FORESCOUT

Forescout

Core Extensions Module: CEF Plugin

Configuration Guide

Version 2.8.2

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

Legal Notice

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2020-07-09 00:19

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 sends policy compliance and other host information detected by Forescout eyeSight 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.

Certification Compliance Mode

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

Overlapping IP Address Support

The CEF Plugin supports working with networks that use overlapping IP addresses. For details about enabling and configuring the Forescout platform's support of overlapping IP address use in an enterprise's network, refer to the *Forescout Working with Overlapping IP Addresses How-to Guide*. See Additional Forescout Documentation for information on how to access this document.

About Support for Dual Stack Environments

The Forescout platform detects endpoints and interacts with network devices based on both IPv4 and IPv6 addresses. However, ***IPv6 addresses are not yet supported by this eyeExtend 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 eyeExtend module.

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

This section describes the requirements for configuring and running the Forescout CEF Plugin.

Forescout Requirements

The following Forescout platform and component versions must be running in your Enterprise Manager and your Appliances:

- Forescout interim release 8.2.1
- Core Extensions Module 1.2.1 with the CEF Plugin
- If you are using Flexx licensing, ensure that you have a valid Forescout eyeControl (ForeScout CounterACT Control) license, to use enforcement actions provided by the component. Refer to the *Forescout Flexx Licensing How-to Guide* for more information about managing Flexx licenses.

SIEM Server Requirements

The CEF Plugin requires that the following capabilities are configured/enabled in target SIEM servers:

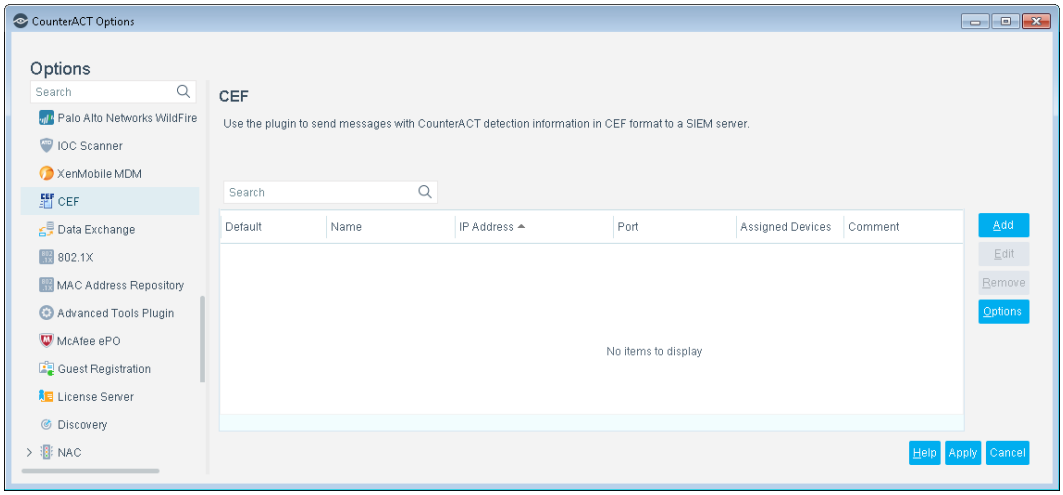
- Target SIEM servers must parse CEF messages.
- Target SIEM servers must be able to receive messages from CounterACT Appliances and Enterprise Managers.

