, define the application schema, perform a test connection, and identify whether the application is authoritative.

See the **Application Configuration** documentation for more information.

Aggregation in Rapid Setup

The Aggregation feature of Rapid Setup lets you set options for how data is aggregated into IdentityIQ for the selected application. While Rapid Setup does not introduce new aggregation functions, it approaches it in a slightly different manner.

Note: see [Sample Rules for Rapid Setup](#) for information about sample rules included with Rapid Setup.

Create Entitlements That Cannot Be Requested

Use this option if you want the aggregation process for this application to create entitlements that will not be requestable in IdentityIQ from the Entitlement Catalog or in Access Requests.

Disable Account / Lock Account

The Disable Account and Lock Account filters only display for applications that do not natively support Disable/Lock.

- An Account can be Disabled/Locked with an Aggregation Customization Rule.
- Filters defined here take precedence over aggregation customization rules defined elsewhere in IdentityIQ.
- If the Disable Account or Lock Account filters match an account during aggregation, then the account will be marked in IdentityIQ as disabled or locked, respectively.

Account and Manager Correlation

Account Correlations determine how application accounts are assigned to identities within IdentityIQ, using account and identity information. **Manager Correlations** configure how managers should be matched to identities.

In Rapid Setup, you can configure only one method of correlation for accounts, and one for managers, for each application. Rapid Setup does not support multiple correlation rules for a single application.

If correlation logic has already been defined in the Application Definition for this application, that correlation logic will be populated by default in this tab. You can modify existing correlation logic as needed, or create a new correlation configuration.

Account Correlation

To create or edit account correlation logic for this application:

-
1. In the drop-down list on the left, choose the **application attribute** you are configuring that can uniquely identify the account on the application. The application schema that has been defined in the Application Configuration determines which attributes are available for you to select here.
 2. Choose an operator. In most cases, your only option here is "Equals"
 3. In the drop-down list on the right, choose the **IdentityIQ attribute** that uniquely defines the identity.

Manager Correlation

To create or edit manager correlation logic for this application:

1. In the drop-down list on the left, choose the **application attribute** you are configuring that identifies the manager for this identity. The application schema that has been defined in the Application Configuration determines which attributes are available for you to select here.
2. Choose an operator. In most cases, your only option here is "Equals"
3. In the drop-down list on the right, choose the **IdentityIQ attribute** that uniquely defines the identity. This is typically the same attribute you use to define the identity for account correlation.

Service Account and RPA Account Correlation in Rapid Setup

The correlation filters for Service Accounts and RPA (Robotic Process or "bot" Applications) let you identify service and RPA accounts in IdentityIQ, based on attributes from the application you are onboarding.

To correlate service accounts:

- When the Service Account filter is true, the identity attribute Type is set to Service Account, and the Application attribute Identity_Type is set to Service.

To correlate RPA accounts:

- When the RPA Account filter is true, the identity attribute Type is set to RPA/BOTS, and the Application attribute Identity_Type is set to RPA.

If you set correlation filters for both Service and RPA accounts:

- When the Service Account filter and RPA Account filter are both true for the same identity, the Identity_Type will be set to Service Accounts.
- When the Service Account filter is deleted, and the RPA Account filter is created, the Identity_Type is set to RPA.

You can configure only one method of correlation for service accounts, and one RPA accounts, for each application.

Joiner Processing in Rapid Setup

The Joiner section is where you configure application behavior and processes when a new user joins your organization.

Although populations, birthright roles, and provisioning policies do not have to be created at this point, for features within joiner to work effectively, the user is advised to create them before configuring joiner processing

Note: Leaver events take priority over joiner events. If an identity is eligible for both a leaver event and a joiner event, the joiner event will not be launched.

Option	Description
Perform Account-Only provisioning	Create an account for the joining identity on this application, even if no entitlements exist for the account.
Identity Selection	<p>This option is used only if Perform Account-Only Provisioning has been enabled. Identity Selection lets you choose which identities should be provisioned with accounts only:</p> <ul style="list-style-type: none">• Everyone – Provision all identities with accounts only.• Filter – Use an XML filter to select identities for account-only provisioning. Enter the filter XML in the text box. See XML Filter Example for more details.• Script – Use a BeanShell script to select identities. Enter the BeanShell source in the text box.• Rule – Use a rule to select identities. You can select from existing rules of type <code>IdentitySelector</code>.• Population – Use a population to select identities. Populations are defined under Intelligence > Advanced Analytics.
Automatically Start Joiner Processing for Newly Created Identities	<p>During aggregation, if a new identity is created, automatically start joiner processing on it.</p> <p>This option is not available for non-authoritative accounts when the global joiner configuration is set up to Exclude Uncorrelated Identities. See Joiner Configuration.</p>

Option	Description
Joiner Email Instructions	Use this field to add any application-specific instructions to the Joiner Completed notification email that is sent to the manager or workgroup responsible for the identity's access. See Joiner Configuration for more information about joiner notification emails.
Joiner Email Password Instructions	Use this field to add any application-specific instructions to the end of the Joiner Temporary Password notification email that is sent to the manager or workgroup responsible for the identity's access. See Joiner Configuration for more information about joiner temporary password emails.

XML Filter Example

You can use an XML-based compound filter in the Identity Selection box to filter identities. The filter should include property values and logical operators for selecting identities.

