Filter

Vulnerabilities finding reference

Protect your AI applications
- Protect AI workloads with AI Protection
- Protect AI applications with Model Armor

Manage compliance and data security
- Assess and report compliance
- Compliance Manager
- Data security posture management

Enhance code security
- Configure Assured OSS support for VPC Service Controls
- Set up remote repository access
- Set up direct repository access
- Security metadata fields
- Access security metadata and verify packages
- Supported packages
- Review code-related security findings from Snyk

Use the Security Command Center API
- List security findings
- Add and manage security marks
- Create, manage, and filter Notification Configs
- Create and manage security sources and findings
- Discover and list assets

Monitor
- Audit logging

Troubleshoot
- Troubleshooting
- Configuration error findings
- Remediate configuration error findings
- Error messages
- FAQ

Assign tickets based on posture cases

Send feedback

On this page
- Overview
- Assign tickets automatically
  - Determining the resource owner
  - Creating cases and grouping findings
  - Creating and assigning tickets
- Assign tickets manually
  - Assign Jira issues in cases
  - Assign ServiceNow tickets in cases
- ...

Enterprise service tier

This page documents the mechanism of an automatic ticket assignment in Security Command Center Enterprise and explains how to manually assign or reassign tickets using the Security Operations console.

Overview

A ticket assignee is a person responsible for addressing and remediating the vulnerabilities. The ticket is assigned to the respective assignee automatically based on either the resource owner value inherited by the finding through the Google Cloud resource hierarchy or the value configured in the connector's **Fallback Owner** parameter.

Assign tickets automatically

The default automatic flow for assigning a ticket consists of the following steps:

1. Determining the resource owner of a finding.
2. Creating cases and grouping related findings into them.
3. Creating and assigning tickets based on cases.

Determining the resource owner

While ingesting and grouping findings into cases, the **SCC Enterprise - Urgent Posture Findings Connector** analyzes every finding for the resource owner and fallback owner values. The fallback owner value configured in the **Fallback Owner** connector parameter is the final option to ensure that a custom finding is assigned to a correct person for remediation when all other prioritized options failed.

For more information about defining the resource owner in Security Command Center Enterprise, refer to Determine ownership for posture findings.

Creating cases and grouping findings

After the connector has ingested a finding, Security Command Center forwards the finding to a new case if the finding is first of a kind, or an existing case if the finding parameters comply with a grouping mechanism. In a case, the finding becomes an *event* which the *alert* is based on. Essentially, an alert is a finding container that includes all information about a finding.

To learn more about how findings are grouped into cases, see Group findings in cases.

Creating and assigning tickets

Creating a case automatically creates a ticket in an integrated ticketing system. All information contained in a case is bidirectionally synchronized with a corresponding ticket, meaning that every time there is an update in a case like a new finding, a new comment, or a status change, the same update appears in the ticket and the other way around.

Security Command Center Enterprise automatically assigns the created ticket to the resource owner of findings grouped in a case. All findings in a case have the same resource owner.

Important: When using a ticketing system like Jira or ServiceNow to manage tickets, make sure to provide the assignable email (ldap) of the resource owner in your ticketing system, not the username.

Assign tickets manually

Assigning tickets manually in requires you to run manual actions on cases.

Assign Jira issues in cases

To manually assign a Jira issue in a case, complete the following steps:

1. In the Google Cloud console, go to **Risk > Cases**.
2. Select a case related to the ITSM ticket.
3. In the **Case Overview** tab, click **Manual Action**.
4. In the manual action **Search** field, enter `Jira`.
5. In the search results under the **Jira** integration, select the **Assign Issue** action. The action dialog window opens.
6. To configure the **Issue Key** parameter, enter the following placeholder: `[Case.Ticket_ID]`

   The placeholder dynamically retrieves the Jira issue ID corresponding to the selected case.

   a. To configure the **Issue Key** parameter for a specific issue, enter the **Jira issue ID** in the following format: `SCCE-NUMBER`

   You can find the issue ID in the Jira issue URL:

   ```
   https://YOUR_INSTANCE_NAME.atlassian.net/browse/ISSUE_I
   ```

7. To configure the **Assignee** parameter, enter the email address of the Jira ticket assignee.

   Alternatively, you can enter the name of the ticket assignee as it is displayed in Jira. The action supports using usernames or displayed names.

8. Click **Execute**.

Assign ServiceNow tickets in cases

To manually assign a ServiceNow ticket in a case, complete the following steps:

1. Retrieve the `sys_id` value to obtain the ServiceNow assignee ID.
2. Assign the ServiceNow ticket.

Retrieve the `sys_id` value

1. In the Google Cloud console, go to **Risk > Cases**.
2. Select a case related to the ServiceNow ticket.
3. In the **Case Overview** tab, click **Manual Action**.
4. In the manual action **Search** field, enter `ServiceNow`.
5. In the search results, select the **Get User Details** action. The action dialog window opens.
6. To configure the **Emails** parameter field, enter the email address of the ServiceNow ticket assignee.