

CISCO Security Cloud App User Guide

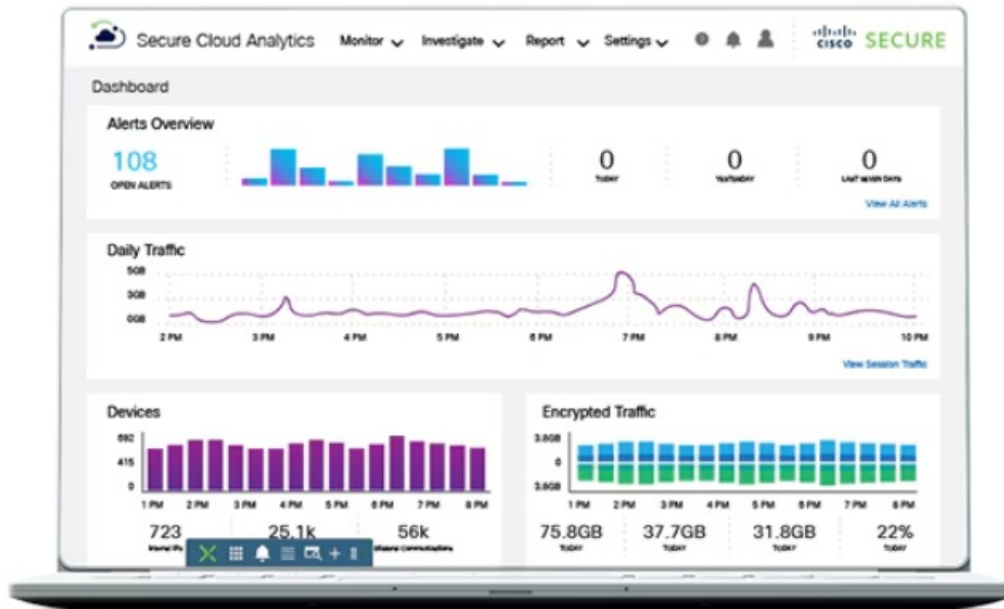
[Home](#) » [Cisco](#) » CISCO Security Cloud App User Guide 

Contents

- 1 CISCO Security Cloud App
- 2 Product Usage Instructions
- 3 Set Up an Application
- 4 Configure an Application
- 5 Cisco Duo
- 6 Cisco Secure Malware Analytics
- 7 Cisco Secure Firewall Management Center
- 8 Cisco Multicloud Defense
- 9 Cisco XDR
- 10 Cisco Secure Email Threat Defense
- 11 Cisco Secure Network Analytics
- 12 Documents / Resources
 - 12.1 References



CISCO Security Cloud App



Specifications

- **Product Name:** Cisco Security Cloud App
- **Manufacturer:** Cisco
- **Integration:** Works with various Cisco products

Product Usage Instructions

Set Up an Application

Application Setup is the initial user interface for the Security Cloud App. Follow these steps to configure an application:

1. Navigate to the Application Setup > Cisco Products page.
2. Choose the desired Cisco application and click on Configure Application.
3. Complete the configuration form which includes Brief app description, Documentation links, and Configuration details.
4. Click Save. Ensure all fields are filled correctly to enable the Save button.

Configure Cisco Products

To configure Cisco Products within the Security Cloud App, follow these steps:

1. On the Cisco Products page, select the specific Cisco product you want to configure.
2. Click on Configure Application for that product.
3. Fill in the required fields including Input Name, Interval, Index, and Source Type.
4. Save the configuration. Correct any errors if the Save button is disabled.

Cisco Duo Configuration

For configuring Cisco Duo within the Security Cloud App, follow these steps:

1. In the Duo Configuration page, enter the Input Name.
2. Provide the Admin API credentials in the Integration key, Secret key, and API hostname fields.

3. If you do not have these credentials, register a new account to obtain them.

Frequently Asked Questions (FAQ)

- **Q: What are the common fields required for configuring applications?**

A: The common fields include Input Name, Interval, Index, and Source Type.

