Policy Management

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

About Policies and Policy Violations

Policies in IdentityIQ check identities for certain conditions that are unwanted, or even considered dangerous. Examples include:

- 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
- cross-application combinations of permissions.

Most policies in IdentityIQ use **rules** to define the conditions of the policy. In some cases, a policy rule will be very simple - for example, if a user has a certain role, they may not also have a certain other role. In other cases, policy rules can be more complex, using filtering, matching, scripts, or rules that use BeanShell code to define the policy's requirements. Risk policies and Account policies check for a specific condition, such as a specific risk score, or whether a user has multiple accounts on a specific application, rather than using rules. See Types of Policies for more information about the kinds of policy rules you will use for different types of policies.

Policy violations occur when an identity is found to be in violation of an active policy. The person or workgroup responsible for the policy violation can take action to revoke or allow the access that violates the policy.

Each policy must have a **policy owner**, which is an individual or workgroup responsible for defining and maintaining the policy itself.

Policies also typically have a **policy violation owner**. This is a person or workgroup that is responsible for acting on policy violations and making decisions on access. The policy violation owner is configured as part of the policy definition, and can be a the manager of the identity that has a violation, a specific user or workgroup, or an identity that is selected via a rule. If no policy violation owner is defined in a policy, ownership of policy violations will default to the **policy owner**.

Policies are defined in **Setup > Policies**. Access to this option is typically restricted to users with **System Administrator** or **Policy Administrator** capabilities, though this can vary based on how your instance of IdentityIQ has been configured.

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. See the Overview of the Policy Violations Page for more details.

How Policies Work

Policies are evaluated per identity. An evaluation can be triggered during aggregation, Identity Cube refresh, a specialized task (such as a dedicated refresh task), or as part of the Lifecycle Manager access request process.

In IdentityIQ, policies can be both **detective** and **preventive**.

Detective Policies

Policies are **detective** when they find and flag any access that already exists and is in violation of your business rules. In IdentityIQ, the Refresh Identities task checks all identities against policies, and marks the ones that are in violation of your active policies. Evaluation during aggregation can also be a detective way of finding violations.

To enable policy evaluation during aggregation or during an Identity Refresh task, the **Check active policies** option must be selected in the aggregation or refresh task. See the **Tasks** documentation for more information.

Preventive Policies

Policies can also be **preventive**, helping you spot and avoid the granting of problematic access before it occurs. Users can be alerted to violations at the time access is requested, and when it is approved. Making policies preventive is *optional*, and is configured using a business process for provisioning. This configuration is optional because there might be some cases, such as when using a Separation of Duties policy, when you do not want to let users know which access combinations can provide an opportunity for fraud or for circumvention of security controls. The out-of-the-box business process that manages this behavior is LCM Provisioning, but you can implement your own business processes as needed, using LCM Provisioning as a model.

IdentityIQ's **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. See the Overview of the Policy Violations Page for more details.

Detective Policy Evaluation

Detective policy evaluation is triggered as part of an aggregation or a task that refreshes identities (such as an Identity Refresh task).

For policy evaluation during aggregation, select the option **Check active policies** in the aggregation task to include policy evaluation as part of the task.

For policy evaluation during an Identity Refresh task, the same option, **Check active policies**, must be selected. In an Identity Refresh task there are two additional options for evaluation during the task:

- **Keep previous violations** keeps all existing violations, even if they are found to be resolved or do not match any active policy.
- **A comma separated list of policy names**. Entering a list of policies in this field means the task will check only the listed policies that are active; leaving this field blank tells the refresh task to check all active policies. Note that if a policy is included in this field but is inactive, it will not be evaluated as part of the task.

Preventive Policy Evaluation

When the Lifecycle Manager module (LCM) is licensed and installed, IdentityIQ can check for policy violations as soon as an access request is submitted. Out-of-the-box business processes like **LCM Provisioning** (used for access requests) and **LCM Create and Update** (used for creating and editing identities) have options to control the policy checking during requests.

The LCM Provisioning business process, for example, includes the following options. These are on the **Process Variables** tab of the business process, in the **Policy Checking** section.

Policy Settings

- **Disable Policy Checking**: No policies are checked. Even if the request would result in a violation, it will not be detected. Approvers will not be presented with any violation details.
- **Continue on Policy Violations**: If a violation is found, any approver will see the violation and can choose to take action if necessary.
- **Present Failures to Requester**: If a violation is found it is presented to the requester. The requester can then remove any items from the request that are causing a violation. If the requester submits the request for approval with violations, any of the approvers will see these violations and can choose to take action if necessary.

