Administration Guide

FortiSOC 26.2.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 17, 2026
FortiSOC 26.2.1 Administration Guide
00-262-1235497-20260617

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-06-02	Initial release.
2026-06-12	Updated FortiAI Insight on page 105 and FortiAI Investigation Agent on page 107.
2026-06-17	Updated Onboarding Fortinet devices on page 28.

About FortiSOC

FortiSOC is a cloud-native AI-driven security operations center (SOC) platform that consolidates log management, correlation, automation, and threat intelligence into one solution. This allows SOC analysts to operate from a single console, moving seamlessly from detection to investigation to response. All data is ingested and normalized in FortiSOC, and predefined detections and playbooks support rapid alert triage and case response. Embedded AI reduces alert noise, further accelerates triage, and automates low-risk response actions to support SOC analysts.

Key features for FortiSOC include:

- Automated alert triage
- Threat detection and alert correlation
- Case investigation and management
- Security orchestration and automated response (SOAR)
- Threat intelligence integration
- Behavioral analytics and anomaly detection
- Compliance and security reporting

For more information about these key features and use cases, see the FortiSOC Ordering Guide.

Intended audience

This document is for FortiSOC administrators. These administrators will manage users, data ingestion, detection rules, and other tools to ensure the SOC analysts can work effectively.

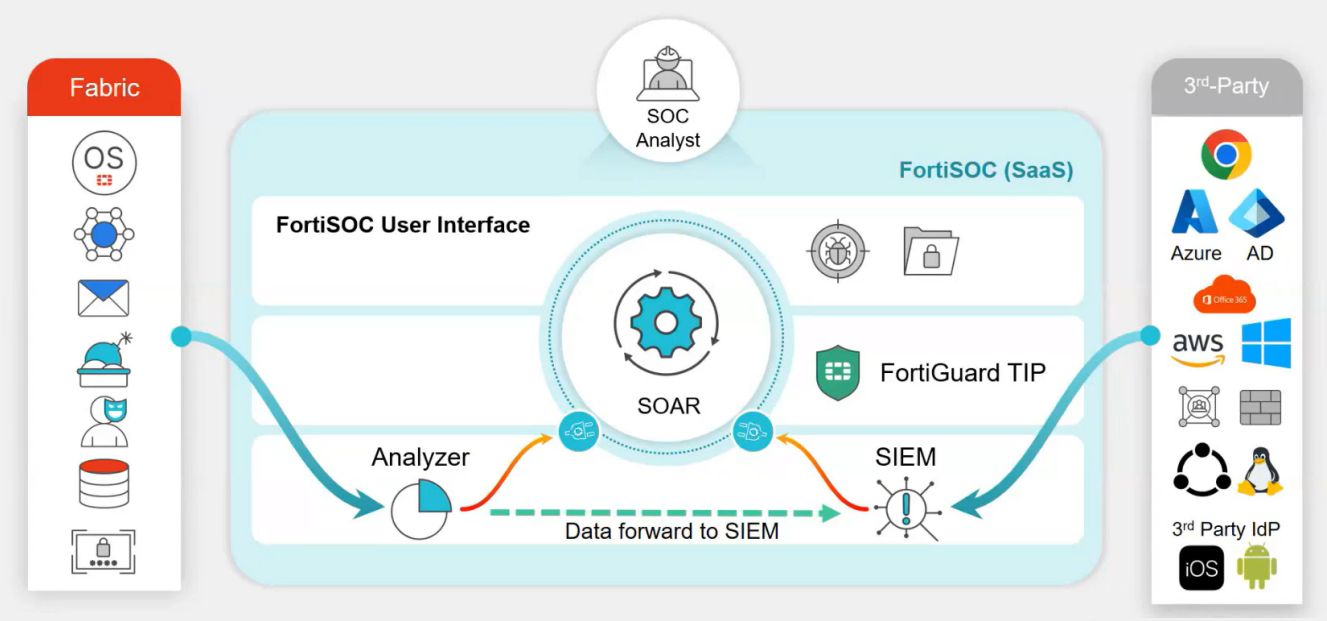
FortiSOC high-level architecture overview

FortiSOC consolidates log management, correlation, automation, and threat intelligence. Using FortiSOC, the SOC analysts can perform threat hunting and work on alerts and cases from a single unified platform.

Log data is ingested into FortiSOC through either **Analyzer** or **SIEM**. Analyzer is used primarily for Fortinet Fabric assets whereas SIEM can be used for a large suite of third-party assets. Analyzer forwards all data to SIEM to avoid duplication and so the assets do not need to be integrated again in the SIEM module. FortiSOC uses connectors to ingest the data from Analyzer and SIEM.

Once the data is ingested, it is parsed and normalized for alerts and cases in FortiSOC. Predefined playbooks (**SOAR**) run in the background to group/correlate the alerts. In this stage, indicators, UEBA, and other information will also be extracted to enrich existing alerts and cases in FortiSOC; information from the FortiGuard Threat Intelligence Platform (TIP) will also be used to automatically enrich the alerts and cases. When appropriate, grouped alerts will be escalated to cases so they can be prioritized by the SOC analysts.

The SOC analysts work within the **FortiSOC user interface** to handle the alerts and cases. This interface also includes threat intelligence tools to support triage and case response; further connectors and integrations can be added to enhance their workflow as well.



Getting started

To get started with FortiSOC, review information in the following topics:

Accessing the FortiSOC cloud portal

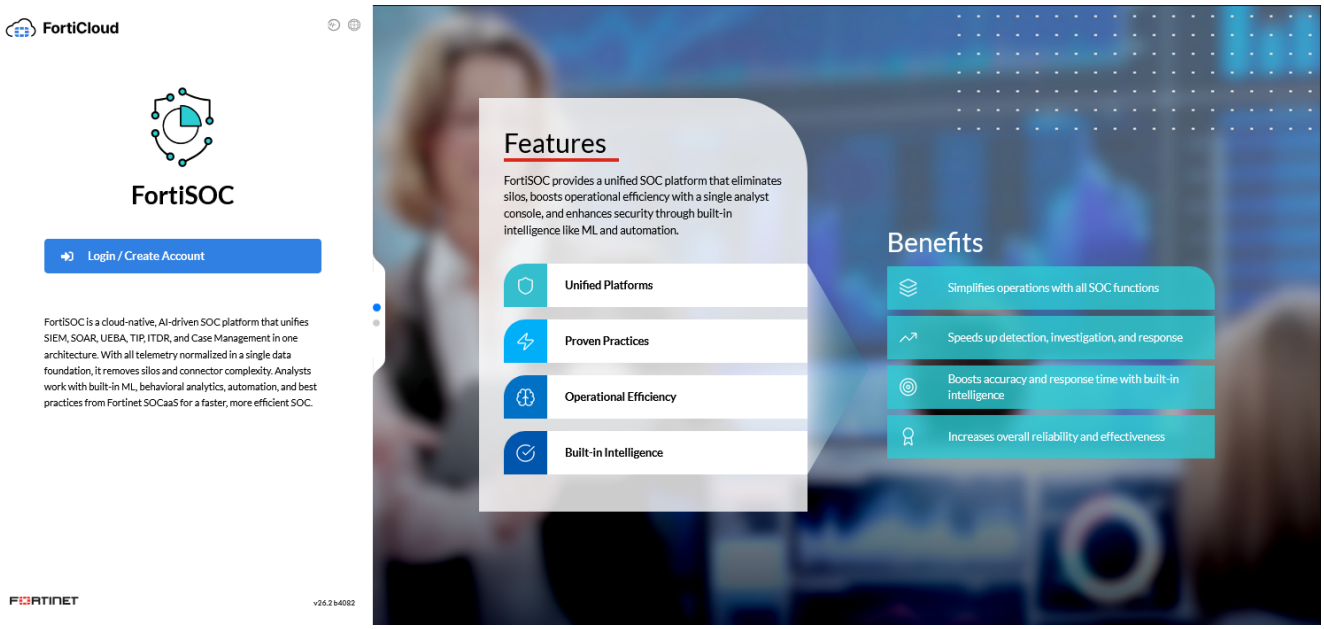
The FortiSOC cloud portal displays account and instance information, including serial number, expiration date, region, status, and entitlements. The entitlement details displayed in this portal includes daily ingestion as well as analytics and archive retention.

Visit the FortiCloud status page to find and subscribe to status information for FortiSOC.

A primary FortiCloud account is required to deploy FortiSOC. A primary FortiCloud account can invite other users to launch FortiSOC as sub users.

You can access the portal through one of the following methods:

- Access FortiSOC through FortiCloud.
- Go to https://fortisoc.forticloud.com. After authentication, you are redirected to your own FortiSOC instance.
- Go directly to your instance using the specific URL for your instance (e.g. https:://{account_id}.{region}.fortisoc.forticloud.com). You can obtain your instance's URL from your browser's address bar once you have accessed FortiSOC through one of the previous methods.



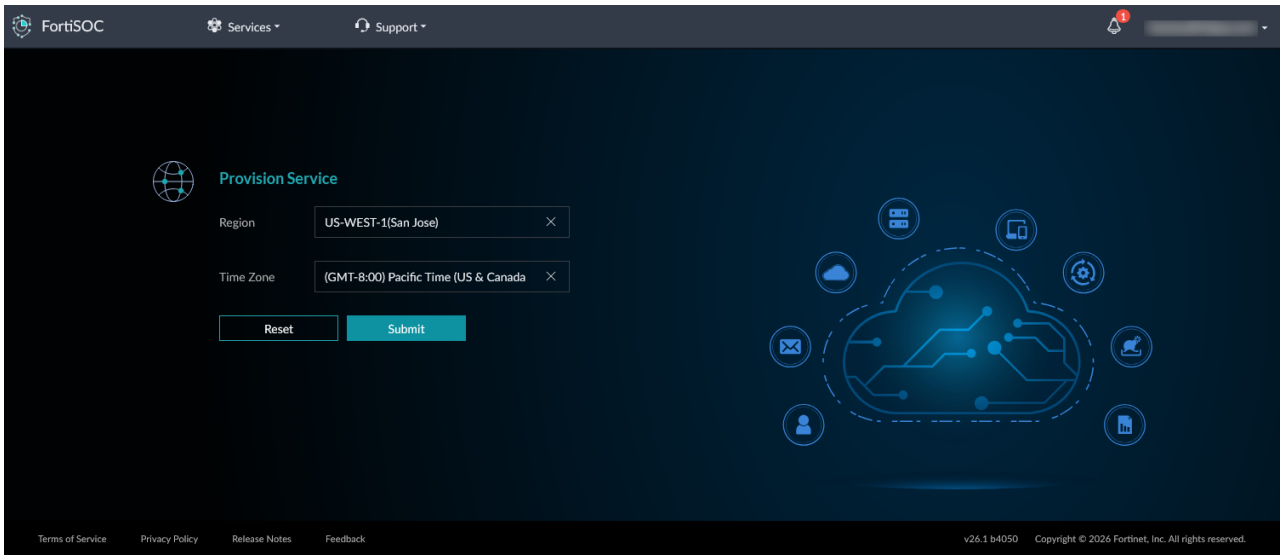
If there are multiple FortiCloud accounts, you must select which account to access when logging into the portal. The accounts are managed in FortiCloud. For more information, see the FortiCloud Services Organization Portal Guide.

Initial login to FortiSOC

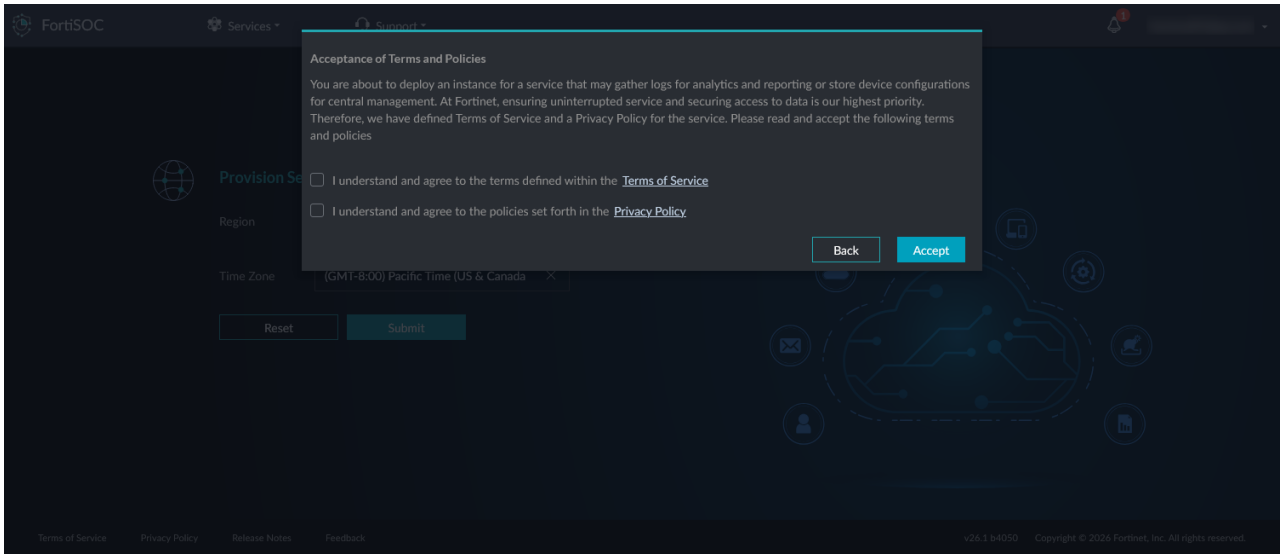
When initially accessing the FortiSOC portal, you must select a region and timezone to provision the FortiSOC cloud instance. You will be asked to agree to terms and conditions, and then the FortiSOC portal will display the progress as it is provisioned.

To complete the initial login to FortiSOC:

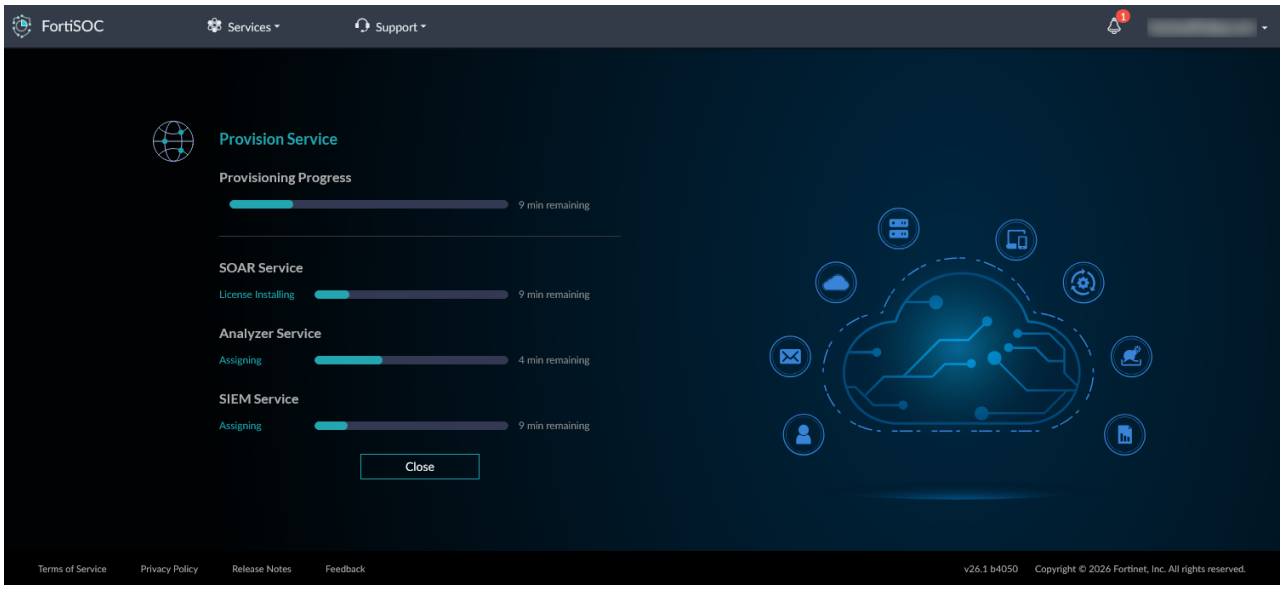
1. Access the FortiSOC portal using one of the methods above.
2. Log into FortiSOC using your FortiCloud credentials.
3. To provision the service, select a *Region* and *Timezone* and then click *Submit*.



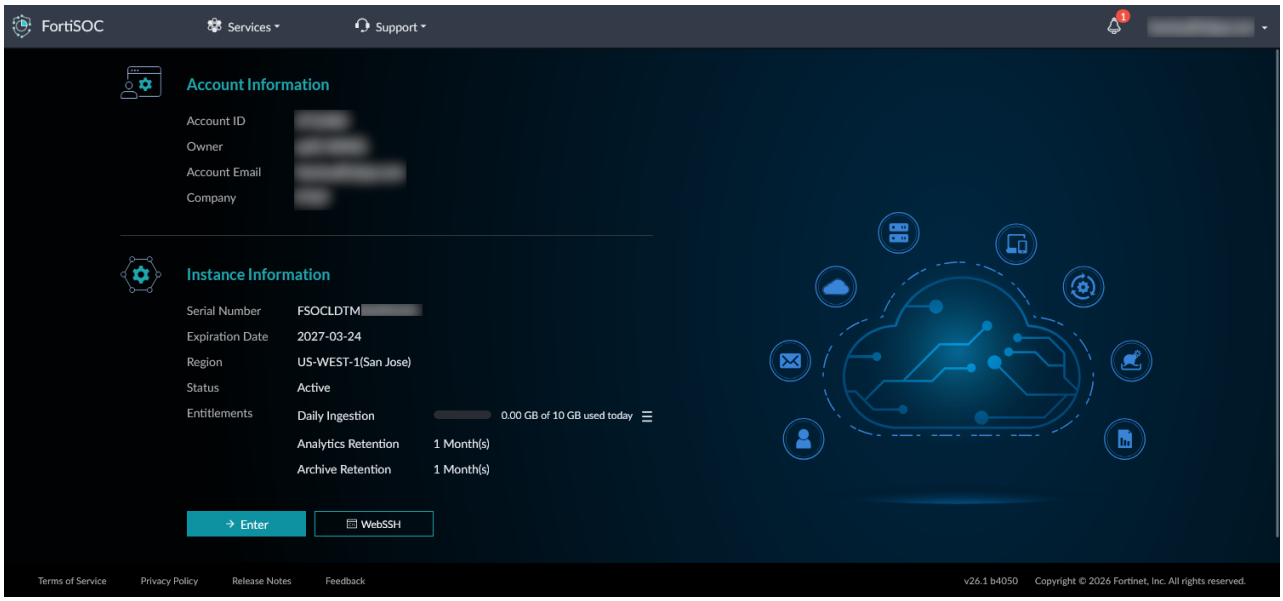
4. Confirm your selections and click *Next*.
5. Review and *Accept* the terms and policies for provisioning the instance.



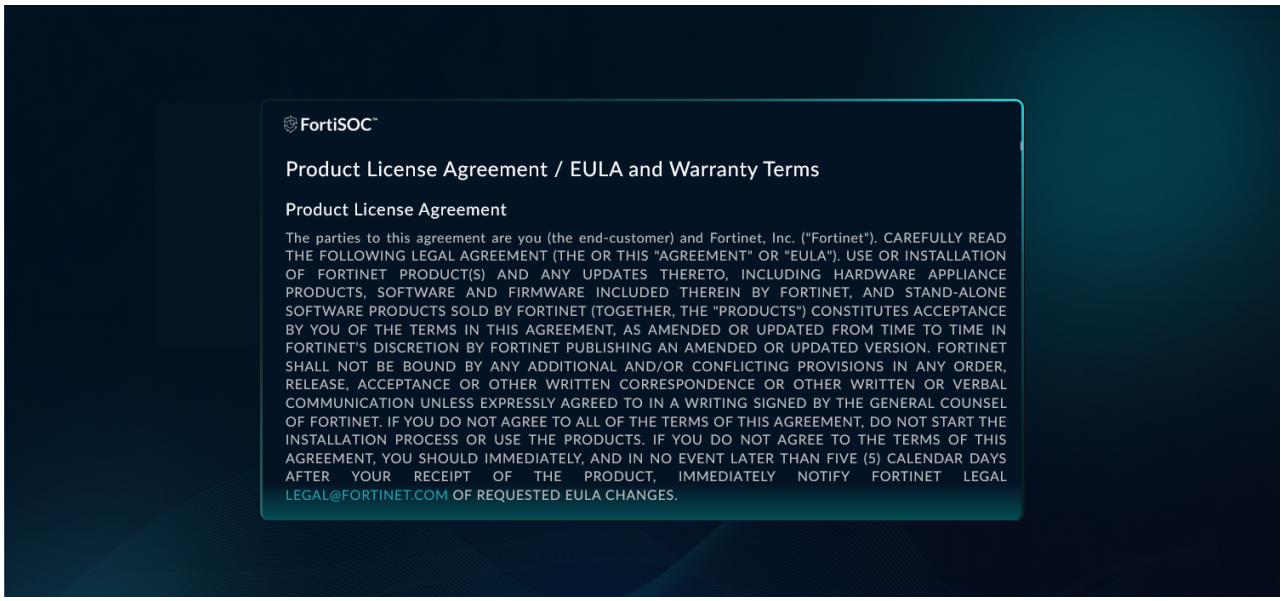
The service takes approximately 10 minutes to provision. The progress is displayed during provisioning.



Once provisioned, the *Account Inofrmation* and *Instance Information* displays.



6. To access the instance, click *Enter*.
7. Review and accept the *Product License Agreement*.



The FortiSOC instance now displays in the default landing page.

Navigating the FortiSOC GUI

The initial landing page for the FortiSOC GUI is the *Dashboard*. You can navigate to the other modules using the tree menu on the left. The available modules vary depending on the privileges (Role) of the user.

The table below lists the modules available by default for super user administrators.

Module	Description
Dashboard	View dashboards to check the network for threat readiness, monitor existing and potential threats, and to review threat response. Many default dashboards are available to monitor the network according to the user's role or goals. For more information, see Dashboards, reporting, and visibility on page 90
Cases & Alerts	View and update cases and alerts. For more information, see Alerts and case management on page 63.
Automation	View and update automation tools, including connectors, playbooks, data ingestion, and schedules. For more information about data ingestion, see Data ingestion and onboarding on page 28. For more information about connectors, see Connectors, APIs, and integrations on page 36. For more information about playbooks, see Automation and response on page 77.

Module	Description
Threat Intel Management	View threat intelligence, using tools such as indicators, dashboards, and a threat intel search. You can also view threat intelligence from FortiGuard and tactics / techniques in the MITRE ATT&CK matrices to support threat hunting. Create threat hunts within the *Hunts* pane to track and report on findings within FortiSOC over a set period of time. The *Threat Intel Management* GUI is powered by the Threat Intel Management solution pack, which comes preconfigured for FortiSOC. For more information about this solution pack, go to *Content Hub > Manage > Threat Intel Management > Documentation* in the FortiSOC GUI.
Assets & Identities	View and update asset and identity information to enhance user and entity behavior analytics (UEBA) within FortiSOC. For more information, see Assets and identity context on page 42.
Reports	View and update reports. The reports are organized into the following categories: • SOC Reports • Analyzer Reports • SIEM Reports For more information, see Reports and scheduled delivery on page 96.
Resources	View and update resources, including attachments, email templates, keys, and escalation rules. In this module, you can also manage queues, shifts, and leave schedules for analysts. Use the *SLA Templates* pane to configure SLAs for cases and alerts.
Analyzer	View and edit configuration for connected Fortinet logging devices and related detection rules. For more information about onboarding devices in the *Analyzer* module, see Onboarding Fortinet devices on page 28
SIEM	View and edit configuration for the collectors and agents used to ingest data from third-party sources and related detection rules. For more information about onboarding data sources in the *SIEM* module, see Onboarding third-party data sources on page 32.
Content Hub	Discover, install, and manage solution packs, connectors, and widgets for FortiSOC. You can also create your own solution packs from this module.
Recycle Bin	View soft-deleted playbooks and playbook collections. From this module, you can restore or permanently delete these records.

In general, there are four primary components visible within any module: the banner, toolbar, tree menu, and content pane.

Component	Description
Banner	Along the top of the page. The banner includes: • Live sync status • Global search

Component	Description
	• Settings • Executed playbook logs • Notifications • Pending tasks • User preference • Support (downloads, resources, and FortiCare) • Services (available through FortiCloud) • Account
Tree menu	On the left side of the screen. Use this navigation menu to open panes in the GUI. Different modules and panes are available depending on the users' role. You can collapse the tree menu to provide more space for the content pane. When the tree menu is collapsed, the module icons are still visible on the left side of the screen. You can mouse over the icons to display the full name of the module and its panes for navigation.
Content pane	Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane. The content pane is primarily made up of charts, grids, and detail views which are described below. For many content panes, you can edit the template to change the information that is displayed.
Toolbar	Directly above the content pane. The toolbar includes options for managing content in the content pane, such as *Add* and *Execute*.

Modules and display templates

With sufficient permissions, you can add, edit, and change the order of modules within the FortiSOC GUI.

Modules can added and edited from *Settings* > *Application Editor* > *Modules*. In this editor, you can select a display template for the module.

In many panes, you can click the edit icon at the top right to edit the existing template:

Option	Description
Template Title	The title for the template.
Add Row	A container for widgets within the template.
Define a new structure	The layout for widgets in the row.
Add Widget	The widget type for the content as well as the data source.

The default templates are primarily made up of charts, grids, and detail views which are described below.

Charts

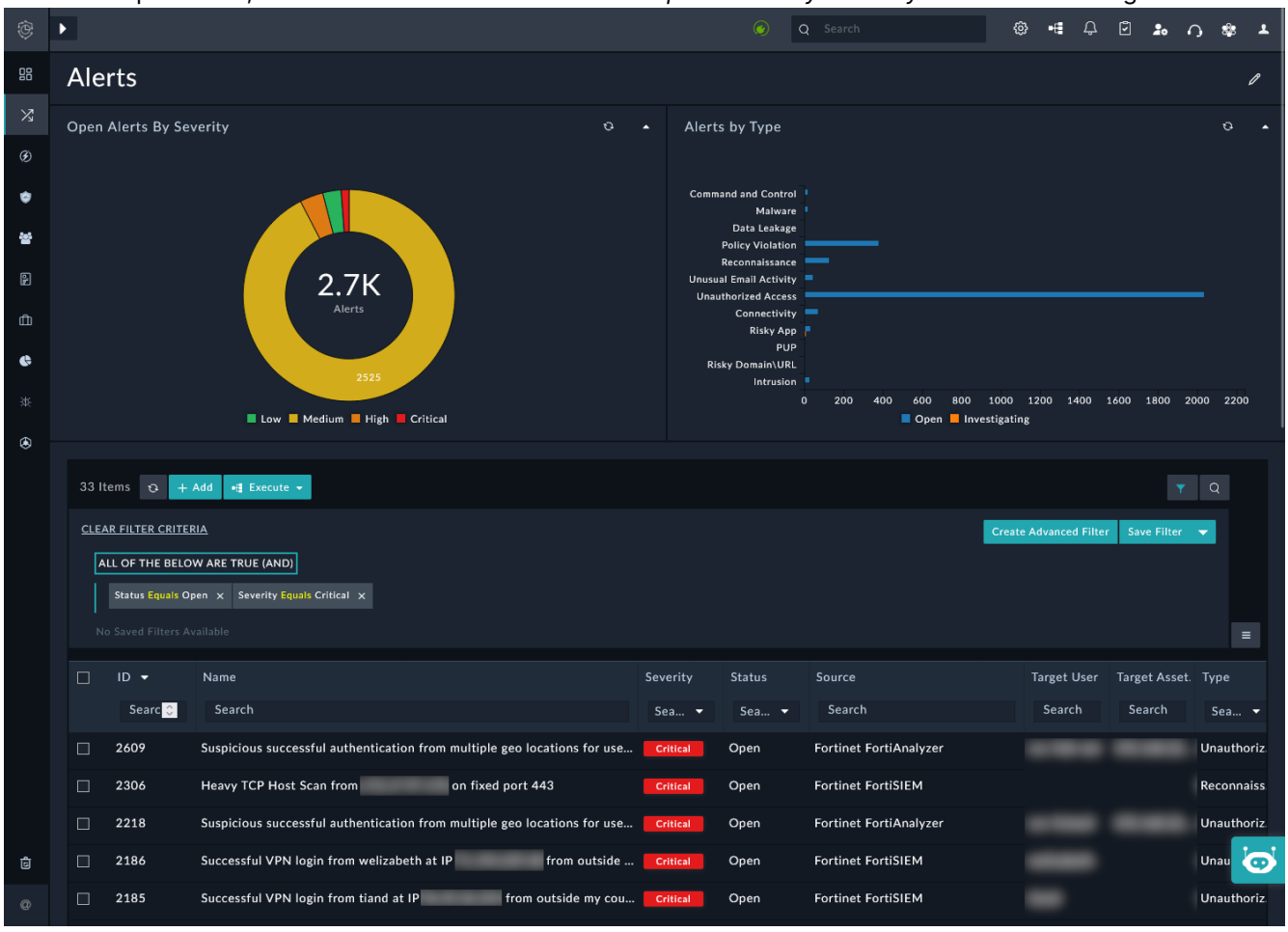
Charts will often display in the top row, above a grid view in the content pane. For example, the *Cases*, *Alert List*, *Assets*, and *Identities* modules display with charts at the top. These donut charts and bar charts provide a summary of the information in the grid view below. In many cases, the charts can be used to quickly filter the grid.

You can perform the following actions with most charts:

- Click the *Refresh* icon above the chart to refresh the information.
- Click the *Collapse/Expand* icon above the chart to hide/show the chart.
- Mouse over a section of the chart to display the related summary information in a tooltip.
- Click a section of the chart to filter the grid below by that criteria.

When you click a chart to filter the grid, the filter criteria will appear above the grid. Click another chart or another area of the same chart to replace the filter criteria. To remove the filter, remove the filter criteria displayed above the grid.

In the example below, the user has clicked *Critical* in the *Open Alerts By Severity* chart to filter the grid.

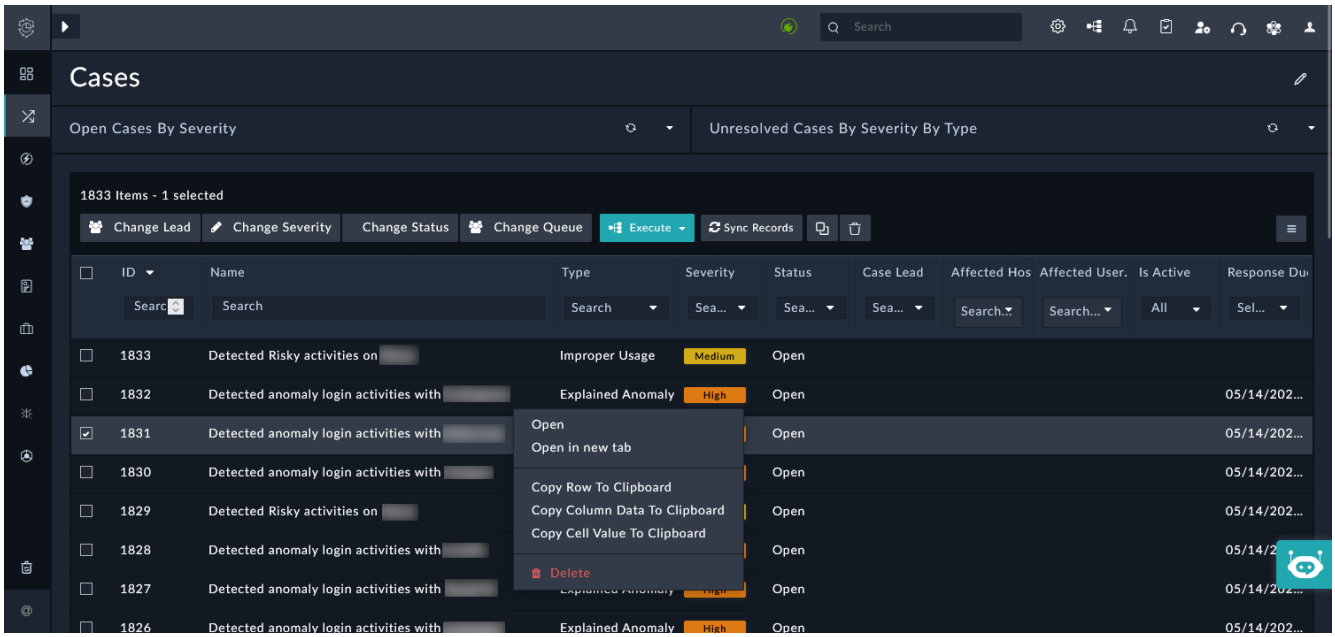


Grids

Grids display a list of records in the content pane, allowing you to search, filter, and perform actions on the content, when applicable.

Using buttons above the grid, you can perform the following actions:

- Click the *Refresh* icon to refresh the records in the grid.
- Click the *Filter* icon to use or create an advanced grid filter.
  For simple filters, use the *Search* fields or dropdowns above at the top of the columns.
- Click the *Search* icon to search the table across all columns and rows.
- Click the *Menu* icon to:
  - Export all columns as CSV, or export all visible column as CSV or PDF.
  - Show/hide columns; you can also reset columns to default.
- Click a column header to sort the records by that column. Click the column header again to reverse the sort order.
- Select the checkbox for a record to perform actions on that record.
- Click a record to open the detail view.
- Right-click a record to open the detail view in a new tab, or to copy the row, column, or cell data to clipboard.



Detail views

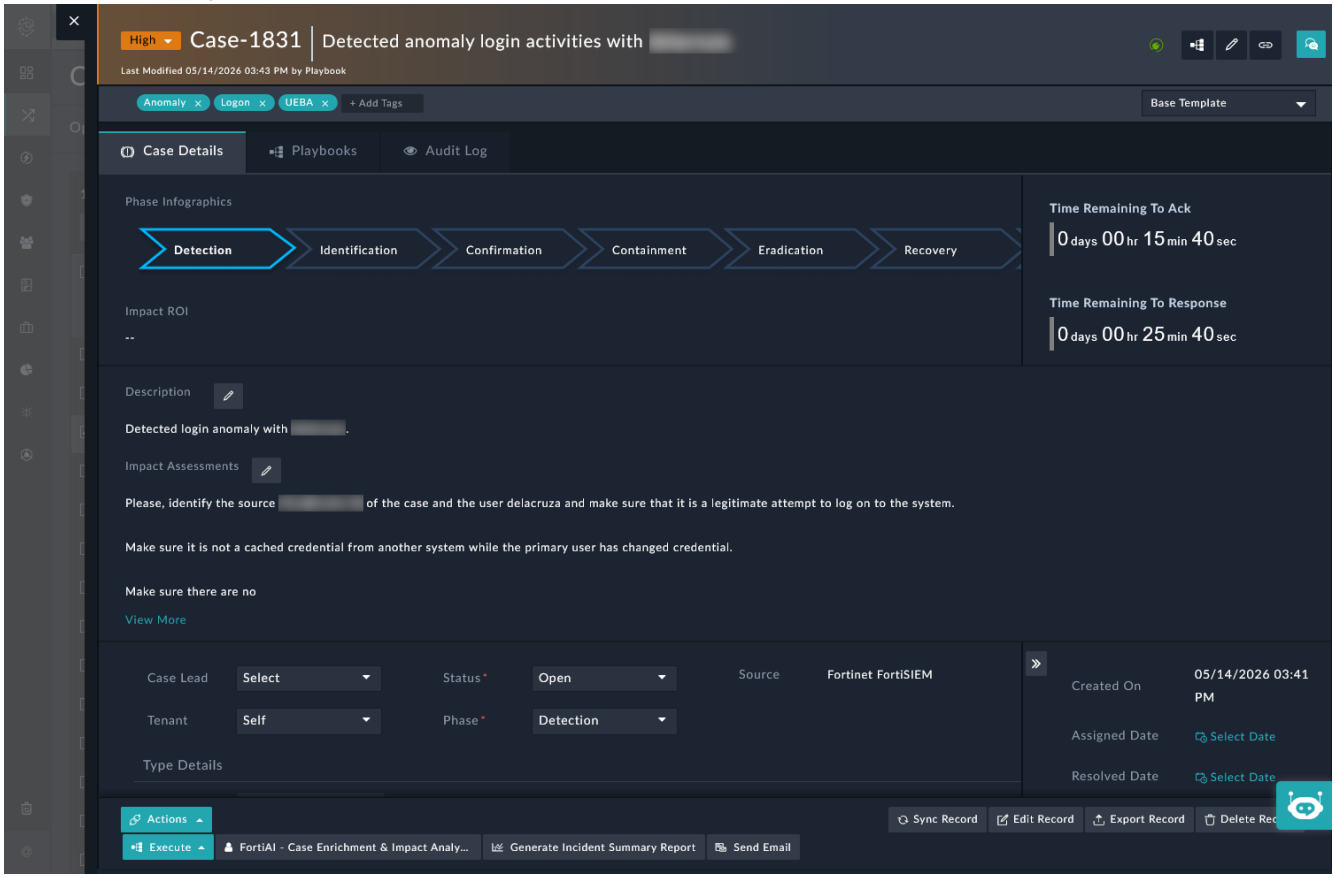
You can access detail views by clicking records within the grids. The detail views open as a pane above the module; you can click the X in the top left to close the pane.

The detail views will include many sections, depending on the type of record. Most detail views will include:

- Header information, such as the record name, last modified time, and tags. The header is fixed to the top as you scroll through the details view.
- Tabs, such as Details, Playbooks, and Audit Logs.
- Sections, such as details, correlations, and more.

  There may be grids, charts, and other widgets included within sections of the detail view. These are interactive, as they would be in regular modules throughout FortiSOC.
- Actions in the footer which can be performed on the record. The footer is fixed to the bottom as you scroll through the details view.

Below is an example of the *Case* detail view.



Global settings

The *Global Settings* for FortiSOC are accessed from the *Settings* icon in the banner.

The following settings can be managed from *Global Settings* > *System*.

System Configuration

Tab	Description
General	Configure general options for the FortiSOC instance, including the language, theme, and datetime format.
Application Configuration	Configure various application options, including purge criteria for audit logs, playbook recovery, playbook log movement, and more.
Log Forwarding	Enable log forwarding for FortiSOC application and audit logs to your central log management server.
Evironment Variable	Configure environment variables to be set for playbooks and connectors.
Branding	Customize FortiSOC branding by configuring logo settings, product name, company name, and more.
System Fixtures	View the links to email templates and the self agent and self tenant pages, which are included by default with FortiSOC.
Advanced Development Features	Review the associated risks and usage guidelines for creating or updating custom connectors and widgets. Then, based on organizational needs, provide explicit consent to enable users to create new connectors or widgets or update existing ones.

Audit Log

View the historical record of activities across FortiSOC using the audit logs. The audit logs are displayed in a grid view and can be searched, filtered, and exported according to your needs.

License Manager

View the details about your FortiSOC licensing. This includes the license expiry, daily ingestion, analytics retention, and archive retention.

Notifications

Manage Delivery Rules and Notification Channels. Notification Delivery Rules define the conditions to generate notifications. For example, a rule, "High Severity Email Notifications" can be set up to send email notifications (using the Email Channel) for all newly created alerts with High or Critical Severity. Notification Channels define various modes of communicating notifications, such as in-app notifications and email notifications.

Data Archival

Review the preferred archive destination and medium and view archived records. You can use one of or a combination of the following methods for data archival:

- External database
- Internal database
- Syslog forwarding
  Data archived using only Syslog Forwarding cannot be searched within the *Archival Search* tab.

Licensing

FortiSOC is a cloud service which requires licensing to access the portal and create an instance. The service has two tiers of licensing: Base and Advanced. Service add-ons can be purchased for either of these tiers for additional archive and analytics retention.

This topic summarizes the licensing information. For more details, see the FortiSOC Ordering Guide.

FortiSOC licenses

FortiSOC licensing is based on log ingestion volume (GB/day) and comes in two tiers.

License	SKU
FortiSOC Base Subscription	FC1-10-FSCLD-1310-02-DD
FortiSOC Advanced Subscription	FC1-10-FSCLD-1318-02-DD

Both tiers include the following:

- 1GB/day ingestion
- FortiCare premium and one-month analytics
- Support -1, -3, and -5 year terms

The Base tier supports Fortinet data sources and a curated set of third-party integrations with built-in SOAR automation. The Advanced tier delivers everything included with the Base tier as well as:

- full SIEM log ingestion,
- user entity and behavior analytics (UEBA) with advanced SIEM analytics,
- full access in the content hub to AI-assisted playbooks,
- and detection rules and playbooks for identity threat detection & response (ITDR).

For complete feature comparison, see the FortiSOC Ordering Guide.