- **Q: How can I handle authorization with Duo API?**

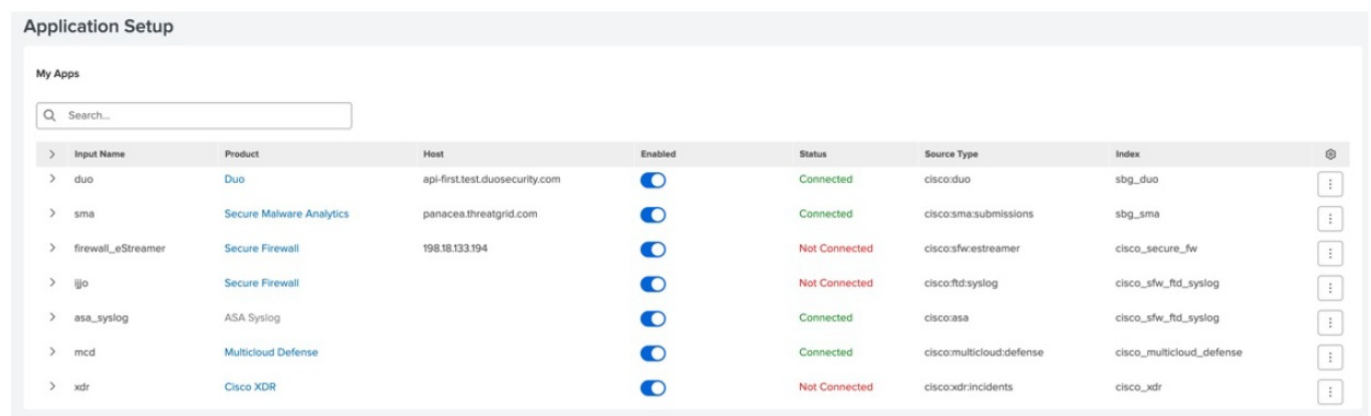
A: Authorization with Duo API is handled using the Duo SDK for Python. You need to provide the API Hostname obtained from the Duo Admin Panel along with other optional fields as required.

This chapter guides you through the process of adding and configuring inputs for various applications (Cisco products) within the Security Cloud App. Inputs are crucial because they define the data sources that the Security Cloud App uses for monitoring purposes. Proper configuration of inputs ensures that your security coverage is comprehensive and that all data is properly displayed for future tracking and monitoring.

Set Up an Application

Application Setup is the first user interface for the Security Cloud App. The Application Setup page consists of two sections:

Figure 1: My Apps



The screenshot shows the 'Application Setup' page with a 'My Apps' section. It contains a search bar and a table of configured inputs. The table has columns for Input Name, Product, Host, Enabled, Status, Source Type, and Index. Each row represents a different input configuration, with status indicators (Connected or Not Connected) and action menus (three dots) for each input.

>	Input Name	Product	Host	Enabled	Status	Source Type	Index	
>	duo	Duo	api-first.test.duosecurity.com	<input checked="" type="checkbox"/>	Connected	cisco:duo	sbg_duo	⋮
>	sma	Secure Malware Analytics	panacea.threatgrid.com	<input checked="" type="checkbox"/>	Connected	cisco:sma:submissions	sbg_sma	⋮
>	firewall_eStreamer	Secure Firewall	198.18.133.194	<input checked="" type="checkbox"/>	Not Connected	cisco:fwestreamer	cisco_secure_fw	⋮
>	ljo	Secure Firewall		<input checked="" type="checkbox"/>	Not Connected	cisco:ftd:syslog	cisco_sfwd_ftd_syslog	⋮
>	asa_syslog	ASA Syslog		<input checked="" type="checkbox"/>	Connected	cisco:asa	cisco_sfwd_ftd_syslog	⋮
>	mcd	Multicloud Defense		<input checked="" type="checkbox"/>	Connected	cisco:multicloud:defense	cisco_multicloud_defense	⋮
>	xdr	Cisco XDR		<input checked="" type="checkbox"/>	Not Connected	cisco:xdr:incidents	cisco_xdr	⋮

- The My Apps section on the Application Setup page displays all user input configurations.
- Click a product hyperlink to go to the product dashboard.

>	Input Name	Product	Host
>	duo	Duo	api-first.test.duosecurity.com

- To edit inputs, click Edit Configuration under the action menu.
- To delete inputs, click Delete under the action menu.