Configure the Plugin

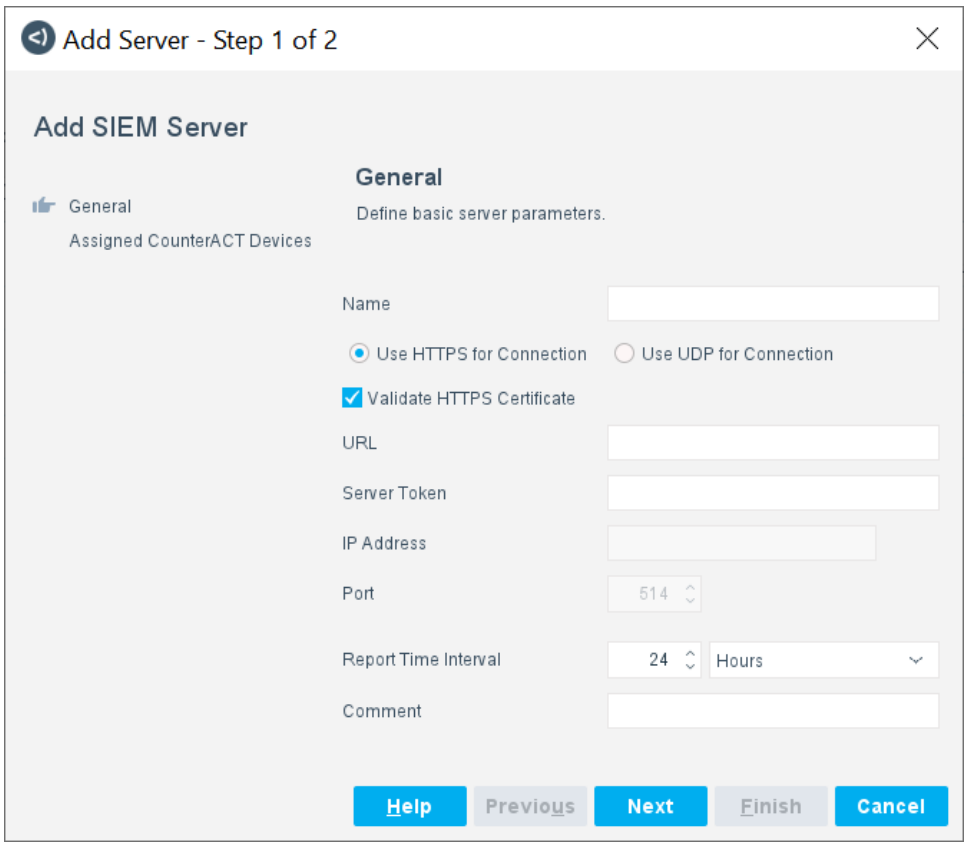
Configuration information is needed to ensure authentication and connection from the plugin to the SIEM server and to handle message transactions. Several CounterACT devices can be assigned to a specific SIEM server. A default server can be defined to handle CounterACT devices that have not been assigned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

To add a SIEM server entry to the plugin configuration:

1. Select **Tools** menu > **Options** > **Modules** > **Core Extensions** > **CEF** > **Configure**. The *CEF* pane opens.



2. Select **Add**. The General pane opens.



3. In the *General* pane, enter the following server parameters:

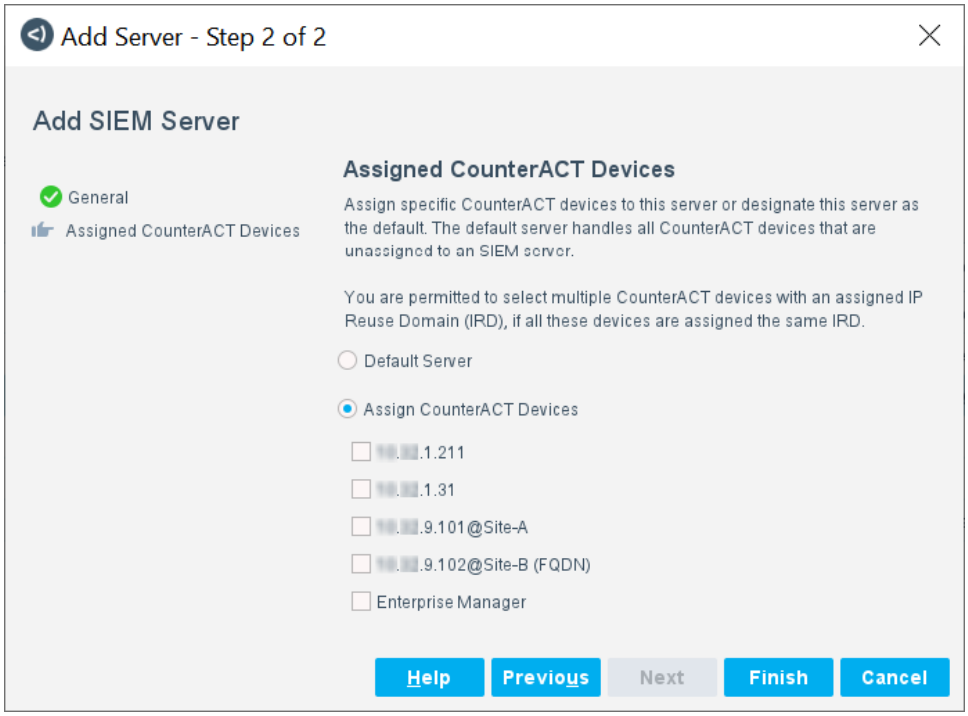
Field / Setting	Description
Name	Enter the name of the SIEM server.

