ForeScout

CounterACT™ CEF Plugin

Configuration Guide

Version 2.6.0 and Above

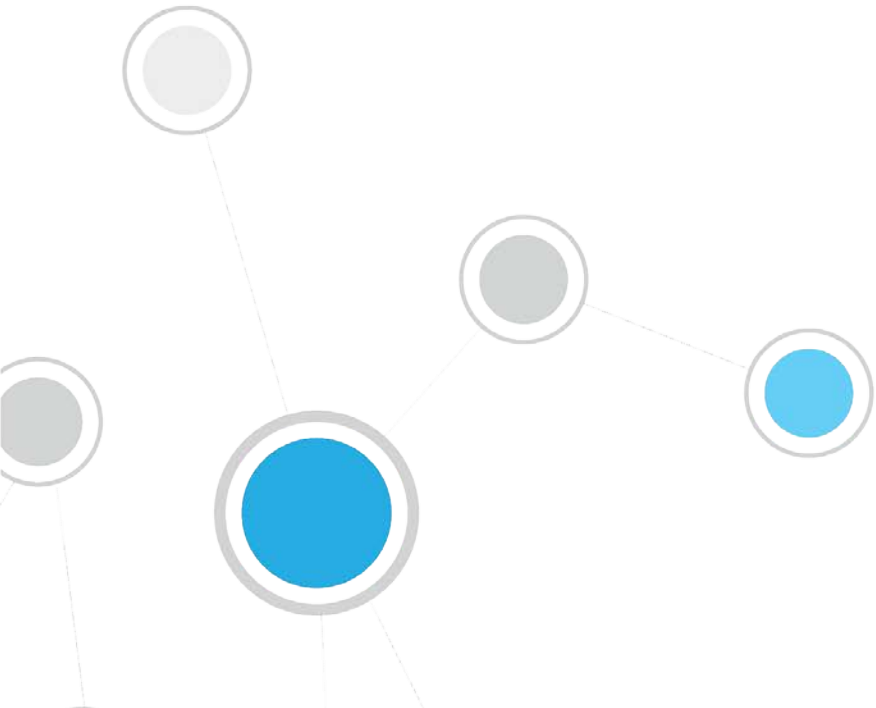


Table of Contents

About the CounterACT CEF Plugin

CounterACT CEF integration lets CounterACT send policy compliance and other host information detected by CounterACT to SIEM systems using the CEF messaging format.

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

Automated Reporting Using CEF

CounterACT can automatically update SIEM servers in several ways:

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 For example, such policies detect hosts running out-of-date antivirus signature files; hosts using unauthorized Peer to Peer applications, or hosts with missing vulnerability patches.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

Trigger CounterACT Actions Based on SIEM Messages

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

Open Integration with ControlFabric Technology

ControlFabric technology enables CounterACT and other solutions to exchange information and resolve a wide variety of network, security and operational issues. ControlFabric uses a variety of standard-based, easily implemented mechanisms for bi-directional integration with a wide variety of services and platforms.

The CEF plugin provides core ControlFabric functionality that lets CounterACT communicate with external platforms and trigger policy-driven actions.

For more information about other integration mechanisms, visit the ControlFabric Resource Page.

CounterACT/CEF Architecture

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

- A default server can be defined and handles 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 the plugin is installed, CounterACT updates CEF with compliance status changes in real-time. CounterACT 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 CounterACT *Compliance* policies.

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

What to Do

Perform the following in order to work with this plugin:

- Download the plugin from the ForeScout website.
- Verify that requirements are met. See Requirements.
- Install, configure and start the plugin. See Install the Plugin.
- Configure CounterACT Compliance policies to handle CEF events.
- Set up the CEF Console to view CounterACT information.

Requirements

This section describes:

CounterACT Software Requirements

Reporting based on CEF messaging is supported by CounterACT versions 6.3.4.1 or higher.

Use of CounterACT actions based on SIEM server alert messages is supported by CounterACT version 6.3.4.10 and version 7.0.0 Hotfix 1.3 and above and requires CounterACT CEF Plugin version 2.5.0.