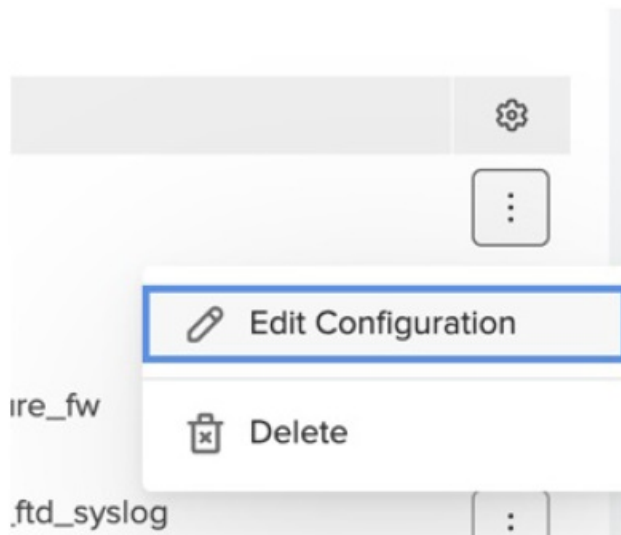
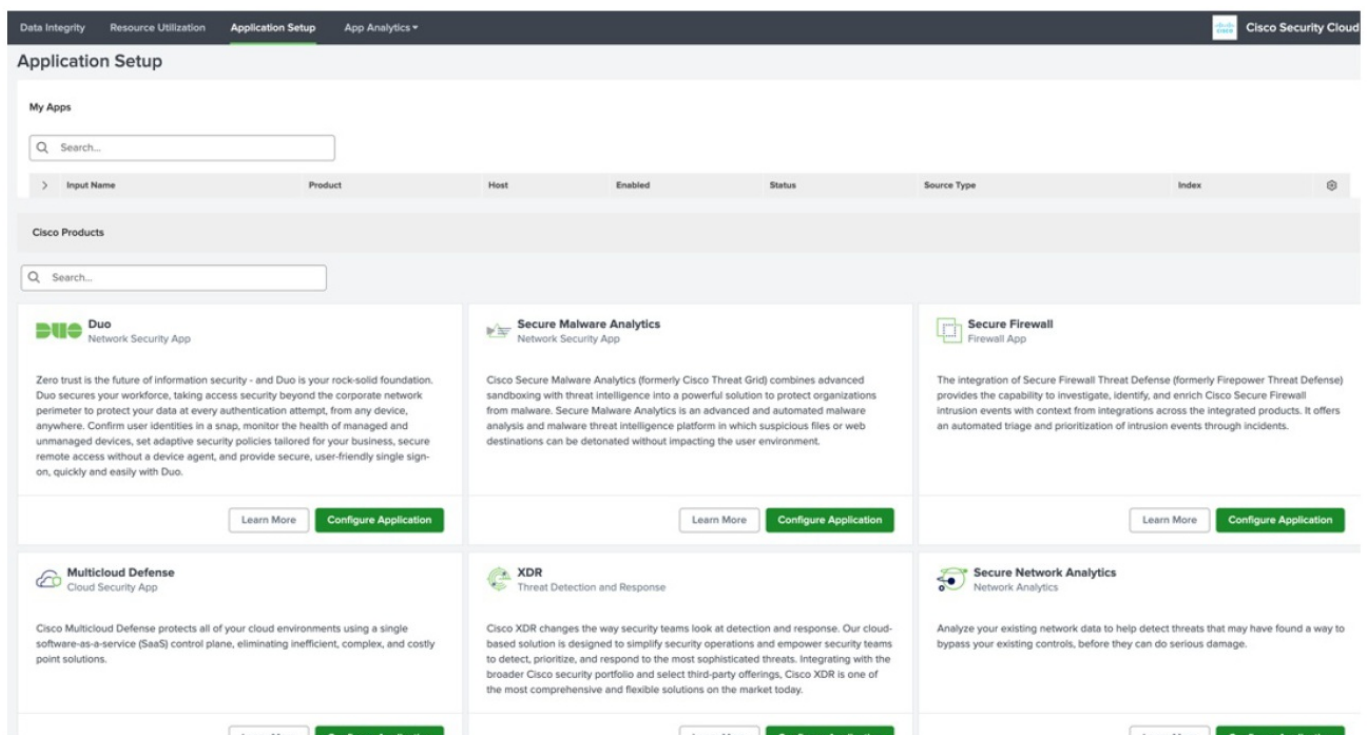


Figure 2: Cisco Products



- The Cisco Products page displays all available Cisco products that are integrated with Security Cloud App.
- You can configure inputs for each Cisco product in this section.