Field / Setting	Description
Use HTTPS for Connection or **Use 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 by default.
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**. *Note*: If *Use HTTPS for Connection* is selected, the Forescout platform uses the provided URL to resolve the SIEM server's IP address, which the Forescout platform then enters in the *IP address* field.
Port	Enter the UDP Syslog port that the CEF Plugin must use, 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.

   – Selecting **Yes** transitions you onward to the *Assigned CounterACT Devices* pane.
   – Selecting **No** returns you to the *General* pane.



5. In the *Assigned CounterACT Devices* pane, select any one of the following options:

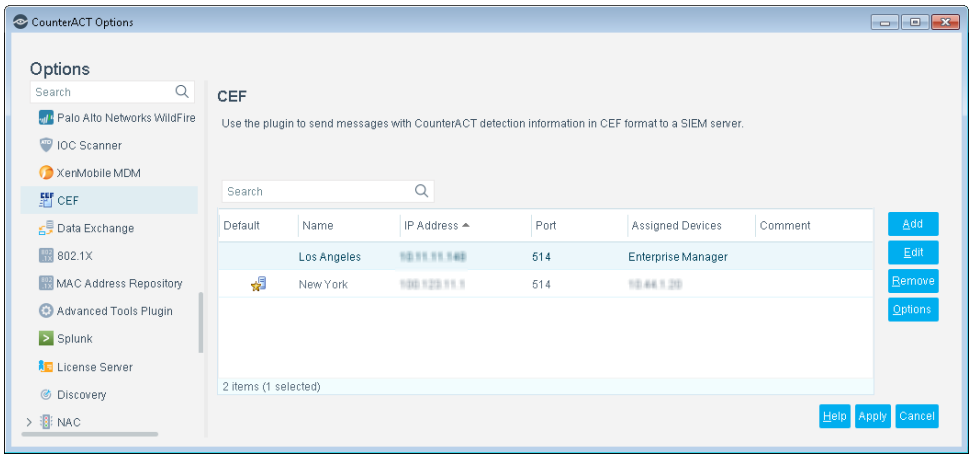
- Select **Default Server** to designate this SIEM server as the default SIEM server. CounterACT devices that are not explicitly assigned to work with any other SIEM server are assigned to work with the default SIEM server.
- Select **Assign CounterACT Devices** and then select one or more of the listed CounterACT devices thereby assigning these CounterACT devices to work with this SIEM server. A CounterACT device that is currently assigned to a SIEM server appears in the list with the name of the assigned SIEM server shown in parentheses to its right. For example, 192.168.59.111 (NorthServer).

  When the Forescout platform is enabled to support overlapping IP addresses:

  - If the SIEM server's IP address is located within an assigned IP Reuse Domain (IRD) of one or more than one of the listed CounterACT devices, then these CounterACT devices display with their IRD as a suffix of the IP address, in the form *<IP address>@<IRD>*. For example, 192.168.19.207@Site–B.

    IP Reuse Domains are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.
  - You can select multiple CounterACT devices each having an assigned IRD, however, all these devices must have the same assigned IRD.
  - You cannot select the following mixture of CounterACT devices: CounterACT device(s) having an assigned IP Reuse Domain and CounterACT device(s) that are located in the default/global network.

