FORESCOUT

Forescout

Core Extensions Module: CEF Plugin

Configuration Guide

Version 2.8

Contact Information

Forescout Technologies, Inc.

190 West Tasman Drive

San Jose, CA 95134 USA

https://www.forescout.com/support/

Toll-Free (US): 1.866.377.8771

Tel (Intl): 1.408.213.3191

Support: 1.708.237.6591

About the Documentation

- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice

2019-03-19 08:45

Table of Contents

About the CEF Plugin

The CEF Plugin is a component of the Forescout® Core Extensions Module. See Core Extensions Module Information for details about the module.

The CEF Plugin lets the Forescout platform send policy compliance and other host information detected by the Forescout platform to SIEM systems using the CEF messaging format.

In addition, SIEM servers can trigger remediation actions by sending alert messages to the Forescout platform. This functionality uses the alert messaging function common to most SIEM servers, and non-CEF-standard text messages.

About Certification Compliance Mode

Forescout Core Extensions Module: CEF Plugin supports Certification Compliance mode. For information about this mode, refer to the *Forescout Installation Guide.*

Automated Reporting Using CEF

The Forescout platform can automatically update SIEM servers in several ways:

Compliance-based Reporting – The Forescout platform can automatically notify SIEM servers of endpoints that pass or fail Forescout compliance policies. For example, such policies detect hosts running out-of-date antivirus signature files, hosts using unauthorized Peer to Peer applications, or hosts with missing vulnerability patches.

Host Property Tracking – This plugin lets the Forescout platform send customized CEF messages based on any policy conditions. Typically, CEF messaging is used to report a change in the broad range of host conditions that the Forescout platform monitors.

Trigger Forescout Actions Based on SIEM Messages

You can implement a variety of Forescout actions on hosts, based on messages received from the SIEM server. To trigger actions, SIEM servers send the Forescout platform a simple text message. See Receive SIEM Messages – Policy Properties for details.

Forescout/CEF Architecture

You should have a basic understanding of the architecture of the CEF and Forescout platforms.

- Several CounterACT® devices can be assigned to a specific SIEM server or to several SIEM servers.

- A default server can be defined to handle CounterACT devices that have not been assigned to a SIEM server.
- Each CounterACT device can only be assigned to one SIEM server.

How it Works

When using the plugin for the first time, the Forescout platform updates CEF with compliance status changes in real-time. The Forescout platform reports the compliance status of each endpoint whenever it changes.

Predefined periodic update messages can be sent as well. The time interval of the periodical report is configurable.

Automated compliance status reporting is based on evaluation of Forescout compliance policies.

In addition, customized CEF messages can report host information for hosts that satisfy the conditions of any Forescout policy.

What to Do

To work with this plugin:

- Verify that requirements are met. See Requirements.
- Configure and start the plugin. See Configure the Plugin.
- Configure Forescout compliance policies to handle CEF events.
- Set up the CEF Console to view Forescout information.

Requirements

The plugin requires the following Forescout releases and other components:

- Forescout version 8.1.
- Target SIEM servers must parse CEF messages.
- Target SIEM servers must be able to receive messages from CounterACT Appliances and Enterprise Managers.

About Support for Dual Stack Environments

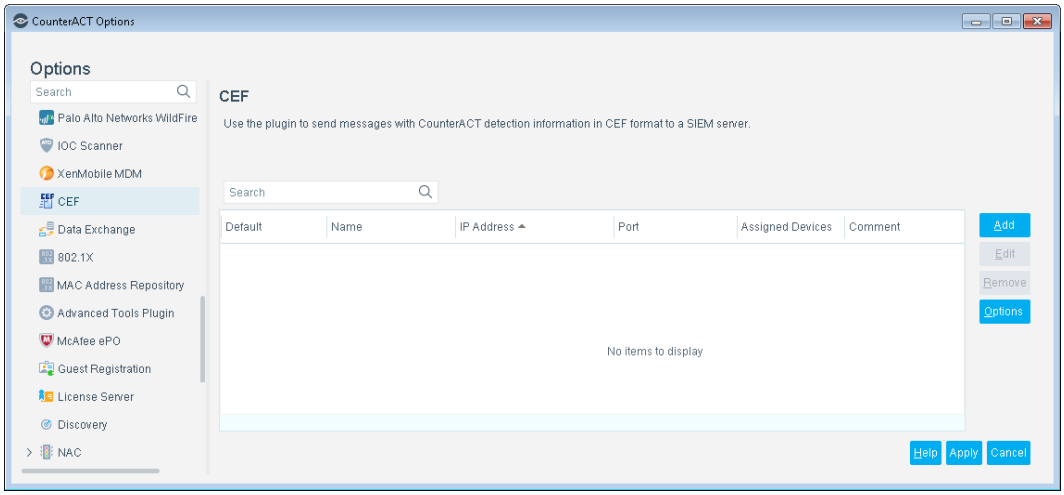
Forescout version 8.1 detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this module.*** The functionality described in this document is based only on IPv4 addresses. IPv6-only endpoints are typically ignored or not detected by the properties, actions, and policies provided by this module.