Configure an Application

- Some configuration fields are common across all Cisco products and they are described in this section.
- Configuration fields that are specific to a product are described in the later sections.

Table 1: Common fields

Field	Description
Input Name	(Mandatory) A unique name for inputs of the application.
Interval	(Mandatory) Time interval in seconds between API queries.
Index	(Mandatory) Destination index for application logs. It can be changed if required. Auto-complete is provided for this field.
Source Type	(Mandatory) For most apps, it is a default value and is disabled. You can change its value in Advance Settings .

- **Step 1** In the Application Setup > Cisco Products page, navigate to the required Cisco application.
- **Step 2** Click Configure Application.

The configuration page consists of three sections: Brief app description, Documentation with links to useful resources, and Configuration form.

The screenshot displays the 'Application Setup' page in the Cisco Security Cloud interface. The page is organized into sections: 'My Apps' with a search bar, and 'Cisco Products' which lists various security applications. Each application card provides a brief overview and links to 'Learn More' and 'Configure Application'.

- **Step 3** Fill in the configuration form. Note the following:
 - Required fields are marked with an asterisk *.
 - There are also optional fields.
 - Follow the instructions and tips described in the specific app section of the page.
- **Step 4** Click Save.

If there is an error or empty fields, the Save button is disabled. Correct the error and save the form.

Cisco Duo

Figure 3: Duo Configuration page

Duo

Duo Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

Documentation

- Duo Documentation
- Quick Sign Up
- Testimonials

Add Duo

Duo Security API

*Input Name
Enter a unique name

*Integration key
Enter the integration key for this account

*Secret key
Enter the Secret key for this account

*API hostname
Enter the API hostname for this account

> Duo Security Logs

> Additional Settings

Cancel Save

In addition to the mandatory fields described in the Configure an Application, on page 2 section, the following credentials are required for authorization with Duo API:

- ikey (Integration key)
- skkey (Secret key)

Authorization is handled by the Duo SDK for Python.

Table 2: Duo configuration fields

Field	Description
API Hostname	(Mandatory) All API methods use the API hostname. https://api-XXXXXXXXX.duosecurity.com . Obtain this value from the Duo Admin Panel and use it exactly as shown there.
Duo Security Logs	Optional.
Logging Level	(Optional) Logging level for messages written to input logs in \$SPLUNK_HOME/var/log/splunk/duo_splunkapp/

- **Step 1** In the Duo configuration page, enter the Input Name.
- **Step 2** Enter the Admin API credentials in the Integration key, Secret key, and the API hostname fields. If you do not have these credentials, [register a new account](#).
 - Navigate to Applications > Protect an Application > Admin API to create a new Admin API.

Admin API

Setup instructions are in the [Admin API documentation](#).

The Admin API allows you to programmatically create, retrieve, update, and delete users, phones, hardware tokens, admins, applications, and more.

Details

Integration key

DIP0iNABX90E0G2Y5C32

[Copy](#)

Secret key

*****u/ct

[Copy](#)

Don't write down your secret key or share it with anyone.

API hostname


api-17efc794.duosecurity.com

[Copy](#)

- **Step 3** Define the following if required:
 - Duo Security Logs
 - Logging Level
- **Step 4** Click Save.

Cisco Secure Malware Analytics

Figure 4: Secure Malware Analytics Configuration page


**Secure Malware Analytics**
Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

When integrated, Secure Malware Analytics is a reference module that provides licensed users the ability to pivot into the Secure Malware Analytics Cloud portal to gather additional intelligence about file hashes, IPs, domains, and URLs. It also provides a number of dashboard tiles for quick insight into current Secure Malware Analytics sample submission data.

