How to- Configure ForeScout CounterAct to forward logs to EventTracker

EventTracker v9.0 and Above

Publication Date: June 13, 2019

Abstract

This guide provides instructions to configure ForeScout CounterAct to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor the network access control.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and ForeScout CounterAct v8.0.

Audience

IT Admins, ForeScout CounterAct administrator, and EventTracker users who wish to forward logs to EventTracker and monitor events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Overview

ForeScout CounterAct gives you network access control. It maintains the policies and network configuration and deploys them to the ForeScout CounterACT appliances.

ForeScout CounterAct can be integrated with EventTracker using syslog. With the help of ForeScout CounterAct KP items, we can monitor the network access control activities, malicious process and mail infection on applications and also trigger the alert whenever any malicious process is running, and mail infection is detected. EventTracker dashboard will help you to visualize the web activities on applications. It can even create the report that helps to collect user activities happening in the applications for a time interval. This will help you to review the different malicious and network activities. EventTracker CIM will help you to correlate from network access control activities, malicious process, and mail infection, etc.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **ForeScout CounterAct v8.0** or latest version should be installed.
- **ForeScout CounterAct core extension module Syslog plugin v3.5** should be installed**.**

Configuring ForeScout CounterAct syslog

Syslog plugin Configuration

This section describes how to configure the syslog plugin. There are two types of messages that you can send to syslog:

- Sending ForeScout event messages.
- Using actions to send endpoint messages.

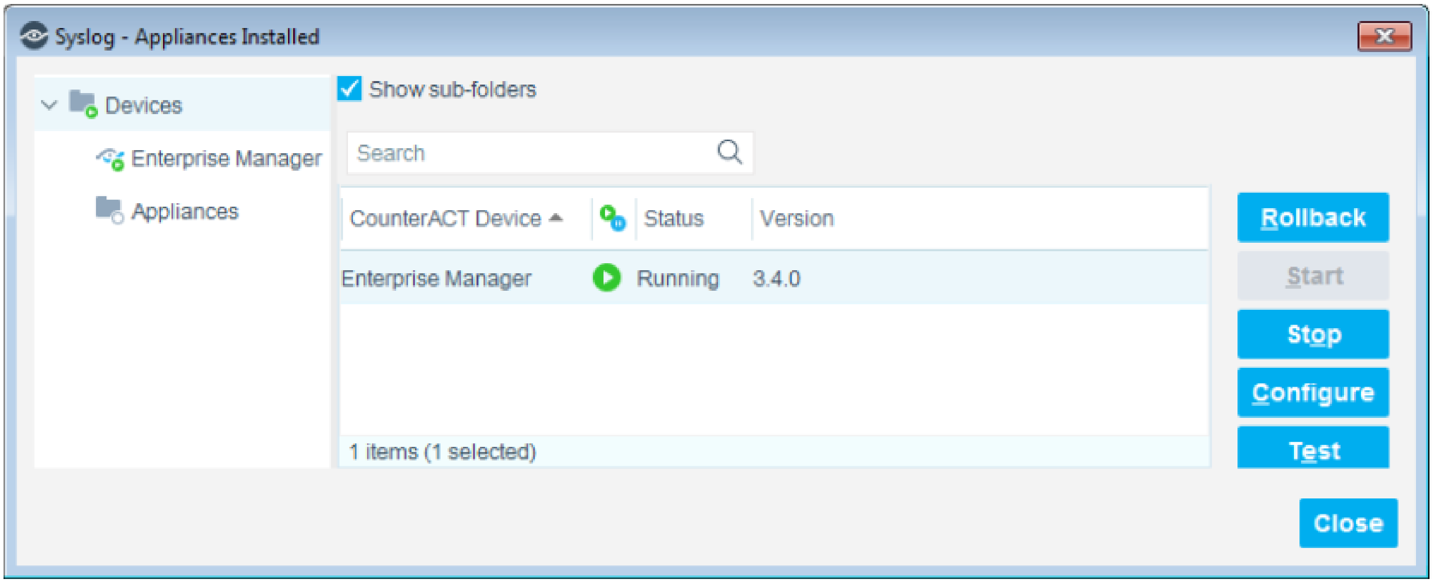
Sending ForeScout event messages

Select an Appliance to Configure:

This section describes how to configure the plugin to ensure that the CounterACT device can properly communicate with syslog servers.