Configure the Plugin

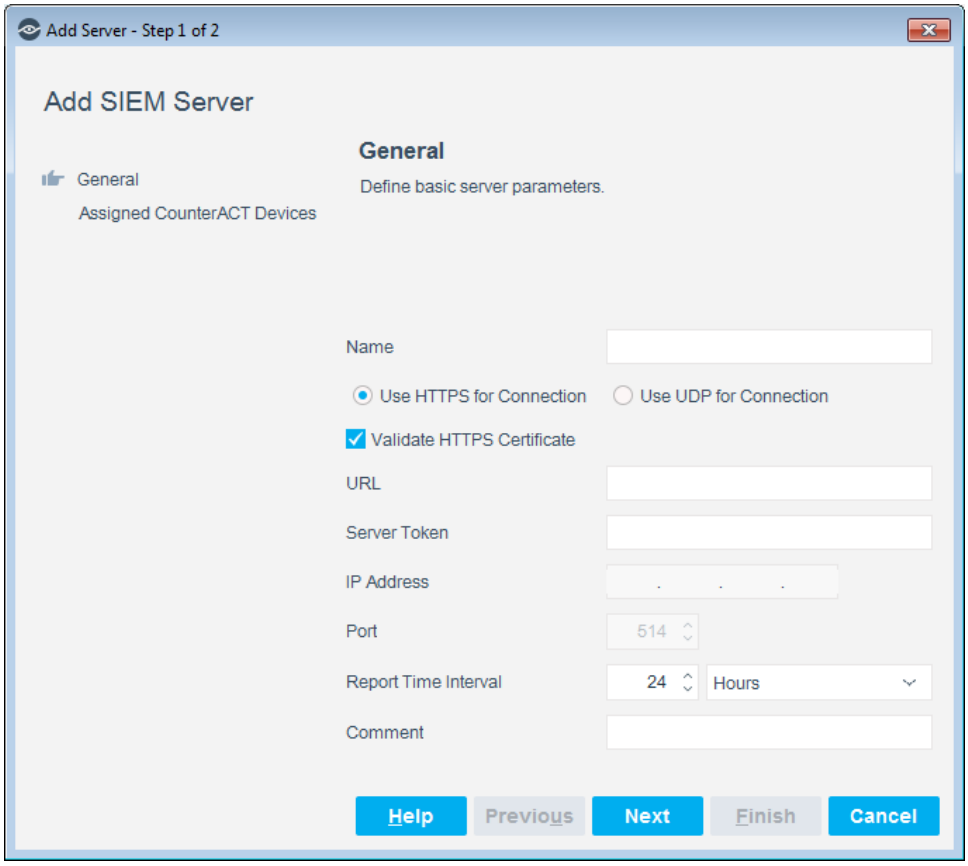
Configuration information is needed to ensure authentication and connection from the plugin to the SIEM server and to handle message transactions. Several CounterACT devices can be assigned to a specific SIEM server. A default server can be defined to handle CounterACT devices that have not been assigned to a SIEM server.

To configure the plugin:

1. Select **Configure**.



2. To add a SIEM server, select **Add**.



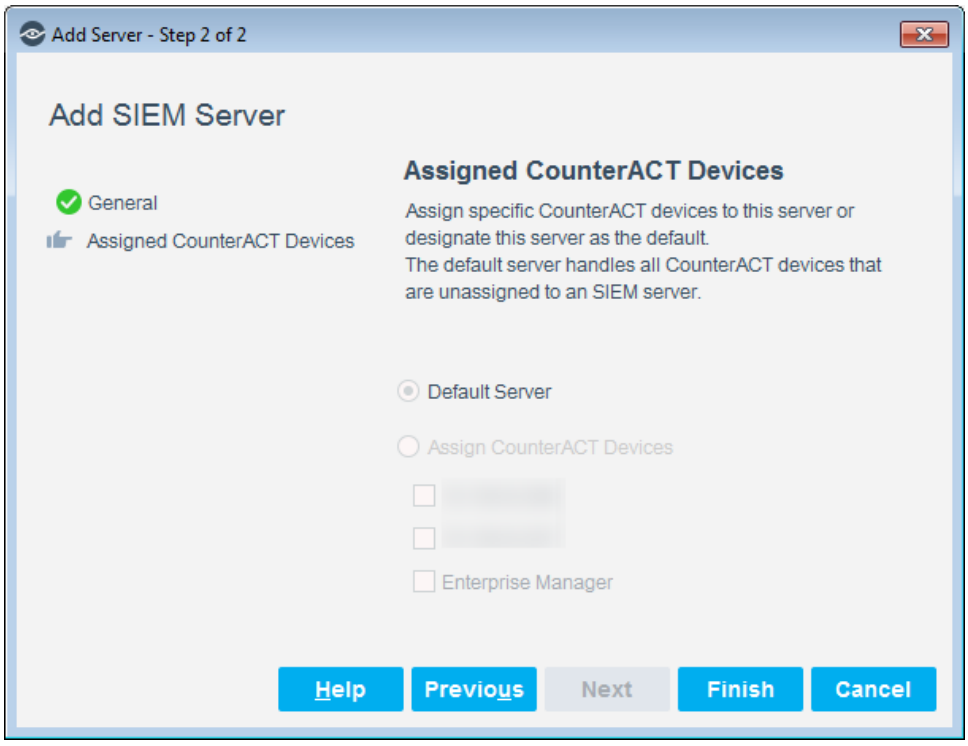
3. In the General pane, enter the server parameters.

Name	Enter the name of the SIEM server.
Use HTTPS/UDP for Connection	Select either **Use HTTPS for Connection** or **Use UDP for Connection**. Use HTTPS when you want a secure connection. When **Use HTTPS for Connection** is selected, the **URL** and the **Server Token** fields are enabled. When **Use UDP for Connection** is selected, the **IP Address** and **Port** fields are enabled.
Validate HTTPS Certificate	Enable or disable validation of the HTTPS certificate. When you select **Use HTTPS for Connection**, the **Validate HTTPS Certificate** option is selected.
URL	Configure a URL as the connection to the SIEM server if you selected **Use HTTPS for Connection**. This is the URL of the HTTPS portal.
Server Token	Enter the server token if you selected **Use HTTPS for Connection**.
IP Address	Enter the IP address of the SIEM server if you selected **Use UDP for Connection**.
Port	Enter the UDP Syslog port used by CEF if you selected **Use UDP for Connection**.

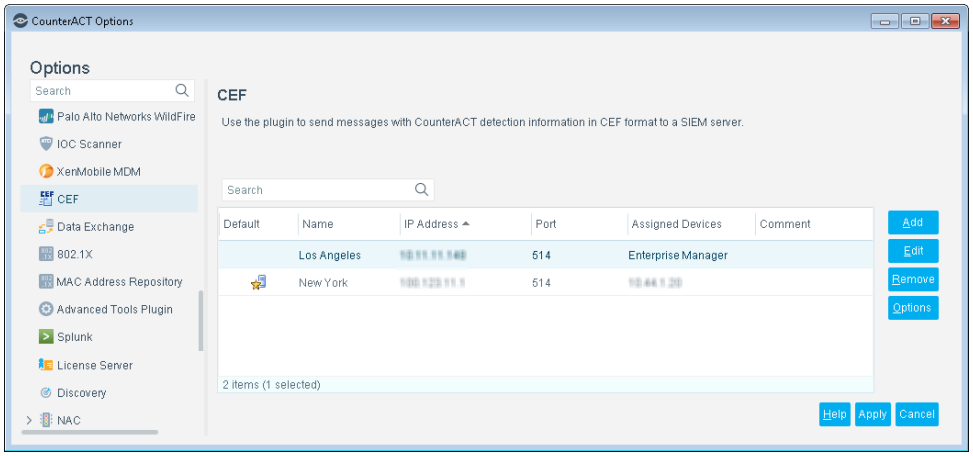
Report Time Interval	Specify how often to update the SIEM server with compliance information. If a compliance event occurs before this time period elapses, a message is sent. The Forescout platform reports the compliance status of each endpoint both periodically and whenever this status changes.
Comment	Enter comments about the SIEM server.

4. Select **Next**.

   If **Validate HTTPS Certificate** is not selected, a warning message about the security of the connection is displayed. Select **Yes**.



5. Select **Default Server** to designate this server as the default server or select **Assign CounterACT Devices** to assign specific CounterACT devices to this server.
6. Select **Finish**. The server configuration is listed in the CEF pane.



