Configure Cisco Products in Cisco Security Cloud App

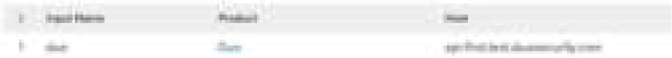
This chapter guides you through the process of adding and configuring inputs for various applications (Cisco products) within Security Cloud App. Inputs are crucial because they define the data sources that Security Cloud App uses for monitoring purposes. Proper configuration of inputs ensures that your 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 Security Cloud App. The **Application Setup** page consists of two sections:

Figure 1: My Apps

- 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
1	duo	Duo	[illegible]

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

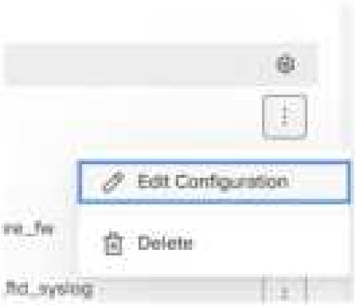
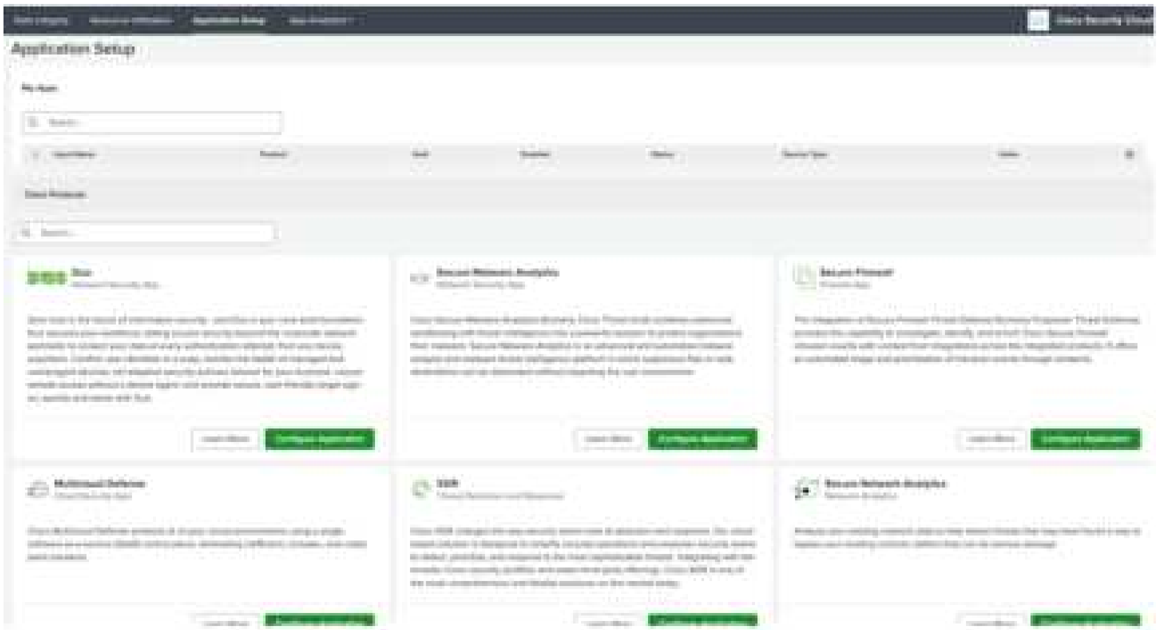


Figure 2: Cisco Products



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.

