Integrate Security Command Center Enterprise with ticketing systems

Send feedback

Enterprise service tier

This document explains how to integrate the Enterprise tier of Security Command Center with ticketing systems after configuring security orchestration, automation, and response (SOAR).

Integrating with ticketing systems is optional and requires manual configuration. If you use the default Security Command Center Enterprise configuration, you don't need to perform this procedure. You can integrate with a ticketing system later at any time.

Overview

You can track findings using the console and APIs with the default Security Command Center Enterprise configuration. If your organization uses ticketing systems to track issues, integrate with Jira or ServiceNow after you have configured your Google Security Operations instance.

Upon receiving findings for resources, the **SCC Enterprise – Urgent Posture Findings Connector** analyzes and groups them into new or existing cases, depending on the finding type.

If you integrate with a ticketing system, Security Command Center creates a new ticket every time it creates a new case for findings. Security Command Center automatically updates the related ticket whenever a case is updated.

A single case can contain multiple findings. Security Command Center creates one ticket for each case and synchronizes the case content and information with the corresponding ticket to let ticket assignees know what to remediate.

The synchronization between a case and its ticket works both ways:

- Changes within a case, such as a status update or new comment, are automatically reflected in the associated ticket.
- Similarly, ticket details synchronize back to the case, enriching it with information from the ticketing system.

Before you begin

Before configuring Jira or ServiceNow, provide a valid email address for the **Fallback Owner** parameter in the **SCC Enterprise – Urgent Posture Findings Connector**, and make sure that this email is assignable in your ticketing system.

Integrate with Jira

Make sure to complete all integration steps to synchronize the case updates with Jira issues and ensure the correct playbook flow.

A *case priority* is reflected in the Jira *issue severity*.

Create a new project in Jira

To create a new project in Jira for the Security Command Center Enterprise issues called **SCC Enterprise Project (SCCE)**, run a manual action in the case. You can use any existing case or simulate one. For more information about simulating cases, refer to the Simulate cases page in the Google SecOps documentation.

Creating a new Jira project requires Jira admin-level credentials.

> ★ **Note:** To create a new Jira project and configure the custom issue layout, use your Jira admin credentials.

To create a new Jira project, complete the following steps:

1. In the Google Cloud console, go to **Risk > Cases**.
2. Select an existing case or the one that you've simulated.
3. In the **Case Overview** tab, click **Manual Action**.
4. In the manual action **Search** field, enter `Create SCC Enterprise`.
5. In search results under the **SCCEnterprise** integration, select the **Create SCC Enterprise Cloud Posture Ticket Type Jira** action. The dialog window opens.
6. To configure the **API Root** parameter, enter the API root of your Jira instance, such as `https://YOUR_DOMAIN_NAME.atlassian.net`
7. To configure the **Username** parameter, enter the username that you use to sign in to Jira as an administrator.
8. To configure the **Password** parameter, enter the password that you use to sign in to Jira as an administrator.
9. To configure the **API Token** parameter, enter the API token of your Atlassian admin account that was generated in the Jira console.
10. Click **Execute**. Wait until the action is completed.

Optional: Configure custom Jira issue layout

1. Sign in to Jira as an administrator.
2. Go to **Projects > SCC Enterprise Project (SCCE)**.
3. Adjust and reorder issue fields. For more details about managing issue fields, see Configuring issue field layout in Jira documentation.

Configure Jira integration

> ★ **Note:** To configure the Jira integration, use credentials for a regular Jira user with permissions to create and update issues in the newly created project.

1. In the Google Cloud console, go to **Response > Playbooks** to open the Security Operations console navigation.
2. In the Security Operations console navigation, go to **Response > Integrations Setup**.
3. Select the **Default Environment**.
4. In the integration **Search** field, enter `Jira`. The **Jira** integration returns as a search result.
5. Click ⚙ **Configure Instance**. The dialog window opens.
6. To configure the **API Root** parameter, enter the API root of your Jira instance, such as `https://YOUR_DOMAIN_NAME.atlassian.net`
7. To configure the **Username** parameter, enter the username that you use to sign in to Jira. Don't use your admin credentials.
8. To configure the **API Token** parameter, enter the API token of your *non-admin* Atlassian account that was generated in the Jira console.
9. Click **Save**.
10. To test your configuration, click **Test**.

Enable the Posture Findings With Jira playbook

1. In the Google Cloud console, go to **Response > Playbooks** to open the Security Operations console **Playbooks** page.
2. In the Playbook **Search** bar, enter `Generic`.
3. Select the **Posture Findings - Generic** playbook. This playbook is enabled by default.
4. Switch the toggle to **disable the playbook**.
5. Click **Save**.
6. In the Playbook **Search** bar, enter `Jira`.
7. Select the **Posture Findings With Jira** playbook. This playbook is disabled by default.
8. Switch the toggle to **enable the playbook**.
9. Click **Save**.

Integrate with ServiceNow

Make sure to complete all integration steps to synchronize the updates of Google SecOps cases with ServiceNow tickets and ensure the correct playbook flow.

Create and configure ServiceNow custom ticket type

Make sure to create and configure the ServiceNow custom ticket type enable the Activities tab in the ServiceNow UI and avoid using the erroneous ticket layout.

Create ServiceNow custom ticket type

Creating a custom ServiceNow ticket type requires ServiceNow admin-level credentials.

To create a custom ticket type, complete the following steps:

1. In the Google Cloud console, go to **Risk > Cases**.
2. Select an existing case or the one you've simulated.
3. In the **Case Overview** tab, click **Manual Action**.
4. In the manual action **Search** field, enter `Create SCC Enterprise`.
5. In search results under the **SCCEnterprise** integration, select the **Create SCC Enterprise Cloud Posture Ticket Type SNOW** action. The dialog window opens.
6. To configure the **API Root** parameter, enter the API root of your ServiceNow instance, such as `https://INSTANCE_NAME.service-now.com/api/now/v1/`
7. To configure the **Username** parameter, enter the username that you use to sign in to ServiceNow as an administrator.
8. To configure the **Password** parameter, enter the password that you use to sign in to ServiceNow as an administrator.
9. To configure the **Table Role** parameter, leave the field empty or provide a value if you have one. This parameter only accepts one role value.

   By default, the **Table Role** field is empty. You must create a new custom role in ServiceNow to specifically manage the Security Command Center Enterprise tickets. Only ServiceNow users granted this new custom role have access to the Security Command Center Enterprise tickets.

   If you already have a dedicated role for users who manage incidents in ServiceNow and you'd like to use this role for managing the Security Command Center Enterprise findings, enter the existing ServiceNow role name in the **Table Role** field. For example, if you provide the existing `incident_handler_role` value, all of the users who are granted the `incident_handler_role` role in ServiceNow can access the Security Command Center Enterprise tickets.
10. Click **Execute**. Wait until the action is completed.