- **Fail Workflow**: If a violation is found, the request process is terminated with an error message.

Policies to Check

Choose **All** to check all active policies, or choose **Selected** to specify which policies you want to check during provisioning. Note that only *active* policies are evaluated.

Types of Policies

IdentityIQ supports these types of policies. Each policy can contain one or more policy rules that make up the entire policy.

Role SOD Policy

This separation of duties (SOD) policy type checks for any conflicting roles that an identity could have. The policy rules define two side-by-side lists, where any rule from the left-side list cannot be combined with any rule from the right-side list. For example the roles “Payment” and “Payment Approval” could be conflicting roles; in this example, the left-side list would contain “Payment” and the right-side list would contain “Payment Approval”. The roles in either list can be of any role type.

Entitlement SOD Policy

This separation-of-duties policy type checks for conflicting entitlements within an application or across applications. This is similar to the Role SOD Policy, but is used for values of application attributes that are marked as entitlements in the application schema. The policy rules are defined as two entitlement sets: “First Entitlement Set” and “Second Entitlement Set”. These sets are more advanced than the role sets of the Role SOD Policy type: the sets can use multiple levels of and/or expressions to combine entitlements within one set.

Effective Entitlement SOD Policy

An effective entitlement SOD policy is similar to an entitlement SOD policy, but it checks for effective entitlements rather than direct entitlements. Effective entitlements are any indirect access that was granted through another object, such as a nested group, an unstructured target, or another role.

Activity Policy

When Activity Data Sources are enabled on one or more applications this policy type can be used to check for any undesirable activities, such as login, logout, or creation or deletion of accounts. An activity rule can first select identities to check using a set of filters. Identities matching these criteria are now evaluated using the defined activity filters. An activity policy scans activity data for specific events, with the option to select time frames, source and target applications, and more.

Account Policy

Account policies only have a single policy rule: they check whether an identity has multiple accounts on an application.

Risk Policy

Risk policies check for any identity with a composite risk score equal to or higher than the configured threshold. Like the account policy, this type of policy will only have a single policy rule.

Advanced Policy

An advanced policy handles situations where the other types do not suffice. An advanced policy can contain multiple types of rules using match lists, filters, scripts, BeanShell rules, or populations, which allows for greater flexibility.

Compensating Controls and Correction Advice

At the rule level, policies can include text describing **Compensating Controls** and **Correction Advice**, which can help policy violation owners resolve violations correctly, according to your organization's business rules. This text is informational only; it can help explain what the violation owner should know or do, but does not supply any automated logic that IdentityIQ will enforce.

Compensating Controls give 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.

Correction Advice is information that can be used by a policy violation owner to make the correct decision on the violation.

The policy violation owner sees this information in the **Details** view of the policy violation. The **Details** view is accessed through the three-line icon on each policy violation.

Notifications, Reminders, and Escalations for Policies

Every policy can be configured to send notifications, escalations, and reminders to the policy violation owner. By default, these options are disabled when you define a new policy.

To enable them, check the **Send Alerts** option in the policy.

Once the **Send Alerts** is checked. options for configuring specific behavior for notifications, reminders, and escalations are shown.

Notifications

Notifications let a policy violation owner know when a there is a policy violation awaiting action. Use the Initial Notification Email field to choose an email template to use for notifying violation owners. If you do not choose an email template, then notifications are not sent; in other words, leave this field blank if you do not want to send notifications. IdentityIQ provides an out-of-the-box email template called Policy Violation for notifications, but you can create and use your own email templates as needed. See the IdentityIQ **System Configuration** documentation for more information.

Reminders and Escalations

Reminders can be sent to the policy violation owner if the policy violation has not been addressed within a specified timeframe. **Escalations** transfer control of the policy violation to someone else, such as the policy violation owner's manager, or the application owner, if the person originally responsible for the policy violation has not completed it within a specified timeframe. The new owner of the item, when it is escalated, is determined by a rule.

For detailed information on configuring notifications, reminders, and escalations, see Editing PoliciesEditing Policies

Testing Policies

You can test the behavior and outcomes of your policies and policy rules by running a **simulation** of the policy. When you run simulations, the simulation tests the policy or policy rule against every identity in your system; however, it does not mark any identities as being in violation, create work items for remediating violations, or provide a list of identities in violation. It only gives you a count of the identities that are in violation of the policy or policy rule.