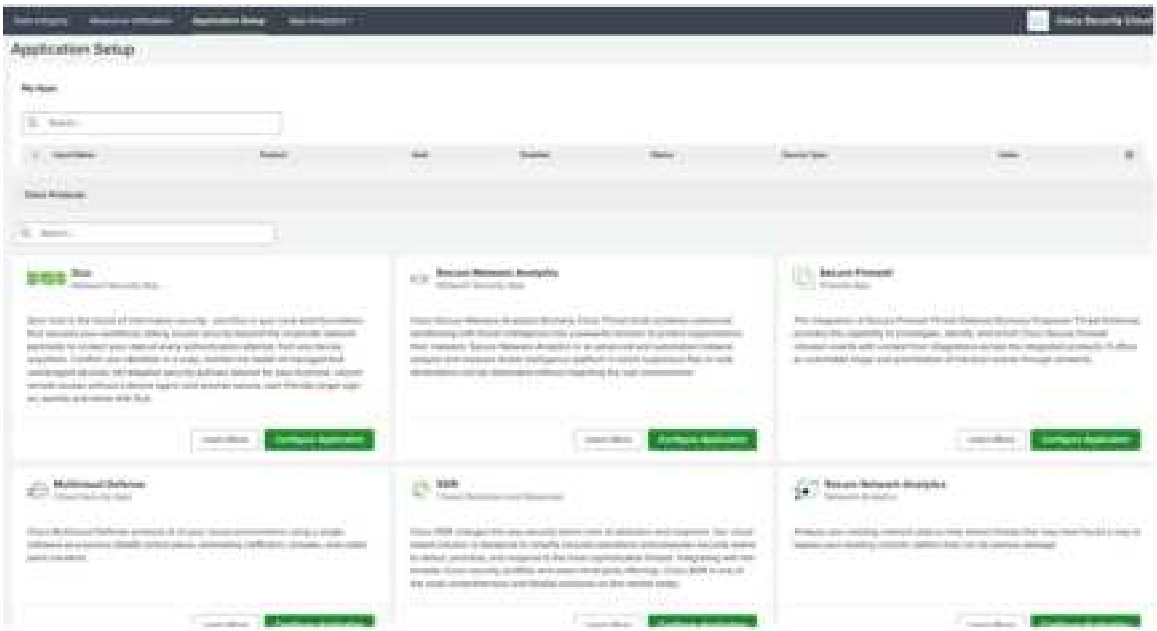
Table 1: Common fields

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.



Step 3 Fill in the configuration form. Note the following:

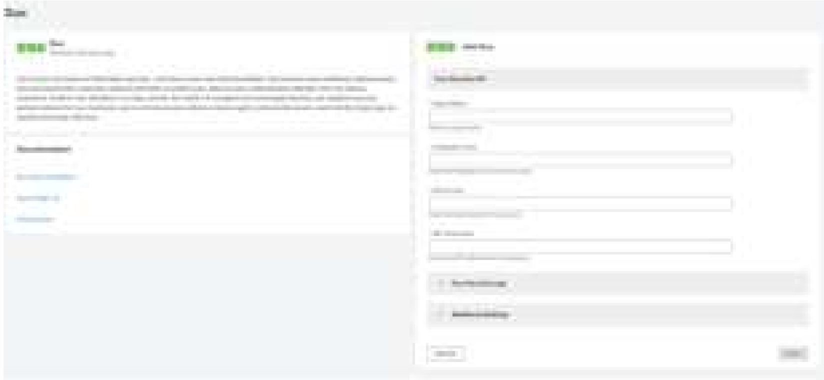
- Required fields are marked with asterisk *.
- There are also optional fields.
- Follow the instructions and tips described in the specific app section of the page.

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



In addition of 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)**
- **skey (Secret key)**

Authorization is handled by the Duo SDK for Python.

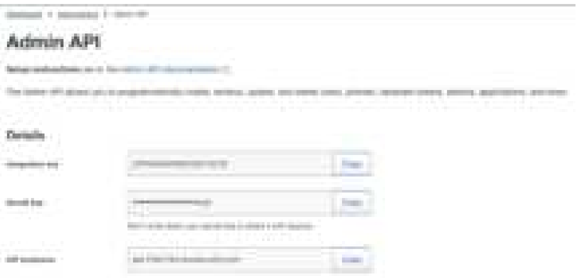
Table 2: Duo configuration fields

Field	Description
API Hostname	(Mandatory) All API methods use the API hostname. https://api-XXXXXXXX.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 new Admin API.



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

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

- **Host**: (Mandatory) Specifies the name of the SMA account.
- **Proxy Settings**: (Optional) Consists of Proxy Type, Proxy URL, Port, Username, and Password.
- **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.

