SailPoint IdentityIQ

Version 8.1

Policy Guide

Table of Contents

IdentityIQ Introduction

SailPoint IdentityIQ is an identity and access management solution for enterprise customers that delivers a wide variety of IAM processes-including automated access certifications, policy management, access request and provisioning, password management, and identity intelligence. Furthermore, IdentityIQ has a flexible connectivity model that simplifies the management of applications running in the datacenter or the cloud.

Compliance Manager — IdentityIQ Compliance Manager automates access certifications, policy management, and audit reporting through a unified governance framework. This enables you to streamline compliance processes and improve the effectiveness of identity governance, all while lowering costs.

Lifecycle Manager — IdentityIQ Lifecycle Manager manages changes to access through user-friendly self-service request and password management interfaces and automated lifecycle events. It provides a flexible, scalable provisioning solution for addressing the constantly evolving access needs of your business in a way that's both efficient and compliant.

IdentityAI – Integrating IdentityAI within IdentityIQ enables the delivery of Predictive Identity. IdentityAI is a rule based machine learning engine using identity graph technology to provide recommendations for access review and access request decisions. With IdentityAI enabled, you can also review access history for identity cubes, create dashboards that can be customized from an administrative perspective, and view peer groups within the IdentityAI user interface.

Privileged Account Management Module — IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.

Connectors and Integration Modules — IdentityIQ offers Integration Modules that support the extended enterprise IT infrastructure. Third party provisioning and service desk integration enable multiple sources of fulfillment to access change. Service catalog integration supports a unified service request experience with integrated governance and fulfillment. Mobile device management integration mitigates risk posed by mobile devices through centralized visibility, control and automation. And IdentityIQ's IT security integration provides enhanced security with improved responsiveness and controls.

Open Identity Platform — SailPoint's Open Identity Platform lays the foundation for effective and scalable IAM within the enterprise. It establishes a common framework that centralizes identity data, captures business policy, models roles, and takes a risk-based, proactive approach to managing users and resources. The Open Identity Platform is fully extensible, providing robust analytics which transforms disparate and technical identity data into relevant business information, resource connectivity that allows organizations to directly connect IdentityIQ to applications running in the datacenter or in the cloud, and APIs and a plugin framework to allow customers and partners to extend IdentityIQ to meet a wide array of needs. An open platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications-in the datacenter and the cloud. SailPoint IdentityIQ applies consistent governance across compliance, provisioning and access management processes, maximizing investment and eliminating the need to buy and integrate multiple products.

Password Manager — IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device. By providing intuitive self-service and delegated administration options to manage passwords while enforcing enterprise-grade password, IdentityIQ enables businesses to reduce operational costs and boost productivity.

Amazon Web Services (AWS) Governance Module — Enables organizations to extend existing identity lifecycle and compliance management capabilities within IdentityIQ to mission-critical AWS IaaS environments to provide a central point of visibility, administration, and governance across the entire enterprise. This includes policy

discovery and access history across all organization accounts, provisioning AWS entities and objects, access review and certification, and federated access support.

SAP Governance Module — Improves the user experience by introducing a new integrated visual interface for navigating and selecting SAP identities and roles as part of IdentityIQ lifecycle management and compliance solution. SAP data is presented in a familiar hierarchy format that closely represents deployed system resources and organizational structures. New filtering capabilities enable more efficient browsing and selection of SAP data so tasks can be performed faster. Improved granular support for separation of duty (SOD) violation policies provides flexibility for customers to craft more detailed identity governance policies that include SAP role details such as T-Codes and Authorization Objects.

Chapter 1: Policy Violations

Policies in IdentityIQ check identities for certain conditions that are unwanted, or even considered dangerous - for example, a set of roles that should not be combined in a single identity (such as “payment preparation” and “payment approval”), two conflicting values of a multi-valued attribute, a high risk score, or even cross-application combinations of permissions.

Policy violations occur when an identity is found to be in violation of an active policy.

The Policy Violations page shows you any policy violations you are responsible for acting on. You can revoke the problematic access, allow the violation to continue for a set period of time, or take other actions such as forwarding the violation to another user.

Use the Policy Violations page to manage policy violations outside of certifications. This page enables you to identify policy violations as soon as they are detected, and take immediate action to resolve those violations.

Overview of the Policy Violations Page

The Policy Violations page lists policy violations that are marked as active and violations owned by you or one of the workgroups to which you belong. When a policy is defined, an owner to a policy violation can be defined. The policy violation owner is a chosen identity, manager of the person who violated the policy, or an identity created by running a rule. You cannot take action on your own violations.

Based on how your system is configured the Policy Violations page can have the following tabs and actions:

Note: The number on the tab indicates the number of items listed on the associated tab page.