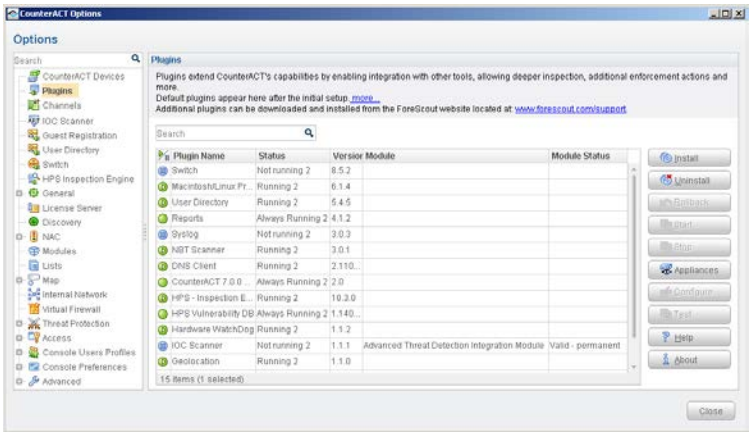
- Target SIEM servers must parse CEF messages.
- Target SIEM servers must be able to receive messages from CounterACT Appliances and Enterprise Managers.

Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   - If you are installing a Beta release of this plugin, acquire the plugin **`.fpi`** file from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support, Base Plugins page and download the plugin **`.fpi`** file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.



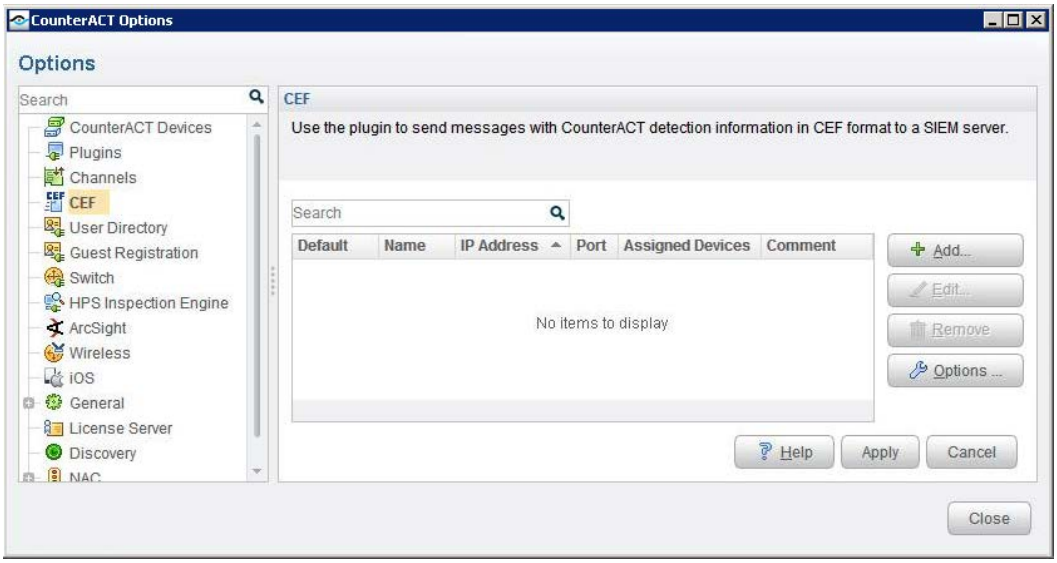
5. Select **Install**. The Open dialog box opens.
6. Browse to and select the saved plugin **`.fpi`** file.
7. Select **Install**.
8. An installation or upgrade information dialog box and a license agreement dialog box will open. Accept the license agreement to proceed with the installation.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.

