SailPoint Identity **IQ**

Rapid Setup Guide

Version: 8.1p1 Revised: July 10, 2020

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2020 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," "SailPoint & Design," "SailPoint Technologies & Design," "AccessIQ," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "Managing the Business of Identity," and "SecurityIQ" are registered 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 with regard to this manual 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

Copyright and Trademark Notices.	i
Contents	ii
Getting Started	1
Joiner	1
Mover	1
Leaver	2
Configuration	3
Joiner	4
Mover	5
Leaver	6
Identity Operations	7
Miscellaneous	8
Defining Trigger Filters	8
Using Rapid Setup	9
Aggregation	9
Account Disable and Account Lock	9
Identity and Manager Correlation	9
Service Account and RPA Accounts	10
Joiner	10
Mover	11
Leaver/Terminate Options	11
Configuring the Leaver Plan	11
Terminate Identity	13
Terminate Identity	13
Terminate Identity Page Overview	13
Terminate Identity Procedure	13

Getting Started

The terms Business Process and workflows are used interchangeably.

Use the following information to activate your RapidSetup installation.

- 1. Log on to your instance of IdentityIQ as an administrator.
- 2. Click on Global Settings under the gear icon and select the Import from File page.
- 3. Click **Browse** and browse to the following directory: identityiq_home\WEB-INF\config where identityiq_home is the directory in which you extracted the *identityiq.war* file during the IdentityIQ installation procedure.
- 4. Select the init-rapidsetup.xml file and click Import.
- 5. When the import is complete, click Done.

If a problem arises, add these lines to access troubleshooting tips:

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

logger.sm.level=debug

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

```
logger.sl.level=debug
```

Joiner

Enable the Joiner process to define the operations that are launched when a new user joins your organization.

These can include:

- Building a provisioning plan which includes:
 - Assignment of birthright roles which have an assignment rule matching the identity.
 - For each application which has enabled account-only provisioning, create a new account on the application (if none exists yet) if identity meets account-only creation criteria.
- Executing the provisioning plan. By default, the "LCM Provisioning" workflow is used to execute the plan.
- Notifying the manager with results of the provisioning.
- Optionally notifies the manager when a temporary password is generated.
- Running an optional post-joiner rule.

Mover

Enable the Mover process to define the operations that are launched when a user moves within your organization and roles have to be adjusted.

These can include:

- Performing a certification on the moving identity. Application can choose whether or not to certify their additional entitlements.
 - Global setting available to skip certifications during mover.
 - Perform a joiner-type provisioning on the moving identity. Birthright roles will always be assigned/removed as appropriate. Applications can choose whether or not to perform account-only provisioning during move.
- Global setting available to skip joiner-type provisioning.
- Running an optional post-mover rule.

Leaver

Enable the Leaver process to define the operations that are launched when someone leaves your organization.

These can include:

- Reassigning the owner of objects currently owned by the leaving identity.
- Notifying the manager of the leaving identity about the reassigned object.
- Reassigning of administrator of identities currently administered by the leaving identity.
- Notifying the manager of the leaving identity about the re-administered identities.
- Auto-reject requests targeted for the leaving identity.
- Building immediate provisioning plan:
 - Removal of the identity's IIQ roles
 - For each application on which identity has an account, and leaver is enabled. The RapidSetup configuration for each application declares which of the below actions to perform, and the timing of whether to perform immediate or deferred:
 - Removal of the identity's entitlements (unless excluded from removal)
 - Scrambling the identity's password on application
 - Adding a comment to an account attribute
 - Moving account to a different OU on a container-based application
 - Disabling/deleting account
- Executing the immediate provisioning plan. By default, the "LCM Provisioning" workflow is used to execute the plan.
- Notifying the manager with results of the immediate provisioning.
- Updating links which may need updating due to a move.
- Running an optional post-leaver rule.

Configuration

After you activate Rapid Setup, you can configure it to meet the needs of your organization. A user can configure various workflows depending on needs surrounding the organizations identities.

To configure Rapid Setup, navigate to the Gear Icon > Global Settings > Rapid Setup Configuration.