Documentation

- [Free Trial](#)
- [Product Overview](#)
- [FAQ](#)
- [Support](#)
- [Privacy Policy](#)
- [Sign Up](#)

 Add Secure Malware Analytics

SMA Connection

*Input Name

Enter a unique name

*Host

Enter the Host for this account

*API Key

Enter the API Key for this account

> Proxy Settings

> Logging Settings

Input Configuration

*Interval

300

Time interval in seconds between API queries

Source Type

cisco/sma/submissions

*Index

sdg_sma

Specify the destination index for SMA Security Logs

*After

10 minutes ago

This initial after value used when querying the Threat Grid API. Should be 10 minutes ago

Cancel

Save

Note

You need an API key (api_key) for authorization with Secure Malware Analytics (SMA) API Pass the API key as the Bearer type in the Authorization token of the request.

Secure Malware Analytics configuration data

1. **Host:** (Mandatory) Specifies the name of the SMA account.
2. **Proxy Settings:** (Optional) Consists of Proxy Type, Proxy URL, Port, Username, and Password.
3. **Logging Settings:** (Optional) Define the settings for logging information.

- Step 1 In the Secure Malware Analytics configuration page, enter a name in the Input Name.
- Step 2 Enter the Host and the API Key fields.
- Step 3 Define the following if required:
 - Proxy Settings
 - Logging Settings
- Step 4 Click Save.

Cisco Secure Firewall Management Center

Figure 5: Secure Firewall Management Center Configuration page

The screenshot displays the 'Secure Firewall' management console. On the left, a sidebar contains a 'Secure Firewall' logo and a 'Documentation' section with links for 'Free Trial', 'FAQ', 'Support', and 'Sign up'. The main area is titled 'Add Secure Firewall' and features two tabs: 'E-Streamer' (selected) and 'Syslog'. The 'E-Streamer' tab contains a 'Firewall Connection' section with the following fields:

- * Input Name:** A text input field with a placeholder 'Enter a unique name'.
- * FMC Host:** A text input field with a placeholder 'Enter the FMC Host for this account'.
- Port:** A text input field containing '8302' with a placeholder 'Enter the Port for this account'.
- * PICS Certificate:** A section with a file upload button 'Drop your file here or upload file...' (supported types: png, jpg) and a password field 'Enter the password for the PICS certificate'.
- * Event Types:** A row of four buttons: 'Connection' (selected), 'File Events', 'Intrusion', and 'Intrusion Packet'.
- Source Type:** A dropdown menu showing 'cisco:other:streamer'.
- * Index:** A text input field containing 'cisco_secure_fw' with a placeholder 'Specify the destination index for Firewall Security logs'.
- * Interval:** A text input field containing '600' with a placeholder 'Time interval in seconds between API queries'.


At the bottom of the form are 'Cancel' and 'Save' buttons.

- You can import data into the Secure Firewall application using any one of the two streamlined processes: eStreamer and Syslog.
- The Secure Firewall configuration page provides two tabs, each corresponding to a different data import method. You can switch between these tabs to configure the respective data inputs.

Firewall e-Streamer

[eStreamer SDK](#) is used for communication with the Secure Firewall Management Center.

Figure 6: Secure Firewall E-Streamer tab


Add Secure Firewall

E-Streamer

Syslog

Firewall Connection

*Input Name


Enter a unique name

*FMC Host

Enter the FMC Host for this account

*Port

Enter the Port for this account

*PKCS Certificate 

Drop your file here or [upload file...](#)

Supported types: pkcs12.

*Password

Enter the password for the PKCS certificate


*Event Types

Connection

File Events

Intrusion

Intrusion Packet

Source Type 

*Index

Specify the destination index for Firewall Security Logs

*Interval

Time interval in seconds between API queries

Cancel

Save

Table 3: Secure Firewall configuration data

Field	Description
FMC Host	(Mandatory) Specifies the name of the management c enter host.
Port	(Mandatory) Specifies the port for the account.
PKCS Certificate	(Mandatory) The certificate must be created on the Fir ewall Management Console – eStreamer Certificate Creation . The system supports only the pkcs12 file ty pe.
Password	(Mandatory) Password for the PKCS Certificate.
Event Types	(Mandatory) Choose the type of events to ingest (All, Connection, Intrusion, File, Intrusion Packet).

- Step 1 In the E-Streamer tab of the Add Secure Firewall page, in the Input Name field, enter a name.