6. Select **Finish**. The *CEF* pane lists the added server configuration.

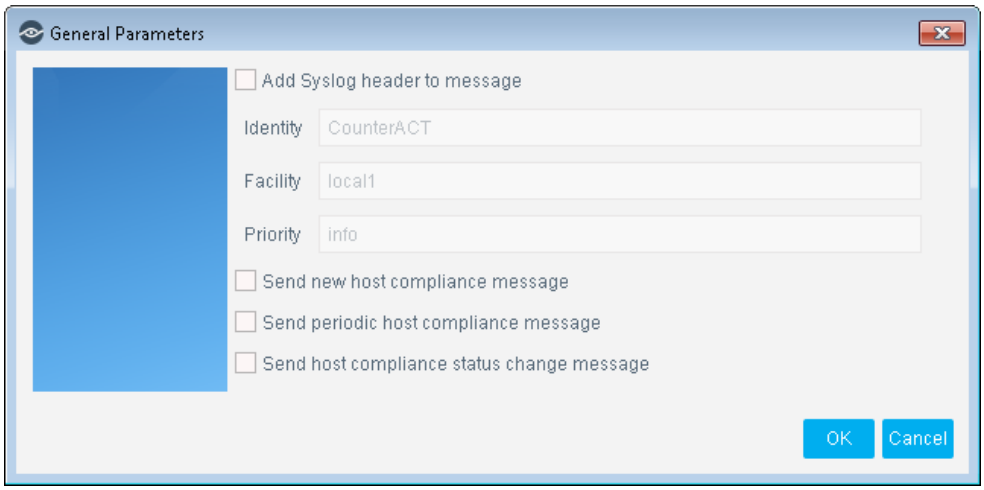


Include Syslog Message Header

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. In the *CEF* pane, select **Options**. The *General Parameters* dialog box opens.



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

Field / Option	Description
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*)

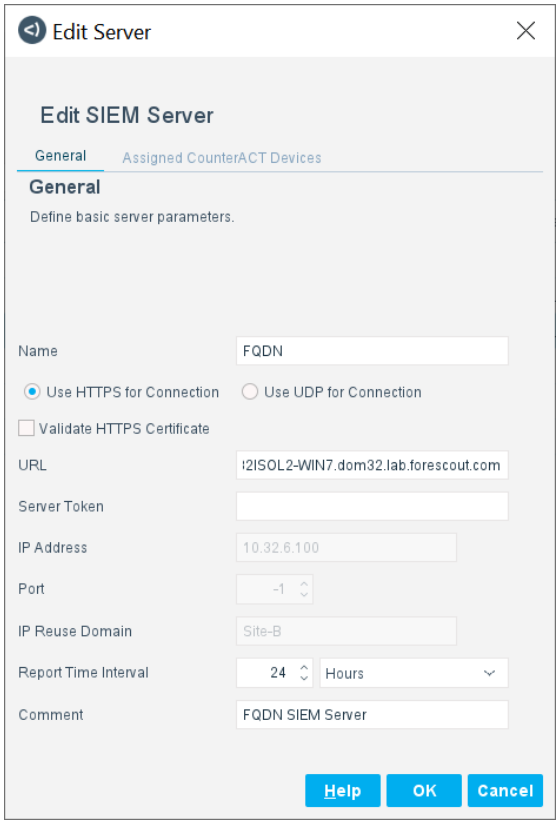
Edit a SIEM Server Entry

You can edit the plugin configuration for a SIEM server entry, including enabling/disabling specific settings and/or options.

To edit a SIEM server entry:

1. Select **Tools** menu > **Options** > **Modules** > **Core Extensions** > **CEF** > **Configure**. The *CEF* pane opens.
2. In the *CEF* pane, select a SIEM server entry and then select **Edit**. The *Edit SIEM Server* window opens.
3. Modify fields, settings and/or options in the various tabs. For details about these tabs and their content, see In the General pane and In the Assigned CounterACT Devices pane.

When the Forescout platform is enabled to support overlapping IP addresses, the *Edit SIEM Server* window displays the *IP Reuse Domain* field (view-only).



The field contains either one of the following entries:

- The IRD in which the SIEM server is located.

  IP Reuse Domains are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.

- A blank entry identifying that the SIEM server is located within the enterprise's default/global network.

Remove a SIEM Server Entry

Removing a SIEM server entry stops all plugin interaction with that SIEM server.

To remove a SIEM server entry:

1. Select **Tools** menu > **Options** > **Modules** > **Core Extensions** > **CEF** > **Configure**. The *CEF* pane opens.
2. In the *CEF* pane,, select a SIEM server entry and then select **Remove**.

   *You cannot remove the currently designated, default SIEM server. The **Remove** button is disabled upon user selection of the default SIEM server.*

3. Select **Apply** to save the updated plugin configuration in the Forescout platform.

Ensure That the CEF Plugin Is Running

After installing the CEF Plugin (and configuring it, if necessary), ensure that it is running.

To verify:

1. Select **Tools** > **Options** > **Modules**.
2. In the *Modules* pane, hover over the CEF Plugin name to view a tooltip indicating if it is running on Forescout devices in your deployment.

   The name is preceded by one of the following icons:

   –  - The CEF Plugin is stopped on all Forescout devices.