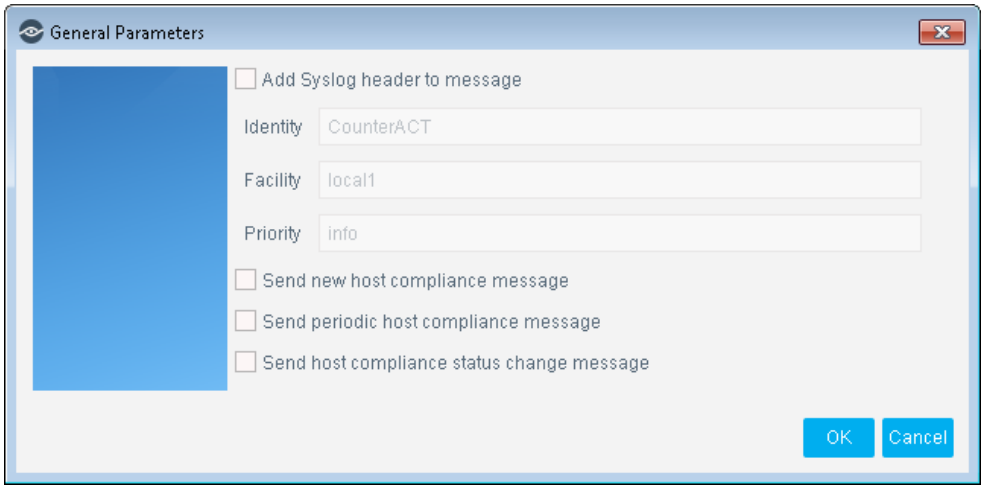
7. Use **Add/Edit/Remove** to manage the CEF configurations.

Include Syslog Message Header

You can add a syslog header to all CEF messages delivered to the SIEM servers. This option may require additional configuration on the SIEM servers.

To include syslog message headers in CEF messages:

1. Select **Options** in the CEF pane.



2. Select **Add Syslog header to message** and define the following parameters.

Identity	A string to identify the source of the syslog message (default: CounterACT)
Facility	Syslog message facility (default: local1)
Priority	Syslog message priority (default: info)

Verify That the Plugin Is Running

After configuring the plugin, verify that it is running.

To verify:

1. Select **Tools**>**Options** and then select **Modules**.
2. Navigate to the plugin and select **Start** if the plugin is not running.

Create Custom CEF Policies

Custom policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct the Forescout platform to apply a policy action to hosts that match (or do not match) property values defined in policy conditions.

For more information about working with policies, select **Help** from the policy wizard.

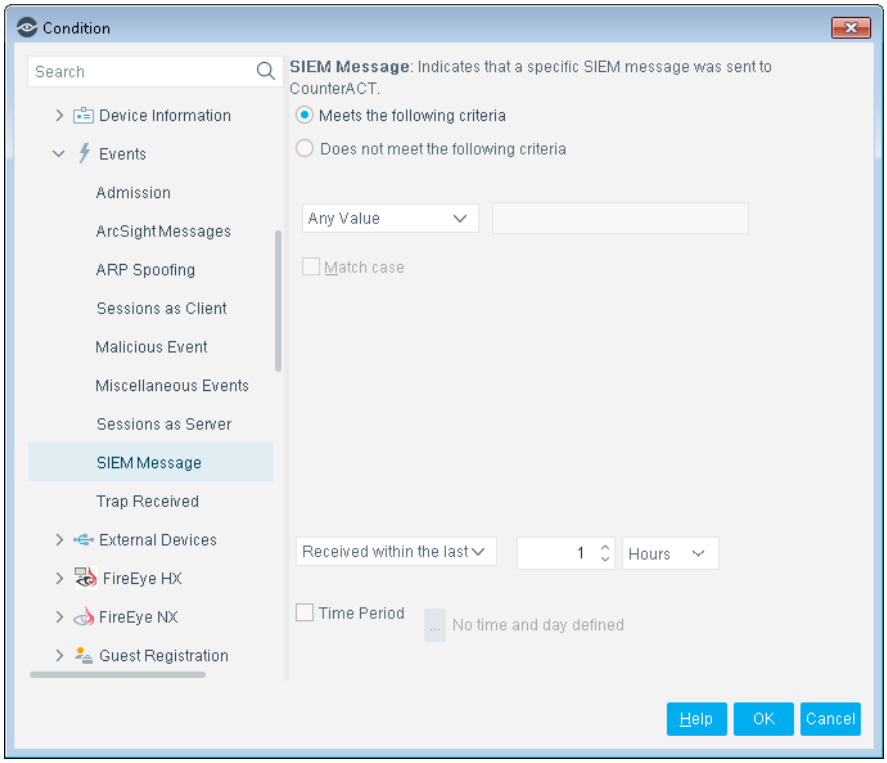
To create a custom policy:

1. Log in to the Console and select **Policy**.
2. Create or edit a policy.

Receive SIEM Messages – Policy Properties

Policy properties let you instruct the Forescout platform to detect hosts with specific attributes. For example, create a policy that instructs the Forescout platform to detect hosts running a certain Operating System or with a certain application installed.