- **Open** Tab - From this tab you can:
  - **Allow** or **Revoke** a violation.
  - Make **Bulk Decisions** on multiple violations.
  - View **Details** about a violation from the menu icon for the violation.
  - Launch a certification of items, using the **Certify** option (in the **Bulk Decisions** menu)
- **Complete** Tab - From this tab you can
  - Launch a certification of items, using the **Certify** button
  - **Edit Decision** from the **3-line menu** icon for the violation.
  - **View Decision** for a revoked violation from the **3-line menu** icon .
  - View **Details** about a violation from the **3-line menu** icon for the violation.

For information on managing policy violations through work items, refer to the *IdentityIQ User Guide* .

Accessing the Policy Violations Page

Policy violation can be accessed from the menu bar using **MyWork > Policy Violations**. Depending on how your system is configured, you can also access the Policy Violations page from the QuickLinks menu > **My Tasks > Policy Violations** or from a Home page QuickLink card.

Most users will see the same list of policy violation from the menus and the QuickLinks card. Users with **System Administrator** or **Policy Administrator** capabilities will see different results based on how they access the page:

- The QuickLinks menu and card will show System Administrators and Policy Administrators o**nly the violations for which they are themselves are responsible**.
- The My Work > Policy Violations menu will show System Administrators and Policy Administrators **all policy violations in the system,** not just the ones they are responsible for.

Display Options

Use the **Filter** icon to limit what is displayed on the Policy Violations Page. You can filter violations by user name, (including first name and last name), policy type, status, and policy violation ID, using any combination of filters and values. To apply your filter criteria, click **Apply**.

When filtering is applied, the Filter button in the Policy Violations turns green, to alert you that you are seeing a filtered subset of all your items. To clear filtering, click **Filter** again, then click **Clear**.

You can sort the information in the table in ascending or descending order by clicking on any of the column headings.

Accessing Policy Violation Work Items

Depending on how the policy was configured, you can also view your policy violation items in your work item listing, by clicking **My Work > Work Items**. In the Work Items page, policy violations are listed along with any other work items you may have. You can filter, search, and sort the items in this list to limit what is shown.

In the Work Items Page, you can:

- Click the **Info** icon to see information about violation item
- Forward the violation item to another user to process, using the **Forward (arrow)** icon
- Click **View** to open a detailed view of the item. When you click **View**, you have additional options for managing the item:
  - **Add Comments** to the item
  - Click the **Go to violation link** to see options to Allow, Revoke/Correct, or Certify the item
  - Save any changes (such as the addition of a comment) you have made to the item

For more detailed information about the details and options in this page, see “Policy Violation Work Items” on page 8.

Policy Violations Open Tab

The Open tab lists policy violations awaiting your attention. The **Open** tab includes the following:

Table 1—Policy Violations Page: Open Tab Column Descriptions

Column	Description
Identity	First and last name of the user who is in violation of the policy
Policy Name	Name of policy that is violated.

Table 1—Policy Violations Page: Open Tab Column Descriptions

Column	Description
Rule	Specific rule in the policy that is in violation.
Owner	The person responsible for acting on the violation. If the creation of work items is enabled in the policy configuration, this is also the person who receives the work item triggered by the violation.
Description	Description of the violation from the Policy Configuration page.
Decisions	The available decisions you can make on this violation.
Details	Click the 3-line menu icon for the option to view details about the item.
Bulk Decisions	Depending on how the policy was configured, you may have the option to select multiple items and process them in bulk. The **Bulk Decisions** menu is also where the option to **Certify** the item is located.

Violation Decisions and Actions

Note: You cannot take action on your own violations.

Depending on how your system is configured the following decision options can be available:

Table 2—Policy Violations Page: Open Tab Decisions and Actions

Decision	Description
Allow	Select the **Allow** icon to open the **Allow Violations** dialog. When you allow, or mitigate, a violation you are setting a time period in which the identity is allowed to work in violation of the policy without affecting compliance or risk. The date field shows the end date of this period, when the violation will reappear in this list and in certifications. Whether or not you can edit the date field depends on how your system administrator has configured your system's Compliance Manager settings. Add any comments necessary to explain this mitigation decision.
Revoke	You cannot perform bulk violation corrections and only SOD violations can be corrected. Select the **Revoke** icon to display the detailed view of the violation and make a revocation decision based on the items displayed. You must revoke one complete set of offending roles or the violation remains. The Revocations can be done automatically, if your provisioning provider is configured for automatic revocation, by generating a help ticket, if your implementation is configured to work with a help desk solution, or manually using a work request assigned to a IdentityIQ user.
Delegate	This option is available only when the **Enable Line Item Delegation** option is enabled in your system's Compliance Manager global settings. Select **Delegate Violation** to display the delegate violation panel. Use the fields to associate a work item with the selected policy violations and assign it to the appropriate user for corrective action. The owner of a policy, or a compliance officer who is tracking violations, may not be the same person who can make the decision as to how to correct the violation. On the delegate violation panel, enter the full name of the person to whom you assigning this work item. Entering the first few letters of a name displays a pop-up menu of IdentityIQ users with names containing that letter string. You can also select a recipient from the **Manually Select Recipient** drop-down list. Enter a description and comments as needed to assist the recipient.
Bulk Decisions	Select multiple violations and use this option to take bulk actions, such as Allow and Certify.