FortiSOC service add-ons for data retention

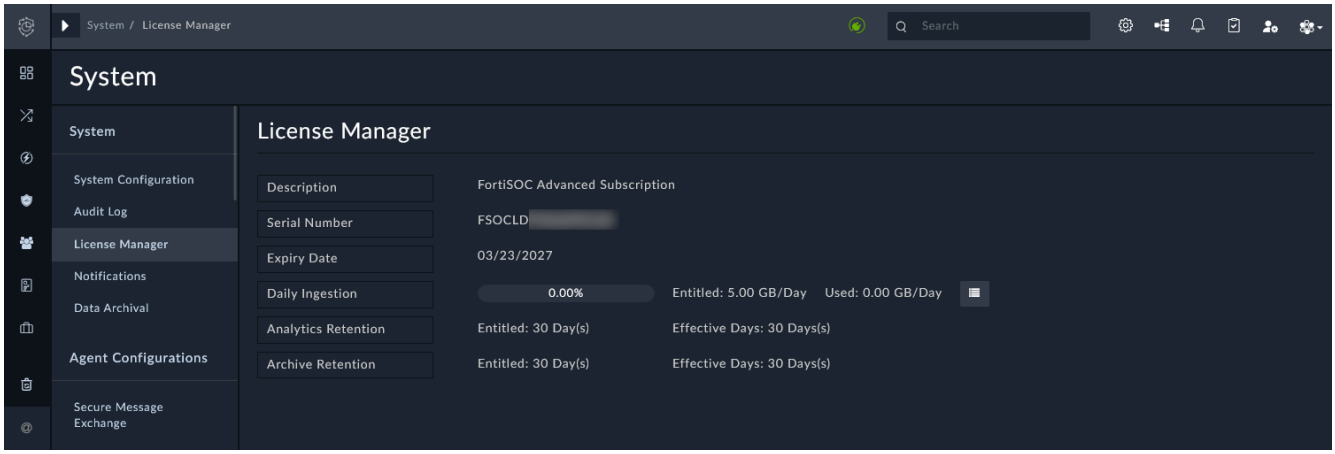
In addition to the above licenses, service add-ons are available for data retention.

Service add-on	Description
Analytics Retention FC1-10-FSCLD-1311-02-DD	Adds one month of analytics retention per GB/day of licensed ingestion.
Archive Retention FC1-10-FSCLD-1312-02-DD	Adds one month of archive retention per GB/day of licensed ingestion.

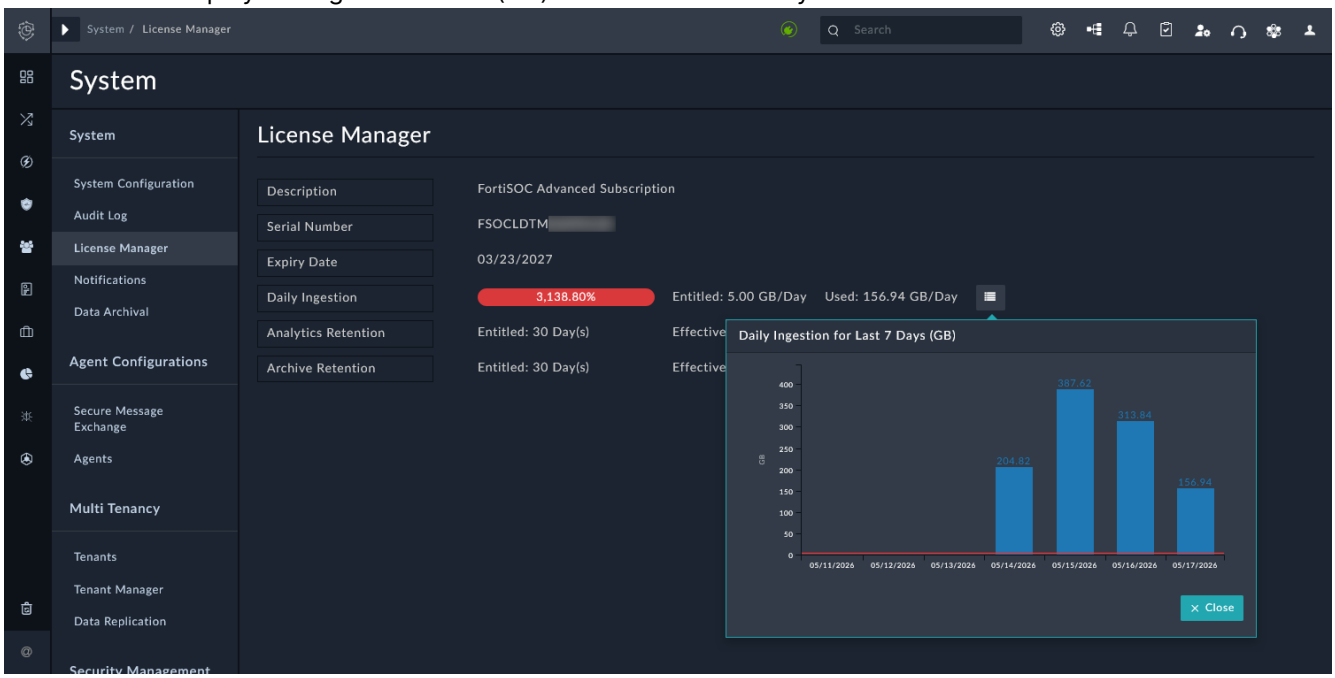
Usage, limits, and quotas

FortiSOC licensing is based on a committed daily ingestion volume (GB/day). FortiSOC licensing also establishes a storage limit for archive and analytics data, which can be increased with service add-ons. Usage is metered, and the administrators will be notified when the quotas are exceeded.

Usage for these entitlements (daily ingestion, archive retention, and analytics retention) can be viewed from the FortiSOC portal and from with the instance in *Global Settings* > *System* > *License Manager*.



The *Daily Ingestion* field displays the current daily usage as well as the entitled GB/day. Click the menu icon next to this field to display the ingestion totals (GB) for the last seven days.



Exceeding the daily ingestion quota

Short-term spikes above the committed daily ingestion volume are allowed. FortiSOC does not block ingestion or analytics. A customer can send in more data than their daily GB as long as the monthly average GB/day does not exceed their subscribed GB/day. For example, if your limit is 50GB/day, you can send in 50GB * 30 days = 1.5TB of raw data. Instead, daily usage is tracked continuously, and each day exceeding the committed daily ingestion volume is recorded for billing or license adjustment reviews.

A notification is added in the FortiSOC GUI banner if the daily ingestion exceeds the licensed amount. This notification is visible for all administrators and users.

Sustained overages can be handled by adjusting the license tier or billing for the additional usage.

User management

User access to FortiSOC is managed within the FortiCloud Identity & Access Management (IAM) portal. In this portal, you can create IAM users and assign permission profiles to define portal access.

Permission profiles allow you to explicitly enable or disable access to portals, including FortiSOC, and grant portal-specific permissions for the enabled portals. In addition, you can further configure Role-Based Access Controls (RBAC) within the FortiSOC GUI. For more information, see Role-based access control (RBAC) on page 23.

FortiCloud also offers an IAM feature that enables you to create and manage external IdP roles that allow users from your organization to log in to the FortiSOC portal using the user credentials with your organization's ID provider. External IdP users are authenticated by your organization's ID provider. After the user is authenticated, they can access FortiSOC based on their role. For more information, see Authentication and single sign-on (SSO) on page 27.

To create a permission profile:

> Before you can create IAM users or external IdP roles, you must create the permission profiles that will be assigned to them.

1. Login to https://support.fortinet.com/.
2. To access the IAM portal, go to *Services* > *IAM*.
3. In the IAM portal, go to *Permission Profiles*.
4. Click *Add New*.
   The *New Portal Permission Profile* page displays.
5. In the *Basic Info* section, enter the permission profile name and select the status.
6. Click *Add Portal*.
   A list of available portals displays.
7. Select *FortiSOC* and any other required portals, and the click *Add*.
   The selected portals are displayed in cards.
8. Define the portal permissions in the *FortiSOC* card.
   The permissions define the users' *Roles* within FortiSOC.
   - *Admin*: Full Admin role
   - *Read / Write*: Analyst role
   - *Read Only*: Read-Only Admin role
   - *Custom*: Assign the user to a predefined or custom role in the FortiSOC GUI.

   For more information about those roles, see Role-based access control (RBAC) on page 23.
9. Click *Save*.
   This permission profile can now be assigned to users. If needed, create another permission profile with a different level of access to FortiSOC (or other portals).
   For information on creating permission profiles, see the FortiCloud Account Services Identity & Access Management documentation.

To create an IAM user:

1. Login to https://support.fortinet.com/.
2. To access the IAM portal, go to *Services* > *IAM*.
3. In the IAM portal, go to *Users*.
4. Click *Add New* > *IAM User*.
5. In the *User Details* page, enter the user details, and then click *Next*.
6. In the *User Permissions* page, assign the IAM user the appropriate permission scope and profile, and then click *Next*.
7. In the *Confirmation* page, click *Confirm* to complete the user creation process.
8. In the *Successful User Registration* page, click *Generate Password* to generate a reset password link for the user to login.
9. Click *Copy Reset Link*.

Once this is complete, you can share the link with the user to access their FortiCloud account. They will have access to the FortiSOC portal as defined in the permission profile.

Role-based access control (RBAC)

Role-based access controls (RBAC) for modules within the FortiSOC GUI are managed using *Roles* in FortiSOC.

When creating IAM users, the permission profile will determine the predefined role assigned to the user in FortiSOC.

- *Admin*: Full Admin role
- *Read / Write*: Analyst role
- *Read Only*: Read-Only Admin role
- *Custom*: Read-Only Admin role. Once the Custom user logs into FortiSOC, a Full Admin can assign another predefined or custom role for the user in the FortiSOC GUI. The newly assigned role will be applied to the Custom user when they next login. See Creating custom roles on page 26 and Assigning roles on page 27.

Sub users are automatically assigned the *Read-Only Admin* role. Once the sub user logs into FortiSOC, a Full Admin can assign another predefined or custom role for the user in the FortiSOC GUI. The newly assigned role will be applied to the user when they next login.

Predefined roles

The following predefined roles are available to control user access within the FortiSOC GUI.

Role	Description
Analyst	Responsible for Case Investigation and other remediation and containment-related tasks.

Role	Description
	This is the core operation role in the SOC for continuous monitoring and response. The analysts can monitor alerts and manage cases; they can also review information that supports triage, such as assets/identities, attachments, dashboards, vulnerabilities, and more. However, they cannot add devices, configure agents, or manage users.
Full Admin	Essentially the root user, use carefully. Responsible for managing users, data ingestion, and system configuration for FortiSOC. They also have full access to all other features in FortiSOC, so they can perform the duties of the analysts as needed as well.
FortiSOC Agent	Agent appliances will be auto-assigned this role. Defaults to access to files and attachments.
Read-Only Admin	Access with viewing rights only, no editing or modification capabilities.

The table below lists the default permissions for the predefined roles. The following permissions can be defined for each module:

- *Read & Write*: the user can view and make changes in the FortiSOC module.
- *Read Only*: the user can only view information in the FortiSOC module.
- *None*: the user can neither view or make changes in the FortiSOC module.

Module	Analyst	Full Admin	FortiSOC Agent	Read-Only Admin
Agents	Read Only	Read & Write	Read Only	Read Only
Alerts	Read & Write	Read & Write	None	Read Only
Analytics	Read Only	Read & Write	None	Read Only
Analyzer	Read Only	Read & Write	None	Read Only
Announcements	Read & Write	Read & Write	None	Read Only
Appliances	Read Only	Read & Write	None	Read Only
Application	Read Only	Read & Write	Read Only	Read Only
Approvals	Read & Write	Read & Write	None	Read Only
Assets	Read & Write	Read & Write	None	Read Only
Attachments	Read & Write	Read & Write	None	Read Only
Audit Log Activities	Read Only	Read & Write	None	Read Only
CMDB	Read Only	Read & Write	None	Read Only
CVEs	Read & Write	Read & Write	None	Read Only
Campaigns	Read & Write	Read & Write	None	Read Only
Comment	Read & Write	Read & Write	None	Read Only

Module	Analyst	Full Admin	FortiSOC Agent	Read-Only Admin
Communications	Read & Write	Read & Write	None	Read Only
Companies	Read Only	Read & Write	None	Read Only
Connectors	Read Only	Read & Write	None	Read Only
Content Hub	Read Only	Read & Write	None	Read Only
Dashboard	Read & Write	Read & Write	None	Read Only
Data Archival	Read Only	Read & Write	None	Read Only
Email Templates	Read & Write	Read & Write	Read Only	Read Only
Escalation Rules	Read & Write	Read & Write	None	Read Only
Events	Read & Write	Read & Write	None	Read Only
FAZ Reports	Read Only	Read & Write	None	Read Only
Files	Read & Write	Read & Write	None	Read Only
Groups	Read Only	Read & Write	None	Read Only
Hunts	Read & Write	Read & Write	None	Read Only
Identities	Read & Write	Read & Write	None	Read Only
Incidents	Read & Write	Read & Write	None	Read Only
Indicators	Read & Write	Read & Write	None	Read Only
Key Store	Read Only	Read & Write	None	Read Only
Leave Schedules	Read Only	Read & Write	None	Read Only
Mitigations	Read Only	Read & Write	None	Read Only
Notification Rules	Read & Write	Read & Write	None	Read Only
People	Read Only	Read & Write	None	Read Only
Playbooks	Read & Write	Read & Write	None	Read Only
Preprocessing Rules	Read & Write	Read & Write	None	Read Only
Queues	Read Only	Read & Write	None	Read Only
Reporting	Read & Write	Read & Write	None	Read Only
Secure Message Exchange	Read Only	Read & Write	None	Read Only
SLA Templates	Read & Write	Read & Write	None	Read Only
Saved Reports	Read Only	Read & Write	None	Read Only
Scans	Read Only	Read & Write	None	Read Only

Module	Analyst	Full Admin	FortiSOC Agent	Read-Only Admin
Scenario	Read Only	Read & Write	None	Read Only
Schedules	Read & Write	Read & Write	None	Read Only
Security	None	Read & Write	None	Read Only
Shifts	Read & Write	Read & Write	None	Read Only
Software	Read Only	Read & Write	None	Read Only
Solution Packs	Read Only	Read & Write	None	Read Only
Sub-techniques	Read & Write	Read & Write	None	Read Only
Tactics	Read & Write	Read & Write	None	Read Only
Tasks	Read & Write	Read & Write	None	Read Only
Techniques	Read & Write	Read & Write	None	Read Only
Tenants	Read Only	Read & Write	None	Read Only
Threat Actors	Read Only	Read & Write	None	Read Only
Threat Intel Feed	Read Only	Read & Write	None	Read Only
Threat Intel Reports	Read Only	Read & Write	None	Read Only
Vulnerabilities	Read & Write	Read & Write	None	Read Only
War Rooms	Read & Write	Read & Write	None	Read Only
Widgets	Read Only	Read & Write	None	Read Only
Workspaces	Read & Write	Read & Write	None	Read Only

Creating custom roles

Roles can be created and viewed in *Settings* > *Security Management* > *Roles*. The predefined roles are listed in the table view. Click *Add* to create new roles, if needed.

When adding a new role, you must configure the following:

Option	Description
Role Name	Enter a role name; the purpose of the role should be clear according to the name.
Description	(Optional) Enter a description for the role.
Set Role Permissions	Set the permission (Read & Write, Read Only, or None) for each of the modules.

Option	Description
	The modules listed in the roles' permission table represent discrete areas or record sets within FortiSOC. Some of these modules are accessible within the navigation tree on the left, while others are available from within the global settings for administrators. The administrator modules in the list often refer to the main module, and they control permissions for all sub-menus or tabs within that module. For example, the Security module controls access for all user related menus under *Settings* > *Security Management*: Teams, Roles, Users, and so on.

Assigning roles

Roles can be assigned in *Settings* > *Security Management* > *Users*.

When editing a user, select from the list of available roles. The user will be restricted to the permissions defined in the selected roles.

Users can be assigned multiple roles. Each role granted to a user is additive to their overall RBAC permission set. Therefore, a user's RBAC permissions are an aggregation of all the permissions granted to them by each role they are assigned.

Authentication and single sign-on (SSO)

FortiCloud supports using an external identity provider with SAML 2.0 and IdP initiated authentication. External IdP roles enable external users to log in to the Cloud portal using their company's credentials through a third-party ID provider. The company's ID provider verifies the identity of external IdP users. Following authentication, users can access the cloud application according to their permission profile.

For more information on managing external IdP roles and users for cloud products, see the FortiCloud Services Identity & Access Management (IAM) guide.

Data ingestion and onboarding

FortiSOC supports both Fortinet and third-party data sources. The ingested raw data from these sources is automatically parsed and normalized in the FortiSOC instance. FortiSOC stores the structured (parsed and normalized) data for alerts, correlation, case investigation, and response. In addition, the data is also enriched in FortiSOC through predefined ingestion from FortiGuard, MITRE ATT&CK, and other Threat Intelligence Platforms (TIPs). Further connectors can be added for enrichment from a wide range of sources, including Active Directory.

With a Base Subscription, FortiSOC includes the *Analyzer* module, which can be used for Fortinet Fabric devices, including FortiGate, FortiWeb, FortiMail, FortiClient, and more. With this license, you can also create connectors from on-premise FortiAnalyzer devices, allowing you to ingest data collected from their authorized Fortinet and third-party logging devices. Additional connectors can be configured within FortiSOC for API integrations. The available connectors can be configured through the *Content Hub* and *Automation* > *Data Ingestion* modules.

With an Advanced Subscription, FortiSOC also includes the *SIEM* module, which can be used to configure Collectors and agents for an extensive suite of third-party devices and applications. Data collected in the *Analyzer* module is also forwarded to SIEM, so you do not need to duplicate device integrations.

Onboarding Fortinet devices

Fortinet devices configured for logging to FortiSOC are visible within the *Analyzer* module.

There are two methods to collect logs through the *Analyzer* module in ForitSOC:

- Using an on-premise FortiAnalyzer for log collection on page 28
- Using Analyzer for log collection on page 29

Using an on-premise FortiAnalyzer allows you to collect logs from some third-party sources in addition to the Fortinet logging devices supported by FortiAnalyzer.

Using an on-premise FortiAnalyzer for log collection

To use an on-premise FortiAnalyzer for log collection, create a FortiSOC Connector in the on-premise FortiAnalyzer. Using this connector, all logs in the FortiAnalyzer root ADOM will be forwarded to FortiSOC. This includes forwarding logs Fortinet Fabric and third-party data sources authorized on the FortiAnalyzer.

The FortiSOC Connector requires an access token to establish the connection. Access tokens can be created, renewed, edited, and deleted from the FortiSOC GUI.

To forward logs from an on-premise FortiAnalyzer to FortiSOC:

1. Go to *Analyzer > Settings > Advanced > Access Tokens*.
2. Click *Create New*.
3. In the *Token Name* field, enter a name for the token.
   Optionally, enter a *Description* for the token as well.
4. Click *OK*.
   A *New Access Token* is generated. The token is valid for 90 days after creation.
5. Copy the *New Access Token*. Please keep the token safe and secure.
6. In the root ADOM for the on-premise FortiAnalyzer, create a FortiSOC Connector.

   The FortiSOC Connector is only available in FortiAnalyzer 7.6.7 and later. If you are using an earlier version of FortiAnalyzer, you must create a FortiAnalyzer Cloud Connector using the FortiSOC access token.

7. When configuring the connector, paste the access token from FortiSOC in the *Access Token* field.
   For more information about configuring the connector, see the FortiAnalyzer Administration Guide.
   Once the connector is configured and enabled, FortiAnalyzer will securely forward logs from authorized devices (Fortinet Fabric and third-party) in the root ADOM to FortiSOC.

The authorized devices sending logs to the on-premise FortiAnalyzer will be visible in FortiSOC from *Analyzer > Device Manager* and the logs can be found in *Analyzer > Log View*.

To manage access tokens:

You can manage the access token(s) from the FortiSOC GUI in *Analyzer > Settings > Advanced > Access Tokens*. In this pane, you can perform the following actions:

- Create new access tokens.
- Edit an access token name or description.
- Delete an access token.
- Renew an access token. A new access token is created and valid for 90 days; you must replace the token in the configured device.
- Download an access token. When downloading a token, you must enter an *Encrypt Password*. The password is used to unzip the downloaded folder and access the token.

Using Analyzer for log collection

The process for onboarding Fortinet Fabric devices to the Analyzer module is that same as onboarding devices to FortiAnalyzer Cloud.

FortiSOC has the same support as FortiAnalyzer Cloud 7.6.5 for Fortinet Fabric devices.

Configuring FortiOS devices

To configure FortiOS logging to FortiAnalyzer Cloud / FortiSOC, see the FortiAnalyzer Cloud Deployment Guide.

Once the FortiOS device is configured, it can be found in the FortiSOC GUI under *Analyzer > Device Manager*. You can *Edit* the FortiGate device and change the name to something meaningful, if needed. You can confirm the logs are in FortiSOC by checking *Analyzer > Log View* for the device.

Configuring FortiWeb devices

To configure FortiWeb logging to FortiAnalyzer Cloud / FortiSOC, see the FortiAnalyzer Cloud Deployment Guide.

Once configured, FortiWeb will be automatically added and authenticated to FortiSOC in *Analyzer > Device Manager*. You can view the logs in *Analyzer > Log View*.

Configuring FortiClient EMS

To configure FortiClient EMS logging to FortiAnalyzer Cloud / FortiSOC, see the FortiAnalyzer Cloud Deployment Guide.

Once FortiClient EMS is authorized in the FortiSOC *Analyzer > Device Manager*, it uploads logs as defined by the upload schedule. You can find the logs from FortiClient in *Analyzer > Log View*.

Configuring FortiMail devices

To configure FortiMail logging to FortiAnalyzer Cloud / FortiSOC, see the FortiAnalyzer Cloud Deployment Guide.

Once FortiMail is authorized in the FortiSOC *Analyzer > Device Manager*, you can find the logs in *Analyzer > Log View*.

Configuring FortiNDR devices

To configure FortiNDR logging to FortiAnalyzer Cloud / FortiSOC, see the FortiAnalyzer Cloud Deployment Guide.

Once FortiNDR is configured to send logs to FortiAnalyzer Cloud / FortiSOC, you can configure log categories and severity level on FortiNDR using the CLI `config system syslog cloud settings`. For more information, see the FortiNDR CLI Reference Guide.

The FortiNDR device can be found in FortiSOC *Analyzer > Device Manager* and the logs can be found in *Analyzer > Log View*.

Configuring FortiSandbox devices

To configure FortiSandbox logging to FortiSOC, add FortiSOC as a log server on the FortiSandbox device. Access tokens are configured in FortiSOC to establish the connection. These access tokens can be created and managed in the FortiSOC GUI from *Analyzer > Settings > Advanced > Access Tokens*.

To configure FortiSandbox logging to FortiSOC:

1. In the FortiSOC GUI, go to *Analyzer > Settings > Advanced > Access Tokens*.
2. Click *Create New*.
3. In the *Token Name* field, enter a name for the token. For example, the FortiSandbox hostname.
   Optionally, enter a *Description* for the token as well.
4. Click *OK*.
   A *New Access Token* is generated. The token is valid for 90 days after creation.
5. Copy the *New Access Token*. Please keep the token safe and secure.
6. To configure FortiSOC as a log server in FortiSandbox, see the FortiSandbox Administration Guide.
   For log server *Type*, select FortiAnalyzer-Cloud. Paste the access token in the *Log Server Cloud Token* field.

To renew an access token for FortiSandbox logging to FortiSOC:

1. In the FortiSOC GUI, go to *Analyzer > Settings > Advanced > Access Tokens*.
2. Select the access token for the FortiSandbox log server.
3. Click *Renew*.
   A *Confirm Renewal* dialog displays.
4. Click *OK* to confirm the renewal.
   The token is now valid for the next 90 days.
5. Copy the new access token.
6. In the FortiSandbox device, go to the FortiSOC log server configuration.
7. In the *Log Server Cloud Token* field, paste the access token.
   For more information see the FortiSandbox Administration Guide.

Using the Add Device wizard

You can use the *Add Device* wizard to add model devices using a serial number or a pre-shared key. Note that you must also complete configuration on the logging devices to send logs to FortiSOC. For example, when adding FortiGate devices using a pre-shared key in the device wizard, you must also configure the FortiGate devices to send logs to FortiSOC.

To add devices using the device wizard:

1. Go to *Analyzer > Device Manager* and click *Add Device*.
   The *Add Device* wizard displays.
2. Configure the following options:

Option		Description
Name		Type a name for the device.
Link Device By		Select *Serial Number* or *Pre-shared Key*. Depending on your selection, the device model will automatically link to a real device by serial number or configured pre-shared key.
	Serial Number	Enter the device's serial number.

	Pre-shared Key	Enter a pre-shared key for the device. If using a pre-shared key, each device must have a unique pre-shared key
		Only FortiGate devices can be added using a pre-shared key. You must also configure this pre-shared key on the corresponding FortiGate device after configuring it to send logs. In the FortiGate CLI, enter the following commands:
		`config log fortianalyzer setting`
		`set preshared-key <pre-shared key>`

Device Model		Select the model of the device from the dropdown.
Description		Type a description of the device (optional).
Allow Access to FortiAnalyzer REST API		Enable to allow the authorized FortiGate device to consume the Analyzer's REST API.
Allow Access to FortiGate REST API		This toggle is read-only. This setting indicates if the device allows Analyzer to access its JSON APIs configured on the device side. This setting must be configured on the FortiGate.

3. Click *Next*.
   The device is added to *Analyzer* and, if successful, is ready to begin sending logs.
4. Click *Finish* to finish adding the device and close the wizard.

Onboarding third-party data sources

The *SIEM* module in FortiSOC is available with an Advanced Subscription. This license allows for data collection from a large suite of third-party sources, enhancing your SOC monitoring potential. For more information about licensing, see Licensing on page 19.

Collectors are used for data collection through the *SIEM* module in FortiSOC. Once a Collector is setup, you can configure third-party sources for monitoring in FortiSOC. If you are collecting logs from Windows and Linux systems through agents, you can install and map those agents through the Collector in FortiSOC as well. See Install and map agents to the Collector on page 35.

For a complete list of supported external systems, including their required configurations to send logs to a Collector, see the FortiSIEM External Systems Configuration Guide.

Setup a Collector

The Collector is created within the FortiSOC GUI. Once a Collector has been created, it can be installed and registered. A FortiSIEM user created in the FortiSOC GUI is required to complete the registration.

To add a Collector in FortiSOC:

1. In the FortiSOC GUI, go to *SIEM > Settings > Setup > Collector*.
2. Click the *Add* icon (+).
   The *Event Collector Definition* dialog displays.
3. Enter the following options, and then click *Save*.

Option	Description
Name	[Required] Collector name.
Guaranteed EPS	[Required] Events from this Collector are always accepted when its event rate is below this guaranteed events per second (EPS).
Upload Rate Limit (Kbps)	Maximum rate limit (in Kbps) at which a Collector can send events. Rate limit is enforced at periodic three minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Upload EPS Limit	Maximum events per second at which a Collector can send events. EPS limit is enforced at periodic three minute intervals. When either the upload rate limit or EPS limit are hit, events are buffered at the Collector and sent later.
Start Time	[Required] Select a specific start date or select *Unlimited*. Collectors will not work outside of start and end dates if specific dates are chosen.
End Time	[Required] Select a specific end date or select *Unlimited*. Collectors will not work outside of start and end dates if specific dates are chosen.

To create a FortiSIEM user for Collector registration:

1. In the FortiSOC GUI, go to *SIEM > CMDB > Users > FortiSIEM Users*.
2. Click the *Add* icon (+).
   The *New User* dialog displays.
3. In the *General* tab, enter a *User Name* and *Full Name*.
4. In the *Contact* tab, enter an *Email*.
5. In the *FortiSIEM Attributes* tab, select the checkbox for *FortiSIEM Role*, and then configure the following:

Option	Configuration
Agent Admin	Leave unselected.
Mode	Leave as *Local*.
Password	Enter a password for the user.

Option	Configuration
Confirm Password	Re-enter the password for the user.
Default Role	Select *Full Admin*.

6. Click *Save*.
7. Click *Save* again to save the user.

The *User Name* and *Password* configured in the above steps are required when registering the Collector.

To install and register a Collector:

1. Installation varies by platform. To install the collector, see the *Install Collector* section within the relevant Installation Guides on the Fortinet FortiSIEM Document Library.
   - AWS Installation Guide
   - Azure Installation Guide
   - ESX Installation Guide
   - Google Cloud Platform (GCP) Installation Guide
   - Hyper-V Installation Guide
   - KVM Installation Guide
   - Nutanix AHV Installation Guide
   - Oracle Cloud Infrastructure (OCI) Installation Guide
   - Proxmox Installation Guide
2. To register the Collector, SSH to the Collector and run the following command:
   `phProvisionCollector {--add | --update} <user> <FSM URL> <organization> <collectorName>`
   You will be prompted to enter the password.

Variable	Description
{--add | --update}	To add a new Collector, use `--add`. To re-register a Collector and retain the same Collector ID, use `--update`.
<user>	Enter the user name of the FortiSIEM user created for Collector registration.
<FSM URL>	Enter your FSM URL in the following format: `{tenantid}-fsm.{region}.fortisoc.forticloud.com` You must include "`-fsm`" in the URL to register the Collector.

Variable	Description
	You can also find this URL in the FortiSOC GUI by checking *Automation > Connectors*. 1. Go to *Automation > Connectors*. This displays the *Content Hub > Manage* tab filtered by *Connectors*. 2. Click the *Fortinet FortiSIEM* connector. You can use the search bar to quickly find this connector. 3. In the *Configurations* tab, ensure the *Embedded-SIEM* configuration is selected. 4. Copy the *Server URL* to use as the `<FSM URL>`.
<organization>	Enter the organization name. The default organization name is `super`.
<collectorName>	Enter the name of the Collector created in FortiSOC.

The Collector should display "`This collector is registered successfully. Waiting for reboot...`". Once the Collector has rebooted, you can check the status of all processes by entering `phstatus` in the Collector SSH session.

To check Collector health:

1. In the FortiSOC GUI, go to *SIEM > Settings > Health > Collector Health*.
2. In the table view, review the *Health* column for the Collector.
   After registering the Collector, the *Health* should change from `No Connection` to `Normal`.

Install and map agents to the Collector

Agents can be used to monitor Windows and Linux machines. After you setup a Collector, you can install and map the agents. A FortiSIEM user created within the FortiSOC GUI is required for agent installation. The agents are installed on the data ingestion sources and mapped to the Collector. For Windows and Linux agents, you can use predefined *Host to Template Associations* in FortiSOC. Once the agents are mapped, FortiSOC can receive logs from these sources.

To create a FortiSIEM user for agent installation:

1. In the FortiSOC GUI, go to *SIEM > CMDB > Users > FortiSIEM Users*.
2. Click the *Add* icon (+).
   The *New User* dialog displays.
3. In the *General* tab, enter a *User Name*.
   The remaining fields in this tab are not mandatory.
4. In the *FortiSIEM Attributes* tab, select the checkbox for *FortiSIEM Role*.
5. Select the checkbox for *Agent Admin*.
6. In the *Password* field, enter a password for the user.
7. In the *Confirm Password* field, re-enter the password.

8. Click *Save*.
9. Click *Save* again to save the user.

> The *User Name* and *Password* configured in the above steps are required when installing the agents.

To configure Host To Template Associations for Windows and Linux agents:

There are many predefined *Windows Agent Monitor Templates* and *Linux Agent Monitor Templates* available within FortiSOC. You can use or clone these templates according to your needs. If needed, you can also create new templates from scratch.

Once you have decided the agent monitor template, set up a host to template association between the agent and the FortiSOC service using the steps below.

1. Go to *SIEM > Settings > Setup > Windows Agent*.
2. Under *Host To Template Associations*, click the *Add* icon (+).
   The *Host To Template Associations* dialog displays.
3. In the *Name* field, enter a name for the host to template association.
4. For the *Template* field, select the agent monitor template.
5. For the *Collector* field, select the Collector.
6. Click *Save*.
7. To refresh the list and display the new record, click the *Refresh* icon above the *Host to Template Associations* table.
8. Select the checkbox for the new record, and click the *Apply* icon to apply all changes.

To install the agent:

Install the agents on the data sources using the appropriate Installation Guide on the Fortinet FortiSIEM Document Library.

- FortiSIEM Windows Agent Installation Guide
- FortiSIEM Linux Agent Installation Guide

To check the agent health:

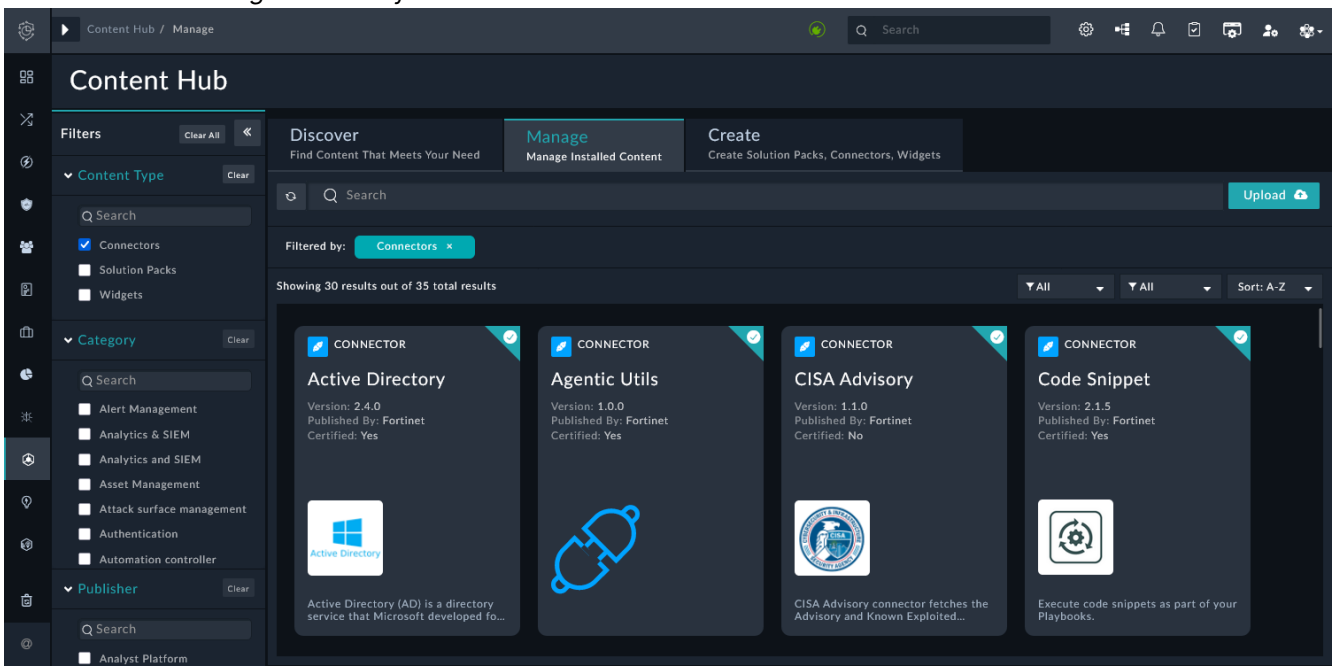
You can find information about the agent's health in the FortiSOC GUI:

- In *SIEM > Settings > Health > Agent Health*, view the *Agent Status*.
- In *SIEM > CMDB > Devices*, view the device status. If the status is *Active*, FortiSOC can receive logs from this device.

Connectors, APIs, and integrations

Connectors are used to send and retrieve data from various Fortinet Fabric and third-party sources. Using connectors, you can connect to external cybersecurity tools and perform various automated interactions using FortiSOC playbooks.

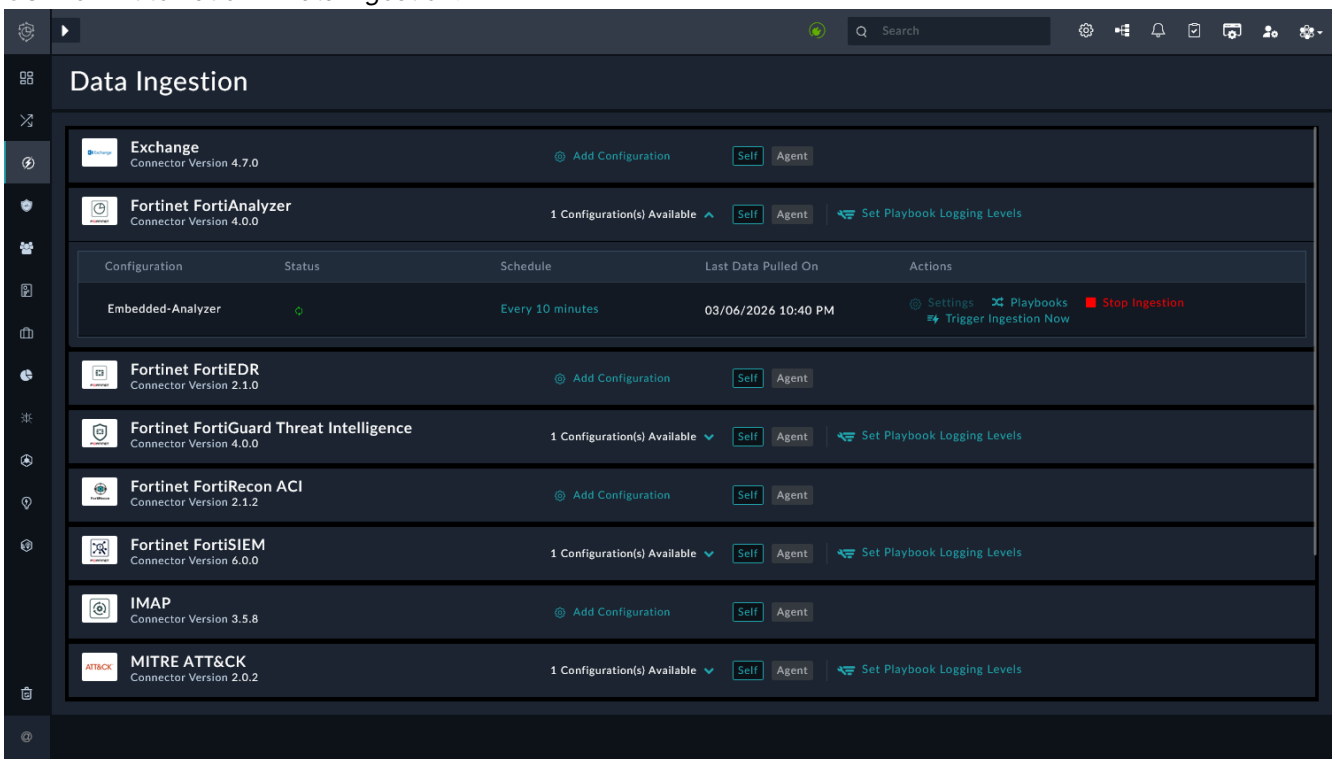
Fortinet has already developed several connectors that can be used to integrate with many external cybersecurity tools like SIEMs, such as Splunk, and ticketing systems, such as Jira. Connector-specific documentation is included with each connector to explain the process of installing, configuring, and using these connectors. You can find all published connectors, including links to their documentation, from within the FortiSOC in the *Content Hub* module. Alternatively, you can go to *Automatation* > *Connectors*, which opens *Content Hub* > *Manage* filtered by `Connectors`.



> You can view the connector specific information by selecting the *Connector*, and then clicking *Documentation*. Alternatively, you can find the connector in the FortiSOAR Connectors page of the Fortinet Document Library.

FortiSOC also includes some predefined connector configurations to establish the Analyzer and SIEM data ingestion and to enhance threat intelligence. These connectors can be viewed and managed in the FortiSOC

GUI from *Automation* > *Data Ingestion*.



Predefined connector	Description
Fortinet FortiAnalyzer	This connector is used to ingest data from the *Analyzer* module into the FortiSOC user interface. By default, this connector ingests data every 10 minutes; the schedule can be updated according to your needs.
Fortinet FortiSIEM	This connector is used to ingest data from the *SIEM* module into the FortiSOC user interface. By default, this connector ingests data every 8 minutes; the schedule can be updated according to your needs.
Fortinet FortiGuard Threat Intelligence	FortiGuard Threat Intelligence is the global threat intelligence and research organization at Fortinet. This connector facilitates automated operations to check IP, URL, Domain and File Hash Lookup's and ingestion of daily threat feeds. For example, this connector allows analysts to leverage tools in the *Threat Intel Management* module, such as the *Threat Intel Search* and the *Indicators* pages.
MITRE ATT&CK	The MITRE ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies. This connector helps to replicate the knowledge base of adversary tactics and techniques based on real-world observations. Analysts can leverage the data for threat hunting and to correlate records (alerts, assets, identities, cases, and so on) based on techniques/sub-techniques. In particular, analysts can review this information in *Threat Intel Management* > *MITRE ATT&CK* pane. By default, this connector is schedule to ingest data daily at 12:01 AM; the schedule can be updated according to your needs.