The Rapid Setup Configuration has tabs that can be customized to meet your organizations needs. The following tabs are available for configuration:

- Joiner
- Mover
- Leaver
- Identity Operations
- Miscellaneous

₩ Home My	Work - Identities	 Applications - 	Intelligence - Set	up 👻				p -	۰.	21	The Administrator 👻
Rapid Setup	Configuratio	n									
Joiner Mo	ver Leaver	Identity Operation	ns Miscellaneo	us							
Enable Joiner Pro	ocessing										
					Return to Global Settings	Save					

When a process is enabled, a dot will display with the tab title. The blue dot signifies that changes were made on the page and were not saved. Remember to save selected options once done.

Joiner

If a new identity is coming into the organization, configure a joiner workflow for that joining identity.

Enable Joiner Processing displays the following:

Options	Description
Generate Approvals	Select if the workflow should have approvals.
Automatically Join New Empty Identities	Perform joiner processing on new identities which have no accounts.
Exclude Uncorrelated Identities	Do no include identities which have not been correlated.
Alternative Workgroup for Joiner Completed Notification Email	Select a workgroup to receive Joiner notification emails rather than a manager.
Joiner Completed Notification Email Template	Specify the template to use for notification emails.
Send Temporary Password Email	If enabled, send an email notification with temporary password info to the newly created joining identity's manager.
Post Joiner Rule	Specify a user rule to use after running a Joiner workflow.
Joiner Business Process	Specify which business process workflow is executed during the Joiner process.
Trigger Filter	Define a variety of customizable filters that specifies when joiner processing is run.

Mover

If an identity is moving job functions, configure a mover workflow for that moving identity.

Enable **Mover Processing** displays the following:

Mover Configuration Options

Options	Description
Generate Approvals	Select if the workflow should have approvals.
Launch a Mover Cer- tification	Launch a certification campaign during the Mover process. This certification must be complete before joiner processing.
Stage the Cer- tification	Stage the certification. Refer to the "Phases of a Certification" section in the SailPoint IdentityIQ Certification and Access Review Guide.
Include Birthright Roles	Include birthright roles that were previously assigned to this user in the cer- tification.
Certification Owner	The owner of the defined certification.
Backup Certifier	Select an alternate identity to receive the access review created by this cer- tification if the original owner is unable to certify.
Include Previous Manager as a Cer- tifier	Assign an access review to an identity's previous manager.
Joiner Processing	Run the Joiner process as part of the Mover process to perform the basic access assignment.
Post Mover Rule	Specify a rule to use after running a Mover workflow.
Mover Business Pro- cess	Select the business process workflow executed during the Mover process.
Trigger Filter	Define a filter that specifies when mover processing is run.

Leaver

If an identity is leaving the organization, configure the leaver workflow for that leaving identity.

Enable Leaver Processing to display the following:

Leaver Configuration Options

Options	Description
Generate Approvals	Select if the workflow should have approvals.
Exclude Uncorrelated Iden- tities	Do no include identities which have not been correlated.
Remove Assigned Roles	Remove assigned roles from an identity during Leaver processing.
	Reassign objects owned by a leaving user.
Reassign Artifacts	Select the reassignment objects from the drop-down list. Multiple objects can be selected.
Reassignment Artifacts Types	Specify which object types should have the owner attribute reas- signed if the current owner is the leaving identity.
Reassign Artifacts to Man- ager	Reassign objects to the manager of the leaving identity.
Reassign Artifacts Rule	Handle reassignment of object using this rule.
Reassign Artifacts Alternate	Reassign objects to this identity if none were discovered for man- ager or by the reassignment rule.
Reassign Identities	Reassign any identities, of type rpa or service, administered by a leaving identity.
Reassign Identities to Man- ager	Reassign the identities to the manager of the leaving identity.
Reassign Identities Rule	Handle reassignment of managed identities using this rule.
Reassign Identities Alternate	Reassign managed identities to this identity if none were discovered for 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 reas- signments (used for both artifact and identity reassignment).
Leaver Completed Noti- fication Email Template	Specify the template to use for notification emails.
Post Leaver Rule	Specify a rule to use after running a Leaver workflow.
Leaver Business Process	Select the business process workflow executed during the Mover process.
Trigger Filter	Define a filter that specifies when leaver processing is run.

Identity Operations

If an identity is terminated from the organization, configure the identity operations workflow for that terminated identity.