Table 2—Policy Violations Page: Open Tab Decisions and Actions

Decision	Description
Certify	The **Certify** option is under the **Bulk Decisions** menu. Select items in your list, then click **Certify** to open the Schedule Certification page, to set up a certification. From this page you can schedule full certifications for the identities appearing on the policy violations list. You can use this option to provide another way to monitor identities that might be at risk within your enterprise.
Comments	If this option is enabled, you can add comments. In some instances, you may be *required* to add comments.
Details	Select this option to view detailed information.

The following reference table lists the available options for specific policy types:

Table 3—Policy Violations: Available Options by Policy

Policy Type	Available Policy Violation Options
Account	Allow, Certify
Advanced Entitlement Policy	Allow, Certify, Revoke
Advanced Policy	Allow, Certify
Entitlement Policy	Allow, Certify, Revoke
Activity Policy	Allow, Certify
Risk Policy	Allow, Certify
SOD Policy	Allow, Certify, Revoke

After you have made your decisions, click **Save**.

Policy Violations Complete Tab

The **Complete** tab lists the items you have made a decision on and saved. The **Complete** tab contains information about the Identity, Policy Name, Rule, Owner, Description, and Decisions for each policy violation in the list.

Based on how your system is configured, the **Complete** tab can include the following options:

Table 4—Policy Violations Page: Complete Tab Decisions

Options	Description
Certify	You can select items in your list and click **Certify** to open the Schedule Certification page, to set up a certification. From this page you can schedule full certifications for the identities appearing on the policy violations list. You can use this option to provide another way to monitor identities that might be at risk within your enterprise.
Edit Decision	Click Edit to make changes to the decision
Details	Select this option to view detailed information.

Policy Violation Work Items

Policy violation work items can be assigned by policy reviewers from the Policy Violation page, or automatically by business processes, violation rules, or alerts configured in your enterprise. These work items are generated outside of the certification process. Policy violation work items can also be created when the Check Active Policies task detects active policy violations.

Approve Policy Violation work items created through a business process can appear and act differently than work items created manually or automatically through an alert or rule. Work items created through a business process are highly customizable, and allow you to take action on the policy violation directly from the work item, instead of having to go to the Policy Violations page. The actions that are enabled, and the resulting actions based on the selection made, depend upon how the business process was defined.

In the Work Items Page, you can:

- Click the **Info** icon to see information about violation item
- Forward the violation item to another user to process, using the **Forward (arrow)** icon
- Click **View** to open a detailed view of the item. When you click **View**, you see more information about the item, and have additional options for managing the item, as described in Table 5 :

Table 5—Policy Violation Work Item Description

Category	Description
Summary:	
Requester	The name of the person or workgroup that assigned the work item.
Owner	The name of the person who is responsible for this work item.
Description	A brief description of the action required for this work item.
Created	The creation date of this work item.
Expiration	The work item expiration date, if one applies. Default work item expiration dates can be set when IdentityIQ is configured.
Priority	The severity of the work item.
History	Any historical information attached to this work item.

Table 5—Policy Violation Work Item Description

Category	Description
Comments Button	
Comments	This section contains any comments that the requester of the work item or the assignee entered. When new comments are added, the requester and the assignee are notified. This notification provides a communication and tracking mechanism for this work item.
Address the following policy violation:	
Identity name	The user name or login ID of the identity that is in violation of the policy.
Policy	The policy type, Separation of Duty, Activity, Account, or Risk.
Policy Description	The description of the policy as entered when the policy was created.
Policy Violation Owner	The name of the person who owns this violation.
Rule	The name of the rule that caused the policy to be in violation.
Rule Description	The description of the rule that was broken.
Compensating Control	Any compensating controls associated the policy. For example, in some cases managers may be exempt for certain separation of duty policies.
Correction Advice	Any correction advice associated with the policy. This advice is added when the policy is created.
Score Weight	The risk score assigned to this violation. This score is used for identity risk score generation. **Note: Risk scores for policy violations are configured in the Risk Scoring Configuration feature, in Identities > Identity Risk Model**
Go to violation	A link to the policy violation page.
Policy Violation Page	
Summary	Details of the policy and the rule that caused the violation.
Violation Decision	Can include Allow, Revoke, and Certify. Only available on work items created by a business process. The action enabled by the business process used to create this work item.

The Policy Violation View Work Item page can have the following action buttons:

- **Forward** — Displays the Forward Work Item dialog enabling you to forward the work item to another user or workgroup.
  You can enter the first few letters of a name in the **Forward To** field to display a pop-up menu of IdentityIQ users and workgroups with names containing that letter string. Select a name from the list and add your comments.
- **Add Comment** — Inserts a comment about the work item or policy violation.
  When you add comments to work item, the requester of the work item is notified. This notification provides a communication and tracking mechanism for the work item because all comments are stored and displayed until the work item is complete.
- **Complete** — Displays a dialog where you can add comments prior to closing the work item and marking it as complete.
- **Back To Home** — Returns you to the Policy Violations list page. If you do not have access to that page, your IdentityIQ Home page is displayed.