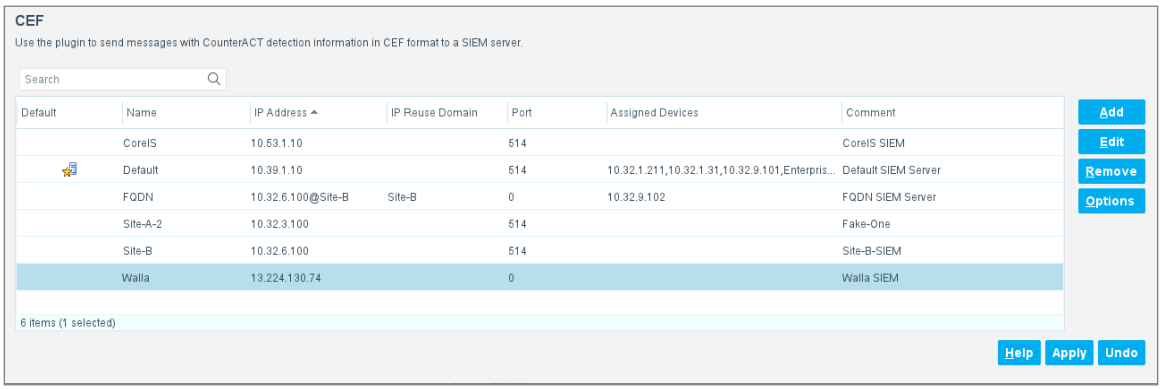
   –  - The CEF Plugin is stopped on some Forescout devices.

   –  - The CEF Plugin is running on all Forescout devices.

3. If the CEF Plugin is not running, select **Start**, and then select the relevant Forescout devices.
4. Select **OK**.

CEF Pane Display

The Console's *CEF* pane displays information about each SIEM server that the plugin is configured to work with. Access the *CEF* pane via the following Console selections: **Tools** menu > **Options** > **Modules** > **Core Extensions** > **CEF** > **Configure**.



The *CEF* pane can display the following SIEM server information:

Column	Description
Assigned Devices	The CounterACT devices that are assigned to the SIEM server.
Comment	The text entered in the *Comment* field of the *General* pane/tab's for the SIEM server.
Default	If the icon entry displays in this column, it identifies the SIEM server as the designated, default SIEM server. Any CounterACT device that is not assigned to a specific SIEM server, is assigned to this default SIEM server.
IP Address	The IP address (IPv4) of the SIEM server. When the SIEM server is located within an IP Reuse Domain (IRD), that IRD displays as a suffix of the IP address, in the form *<IP address>@<IRD>*. For example, 192.168.17.209@Site-W.
IP Reuse Domain	This column is only available for display in the CEF pane when the Forescout platform is enabled to support overlapping IP addresses. Displays either the IRD in which the SIEM server is located or the entry is blank. A blank entry identifies that the SIEM server is located within the enterprise's default/global network. IP Reuse Domains are used to distinguish several instances of an overlapping IP address. IP addresses are unique in each IP Reuse Domain and cannot overlap within a domain.
Name	The name of the SIEM server, which is entered in the *Name* field of the *General* pane/tab.
Port	The port on the SIEM server to which CounterACT devices must send their UDP messages to, when the plugin is configured to **Use UDP for Connection** with the SIEM server. When the plugin is configured to **Use HTTPS for Connection** with the SIEM server, the port value is 0 (zero).

*Not all columns display by default. To edit the display, right-click a column heading and select **Add/Remove Columns**.*

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.

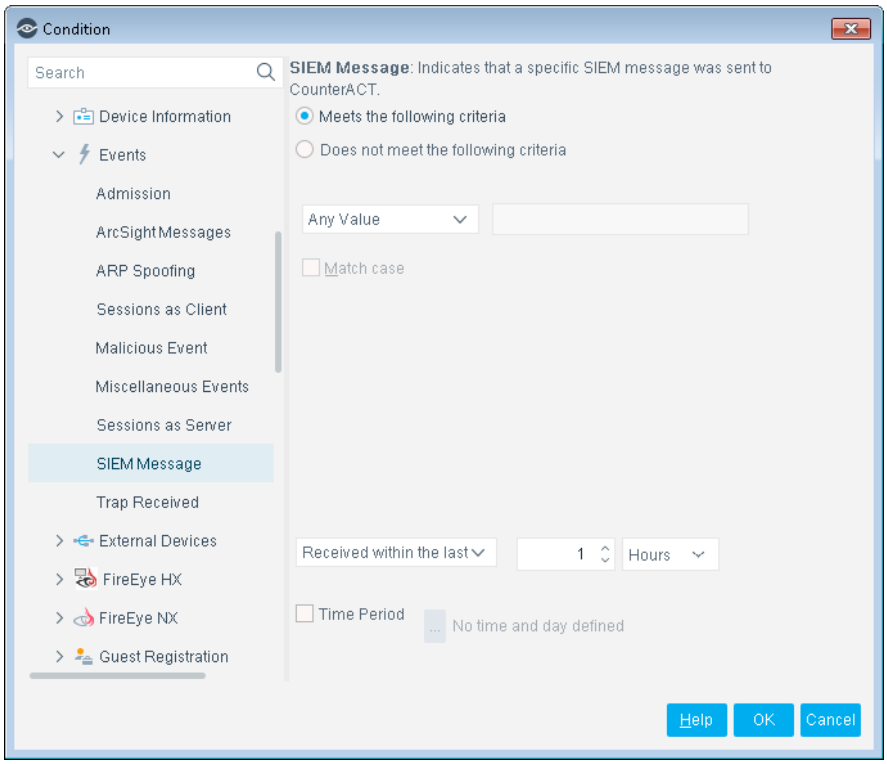
To create a custom policy:

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

The *SIEM Message* 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 Message's 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 Message Host Property
- Delete a String from the SIEM Message Host Property
- Clear the SIEM Message Host Property

Add a String to the SIEM Message Host Property

To update the value of the *SIEM Message* 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 Message* 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 Message* 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

If you experience any problem with the proper functioning of the **fstool siem_update** command, contact Forescout Technical Support.

Delete a String from the SIEM Message Host Property

To delete a value in the *SIEM Message* 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 Message* 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 Message* property of this host.

If you experience any problem with the proper functioning of the **fstool siem_update** command, contact Forescout Technical Support.

Clear the SIEM Message Host Property

To delete *all* values in the *SIEM Message* 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 Message* property for the specified host.

If you experience any problem with the proper functioning of the **fstool siem_update** command, contact Forescout Technical Support.

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:

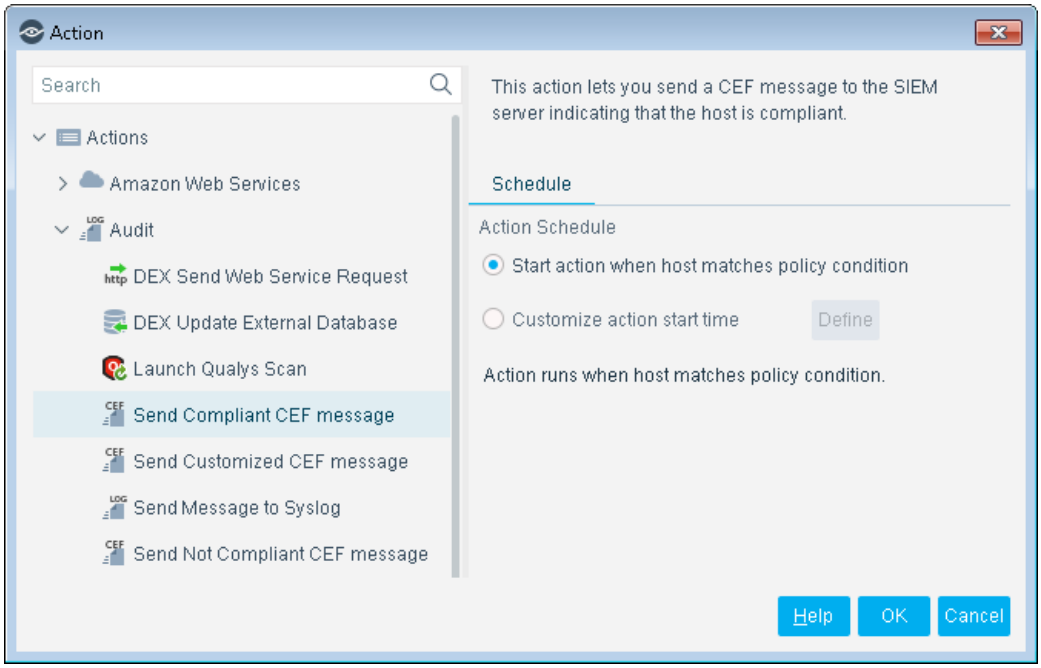
1. Go to the *Actions* tree from the *Policy Actions* dialog box.
2. Expand the **Audit** folder. The following actions are available:
   - Send Compliant CEF Message
   - Send Customized CEF Message
   - Send Not Compliant CEF Message

Send Compliant CEF Message

The *Send Compliant CEF message* 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.