Configuring the syslog plugin:

1. In the Modules pane, select **Core Extensions >Syslog** and then select **Appliances**. The syslog - Appliances installed dialog box opens.

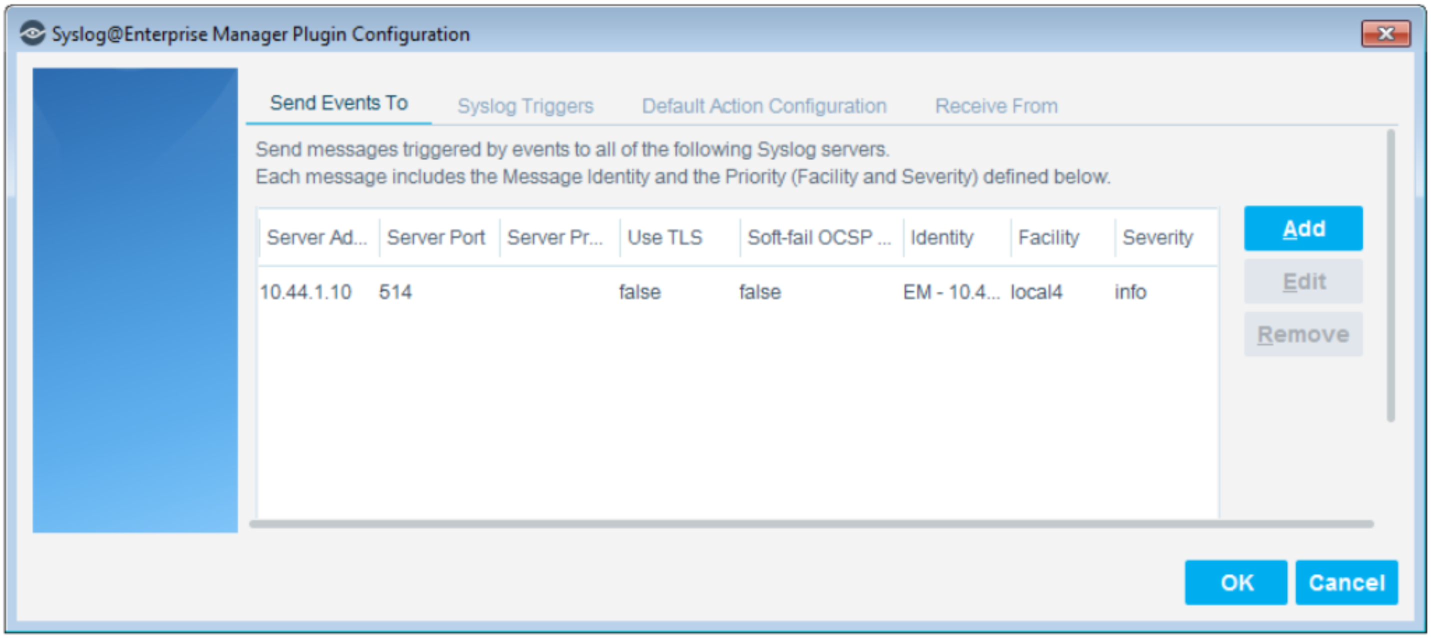


CounterACT Device		Status	Version
Enterprise Manager	●	Running	3.4.0

1 items (1 selected)

Figure 1

2. Select any appliance or the **Enterprise Manager** and select **Configure**. You cannot configure multiple CounterACT devices simultaneously. The Configuration dialog box opens. Need to configure send events to, syslog triggers, default action configuration for sending logs to the EventTracker.


Syslog@Enterprise Manager Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From
Add
Edit
Remove
OK
Cancel

Send messages triggered by events to all of the following Syslog servers.
Each message includes the Message Identity and the Priority (Facility and Severity) defined below.