Configure the Plugin

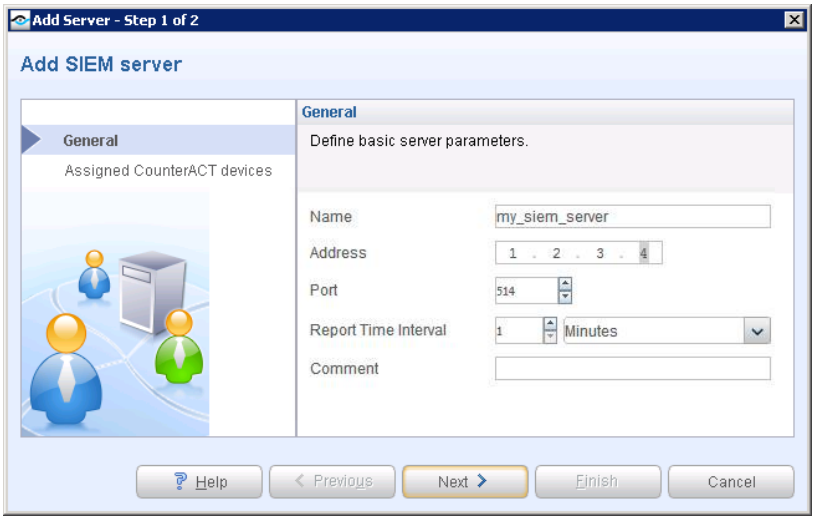
Configuration information is needed to ensure authentication and connection from the plugin to the SIEM server and to handle message transaction. Several CounterACT devices can be assigned to a specific SIEM server. A default server can be defined and handles CounterACT devices that have not been assigned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

To configure the plugin:

1. Select **Configure**. The CEF configuration pane opens.



2. To add a SIEM server, select **Add**. The Add SIEM server wizard opens.

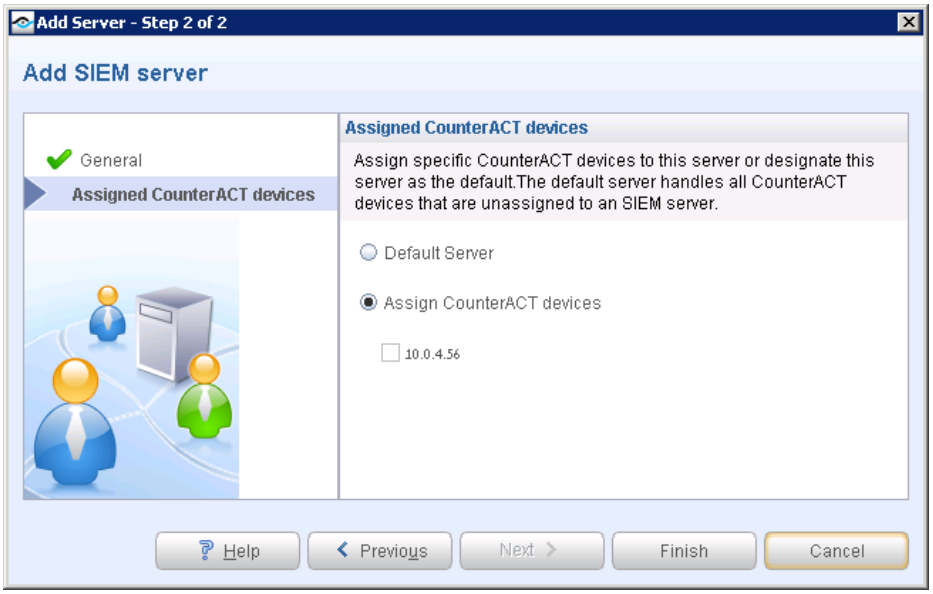


3. In the General pane, enter basic server parameters.

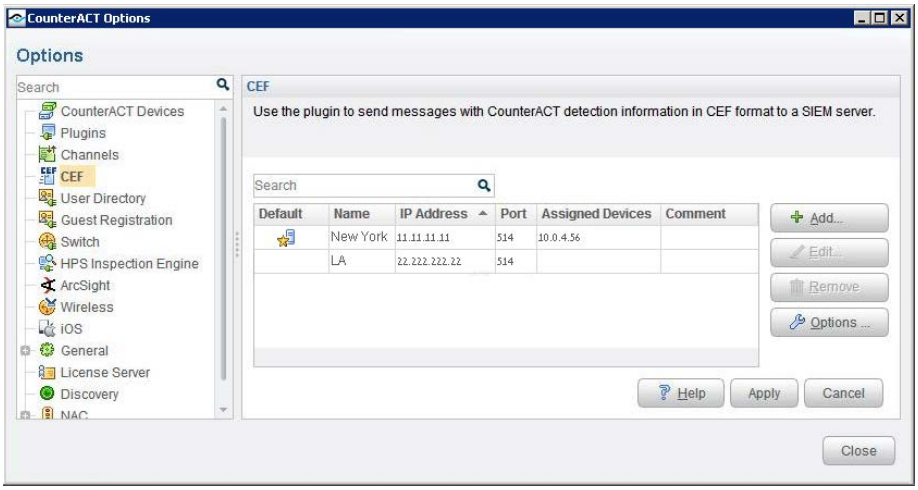
Name	The name of the SIEM server.
Address	The IP address of the SIEM server.
Port	The UDP Syslog port used by CEF.
Report time interval	The frequency with which to update the SIEM server with compliance information. If a compliance event occurs before this time period elapses, a message is sent. CounterACT reports the compliance status of each endpoint both periodically and whenever this status changes.

Comment	Comments regarding the server.

4. Select **Next**. The Assigned CounterACT Devices pane opens.



5. Do one of the following:
   - Select **Default Server** to designate this server as the default server. The default server handles all CounterACT devices that are not assigned to an SIEM server.
   - Select **Assign CounterACT Devices** to assign specific CounterACT devices to this server. You can later define another server to function as the default.
6. Select **Finish**. The server configuration appears in the CEF pane.



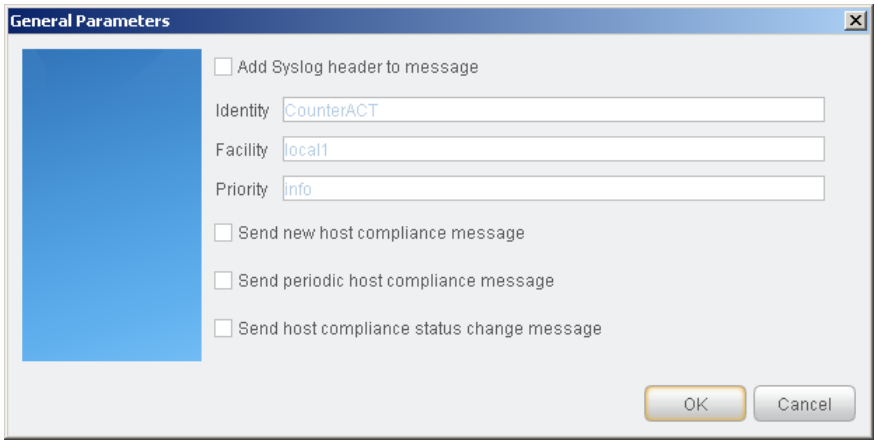
7. Use **Add / Edit / Remove** to manage the CEF configurations.

Include Syslog Message Header

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

To include syslog message headers in CEF messages:

1. Select the **Options** from the CEF pane. The General Parameters dialog box opens.

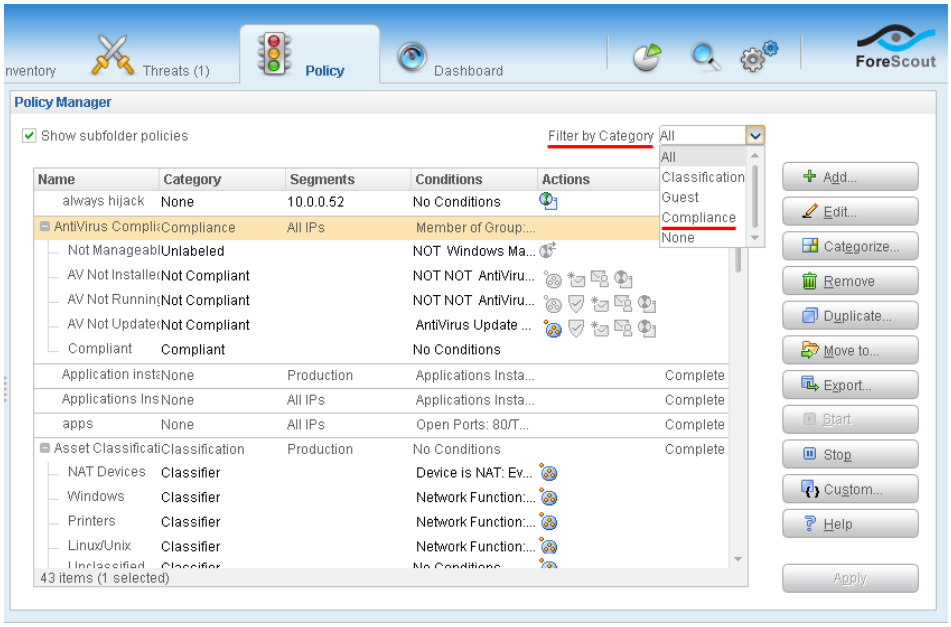


2. Select **Add Syslog header to message** and define the following fields.

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)

Automatically Report CounterACT Compliance Status

CounterACT policy categories help you logically organize and view policies. Policies categorized as *Compliance* policies are evaluated for automated CEF messaging.

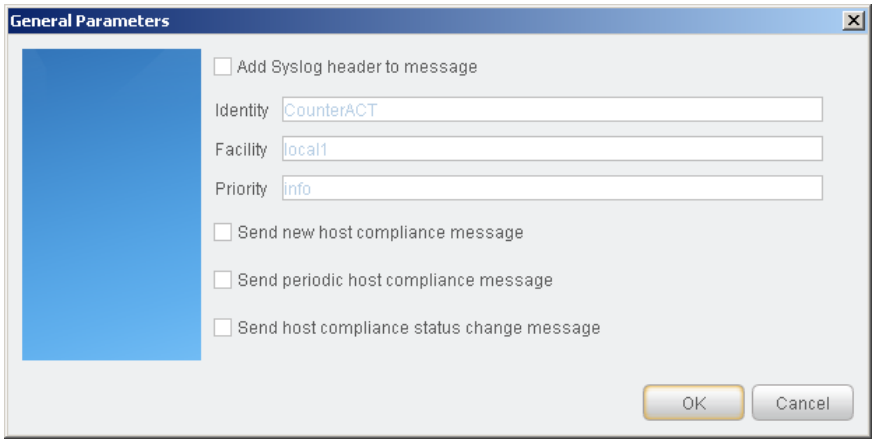


With this plugin, CounterACT can automatically report general host compliance status based on the *Compliance Status* host property in CounterACT. This property indicates whether a host satisfies the set of compliance policies defined in CounterACT. Refer to the *Policy Management* chapter in the *Console User Guide* for more information about compliance policies.

Automatic messaging implements the Send Compliant CEF message action and the Send Not Compliant CEF message action described below. Refer to these actions for details of the message formats used.

To configure automatic reporting of coverall compliance status:

1. Select the **Options** from the CEF pane. The Edit General Parameters dialog box opens.



2. Select **Send new host compliance message** to send a compliance message when a new host is resolved as *compliant* by all Compliance policies, or *not compliant* by *any* Compliance policy. This feature is useful if you want to globally send compliance messages, regardless of policy definitions.

3. Select **Send periodic host compliance message** to periodically report compliance status for all hosts within the scope of Compliance policies. The frequency of these reports is determined by the **Report Time Interval** field of the SIEM Server configuration.

   For each host, CounterACT issues a CEF message for each policy that includes the host in its scope. For example, if four compliance policies include the host, and the host complies with two of these policies and is non-compliant with the other two, CounterACT sends two *Compliant* messages and two *Not Compliant* messages.

4. Select **Send host compliance status change message** to send a compliance message when the *total host compliance status* has changed for a host.

Create Custom CEF Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, use the policy to instruct CounterACT 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.