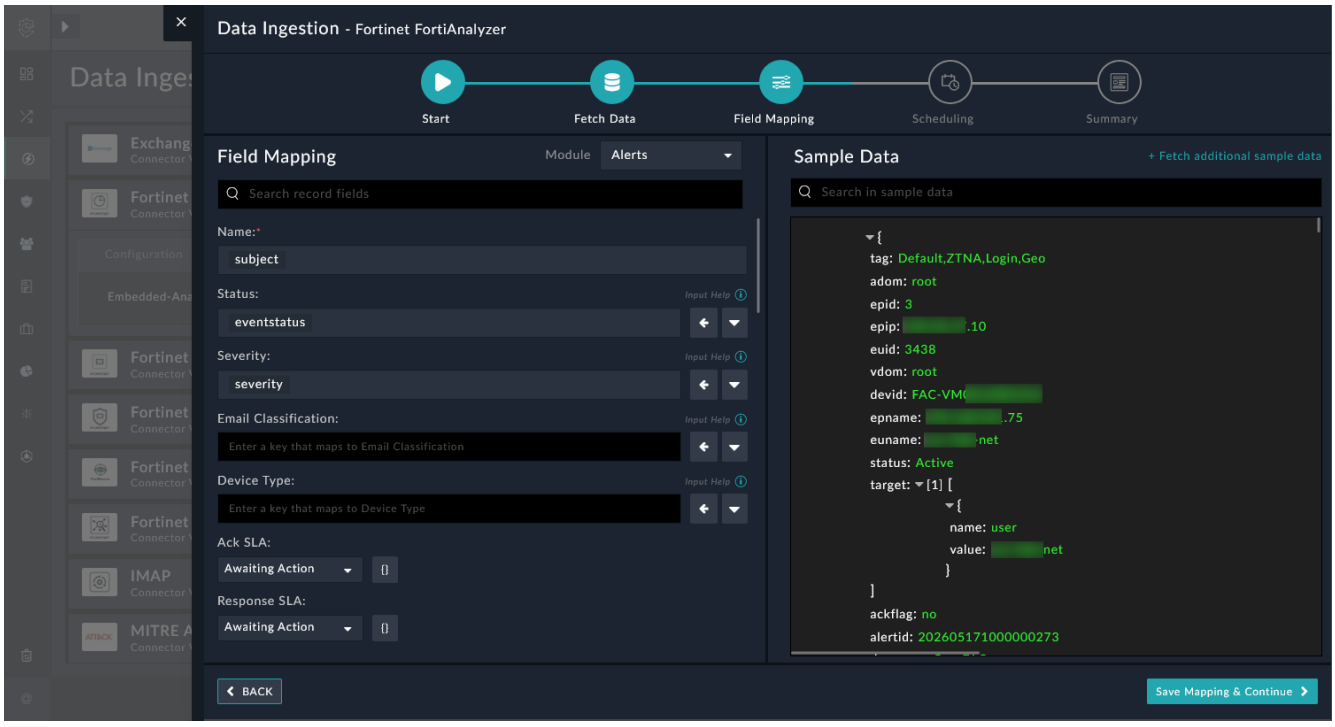
Data normalization and enrichment

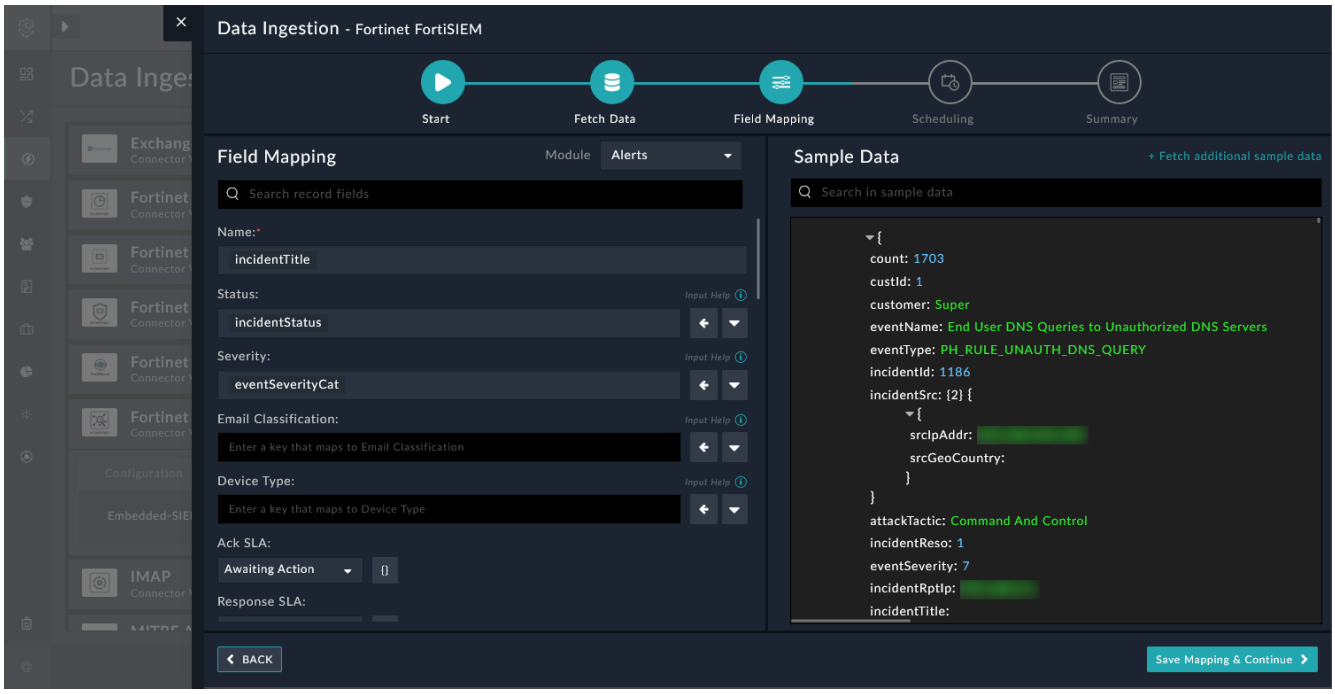
FortiSOC is used as a single-pane of glass for the SOC analysts to monitor the network, triage alerts, and respond to cases. Thus, it is critical that the ingested data from logging security devices and other integrations be normalized to effectively triage and correlate alerts/cases. As part of the normalization process, FortiSOC will also automatically enrich alerts and cases with information from other ingested data, including asset and identity information. This further enhances alerts and cases with correlation information, greatly supporting the triage process for SOC analysts.

Data normalization

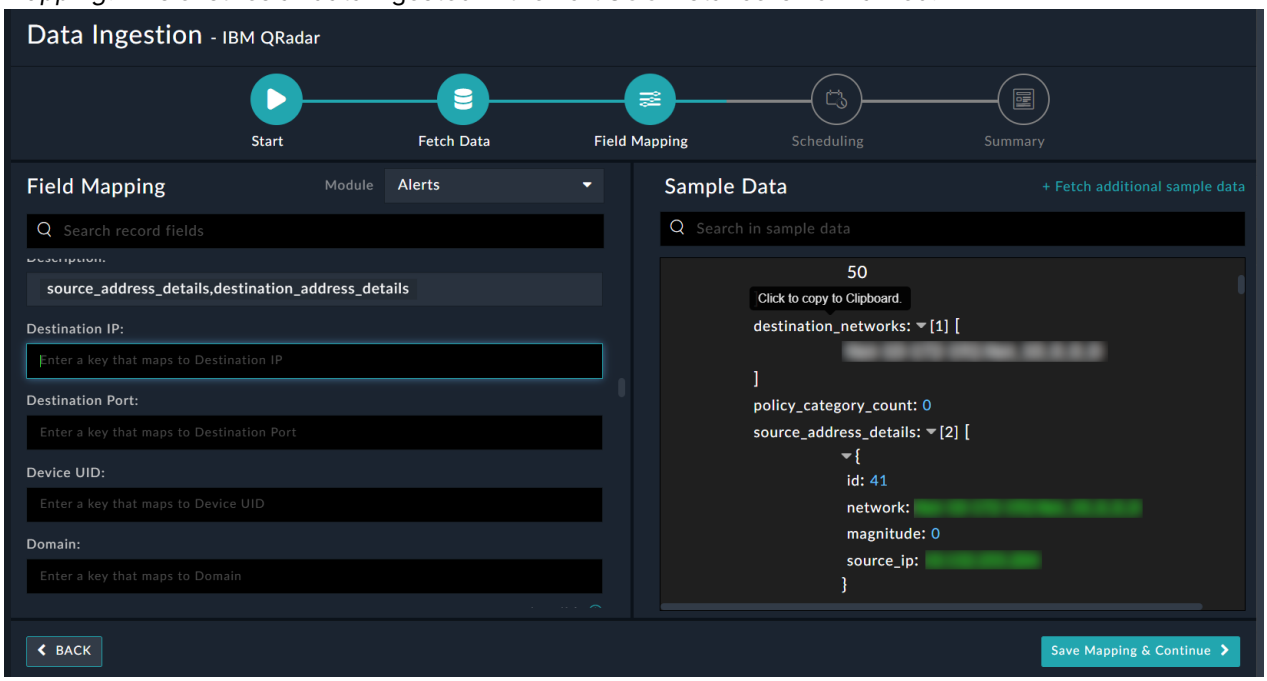
Data normalization in FortiSOC is accomplished using *Field Mapping* defined in connectors for data ingestion. This field mapping indicates which FortiSOC fields are represented by fields in the raw data. For example, the `eventstatus` from the *Analyzer* module maps to the `Alert Status` in FortiSOC alerts.

The *Field Mapping* is preconfigured in the predefined *Fortinet FortiAnalyzer* and *Fortinet FortiSIEM* connectors, which are used ingest data from the *Analyzer* and *SIEM* modules, respectively. The data ingested from these modules into FortiSOC alerts, cases, and so on, are normalized and can be easily correlated as part of alert triage and response. If custom fields must be added according to your organization's unique needs, they can be added in the *Field Mapping* configuration for these connectors.





When adding other connectors in FortiSOC from the *Content Hub*, you will be prompted to configure the *Field Mapping*. This ensures all data ingested in the FortiSOC instance is normalized.



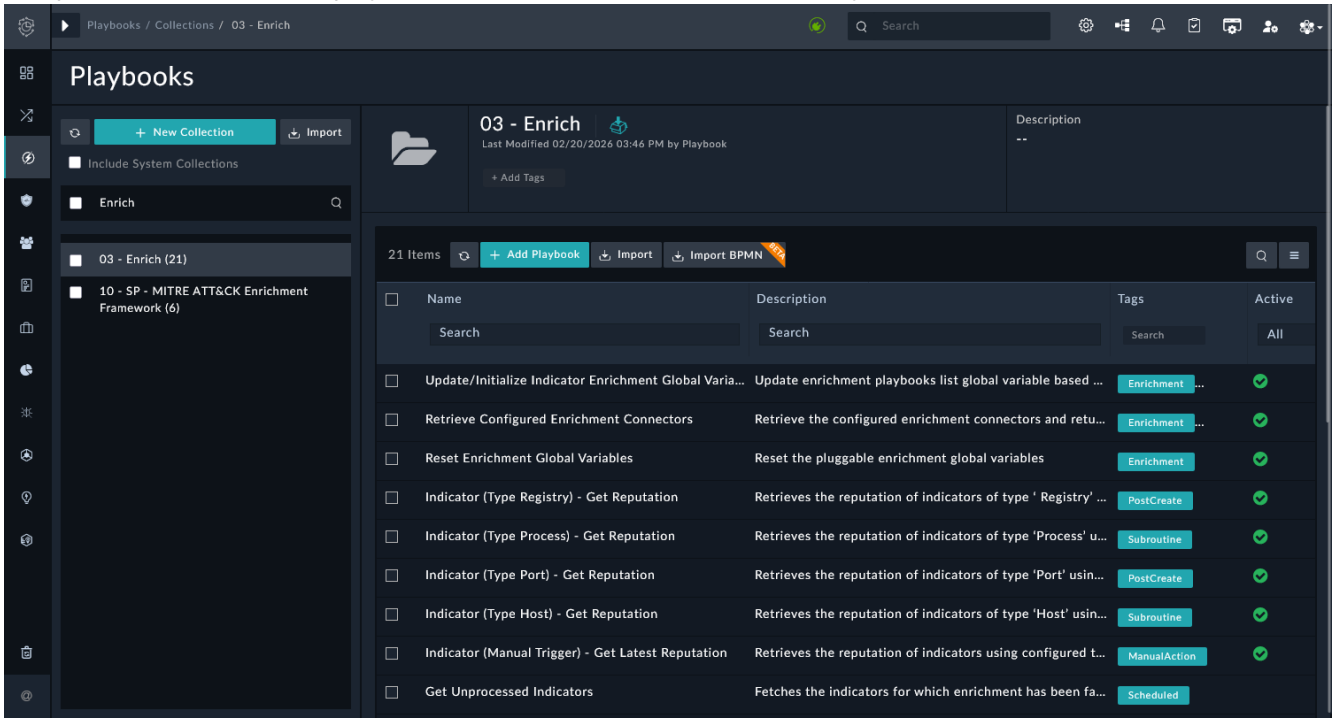
For more information about configuring *Field Mapping*, see the *Data Ingestion* section of the Connectors Guide.

Enrichment

When data is ingested to FortiSOC from the *SIEM* and *Analyzer* modules, information is extracted so it can be used for enrichment. Predefined playbooks automatically run to fetch data such as identities, assets, indicators of compromise (IoCs), and more from the alerts so they can be correlated to other alerts and cases in FortiSOC.

These playbooks ultimately automate the initial triage process for SOC analysts, correlating alerts, cases, UEBA, and more to support further triage and response.

The predefined enrichment playbooks can be found in *Automation* > *Playbooks* > *Enrich*.



Below is a brief, high-level summary of data normalization and enrichment:

1. The *Analyzer* and *SIEM* modules collect logs and alerts from connected devices.
2. Data ingestion runs in FortiSOC to ingest the data from the *Analyzer* and *SIEM* modules, normalizing the data according to the configured *Field Mappings*.
3. Playbooks run in FortiSOC to extract UEBA, IoC, and other information as data is ingested.
4. Playbooks run in FortiSOC to enrich the existing and newly ingested alerts with the extracted information.
5. Playbooks run in FortiSOC to group alerts.
6. Escalation rules in FortiSOC escalate select alerts/grouped alerts to cases.
7. The FortiSOC GUIs, such as the *Cases & Alerts*, display the normalized, enriched, and correlated information for the SOC analysts.

Assets and identity context

Assets represent your attack surface, including machines like computers, servers, and laptops as well as mobile devices, network devices, IoT devices, and VMs/containers. These are the main entry points in a cybersecurity breach. Knowing the assets in your network is critical to the case response lifecycle. By understanding what assets are vulnerable or already compromised, you can effectively contain the breach and perform further analysis and remediation.

Identities are the digital identities in your network, such as email addresses and user IDs. These identities can be related to multiple assets monitored by the SOC. For example, a single identity can be related to a desktop, mobile device, and various IoT devices as well. The aggregated risk of these assets based on their alerts and vulnerabilities can be useful when reporting on identities, enabling the SOC to quickly identify potential compromise.

Asset and identity inventories

An accurate inventory of both assets and identities within FortiSOC ultimately supports better grouping and correlation for alerts and cases, increasing the SOC's efficiency in reporting, threat identification, and remediation.

Assets and identities are extracted from the alerts and cases ingested by the data sources configured in the Analyzer and SIEM modules. Assets and identities can also be extracted and enriched from other connected analytics platforms (EDR, FoirtiAnalyzer, and so on) or authentication servers (Active Directory, LDAP, TACACS, and so on).

- If the extracted asset or identity **doesn't match** an existing record, it is added to the table in *Assets & Identities*.
- If the extracted asset or identity **matches** an existing record, the related alert or case is linked to the asset/identity.

Data extracted from ingested alerts and cases is often limited. Once the asset or identity is tracked, it should be further enriched with data from cases and other sources, such as other analytics platforms or authentication servers. This additional information supports with identification as well as investigation. Enrichment is completed automatically in FortiSOC using connectors to analytics platforms/authentication servers and predefined playbooks.

It is critical that the assets and identities in FortiSOC stay up-to-date in order to avoid duplicate records. Thus, the predefined playbooks regularly enrich the assets and identities with information included with the most recent associated alerts or cases. When necessary, you can also manually add, modify, and delete asset and identity records in the FortiSOC GUI.

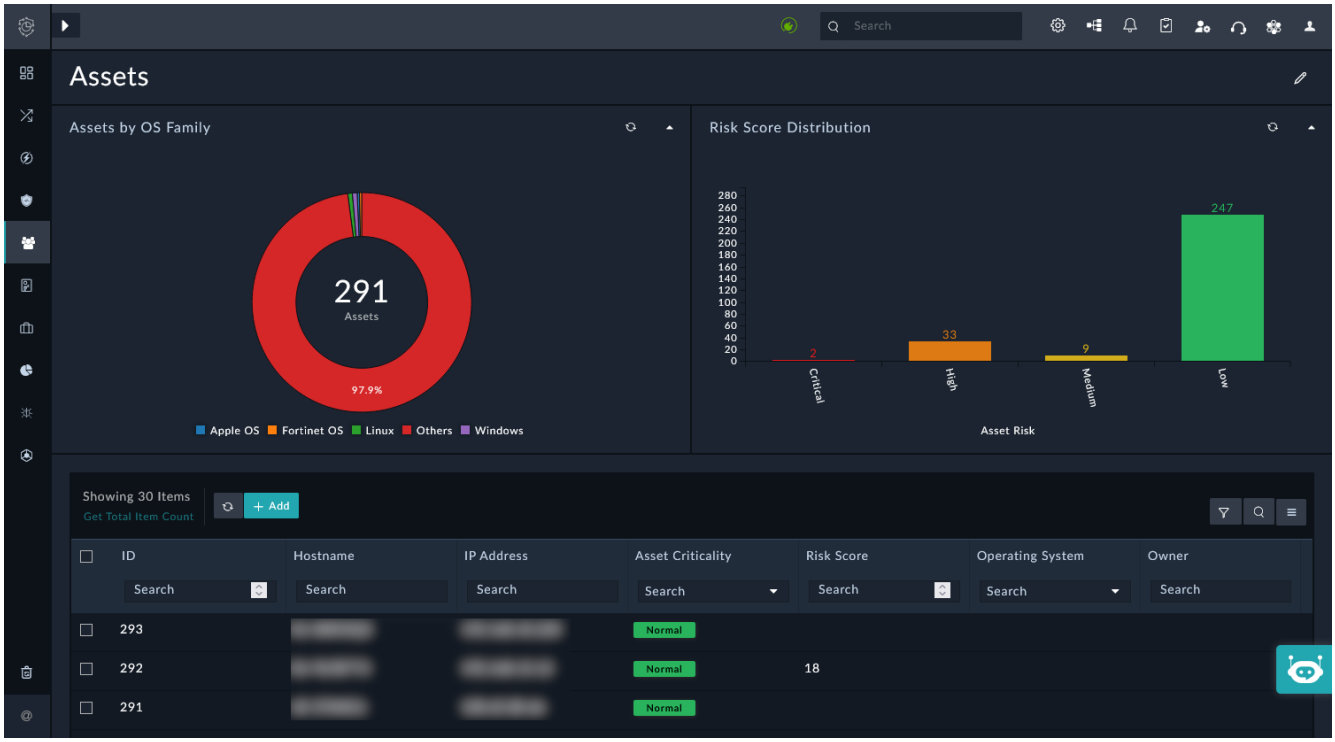
Managing assets and identities

Assets and identities can be viewed and managed in *Assets & Identities*.

Assets and identities are automatically enriched as new alerts and cases are ingested into FortiSOC. FortiSOC also periodically performs data enrichment by using playbooks to retrieve data from Analyzer and SIEM. However, if needed, you can manually add, modify, or delete the records from this module.

To manage assets:

Go to *Assets & Identities* > *Assets*.



The following charts are available above the table of records:

- *Assets by OS Family*
- *Risk Score Distribution*

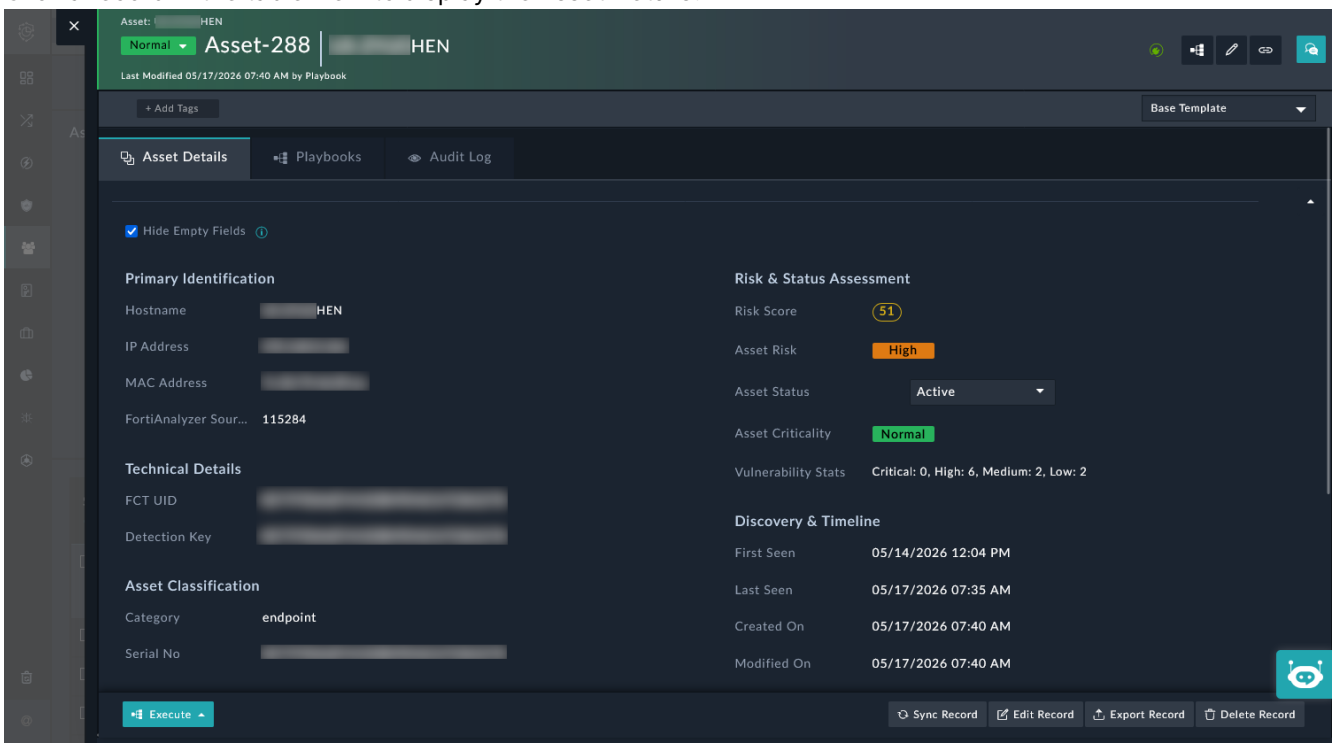
You can perform the following actions in the *Assets* table view:

- *Add* a record
- *Export* the table view

After selecting record(s) in the table you can:

- *Execute* a playbook for the record
- *Sync* records with peer
- *Clone* the record
- *Delete* the record

Click a record in the table view to display the *Asset Details*.



When you view a record, you can navigate to the following tabs:

- *Asset Details*: details about the asset, including primary identification, risk assessment, discovery timeline, correlations, and more.
- *Playbooks*: executed playbook logs for this asset.
- *Audit Log*: a timeline of audit logs, such as when the asset was created in FortiSOC and when identities were linked.

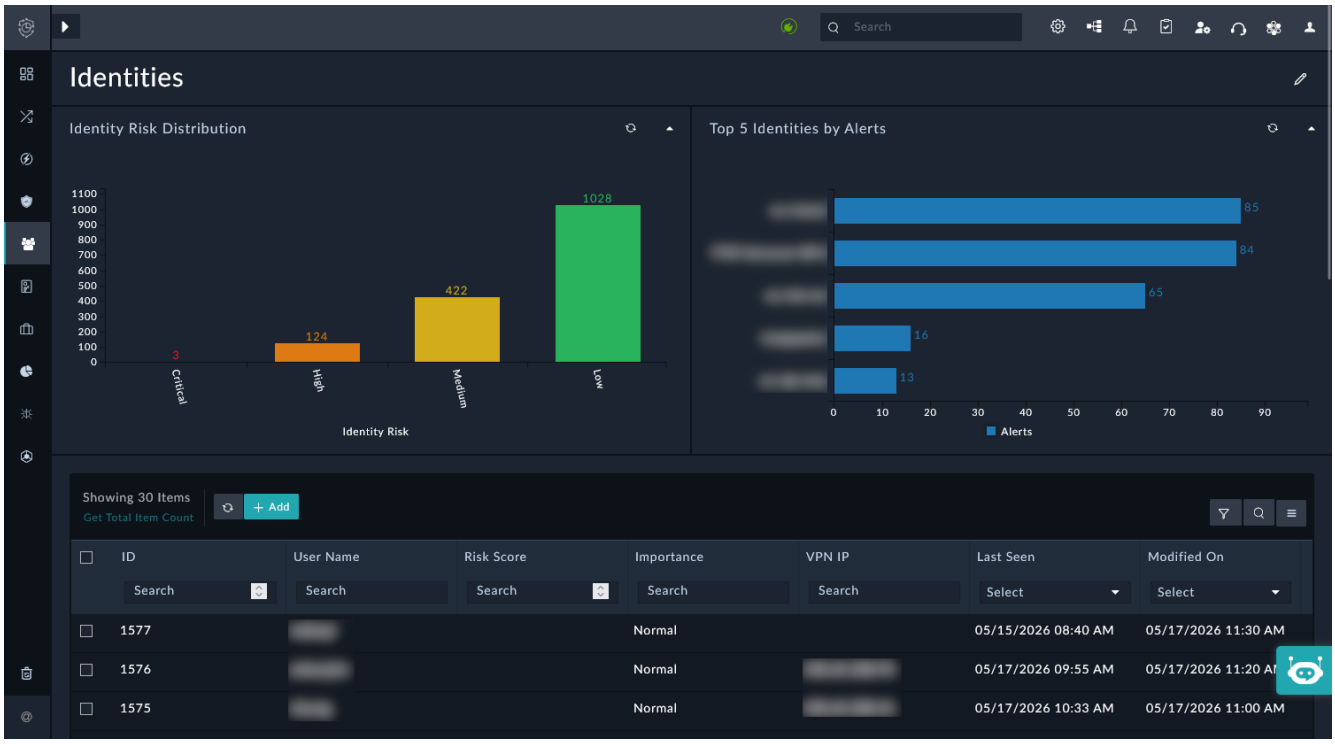
You can perform the following actions when viewing a record:

- *Execute* playbooks
- *Edit* the record
- *Export* the record
- *Delete* the record
- *Sync* the record with peer

In the *Asset Details* tab, you can also view *Correlations* and *Source Data* at the bottom of the pane. *Correlations* includes identities, alerts, cases, and more that are correlated with the asset to support effective triage. You can *Add*, *Link*, or *Execute* playbooks for the correlated records directly from these table views.

To manage identities:

Go to *Assets & Identities* > *Identities*.



The following charts are available above the table of records:

- *Identity Risk Distribution*
- *Top 5 Identities by Alerts*

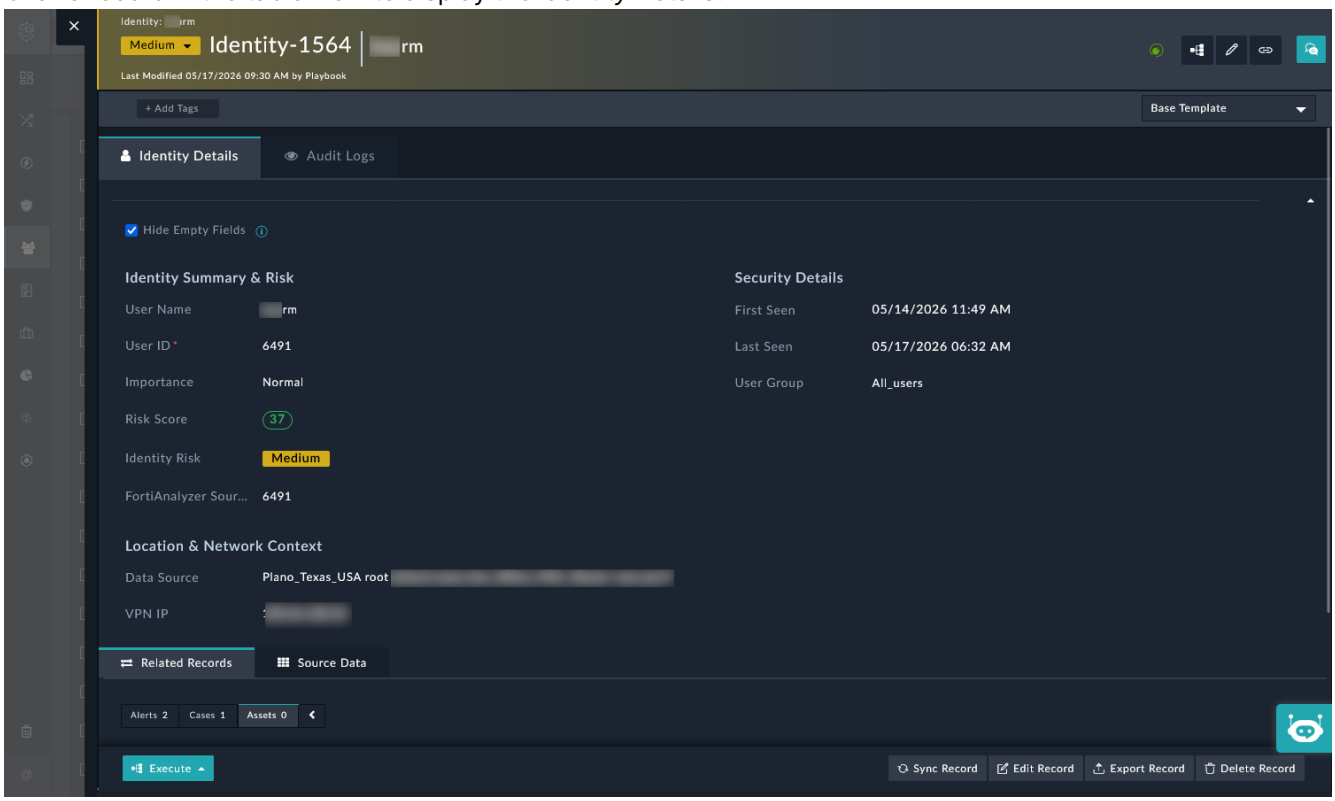
You can perform the following actions in the *Identities* table view:

- *Add* a record
- *Export* the table view

After selecting record(s) in the table you can:

- *Execute* a playbook for the record
- *Sync* records with peer
- *Clone* the record
- *Delete* the record

Click a record in the table view to display the *Identity Details*.



When you view a record, you can navigate to the following tabs:

- *Identity Details*: details about the asset, including identity summary and risk, security details, location and network context.
- *Playbooks*: executed playbook logs for this identity.
- *Audit Log*: a timeline of audit logs, such as when the identity was created in FortiSOC and when assets were linked.

You can perform the following actions when viewing a record:

- *Execute* playbooks
- *Edit* the record
- *Export* the record
- *Delete* the record
- *Sync* the record with peer

In the *Identity Details* tab, you can also view *Related Records* and *Source Data* at the bottom of the pane. *Related Records* includes alerts, assets, and cases related to the identity, supporting effective triage. You can *Add*, *Link*, or *Execute* playbooks for the related records directly from these table views.

Entity correlation and context enrichment

When alerts and cases are ingested into FortiSOC, playbooks are automatically run to extract the assets and identities. As part of these playbooks, FortiSOC will also enrich the existing assets and identities with the latest information, including additional details and the latest risk score. The playbooks will also correlate the assets and identities to each other and to other records, such as alerts, cases, indicators, and more. This provides strong visibility in FortiSOC for alert triage and response.

Playbooks can also be manually run in FortiSOC to link assets and identities.

> It is important to have assets and identities well defined in the systems that FortiSOC is ingesting the data from; this can improve triaging in FortiSOC and reduce the risk of redundant assets and identities that impede effective correlation.

For the Analyzer data sources, the enrichment playbooks can be found in *Automation* > *Playbooks* > *FortiAnalyzer Assets & Identities*.

For SIEM data sources, the entities are not periodically ingested. They are always ingested in runtime when an alert is ingested.

Similarly, playbooks are used in FortiSOC when entities are pulled from other analytics platforms or authentication servers. Some of these playbooks may need to be cloned after installing the related connector; for example, see the sample playbooks included with the Active Directory connector, available through the *Content Hub* in the FortiSOC GUI.

Risk context

Risk context is included in the details for assets and identities in FortiSOC. This provides a brief summary of the entities risk to the network, so the SOC analysts can take appropriate action for triage or remediation.

In the *Asset Details*, you can view the risk context in the *Risk & Status Assessment*.

In the *Identity Details*, you can view the risk context in the *Identity Summary & Risk*.

The risk context includes the asset criticality / identity importance, asset status, and asset vulnerability status. It also includes the *Risk Score* and *Asset Risk / Identity Risk*, which can support analysts with a quick view of the risk the entity poses to the network.

Risk Score

The *Risk Score* is a score from 0 (no *Risk Score*) to 100 that represents how at-risk the asset or identity is to potential threats. The score appears with a color to represent the *Asset Risk / Identity Risk*.

Risk Score	Description
70-100	Critical (red)

Risk Score	Description
40-69	High (orange)
20-39	Medium (yellow)
0-19	Low (green)

The *Risk Score* is calculated differently according to the data ingestion source (Analyzer / SIEM) using proprietary algorithms.

The *Risk Score* allows the analysts to quickly and effectively prioritize threat mitigation and response. For example, a high risk asset may require immediate updates, or a critical risk asset may need to be quarantined for remediation.

Detection and analytics administration

FortiSOC has built-in detection rules to trigger alerts from incoming logs. These rules can be tuned according to your needs in order to reduce noise from false positives. You can also create your own custom detection rules for security events that may be impacting your network. FortiSOC includes detection testing and validation, so you can effectively review the detection criteria against sample logs, validating their use case in your SOC.

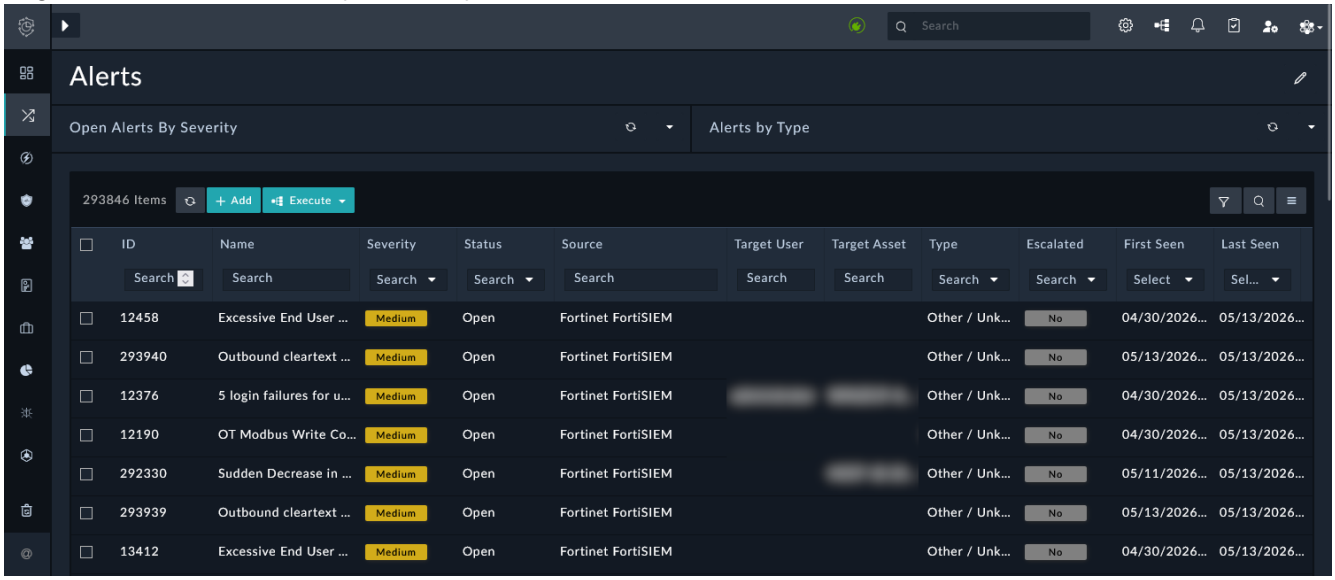
Key terms

- **Detection rules**: Detection rules define the logic for generating alerts from collected event logs.
  - **Event handlers**: Event handlers configured in the *Analyzer* module contain detection rules. The detection rules within these event handlers define when alerts will be triggered by incoming event logs to the *Analyzer* module.
  - **Rules**: "*Rules*" configured in the SIEM module are detection rules. These *Rules* define when alerts will be triggered by incoming event logs to the *SIEM* module.

The detection rules are configured according to module that is collecting the event logs:

- *Analyzer > Detection & Automation > Event Handlers*
- *SIEM > Resources > Rules*

The Analyzer *Event Handlers* will only generate alerts using devices configured in the *Analyzer* module, and the SIEM *Rules* will only generate alerts using devices configured in the *SIEM* module. FortiSOC will correlate and display all generated alerts in the *Cases & Alerts > Alerts* modules. The *Source* column indicates where the alert originated: *Fortinet FortiAnalyzer* (Analyzer) or *Fortinet FortiSIEM* (SIEM).



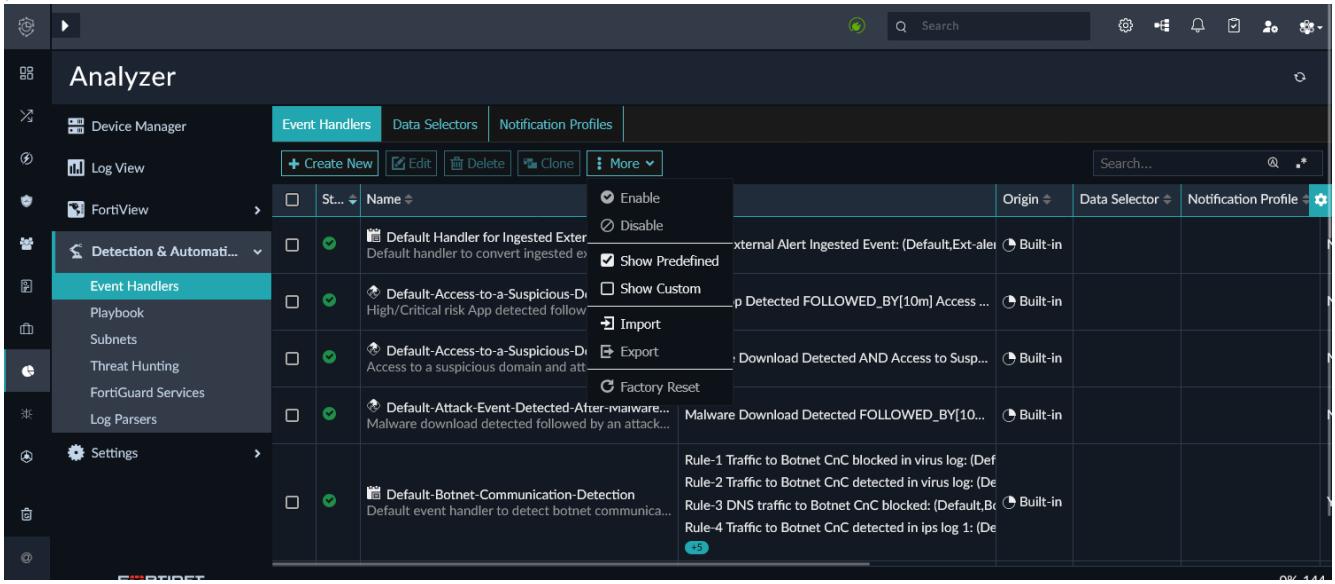
Predefined detection rules

The predefined detection rules can be found in the module that is collecting the data, *Analyzer* or *SIEM*. Keep in mind that detection rules will generate alerts using the data collected in its respective module. The alerts will then be ingested into FortiSOC for correlation and enrichment.

Many predefined detection rules are enabled by default; however, some must be enabled manually when the use case is deemed appropriate for your network.