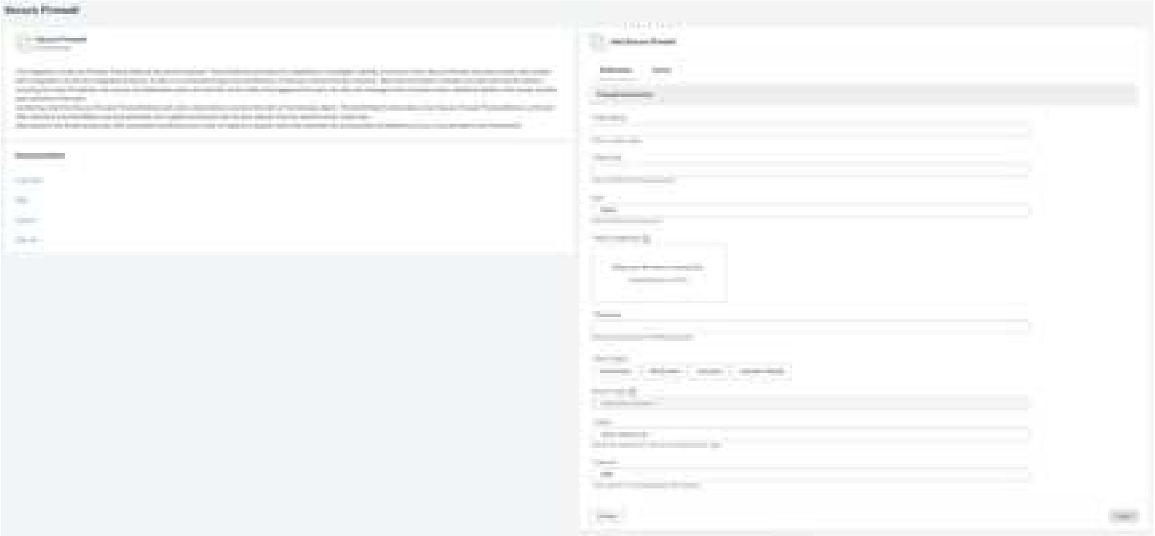
Step 3 Define the following, if required:

- Proxy Settings
- Logging Settings

Step 4 Click **Save**.

Cisco Secure Firewall Management Center

Figure 5: Secure Firewall Management Center Configuration page



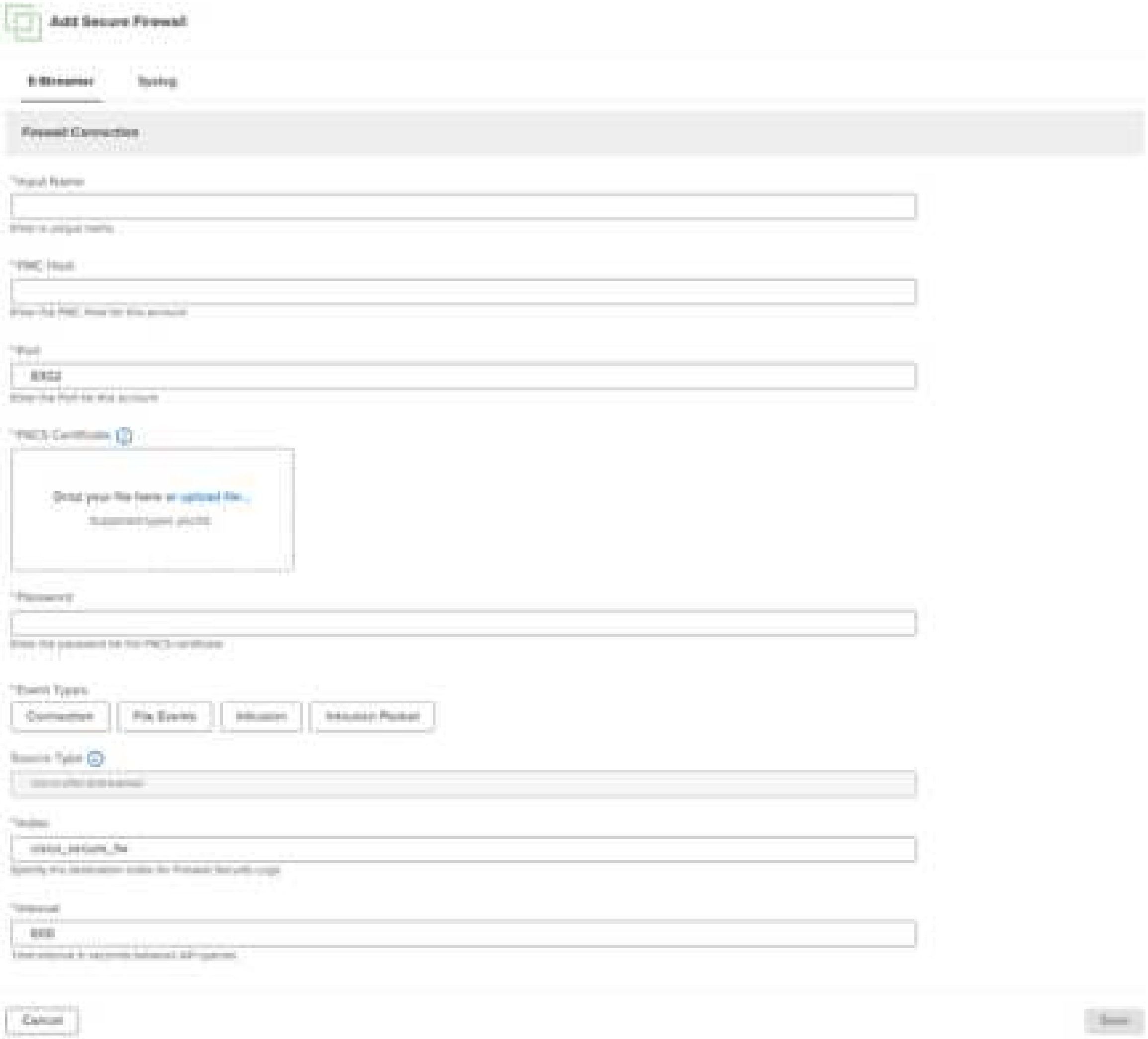
You can import data into the Secure Firewall application using any one of the two streamlined processes: **eStreamer** and **Syslog**.

