Send Events Directly to Cisco Splunk

Splunk Integration: Send Events Directly from 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 Firewall Management Center versions earlier to 10.0, security events were sent to Splunk using eStreamer. From Firewall Management Center version 10.0, you can send events directly to the Splunk server using the Firewall Management Center web interface. 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 Management Center or 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 Management Center's management interface or Firewall Threat Defense device's management or data interfaces.
- Create profiles with various configurations to suit different monitoring requirements.

Note While the integration procedure described in this topic is for Splunk, you can use the Splunk Integration wizard to integrate any SIEM tool with Firewall Management Center to send syslog messages to an external syslog server.

Guidelines and Limitations for Splunk Integration

- 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-Premises Management Center does not get migrated.
- You cannot configure a Splunk profile to send events from both Firewall Management Center and Firewall Threat Defense device for the same event type.
- If you set up domains in 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.
- 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 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.
- Splunk integration does not support analytics devices managed by another Firewall Management Center, for example, cdFMC.
- cdFMC does not support sending events from a Firewall Management Center source. Hence, cdFMC cannot have events that support only Firewall Management Center source.

Configure Splunk in Secure Firewall Management Center

Before you begin:

- Ensure that the Splunk server can be reached by both Firewall Management Center and Firewall Threat Defense device.
- Configure the Cisco Secure Firewall App in Splunk. You need a valid Splunk server license and Cisco Secure Cloud account. For configuration information, see Configure Secure Firewall App in Splunk, on page 7.
- 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, see 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.
- Connection events from Firewall Management Center or Firewall Threat Defense device will be sent to the configured Splunk server or SIEM syslog server only when the logging destination is appropriately selected in the Access Control policy rules page. For more information, see Creating and Edit Access Control Rules.

The Splunk integration wizard allows you to create a profile that enables you to stream events and syslog from the Firewall Management Center and its 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 events from Firewall Threat Defense devices to one server, while directing events from the Firewall Management Center to another. Another scenario where multiple profiles can be created is when you have 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.

To open the **Splunk integration** wizard, go to **Integrations** > **Splunk**.

The steps for configuring Splunk integration in Secure Firewall Management Center are listed in this table.

	Do This	**More Information**
Step 1	Configure Splunk or similar SIEM tool server.	See Configure Splunk Server, on page 3.
Step 2	Choose the event types that you want to send to the Splunk server.	See Select Event Types, on page 4.
Step 3	Specify the devices and the interfaces from which you want to send syslog events to Splunk.	See Select Devices and Interfaces, on page 5.
Step 4	(Optional) Specify the device certificate to be used for sending events securely to Splunk.	See Configure Firewall Certificates, on page 6
Step 5	View the summary of the profile that is being created.	See Summary, on page 7.

Configure Splunk Server

In this step, provide networking information about the Splunk syslog server, and specify the protocols, and ports for receiving syslog events.

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 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

In this step, you can specify the type of events that you want to send to Splunk. The recommended event types are selected by default. However, you can modify the default source for the event types.

Procedure

Step 1 To specify the event source for the event types, from the **Source** drop-down list, choose **FTD** or **FMC**, as applicable. The system default event sources are listed in this table.

Event type	Source (Default)	Applicable sources (Firewall Threat Defense, Firewall Management Center, or both)
Connection—Security or All • **Security** connection events implies sending only high-priority connection events • **All** implies sending all connection events.	Firewall Threat Defense	Both **Important** Sending connection events from the Management Center may cause performance issues.

Event type	Source (Default)	Applicable sources (Firewall Threat Defense, Firewall Management Center, or both)
Intrusion	Firewall Management Center	Both **Note** Sending intrusion events from the Threat Defense devices will not include impact flags.
AMP/Retrospective	Firewall Management Center	Firewall Management Center
File/Malware	Firewall Threat Defense	Both
User activity	Disabled	Firewall Management Center
Correlation	Disabled	Firewall Management Center
Discovery	Disabled	Firewall Management Center
Intrusion packet	Disabled	Both

Step 2 After selection, 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

In this step, 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

In this step, 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 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**.

Summary

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**.

Note
When you configure Management Center events to be sent to Splunk, eventing files are generated immediately after the profile is saved. You will be able to view the events sent from Management Center in Splunk. Deploy is not needed for events from Management Center.

Configure Secure Firewall App in Splunk

To ensure that the Splunk server is reachable by Firewall Management Center and Firewall Threat Defense, and to receive the events from the device, 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 Management Center and Firewall Threat Defense, go to **Apps** > **Cisco Security Cloud** > **Secure Firewall** > **Configure Application**, and then click the **Syslog** tab.

Step 9 In the **Input Name** field, enter any name.

Step 10 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, see Configure TLS on Splunk Server.

Step 11 In the **Port** field, enter a value between 1025 and 65535. The default port is 514.

Step 12 Leave the **Host** field blank. This will allow the Splunk to process events from any Firewall Management Center and Firewall Threat Defense.

Step 13 In the **Source Type** field, enter *cisco:ftd:syslog*.

Step 14 In the **Interval** field, enter *600* seconds.