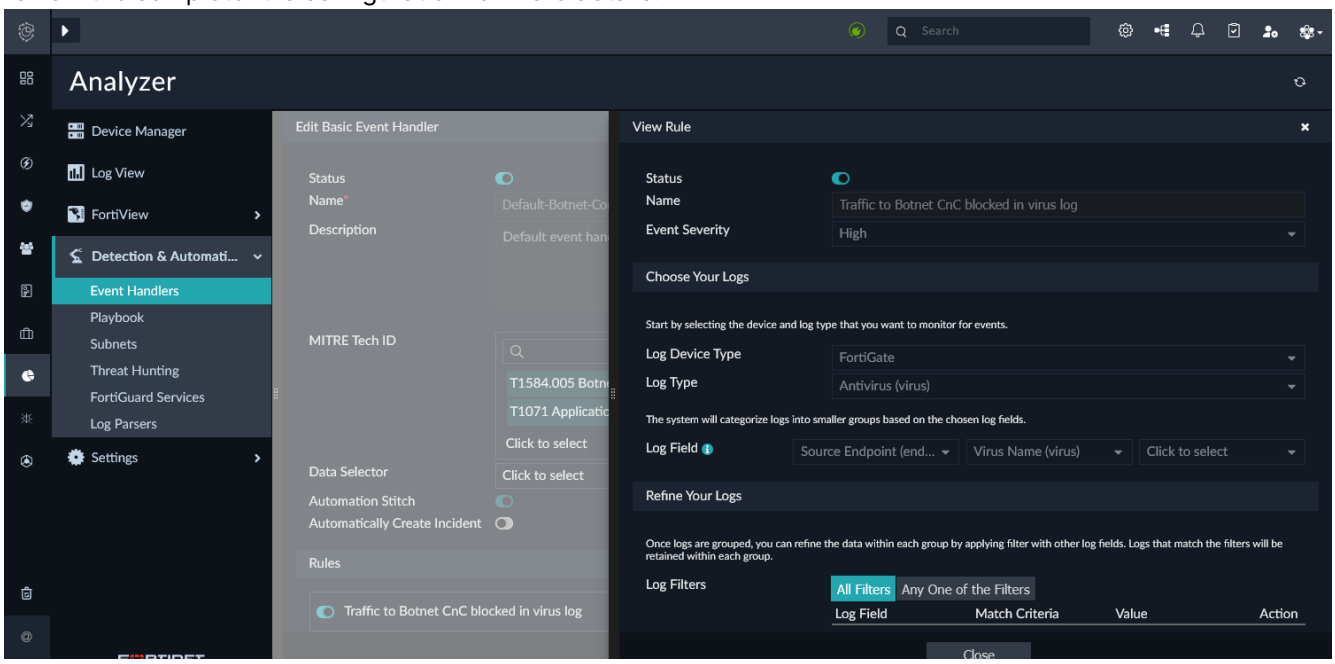
Predefined Analyzer event handlers

The predefined Analyzer event handlers can be found in *Analyzer > Detection & Automation > Event Handlers > Event Handlers*. From the *More* dropdown, select *Show Predefined* and deselect *Show Custom* to list only the predefined event handlers.



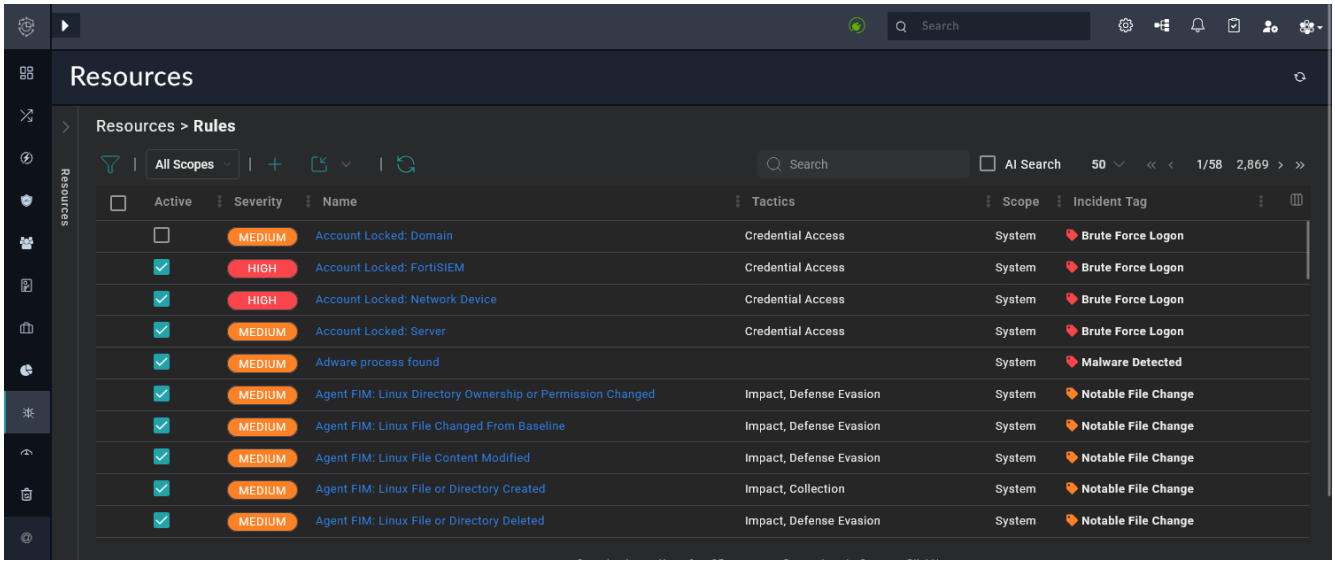
Double-click an event handler to view its rules for generating alerts using devices and logs in the *Analyzer* module. The rule names provide a summary of the criteria in event logs that will generate alerts; you can also

review the complete rule configuration for more details.



Predefined SIEM rules

The predefined SIEM rules can be found in *SIEM* > *Resources* > *Rules*. These rules define the criteria for generating alerts using devices and logs in the *SIEM* module. For a complete list of SIEM detection rules, see FortiSIEM Rules.

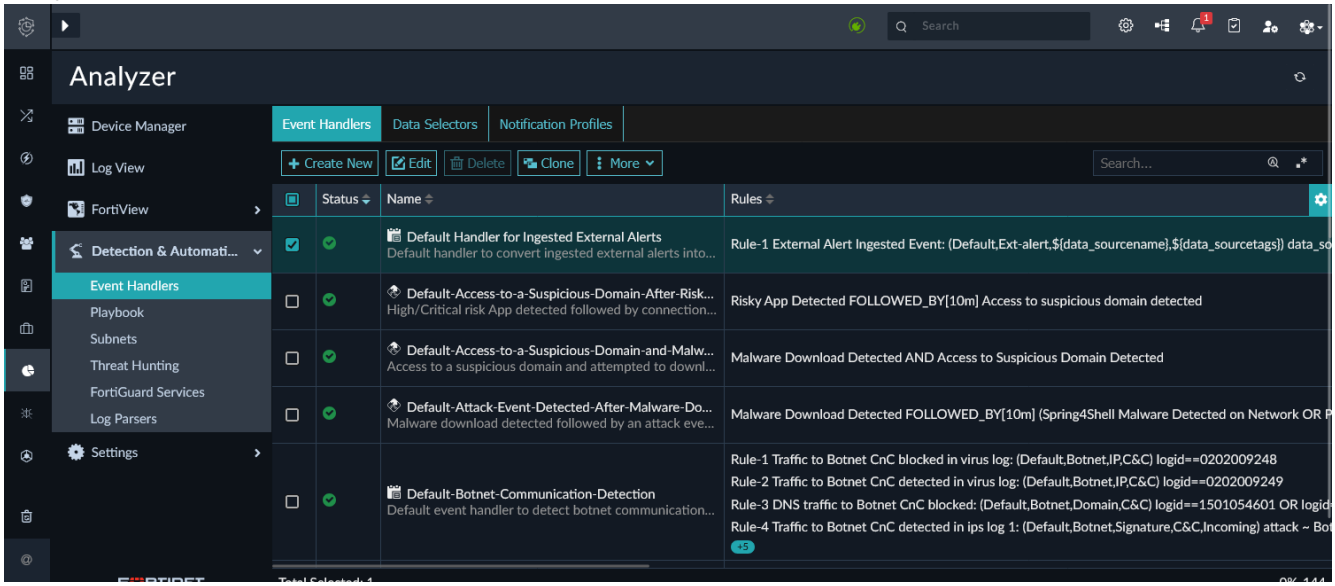


Creating and customizing detection rules

You can create an customize detection rules from the respective module that is collecting the data, *Analyzer* or *SIEM*.

Creating Analyzer detection rules

Analyzer detection rules are configured within event handlers. The Analyzer event handlers can be configured in *Analyzer > Detection & Automation > Event Handlers*.



Event handlers contain detection rules that use logs from the authroized devices in the *Analyzer* module to generate alerts. These rules define criteria for generating alerts according to device types, log types, and log filters.

There are two types of event handlers. The type is defined when creating the event handler:

- *Basic*: an alert is generated when one of the rules in the event handler is met. Each rule in the basic event handler has an OR relationship with the others.
- *Correlation*: an alert is generated when a set of rules are met in correlation sequence. For correlation handlers, you can define both the rules and the operators that correlate them (AND, AND_NOT, OR, FOLLOWED_BY, and NOT_FOLLOWED_BY).

In *Analyzer > Detection & Automation*, you can also configure the data selectors and notification profiles that can be used in the event handlers.

- *Data Selectors*: Data selectors are used to select devices, subnets, and filters for event handlers. The filters in the data selector are applied before every rule configured in the event handler. This means the filter criteria does not need to be added individually within each rule of the event handler(s) that the data selector is assigned to.
- *Notification Profiles*: Notification profiles are used to send alert notifications when an event is generated by an event handler. You can configure the notification profile to send the alert to an email address, SNMP community, and/or syslog server.

To configure an event handler:

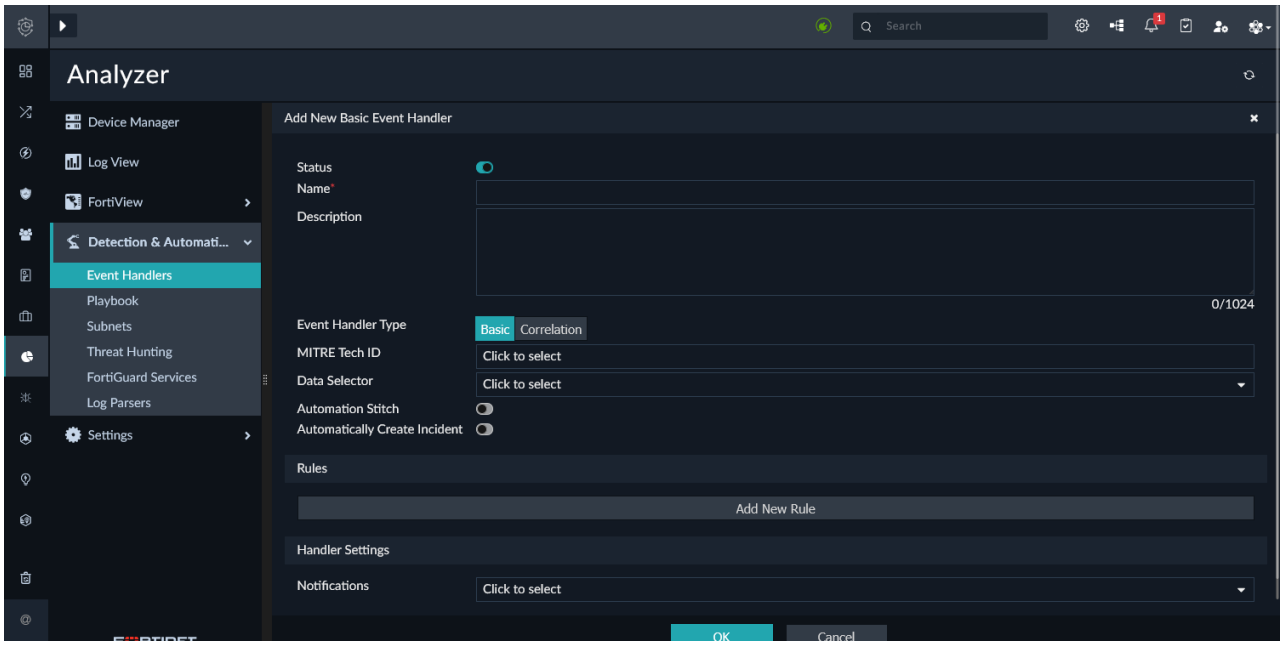
1. In the FortiSOC GUI, go to *Analyzer* > *Detection & Automation* > *Event Handlers* > *Event Handlers*.
2. Click *Create New*.

   Alternatively, select an existing event handler and click *Clone* to use it as a template.

3. Configure the event handler.

   Basic event handlers

   See below for the high-level steps to creating a *Basic* event handler. For more details about the configuration options, see *Creating a custom event handler* in the FortiAnalyzer Administration Guide.

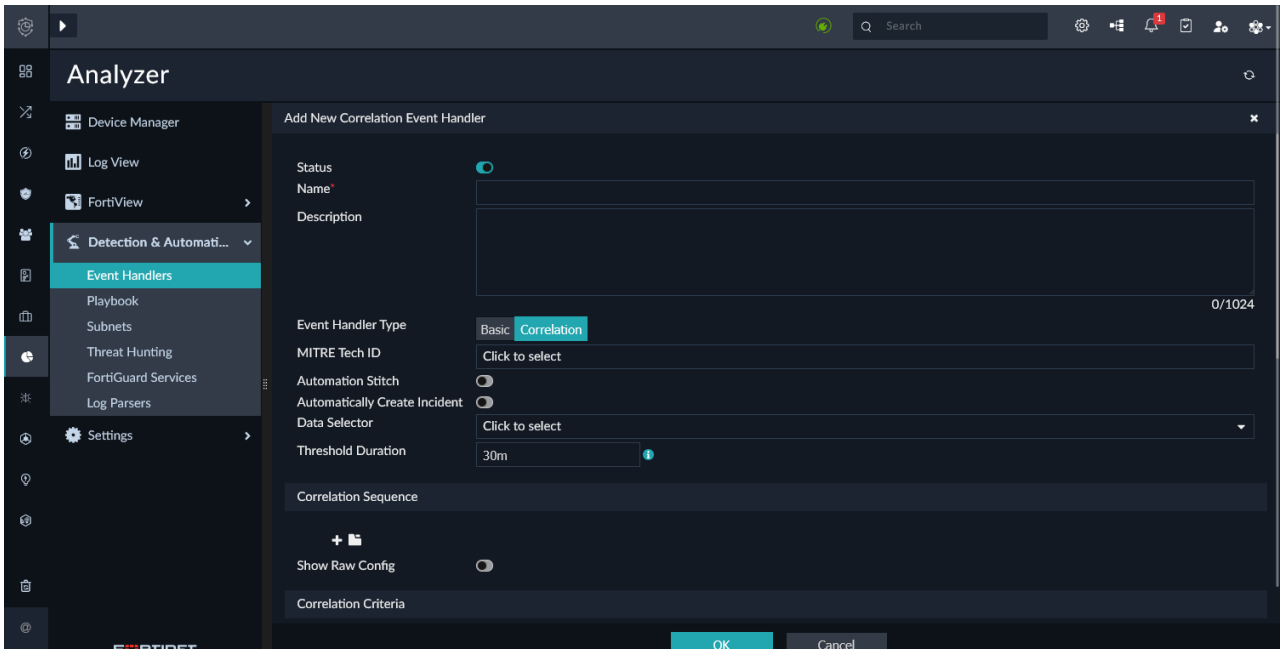


Configuration	Description
Event handler attributes	The status, name, description, event handler type (basic), MITRE techniques, data selector, and automation stitch for the event handler. You can also enable the event handler to automatically create a case, if needed.
Rules	The detection rules for generating alerts. 1. *Choose Your Logs*: Start by selecting the device and log type that you want to monitor for events. Choose log fields to categorize logs into smaller groups. 2. *Refine Your Logs*: Once logs are grouped, you can refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group. 3. *Define Event Conditions*: Once you've organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group. 4. *Advanced Settings*: Optional configuration for the event type

Configuration	Description
	override, event message, event status, tags, and indicators.
Handler Settings	The notification profile for the event handler.

Correlation event handlers

See below for the high-level steps to creating a *Correlation* event handler. For more details about the configuration options, see *Creating a custom correlation handler* in the FortiAnalyzer Administration Guide.



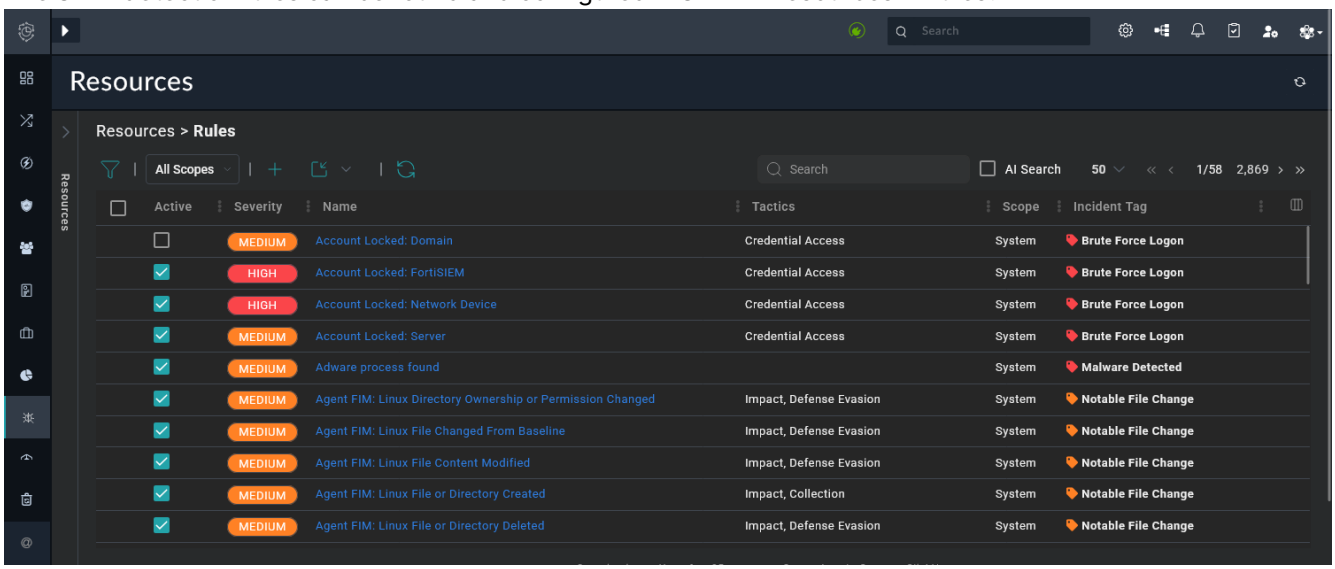
Configuration	Description
Correlation event handler attributes	The name, description, event handler type (correlation), MITRE techniques, automation stitch, data selector, and threshold duration for the correlation handler. You can also enable the event handler to automatically create a case, if needed.
Correlation Sequence	The detection rules in sequence and logic group for generating alerts. 1. *Choose Your Logs*: Start by selecting the device and log type that you want to monitor for events. Choose log fields to categorize logs into smaller groups. 2. *Refine Your Logs*: Once logs are grouped, you can refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group. 3. *Define Event Conditions*: Once you've organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group.
Correlation Criteria	The correlation criteria to specify the type of logs that the event handler will look for. The criteria is applied to two rules on a field from each rule.

Configuration	Description
Handler Settings	The event fields, including the event type override, event message, event status, event severity, indicators, and tags. This section also includes the notification profile for the correlation handler.

4. Click *OK* to save the event handler.

Creating SIEM detection rules

The SIEM detection rules can be found and configured in *SIEM* > *Resources* > *Rules*.



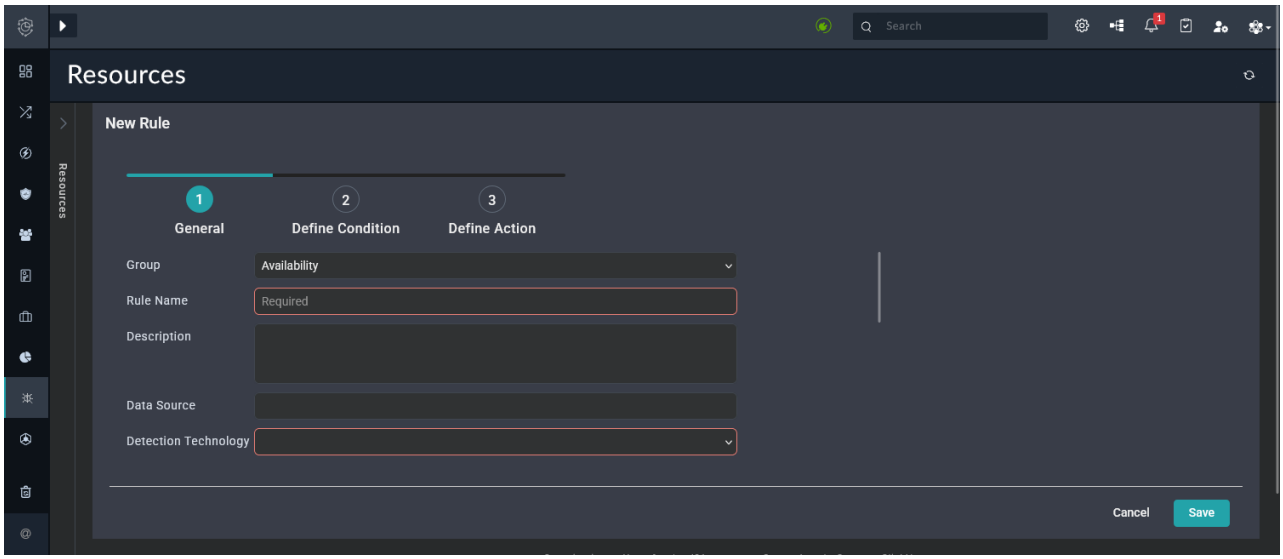
The SIEM rules use data from various third-party sources in the *SIEM* module to generate alerts. These rules define the applicable data source and the conditions that, when met by the incoming data, will generate an alert.

To configure SIEM rules:

1. In the FortiSOC GUI, go to *SIEM* > *Resources* > *Rules*.
2. Click + to create a new rule.

   Alternatively, select an existing rule and click the *Clone* icon to use it as a template.

3. There are three steps to the rule configuration:



Configuration step	Description

General	Define the general configuration for the rule, including the:
	• Group
	• Name
	• Description
	• Data Source
	• Detection Technology
	  • *Correlation*: Uses an association between variables for discovery.
	  • *Correlation Using Lookup Table*: Uses lookup table for discovery.
	  • *Machine Learning*: Uses machine learning models for discovery.
	  • *Profiling*: Collects specific data for discovery.
	• Event Type
	• Evaluation Mode
	  • *Streaming*: Streaming rules run in real-time.
	  • *Scheduled*: Scheduled rules run on a defined schedule.
	  • *Scheduled via SQL*: Scheduled via SQL rules will run a rule based off a SQL query.

Define Condition	Configure the rule conditions, which define the event attributes and thresholds that will trigger an alert. Rule conditions are built from subpatterns of event attribute filters and aggregation functions. You can specify more than one subpattern and the relationships and constraints between them. If the *Evaluation Mode* is *Scheduled via SQL*, then you will instead configure the conditions using an SQL query.
Define Action	Define the attributes that will be applied to the resulting alerts, including their: • Severity

Configuration step	Description
	• Category and Subcategory • MITRE ATT&CK Techniques • Action (the alert attributes and triggered attributes that will be generated by the rule) • Tags • Impacts You can also define the: • Exceptions • Notification frequency • Watch list • Clear conditions Exception and clear conditions can be used to reduce noise for SOC analysts. For more information, see Tuning detection rules for noise reduction on page 57.

For more details about the configuration options, see *Creating Rules* in the FortiSIEM User Guide.

Tuning detection rules for noise reduction

FortiSOC administrators and SOC analysts should regularly review the detection rules to ensure they are generating relevant alerts that represent real security events in the network. For example, if detection rules are regularly generating alerts that are closed as false positives, then the rule conditions should be updated to account for the identified issues.

To identify problem rules, you must review the *Alert Details*, including:

- *Closure Reason*: Alerts may be closed for reasons that indicate they are simply noise, such as *False Positive* or *Invalid*.
- *Source*: The connector used as the data ingestion source, indicating which module the rule can be found in: *Fortinet FortiAnalyzer* (Analyzer) or *Fortinet FortiSIEM* (SIEM).
- *Rule Name*: The detection rule that generated the alert.

This review takes long periods of time and requires knowledge of the network to identify the root causes for the false positives. However, there may be scenarios where you can proactively identify opportunities for noise reduction. For example:

- **Impossible travel**: When an employee travels, they may access corporate resources from multiple devices, such as a cell phone and a remote PC acting as a jump station. These access attempts, originating from different locations, may trigger impossible travel alerts that could be suppressed or configured with exceptions for the appropriate timeframe.
- **High resource usage**: A heavily loaded server may trigger high resource usage events, potentially indicating a denial-of-service attack. However, if the cause high resource usage has been identified or you want to reduce alerts while SOC analysts complete investigation, you may suppress these alerts for an appropriate timeframe.

- **Server or device maintenance**: A device may have a planned upgrade, which could trigger detection rules related to their downtime. Similarly, a server may be down for a planned maintenance window, and this could trigger a *Server Down - No Ping Response* to trigger alerts from the *SIEM* module. Thus, you may suppress these alerts or configure exceptions for the planned window.

Tuning Analyzer detection rules

A playbook is available in FortiSOC to suppress alerts generated by Analyzer detection rules: *FortiAnalyzer Alert Suppression*.

Alert suppression does not have to completely prevent an rule from generating alerts. As in the impossible travel example above, the events can be suppressed according to specific criteria applied to the rule, such as suppressing only related alerts involving the user that is traveling. When you are suppressing events, the suppression criteria is based on the alert the playbook is executed against.

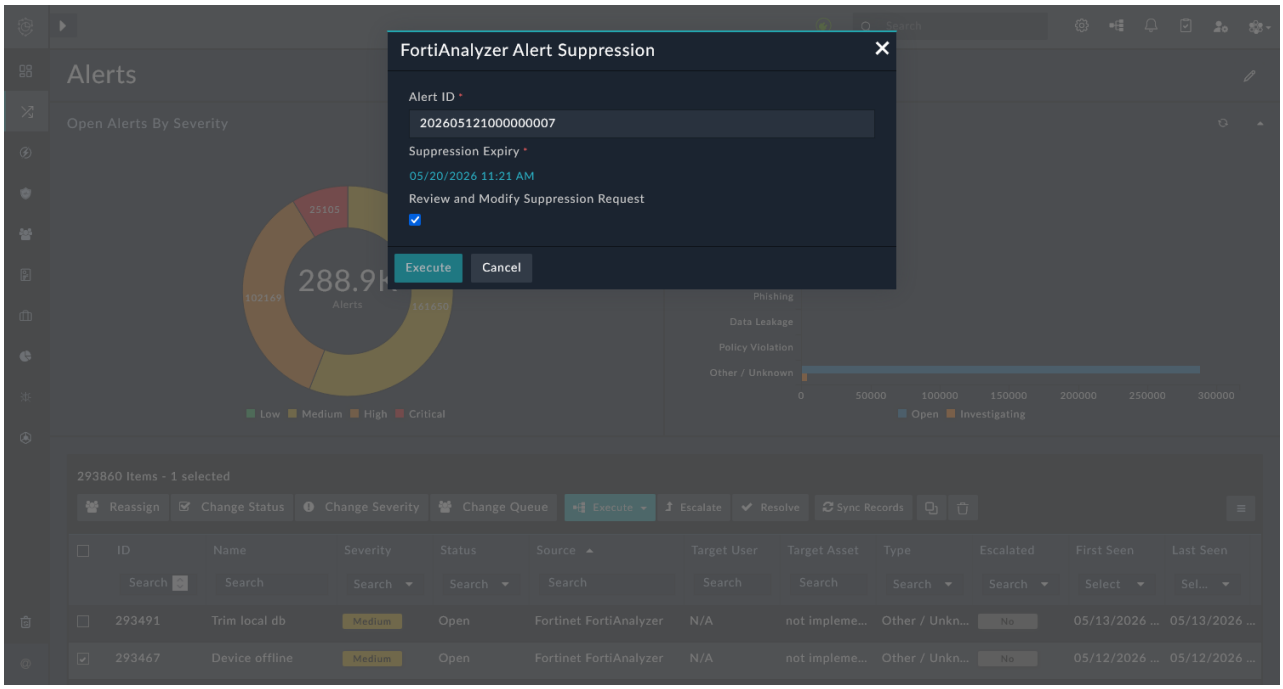
To suppress alerts from an Analyzer detection rule:

1. In the FortiSOC GUI, go to *Cases & Alerts* > *Alerts* > *Alert List*.
2. Select an alert with *Source* = *Fortinet FortiAnalyzer*.
3. From the *Execute* dropdown, select *FortiAnalyzer Alert Suppression*.

   You can also execute this playbook from the *Alert Details* or from any list that displays the alert, such as *Case Details* > *Correlations* > *Alerts*.

   This enables you to suppress alerts within the regular triage workflow without navigating somewhere else in the platform.

   The *FortiAnalyzer Alert Suppression* dialog displays. The *Alert ID* field is automatically populated with the selected alert.

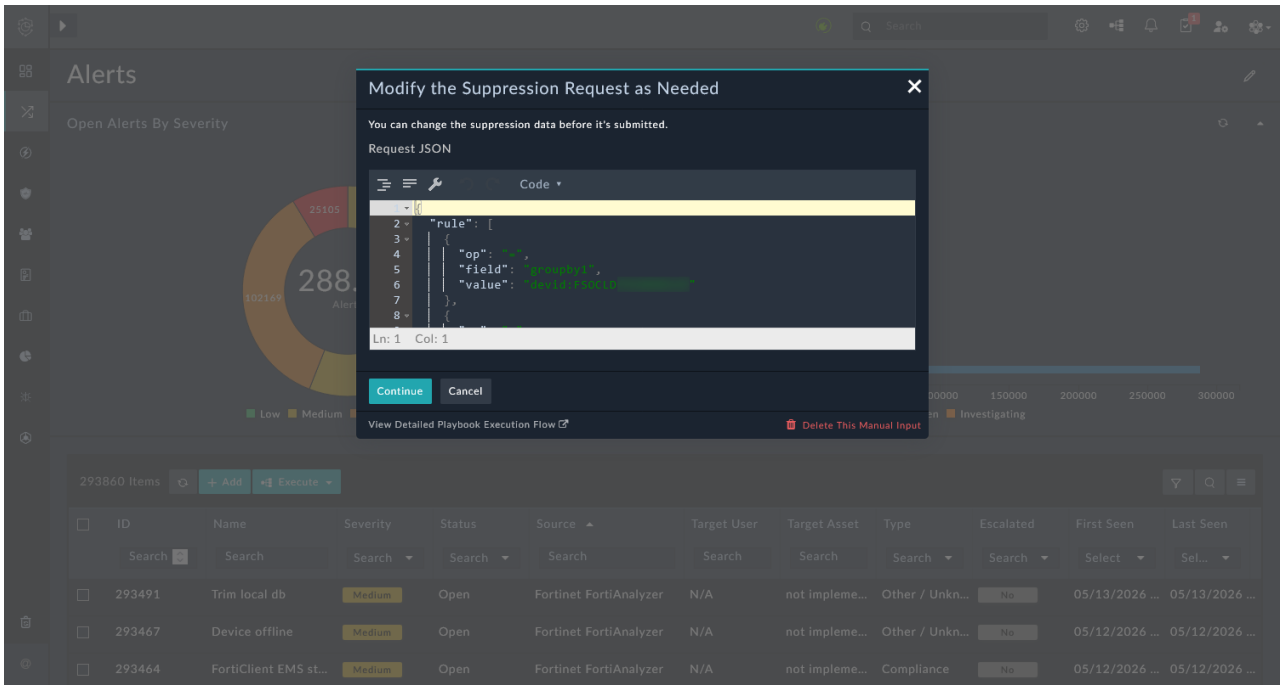


4. For the *Suppression Expiry* field, set the suppression expiry date and time.

All alerts that would have been generated by the same event handler rule as the selected alert will be suppressed until this date and time.

5. Select or deselect the *Review and Modify Suppression Request* checkbox.
6. Click *Execute*.

   If the *Review and Modify Suppression Request* checkbox was selected, the *Modify the Suppression Request as Needed* dialog displays. You can change the suppression data as needed and then click *Continue*.



To view, edit, or delete alert suppression for Analyzer detection rules:

1. Go to *Analyzer > Detection & Automation > Event Handlers > Event Handlers*.
2. Select the handler with the suppressed rule and click *Edit*.

   The *Edit Event Handler* pane displays.

   In the *Rules* section, each rule has a *Suppression* icon. This icon is only clickable when there is event suppression configured using events generated by the rule.
3. Click the *Suppression* icon for the suppressed rule.

   The *Suppress* pane displays. The configured suppression(s) display in a table view. The table will also display expired suppression.
4. From this pane, you can view, edit, and delete event suppression:
   - To view and edit, select the event suppression and click *Edit*.
   - To delete, select the event suppression and click *Delete*.

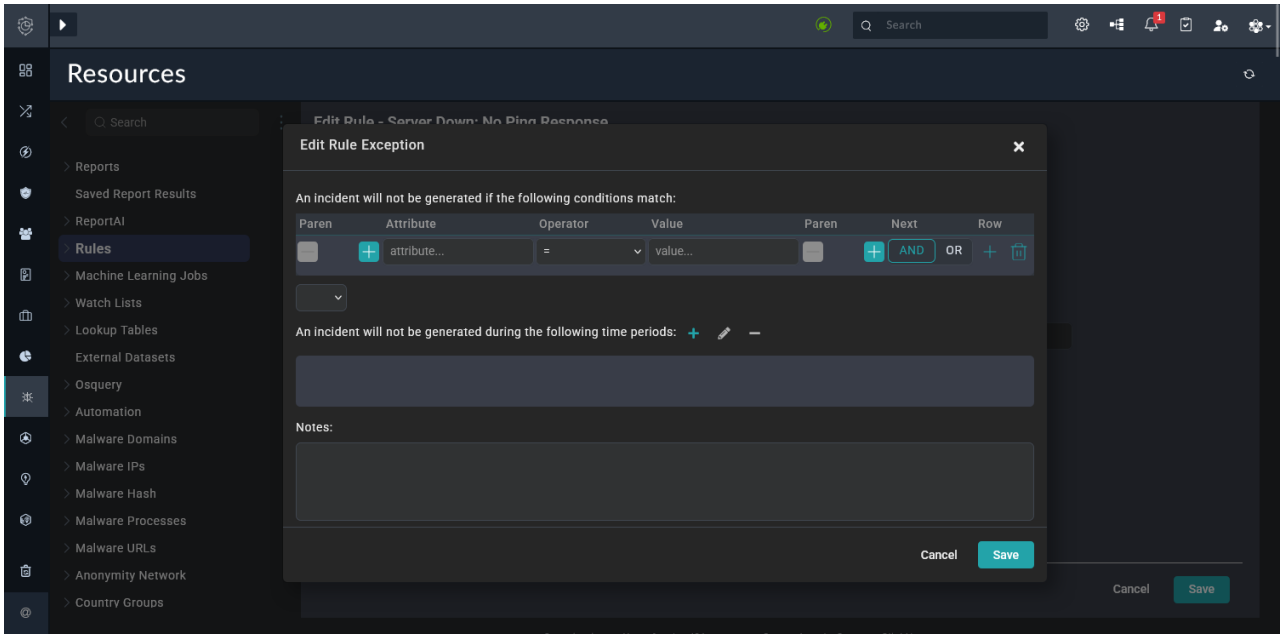
Tuning SIEM detection rules

SIEM detection rules can be configured with exceptions and clear conditions, which are used to reduce alert noise for the SOC analysts.

- *Exceptions*: Once you activate a rule, it continuously monitors your IT infrastructure for conditions that would trigger an alert. However, you may also want to define exceptions to those conditions. For example, you may know that a server will be going down for maintenance during a specific time period and you don't want your *Server Down - No Ping Response* rule to trigger an alert for it.
- *Clear*: Specify conditions in which alerts will have their status changed from *Active* to *Cleared*. You can set the time period that must elapse for the clear condition to occur, and then set the conditions based on the triggering of the original rule, or on a subpattern based on the alert attributes.

To configure exceptions for a SIEM rule:

1. Go to *SIEM* > *Resources* > *Rules*.
2. Select the rule to add exceptions to and click the *Edit* icon.
3. Go to the tab for *Step 3: Define Action*.
4. For the *Exception* field, click the *Edit* icon.
   The *Edit Rule Exception* dialog displays.

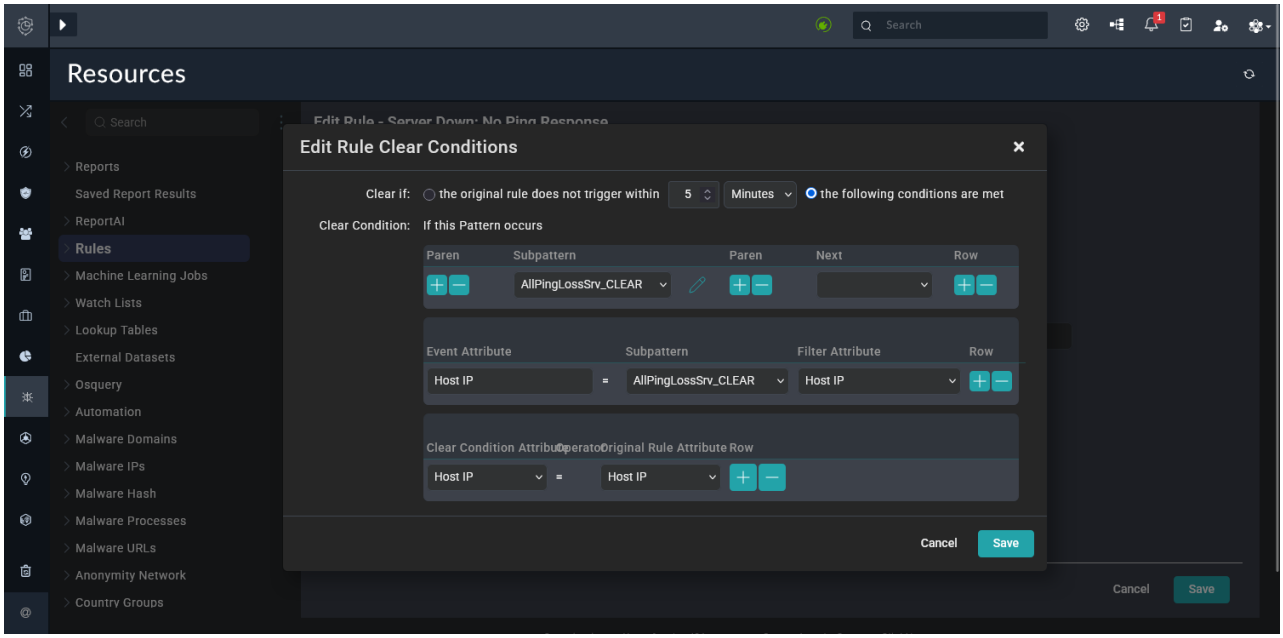


5. Select an *Attribute* and *Operator*, and enter a *Value* for the conditions that will prevent a case from being generated.
   The values in the *Attribute* menu are from the *Event Attributes* associated with the alert definition.
6. For *A case will not be generated during the following time periods*, click the + icon to set an effective time period for the exception.
   You can set effective time periods for single and recurring events, and for durations of time from hours to days.
7. In the *Notes* field, enter any notes about the exception.
8. Click *Save*.

To configure clear conditions for a SIEM rule:

1. Go to *SIEM* > *Resources* > *Rules*.
2. Select the rule to add exceptions to and click the *Edit* icon.

3. Go to the tab for *Step 3: Define Action*.
4. For the *Clear* field, click the *Edit* icon.
   The *Edit Rule Clear Conditions* dialog displays.



5. For the *Clear if* option, set the time period that should elapse for the clear condition to go into effect.
6. If you want the clear condition to go into effect based on the firing of the original rule, select the radio button for *the original rule does not trigger within*. This option is not selectable for Scheduled Rules.
   For example, if you wanted the clear condition to change the status of `Active` alerts to `Cleared` after the original rule had not been triggered for ten minutes, you would set cleared within to *10 Minutes* and select this option.
   When selected, you do not have to configure the *Clear Condition* option; you can proceed to *Save* the clear condition.
7. If you want to base the clear condition on a sub-pattern of the alert attributes, select *the following conditions are met*.
   The case attributes from your rule will load and the clear condition attributes will be set to match.
8. Define the pattern to use by clicking the *Edit* icon next to the clear subpattern.
9. Click *Save*.

Testing and validating detection rules

When activating predefined detection rules or creating custom detection rules, it is important to test them and validate the resulting alerts. This testing ultimately minimizes noise for the SOC analysts, ensure the alerts ingested by FortiSOC are relevant security events that should be triaged.