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 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

8302

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

cisco:sfw:estreamer

*Index

cisco_secure_fw

Specify the destination index for Firewall Security Logs

*Interval

600

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 center host.
Port	(Mandatory) Specifies the port for the account.
PKCS Certificate	(Mandatory) Certificate must be created on the Firewall Management Console - eStreamer Certificate Creation. The system supports only pkcs12 file type.
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:

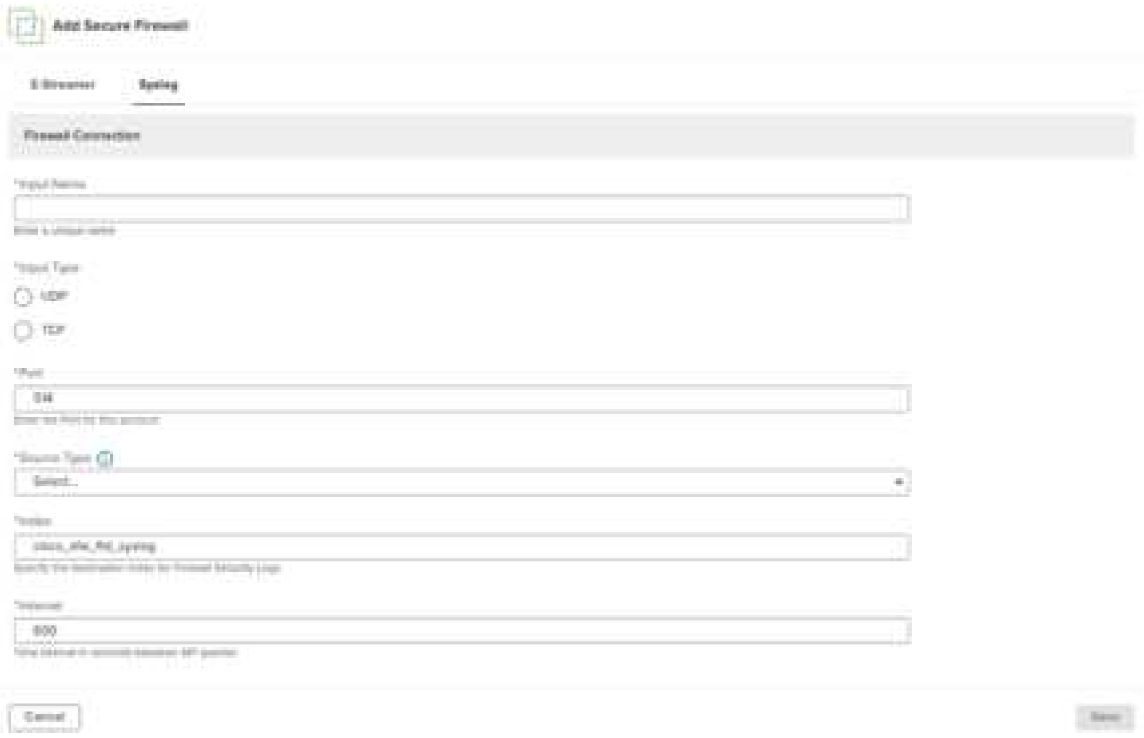
- Duo Security Logs
- Logging Level

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, on page 2 section, the following are the configurations that are required on the management center side.