Server Ad...	Server Port	Server Pr...	Use TLS	Soft-fail OCSP ...	Identity	Facility	Severity
10.44.1.10	514		false	false	EM - 10.4...	local4	info

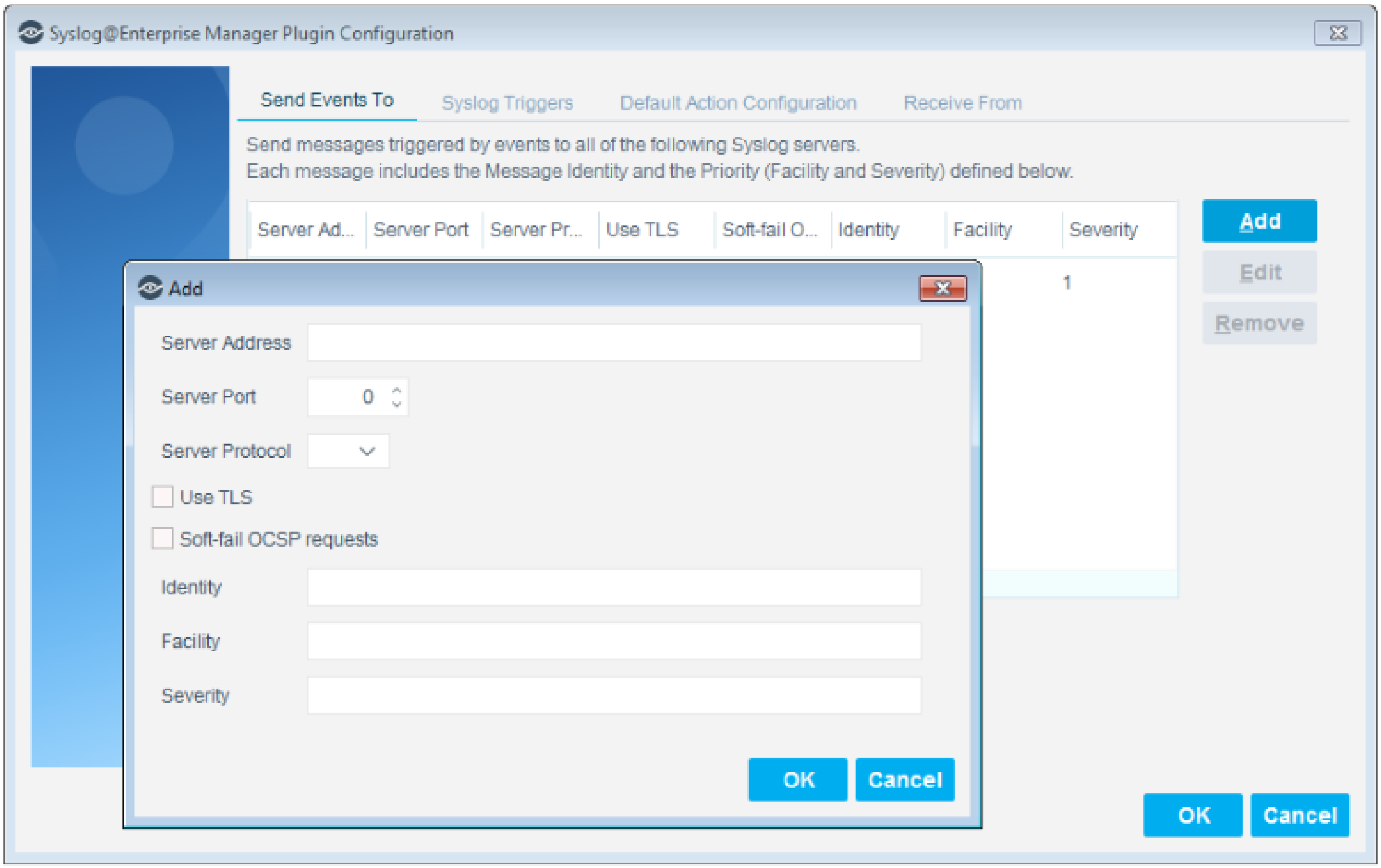
Figure 2

3. When the configuration is complete, select **ok**.

Send Events To:

The **Send Events To** tab lists the syslog servers to which the CounterACT device will send messages regarding the event types selected in the syslog triggers tab. For each syslog server, define:

1. In the **Send Events Total**, do one of the following:
    - To define a syslog server not in the table, select **Add**.