Chapter 2: Define Policies

Policies are composed of rules used to enforce any policies, separation of duty, activity or risk, defined within your enterprise. Policies are defined and used to monitor for identities that are in violation of those policies. For example, a separation of duties policy (SOD) can disallow one identity from requesting and approving purchase orders. An activity policy can disallow an identity with the Human Resource role from updating the payroll application even though the identity has view access to that application.

Custom policies are any policies that were created outside of IdentityIQ to meet special needs of your enterprise. You cannot create a custom policy from inside the product. Use the Edit Policy page to view information about a custom policy. However, changes made here do not impact the performance of the policy.

Note: Access to the Policies page requires IdentityIQ administrative capabilities.

To access Policies, click **Setup > Policies**.

This chapter has the following topics:

- Policies Page — Define new policies, and view existing policies
- Edit Policy Page — Create or edit policies
- Policy Rules — Create or edit policy rules
- Working with Policies — How-to tasks

Policies Page

Use the Policies page to create new policies and view or edit existing policies. To find specific policies to view or edit, you can search by policy name and policy type. Enter a letter or partial name in the **Policy Names** field to display any policies with names beginning with that letter pattern.

To create a new policy, click **New Policy** and choose a policy type. (Policy types are defined in Table 6)

Before you make a policy active in your production environment, you can run a simulation to test the enabled rules that are defined in the policy. See “Policy Simulation” on page 15.

Table 6—Policies Page Column Definitions

Column Name	Description
Name	The name of the policy.

Table 6—Policies Page Column Definitions

Column Name	Description
Type	The type of policy. **SOD** – separation of duties policies ensure that identities are not assigned conflicting roles. **Entitlement SOD** — separation of duties policies ensure that identities are not assigned conflicting entitlements. **EffectiveEntitlementSOD** — ensure that identities are not assigned conflicting entitlements indirectly, through other objects. **Activity** — ensure that users are not accessing sensitive application if they should not or when they should not. **Account** — ensure that an identity does not have multiple accounts on an application. **Risk** — ensure that users are not exceeding the maximum risk threshold set for your enterprise. **Advanced** — custom policies created using match lists, filters, scripts, rules, or populations.
Description	A brief description of the policy as entered when it was defined.
State	The status of the policy. **Active** — the policy is currently being used. **Inactive** — the policy is not being used.

Edit Policy Page

Use the Edit Policy page to create new policies and to edit existing policies. The Edit Policy page contains the following information:

Table 7—Edit Policy Page Field Description

Field Name	Description
Name	A descriptive name of this policy. This is the name that displays on the Policies page.
Owner	The owner of the policy. The policy owner serves as the “fallback” owner if a Policy Violation Owner (that is, the person responsible for taking action on the policy violations arising from this policy) is not specified. If the notification option is enabled as part of policy, the policy owner receives an email notification for each violation of the policy by default. Entering the first letter, or letters, of a name or workgroup displays a selection list of valid users and workgroups with names containing that letter string.

Table 7—Edit Policy Page Field Description

Field Name	Description
Policy Violation Owner	The owner of the violations arising from this policy, that is, the person responsible for taking action on the policy violations. This can be a specific identity, the manager of the user in violation of the policy, or someone selected according to a rule. You can also assign owners to each individual rule that makes up the policy. If you assign an owner at the rule level, it overrides the policy-level violation owner. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.** If the notification option is enabled, only the owner receives a work item, the observers only receive email notifications.
Scope	If scoping is enabled in your system, you can set a scope for this policy. If scoping is not enabled, you will not see this option. If a scope is assigned, only the owner of the policy and users who control the designated scope can see this policy on the Policies page. The scope assigned to the policy does not impact the way violations are displayed, reported, or monitored. Depending on configuration settings, objects with no scope assigned might be visible to all users with the correct capabilities.
Description	A brief description of the policy and its use in your organization. To enter description in multiple languages, use the language selector . The drop-down list displays any languages supported in your instance of IdentityIQ. The description displayed throughout the product is dependent on the language associated with the user's browser. If only one description is entered, that is the description used by default. **Note: You must Save each description before changing languages to enter another description.**
Violation formatting rule	If you want to use a rule to control violation formatting, select a violation rule from the drop-down list. Violation formatting rules are defined when your system is configured. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**
Violation business process	Business processes can be used to define how violation work items are assigned, or how to handle the violation based on decision made on the work item. If you want to use a business process for the violation, select the business process from the drop-down list. A business process specified here for the entire policy will be overwritten by any business process that is specified as part of a policy rule on the Edit Rule pages.
State	The state of the policy: **Active** — use the policy to monitor roles or activity. **Inactive** — do not use the policy to monitor role or activity at this time.