Enable Terminate Processing to display the following:

Identity Operations Configuration Options

Options	Description
Generate Approvals	Select if the workflow should have approvals.
Remove Assigned Roles	Remove assigned roles from an identity during Terminate pro- cessing.
	Reassign objects owned by a terminated user.
Reassign Artifacts	Select the reassignment objects from the drop-down list. Multiple objects can be selected.
Reassign Artifacts Types	Specify which object types should have the owner attribute reas- signed if the current owner is the leaving identity.
Reassign Artifacts to Manager	Reassign objects to the manager of the terminated identity.
Reassign Artifacts Rule	Handle reassignment of object using this rule.
Reassign Artifacts Alternate	Reassign objects to this identity if none were discovered for man- ager or by the reassignment rule.
Reassign Identities	Reassign any identities, of type rpa or service, administered by a leaving identity.
Reassign Identities to Man- ager	Reassign the identities to the manager of the leaving identity.
Reassign Identities Rule	Handle reassignment of managed identities using this rule.
Reassign Identities Alternate	Reassign managed identities to this identity if none were dis- covered for manager or by the reassignment rule.
Send Terminate Complete Notification to this Workgroup	Select a workgroup to receive Terminate notification emails rather than a manager.
Ownership Reassignment Notification Email Template	Email template to compose the email notification regarding reas- signments (used for both artifact and identity reassignment).
Terminate Completed Noti- fication Email Template	Specify the template to use for notification emails.
Post Terminate Rule	Specify a rule to run after the Terminate Business Process com- pletes.
Terminate Business Process	Select the business process workflow executed during the Mover process.

Miscellaneous

The following options display within Miscellaneous:

Μ	iscellaneous Configuration Options
Options	Description
Business Process Requester	Select an identity to use as the requester for Rapid Setup life- cycle workflows.
Alternative Workgroup for Rapid	Select a workgroup to receive emails.
Setup Notification	By default, No Manager is an empty workgroup. Add people to this workgroup or select a different one.
Workgroup to Dessive Error Nati	Select a workgroup to be notified of errors by email.
Workgroup to Receive Error Noti- fication Email	By default, Rapid Setup Error Notification is a stand-in. Review and update if desired.
Notification Style Sheet Email Template	Select a style sheet for emails.
Notification Header Email Tem- plate	Select an email header template.
Notification Footer Email Tem- plate	Select an email footer template.
Role Types to Treat as Rapid Setup Birthright Roles	Select a role type with Birthrights.

Defining Trigger Filters

Identity triggers are the core of what drives joiner, mover, leaver within Rapid Setup. Trigger Filters are the constraint logic that is applied to the identities to determine or control which identities will participate in the joiner, mover, leaver workflows.

This filter is created using the new query builder in the Rapid Setup Configuration page and applies to all applications using Rapid Setup.

Using Rapid Setup

The Rapid Setup application is where the business user functions reside. Full access to Rapid Setup allows the user to access the Rapid Setup page with edit privileges.

Applications -	Intellige
Application Defini	tion
Rapid Setup	
Entitlement Catal	og
Application Risk N	Nodel
Activity Target Ca	tegories

Aggregation

Review this section before configuring aggregation using Rapid Setup. While Rapid Setup does not introduce new aggregation function, it approaches it in a slightly different manner.

For detailed information about aggregation in IdentityIQ, refer to the 8_1p1_IdentityIQ_System_Administration_Guide and the IdentityIQ_System_Administration_Guide.

Account Disable and Account Lock

Account Disable and Lock filter only display for applications that do not support Disabled/Locked.

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

If an application does not have ENABLE or UNLOCK in its features string, the disabled and/or locked fields will appear in the Rapid Setup aggregation UI. During aggregation, the account representation in IIQ will be marked with "IIQDisabled" or "IIQLocked" attributes if the corresponding filter matches. The account on the native application is not modified. Applications that natively support disabled and/or locked (indicated with a features string containing ENABLE and/or UNLOCK, respectively), will not see the Disabled or Locked filter settings option in the Rapid Setup aggregation UI.

Identity and Manager Correlation

Identity and Manager Correlations are configurations to support matching an account to an identity and matching an identity to its manager. These configurations are available on the Application Definition page but are surfaced here. More than one filter cannot be created or displayed in the App Onboarding user interface.