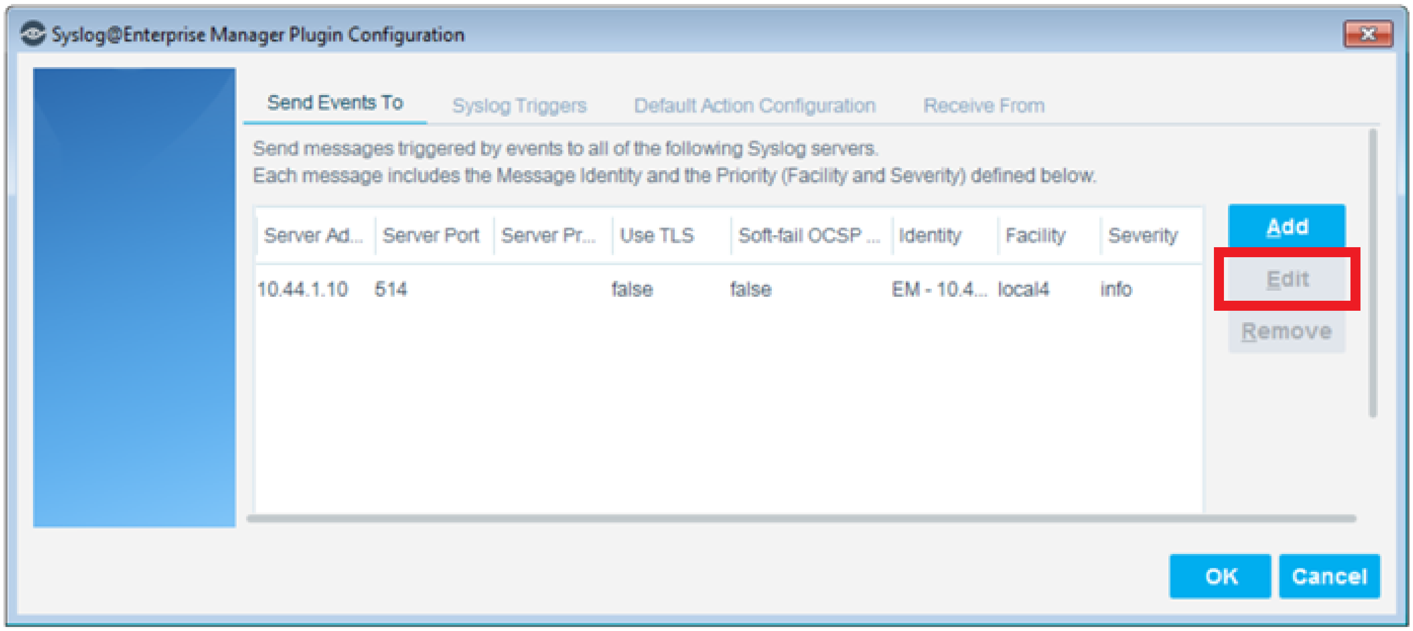


Send messages triggered by events to all of the following Syslog servers.
Each message includes the Message Identity and the Priority (Facility and Severity) defined below.

Server Address
Server Port 0
Server Protocol
☐ Use TLS
☐ Soft-fail OCSP requests
Identity
Facility
Severity

Figure 3

- To modify the definition of an existing server, select it in the table and select **Edit**.


Syslog@Enterprise Manager Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From
Add
Edit
Remove
OK
Cancel

Send messages triggered by events to all of the following Syslog servers.
Each message includes the Message Identity and the Priority (Facility and Severity) defined below.

Server Ad...	Server Port	Server Pr...	Use TLS	Soft-fail OCSP ...	Identity	Facility	Severity
10.44.1.10	514		false	false	EM - 10.4...	local4	info