Table 7—Edit Policy Page Field Description

Field Name	Description
Send Alerts	Activate to display the Alert Properties section. You can set alerts to be sent by email and a work item opened each time a violation is detected.
Alert Properties: Not all of the alert property options are visible initially. This section expands as options are activated.	
Initial Notification Email	The email template used for the initial notification of the policy violation and work item assignment.
Escalation	Specify a level of escalation for this policy. **None** — after the initial alert no further messages are sent and the work item is never escalated. **Send Reminders** — email reminders are sent periodically until the work item is complete. **Reminders then Escalation** — email reminders are sent periodically until the work item is complete or, if the work item is not completed in a timely manner, the work item is escalated. **Escalation Only** — the work item is escalated after a specified time period with no notifications or warning being sent.
Open Work Item	Select to automatically generate a work item for this violation.
Days Before First Reminder	The number of days after which the first email reminder is sent.
Reminder Frequency	The number of days, or interval, between email reminders being sent.
Reminder Email Template	Template used to format the reminder email. If none is selected, a system default is used.
Reminders Before Escalation	Maximum number of reminders to send before escalation begins. If this field is set to zero, no reminders are sent and escalation begins immediately.
Escalation Owner Rule	The rule used to determine the new owner of the escalated work item.
Escalation Email	Template used to format the escalation email.
Observers	Identities to whom the email notifications and work items are sent. Enter the first letter, or letters, of an identity name to display the suggest list or click the arrow to the right of the field to display all identities and select from the list. Select as many observers as required.
Rule Table	A list of the rules contained in this policy and a description of each. Click on a rule to access the edit rule pages. Account and Risk policies do not have a separate rule page.

Policy Simulation

Before you make a policy active in your production environment, you can run a simulation for:

- All enabled rules in policy — Click **Run Simulation** next to the **Cancel** button. To view the number of violations, click **View Simulation**.
- A single rule in a policy with multiple rules — Click the **Run Simulation** link next to the rule. To view the number of violations, click the **View Simulation** link.

Note: Policy simulation runs a background task that iterates over all identities to determine if a policy violation occurs for the rule or policy. This process can be time consuming and resource intensive, depending on the complexity of the policy definition and the number of identities and accounts.

When you run a simulation on a policy, the policy is saved and the test is run for all the enabled rules. The rule or rules are disabled and the status of the policy is changed to **Inactive**. To activate the policy, you must edit the policy, change the state to **Active** and save the changes to the policy.

Note: Before testing the rule, make sure the names of rules are unique in a policy. When you run a simulation for a single rule, only the rule is disabled. The state of the policy is NOT changed. When you run a simulation for all the enabled rules in a policy, the state of the policy is changed to inactive. To activate the policy, you must change the state to Active and save the changes to the policy.

To work with the rules for each policy type, see “Policy Rules” on page 15.

Policy Rules

Rules are used to enforce policies. Violations on each rule in a policy, when detected, are stored in the Identity Cube. These violations also appear on identity score cards and enable you to identify high-risk employees and respond. You can configure policy violations to trigger a business process that immediately sends email notifications and generates work items when a violation is detected. Policy violations can be managed through certifications or through the policy violations page.

You can use the simulation option to simulate the policy rule before you make it active in your production environment. See "Policy Simulation" on page 15.

This section has the following topics:

- Edit SOD Rule Page
- Edit Activity Rule Page
- Edit Advanced Policy Rule Page

Edit SOD Rule Page

Use the Edit SOD Rule page to define new rules for separation of duty polices or edit existing rules. Rules are used to monitor roles or entitlements for conflicts of interest. This enables you to identify high-risk employees and take the appropriate action as needed.

To create or Edit a policy, see “How to Create or Edit a Separation of Duty Policy” on page 22.

To access the Edit SOD Rule Page, navigate to **Setup > Policies**, select the **SOD Policy** you want to edit, then scroll down to the bottom of the page. Select an existing rule from the table, or click **Create New Rule.** The following information is displayed on an Edit SOD Rule page:

Table 8—Edit SOD Rule Page Field Descriptions

Field Name	Description
Summary	A brief summary of this rule. This information is displayed in the **Rules** column of the Rules table on the Edit Policy page.
Description	A brief description of the rule.
Policy Violation Owner	The owner of the violations arising from this policy, that is, the person responsible for taking action on the policy violations. This can be a specific identity, the manager of the user in violation of the policy, or someone selected according to a rule. You can also assign owners to each individual rule that makes up the policy. If you assign an owner at the rule level, it overrides the policy-level violation owner. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.** If the notification option is enabled, only the owner receives a work item, the observers only receive email notifications.
Violation formatting rule	If you want to use a rule to control violation formatting, select a violation rule from the drop-down list. Violation formatting rules are defined when your system is configured. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**
Violation business process	Business processes can be used to define how violation work items are assigned, or how to handle the violation based on decision made on the work item. If you want to use a business process for the violation, select the business process from the drop-down list. A business process specified here for the entire policy will be overwritten by any business process that is specified as part of a policy rule on the Edit Rule pages.
Disabled	Enable or disable the rule
Compensating Control	A description of exceptions or compensating factors that apply to this rule. For example, certain policies or rules might not apply to users at the executive level in your organization. **Note: This field is for documentation purposes only. Information entered here does not impact risk scoring associated with this rule or the reporting of policy violations.**
Correction Advice	Text entered in this field is displayed if a violation of this policy appears on a certification request and is selected for revocation. Use this field to enter information that can be used by a certifier to make the correct revocation decision.
Role SOD Rules:	