The following table presents a sample, compliance message in CEF format:

Field	Sample Message
Version	CEF:0 |
Device vendor	Forescout Technologies |
Device product	CounterAct |
Device version	8.2.1 |
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 name	dhost=QA-LAP-TOSHIBA
Destination domain name	dntdom=DOM31
Host IP address	dst=10.31.1.101
Host IP Reuse Domain	ird=Unknown
Host user	duser=administrator (local)
CounterACT device IP	dvc=10.31.1.153
CounterACT device name	dvchost=Q31A
Event report time	rt=1346923305000

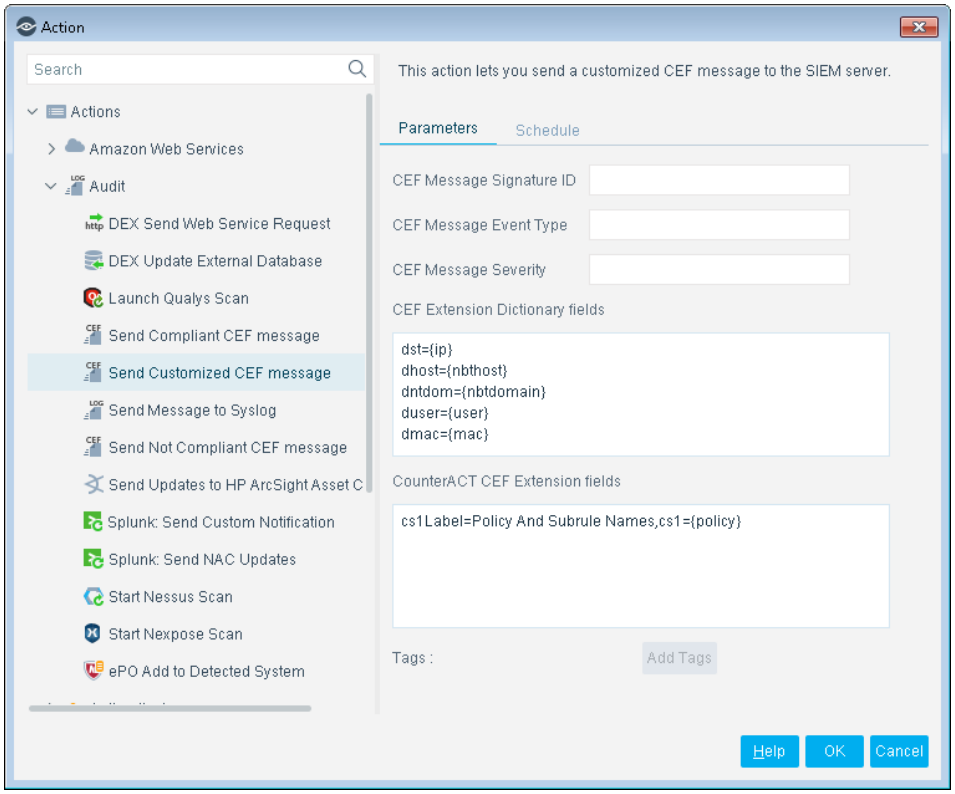
Send Customized CEF Message

The *Send Customized CEF message* 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}

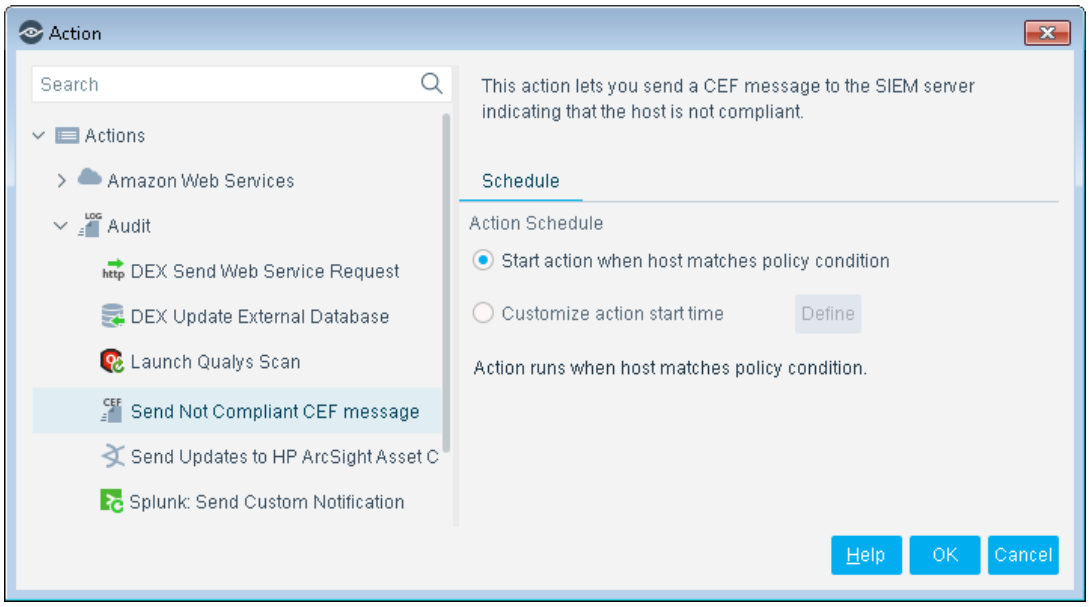
   Select **Add Tags** to insert a CounterACT property tag in an entry.
6. (Optional) Select the Schedule tab to apply standard scheduling options to the action.
7. Select **OK** to add the action to the policy.