Figure 4

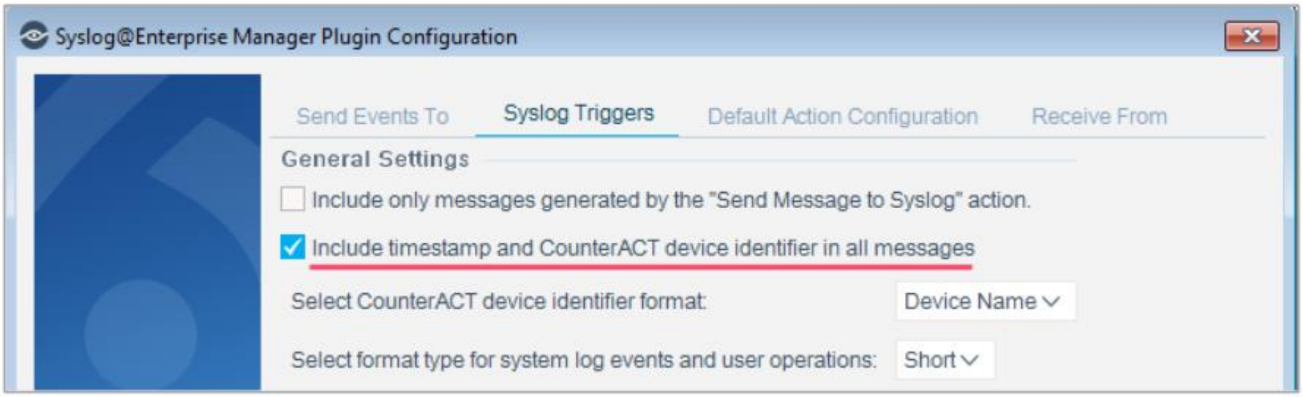
2. Specify the following information for the server:
   - **Server Address**: Provide EventTracker installed host IP address.
   - **Server Port**: Provide syslog (default 514) port.
   - **Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this syslog server.
   - **Identity**: Free-text field for identifying the syslog message.
   - **Facility**: (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local5**.
   - **Severity**: Mention severity as **Info.**
3. Select OK. The updated server definition appears in the table.

Syslog Triggers:

Configure the settings in the syslog triggers tab.

Syslog messages can be generated by Forescout platform policies when endpoints meet conditional criteria.

1. Select “**Include timestamp and CounterACT device identifier in all messages”.**


Syslog@Enterprise Manager Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From

General Settings

□ Include only messages generated by the "Send Message to Syslog" action.

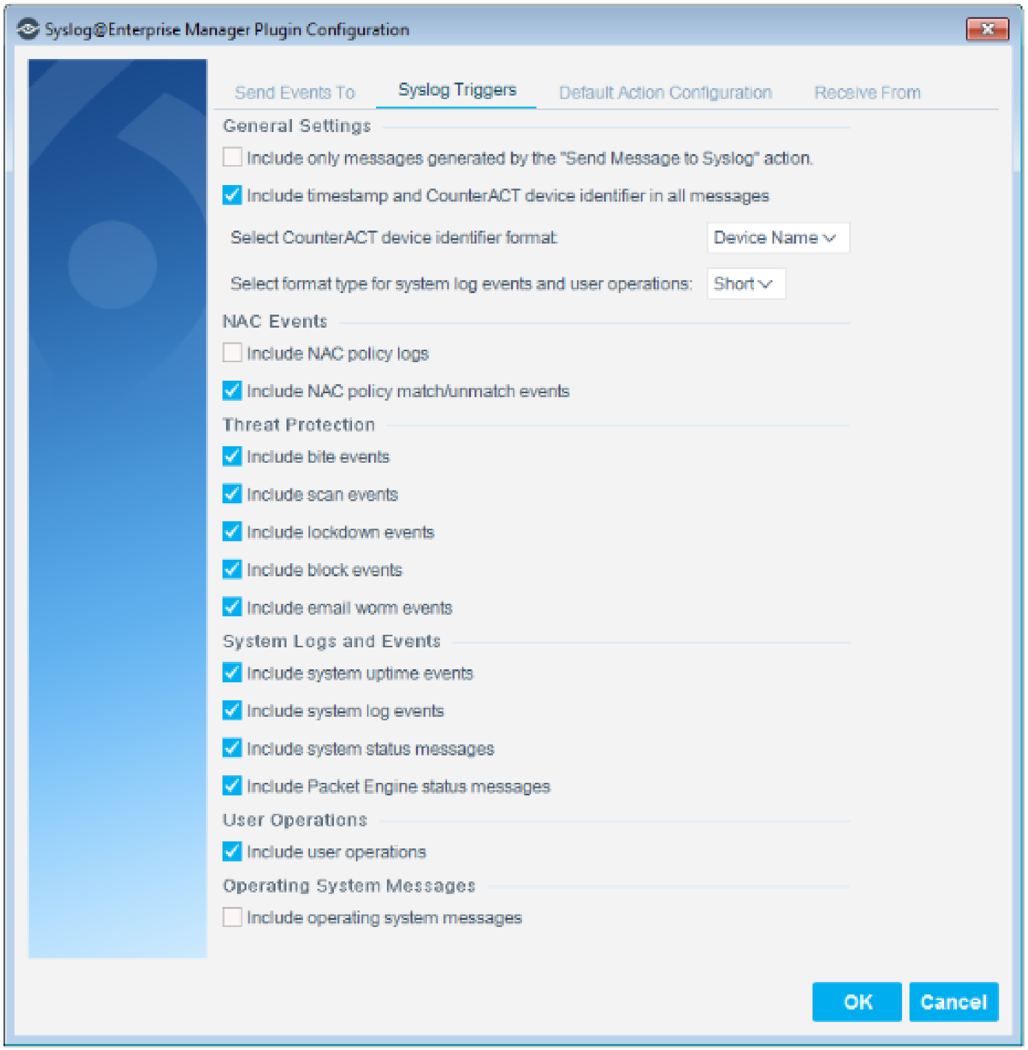
☑ Include timestamp and CounterACT device identifier in all messages