Table 8—Edit SOD Rule Page Field Descriptions

Field Name	Description
Any of these roles/entitlements conflict with any of these roles/entitlements	The lists of conflicting roles that define this rule. If an identity is assigned ANY of the roles from the **Any of these** table and ANY of the roles from the **conflict with any of these** table, they are in violation of this rule and their risk score card reflects that violation. Each table can contain multiple items, but if a user has even one role in each list it is a violation of the policy.
Entitlement SOD Rule:	
First Entitlement Set Second Entitlement Set	The list of conflicting entitlements that define this rule. Add identity attributes or account attributes and permissions to create lists of conflicting entitlements. Use the **Or/And** drop-down list to determine if an identity has to match all of the items in the list or just one to be in violation of this policy.
Effective Entitlement SOD Rule:	
First Entitlement Set Second Entitlement Set	The list of conflicting entitlements that define this rule. Add identity attributes, account attributes and permissions, and target permissions to create lists of conflicting entitlements. Use the **Or/And** drop-down list to determine if an identity has to match all of the items in the list or just one to be in violation of this policy.
Run or View Simulation	Use the simulation option to simulate the policy rule before you make it active in your production environment. **Note: Before testing the rule, make sure the names of rules are unique in a policy. When you run a simulation for a single rule, only the rule is disabled. The state of the policy is NOT changed.** **When you run a simulation for all the enabled rules in a policy, the state of the policy is changed to inactive. To activate the policy, you must change the state to Active and save the changes to the policy.**

Edit Activity Rule Page

Use the Edit Activity Policy Rule page to define new rules for activity polices or edit existing rules. Rules are used to monitor the activities performed by users within your enterprise.

To create or Edit a policy, see "How to Create or Edit an Activity Policy" on page 22.

To access the Edit Activity Rule Page, navigate to **Define > Policies**, select the **Activity Policy** and then scroll down to the bottom of the page. Select an existing rule from the table or click **Create New Rule.** The following information is displayed on the Edit Activity Policy Rule page:

Table 9—Edit Activity Policy Rule Page Field Descriptions

Field Name	Description
Activity Rule:	
Summary	A brief summary of this rule. This information is displayed in the **Rules** column of the Rules table on the Edit Policy page.

Table 9—Edit Activity Policy Rule Page Field Descriptions

Field Name	Description
Description	A brief description of the rule.
Policy Violation Owner	The owner of the violations arising from this policy, that is, the person responsible for taking action on the policy violations. This can be a specific identity, the manager of the user in violation of the policy, or someone selected according to a rule. You can also assign owners to each individual rule that makes up the policy. If you assign an owner at the rule level, it overrides the policy-level violation owner. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.** If the notification option is enabled, only the owner receives a work item, the observers only receive email notifications.
Violation formatting rule	If you want to use a rule to control violation formatting, select a violation rule from the drop-down list. Violation formatting rules are defined when your system is configured. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**
Violation business process	Business processes can be used to define how violation work items are assigned, or how to handle the violation based on decision made on the work item. If you want to use a business process for the violation, select the business process from the drop-down list. A business process specified here for the entire policy will be overwritten by any business process that is specified as part of a policy rule on the Edit Rule pages.
Disabled	Enable or disable the policy.
Compensating Control	A description of exceptions or compensating factors that apply to this rule. For example, certain policies or rules might not apply to users at the executive level in your organization. **Note: This field is for documentation purposes only. Information entered here does not impact risk scoring associated with this rule or the reporting of policy violations.**
Corrective Advice	Text entered in this field is displayed if a violation of this policy appears on a certification request and is selected for revocation. Use this field to enter information that can be used by a certifier to make the correct revocation decision.
Identity Filters: Enable you to identify which types of identities should be considered when scanning activities for violations of this policy. These filters can be grouped and controlled using AND\OR operations and be as simple or complex as needed. The Add a Filter box is used to create the individual filters, the Filter(s) box is used to view and manipulate the existing filters.	
Operation	The operation used to control the interaction between the filters.