- Step 2 In the PKCS Certificate space, upload a .pkcs12 file to set up the PKCS certificate.
- Step 3 In the Password field, enter the password.
- Step 4 Choose an event under Event Types.
- Step 5 Define the following If required:
 - Duo Security Logs
 - Logging Level

Note

If you switch between the E-Streamer and Syslog tabs, only the active configuration tab is saved.
Therefore, you can only set one data import method at a time.

- Step 6 Click Save.

Firewall Syslog

In addition to the mandatory fields that are described in the Configure an Application, section, the following are the configurations that are required on the management center side.

Add Secure Firewall

E-Streamer

Syslog

Firewall Connection

*Input Name

Enter a unique name

*Input Type

UDP

TCP

*Port

514

Enter the Port for this account

*Source Type

Select...

*Index

cisco_sfw_ftd_syslog

Specify the destination index for Firewall Security Logs

*Interval

600

Time interval in seconds between API queries

Cancel

Save

Table 4: Secure Firewall Syslog configuration data

Field	Description
TCP/ UDP	(Mandatory) Specifies the type of input data.
Port	(Mandatory) Specifies a unique port for the account.

- Step 1 In the Syslog tab of the Add Secure Firewall page, set up the connection on the management center side, in the Input Name field, enter a name.

- Step 2 Choose TCP or UDP for the Input Type.
- Step 3 In the Port field, enter the port number
- Step 4 Select a type from the Source Type drop-down list.
- Step 5 Choose event types for the selected source type.

Note

If you switch between the E-Streamer and Syslog tabs, only the active configuration tab is saved. Therefore, you can only set one data import method at a time.

- Step 6 Click Save.

Cisco Multicloud Defense

Figure 7: Secure Malware Analytics Configuration page

Multicloud Defense

Multicloud Defense
Cloud Security App

Cisco Multicloud Defense protects all of your cloud environments using a single software-as-a-service (SaaS) control plane, eliminating inefficient, complex, and costly point solutions.

Set Up Guide

1. Go to **Data Inputs Console** in Splunk Settings
Settings → Data Inputs → HTTP Event Collector
2. Copy the Token Value for the collector with the name you specified during the input creation.
3. On the Multicloud Defense instance go to **Log Forwarding** tab
Manage → Profiles → Log Forwarding
4. Create a Log Forwarding Profile:
 - a. Click Create
 - b. Enter unique name for the profile
 - c. Choose **"Standalone"** from the Type dropdown.
 - d. Choose **"Splunk"** from the Destination dropdown.
5. Enter the link to the Http Event Collectors with port on your Splunk instance
e.g. https://your_splunk_host:5143/services/collector
6. Enter the token you copied in Data Inputs Console in the Token field.
7. Enter the index you specified in the created input in the Index field.

Documentation

[About Multicloud Defense](#)

Go to Cisco Defense Orchestrator and follow the steps in the Set Up Guide to the left to install Multicloud Defense instance.

[Go to CDO](#)

Add Cisco Multicloud Defense

Multicloud Defense Connection

*Input Name
Enter a unique name

*Interval
200
Time interval in seconds between API queries

*Source Type
cisco-multicloud-defense

*Index
cisco_multicloud_defense
Specify the destination index for MCD Security Logs

*Port
8088
Enter the Port for this account

Cancel Save

- Multicloud Defense (MCD) leverages the HTTP Event Collector functionality of Splunk instead of communicating through an API.
- Create an instance in Cisco Defense Orchestrator (CDO), by following the steps that are defined in the Set Up Guide section of the Multicloud Defense configuration page.

Set Up Guide

1. Go to **Data Inputs Console** in Splunk Settings
Settings -> Data Inputs -> HTTP Event Collector
2. Copy the Token Value for the collector with the name you specified during the input creation.
3. On the Multicloud Defense instance go to **Log Forwarding** tab
Manage -> Profiles -> Log Forwarding
4. Create a Log Forwarding Profile:
 - a. Click Create
 - b. Enter unique name for the profile
 - c. Choose **"Standalone"** from the Type dropdown.
 - d. Choose **"Splunk"** from the Destination dropdown.
5. Enter the link to the **Http Event Collectors** with port on your Splunk instance
e.g. `https://<your_splunk_host>:<hec_port>/services/collector`
6. Enter the token you copied in Data Inputs Console in the Token field.
7. Enter the index you specified in the created input in the Index field.