*Input Name

Enter a unique name

*Input Type

○ UDP

○ TCP

*Port

514

Enter the Port for this protocol

*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

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.

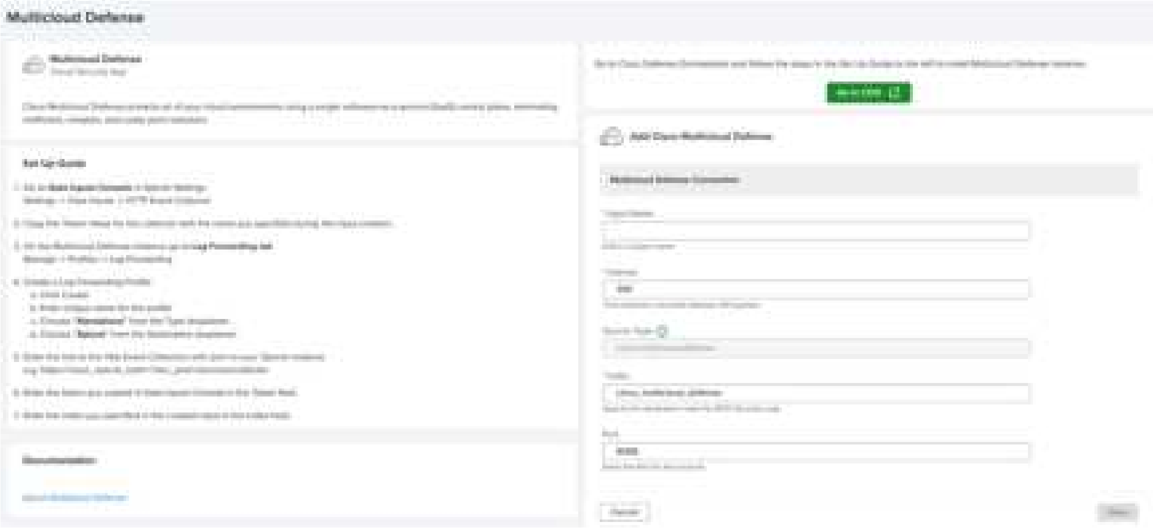
Step 5 Choose event types for the selected source type.

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**.

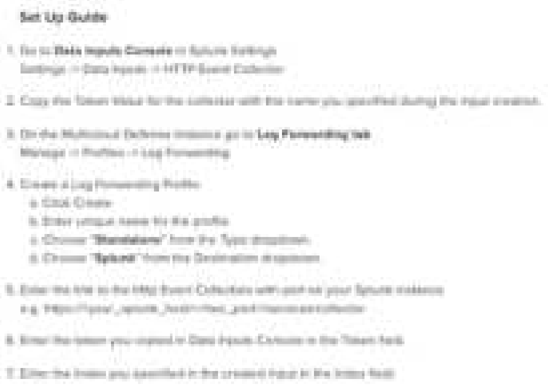
Cisco Multicloud Defense

Figure 7: Secure Malware Analytics Configuration page



Multicloud Defense (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** => 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 as 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, on page 2 section are required for authorization with Multicloud Defense.