There are **Run Simulation** options at both the policy level, and the policy rule level. To run a simulation, click **Run Simulation** and confirm that you want to run the simulation. Running a simulation on a policy or policy rule auto-

matically **disables** it, making it inactive; be sure that both the policy and policy rules have been reactivated when your testing is done.

To view the results of the simulation, open the policy and click **View Simulation**. (The **View Simulation** button replaces **Run Simulation** is replaced when a simulation is run.)

See Policy Simulation for more details.

You can also set a policy's state as **Active** or **Inactive**, giving you the opportunity to work iteratively on a policy, or temporarily suspend it while making updates, without impacting your daily operations. It is a good idea to leave policies inactive until you have assessed them and are certain they are functioning as intended. Individual policy rules within a policy can also be enabled or disabled as needed, without impacting other policy rules that may be part of the policy.

Best Practices for Policies

These are some general best practices for developing and using policies in your organization:

One Policy or Many?

A single policy can contain multiple policy rules. As you develop your policies, think about what belongs under one policy umbrella, versus what should be distinct. For example, you might create one policy for "Finance Department Role Conflicts" that could include many individual rules defining which roles cannot be shared within the Finance department. If your policies do not fit logically into categories, individual policies for each unique use case might be the right approach.

Names and Descriptions

Always provide user-friendly and intuitive names and descriptions for each policy and policy rule. The description of the policy (though not of the policy rules) can also be localized if you need multilingual translations. A good rule of thumb is that the policy name should indicate the purpose of the policy, and the policy rule name should indicate what the rule actually does.

Preventive Controls

Whether or not to alert requestors or approvers that granting certain access will result in a policy violation is something you can configure in the Lifecycle Management business process for provisioning. There may be some cases when you do not want to let users know which access combinations can provide an opportunity for fraud or for circumvention of security controls.

Test Policies and Policy Rules Before Activating Them

Fully testing policies before making them live is an essential step. See Testing Policies

Provide Useful Guidance

Every policy should include clear language about the policy's purpose, and how to manage violations. Policy rules include fields for giving important information and guidance to users. Be sure to provide meaningful and complete information with each rule, so that users have a clear understanding of the purpose of the rule and how to manage violations. See Compensating Controls and Correction Advice for more information.

Defining Policies

Policies are composed of general information about the purpose, ownership, and general behavior of the policy, and rules that are define how the policy works. Policies monitor for identities that are in violation of the rules defined in the policy. For example, a separation of duties policy 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.

> Access to the Policies page requires IdentityIQ administrative capabilities.

Policies Page

Click **Setup > Policies** to open the Policies page. This page lists any existing policies that are have been defined in your system, and includes a **New Policy** button for creating new policies. Options on this page to **Filter by Policy Name** and perform an **Advanced Search** help you quickly find existing policies.

- To edit a policy, click the policy to open it.
- To delete a policy, right-click on the policy and choose delete.
- To create a new policy, click **New Policy** and choose a policy type. See Types of Policies for more information.

The Policies page shows this information for all your existing policies.

Column Name	Description
Name	The name of the policy.
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	Select the state (Active or Inactive), indicating whether the policy should be evaluated or not during policy checks. **Active** — the policy is currently being used. **Inactive** — the policy is not being used.

Editing Policies

The **Edit Policy** page is where you create new policies, and edit existing policies.

In the **Edit Policy** page you can define the following information for your policy. You can also run a Policy Simulation from this page, and view, add, or open Policy Rules.

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 the 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.
Policy Violation Owner	The person responsible for taking action on the violations of this policy. 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 descriptions 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. You must **Save** each description before changing languages to enter another description.

Field Name	Description
Violation formatting rule	A violation formatting rule adds extra information to a policy violation, like an extra description, or the relevant applications that contain attributes that contributed to the violation. This can be especially relevant for advanced policies, for which IdentityIQ cannot always collect all information that may be relevant to the person who has to review the violation. 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	Select the state (Active or Inactive), indicating whether the policy should be evaluated or not during policy checks. **Active** — use the policy to monitor roles or activity. **Inactive** — do not use the policy to monitor role or activity at this time.
Send Alerts	Select this option 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. See Notifications, Reminders, and Escalations for Policies for more information.
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	Select to automatically generate a work item for this violation.