Only the mandatory fields defined in the Configure an Application, section are required for authorization with Multicloud Defense.

- Step 1 Install a Multicloud Defense instance in CDO by following the Set Up Guide on the configuration page.
- Step 2 Enter a name in the Input Name field.
- Step 3 Click Save.

Cisco XDR

Figure 8: XDR Configuration page

Cisco XDR

XDR
Threat Detection and Response

Cisco XDR changes the way security teams look at detection and response. Our cloud-based solution is designed to simplify security operations and empower security teams to detect, prioritize, and respond to the most sophisticated threats. Integrating with the broader Cisco security portfolio and select third-party offerings, Cisco XDR is one of the most comprehensive and flexible solutions on the market today.

Designed by security practitioners for security practitioners, Cisco XDR helps analysts aggregate and correlate data from multiple sources into a unified view to streamline investigations, reduce false positives, prioritize alerts, and achieve the shortest path from detection to response. Built-in automation, orchestration, and guided remediation recommendations help analysts automate repetitive tasks and mitigate threats more effectively, freeing up time and resources to focus on other critical security tasks.

The data-driven Cisco XDR approach allows SOC teams to define the most impactful events and focus remediation strategies there first, strengthening the organization's overall security posture and increasing resilience.

Documentation

- [About XDR](#)
- [Data Sheet](#)
- [Privacy Policy](#)
- [Get started](#)

Add XDR

XDR Connection

*Input Name
Enter a unique name

*Region
Select...
Enter the Region for this account

*Authentication Method ⓘ
Select...

*Import Time Range ⓘ
Select...

Promote XDR Incidents to ES Notables? ⓘ
All Critical Medium Low Info Unknown None

*Interval
300
Time interval in seconds between API queries

Source Type ⓘ
cisco:xdr:incidents

*Index
cisco_xdr
Specify the destination index for XDR Security Logs

Cancel Save

The following credentials are required for authorization with Private Intel API:

- client_id
- client_secret

Every input run results in a call to the GET /iroh/oauth2/token endpoint to obtain a token that is valid for 600 seconds.

Table 5: Cisco XDR configuration data


Field	Description
Region	(Mandatory) Select a region before selecting an Authentication Method.
Authentication Method	(Mandatory) Two authentication methods are available: Using Client ID and OAuth.
Import Time Range	(Mandatory) Three import options are available: Import All Incident data, Import from the created date-time, and Import from the defined date-time.
Promote XDR Incidents to ES Notables?	<p>(Optional) Splunk Enterprise Security (ES) promotes Notables.</p> <p>If you have not enabled Enterprise Security, you can still choose to promote to notables, but events do not appear in that index or notable macros.</p> <p>After you enable Enterprise Security, events are present in the index.</p> <p>You can choose the type of incidents to ingest (All, Critical, Medium, Low, Info, Unknown, None).</p>

- Step 1 In the Cisco XDR configuration page, enter a name in the Input Name field.
- Step 2 Select a method from the Authentication Method drop-down list.
 - **Client ID:**
 - Click the Go to XDR button to create a client for your account in XDR.
 - Copy and paste the Client ID
 - Set a password (Client_secret)
 - **OAuth:**
 - Follow the generated link and authenticate. You need to have an XDR account.
 - If the first link with the code didn't work, in the second link, copy the User code and paste it manually.
- Step 3 Define an import time in the Import Time Range field.
- Step 4 If required, select a value in the Promote XDR Incidents to ES Notables. field.
- Step 5 Click Save.

Cisco Secure Email Threat Defense

Figure 9: Secure Email Threat Defense Configuration page

Cisco Secure Email Threat Defense



Cisco Secure Email Threat Defense
Email Security

Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and costly threats that compromise your organization's brand and operations.

AI-driven threat detection uses multiple detection engines to simultaneously evaluate different portions of an incoming email. These verdict details help ensure accurate threat classification, identify business risk, and promote an appropriate response action.

Using rapid message remediation directly in Email Threat Defense or through Cisco XDR empowers your team to act quickly and easily to help ensure maximum threat protection.