In addition to the bundled properties and actions available for detecting and handling endpoints, you can work with plugin related properties to create custom policies.



To access properties:

1. Go to the Properties tree from the Policy Conditions dialog box.
2. Expand the **Events** folder in the Properties tree. The following property is available:
   - SIEM Message

SIEM Message

This property stores an unordered list of SIEM message strings. Messages are added to a host when the message references that host. For example, the SIEM Messages field for a host can contain the following values:

`VulnerabilityDetected, AntiVirusUpdate, RestoreFromVLAN`

Each entry corresponds to a message string that is sent by the SIEM server. New message strings are added to the existing values, but the queue contains only one instance of each message string. For example, if another vulnerability is detected on a host, the new *VulnerabilityDetected* message overwrites the existing message in the list.

You can use this property with the alert messaging capabilities of most SIEM servers to trigger Forescout actions. For example, you can configure a policy to assign hosts to a specific VLAN when the message *VulnerabilityDetected* is sent by the SIEM server.

To set up this functionality:

- Define a policy with a condition that detects hosts based on SIEM messages.

- Use the messaging or alert capabilities of your SIEM server to define a message to the Forescout platform with the desired message string.

When SIEM server logic generates an alert or remediation condition:

1. The SIEM server sends the predefined message to the Forescout platform.
2. The Forescout platform parses the message and stores the message text in the SIEM Messages property of the relevant host.
3. The Forescout policy detects hosts by matching values in the SIEM Messages property.
4. The Forescout platform implements the actions defined in the policy.
5. The SIEM Message event is displayed in the Console, for example, in the Profile tab.

SIEM Server Event Messages

Embed the following command strings in the message that the SIEM server sends to the Forescout platform. When the Forescout platform receives these messages, it parses the command strings to modify the *SIEM Message* property of the target host.

Add a string to the SIEM Messages host property

To update the value of the *SIEM Messages* host property, embed the following command string in the message that the SIEM server sends to the Forescout platform:

```
fstool siem_update [-N] [-O] <MessageString> <IPAddress>
```

Where

<MessageString> is a one-word string. No spaces are allowed. This string is added to the contents of the *SIEM Messages* property.

Use a string related to the trigger condition at the SIEM server, or to the action you want the Forescout platform to implement.

<IPAddress> identifies the host on which the action is performed. The Forescout platform updates the *SIEM Messages* property of this host with the *MessageString* value.

You can use the following optional flags with this command:

-N creates a new host if the host does not exist

-o updates online status when updating a property

Delete a string from the SIEM messages host property

To delete a value in the *SIEM Messages* host property, embed the following command string in the message that the SIEM server sends to the Forescout platform:

```
fstool siem_update -d <MessageString> <IPAddress>
```

Where

<MessageString> is a one-word string. No spaces are allowed. If this string exists in the *SIEM Messages* list for the host, it is deleted.

<IPAddress> identifies the host on which the action is performed. The Forescout platform deletes the *MessageString* entry from the *SIEM Messages* property of this host.

Clear the SIEM messages host property

To delete *all* values in the *SIEM Messages* host property, embed the following command string in the message that the SIEM server sends to the Forescout platform:

```
fstool siem_update -D <IPAddress>
```

Where **<IPAddress>** identifies the host on which the action is performed. The Forescout platform clears the SIEM Messages property for the specified host.

Send CEF Messages – Policy Actions

Policy actions let you instruct the Forescout platform how to control detected devices. For example, assign potentially compromised endpoints to an isolated VLAN, or send the endpoint user or IT team an email.

In addition to the bundled actions available for handling endpoints, you can work with the plugin related actions to create custom policies.

To access actions:

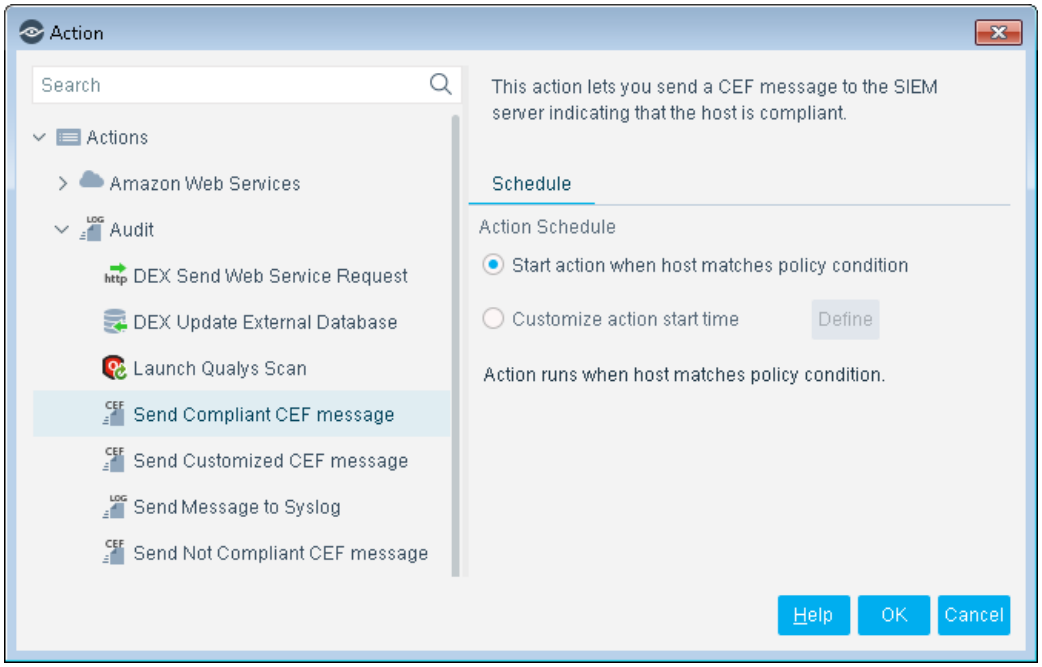
1. Go to the Actions tree from the Policy Actions dialog box.
2. Expand the **Audit** folder. The following actions are available:
   - Send Compliant CEF message
   - Send Customized CEF Message
   - Send Not Compliant CEF message

Send Compliant CEF message

This action sends a CEF message to the SIEM server for each host that meets the conditions of the policy. It is located in the Audit group of the Actions tree.

You can apply standard scheduling options to this action.

The message combines standard CEF message and dictionary fields with extension fields defined by the Forescout platform. For more information on message data fields, see Device Event Mapping to CEF Data Fields.



A sample message in CEF format is shown below.

Field	Sample Message
Version	CEF:0 |
Device vendor	Forescout Technologies |
Device product	CounterAct |
Device version	6.3.4 |
Signature ID	COMPLIANCE |
Name	host is compliant |
Priority	1 |
CounterACT CEF extension fields	cs1Label=Compliancy Policy Name cs2Label=Compliancy Policy Subrule Name cs3Label=Host Compliancy Status cs4Label=Compliancy Event Trigger cs1=AntiVirus Compliance cs2=Compliant cs3=yes cs4=CounterAct Action
Host MAC address	dmac=00:1c:7e:d3:36:a4
Host IP address	dst=10.31.1.101
Destination domain name	dntdom=DOM31
Host name	dhost=QA-LAP-TOSHIBA
Host user	duser=administrator (local)
CounterACT device IP	dvc=10.31.1.153
CounterACT device name	dvchost=Q31A
Event report time	rt=1346923305000

