Rapid Setup Guide

Version: 8.1p1

Revised: July 10, 2020

Copyright and Trademark Notices.

Contents

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.

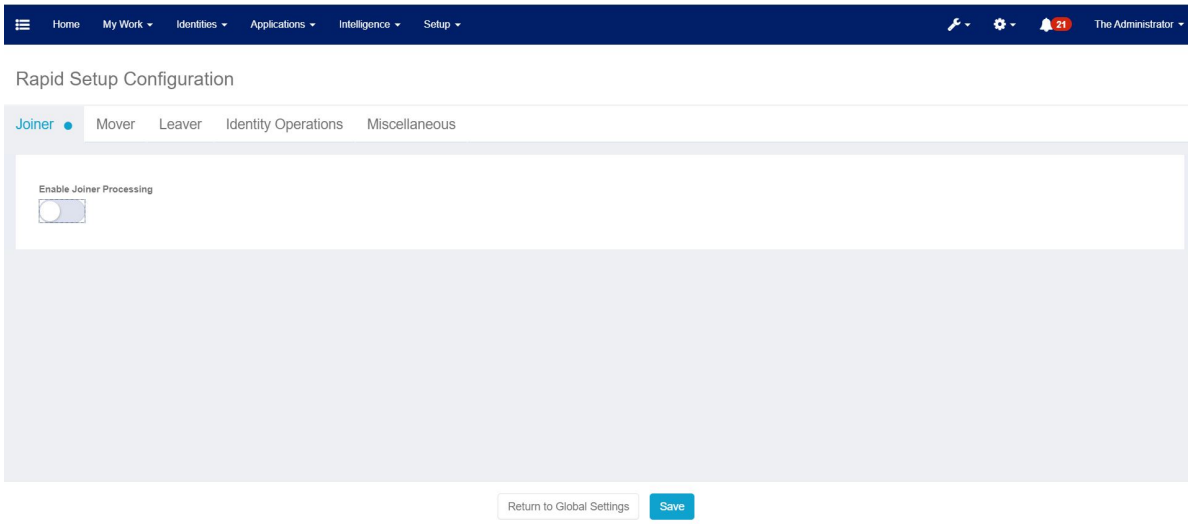
Configuration

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



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:

Joiner Configuration Options

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 Certification	Launch a certification campaign during the Mover process. This certification must be complete before joiner processing.
Stage the Certification	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 certification.
Certification Owner	The owner of the defined certification.
Backup Certifier	Select an alternate identity to receive the access review created by this certification if the original owner is unable to certify.
Include Previous Manager as a Certifier	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 Process	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 Identities	Do no include identities which have not been correlated.
Remove Assigned Roles	Remove assigned roles from an identity during Leaver processing.
Reassign Artifacts	Reassign objects owned by a leaving user. 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 reassigned if the current owner is the leaving identity.
Reassign Artifacts to Manager	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 manager or by the reassignment rule.
Reassign Identities	Reassign any identities, of type rpa or service, administered by a leaving identity.
Reassign Identities to Manager	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 reassignments (used for both artifact and identity reassignment).
Leaver Completed Notification 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 processing.
Reassign Artifacts	Reassign objects owned by a terminated user. 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 reassigned 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 manager or by the reassignment rule.
Reassign Identities	Reassign any identities, of type rpa or service, administered by a leaving identity.
Reassign Identities to Manager	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 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 reassignments (used for both artifact and identity reassignment).
Terminate Completed Notification Email Template	Specify the template to use for notification emails.
Post Terminate Rule	Specify a rule to run after the Terminate Business Process completes.
Terminate Business Process	Select the business process workflow executed during the Mover process.

Miscellaneous

The following options display within Miscellaneous:

Miscellaneous 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 Setup Notification	Select a workgroup to receive emails. By default, No Manager is an empty workgroup. Add people to this workgroup or select a different one.
Workgroup to Receive Error Notification Email	Select a workgroup to be notified of errors by 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 Template	Select an email header template.
Notification Footer Email Template	Select an email footer template.
Role Types to Treat as Rapid Setup Birthright Roles	Select a role type with Birthrights.

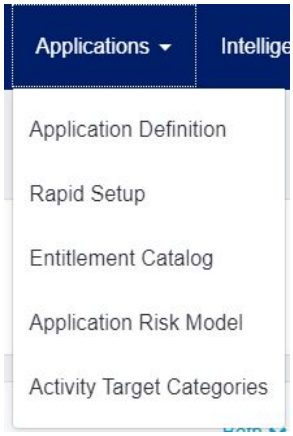
Defining Trigger Filters

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.



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.

Joiner Workflow

Option	Description
Perform Account-Only provisioning	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 Processing for Newly Created Identities	Set Rapid SetupProcessingState to Needed for newly created identities.
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 Instructions	If a string is present, expand it. This information is added to the end of the Joiner Temporary Password Notification email to the manager. This is typically used to inform the manager of the temporary user of an account.

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 Entitlements in a Certification for This Application	Include entitlements the user has from this application in the certification if they are not encapsulated in a role the user has.
Include Targeted Permissions in a Certification for This Application	Ability to add target permissions during certification.
Perform Account-Only Provisioning	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 Password	Scramble the value of the specified account attribute. Useful on applications that do not perform password maintenance natively.
Remove Entitlements	Remove entitlements from the account. 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**.