Identify the malicious techniques used in attacks targeting your organization. Understand the specific business risks and categorize threats to gain insight into the parts of your organization that are most vulnerable to attack.

Documentation

[At-A-Glance](#)

[Q+A](#)

[Data Sheet](#)

Add Cisco Secure Email Threat Defense

ETD Connection

*Input Name
Enter a unique name

*API Key
Enter the API Key for this account

*Client ID
Enter the Client ID for this account

*Secret Key
Enter the Secret Key for this account

*Region
Select...
Enter the Region for this account

*Import Time Range ⓘ
Select...

Input Configuration

*Interval
300
Time interval in seconds between API queries

Source Type ⓘ
cisco-std

*Index
cisco_std
Specify the destination index for ETD Security Logs

Cancel

Save

The following credentials are required for authorization of Secure Email Threat Defense APIs:

- api_key
- client_id
- client_secret

Table 6: Secure Email Threat Defense Configuration data


Field	Description
Region	(Mandatory) You can edit this field to change the region.
Import Time Range	(Mandatory) Three options are available: Import All message data, Import from the created date-time, or Import from the defined date-time.

- Step 1 In the Secure Email Threat Defense configuration page, enter a name in the Input Name field.
- Step 2 Enter the API Key, Client ID, and Client Secret Key.
- Step 3 Select a region from the Region drop-down list.
- Step 4 Set an import time under Import Time Range.
- Step 5 Click Save.

Cisco Secure Network Analytics

Secure Network Analytics (SNA), formerly known as Stealthwatch, analyzes the existing network data to help identify threats that may have found a way to bypass the existing controls.

Figure 10: Secure Network Analytics Configuration page



Secure Network Analytics

Network Analytics

Analyze your existing network data to help detect threats that may have found a way to bypass your existing controls, before they can do serious damage.

Detect attacks in real time across the dynamic network with high-fidelity alerts enriched with context, including user, device, location, timestamp, and application.

Validate the efficacy of policies, adopt the right ones based on your environment's needs, and streamline policy violation investigations.

Use advanced analytics to quickly detect unknown malware, insider threats like data exfiltration and policy violations, and other sophisticated attacks.

Identify and isolate threats in encrypted traffic without compromising privacy and data integrity.


Documentation

Free Trial

FAQ

Support

Sign Up



Add Secure Network Analytics

SNA Connection

*Input Name

Enter a unique name

*SMC Address (IP Address or Hostname)

*SMC Domain ID

*SMC Username

*SMC Password


> Proxy Settings

> Logging Settings

Input Configuration

*Interval

Time interval in seconds between API queries

Source Type 

*Index

Specify the destination index for SMA Security Logs

Cancel

Save

Credentials required for authorization:


- smc_host: (IP address or hostname of the Stealthwatch Management Console)
- tenant_id (Stealthwatch Management Console domain ID for this account)
- username (Stealthwatch Management Console username)
- password (Stealthwatch Management Console password for this account)

Table 7: Secure Network Analytics Configuration data

Field	Description
Proxy type	choose a value from the drop-down list: <ul style="list-style-type: none"> • Host • Port • Username • Password
Interval	(Mandatory) Time interval in seconds between API queries. By default, 300 secs.
Source type	(Mandatory)
Index	(Mandatory) Specifies the destination index for SNA Security Logs. By default, state: cisco_sna.
After	(Mandatory) The initial after value is used when querying the Stealthwatch API. By default, the value is 10 minutes ago.

- Step 1 In the Secure Network Analytics configuration page, enter a name in the Input Name field.
- Step 2 Enter the Manager Address (IP or Host), Domain ID, Username, and Password.
- Step 3 If required, set the following under Proxy settings:
 - Choose a proxy from the Proxy type drop-down list.
 - Enter the host, port, username, and password in the respective fields.
- Step 4 Define the Input configurations:
 - Set a time under Interval. By default, the interval is set to 300 seconds (5 minutes).
 - You can change the Source type under Advanced Settings if required. The default value is cisco:sna.
 - Enter the destination index for the Security logs in the Index field.
- Step 5 Click Save.

Documents / Resources

	CISCO Security Cloud App [pdf] User Guide Security Cloud App, Cloud App, App
---	---

References

- [User Manual](#)