Table 9—Edit Activity Policy Rule Page Field Descriptions

Field Name	Description
Field	A distinguishing characteristic associated with the identity type for which you are searching. The drop-down list contains all of the categories by which identities can be differentiated.
Search Type	The qualifier associated with the attribute value. For example, `equals` or `is like`. The choices in this drop-down list are dependent on the Field specified.
Value	The value of the attribute.
Ignore Case	Specifies if case should be a factor when scanning for the value specified.
Activity Filters: Enable you to select which types of activities should be considered violations of this policy. You can also choose Time Periods in order to define when this activity is considered a violation of this policy.	
Time Periods	The time periods during which the activity is in violation of the policy. For example, if someone is logging into a sensitive application on the weekends or during non-office hours it might be a violation. The time periods are configured during the deployment of IdentityIQ.
Operation	The operation used to control the interaction between the filters.
Field	A distinguishing characteristic associated with the action for which you are searching. For example, start or end date, or the data source on which the action occurred.
Search Type	The qualifier associated with the field value. For example, `equals` or `is like`. The choices in this drop-down list are dependent on the Field specified.
Value	The value of the attribute.
Ignore Case	Specifies if case should be a factor when scanning for the value specified.
Run or View Simulation	Use the simulation option to simulate the policy rule before you make it active in your production environment. **Note: Before testing the rule, make sure the names of rules are unique in a policy. When you run a simulation for a single the rule, only the rule is disabled. The state of the policy is NOT changed.** **When you run a simulation for all the enabled rules in a policy, the state of the policy is changed to inactive. To activate the policy, you must change the state to Active and save the changes to the policy.**

Edit Advanced Policy Rule Page

Use the Edit Advanced Rule page to define new rules for advanced polices, or to edit existing rules. Advanced rules are used to create custom, violation monitoring based on a variety of entitlement, filters, scripts, rules, and populations.

To create or edit a policy, see "How to Create or Edit an Advanced Policy" on page 23.

The following information is displayed on the Edit Advanced Rule page:

Table 10—Edit Advanced Policy Rule Page Field Descriptions

Field Name	Description
Advanced Rule:	
Summary	A brief summary of this rule. This information is displayed in the **Rules** column of the Rules table on the Edit Policy page.
Description	A brief description of the rule and its use in your organization.
Violation formatting rule	If you want to use a rule to control violation formatting, select a violation rule from the drop-down list. Violation formatting rules are defined when your system is configured. **Note: Click the "..." icon to launch the Rule Editor to make changes to your rules if needed.**
Violation business process	Business processes can be used to define how violation work items are assigned, or how to handle the violation based on decision made on the work item. If you want to use a business process for the violation, select the business process from the drop-down list. A business process specified here for the entire policy will be overwritten by any business process that is specified as part of a policy rule on the Edit Rule pages.
Disabled	Enable or disable the policy.
Compensating Control	A description of exceptions or compensating factors that apply to this rule. For example, certain policies or rules might not apply to users at the executive level in your organization. **Note: This field is for documentation purposes only. Information entered here does not impact risk scoring associated with this rule or the reporting of policy violations.**
Corrective Advice	Text entered in this field is displayed if a violation of this policy appears on a certification request and is selected for revocation. Use this field to enter information that can be used by a certifier to make the correct revocation decision.
Selection Method: **The selection method used when scanning for and assigning policy violations.**	
Match List	A list of entitlements that define a policy violation. An identity that is assigned the entitlements in this list is in violation of this policy.
Filter	A custom filter (XML database query) used to define a rule for this policy.
Script	A custom script used to define a rule for this policy.
Rule	The rule selected from the rules list.
Population	A population of users. Populations are based on saved queries from the Advanced Analytics feature.

Table 10—Edit Advanced Policy Rule Page Field Descriptions

Field Name	Description
Run or View Simulation	Use the simulation option to simulate the policy rule before you make it active in your production environment. **Note: Before testing the rule, make sure the names of rules are unique in a policy. When you run a simulation for a single the rule, only the rule is disabled. The state of the policy is NOT changed.** **When you run a simulation for all the enabled rules in a policy, the state of the policy is changed to inactive. To activate the policy, you must change the state to Active and save the changes to the policy.**

Working with Policies

To create a new policy, use the **New Policy** drop-down menu. Select a type from the drop-down menu to display the Edit Policy page. To work with an existing policy, click on that policy row in the table or right-click on the policy and select **Edit** from the drop-down menu.

To remove a policy, right-click on the policy and select **Delete** from the drop-down menu.

This section includes the following topics:

- How to Create or Edit a Risk Policy
- How to Create or Edit an Account Policy
- How to Create or Edit a Separation of Duty Policy
- How to Create or Edit an Activity Policy
- How to Create or Edit an Advanced Policy

How to Create or Edit a Risk Policy

Use the SailPoint-provided risk policy to set a maximum risk threshold for identities before they are considered in violation of your compliance standards. From the Policies page, click the risk policy in the Policies table to display the Edit Policy page and enter the **Composite score threshold**.

See “Policies Page” on page 11 and “Edit Policy Page” on page 12

You can create multiple risk policies, but only one can be operational within IdentityIQ at any time.

How to Create or Edit an Account Policy

Use the SailPoint provided account policy to ensure that no identities have multiple accounts on any of the applications within your enterprise. Use the Edit Policy page to activate the account policy and add information such as a name and owner.