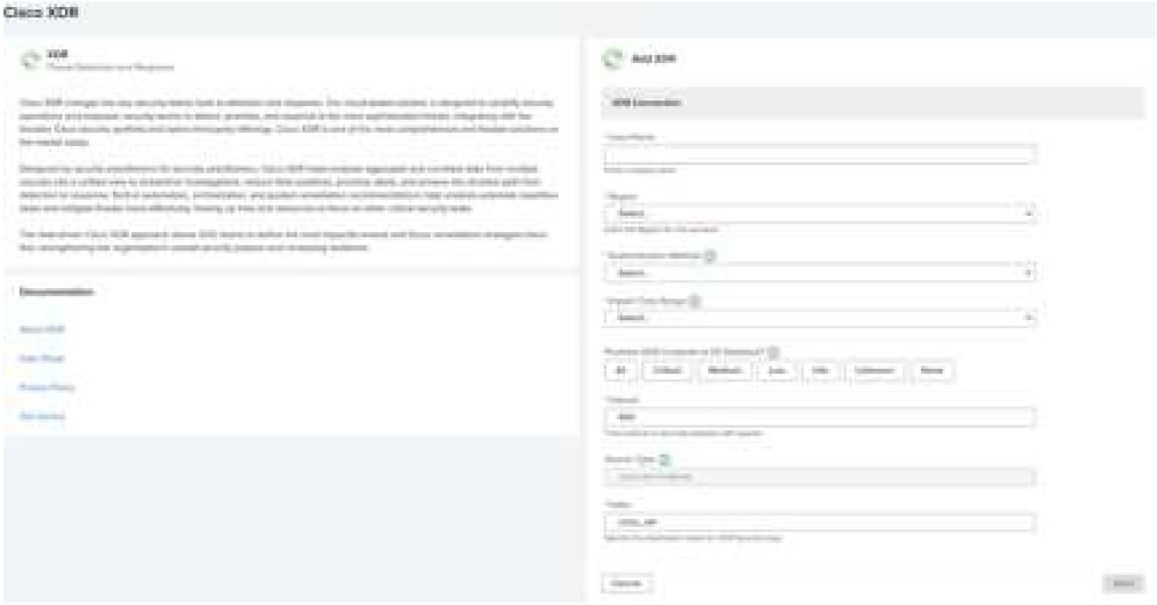
Step 1 Install a Multicloud Defense instance in CDO by following the **Set Up Guide** on the configuration page.

Step 2 Enter a name in the **Input Name** field.

Step 3 Click **Save**.

Cisco XDR

Figure 8: XDR Configuration page



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

- **client_id**

- **client_secret**

Every input run results in a call to 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 created date-time, and Import from defined date-time.
Promote XDR Incidents to ES Notables?	(Optional) Splunk Enterprise Security (ES) promotes Notables. 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. After you enable Enterprise Security, events are present in the index. You can choose the type of incidents to ingest (All, Critical, Medium, Low, Info, Unknown, None).

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:

  a. Click the **Go to XDR** button to create a client for your account in XDR.

  b. Copy and paste the Client ID

  c. Set a password (Client_secret)

- OAuth:

  a. Follow the generated link and authenticate. You need to have an XDR account.

  b. If the first link with the code didn’t work, in the second link, copy the User code and paste it manually.