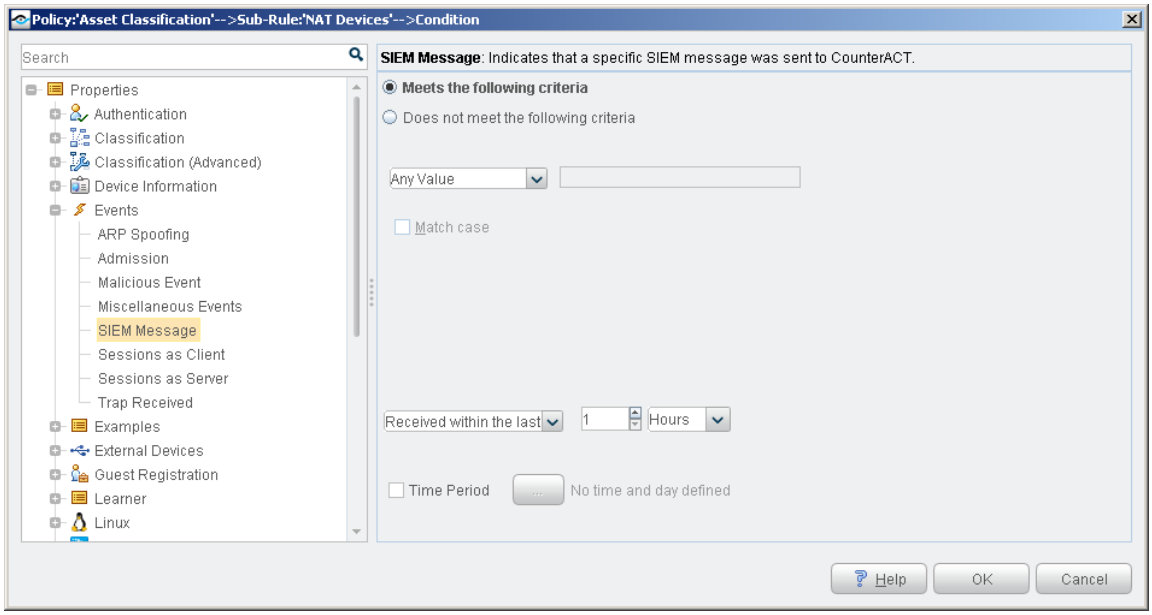
To create a custom policy:

1. Log in to the CounterACT Console.
2. Select the **Policy** icon from the Console toolbar.
3. Create or edit a policy.

Receiving SIEM Messages – Policy Properties

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

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



To access properties:

1. Navigate 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 CounterACT actions. For example, you can configure a CounterACT policy to assign hosts to a specific VLAN when the message *VulnerabilityDetected* is sent by the SIEM server.

This option is available for users working with CounterACT version 6.3.4.10 and above.

To set up this functionality:

- Define a CounterACT 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 CounterACT with the desired message string.

When SIEM server logic generates an alert or remediation condition:

1. The SIEM server sends the predefined message to CounterACT.
2. CounterACT parses the message and stores the message text in the SIEM Messages property of the relevant host.
3. The CounterACT policy detects hosts by matching values in the SIEM Messages property.
4. CounterACT implements the actions defined in the policy.
5. The SIEM Message event appears in the CounterACT 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 CounterACT. When CounterACT 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 CounterACT:

`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 CounterACT to implement.

`<IPAddress>` identifies the host on which the action is performed. CounterACT 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 CounterACT:

`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. CounterACT 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 CounterACT:

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

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

Sending CEF Messages – Policy Actions

CounterACT policy actions let you instruct CounterACT 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 CounterACT actions available for handling endpoints, you can work with the plugin related actions to create custom policies. These actions are available when you install the plugin.

To access actions:

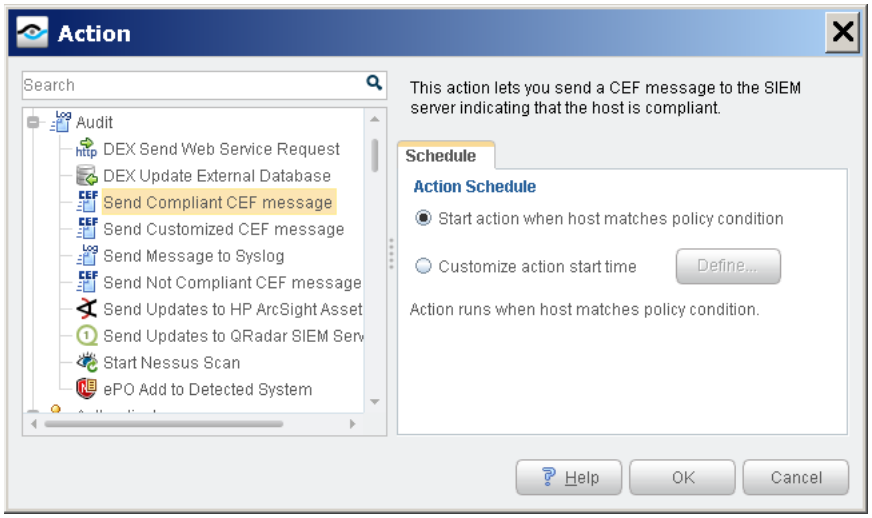
1. Navigate to the Actions tree from the Policy Actions dialog box.
2. Expand the **Audit** folder in the Actions tree. The following actions are available:
   - Send Compliant CEF message
   - Send Customized CEF Message
   - Send Not Compliant CEF message

Send Compliant CEF message

This action sends a CEF message to the SIEM server for each host that satisfies 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 CounterACT. 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

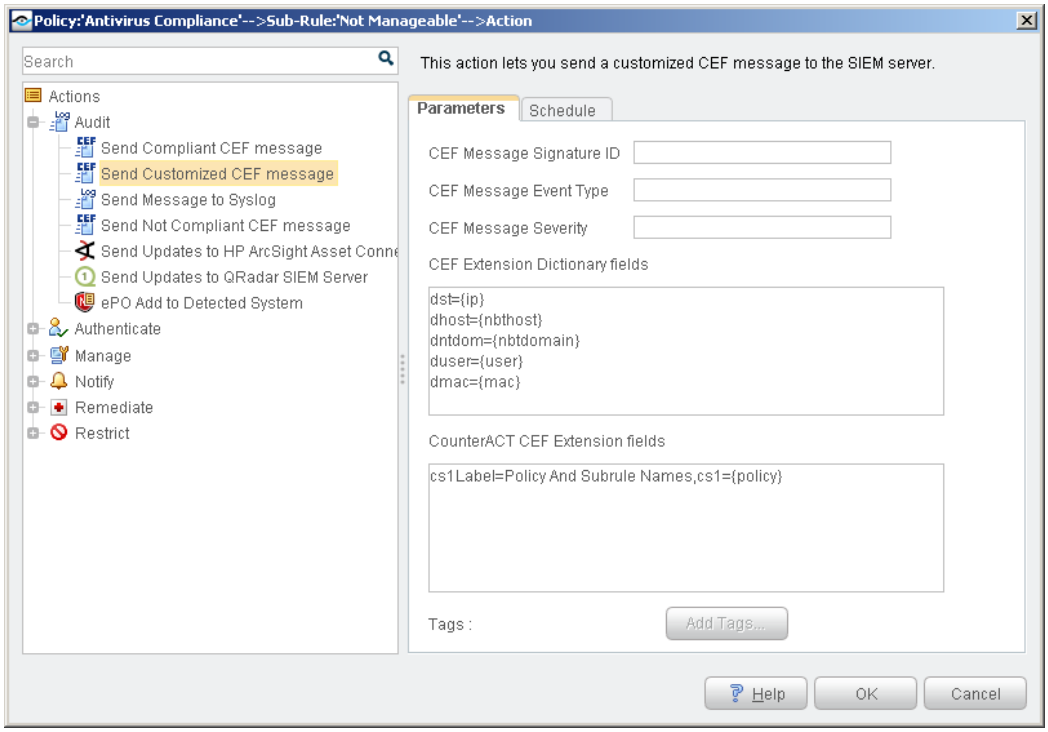
This action sends a customized CEF message to the SIEM server for each host that satisfies the conditions of the policy.

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, open the Audit group and select the **Send CEF message** action.



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

   CounterACT automatically adds vendor-specific fields to the final message header.

4. (Optional) Click in the **CEF Extension Dictionary fields** area to edit the list of dictionary fields that is 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) Click in the **CounterACT CEF Extension fields** area to define CounterACT-specific fields that are 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.