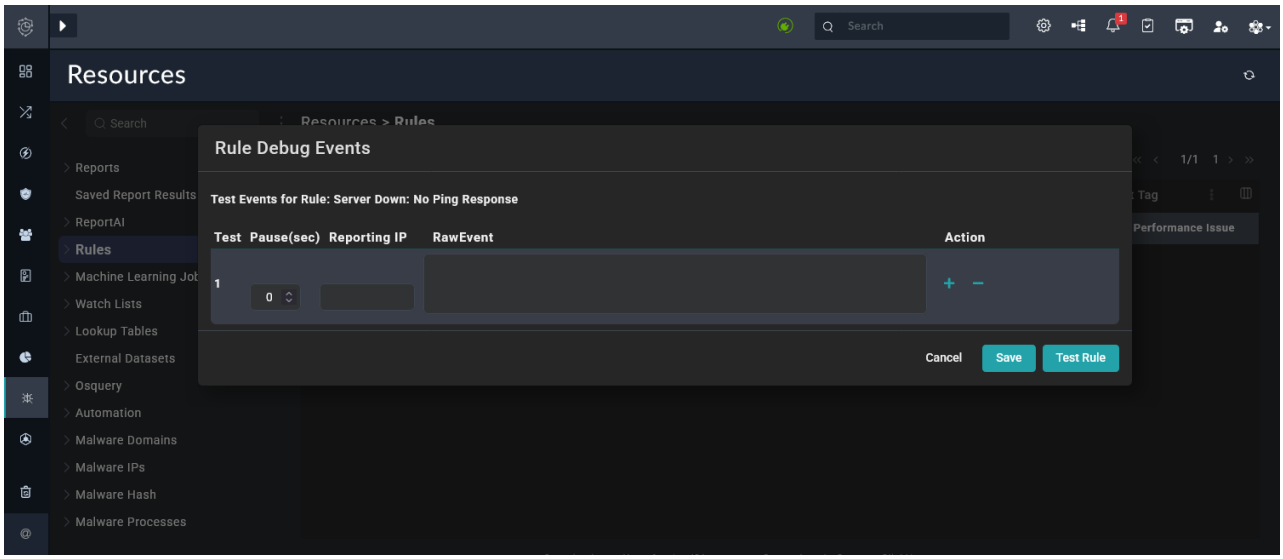
Testing SIEM detection rules

You can perform detection testing for *Streaming* detection rules created in the *SIEM* module.

Scheduled and *Scheduled via SQL* rules in the *SIEM* module cannot be tested.

To test a Streaming detection rule in the SIEM module:

1. In the FortiSOC GUI, go to *SIEM* > *Resources* > *Rules*.
2. Select the rule, and click the *Test* icon.
   The *Rule Debug Events* dialog displays.



3. Enter a *Reporting IP* where the synthetic event should originate from.
   If the rule you are testing specifies that the *Reporting IP* should be a member of a group, make sure that the entered *Reporting IP* is in that group.
4. Under *Raw Event*, enter the raw event log text that contains the triggering conditions for the rule.
5. Under *Pause*, enter the number of seconds before the next test event will be sent.
6. Under *Action*, click + to enter additional test events, if needed.
   Create as many events as necessary to trigger the rule conditions.
7. Click *Test Rule*.

Alerts and case management

You can view and manage alerts and cases in the FortiSOC GUI from the *Cases & Alerts* module.

Key terms

Event log: These logs represent observable events within the system or network. This is raw, unfiltered data, which can be stored and used for compliance and forensics. Most events are perfectly normal, like a user logging in, an allowed firewall connection, or a file being saved.

Alerts: A notification that is triggered when an event, or series of events, matches logic within a detection rule, suggesting something suspicious. It is a red flag raised by the monitoring system to show potential malicious activity. Triggering alerts is the first step for automated triage, reducing noise from the vast number of event logs.

Cases: A validated security issue from a collection of related alerts. At this point, the alert or correlated alerts have been analyzed and confirmed to represent a genuine security threat or compromise, such as a confirmed phishing attack, ransomware infection, or data exfiltration. Cases are actionable, triggering the SOC to respond with next steps for investigation and remediation.

Alert to case lifecycle

1. The *Analyzer* and *SIEM* modules collect event logs, which represent observable events within the system or network.
2. These events (or a series of events) can trigger an alert when they match a detection rule within the respective module (*Analyzer* or *SIEM*), suggesting something is suspicious.
3. FortiSOC ingests the alerts from the *Analyzer* and *SIEM* modules.

   FortiSOC can also collect existing alerts from other data ingestion sources. For more details about their lifecycle, see Alert lifecycle and states on page 64.
4. Alerts are enriched with further data using playbooks in FortiSOC. For example, they may be correlated with other alerts, enriched with asset & identity information, and more. This is automated triage in FortiSOC, though it can also be supported manually by SOC analysts executing playbooks and linking information.
5. If a collection of related alerts has been analyzed and confirmed to represent a genuine security threat or compromise, it will be escalated to an case. This escalation can occur manually by a SOC analyst, or automatically with the support of escalation rules in FortiSOC.
6. The SOC analysts take action on the case, preforming investigation, containment, a remediation. Once resolved, the case is closed.

> If an open case is idle (not modified) for 28 days, the *Status* will automatically change to *Resolved*.
>
> To view the related playbook, see *Automation > Playbooks > 06 - IRP - Case Management > Case - Auto Resolve Inactive Open Cases*.

Alert lifecycle and states

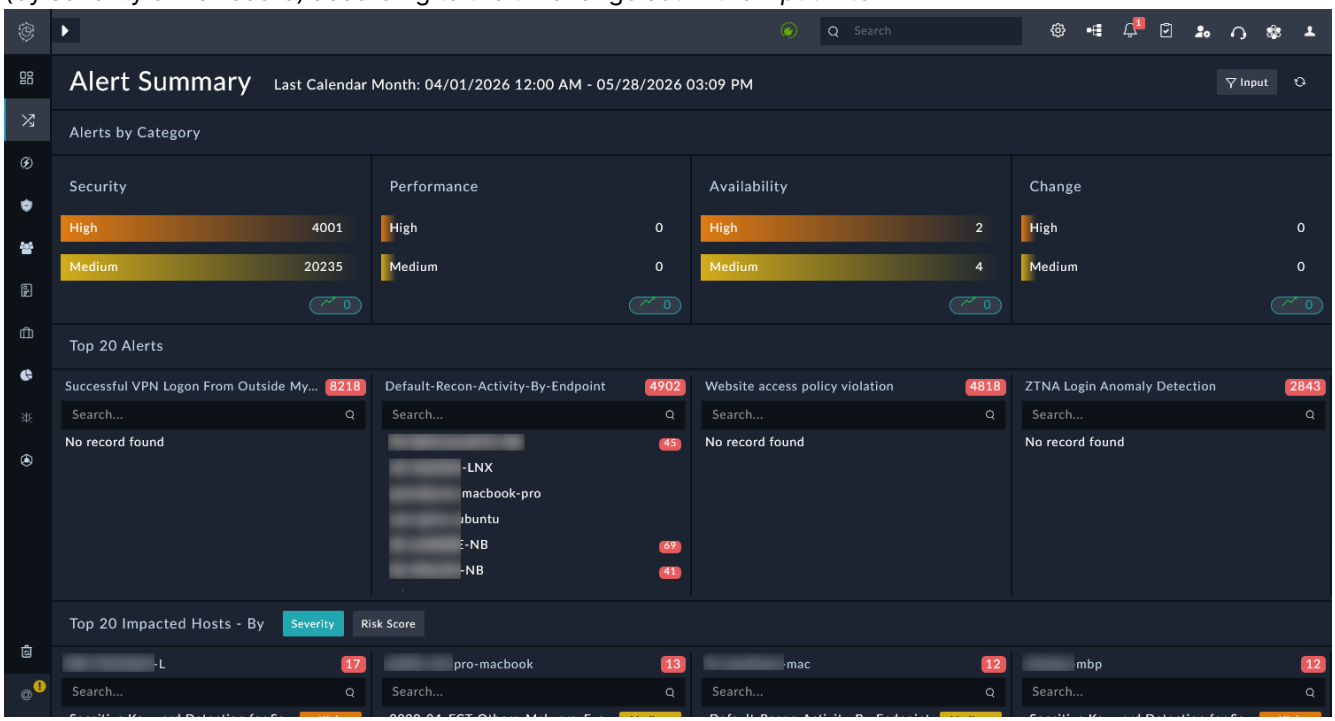
Alerts deliver curated detections with detailed information on the source and target, along with in-depth security context for each detection.

When alerts are ingested to FortiSOC, they are normalized, enriched, and grouped. If appropriate, the grouped alerts will also automatically be escalated to cases according to the escalation rules. These steps are defined in more detail below to depict the alert lifecycle immediately after it is ingested into FortiSOC.

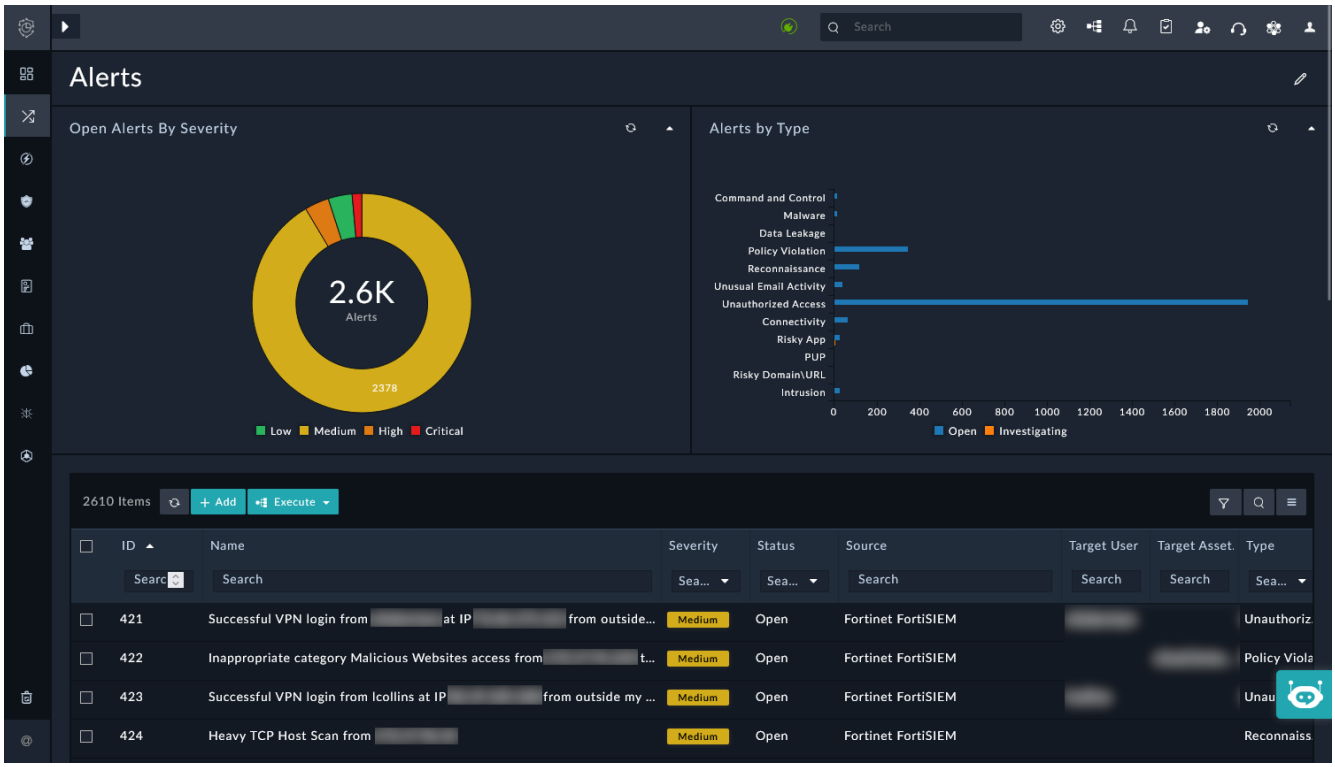
1. **Alerts are normalized**: FortiSOC ingests alerts from many sources, which may use different field names. These fields are normalized and mapped to the fields used in FortiSOC.
2. **Information is extracted from the alerts**: FortiSOC playbooks extract information, such as indicators, from the alert so it can be used for enrichment
3. **Alerts are enriched**: Predefined FortiSOC playbooks enrich the alerts, updating their attributes.
4. **Alerts are correlated**: FortiSOC playbooks correlate the alert with other alerts, assets, identities, and more based on the data available in FortiSOC.
5. **Alerts are escalated (if appropriate)**: Escalation rules in FortiSOC will escalate the alerts to cases if they match the set criteria. Alternatively, alerts can be manually escalated.

This automated initial triage ultimately supports SOC analysts by reducing noise and adding context to support investigation. The alerts continue to be enriched as more data becomes available in FortiSOC. The analysts can also manually execute playbooks to enrich specific alerts during triage; for example, they can execute the *Fetch and Link Asset and Identity* playbook to fetch the most recent data in FortiSOC to enrich an alert with related assets and identities, if available.

Analysts can use the *Cases & Alerts > Alert Summary* dashboard to monitor recent alerts by category (security, performance, availability, and change). This dashboard also lists the top 20 alerts and top 20 impacted hosts (by severity or risk score) according to the time range set in the *Input* filter.



All alerts can be viewed in the FortiSOC GUI from *Cases & Alerts* > *Alert List*.



When alerts are initially ingested, their *Status* is *Open*, even if the alert has been automatically escalated to a *Case* by an *Escalation Rule*. For scenarios where analysts are working directly on an alert, they can update the *Status* of the according to their needs during triage:

- *Open*
- *Investigating*
- *Pending*
- *Closed (Resolved)*
- *Re-Opened*

In general, analysts will investigate and follow up on cases rather than individual alerts. When investigating unescalated alerts, the most common next steps are to close the alert as a false positive OR to escalate the alert (s) to a case. The analyst can manually link the alert(s) to an existing case or escalate the alert(s) to a new case for follow up.

To link an alert to an existing case:

1. Go to the related records at the bottom of the Alert details.
2. In the related records, go to *Correlations* > *Cases*.
3. Click *Link*.
   The *Link Cases* dialog displays.
4. Select the case(s) and click *Save Relationship*.
5. If the alert has not already been escalated, escalate the alert.
   a. In the *Alert* details, update the *Escalated* field to *Yes*.
      The *More information needed for this Alert* dialog displays.

b. Provide a reason for escalating the alert.
c. Click *Update*.

To escalate an alert to a new case:

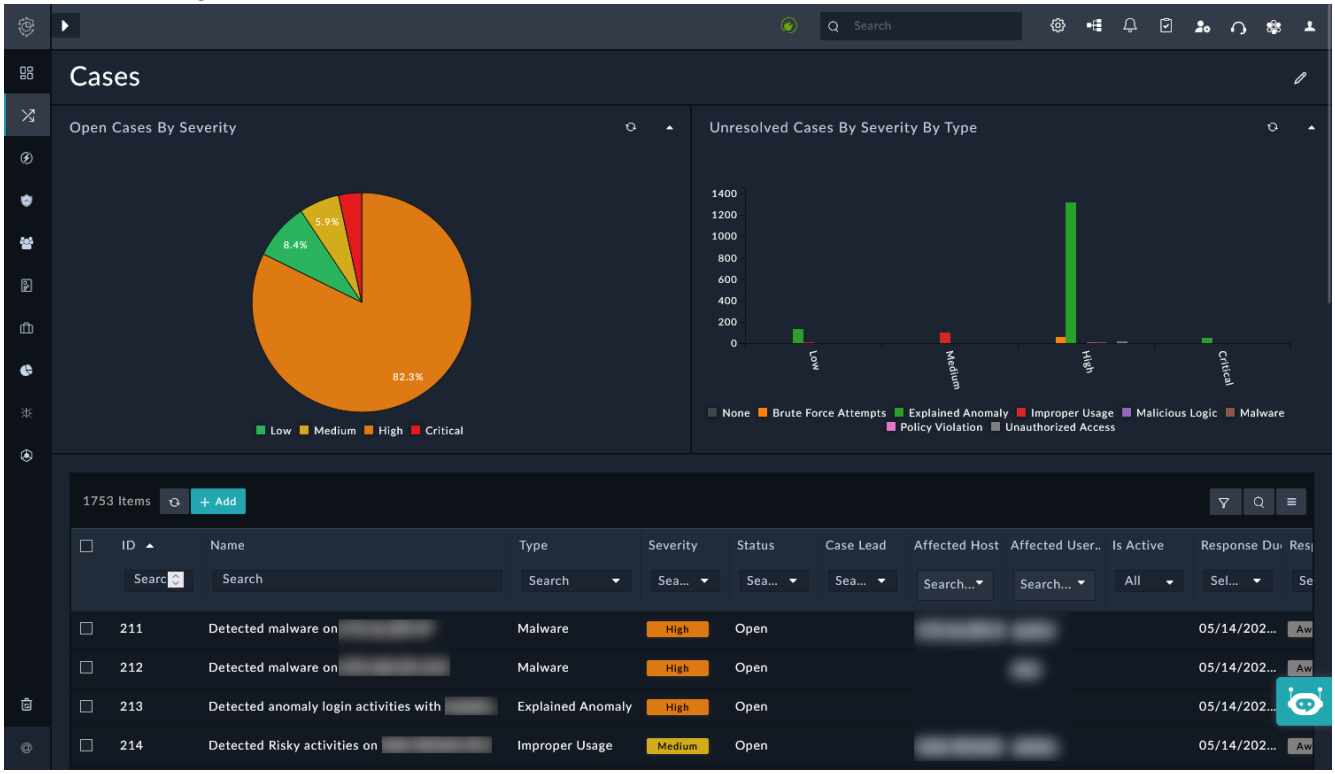
1. In the *Alert List*, select the alert(s) to escalate to a new case.
   Alternatively, you can open the escalate a single alert from within its *Alert* details.
   The *Escalate* dialog displays.
2. Configure the following:

Field	Description
Case Name	Enter a name for the case.
Severity	Select the case severity.
Case Lead	Select a user as the case lead.
Escalation Reason	Displays "`Alert needs to be investigated`" by default. Update this field if more reasoning needs to be provided to the Case Lead.
Case Type	Select an appropriate case type for reporting / tracking.
Close Alert	Select to close the alert(s) after creating the case.

3. Click *Escalate*.

Case creation and correlation

Cases are managed in *Cases & Alerts* > *Cases*.



Cases provide a correlated view of related alerts, surfacing indicators, threats, and correlation details to help analysts identify and respond to threats quickly and effectively.

Cases can be automatically escalated from alerts using escalation rules, manually escalated from alerts, or manually created from scratch. The cases can be correlated to alerts, assets, identities, and more automatically using playbooks to support further triage.

For cases automatically created by escalation rules, the alerts are correlated according to the *Group Alerts By* field. For example, the *FSOC - User login anomaly* escalation rule will group alerts by *Target User*: alerts that meet the escalation rule conditions with the same target user will be correlated in the escalated case. For more information about escalation rules, see Escalation and workflow management on page 74.

To manually create a case:

1. Go to *Cases & Alerts* > *Cases*.
2. Click *Add*.
3. Configure the following information.

Option	Description
Name	Enter a name for the case.

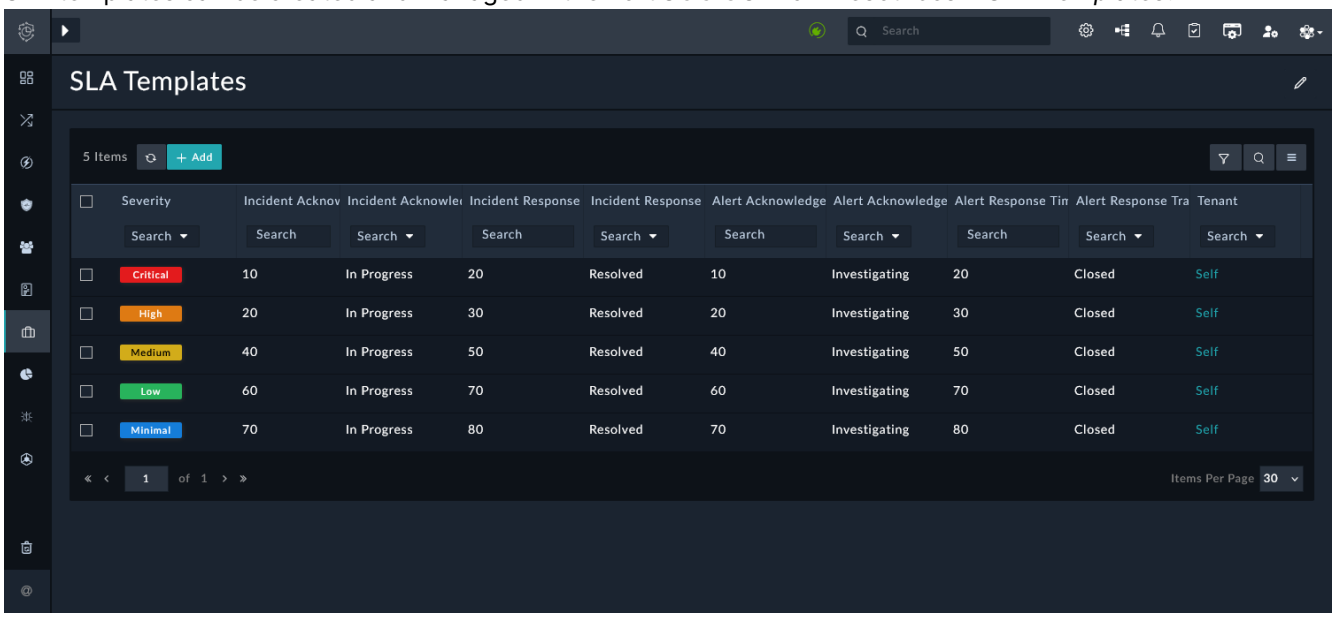
Option	Description
Description	Enter a description.
Summary	
Phase	Select the phase within the response process.
Status	Select the status.
State	Select the state.
Details	
Tenant	Select the tenant.
Severity	Select the severity.
Type	Select the type.
Source	Enter the source.
Source ID	Enter the source ID.
Case Lead	Select the analyst to lead the response.
Tags	Enter tags.
Dates	
Date Of Case	Select the date of the case.
Discovered Date	Select the date the case was discovered.
Dwell Time (Minutes)	Enter the dwell time.
Containment Time (Minutes)	Enter the containment time.
Recover Time (Minutes)	Enter the recover time.

4. Click *Save*.
   The *Case Detail* pane displays. In this pane, you can:
   - Enter more details about the case
   - Add correlations for the case, including alerts, assets, and identities
   - Execute playbooks to enrich the case or perform other actions

Severity, prioritization, and SLA policies

Alerts and cases can be prioritized using service level agreement (SLA) templates in FortiSOC. The SLA defines the expected service level, outlines the metrics by which service is measured, and specifies remedies or penalties if service levels are not met.

SLA templates can be created and managed in the FortiSOC GUI from *Resources* > *SLA Templates*.



SLA templates are based on the alert and case severity. The SLA template defines the amount of time analysts have to acknowledge and respond to a alerts and cases with this severity level. The template also defines what statuses will trigger the SLA time to be tracked, paused, and complete (responded to).

Only one SLA template can be created per severity:

- *Minimal*
- *Low*
- *Medium*
- *High*
- *Critical*

To configure an SLA template:

1. Go to *Resources* > *SLA Templates*.
2. Click *Add*.
3. Configure the following options:

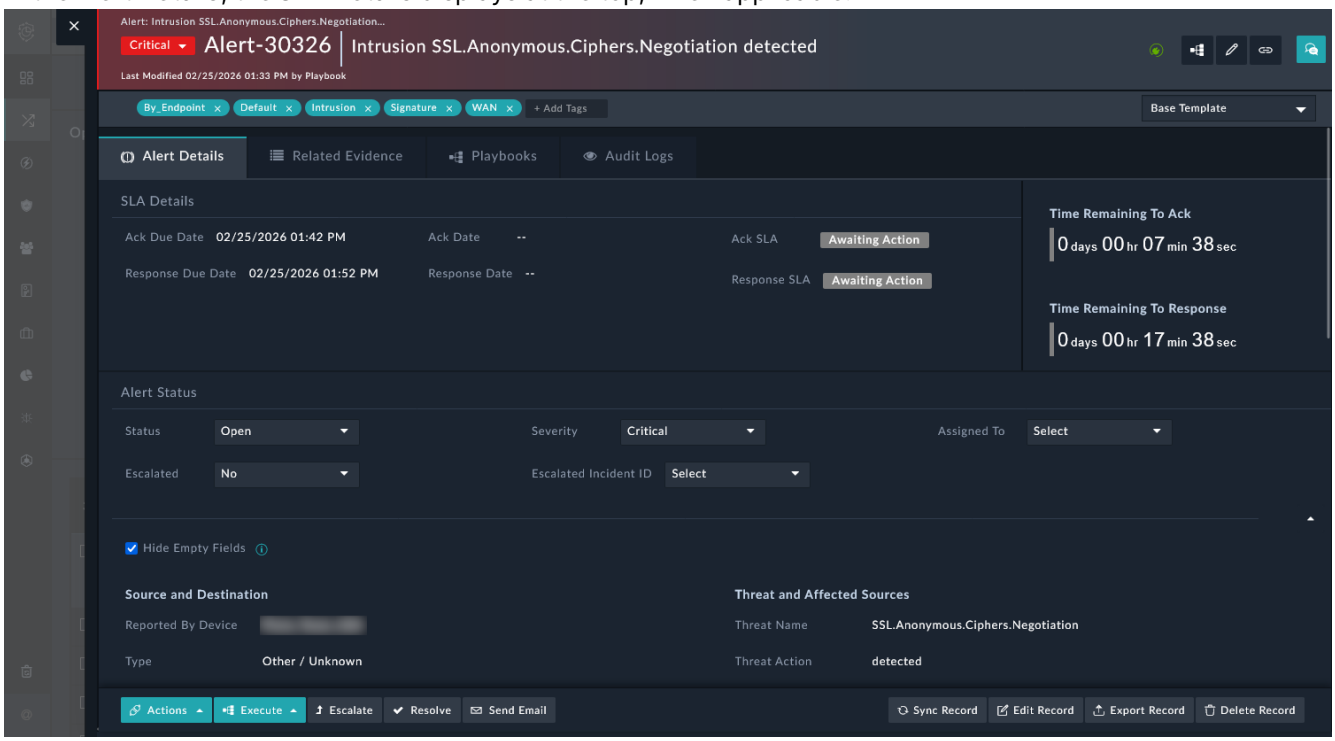
Option	Description
Severity	Select the alert/case severity the SLA will be assigned to.
Tags	Add tags that must be present for the SLA to be assigned.
Tenant	Select the tenant.
Incident SLA	
Incident Acknowledge SLA Tracked on	Select the case status that marks the case as acknowledged.
Incident Acknowledge Time	Enter the time in minutes for analysts to acknowledge the case.

Option	Description
Incident Response SLA Tracked on	Select the case status that marks the case as responded.
Incident Response Time	Enter the time in minutes for analysts to respond to the case.
Alert SLA	
Alert Acknowledge Tracked On	Select the alert status that marks the case as acknowledged.
Alert Acknowledge Time	Enter the time in minutes for analysts to acknowledge the alert.
Alert Response Tracked On	Select the case status that marks the alert as responded.
Alert Response Time	Enter the time in minutes for analysts to respond to the alert.

4. Click *Save*.

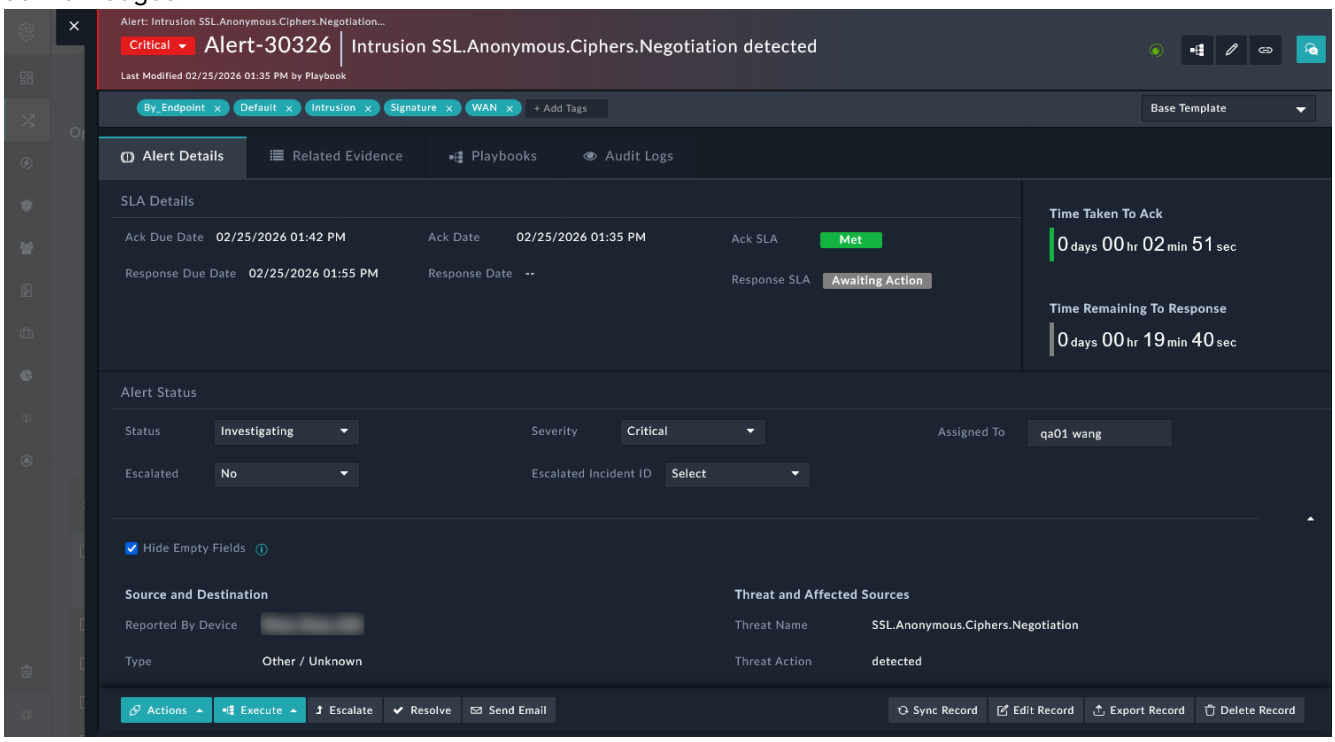
To view the SLA details in an alert:

In the *Alert Details*, the *SLA Details* displays at the top, when applicable.

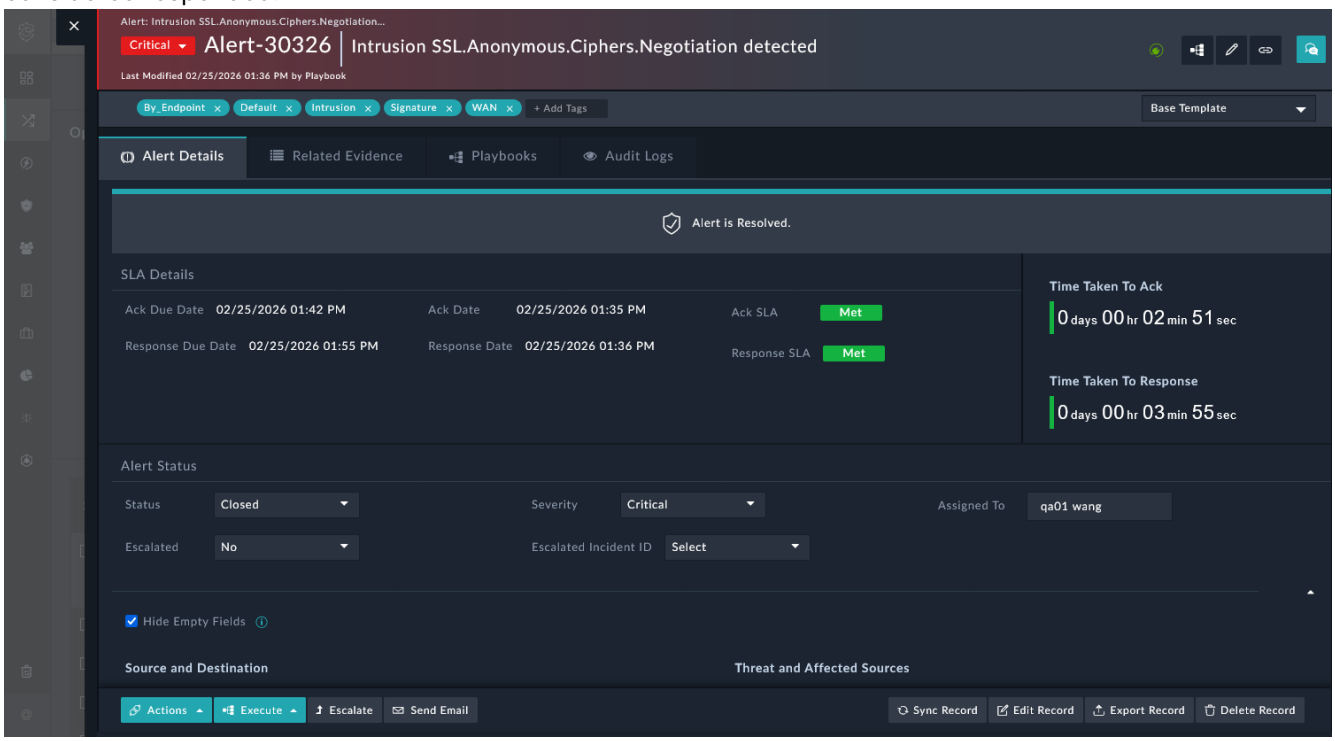


The information in the SLA details is updated as the SOC analysts update the alert. For example, see below where the *Alert Status* has been updated to `Investigating`. As part of the SLA, the alert is now considered

acknowledged.

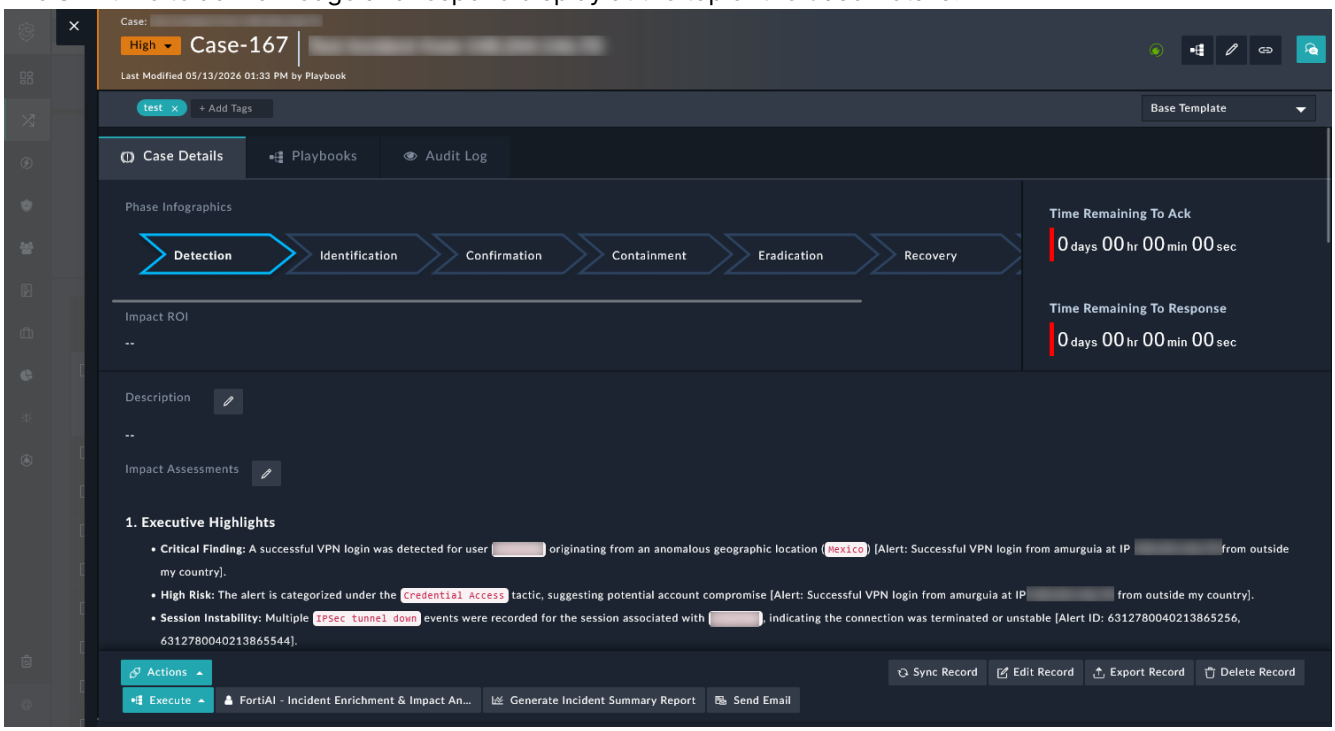


In the example below, the alert has been *Closed* as a `False Positive`. As part of the SLA, the alert is now considered responded.

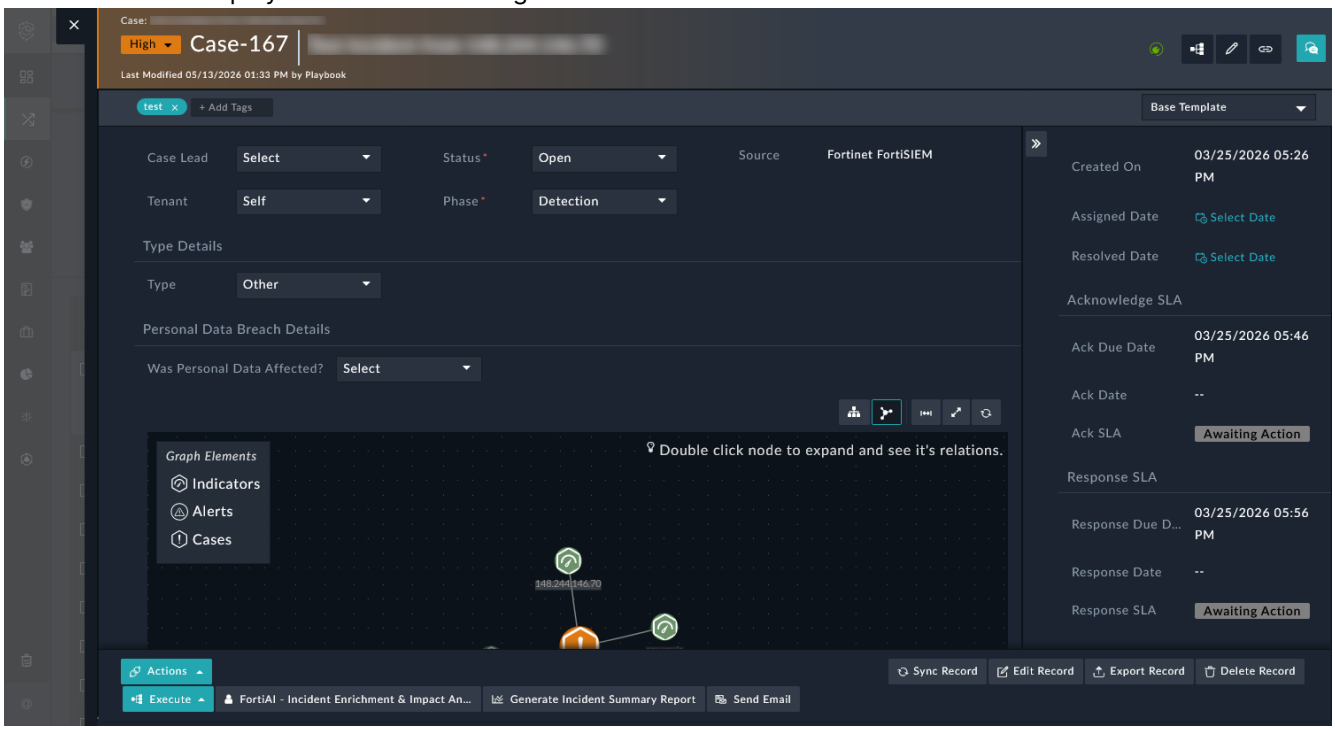


To view SLA details in a case:

The SLA time to acknowledge and respond display at the top of the *Case Details*.



The SLA details display in a drawer at the right side of the *Case Details*.



Admin controls for alerts and cases

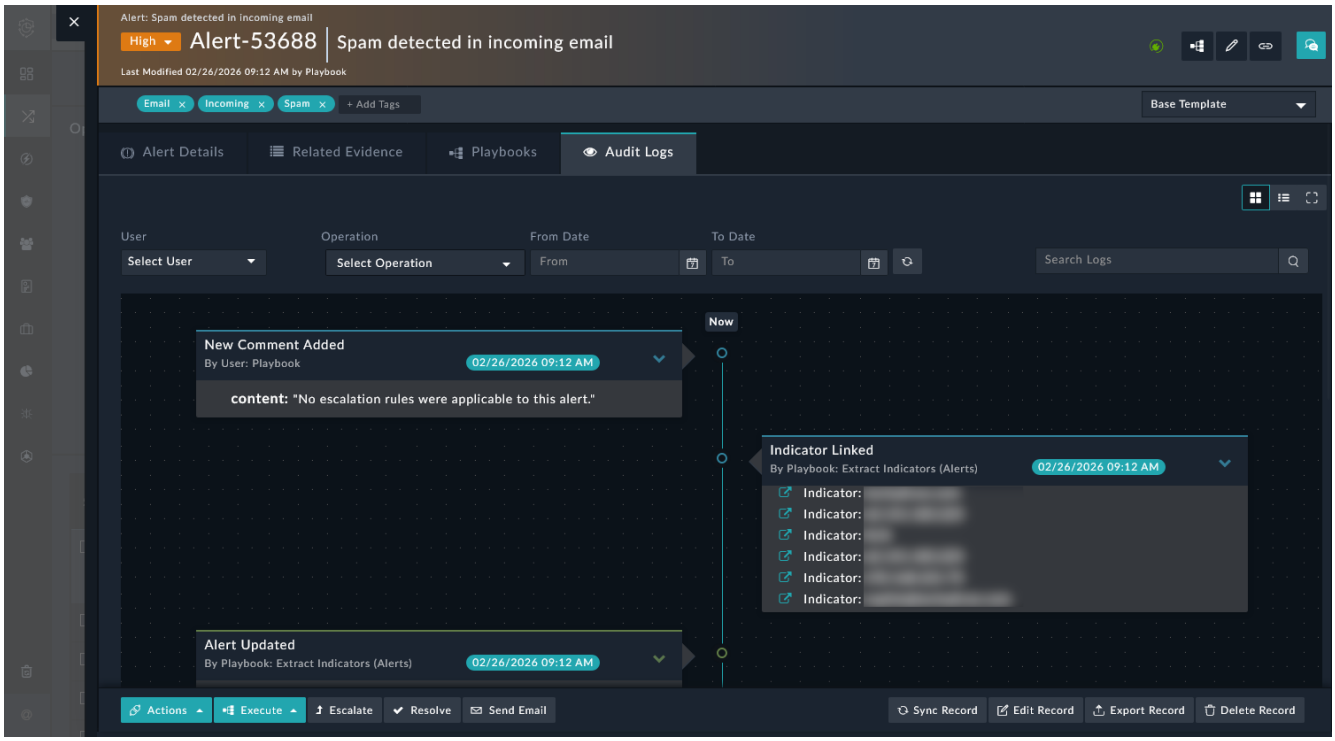
Alerts and cases are primarily managed by the SOC analysts. They are responsible for triage and response.