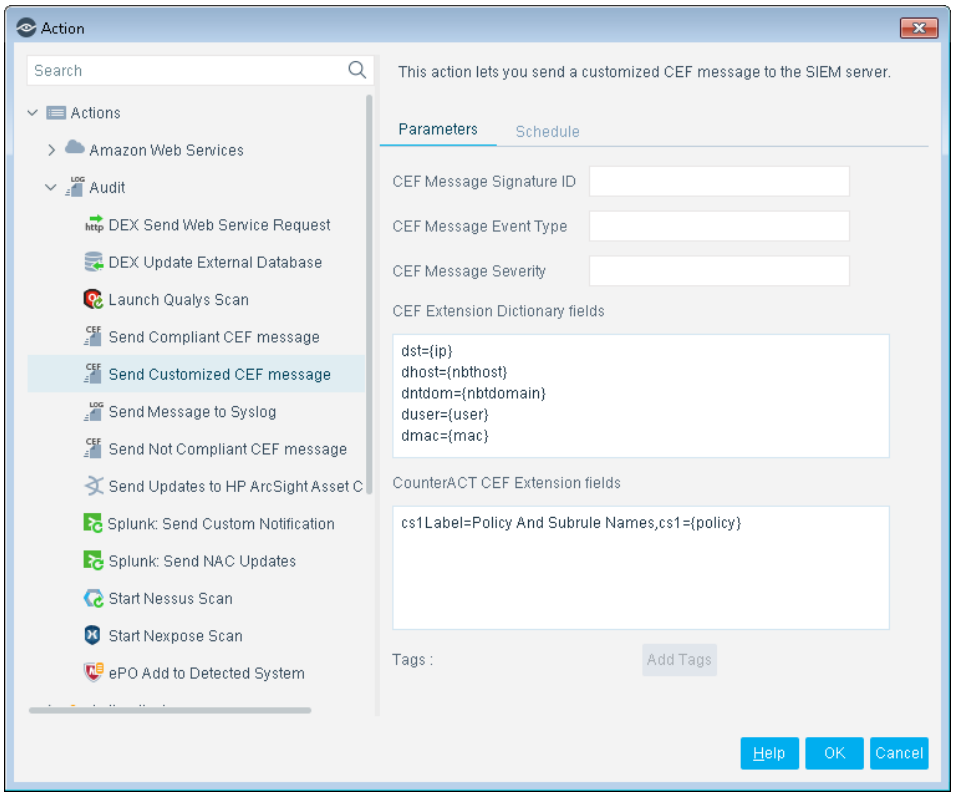
Send Customized CEF Message

This action sends a customized CEF message to the SIEM server for each host that meets the conditions of the policy.

For more information on message data fields, see Device Event Mapping to CEF Data Fields.

To configure a customized CEF message:

1. Edit a policy.
2. Add an action. In the Actions tree, expand the Audit folder and select **Send Customized CEF message**.



3. Specify the following CEF message header parameters:
   - Signature ID
   - Event Type
   - Severity

   The Forescout platform automatically adds vendor-specific fields to the final message header.
4. (Optional) In the **CEF Extension Dictionary fields** area, edit the list of dictionary fields to be included in the message. Each entry in the list has the following format:

   <CEF event data field>={CounterACT property tag}

   Select **Add Tags** to insert a CounterACT property tag in an entry.
5. (Optional) In the **CounterACT CEF Extension fields** area, define the fields to be included in the message. Each entry in the list has the following format:

   Cs#Label=<field label>,cs#={CounterACT property tag}

Select **Add Tags** to insert a CounterACT property tag in an entry.

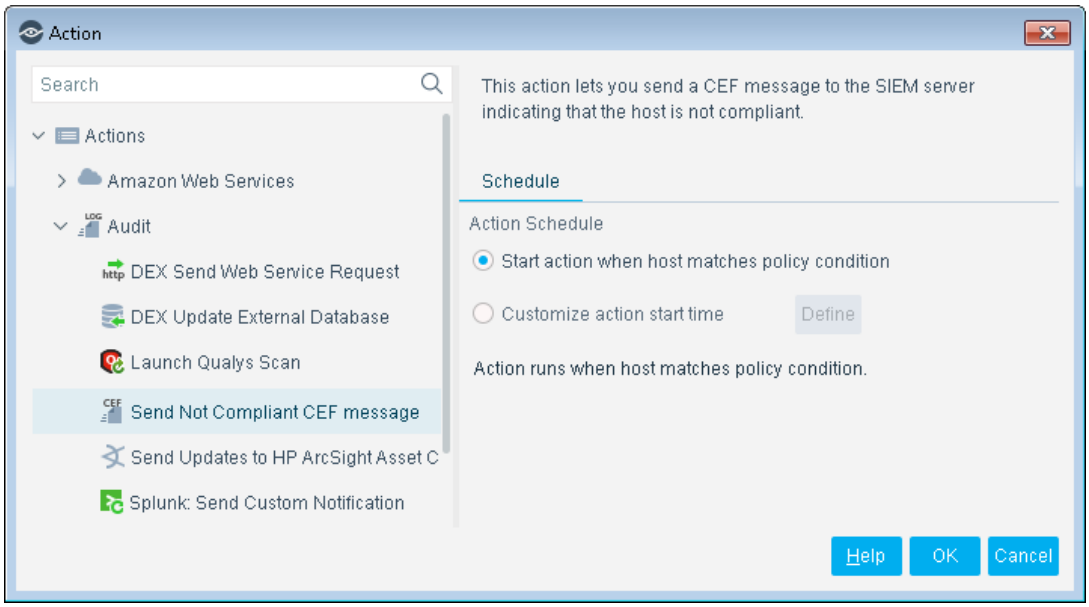
6. (Optional) Select the Schedule tab to apply standard scheduling options to the action.
7. Select **OK** to add the action to the policy.

Send Not Compliant CEF message

This action sends a CEF message to the SIEM server for each host that does not satisfy the conditions of the policy. It is located in the Audit group of the Actions tree.

You can apply standard scheduling options to this action.

The message combines standard CEF message and dictionary fields with extension fields defined by the Forescout platform. For more information on message data fields, see Device Event Mapping to CEF Data Fields.



A sample message in CEF format is shown below.