Send Not Compliant CEF Message

The *Send Not Compliant CEF message* 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.



The following table presents a sample, non-compliance message in CEF format:

Field	Sample Message
Version	CEF:0 |
Device vendor	Forescout Technologies |
Device product	CounterAct |
Device version	8.2.1 |
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 name	dhost=Q31DC1
Destination domain name	dntdom=DOM31
Host IP address	dst=10.31.1.1
Host IP Reuse Domain	ird=Site-E
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	*<FS platform version>*
Signature ID	Host event identifier	Compliancy Event Signature ID	*COMPLIANCE*
		Non-Compliancy Event Signature ID	*NONCOMPLIANCE*

CEF Event Data Field	Data Field Meaning	Forescout Event Definition	Values
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 that 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
dmac	**mac**	The host MAC address, in colon-separated format
dhost	**nbthost**	The host name
dntdom	**nbtdomain**	Destination domain name
dst	**ip**	The host IPv4 address, in dot-separated format
ird	**area_code**	Field displays either the IRD in which the host is located or the value *Unknown* that identifies that the host is located within the enterprise's default/global network.
duser	**user**	String identifying the user logged onto the host when the event occurred
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

If you have existing policies (created before Forescout interim release 8.2.1/Core Extensions Module 1.2.1/CEF Plugin 2.8.2) that use any of the *Audit* actions - *Send Compliant CEF message*, *Send Customized CEF message* or *Send Not Compliant CEF message* - then in order for the CEF Event Field ID **ird** to appear in their resulting CEF message, you must edit the policies in which these actions are used; first remove the action and then add the action anew.

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	Device Data Publisher	IoT Posture Assessment Engine
CEF Plugin	DNS Client Plugin	
Cloud Uploader	DNS Enforce Plugin	NBT Scanner Plugin
DHCP Classifier Plugin	DNS Query Extension Plugin	Packet Engine
Dashboards Plugin	External Classifier Plugin	Reports Plugin
Data Publisher	Flow Analyzer Plugin	Syslog Plugin
Data Receiver	Flow Collector	Technical Support Plugin
Device Classification Engine	IOC Scanner Plugin	Web Client Plugin

The Core Extensions Module is a Forescout Base Module. Base Modules are delivered with each Forescout release. Upgrading the Forescout version or performing a clean installation installs this module automatically.

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 Technical Documentation Page, and 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 Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:

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

Technical Documentation Page

The Forescout Technical Documentation page provides a link to the searchable, web-based Documentation Portal, as well as links to a wide range of Forescout technical documentation in PDF format.

To access the Technical Documentation page:

- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. The portal also provides 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 Support Portal

The Downloads page on the Forescout Customer Support Portal provides product and documentation downloads for Forescout platform releases, Base Modules, Content Modules, and eyeExtend modules. Software and related documentation only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support 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.

To access the Documentation Portal:

- Go to https://updates.forescout.com/support/files/counteract/docs_portal/

Forescout Help Tools

You can access individual documents, as well as the Documentation Portal, 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 in the Console.

Forescout Administration Guide

- Select **Administration Guide** from the **Help** menu.

Plugin Help Files

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

Content Module, eyeSegment Module, and eyeExtend Module Help Files

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

Documentation Portal

- Select **Documentation Portal** from the **Help** menu.