- Filters created display in the Application Definition, and changes to the filter in the Application Definition display here.
- Create more than one filter in the Application Definition displays a warning in the App Onboarding user interface.

Service Account and RPA Accounts

More than one filter cannot be created in the App Onboarding user interface.

- 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.
- 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.
- 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.

Joiner

Though 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.

The Leaver event has priority over Joiner. If an identity is eligible for Leaver event, the Joiner event will not be kicked off.

Option	Description
Perform Account-Only pro- visioning	Enable provisioning for the account only.
Identity Selection	 Specify a selection method: Everyone – Select Everyone if all identities should be provisioned for an account only. Filter – XML filter. Script – Beanshell source. Rule – Select a rule from the drop-down list. Either the Cert Event Trigger Rule or the Policy Violation Owner Rule. Population – Select a population from the drop-down list. Either the High Risk Tokyo Inv Managers or the Rapid Setup Correlated Identities.
Automatically Start Joiner Pro- cessing for Newly Created Identities	Set Rapid SetupProcessingState to Needed for newly created iden- tities.
Joiner Email Instructions	If a string is present, expand it. This information is added to the end of the Joiner Completed Notification email for each application.
Joiner Email Password	If a string is present, expand it. This information is added to the end of the Joiner Temporary Password Notification email to the man- ager.
Instructions	This is typically used to inform the manager of the temporary user of an account.

Joiner Workflow

Mover

Verify that role and entitlements are set up properly with display names and descriptions before this feature is configured.

The Joiner and Leaver events have priority over Mover. If an identity is eligible for Joiner or Leaver events, the Mover event is not kicked off.

	Mover Workflow
Identity Selection	Description
Include Additional Enti- tlements in a Certification for This Application	Include entitlements the user has from this application in the cer- tification if they are not encapsulated in a role the user has.
Include Targeted Per- missions in a Certification for This Application	Ability to add target permissions during certification.
Perform Account-Only Pro- visioning	Perform account-only provisioning during Mover for the identity. The checkbox for Account-Only Provisioning has to be enabled in the Joiner Global Configuration.

Leaver/Terminate Options

Terminate Options are the same as the Leaver options. When setting up the terminate plan, you can use the same leaver setting by toggling **Use the same settings as leaver options**.

Though delete, disable, and unlock account provisioning polices and password policy for scrambling options do not have to be created at this point, for features within Leaver to work effectively, the user is advised to create them before Leaver is configured.

The Leaver feature provides the option to configure the leaver plan by either using a rule or by selecting options to create a deletion plan.

If using a rule, select Use Rule and select a rule from the drop-down list.

Any non-equals operators are comparing against the actual value and not the display name, whereas the equal operator is comparing to the display name.

Configuring the Leaver Plan

No other event has priority over Leaver. If an identity is eligible for Leaver event, the Leaver event will be kicked off.

- Select Delete Account to delete the account completely.
- Select at deletion time, Now or Later. If Later, specify the number of days to wait before the account is deleted.
- If you are configuring the Leaver plan, the following are options are available:

	Leaver Workflow
Identity Selection	Description
Disable Account	Send a request to disable the account.
Scramble Pass-	Scramble the value of the specified account attribute.
word	Useful on applications that do not perform password maintenance natively.
Remove Enti-	Remove entitlements from the account.
tlements	Use the Entitlement Exceptions filter to specify entitlements that should not be removed.
Add Comment	Additional information can be added if needed.

Terminate Identity

Rapid Setup includes a feature that enables you to immediately terminate access for an identity without approvals. This is done by immediately processing the Leaver workflow.

The Terminate Identity option process is initiated from the Identity Operations page.

Terminate Identity

Terminate Identity Page Overview

Information about this pages features can be found in Chapter 33 of the 8_1p1_IdentityIQ_User Guide.

Terminate Identity Procedure

Complete the following steps to terminate an identity:

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

You can use the Search field to find the identity you are looking for or use filters to limit the identities displayed.

- 3. Choose Terminate.
- 4. The **Reason** field is displayed and is required. Enter the reason for the termination and click **Next**.
- 5. Confirm the identity and click **Terminate**.