

Send Firewall Threat Defense Events to Cisco Splunk

- Splunk integration: Send events directly from Cloud-Delivered Firewall Management Center , on page 1
- Guidelines and limitations for Splunk integration, on page 1
- Configure Splunk in Cloud-Delivered Firewall Management Center , on page 2
- Configure Secure Firewall App in Splunk, on page 7

Splunk integration: Send events directly from Cloud-Delivered Firewall Management Center

Cisco Splunk is a Security Information and Event Management (SIEM) tool that provides visibility and monitoring of security events across Cisco Secure Firewall devices.

In Cloud-Delivered Firewall Management Center versions earlier to 10.0, security events were sent to Splunk using eStreamer. From Cloud-Delivered Firewall Management Center version 10.0, you can send events to Splunk from the Firewall Threat Defense device. The wizard-driven interface helps you set up Splunk integration effortlessly.

This integration allows you to perform these actions.

- Customize event flow by specifying event types—such as connection, intrusion, malware, file, user activity, correlation, discovery, intrusion packet—and their sources (Firewall Threat Defense device) according to your monitoring requirements.
- Select the source interface for sending syslog events. You can choose to send events from the Firewall Threat Defense device's management or data interfaces.
- Create profiles with various configurations to suit different monitoring requirements.

Guidelines and limitations for Splunk integration

This topic lists the guidelines and limitations that apply to Splunk integration for event forwarding and syslog processing.

- When you enable Splunk integration, your existing syslog server configuration is not migrated.
- When migrating to Cloud-Delivered Firewall Management Center, you must repeat the Splunk integration procedure because the Splunk configuration from the On-Prem Firewall Management Center does not get migrated.
- If you set up domains in Cloud-Delivered Firewall Management Center, you can configure Splunk only from leaf domains.
- You can create a maximum of 15 Splunk profiles per domain. However, multiple domains can be configured to send syslog messages to the same or different servers.
- Do not create duplicate profiles for the same devices because it results in devices sending duplicated events to the Splunk server.
- Events are duplicated in Splunk destinations, under any of the following scenarios:
  - Platform Settings are configured with at least one syslog configuration.
  - Splunk profile is enabled using at least one data interface option for events.
- Only basic TLS encryption is supported over data interfaces from devices; client and server authentication are not supported.
- The syslog payload is sent to the Splunk server in JSON format.
- In a high availability set up, Splunk configuration is synchronized between the Cloud-Delivered Firewall Management Center HA pair. Only active unit sends the events. In the case of a failover, the new active unit will start sending the events.
- The message header of syslog events sent through data interfaces contains only the syslog tag and not the device IP address.
- cdFMC does not support sending events from a Cloud-Delivered Firewall Management Center source. Hence, cdFMC cannot have events that support only Cloud-Delivered Firewall Management Center source.

Configure Splunk in Cloud-Delivered Firewall Management Center

The Splunk integration wizard in Secure Firewall Management Center allows you to create profiles that send events and syslog data to a designated server. You can create multiple profiles to configure any number of servers for different combinations of devices and event types.

Before you begin

- Ensure that the Splunk server can be reached by Firewall Threat Defense device.
- The Cisco Secure Firewall App in Splunk does not support TLS. Hence, if you choose to use the TLS protocol to send events to Splunk, configure TLS on the Splunk server. For TLS configuration instructions, refer to the section *Configure Splunk indexing and forwarding to use TLS certificates* under *Manage Users and Security* in the Splunk Administer guide.

- Create required objects such as host, security zone, interface group, certificate, and so on, before starting the configuration procedure. Although you can navigate from the **Splunk integration** wizard to create objects, having them in advance will provide a smoother integration experience.

The Splunk integration wizard allows you to create a profile that enables you to stream events and syslog from managed devices to a specific server.

You can create multiple profiles to configure any number of servers for various combinations of devices and events. For example, you can create multiple profiles to send a specific set of events to one server and all the remaining events to a different server. Each profile is independent, but they all apply additively.