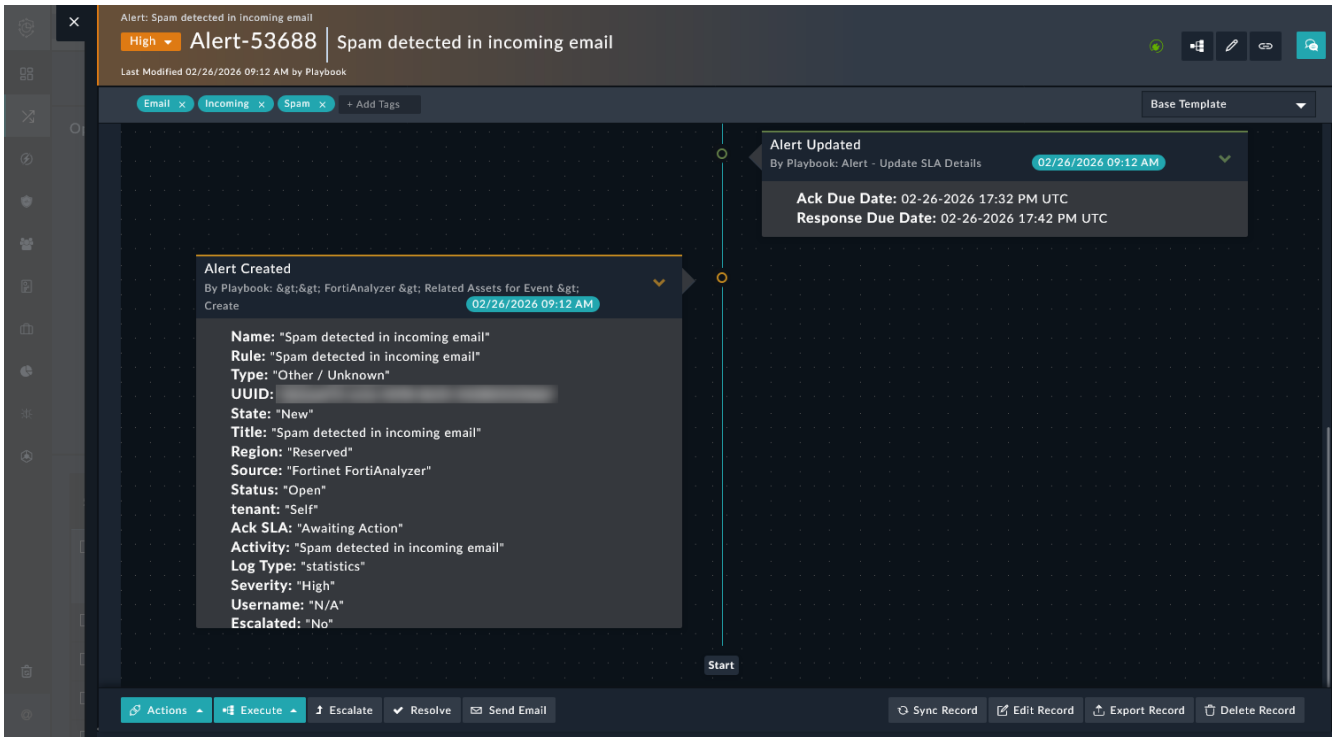
FortiSOC administrators, by contrast, can review alerts and cases to audit threat response and find opportunities to refine SOC processes. For example, administrators may determine:

- Certain alerts are manually escalated on a regular basis, and an escalation rule could be created to automatically triage these alerts.
- Certain actions are regularly taken on select cases or alerts, and a playbook could be created to automate these steps.

In *Alert Details*, go to the *Audit Logs* tab to view a timeline of the alert. This includes the alert creation, playbooks run against the alert, and actions taken by users. You can expand/collapse information in the timeline for further review.

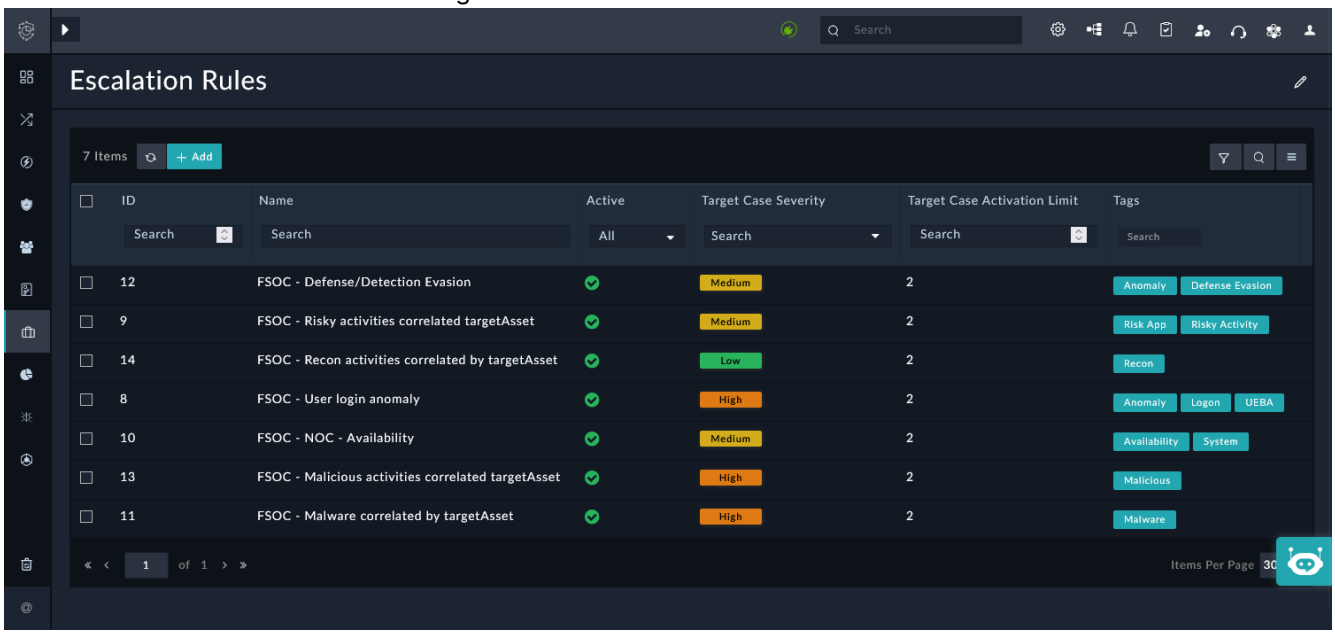
When indicators or entities are linked to the alert, you can click links to the related records for more information.





Escalation and workflow management

Escalation rules are created and managed in *Resources* > *Escalation Rules*.



Escalation rules in FortiSOC are used to automatically group and escalate alerts to cases according to set criteria. There are many predefined escalation rules in FortiSOC, and you can create more according to the needs of your SOC.

There are predefined escalation rules in FortiSOC to automatically group alerts that likely require follow up from SOC analysts. For example, there are predefined escalation rules for scenarios such as:

- Defense evasion activities
- Recon activities
- User login anomalies
- Malware on a target asset

You can review the *Description* in the predefined *Escalation Rules* for more information. The rules also include recommendations, which can help to guide next steps for the case.

The *Description* in the escalation rule is used to generate the initial *Description* in the escalated *Case Details*.

The *Recommendation* in the escalation rule is used to generate the initial *Impact Assessments* in the escalated *Case Details*.

To create an escalation rule:

1. Go to *Resources* > *Escalation Rules*.
2. Click *Add*.
3. Configure the following options:

Option	Description
Name	Enter a name.
Description	Enter a description. This description will be used for the escalated case.
Recommendation	Enter a recommended action for the case. This recommendation will appear as the *Impact Assessments* in the escalated case, describing starting actions for the SOC analysts.
Tags	Enter tags to be assigned to the escalated cases.
Active	Enable/disable the escalation rule.
Target Case Activation Limit	Enter themaximum number of alerts required to activate the case.
Target Case Name	Enter the template to be used to generate the case name.
Target Case Severity	Enter the target case severity. This severity will be assigned to the escalated cases.
Target Case Type	Enter the target case type. This type will be assigned to the escalated cases.

4. Configure the *Rule Configuration* > *Matching Conditions*.
   This defines the filtering logic used to evaluate incoming alerts. If an alert satisfies these criteria, it becomes eligible for correlation and escalation.

   a. Select the main condition group operator:
      - *ALL OF THE BELOW ARE TRUE (AND)*
      - *ANY OF THE BELOW ARE TRUE (OR)*
   b. Select a field for the condition.
   c. Select an operator for the condition.
      The available operators depend on the selected field.
   d. Enter the criteria for the condition.
   e. Add more conditions and condition groups, as needed.
      Alerts that meet the set condition(s) will be escalated to cases.
5. Configure the *Rule Configuration > Correlation Criteria*.
   a. Select the main condition group operator:
      - *ALL OF THE BELOW ARE TRUE (AND)*
      - *ANY OF THE BELOW ARE TRUE (OR)*
   b. On the left-side, select a field for the condition.
   c. On the right-side, select a field to monitor for matching values.
      Alerts with matching values in these fields (left-side and right-side) are considered related. This enables grouping multiple alerts together before escalating them to a case.
   d. Add more conditions and condition groups, as needed.
6. Click *Save*.

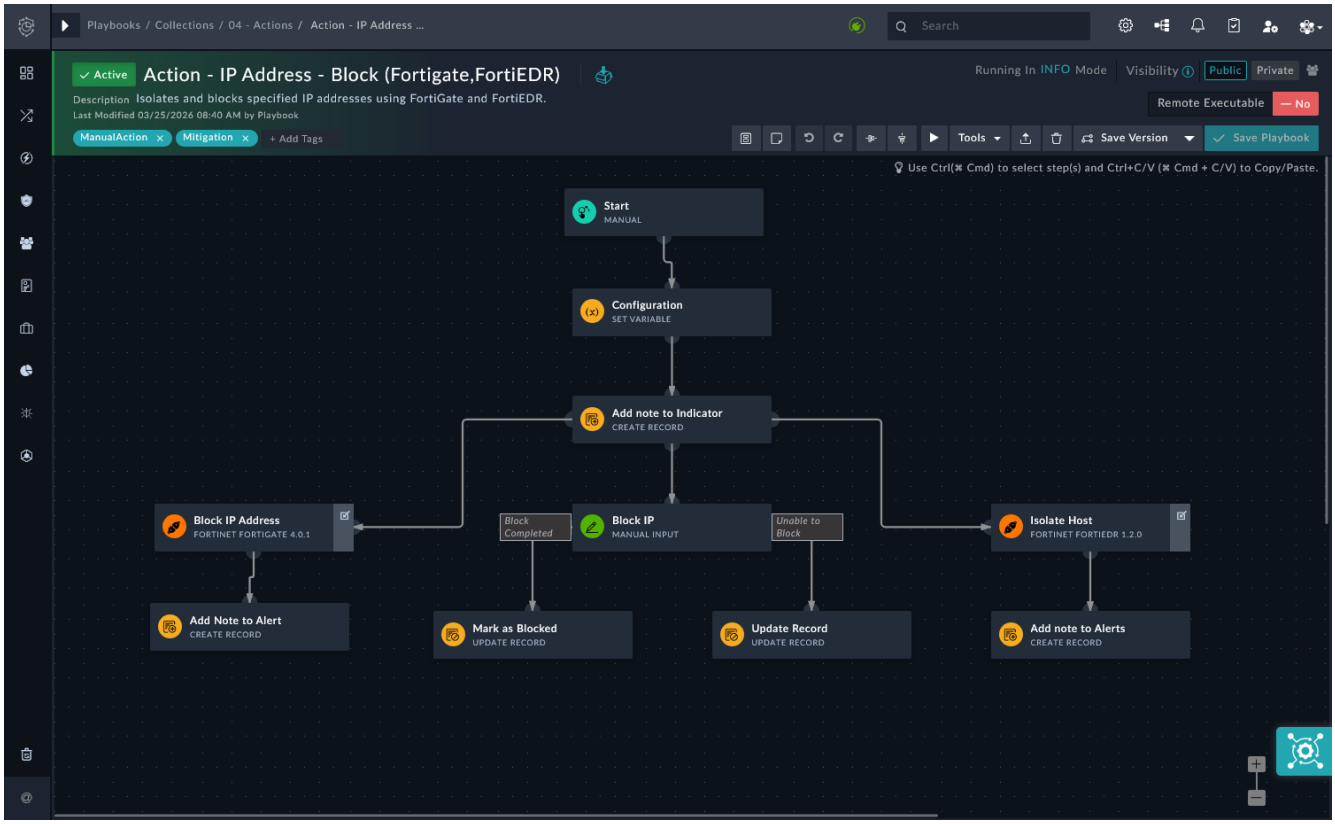
Automation and response

The key components of FortiSOC automation and response are playbooks and connectors. The playbooks can be triggered manually or automatically according to ingested data, and they perform actions within FortiSOC or connected applications and devices to support triage and response.

FortiSOC includes predefined collections of playbooks for automation and response. These predefined collections are to support FortiSOC's functionality and ease-of-use for the SOC. For example, there are playbooks dedicated to automatically enriching the alerts, cases, assets, and identities ingested into FortiSOC. Some of these predefined playbook collections are system playbooks (essential to functionality), while others are included with out-of-the-box solution packs (included for ease-of-use). These playbook collections can be found in the FortiSOC GUI in *Automation* > *Playbooks*.

Further playbook collections are also automatically included in *Automation* > *Playbooks* after a connector or solution pack is installed from the *Content Hub*. When installing an object from the *Content Hub*, you can review the associated contents, including the associated playbook collections and documentation.

In *Automation* > *Playbooks*, you can also customize playbooks with templates or create custom playbooks from scratch according to your organizations unique needs.



Automation framework

Below is a brief summary of the components for automation in FortiSOC.

- **Playbooks**: Playbooks in FortiSOC are workflows that define automated response. They execute sequences of steps and actions such as enrichment, containment, and alert / case notifications.
  - **Playbook triggers**: Triggers define when a playbook is to be executed. The playbooks can be triggered manually, on schedules, or automatically by ingested alerts, cases, or other data.
  - **Playbook steps**: Steps represent discrete elements of data processing during the course of the playbook. There are a variety of step types that can be configured in FortiSOC, including Execute steps which can execute connector functions. The connectors can be used to push actions, such as blocking IPs, containing endpoints, and escalating alerts to cases.
- **Connectors**: Connectors in FortiSOC are configured integrations with security tools, such as SIEMs, EDR, firewalls, ticketing systems, and more. The connectors use APIs to ingest data, such as alerts, logs, or indicators. This data can be used as part of playbook triggers and steps.

For more information about playbook components, including details about the available playbook triggers and steps, see *Playbooks and Components* in the FortiSOAR Playbooks Guide.

Below is a very simple example of a playbook running in FortiSOC.

1. Connector ingests data.
2. Data triggers a playbook to run.
3. Playbook executes actions, such as enriching existing alerts with new data from the connector.
4. Further decisions in the playbook can determine the next steps, such as:
   - escalating alerts to cases.
   - executing actions through the connectors.
   - sending notifications to SOC analysts.

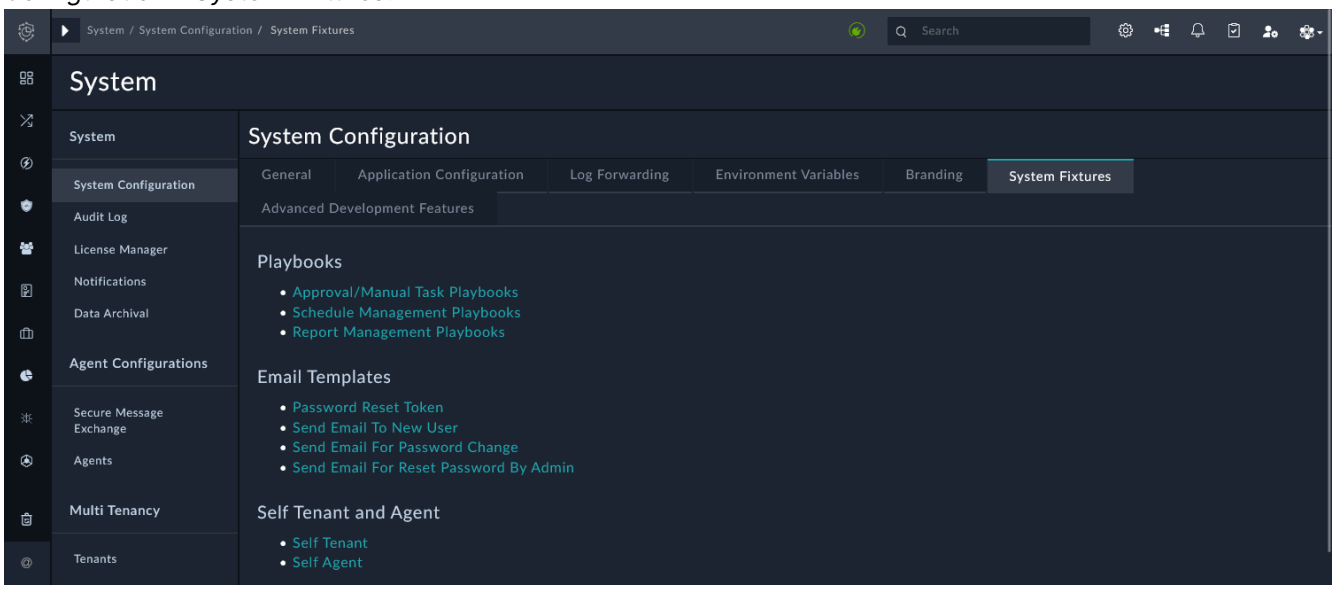
Predefined playbooks and automation

Predefined playbook collections are available in *Automation* > *Playbooks*. This includes both system playbooks and playbooks from installed solution packs.

System playbooks

The predefined system playbooks are critical to FortiSOC functionality. These playbooks are stored in *Automation* > *Playbooks*, however, they can also be found through *Global Settings* > *System* > *System*

Configuration > System Fixtures.



This pane provides links to collections for the following system playbooks:

- *Approval/Manual Task Playbooks*: used to handle approval and manual task workflows within playbooks.
- *Schedule Management Playbooks*: used to schedule various tasks such as cleaning up playbook execution history, purging integration logs, and more.
- *Report Management Playbooks*: used to manage report generation and schedules.

Note that these playbooks are hidden when you navigate to *Automation > Playbooks*. You can find them by enabling the *Include System Collections* in *Automation > Playbooks*.

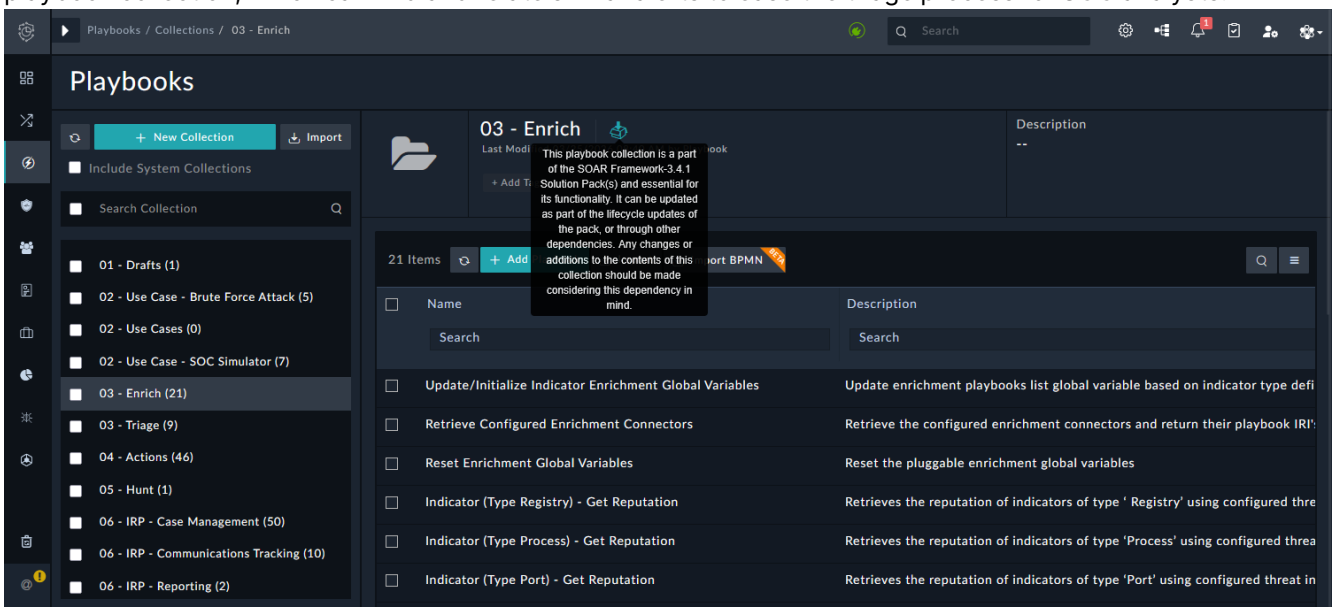
> ⚠ You can modify system playbooks according to your requirements; however, this can affect FortiSOC functionality.

Playbooks from solution packs

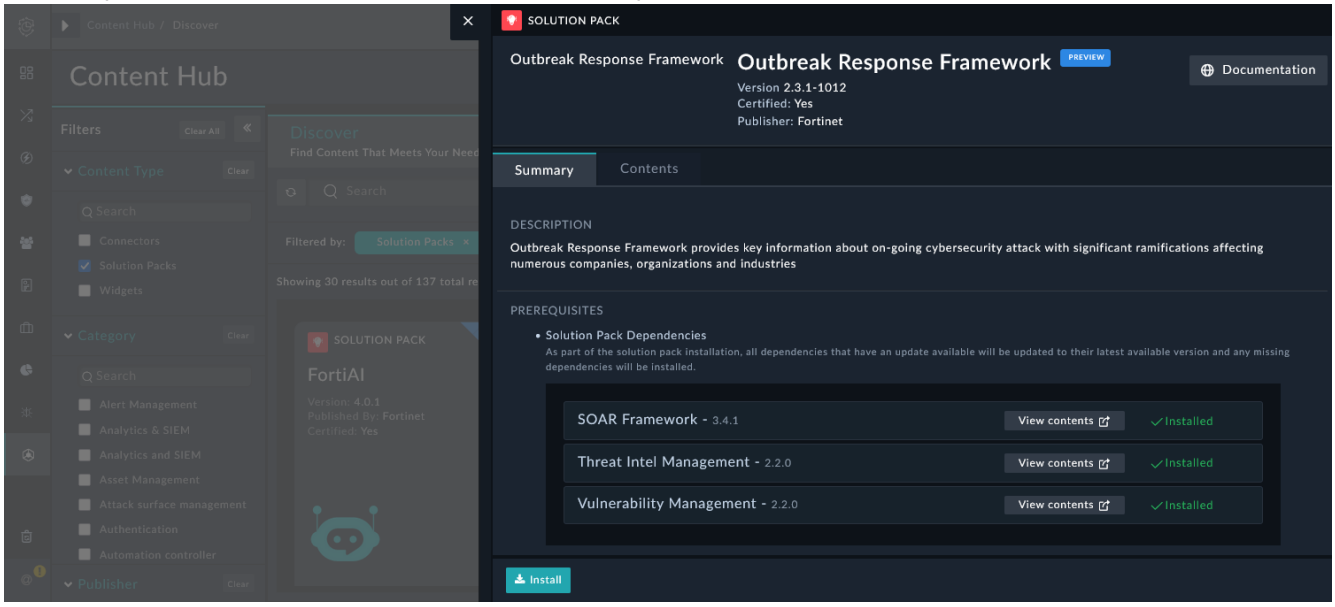
When you open a predefined playbook collection from a solution pack, a download collection icon displays next to the collection title. This icon indicates that playbooks within the collection are part of a solution pack and are critical to its functionality. These playbook collections can be updated automatically as part of lifecycle updates and content pack updates. Mouse-over the icon to display which solution pack the playbook collection is associated with.

There are some out-of-the-box solution packs that include predefined playbooks to enhance FortiSOC and facilitate ease of use. For example, the *SOAR Framework* solution pack lays the foundation to use the FortiSOC platform optimally for response and automation use cases in a SOC. It includes playbook collections, such as *03 - Enrich*, which is used to retrieve and enrich indicators for alerts and cases. It also includes the *03 - Triage*

playbook collection, which can find and relate similar alerts to ease the triage process for SOC analysts.



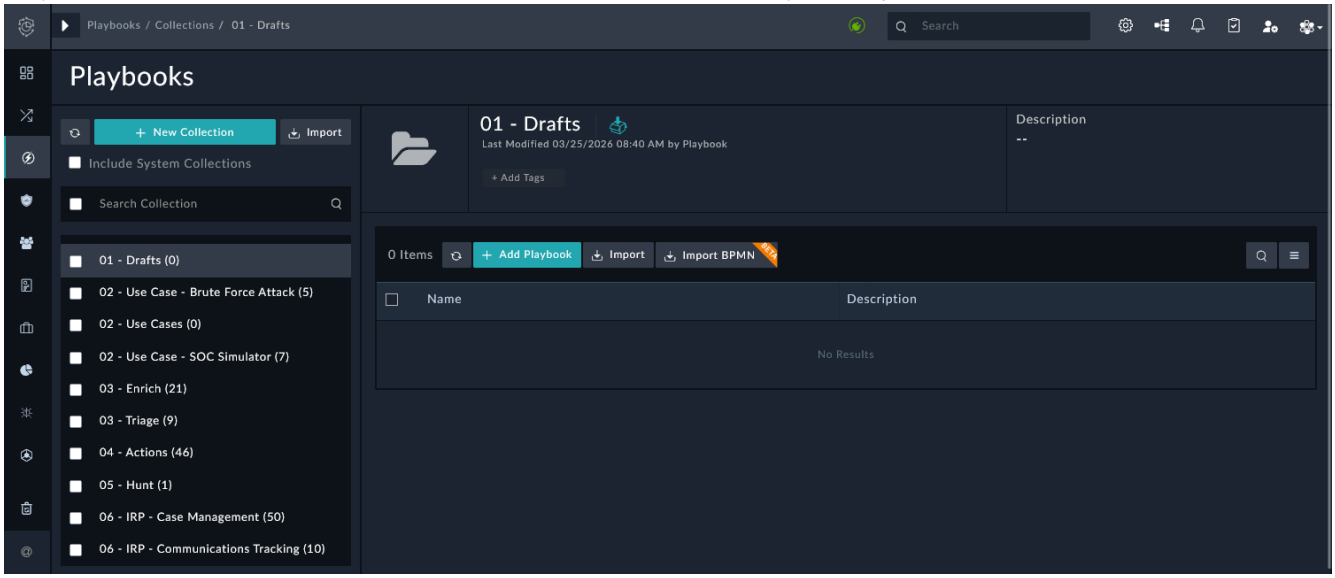
Complete documentation for these solution packs are included within the *Content Hub*. After selecting a solution pack, click *Documentation* to review the complete details.



You can also browse the *Solution Packs* documentation in the Fortinet FortiSOAR Content Hub website.

Creating and customizing playbooks

Playbooks can be created and customized in the *Automation* > *Playbooks* pane.



You can perform the following actions in this pane.

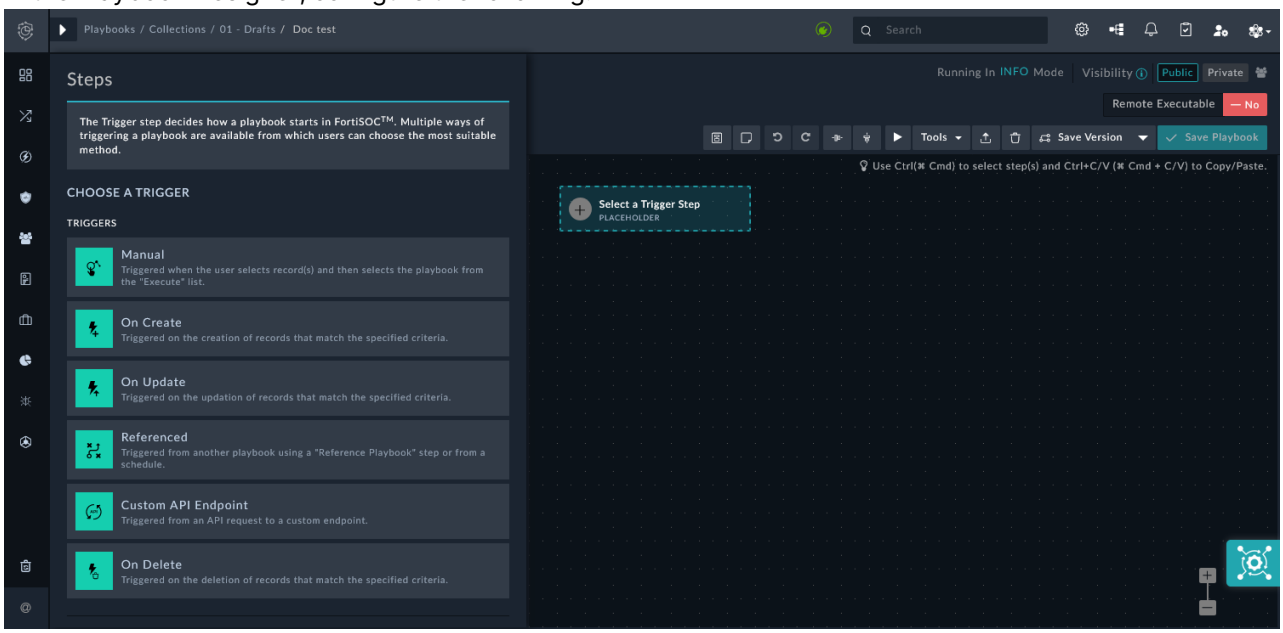
Action	Description
New Collection	Create a new collection to store playbooks in.
Import collection	Import a collection of playbooks in JSON format.
Add Playbook	Create a new playbook from scratch.
Import playbooks	Import an individual playbook in JSON format.
Import BPMN (Beta)	Import a Business Process Model and Notation (BPMN) Shareable Workflow as a playbook. The BPMN Shareable Workflow should have been exported in XML or JSON format from your tool, such as Flowable, Camunda, or Signavio. You can only import these individually; you cannot import a full collection at once. For more details about how the steps in the workflow are converted in the playbook, see the FortiSOAR Playbooks Guide.
After selecting a playbook within a collection:	
Activate	Activate a playbook to run according to its trigger step.
Deactivate	Deactivate the playbook so it cannot be triggered to run.
Clone	Clone the playbook to use as a template for creating a custom playbook.
Move	Move the playbook to another collection.
Export	Export the playbook as a JSON file.

Action	Description
Change Logging Level	Change the execution log level for the playbook.
Delete (trash icon)	Delete the playbook permanently or send it to the *Recycle Bin*.

To create a playbook:

For further details about using the Playbook Designer, see *Creating and Designing Playbooks* in the FortiSOAR Playbooks Guide.

1. Go to *Automation* > *Playbooks*.
2. Go to the collection to create the playbook in. Create a new collection, if needed.
3. Click *Add Playbook*.
   Alternatively, you can clone an existing playbook and move it to the desired playbook collection. Rename the playbook logically according to its use case.
4. Configure the following options in the *Add New Playbook* dialog:
   - *Name*
   - *Description*
   - *Active*
   - *Remote Executable*
   - *Tags*
5. In the Playbook Designer, configure the following:

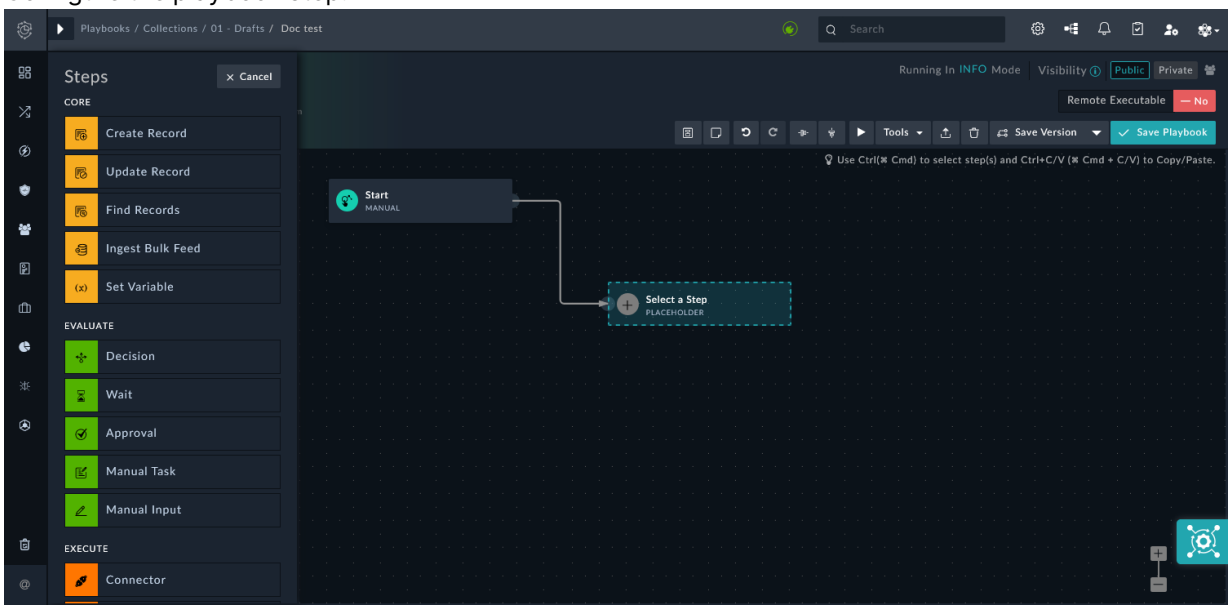


   a. Configure a trigger step for the playbook.
      The following trigger steps are available.
      - *Manual*: Allows you to click to start the playbook from within any module in the system.
      - *On Create*: Triggers immediately after a record of the selected model type is created or ingested. For example, you can define a playbook that is triggered when a case is created.

- *On Update*: Triggers immediately after a record of the selected model type is updated.
- *Referenced*: For playbooks that are exclusively called from a *Reference a Playbook* step. See playbook step descriptions below.
- *Custom API Endpoint*: Specify an arbitrary endpoint that can be used to externally start a playbook using a REST API POST action from another system.
- *On Delete*: Triggers immediately after a record of the selected model type is deleted.

b. Drag-and-drop a connector point from the trigger to add a new step in the playbook.

c. Configure the playbook step.



The following playbook steps are available:

- *Core* steps: Used to find, create, update, or manage records within FortiSOC, or to define variables for use throughout a playbook.
  - *Create Record*
  - *Update Record*
  - *Find Records*
  - *Ingest Bulk Feed*
  - *Set Variable*
- *Evaluate* steps: Define logical flows within the playbook. These include decision points, user approvals, and manual inputs.
  - *Decision*
  - *Wait*
  - *Approval*
  - *Manual Task*
  - *Manual Input*
- *Execute* steps: Perform actions such as executing connector functions or built-in utilities.
  - *Connector*
  - *Utilities*
  - *Code Snippet*
- *References* steps: Used to call child playbooks from a parent playbook.

        - *Reference a Playbook*
        - *Trigger Tenant Playbook*
        - *Add Reference Block*
    - *Email* steps: Automatically send an email to the user(s) identified in the step with either specific static criteria or record-relevant data using dynamic values.
        - *Send Email*
    - *Authentication*: Change the context of the user; in other words, override the default appliance keys.
        - *Set API Keys*

d. Drag-and-drop a connector from the step to configure the next step.

e. Once all steps have been added, click *Save Playbook*.

Integrations with external systems

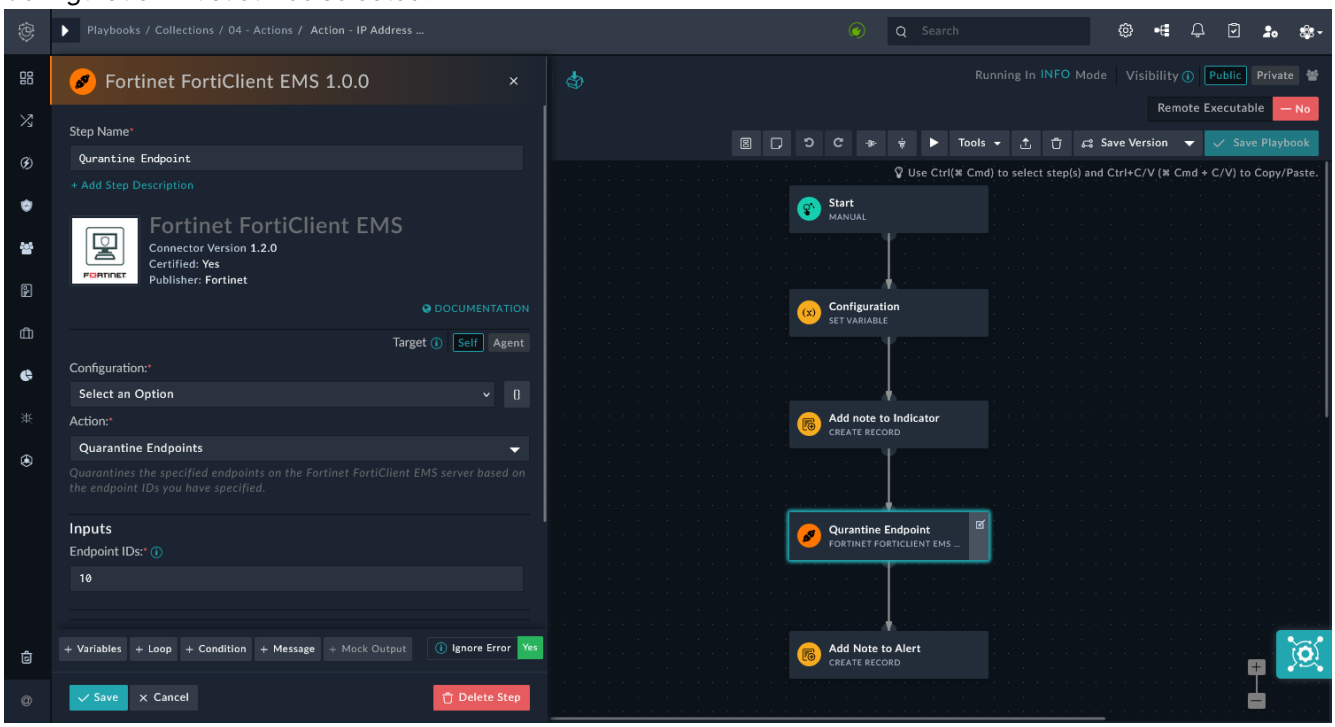
Playbooks automation in FortiSOC can integrate with external systems primarily through the use of *Execute > Connector* playbook steps.

The *Connector* step is used to add connectors to your playbook. Third-party connectors, such as connectors for Elastic, VirusTotal, or Splunk, can retrieve data from custom sources and perform automated operations. The predefined FortiSOC connectors, such as the IMAP connector and the SMTP connector, can also be used within *Connector* steps for playbooks to perform automated operations.

Before use in playbooks, connectors must be configured with necessary details such as API keys, IP addresses, and specific permissions or profiles on the external system. You can review connector configurations and their status in *Automation > Data Ingestion*.