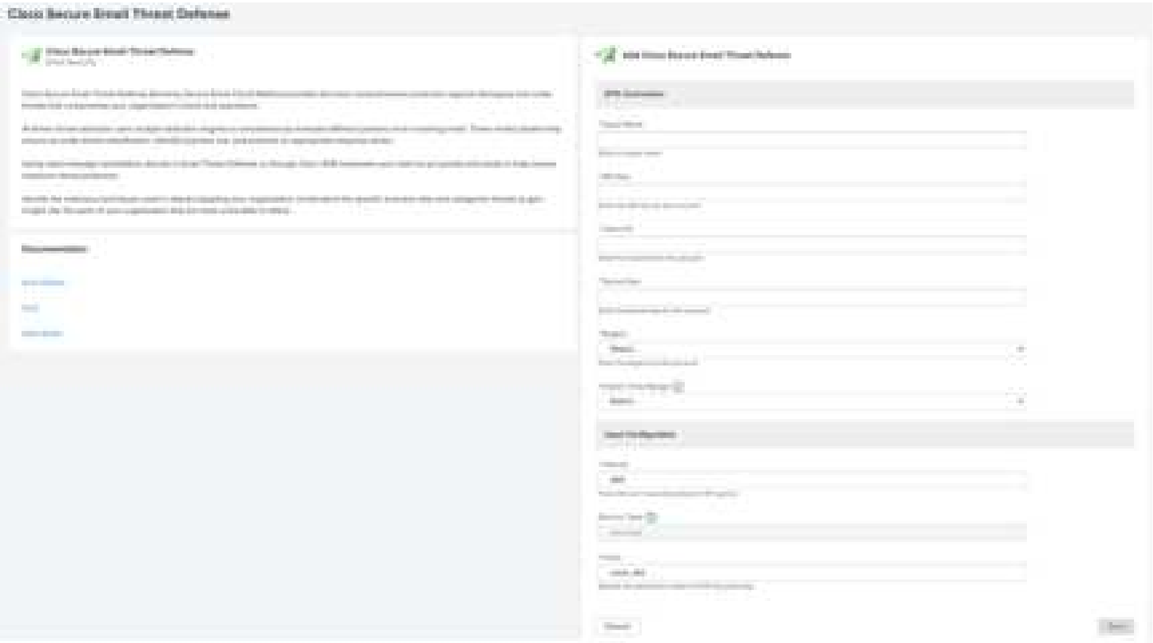
Step 3 Define an import time in the **Import Time Range** field.

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

The following credentials 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 created date-time, Import from 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**, **Client Secret Key**.

Step 3 Select a region from the **Region** drop-down list.

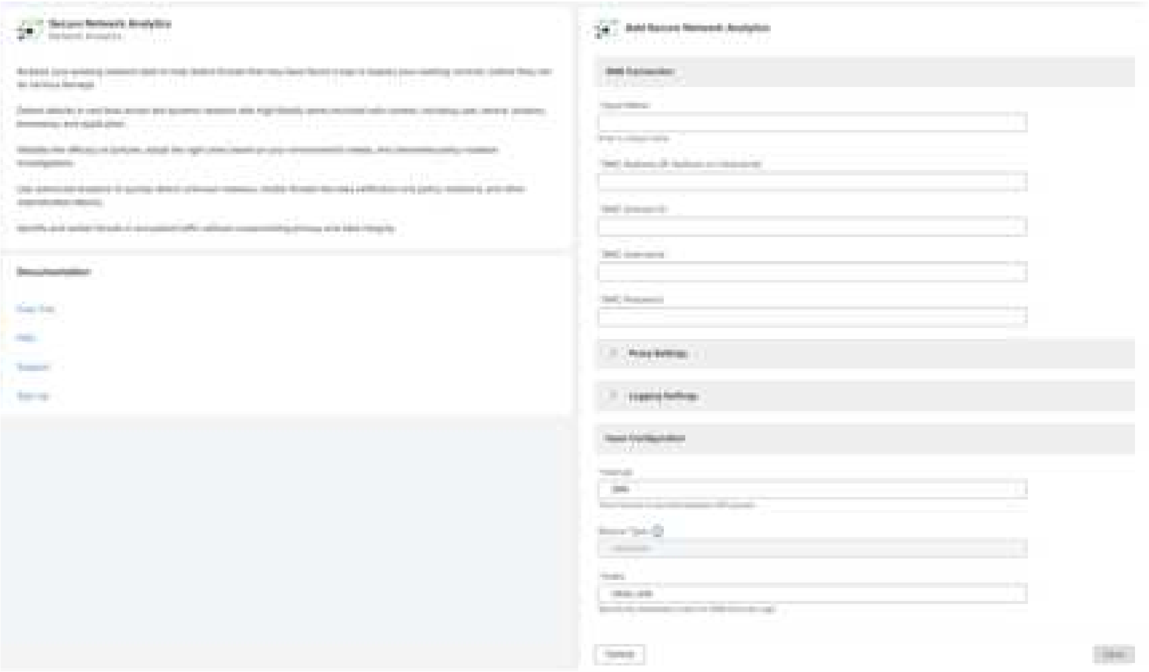
Step 4 Set an import time under **Import Time Range**.

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



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: • 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 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 **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. Default value is *cisco:sna*.
- Enter the destination index for the Security logs in the **Index** field.

Step 5 Click **Save**.