See “Policies Page” on page 11 and “Edit Policy Page” on page 12

How to Create or Edit a Separation of Duty Policy

Separation of Duties (SOD) policies are created using the Edit Policy and Edit SOD Rule pages. Use this procedure to create new policies or edit existing ones.

Procedure

1. Click **Setup > Policies**.
2. ***Optional***: If you are editing an existing policy, you can use the search options to search by policy name and policy type.
3. Select Role SOD, Entitlement SOD, or Effective Entitlement SOD from the **New Policy** drop-down list, or click on an existing policy to display the Edit Policy page.
4. Enter the policy information.
   See "Edit Policy Page" on page 12 for detail description of the Edit Policy page.
5. Right-click on a rule or select **Create New Rule** to display the Edit SOD Rule page.
6. Enter the SOD Rule information in the top portion of the page. See "Edit SOD Rule Page" on page 15 for detailed descriptions of those fields.
7. Do one of the following: Select a role from the Add Role drop-down list below the Any of these roles table.
   a. Select a role from the Add Role drop-down list below the Any of these roles table.
   b. Select a role from the Add Role drop-down list below the conflict with any of these roles table.

   The drop-down list contains all of the roles defined for your organization. You can enter as many roles as are needed to build this rule.

   — OR —

   a. Select an application and use the Add Attribute or Add Permission buttons to build the First Entitlement Set.
   b. Select an application and use the Add Attribute or Add Permission buttons to build the Second Entitlement Set.

      For attributes select an attribute from the drop-down list and type a value.
      For permissions, type the name (target) and value (right).
      You can enter as many attributes and permissions as needed to build this rule.
8. Click **Done** to return to the Edit Policy page.
9. Repeat steps 5 thru 8 until all of the rules needed for this policy have been added or modified.
10. Click **Save** to save the policy and return to the Policies page.

How to Create or Edit an Activity Policy

Advanced policies are created using the Edit Policy and Edit Activity Policy Rule pages. Use this procedure to create new policies or edit existing ones.

Procedure

1. Click **Setup > Policies**.
2. ***Optional***: If you are editing an existing policy, you can use the search options to search by policy name and policy type.
3. Select Activity Policy from the **New Policy** drop-down list, or click on an existing policy to display the Edit Policy page.

4. Enter the policy information. See "Edit Policy Page" on page 12 for detail description of the Edit Policy page.
5. Click on a rule or **Create New Rule** to display the Edit Activity Policy Rule page.
6. Enter the Activity Policy Rule information in the top portion of the page. See "Edit Activity Rule Page" on page 17 for detailed descriptions of those fields.
7. Create the filters necessary to identify the identity and activity types that should be considered when performing the policy scans for this violation.
   Use the Identity Filters and Activity Filters panels to add and combine filters for use in the policy. Apply qualifiers to filters to limit the values returned and then use grouping, AND\OR operations, and time periods to create the rules that make up the policy.

   Add a Filter:

   Create the filters that make up the rules.

   - **Field** — select an attribute value from the drop-down list.
   - **Search Type** — the qualifier to associate with the value, for example equals or like.
   - **Value** — the value of the field selected.
   - **Ignore Case** — specifies if case should be factored into the query.

   Filter(s):

   The Operations drop-down list enables you to specify AND/OR relationships between the filters in the list. Select multiple filters and group them to create sub-filters and use multiple layers of filter grouping to create complex rules.

   Click view/edit filter source to display an editable text version of the filter.

   See the online help or the IdentityIQ *User's Guide* for details on using the advanced filtering functions.
8. Click **Done** to save the new policy and return to the Edit Policies page.

How to Create or Edit an Advanced Policy

Policies are created using the Edit Policy and Edit Activity Policy Rule pages. Use this procedure to create new policies.

Procedure

1. Click or mouse over the Define tab and select **Policies**.
2. ***Optional***: Use the filtering options to limit the number of policies displayed in the table.
   You can filter by both policy name and policy type.
3. Select Advanced Policy from the **Create new policy** drop-down list or click on an existing policy to display the Edit Policy page.
4. Enter the policy information.
   See "Edit Policy Page" on page 12 for detail description of the Edit Policy page.
5. Click **Create New Rule** or right-click on an existing rule to display the Edit Advanced Rule page.
6. Enter the Advanced Rule information in the top portion of the page. See "Edit Advanced Policy Rule Page" on page 19 for detailed descriptions of those fields.

7. Select a method by which to generate this rule. In other words, any condition you define here is considered a violation of this policy:
   - **Match List** — define a list of entitlements to determine the rule.
     For attributes, select an attribute from the drop-down list and type a value.
     For permissions, type the name (target) and value (right).
   - **Filter** — enter a custom XML database query to define user for this rule.
   - **Script** — enter a custom script to define the rule. Scripts are similar to rules, but the source is stored with the policy and can be edited from this page.
   - **Rule** — select an existing rule from the drop-down list.
   - **Population** — select a population from the list. Any identity that matches the criteria defined for the population displayed is in violation of this policy.
8. Click **Done** to save the new policy and return to the Edit Policies page.