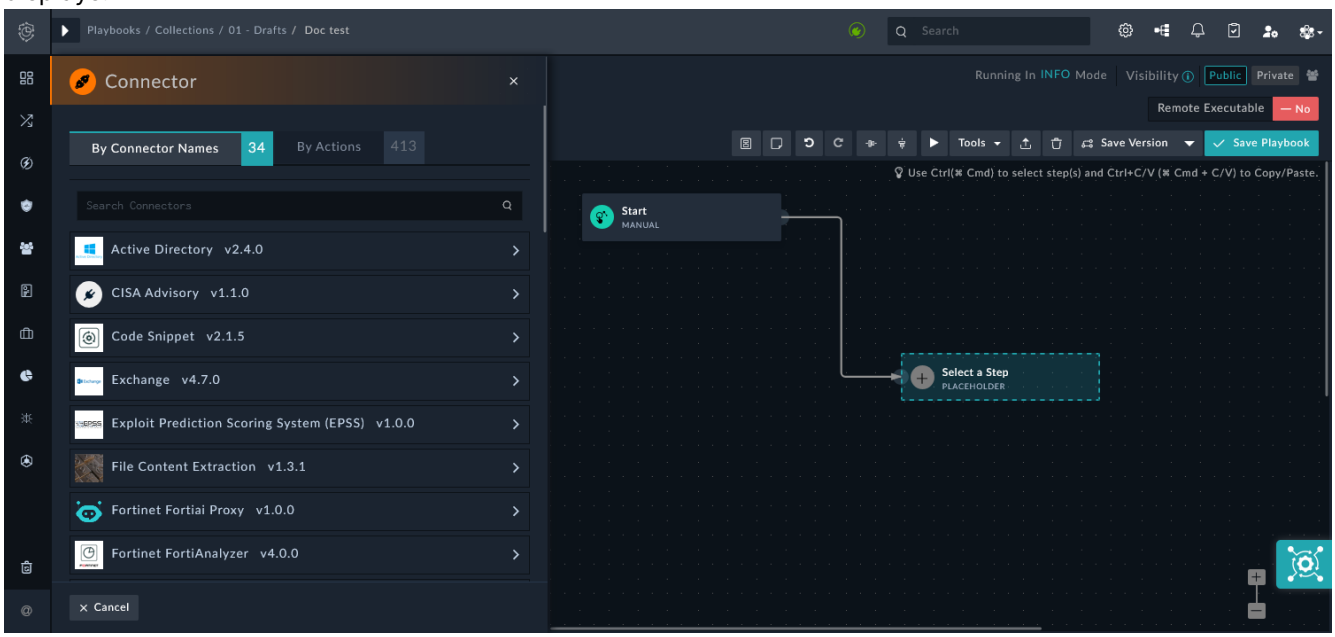
The example below displays the *Connector* step for the predefined *Action - IP Address - Block (Forticlient EMS)* playbook, which is included with the *SOAR Framework* solution pack. Note that the FortiClient EMS connector

Configuration must still be selected.



Configuring a Connector playbook step

When adding a step in the Playbook Designer, select *Execute* > *Connector*. The *Connectors* step dialog displays.



It includes two tabs:

- *By Connector Names*: Displays the connectors configured in your FortiSOC instance with available actions. Use this tab if you want to use a particular connector to perform a particular action.

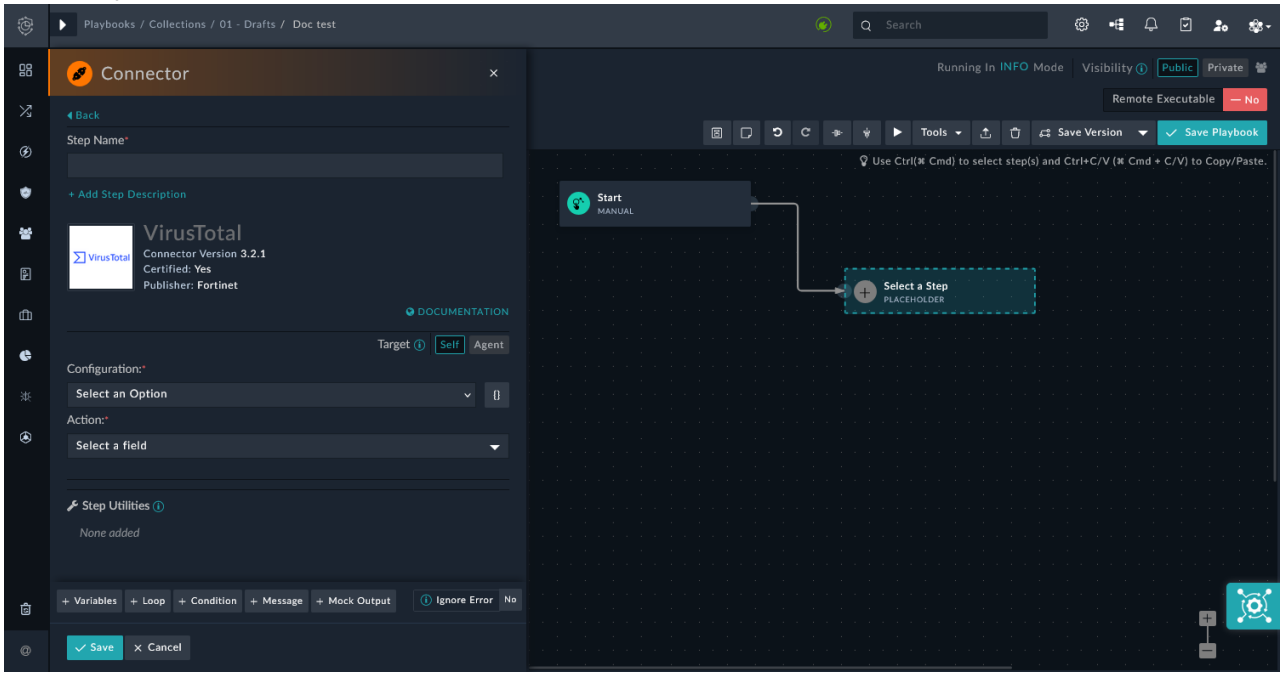
- *By Actions*: Displays the automated actions that you can perform using the connectors installed in your FortiSOC instance. Use this tab to first choose the action that you want to perform and then choose the connector that you want to use to perform the selected action.

You can configure the step using either of these tabs according to your preference.

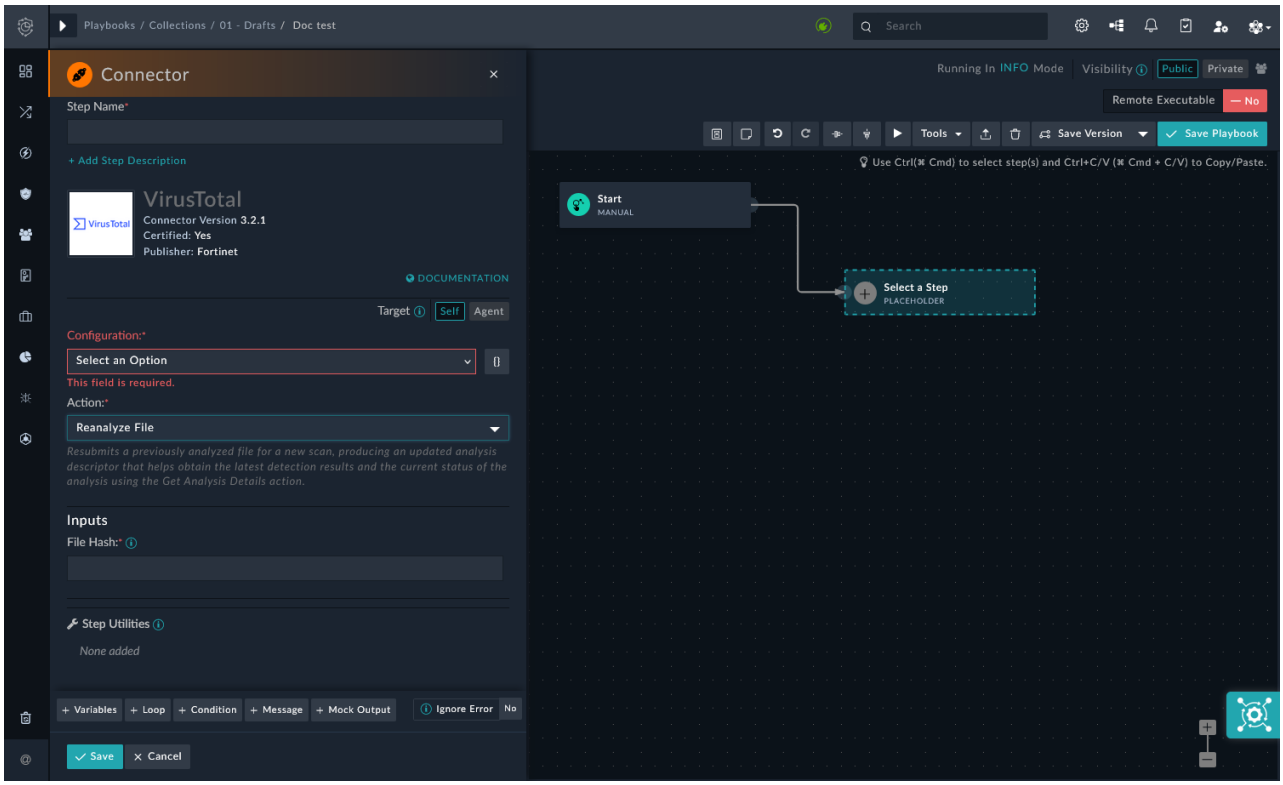
For further details about using the adding a Connector step to a playbook, see *Playbooks and Components > Playbook Steps > Execute Steps > Connector* in the FortiSOAR Playbooks Guide.

To configure the Connector step using the By Connector Name tab:

1. Use the *Search Connectors* field to search for connectors by name.
2. Select the connector that you want to include in your playbook.
   For example, select the VirusTotal connector.



3. In the *Step Name* field, enter a name to briefly describe the purpose of the step.
4. For the *Target* field, specify whether you want to run the action on the current FortiSOC node (*Self*) or remotely on the agent node (*Agent*).
   If you select *Agent*, you must also specify the agent on which you want to run the action.
5. From the *Configuration* dropdown, select the connector configuration that you want to run the action. You may have multiple connector configurations, which can be found and reviewed in *Automation > Data Ingestion*.
   You can also specify the connector configuration by clicking the {} icon and either typing the connector configuration name or specifying a Jinja variable that contains the connector configuration name.
   If you have only one configuration for the connector or have specified a default configuration, then that configuration is automatically selected.
6. From the *Action* dropdown, select the action that you want the connector to perform.
7. In the *Inputs* section, specify the required inputs. This will vary according to the connector and action.

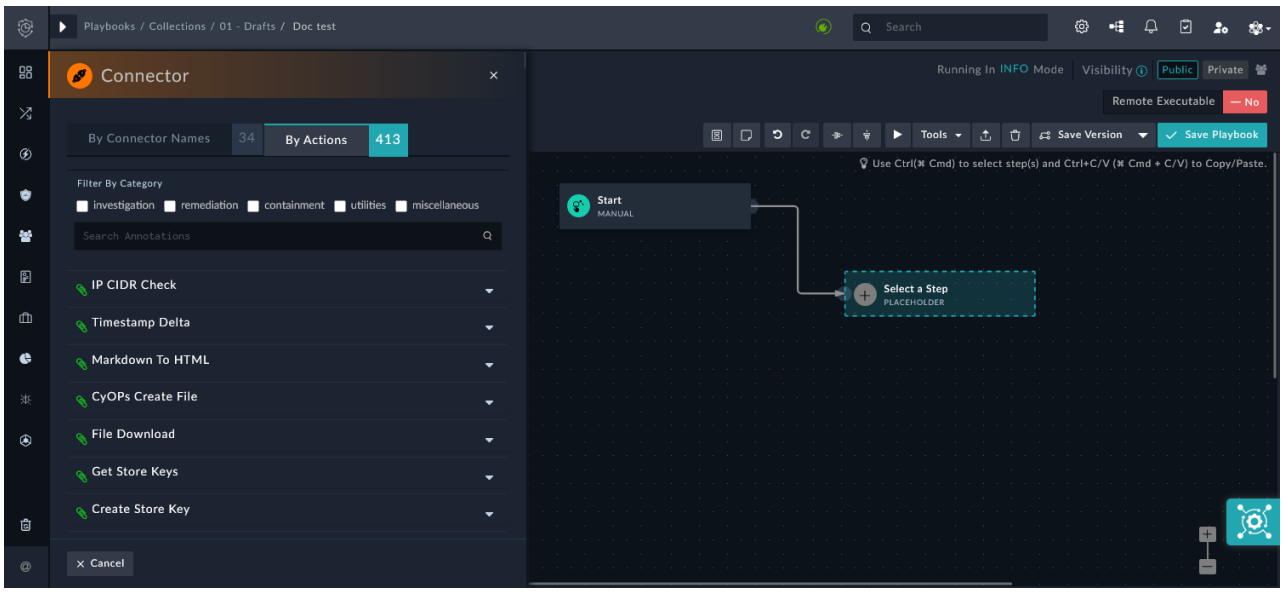


8. Click *Save* to add the connector as a playbook step.

To configure the Connector step using the By Actions tab:

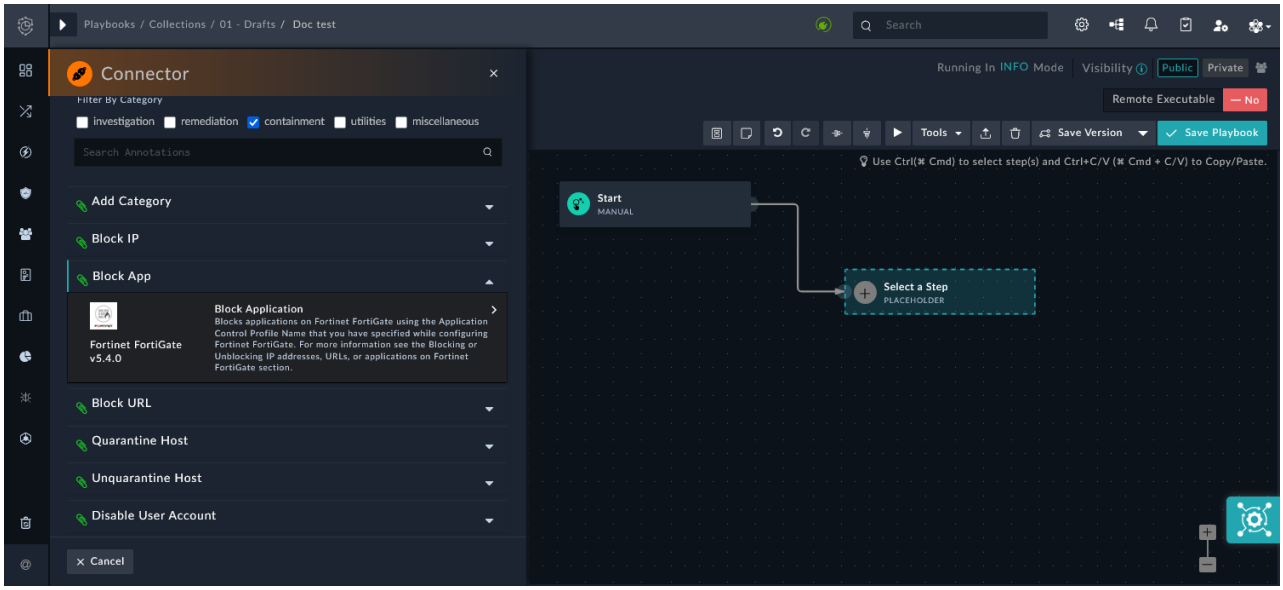
1. Use the *Filter By Category* section to filter the actions on the basis of the type of operation they will perform.

   The operation categories include investigation, remediation, containment, utilities, and miscellaneous categories.

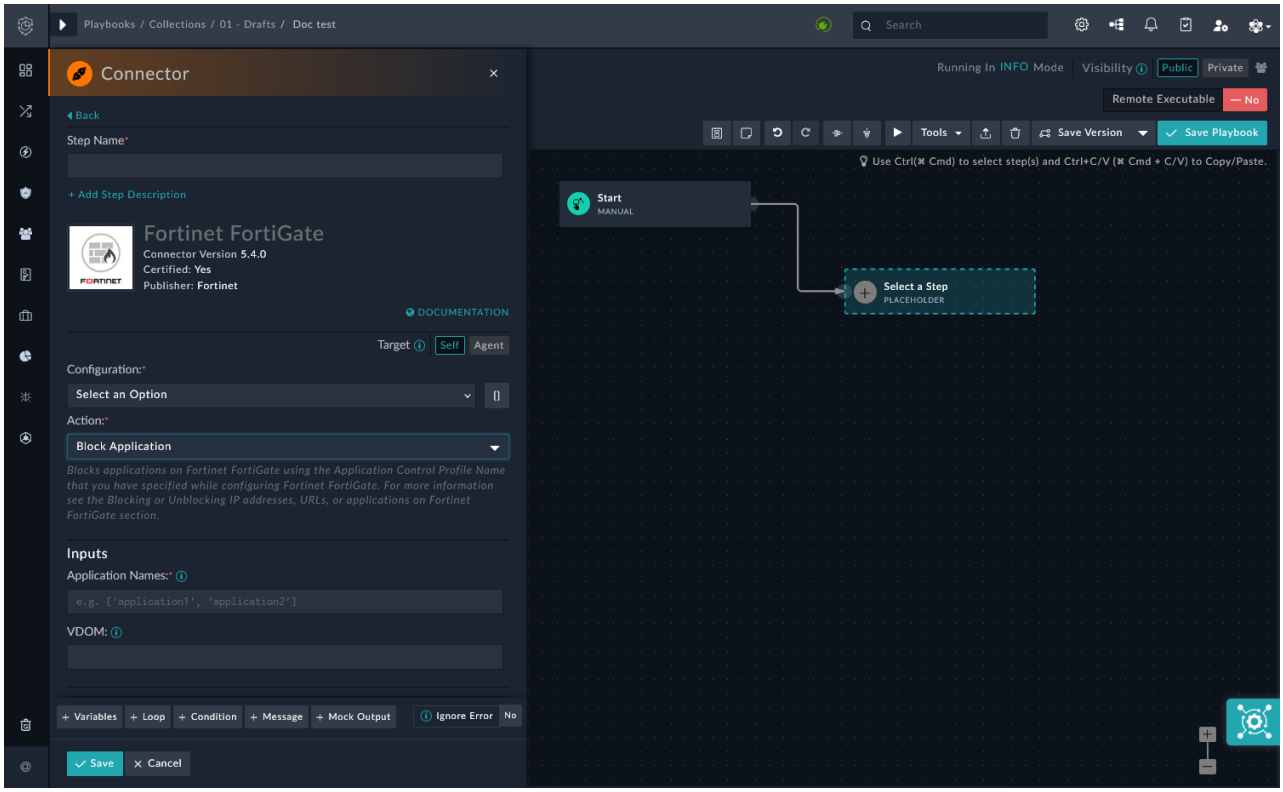


2. To search for a specific action that you want to perform, enter the keyword in the *Search Annotations* field.

3. Click the name of the action that you want to perform.
   An action may be supported by multiple connectors. Once you select the action, a list of configured connectors that can perform that operation is displayed.



4. From the list, select the connector and the exact operation that you want to perform.
   In this example, we have selected *Block App* > *Fortinet FortiGate* > *Block Application*.
5. In the *Step Name* field, enter a clear name to briefly describe the purpose of the step.
6. From the *Configuration* dropdown, select the connector configuration that you want to run the action.
7. In the *Inputs* section, specify the required inputs. This will vary according to the connector and action.



8. Click *Save* to add the connector as a playbook step.

Dashboards, reporting, and visibility

A comprehensive suite of dashboards is available in FortiSOC, delivering visibility into detections across Fortinet security devices, including email metrics and endpoint vulnerabilities. The SIEM dashboards provide insight into integrations with cloud and third-party applications such as AWS, GCP, Office 365, Salesforce, SentinelOne, and other security and network platforms. Additional dashboards offer centralized views of alerts and cases, threat intelligence searches, and vulnerability management.

You can navigate to the relevant information in FortiSOC directly from the dashboards, opening modules and object details from the widgets and lists included in the dashboards. This enables administrators and analysts to quickly triage and respond to critical tasks.

Similarly, predefined reports are also available to enhance visibility for administrators and analysts. SOC reports are built using interactive widgets that enable users to navigate to the relevant information or open object details in the FortiSOC GUI, same as from the dashboards.

Dashboards and reports are assigned by role. Thus, administrators can refine these assignments to ensure users have focused visibility on the information (dashboards and reports) most relevant to their duties.

Default admin dashboards

Dashboards are viewed and managed in the *Dashboard* module, which is the landing page for the FortiSOC instance.

You can select the dashboard from the dropdown in the toolbar. The following dashboards are available by default:

Dashboard	Description
Analyst	Review alerts, cases, and tasks assigned to analysts.
Analyzer - Email Metrics	Review email metrics according to FortiMail devices logging to the Analyzer module. This includes utilization, email counts, email bandwidth, recipients, senders, and more.
Analyzer - Endpoint Vulnerability	Review endpoint vulnerability information according to the FortiClient devices logging to the Analyzer module. This includes vulnerability severity, age distribution, historical trends, app trends, and more.
Analyzer - IoT	Review the internet of things (IoT) information according to licensed FortiGates logging to the Analyzer module. This includes number of devices, device categories, vulnerabilities by vendor, alert distribution, and more.
MITRE ATT&CK Matrices	Review the alert and case spread for the Enterprise, Mobile, and ICS MITRE ATT&CK Matrices. Click the techniques/sub-techniques to view a detailed description, linked procedure examples, and linked mitigations.
Overview	Review the number of alerts, unresolved cases, and further overview information regarding analyst workloads, time/money saved, closure reasons, and more.
ROI Summary	Review key performance metrics, alert trends, and case trends.
SIEM - AWS	Review AWS data, including CloudTrail, CloudWatch, Security Hub, and more when it is ingested in the SIEM module.
SIEM - Azure	Review Azure data, including Defender XDR and Entra ID when it is ingested in the SIEM module.
SIEM - Cloudflare	Review Cloudflare WAF data when it is ingested in the SIEM module.
SIEM - Crowdstrike	Review Cloudstrike Falcon data when it is ingested in the SIEM module.
SIEM - Database	Review the database data ingested in the SIEM module, including: • Logon • System performance • Oracle performance • SQL server performance • MySQL performance
SIEM - Fortinet Cloud Security	Review Fortinet Cloud Security data, including FortiCNAPP, FortiNDR Cloud, FortiDLP, FortiRecon, and more when it is ingested in the SIEM module.
SIEM - Fortinet Security Fabric	Review Fortinet Security Fabric data, including FortiGate, FortiProxy, FortiSandbox, FortiDeceptor, FortiPAM, and more when it is ingested in the SIEM module.
SIEM - GCP	Review the Google Cloud Platform (GCP) data when it is ingested in the SIEM module.

Dashboard	Description
SIEM - Mimecast	Review the Mimecast data when it is ingested in the SIEM module.
SIEM - Network	Review the network data ingested in the SIEM module, including: • Summary • Hardware • Availability • Performance • Netflow • IPSLA • VoIP • CBQoS
SIEM - Nutanix	Review the Nutanix audit data when it is ingested in the SIEM module.
SIEM - O365	Review the Microsoft O365 data when it is ingested in the SIEM module.
SIEM - Oracle Cloud	Review the Oracle Cloud data when it is ingested in the SIEM module.
SIEM - OT/IOT	Review the OT/IOT information from Armis and Nozomi SCADA Guardian when the data is ingested in the SIEM module.
SIEM - Salesforce	Review the Salesforce data when it is ingested in the SIEM module.
SIEM - Security	Review the security data ingested in the SIEM module, including: • Perimeter • Access • Malware • Vulnerability • Exploits • Policy Violation • UEBA AI Alerts • UEBA Events • OT/IoT
SIEM - SentinelOne	Review the SentinelOne data when it is ingested in the SIEM module.
SIEM - Server	Review the server data ingested in the SIEM module, including the summary, hardware, availability, and performance information.
SIEM - Trend Vision One	Review the Trend Vision One data when it is ingested in the SIEM module.
SIEM - Veeam	Review the Veeam data when it is ingested in the SIEM module.
SIEM - VMWare	Review the VMWare data when it is ingested in the SIEM module.
SIEM - Web Server	Review the web server data when it is ingested in the SIEM module, including: • Audit • System Performance • IIS Performance

Dashboard	Description
	• Apache Performance
SIEM - Windows	Review the Windows data when ingested in the SIEM module, including: • General • Security • System/Application • Sysmon • UEBA • Account/Privilege Management • Cases
SOC Admin	Review recent cases, alerts, and tasks.
SOC HQ Dashboard	Review a real-time animation that displays the flow of cases, indicators, assets, and identities from connected data ingestion sources. This is the default dashboard that displays when users first log into FortiSOC. Once logged in, they can set another dashboard as their default, if needed.
System Health Status	Displays the system health status, including the CPU usage, virtual memory usage, swap memory usage, and disk space usage. This dashboard also includes the service statuses, connector health statuses, and playbook execution monitoring.
Threat Intel Search	Search the FortiGuard cyber threat database for malicious indicators.
TIM Overview and ROI	Review the threat intelligence management (TIM) and return on investment (ROI) information, including ingestion volume, feed sources, number of linked indicators, and more.
Vulnerability Management	Review the vulnerability information, including number of critical vulnerabilities, vulnerabilities by severity, number of affected assets, and more.

The toolbar also includes buttons to *Refresh* and display the *Actions* menu. As a FortiSOC administrator, you can perform the following actions in the *Dashboard*:

Action	Description
Assign to Role	Select the roles that will have access to the dashboard. Each dashboard in the dropdown list displays the currently assigned roles.
Set as default for me	Set the dashboard as the default to display when you log into FortiSOC. Your default dashboard displays with a lightning bolt icon in the dropdown list.
Edit Dashboard	Edit the dashboard. You can change the title, define a structure, add widgets, add rows, configure inputs, and assign to roles.
New Dashboard	Create a new dashboard. For more information, see Custom dashboards and reports on page 94.

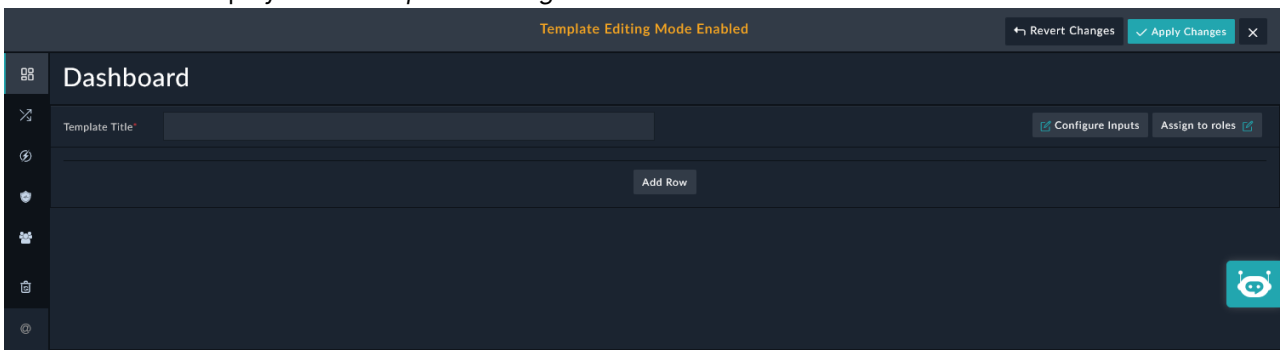
Action	Description
Import Dashboard	Import a dashboard that is in a valid JSON format. After importing the dashboard, you must assign it to roles for it to be visible to other users.
Export Dashboard	Export a dashboard to save the template on your machine in JSON format.
Clone Dashboard	Clone the dashboard.
Remove Dashboard	Remove the dashboard. You will be asked to confirm the action.

Custom dashboards and reports

You can create custom dashboards and reports according to your SOC's unique needs. The process for creating a dashboard template and SOC report template are the same.

To open template editing mode for a dashboard:

1. Go to *Dashboard*.
2. From the *Actions* menu in the toolbar, and then select *New Dashboard*.
   Alternatively, you can select *Clone Dashboard*.
   The *Dashboard* displays with *Template Editing Mode Enabled*.



To open template editing mode for a SOC report:

1. Go to *Reports* > *SOC Reports*, and click *Create New Report*.
   Alternatively, you can click the *Settings* icon for an existing report and select *Clone Template*.
   The *Reporting* module displays with *Template Editing Mode Enabled*.

The steps in this topic do not apply to Analyzer Reports and SIEM Reports. Those reports can be created in their respective modules:

- *Analyzer* > *Settings* > *Report Definitions*
- *SIEM* > *Resources* > *Reports*

To create the dashboard or report template:

1. Access *Template Editing Mode Enabled* as described in:
   - To open template editing mode for a dashboard
   - To open template editing mode for a SOC report
2. In the *Template Title* field, enter a title for the dashboard or report.
3. (Optional) To configure input, click *Configure Inputs*.
   a. (Optional) Select *Enable Auto-Refresh* to automatically refresh the dashboard or report after the set time interval.
   b. Click *Add New Input*.
   c. From the *Input Type* dropdown, select the type of field that is going to be applied as the input variable.
   You can choose from the following options: *Text*, *Number*, *Date*, *Date Range*, *Picklist*, or *Lookup*.
   d. In the *Label* field, enter a name that describes this variable.
   For example, if the *Input Type = Date Range*, the *Label* could be *Modified On*.
   The *Identifier* field is automatically populated with the identifier based on the specified *Label*. For example, if the *Label = Modified On*, the *Identifier* field is populated with the *modifiedOn* variable. The value of the *Identifier* field is the key by which this variable will be identified.
   e. (Optional) In the *Default Value* section, select the value based on which the dashboard or report will be displayed, by default.
   For date ranges, the ranges are relative to the current date. You can choose between a *Relative* date range or a *Custom* relative date range:
      - *Relative*: the dropdown list will include pre-defined relative date ranges such as Last 24 Hours, Last 30 Mins, and so on.
      - *Custom*: you can specify a custom date/time range, such as Last 2 Hours.
   f. (Optional) To make the input field mandatory, select the *Required* checkbox. When selected, the dashboard or report will not be displayed until the user provides the input.
   g. (Optional) To define more input variables, click *Add New Input*.
   h. Click *Save* to save the variable(s).
4. To assign the dashboard or report to roles, click *Assign to roles*.
   a. In the *Assign to Role(s)* dialog, select the roles that will be able to view the dashboard.

   > If you do not assign the dashboard or report to any roles, it will only be visible to you.

5. To configure a row, click *Add Row*.
   a. Using the options in *Define a new structure*, define the number and layout of columns for the row.
   b. To add a widget for the row, click *Add Widget*. and select the appropriate widget from the *Choose Widget* dialog box.
      i. In the *Choose Widget* dialog, select the appropriate widget type.
      The *Choose Widget* dialog includes the categorization of different types of widgets that you can use to build dashboards or reports. For example, the Tabs widget is categorized as a Structure and Navigation widget, and the Richtext Content widget is categorized as a Custom Content widget. Widgets that are installed using the Content Hub such as the Record Distribution, Case Correlations, User Tile, and more are categorized as Widget Library widget. You can also search for a specific widget by typing its name or description in the *Search Widget* text box and then selecting that widget.

ii. In the *Edit <name of widget>* dialog, configure the widget properties, and click *Save*.
The widget options will vary according to the selected widget type.

c. Add further widgets for the row, as needed.

6. Add further rows, as needed.
7. To save the dashboard or report , click *Apply Changes*.

Reports and scheduled delivery

There are predefined reports in FortiSOC to provide insights into Fortinet and third-party device activity, as well as case response operations.

Reports are available in three categories:

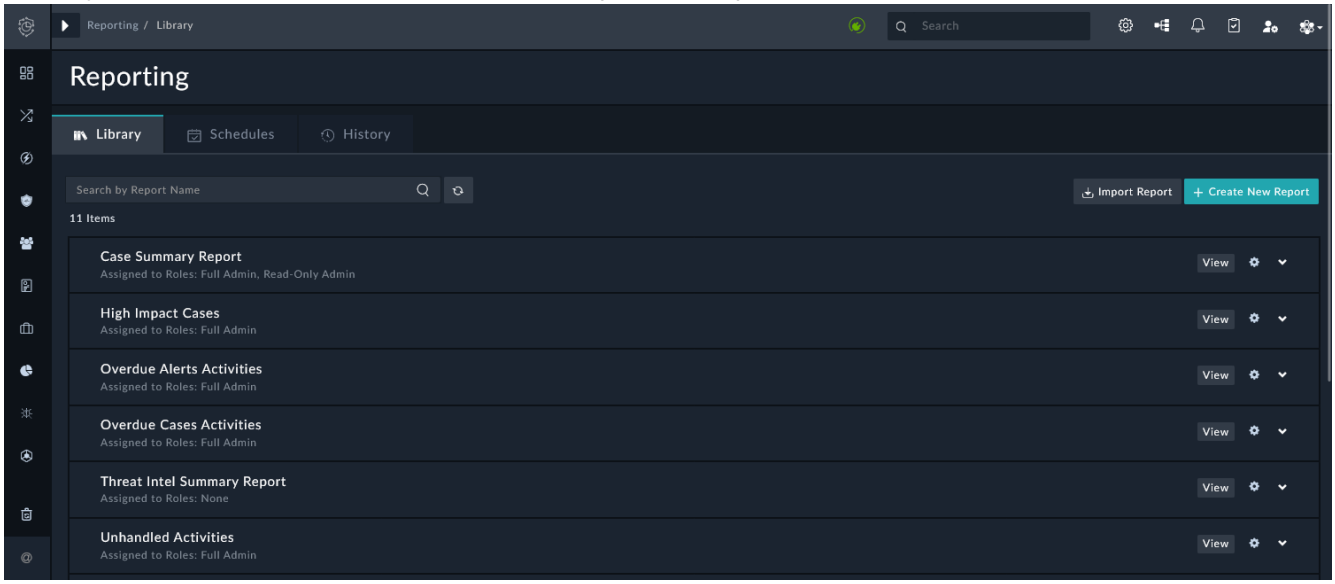
- SOC Reports
- Analyzer Reports
- SIEM Reports

SOC reports display the data within the FortiSOC GUI, so you can use the report to navigate through the GUI and open object details for further information. These reports can also be exported according to your needs.

Analyzer and SIEM reports display data in HTML. Analyzer reports can also be viewed as PDF, XML, CSV, and JSON. Many predefined Analyzer and SIEM reports are available and can be managed in their respective modules (*Analyzer* and *SIEM*); however, only generated reports can be viewed from the FortiSOC Reports module. You can schedule reports from their respective modules, so the generated outputs are available in FortiSOC Reports when they are needed for other admins and analysts.

SOC Reports

This module includes predefined reports, which can be run on-demand or scheduled to run. These reports use all analytics data in FortiSOC. You can create or import new reports.



To view a SOC report, click *View* for the report in the list. You may be required to enter input variables, such as a date range, to view the report.

When viewing a SOC report, you can interact with the rows and widgets to navigate to related areas of the platform or to open related detail views. For example, if a widget displays a case count at a specified severity level, you can click the widget to open the *Cases* list filtered by that criteria. If a table includes a list of alerts, you can click an alert to open the *Alert Details* pane. You can also export the report as a PDF, if needed.

The following predefined reports are available for FortiSOC administrators.

SOC report	Description
Case Summary Report	Displays a complete summary of the case, including case highlights, case timeline, and related records. *Required input*: Case ID.
High Impact Cases	Displays a summary of cases with *Severity = High*. *Required input*: Date range.
Overdue Alerts Activities	Displays open alerts with an overdue response due date.
Overdue Cases Activities	Displays open cases with an overdue response due date.
Threat Intel Summary Report	Displays a threat intelligence summary, including actor group analysis, impact analysis, next steps, and related feed records.
Unhandled Activities	Displays unassigned alerts and cases.
War Room Summary	Displays a summary of data from the war room.
War Room Summary Report	Displays performance metrics from the war room for related cases, alerts, indicators, and assets.
Weekly Alert Report	Displays a summary of alerts created in the past week. This includes number of alerts by type, assignment, and status as well as a list of the high severity open alerts.
Weekly Case Report	Displays a summary of cases created in the past week. This includes number of cases by type, assignment, and status as well as a list of the high severity open cases.
Weekly IOC Report	Displays a summary of indicators of compromise (IOCs) found in the past week.

From the *Settings* icon for the SOC reports, you can perform the following actions:

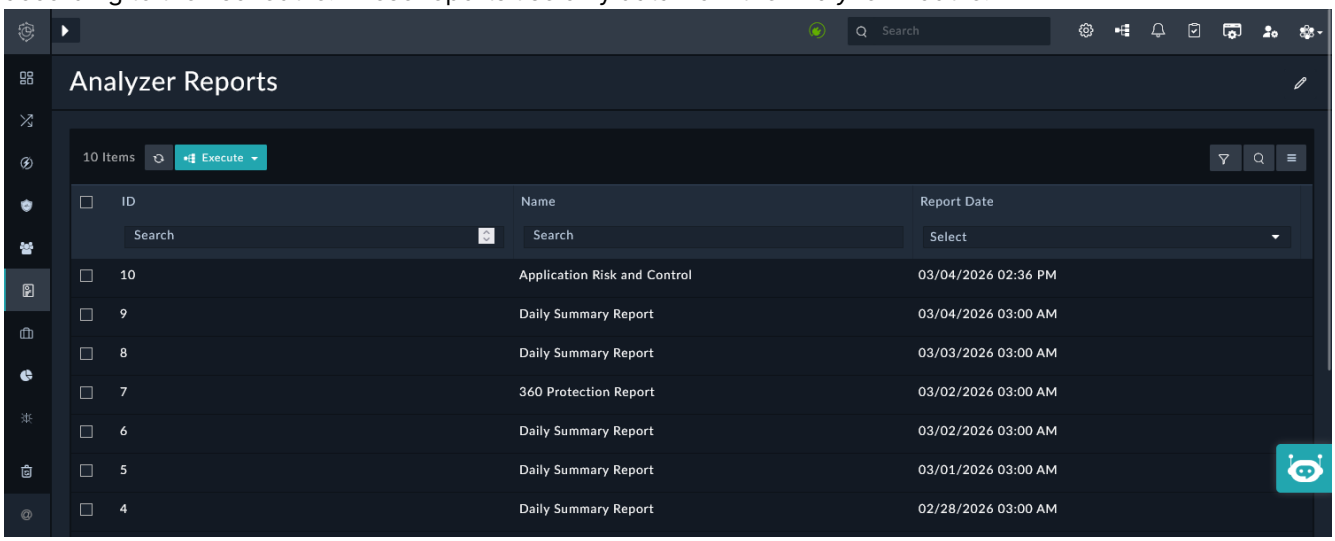
Action	Description
Schedule Report	Schedule the report to generate and send a notification to specified email address(es).
Assign to Role	Select the roles that will have access to the dashboard. Each report in the list displays the currently assigned roles.
Edit Template	Edit the report template.
Clone Template	Clone the report template.

Action	Description
Export Template	Export the report template on your machine in JSON format. You can click *Import Report* in the toolbar to import a report template in the appropriate JSON format.
Remove Template	Remove the report template. You will be asked to confirm the action.

There is a *Create New Report* option in the toolbar. For information about creating a SOC Report, see Custom dashboards and reports on page 94.

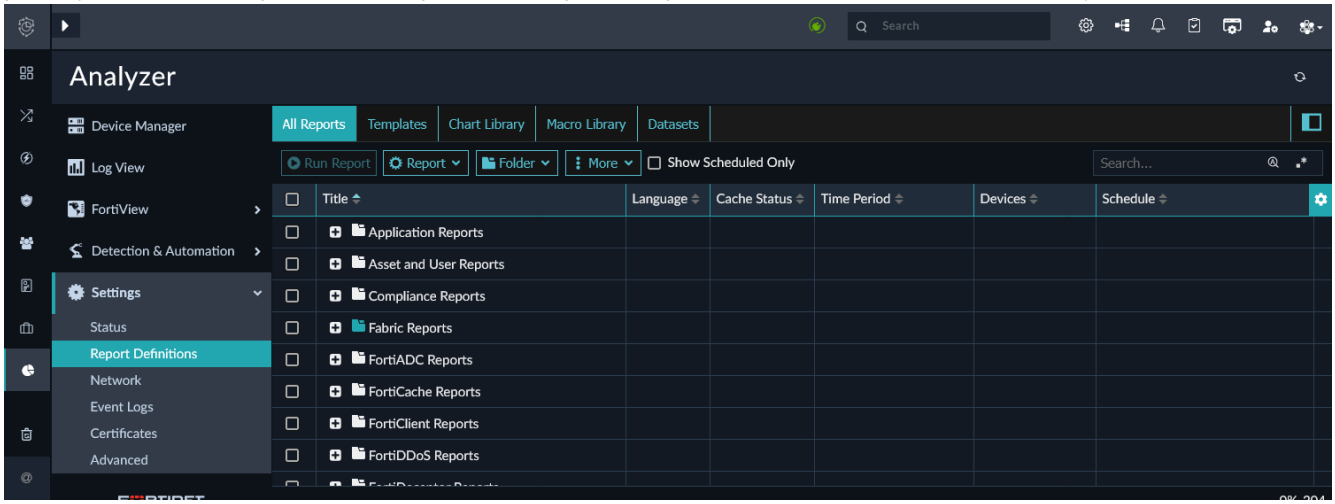
Analyzer Reports

This module displays reports generated in the *Analyzer* module, including reports that were generated according to their schedule. These reports use only data from the *Analyzer* module.