Procedure

	Command or Action	Purpose
Step 1	To open the **Splunk integration** wizard, go to **Integrations** > **Splunk**.	
Step 2	The steps for configuring Splunk integration in Cloud-Delivered Firewall Management Center are listed in this table.	

	Do This	More Information
Step 1	Configure Splunk or similar SIEM tool server.	Refer to Configure Splunk server, on page 4.
Step 2	Choose the event types that you want to send to the Splunk server.	Refer to Select event types, on page 4.
Step 3	Specify the devices and the interfaces from which you want to send syslog events to Splunk.	Refer to Select devices and interfaces, on page 5.
Step 4	(Optional) Specify the device certificate to be used for sending events securely to Splunk.	Refer to Configure Firewall certificates for TLS, on page 6.
Step 5	View the summary of the profile that is being created.	Refer to Review and submit the Splunk profile, on page 6.

Configure Splunk server

Set up a Splunk syslog server to efficiently collect and manage log events from Secure Firewall devices. Use this task when adding a Splunk server as an external syslog destination for your Secure Firewall deployment.

Procedure

Step 1 In the **Configure Splunk server** page, from the **Host object or IP address** drop-down, choose the host object or enter an IP address of the Splunk server. To create a host object, click the **Create** link in the drop-down list.

Step 2 Click the **Protocol** (UDP, TCP, or TLS) that you want the Splunk server to use for communicating with Cloud-Delivered Firewall Management Center and Firewall Threat Defense device.

Step 3 In the **Port** field, enter the port number applicable for the selected protocol:

- UDP: Enter the port number 514, or a number between 1025 and 65535. The default UDP port is 514.
- TCP: Enter the port number between 1025 and 65535. The default TCP port is 1470.
- TLS: Enter the port number between 1 and 65535. The default TLS port is 6514.

Step 4 (Optional) If you selected **TLS**, specify the trusted CA name to securely establish the connection on the Splunk server. From the **Trusted certificate authority** drop-down list, choose the CA. (To import a new CA object, click the **Create** link in the drop-down list.)

Step 5 To forward the events logged by a facility, from the **Facility** drop-down list, choose the corresponding facility.

Step 6 To forward the events with a specific severity, from the **Severity** drop-down list, choose the severity level.

Step 7 (Optional) In the **Tag** field, enter an alphanumeric string by which to identify the message in the server.

Step 8 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 9 To move to the next step in the Splunk configuration, click **Next**.

Select event types

You can specify the type of events that you want to send to Splunk. The recommended event types are selected by default. In Cloud-Delivered Firewall Management Center , the source for event types is always **FTD**.

Procedure

Step 1 Select the check box to specify the event types.

Step 2 After selection of the event types, to reset to default settings, click **Revert to system defaults**.

Step 3 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 4 (Optional) To go back to the previous step, click **Back**.

Step 5 To move to the next step in the Splunk configuration, click **Next**.

Select devices and interfaces

You can specify the Firewall Threat Defense devices and interfaces from which you want to send syslog events to Splunk. To send events from multiple interfaces, use security zones or interface groups.

Note If you are using security zones or interface groups, only routed, management, switched, and loopback zones and groups are allowed.

Procedure

Step 1 Under **Select devices**, click the relevant options:

- **Use management interface** : Click this button to configure the management interface of Firewall Threat Defense device to send the events to Splunk. When this option is chosen, all the devices in the current domain also receive the Splunk configuration.
- **Use security zones and interface groups to specify devices and interfaces** : Click this button to configure the interfaces of corresponding devices in the selected security zones and interface groups to send their respective events to Splunk.
  - From the **Security zones and interface groups** drop-down list, choose the required zones and groups.
  - To create a security zone or interface group for the device's interfaces, click **Create** in the **Certificates** drop-down list.
- **Manually select devices and interfaces** : Click this button to send the events from the deployed device to Splunk. From the **Interface** drop-down list, choose the configured interface through which you want the events to be sent to Splunk. You can choose only security zones that include this device.