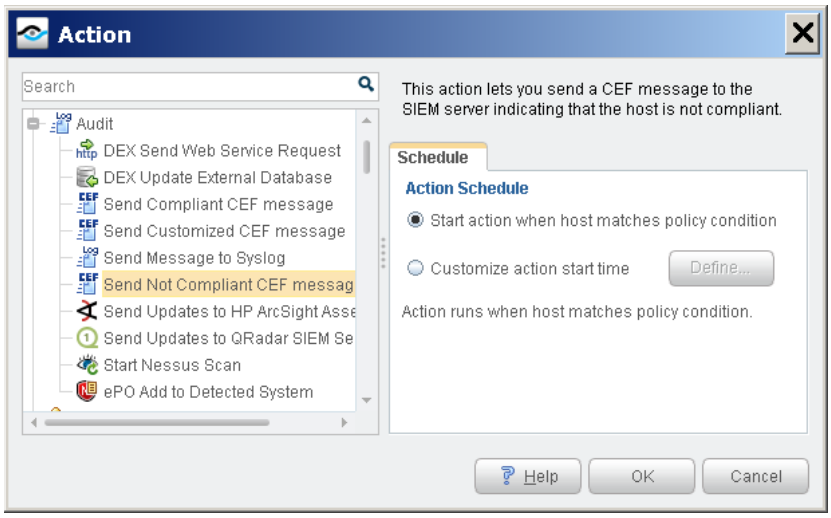
7. Select **OK** to add the action to the policy.

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 CounterACT. 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 CounterACT event definitions.

CEF Event Data Field	Data Field Meaning	CounterACT 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	CounterACT 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

CounterACT Extension Fields

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

CEF Event Data Field ID	Data Field Label	CounterACT Host Property	Values
cs1	Compliancy Policy Name	Compliancy Policy Name	CounterACT 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

CEF Event Data Field ID	Data Field Label	CounterACT Host Property	Values
cs3	Host Compliancy Status	Host Compliance Status	▪ Yes: For compliant host ▪ No: For non-compliant host
cs4	Compliancy Event Trigger	Compliancy Event Trigger	▪ New host: For newly discovered host ▪ Compliancy status changed: For a host whose status changed ▪ Periodical: When host status is unchanged within 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

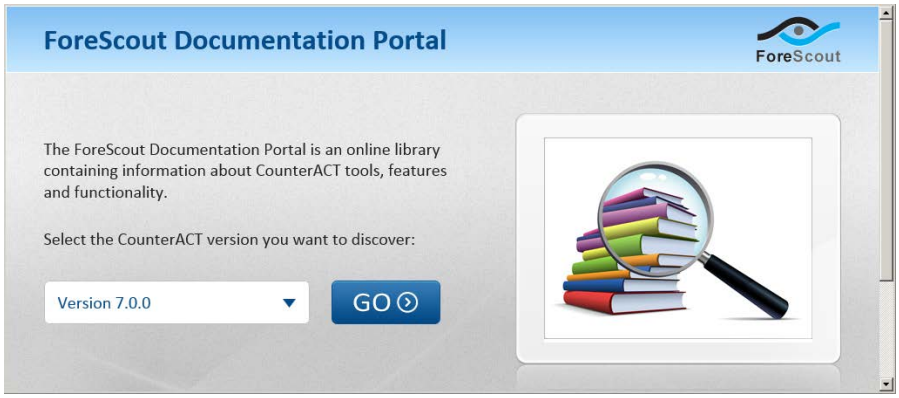
Additional CounterACT Documentation

For more detailed information about the CounterACT features described here or additional CounterACT features and plugins, refer to the following resources:

- Documentation Portal
- Customer Support Portal
- CounterACT Console Online Help Tools

Documentation Portal

The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features and functionality and integrations.



To access the Documentation Portal:

1. Go to www.forescout.com/kb.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:

1. Go to https://updates.forescout.com/support/index.php?url=counteract.
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

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

Console User Manual

1. Select **CounterACT Help** from the **Help** menu.

Plugin Help files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Plugins**.
2. Select the plugin and then select **Help**.

Documentation Portal

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

Legal Notice