Here is an example of a compound filter that will select all identities in the Accounting department that are NOT in either the Europe or Americas regions:

Compound Filter For Selecting Identities

```
<CompoundFilter>
  <CompositeFilter operation="AND">
    <CompositeFilter operation="NOT">
      <CompositeFilter operation="OR">
        <Filter operation="EQ" property="region" value="Europe" />
        <Filter operation="EQ" property="region" value="Americas" />
      </CompositeFilter>
    </CompositeFilter>
    <Filter operation="EQ" property="department" value="Accounting" />
  </CompositeFilter>
</CompoundFilter>
```

For more information on using compound filters, refer to these articles on Compass (login required):

- [Compound Filters](#)
- [Filters and Filter Strings](#)

Mover Processing in Rapid Setup

The mover processing that can be configured at the application level consists of **certifying** the changes in access that can arise when an identity moves within your organization. There are other mover behaviors that can be configured globally in [Mover Configuration](#). At the application level, some additional certification and account creation behavior can be defined.

Note: Joiner and leaver events take priority over mover events. If an identity is eligible for a joiner event or a leaver event, the mover event will not be launched.

Option	Description
Include Additional Entitlements in a Certification for This Application	Enable this option if you want the certification to include entitlements that are not contained in a role. If certifications are not enabled globally for mover processing, this option is ignored. A message above the configuration options indicates when certifications are not globally enabled.
Include Targeted Permissions in a Certification for This Application	Enable this option if you want the certification to include the actions a user can perform on an Unstructured Target such as a file share or folder If certifications are not enabled globally for mover processing, this option is ignored. A message above the configuration options indicates when certifications are not globally enabled.
Perform Account-Only Provisioning	Create an account for the moving identity on this application, even if no entitlements exist for the account.

Leaver Processing in Rapid Setup

Note: Provisioning policies for deleting/disabling/unlocking accounts, and a password policy for password scrambling, should be created before this process is configured.

The leaver feature gives the user the option to configure the leaver plan by either using a rule or by selecting options to configure a plan. If you opt to configure your processes, you can set up separate processes for ordinary leaver events, and for terminations. If you choose to use a rule for leaver processing, you will select one rule to manage both leaver and termination processing.

- To use a rule for leaver processing, select **Use rule**, and choose a rule from the drop-down list.
- To configure a leaver plan, select **Configure**, and use the options below to determine leaver and termination processing behavior.

Note: No other Rapid Setup event takes priority over leaver processing. If an identity is eligible for leaver event as well as a joiner or mover event, the leaver event will be launched, and the other events will not.

Leaver Options

Leaver options are for managing identities that leave your organization in circumstances other than immediate termination. Immediate termination options are configured separately.

Option	Description
Delete Account	<p>To delete a leaving identity's accounts, enable this option. Then choose when the accounts should be deleted:</p> <ul style="list-style-type: none"> Choose Now to delete accounts immediately. Choose Later to set a number of days before accounts should be deleted. When you choose Later, you have additional options for handling accounts before they are deleted, as described below.
Disable Account	<p>Send a request to disable the account. Choose Now to disable accounts immediately, or Later to postpone the disabling.</p> <p>When you choose Later, use the Days to Delay field to set the number of days to wait before disabling accounts.</p>
Scramble Password	<p>Scramble the value of the password account attribute. This option is used when the application does not natively perform password maintenance.</p> <p>Choose Now to scramble passwords immediately, or Later to postpone the action. If you choose Later, use the Days to Delay field to set the number of days to wait before the action occurs.</p>
Move Account	<p>This option is only used for Active Directory applications.</p> <p>Enter the full OU to the container where leaving identities should be moved. You can set this option to run Now or Later.</p>
Remove Entitlements	<p>Choose whether to remove entitlements as part of the leaver process. You can set this option to run Now or Later.</p> <p>If you enable this option, you can use the Entitlement Exceptions filter to choose any entitlements that you do not want to remove as part of the leaver process.</p>
Add Comment	<p>Add Comment lets you enter comments to be added to the application account for the leaving identity.</p>

Option	Description
	<p>The Comment Attribute is the attribute in the application where comments are stored.</p> <p>The Comment field is where you enter the comment to be stored in the Comment Attribute on the application.</p>

Terminate Options

Use this section to configure how termination events should be processed. Termination processes are enabled, and have some global behavior configured, through [Identity Operations Configuration](#). When termination processing is enabled and configured, terminations for individual identities are initiated through the **Identities > Identity Operations** menu. See [Terminating Identities with Rapid Setup](#) for more information.

To configure Terminate Options that are specific to this application:

- If you want termination processing to follow all the same processes you have configured for Leaver Options, choose **Use the same settings as leaver options**
- If you want to set up different processes for terminations than those you have configured for Leaver options, disable the **Use the same settings as leaver options** slider. Then you can configure termination-specific behavior; the fields for configuring termination options are identical to the ones for leaver options. Refer to the table above for information about these fields.

Terminating Identities with Rapid Setup

Rapid Setup's Identity Operations feature lets you immediately terminate access for an identity, without approvals. This is done by immediately processing the Leaver workflow for a selected identity.

The terminate option is enabled and configured globally using [Identity Operations Configuration](#). In addition, you can set application-specific termination processes in [Leaver Processing in Rapid Setup](#).

To terminate an identity:

1. Click **Identities > Identity Operations**.
2. Select the identity to terminate. Only one identity can be selected at a time.

Note: You can use the Search field and filters to find specific identities.

3. Click **Next**.
4. Choose **Terminate**.
5. Enter a **Reason** for the termination. This is a required field.
6. Click **Next**.
7. Review the information, then click **Submit** to complete the process.

Rapid Setup Troubleshooting

To help with troubleshooting any issues in Rapid Setup, add these entries to the log4j2.properties file:

```
logger.rapidsetup.name=sailpoint.rapidsetup
```

```
logger.rapidsetup.level=debug
```

```
logger.rapidsetuplib.name=sailpoint.workflow.RapidSetupLibrary
```

```
logger.rapidsetuplib.level=debug
```