Field	Sample Message
Version	CEF:0 |
Device vendor	Forescout Technologies |
Device product	CounterAct |
Device version	6.3.4 |
Signature ID	NONCOMPLIANCE |
Name	host is not compliant |
Priority	1 |
CounterACT CEF extension fields	cs1Label=Compliancy Policy Name cs2Label=Compliancy Policy Subrule Name cs3Label=Host Compliancy Status cs4Label=Compliancy Event Trigger cs1=AntiVirus Compliance cs2=AV Not Installed cs3=no

	cs4=CounterAct Action
Host MAC address	dmac=00:0c:29:fa:72:9d
Host IP address	dst=10.31.1.1
Destination domain name	dntdom=DOM31
Host name	dhost=Q31DC1
Host user	duser=User
CounterACT device IP	dvc=10.31.1.153
CounterACT device name	dvchost=Q31A
Event report time	rt=1346923402000

Device Event Mapping to CEF Data Fields

This section describes the data fields in CEF notification messages.

CEF Header Fields

The following table maps CEF header data fields to Forescout event definitions.

CEF Event Data Field	Data Field Meaning	Forescout Event Definition	Values
Version	CEF format version	Version	0
Device Vendor	Name of vendor	Device Vendor	Forescout Technologies
Device Product	Product Name	Device Product	CounterACT
Device Version	Forescout Version	Device Version	6.3.4
Signature ID	Host event identifier	Compliancy Event Signature ID	COMPLIANCE
		Non-Compliancy Event Signature ID	NONCOMPLIANCE
Name	Host event name	Compliancy Event Name	Host is compliant
		Non-Compliancy Event Name	Host is not compliant
Priority	Importance of the host event	Compliancy Event Severity	3
		Non-Compliancy Event Severity	5

Forescout Extension Fields

The following table lists Forescout-defined CEF extension fields. These fields are always included in *Compliant* and *Not Compliant* messages.

CEF Event Data Field ID	Data Field Label	Host Property	Values
cs1	Compliancy Policy Name	Compliancy Policy Name	Forescout policy name. This is a compliance policy or the name of a policy that contains a CEF messaging action.
cs2	Compliancy Policy Sub-rule Name	Compliancy Policy Sub-Rule Name	The sub-rule that classified the host as compliant or not compliant.
cs3	Host Compliancy Status	Host Compliance Status	▪ Yes: For a compliant host. ▪ No: For a non-compliant host.
cs4	Compliancy Event Trigger	Compliancy Event Trigger	▪ New host: For a newly discovered host. ▪ Compliancy status changed: For a host whose status changed. ▪ Periodical: When a host status is unchanged within the reporting time interval.

CEF Dictionary Fields

The following table lists standard CEF dictionary extension fields that are always included in *Compliant* and *Not Compliant* messages.

CEF Event Field ID	CounterACT Property Tag	Description
Dst	Ip	The host IP address, in dot-separated format
Dmac	Mac	The host MAC address, in colon-separated format
Duser	user	String identifying the user logged onto the host when the event occurred
Dhost		The host name
Dvc		CounterACT device IP address, in dot-separated format
Dvchost		CounterACT device host name
Rt		Event detection time, in milliseconds elapsed since Jan 1, 1970

Core Extensions Module Information

The CEF plugin is installed with the Forescout Core Extensions Module.

The Forescout Core Extensions Module provides an extensive range of capabilities that enhance the core Forescout solution. These capabilities enhance detection, classification, reporting, troubleshooting and more. The following components are installed with the Core Extensions Module:

Advanced Tools Plugin	Dashboard Plugin	NBT Scanner Plugin
CEF Plugin	Device Classification Engine	Packet Engine
DHCP Classifier Plugin	External Classifier Plugin	Reports Plugin
DNS Client Plugin	Flow Analyzer Plugin	Syslog Plugin
DNS Enforce Plugin	Flow Collector	Technical Support Plugin
DNS Query Extension Plugin	IOC Scanner Plugin	Web Client Plugin
	IoT Posture Assessment Engine	

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. This module is automatically installed when you upgrade the Forescout version or perform a clean installation.

Additional Forescout Documentation

For information about other Forescout features and modules, refer to the following resources:

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- ***Per-Appliance Licensing Mode*** – Product Updates Portal
- ***Flexx Licensing Mode*** – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:

- From the Console, select **Help > About Forescout**.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:

- Go to https://www.Forescout.com/company/resources/, select **Technical Documentation** and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Forescout Customer Portal:

- Go to https://Forescout.force.com/support/ and select **Downloads**.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools

Access information directly from the Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

Forescout Administration Guide

- Select **Forescout Help** from the **Help** menu.

Plugin Help Files

- After the plugin is installed, select **Tools** > **Options** > **Modules**, select the plugin and then select **Help**.

Online Documentation

- Select **Online Documentation** from the **Help** menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).