Note
- Virtual Tunnel Interface (VTI) and Dynamic Virtual Tunnel Interface (DVTI) are excluded from Splunk configuration.
- To encrypt syslog events over TLS, use the management interface to add a certificate. Encryption is not supported for data interfaces configured for TLS.

  - Click the **Send events from this device** toggle button corresponding to the device and its selected interface.
  - To create a security zone or interface group for the device's interfaces, click **Create**.

Step 2 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 3 (Optional) To go back to the previous step, click **Back**.

Step 4 To move to the next step in the Splunk configuration, click **Next**.

Configure Firewall certificates for TLS

You can specify the device certificate to be used for sending events securely to Splunk. This step is optional. It is applicable only if you use the TLS protocol to send events to Splunk.

Before you begin

You can configure the certificates when you have set TLS protocol while configuring the Splunk server. Add certificate object for these clients:

- For Cloud-Delivered Firewall Management Center, use internal certificate objects for authentication.
- For Firewall Threat Defense, use a certificate enrollment object. First, create the object at **Objects** > **PKI** > **Certificate Enrollment**. Then, enroll the certificate on a device at **Devices** > **Certificates**.

Procedure

Step 1 From the **Firewall Management Center client certificate** drop-down list, choose the certificate. To create an internal certificate, click **Create**.

Step 2 In the **Firewall Threat Defense certificates** box, use the search box to choose the device whose certificate you want to assign.

Step 3 From the **Certificates** drop-down list, choose the certificate. Only successfully enrolled device certificates are listed. To enroll a new device certificate, click **Create**.

Step 4 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 5 (Optional) To go back to the previous step, click **Back**.

Step 6 To move to the next step in the Splunk configuration, click **Next**.

Review and submit the Splunk profile

You can view the selections made for the Splunk configuration profile.

Procedure

Step 1 Under **Profile Name**, a system-generated name is displayed. Edit the value in the **Name** field, if you want to use a different name.



Note The name must start with a letter, a number, or an underscore (_). The name can contain include letters, numbers, and special characters: period (.), hyphen (-), underscore (_), and plus (+).

Step 2 To change a value from a previous Splunk server configuration, click **Edit** next to the attribute.

Step 3 (Optional) To cancel the creation of the Splunk profile, click **Cancel**.

Step 4 (Optional) To go back to the previous step, click **Back**.

Step 5 To save the Splunk profile, click **Submit**.

Step 6 If you have configured Threat Defense events to be sent to Splunk, click **Deploy**.

Configure Secure Firewall App in Splunk

To ensure that the Splunk server is reachable to receive the events, configure the Cisco Secure Firewall App in Splunk.

Before you begin

Ensure that you have obtained a Splunk server license and a Cisco Security Cloud account.

Procedure

Step 1 Download and install the Splunk server using the instructions provided in Splunk Enterprise Installation Manual.

Step 2 To install Splunk license, log in to your Splunk server's web interface.

Step 3 Go to **Settings** > **Licensing** > **Add license**. Use the license received by email.



Note Make sure to restart Splunk to complete license registration.

Step 4 Download Cisco Security Cloud from Splunkbase Apps.

Step 5 To install Cisco Security Cloud, log in to your Splunk server's web interface.

Step 6 Go to **Apps** > **Manage Apps** > **Install app from file**.

Step 7 Click **Browse** and select the downloaded application file and upload.

Step 8 To configure the server to receive the syslog events from the Firewall Threat Defense device, go to **Apps** > **Cisco Security Cloud** > **Secure Firewall** > **Configure Application**, and then click the **Syslog** tab.

- In the **Input Name** field, enter any name.
- In the **Input Type** field, enter UDP or TCP.

  TLS is not supported in the Cisco Security Cloud application. Use rsyslog or syslog-ng to establish TLS on Splunk server. For detailed procedures, refer to Configure TLS on Splunk Server.
- In the **Port** field, enter a value between 1025 and 65535. The default port is 514.
- Leave the **Host** field blank. This will allow the Splunk to process events from any Firewall Threat Defense.
- In the **Source Type** field, enter *cisco:ftd:syslog*.

- In the **Interval** field, enter *600* seconds.