In *Reports* > *Analyzer Reports*, click *Execute* > *Get FAZ Reports* to fetch the reports that were generated in the *Analyzer* module.

Analyzer reports, including their schedules, can be managed in *Analyzer* > *Settings* > *Report Definitions*. In this pane, you can find all predefined reports and report templates that can be used for the *Analyzer* module.



There are two predefined Analyzer reports that run on a schedule. Their generated outputs will appear in *Reports* > *Analyzer Reports*.

Analyzer report	Description
360 Protection Report	Displays a summary of findings from the FortiGate devices over a 30 day period, together with recommendations and observations for follow up action where applicable. *Schedule*: Weekly on Monday at 03:00 AM.
Daily Summary Report	Displays the traffic usage, top applications by severity, top threats, and more according to the FortiGate devices. *Schedule*: Daily at 03:00 AM.

To schedule an Analyzer report:

1. Go to *Analyzer* > *Settings* > *Report Definitions* > *All Reports*.
2. Double-click the report and go to the *Settings* tab.
3. Select the checkbox for *Enable Schedule*, and then configure the following options:

Option	Description
Generate Report Every	Select when the report is generated. Enter a number for the frequency of the report based on the time period selected from the dropdown list.
Start Time	Enter a start date and time for the schedule.
End Time	Specify an end date and time for the report schedule, or set it to never ending (default).

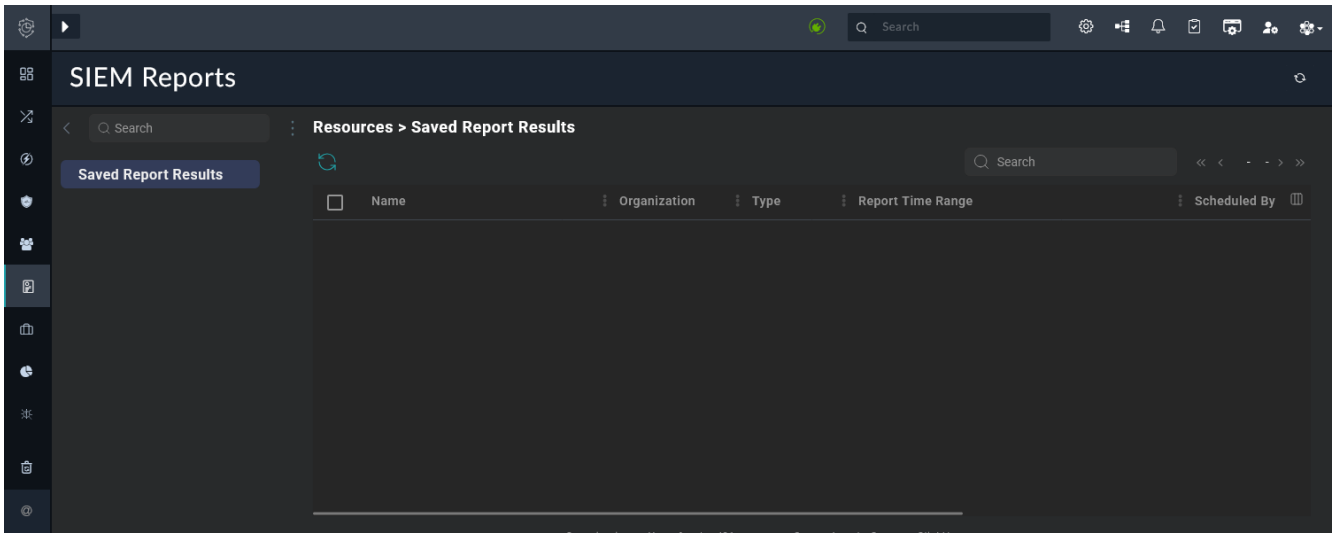
4. Click *Apply*.

To manually generate a report from the Analyzer module:

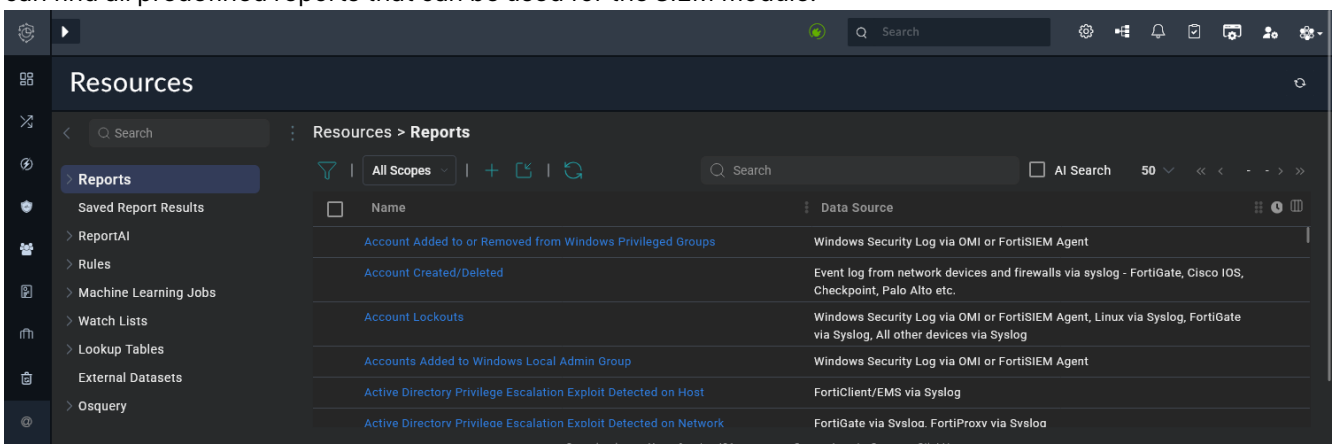
1. Go to *Analyzer* > *Settings* > *Report Definitions* > *All Reports*.
2. Select the report and click *Run Report*.
   You can double-click the report to view the status in the *Generated Reports* tab.
3. Once the report is generated, go to *Reports* > *Analyzer Reports*.
4. To include the newly generated report in the list, click *Execute* > *Get FAZ Reports*.
5. Double-click the record for the report to view it within the GUI. You can download the report as a PDF, XML, CSV, or JSON file.

SIEM Reports

This module displays reports generated in the *SIEM* module, including reports that were generated according to their schedule. These reports use only data from the *SIEM* module.



SIEM reports, including their schedules, can be managed from *SIEM* > *Resources* > *Reports*. In this pane, you can find all predefined reports that can be used for the *SIEM* module.



To schedule a report from the SIEM module:

1. Go to *SIEM* > *Resources* > *Reports*.
2. Select the checkbox for the report, and click the *Schedule* icon in the toolbar.
   The Schedule dialog displays.
3. Configure the following options, and then click *Next*:

Option	Description
Report Time Range	Configure what timeline of data should be used to generate the report.
Trend	Select the granularity of the time axis for the trend chart. If unsure, leave as *Auto*.

4. Configure the following options, and then click *Next*:

Option	Description
Schedule Time Range	Configure the start time for the report generation.
Schedule Recurrence Pattern	Configure how often the report will be generated.
Schedule Recurrence Range	Configure the time range for the schedule recurrence.

5. Configure the following options, and then click *Next*:

Option	Description
Output Format	Select the report output format (PDF or CSV).
Notification	Configure the notifications: • *Default Notification*: send notification to new recipients by adding them using the + icon. • *Custom Notification*: send the notification to the specific email addresses. • *Copy to a remote location*: To copy the report to a remote directory, first define the remote location in *SIEM > Settings > Settings > Analytics > Scheduled Report*.
Retention	Configure how long the report should be kept for in FortiSOC.

6. Click *OK*.
   The generated reports can be found in *Reports > SIEM Reports* according to their configured schedule and retention.

AI overview

The FortiAI service included with FortiSOC provides the following capabilities:

- Case impact analysis, including suggested next steps for a SOC action plan
- Threat summaries, including insights for high-risk cases, alerts, and assets
- Threat investigation support using an AI investigation agent

FortiAI is powered by the *Fortinet FortiAI* connector, which comes preconfigured for your FortiSOC instance. This FortiAI proxy is a secure intermediary that routes chat completion API requests through a controlled layer instead of sending them directly to the LLM provider.

This connector includes the following actions:

Action	Description
Chat Completion	Chat Completions is an API endpoint that allows applications to interact with AI models using a conversation format (messages with roles like system, user, and assistant). It is used to generate responses, answer questions, automate tasks.
Create Response	Create an new AI response using the Responses API.
Get Token Balance Details	Retrieves the token balance details, including entitled tokens, top-up tokens, account tokens, and their respective remaining balances.

FortiAI is used in the following playbooks, which can be found in *Automation > Playbooks* within the *Fortinet FortiAI* playbook collection:

Playbook	Description
FortiAI - Case Impact Assessments	This playbook leverages AI to automatically evaluate the potential business impact of a security incident, providing analysts with a prioritized risk score and context to focus on the most critical threats first.
FortiAI - Case Extraction	AI-powered case data extraction from security alerts for automated triage and response.
FortiAI - Case Enrichment & Impact Analysis	Extract information from cases and assess its impact.
FortiAI - Case Enrichment & Impact Analysis (On Update)	Extract information from cases (on update) and assess its impact.
FortiAI - Case Autonomously Remediation Demo	A demonstration playbook showcasing FortiAI's ability to autonomously investigate and remediate common security cases, providing a hands-on view of fully automated threat resolution from detection to containment.
FortiAI - Asset Threat Posture Timeline	Automatically generates a chronological timeline of security events and posture changes for a specific asset, giving analysts a clear, visual of its exposure to threats and the evolution of its security state.

To leverage AI within FortiSOC, SOC analysts can:

- execute FortiAI playbooks where relevant in the FortiSOC platform, such as within *Cases* or Case details. See FortiAI case enrichment on page 103.
- open the FortiAI Insight pane to view a threat summary of cases, alerts, and assets. See FortiAI Insight on page 105.
- prompt the FortiAI Investigation Agent for threat investigation support. See FortiAI Investigation Agent on page 107.

FortiAI case enrichment

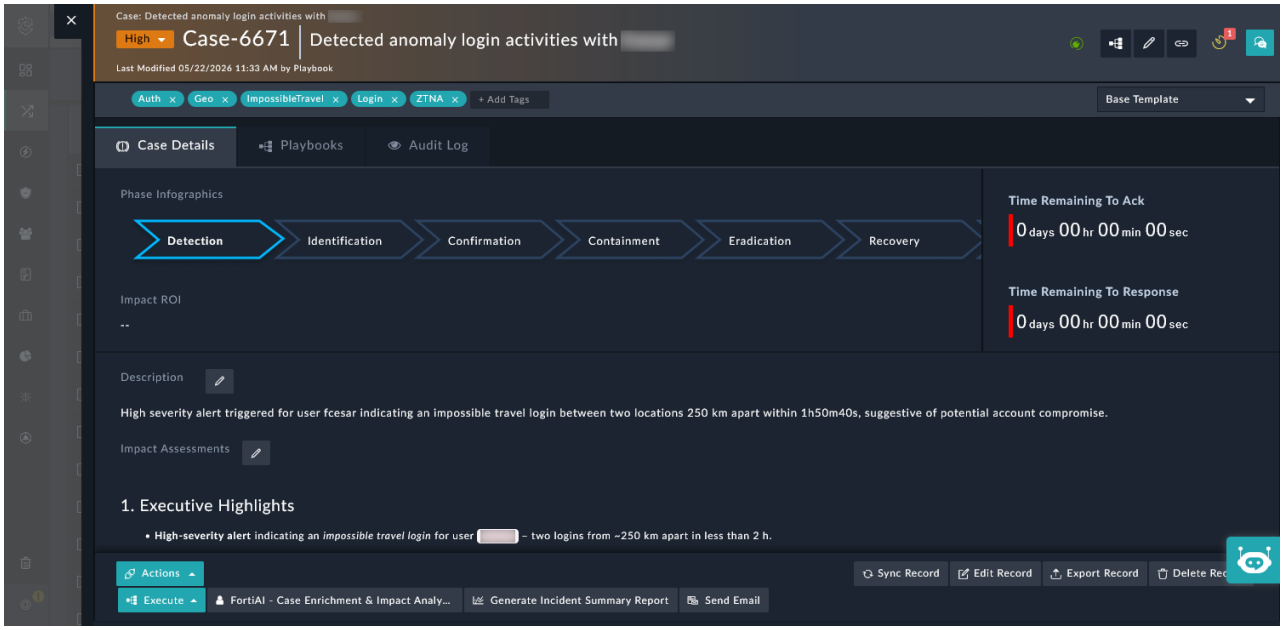
In *Cases & Alerts > Cases*, SOC analysts can execute FortiAI playbooks for case enrichment, impact analysis, and asset threat posture timelines. In the Case details, there is also a shortcut button to execute *FortiAI - Case Enrichment & Impact Analysis*.

To execute the FortiAI - Case Enrichment & Impact Analysis:

1. Go to *Cases & Alerts > Cases*.
2. Double-click a case to open the Case details.
3. Click *FortiAI - Case Enrichment & Impact Analysis*.

   If the case already has impact assessment data, a dialog will display to confirm if you would like to update the existing assessment or start fresh.

   Once the playbook successfully completes, FortiAI will update and/or populate the *Description* and *Impact Assessments* fields in the Case details.

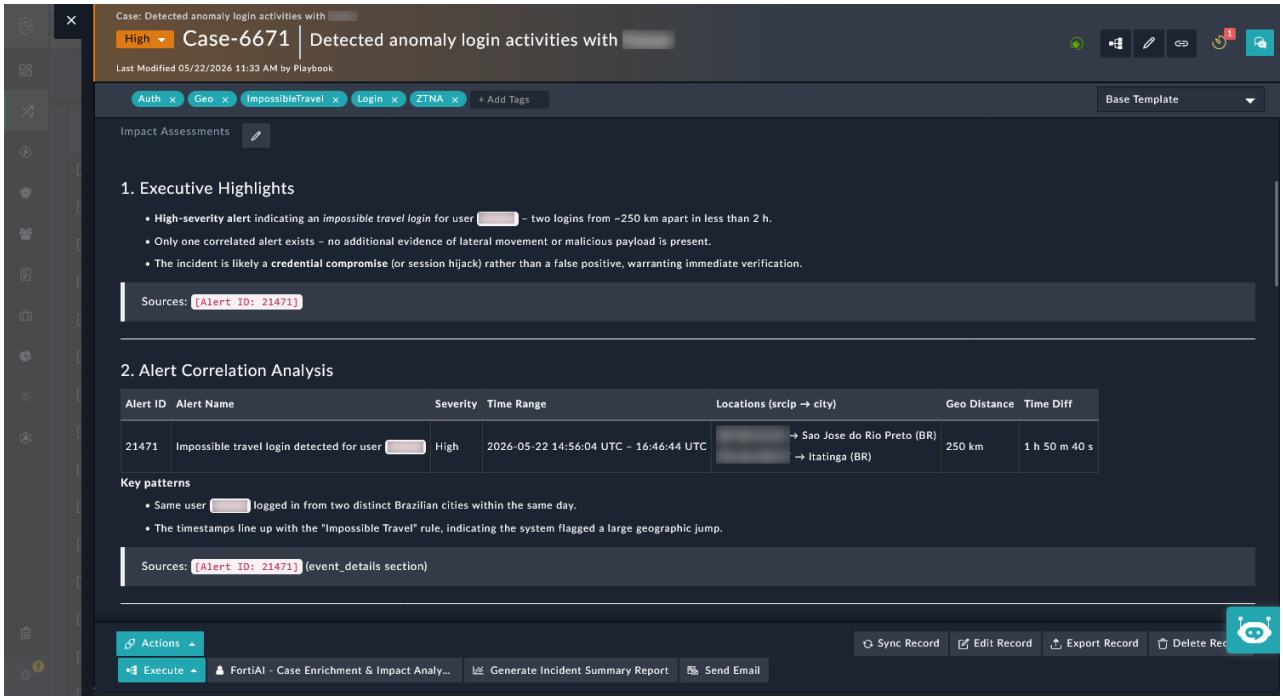


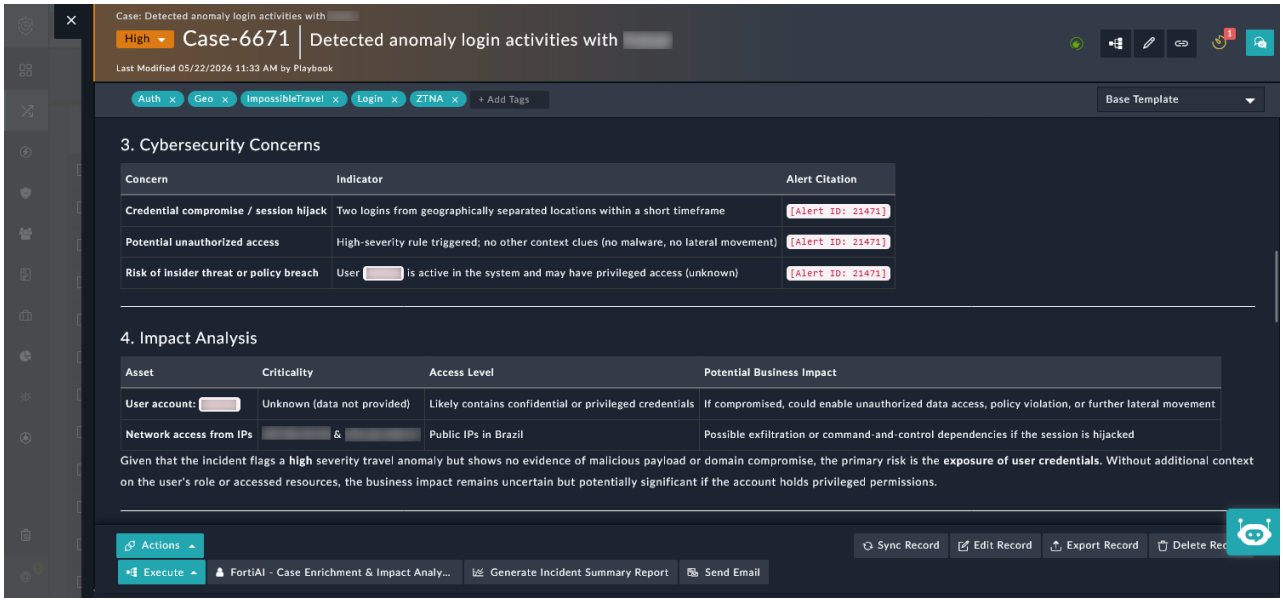
The *Impact Assessments* is structured by a template to include the following information:

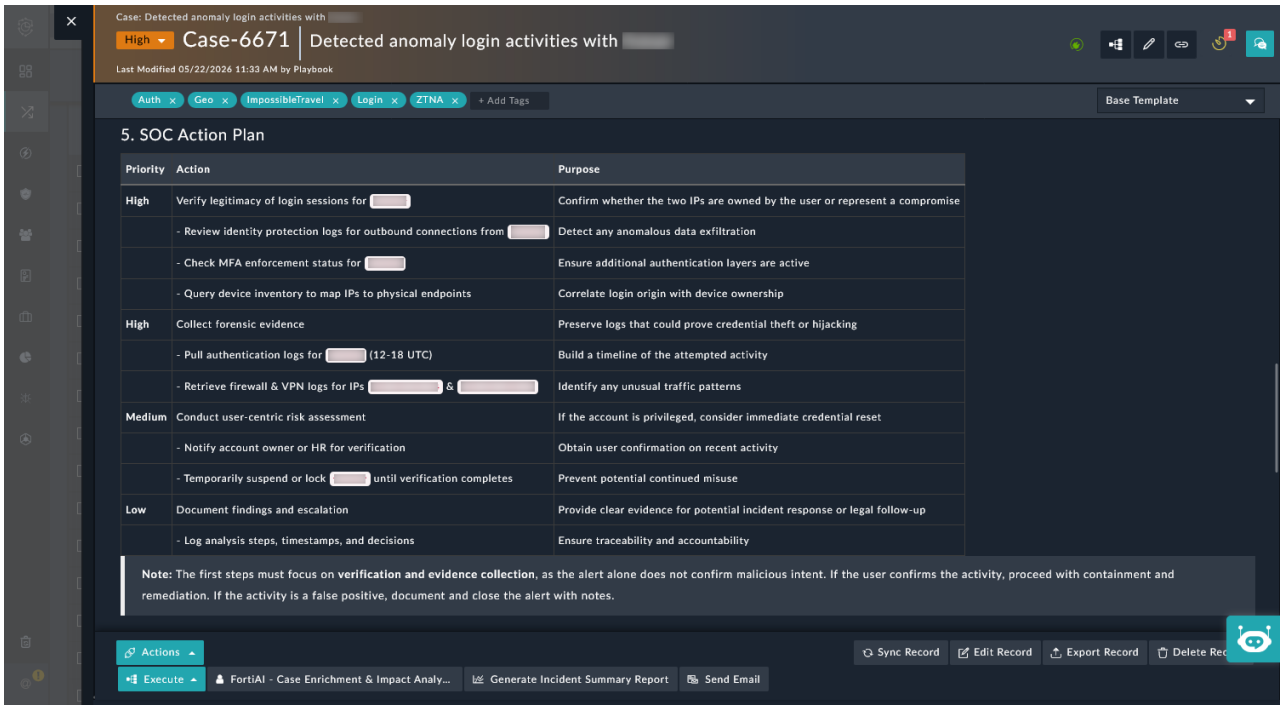
- *Executive Highlights*
- *Alert Correlation Analysis*

- *Cybersecurity Concerns*
- *Impact Analysis*
- *SOC Action Plan*

See below for an example of the *Impact Assessment* from FortiAI:

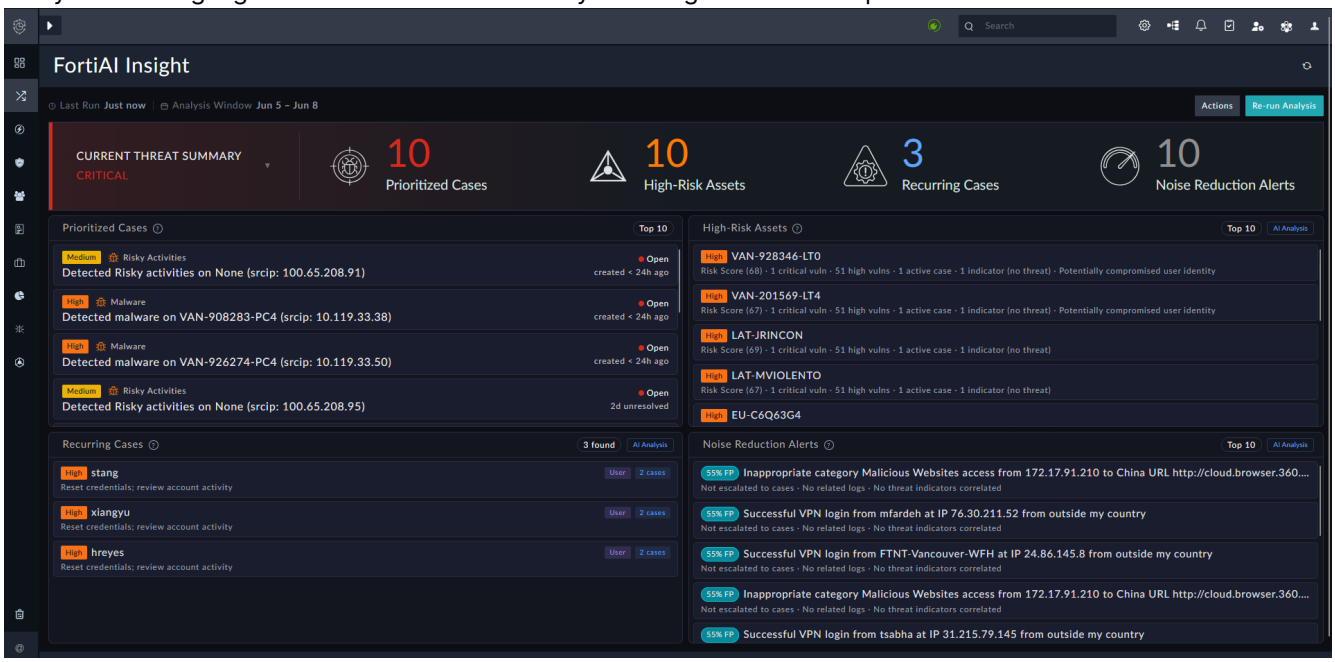






FortiAI Insight

Going to *Cases & Alerts* > *FortiAI Insight* triggers FortiAI to fetch cases and alerts and perform deep correlation analysis. This highlights the threats for SOC analysts and guides next steps.

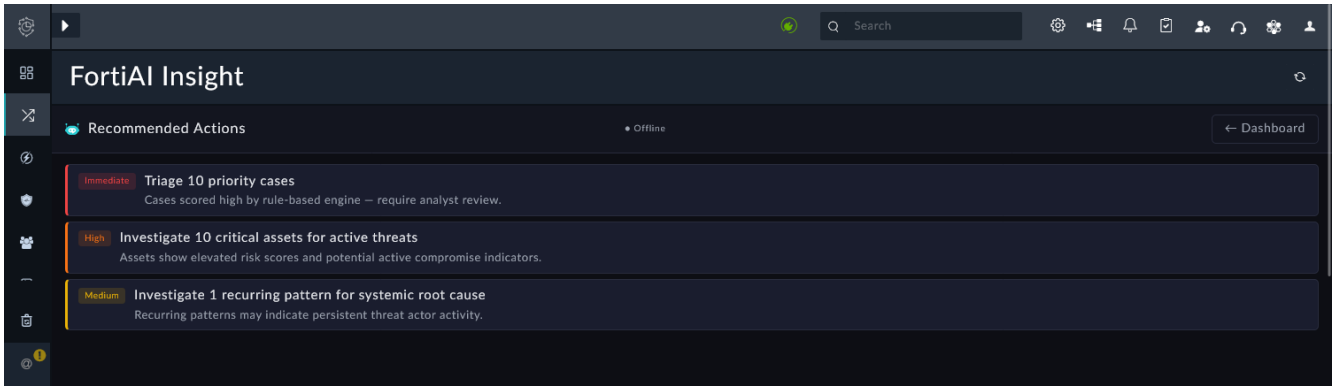


Once FortiAI completes the analysis, the *FortiAI Insight* pane displays the following information:

Widget	Description
Current Threat Summary	Lists the number of prioritized cases, high-risk assets, recurring cases, a reduce noise alerts. See below for further descriptions.
Prioritized Cases	Lists prioritized cases ranked by risk factors, including: • *Severity*: Critical/High severity cases • *SLA State*: Missed SLA deadlines • *Phase*: Active investigation phase • *Threat IOCs*: Correlated malicious and suspicious indicators • *Alert Volume*: Multiple correlated alerts Click a case to display the Case details.
High-Risk Assets	Lists high-risk assets flagged for risk factors, including: • *Vulnerabilities*: Critical/High vulnerability counts • *Active Cases*: Asset involved in open cases • *Threat IOCs*: Associated with malicious and suspicious indicators • *Compromised Identities*: User account shows high-risk behavior Click an asset to display the Asset details. Click *AI Analysis* to view the analysis from FortiAI. This includes the *Risk* and *Score* for the asset as well as the supporting evidence (Risk Score, number of critical and high vulnerabilities, number of active cases, number of indicators, etc.).
Recurring Cases	Detects patterns across cases: • *IOC Reuse*: Same malicious/suspicious indicators (IPs, domain, hashes) appear in multiple cases • *Asset Compromise*: Same asset/hostname targeted across multiple cases • *User Targeting*: Same user/email targeted across multiple cases Click a record in the list to view the details. From these details, you can click the related cases to open their Case details. Click *AI Analysis* to view the analysis from FortiAI. This includes the breakdown of the IOC Reuse, Asset Compromise, or User Targeting identified by FortiAI. Patterns require two or more cases to be flagged.
Noise Reduction Alerts	Alerts flagged as potential false positives, which could be generating noise: • *Low Signal*: Minimal threat indicators present • *Benign Patterns*: Matches known safe activity • *Rule Drift*: Detection rules may need recalibration Review these alerts and, if appropriate, suppress them to reduce noise and analyst fatigue. Click *AI Analysis* to view the analysis from FortiAI, including confidence and brief reasoning for flagging the false positive.

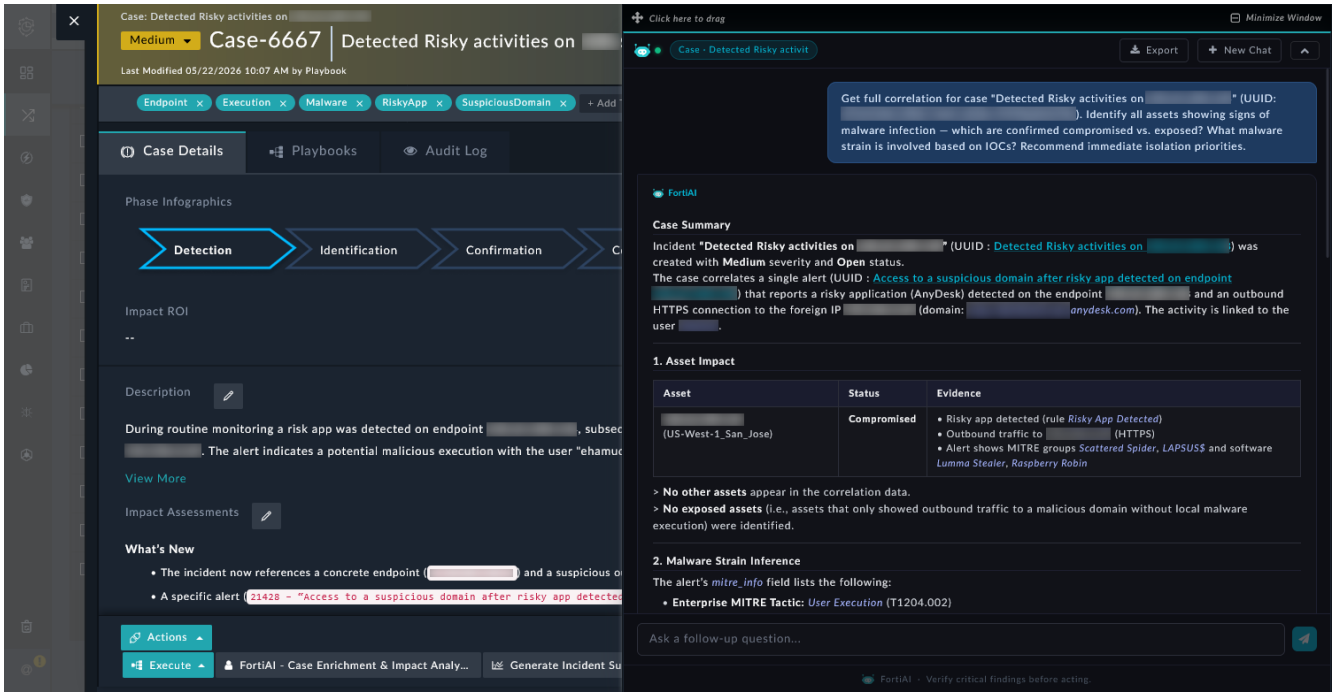
The analysis will remain if the SOC analyst navigates away and returns to the *FortiAI Insight* pane. Click *Re-run Analysis* to trigger a fresh analysis from FortiAI.

Click *Actions* to view the *Recommended Actions* from FortiAI.



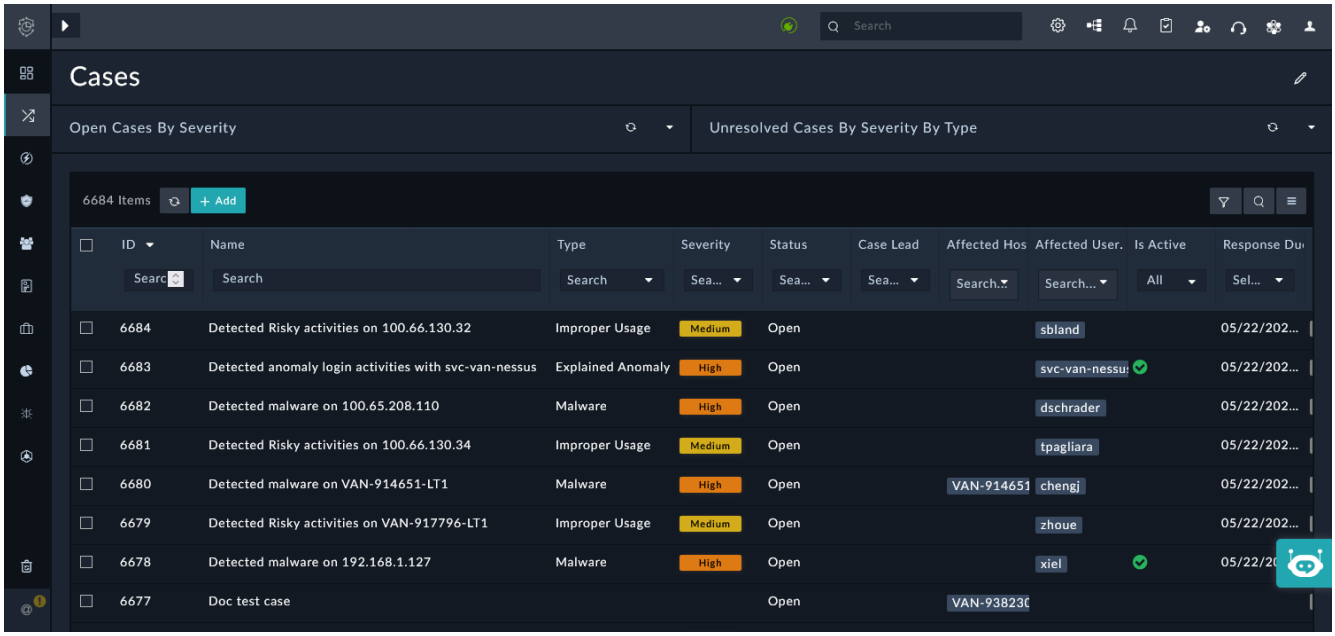
FortiAI Investigation Agent

The *FortiAI Investigation Agent* can be used by SOC analysts to efficiently investigate threats, answer questions, and get suggested next steps using FortiAI's advanced natural language processing capabilities. The agent's responses can include text, images, widgets, and data retrieved directly from your FortiSOC instance. Any response actions remain controlled and require approval by the SOC analyst to complete.

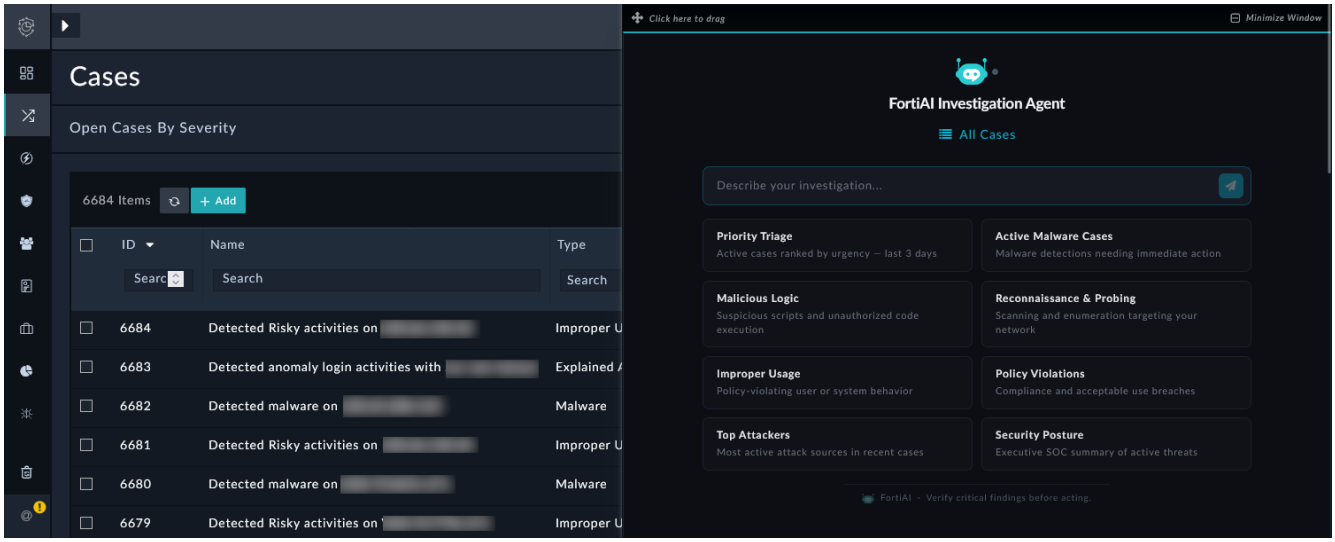


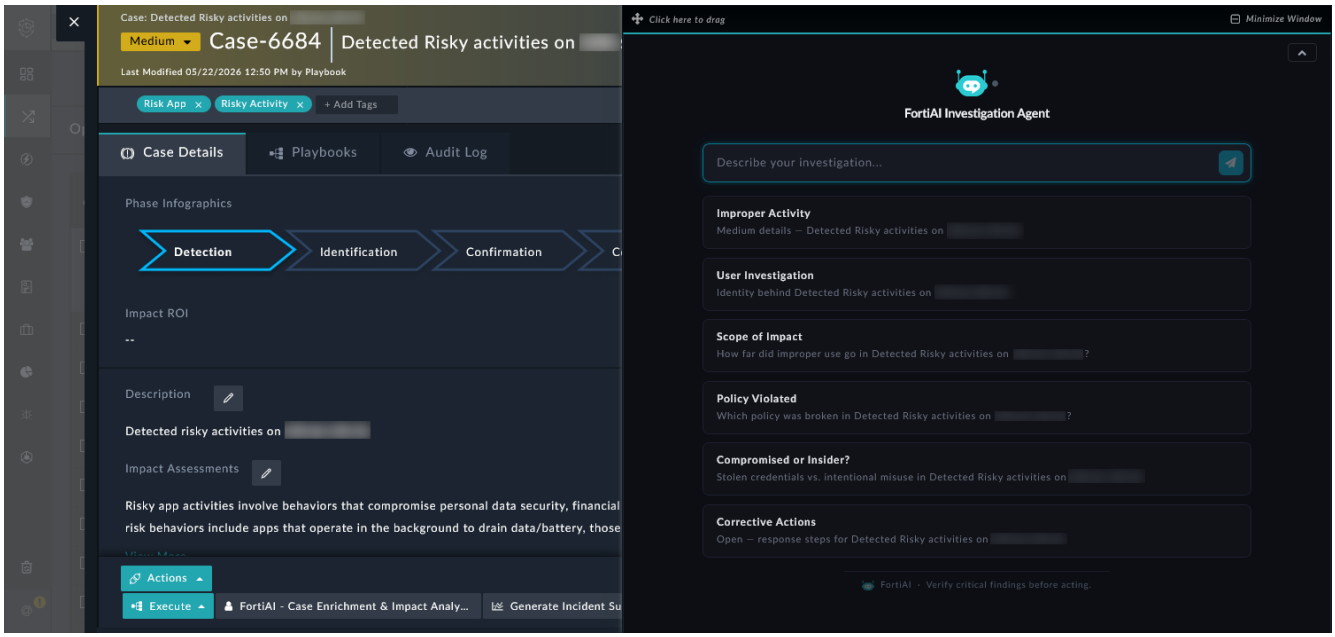
The *FortiAI Investigation Agent* can be opened using the FortiAI button at the bottom right of the following panes:

- *Alerts*
- *Cases*
- *Assets*
- *Identities*
- *Indicators*



The *FortiAI Investigation Agent* window displays suggested prompts according to the pane you are in. You can open the agent within the details view to get more specific investigation suggestions. For example, see below where the *FortiAI Investigation Agent* is opened in *Cases* compared to Case details.





Alternatively, the SOC analysts can enter their own custom prompt to start the chat with the agent. You can use natural language to request actions or information from the agent.

After the initial response from the agent, SOC analysts can perform the following actions from within the FortiAI Investigation Agent window:

- *Show reasoning*: Click *Show reasoning* at the bottom of the response to display the reasoning from the agent.
- *Export the chat*: Click *Export* to export the complete chat as a PDF to download and share with other analysts.
- *Start a new chat*: Click *+ New Chat* to start a new chat with the agent.
- *Ask follow-up questions*: Enter a new prompt in the text box at the bottoms and click the Send button to continue the chat with the agent.

Prompts should be directly related to the information the assistant is programmed to access, enabling efficient and effective data retrieval. A valid prompt is a clear, well-defined question that the agent can easily interpret and process. It should be specific and relevant to the data or queries the agent is designed to handle. For example, the agent can be effectively used to:

- add context, such as asset information, user identity, and threat intelligence.
- correlate events and build a timeline to show what happened.
- analyze the data to identify patterns or possible attack scenarios.
- suggest next steps, such as escalating the case, containing the issue, monitoring, or closing the case.

An invalid prompt is one that cannot be easily interpreted or processed by the agent. This typically includes prompts that are ambiguous, lack sufficient detail, or are outside the scope of the agent's capabilities (e.g. prompts that ask about information outside of FortiSOC).

www.fortinet.com