Field Name	Description
Item	
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.

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.

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 and Editing Policies

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 and Editing Policies

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.

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 general policy information. See Editing Policies
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 for detailed descriptions of those fields.
7. To create a rule based on **roles**:
    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.

8. To create a rule based on **attributes**:
    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.

9. Click **Done** to return to the Edit Policy page.
10. Repeat steps 5 through 9 until all of the rules needed for this policy have been added or modified.
11. 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.

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 general policy information. See Editing Policies.
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 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.

To 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, such as *equals* or *like*.

Value

The value of the field selected.

Ignore Case

Specifies whether case should be factored into the query.

Filter(s)

The Operations drop-down list lets you 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 for details on using the advanced filtering functions.

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.

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 general policy information. See Editing Policies.
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 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 identities 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.

For more information and examples for using Match Lists, Filters, Scripts, Rules, and Populations, see the IdentitySelectors in the IdentityIQ User Interface technical white paper on Compass.

Click **Done** to save the new policy and return to the Edit Policies page.

Policy Simulation

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.

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.

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.

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.

For information on working with the rules for each policy type, see Policy Rules.

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.

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 Working with Policies.

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:

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 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

Field Name	Description
	observers only receive email notifications.
Violation formatting rule	A violation formatting rule adds extra information to a policy violation, like an extra description, or the relevant applications that contain attributes that contributed to the violation. 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. 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. See Compensating Controls and Correction Advice.
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. See Compensating Controls and Correction Advice.
Role SOD Rules:	
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.
conflict with any of these roles/entitlements	
Entitlement SOD Rule:	

Field Name	Description
First 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.
Second Entitlement Set	
Effective Entitlement SOD Rule:	
First 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.
Second Entitlement Set	
Run or View Simulation	Use the simulation option to simulate the policy rule before you make it active in your production environment. 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 Working with Policies.

To access the Edit Activity Rule Page, navigate to **Setup > 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:

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.
Description	A brief description of the rule.
Policy Violation Owner	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

Field Name	Description
	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	A violation formatting rule adds extra information to a policy violation, like an extra description, or the relevant applications that contain attributes that contributed to the violation. 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. 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. See Compensating Controls and Correction Advice.
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. See Compensating Controls and Correction Advice.
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.	

Field Name	Description
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.
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 whether 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 whether 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. Before testing the rule, make sure the names of rules are unique in a policy.

Field Name	Description
	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.

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

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	A violation formatting rule adds extra information to a policy violation, like an extra description, or the relevant applications that contain attributes that contributed to the violation. This can be especially useful for advanced policies, for which IdentityIQ cannot always collect all information that may be relevant to the person who has to review the violation. 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.

Field Name	Description
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. 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. See Compensating Controls and Correction Advice.
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. See Compensating Controls and Correction Advice.

Selection Method:
The selection method used when scanning for and assigning policy violations.

For more information and examples for using Match Lists, Filters, Scripts, Rules, and Populations, see the IdentitySelectors in the IdentityIQ User Interface technical white paper on Compass.

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.
Run or View Simulation	Use the simulation option to simulate the policy rule before you make it active in your production environment. 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 Policy Violations

The users responsible for reviewing and mitigating policy violations use the **Policy Violations** page to see any violations awaiting their review and action.

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

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 these tabs and actions. 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.

Display Options

Use the **Filter** button 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.

Policy Violations Open Tab

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

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.
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

> You cannot take action on your own violations.

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

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	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

Decision	Description
	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. You cannot perform bulk violation revocations, and only Separation of Duties violations can be corrected.
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.
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.

These are the available options for specific policy types:

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

Policy Type	Available Policy Violation Options
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 these options:

Options	Description
Certify	You can select items in your list and click **Certify** to open the Schedule Certification page and 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 Violations in Certifications

Certifications can be configured to include policy violations. To include policy violations in a certification, the option **Include Policy Violations** must be selected in the certification configuration.

This applies to all *identity* certifications: Manager, Application Owner, Advanced, and Targeted certifications. It is also possible to set up a certification of only policies by selecting the **Include Policy Violations** option and also de-selecting these options in the certification configuration:

- Include Additional Entitlements
- Include Roles
- Include Target Permissions
- Certify Accounts With No Entitlements

For more information on certifications, see the **Certifications and Access Reviews** documentation.

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 below:

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.
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.

Category	Description
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. 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.

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.