Select CounterACT device identifier format: Device Name

Select format type for system log events and user operations: Short

Figure 5

2. Select options in the tab to define which event types trigger syslog messages. Follow below screenshot and click ok.


Syslog@Enterprise Manager Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From
OK
Cancel

General Settings

□ Include only messages generated by the "Send Message to Syslog" action.

☑ Include timestamp and CounterACT device identifier in all messages

Select CounterACT device identifier format: Device Name

Select format type for system log events and user operations: Short

NAC Events

□ Include NAC policy logs

☑ Include NAC policy match/unmatch events

Threat Protection

☑ Include bite events

☑ Include scan events

☑ Include lockdown events

☑ Include block events

☑ Include email worm events

System Logs and Events

☑ Include system uptime events

☑ Include system log events

☑ Include system status messages

☑ Include Packet Engine status messages

User Operations

☑ Include user operations

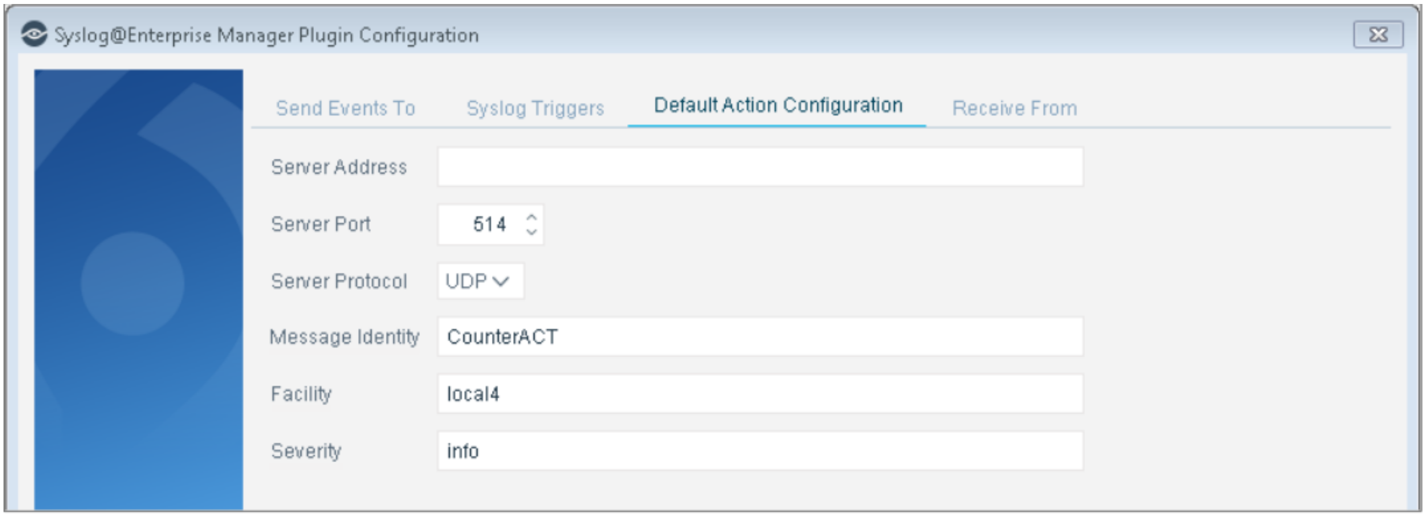
Operating System Messages

□ Include operating system messages

Figure 6

Default Action Configuration:

The Default Action Configuration tab allows you to define default values for the **Send Message** to syslog action parameters. These default values are applied to parameters that are not defined in policies. View Send Message to syslog action for details.


Syslog@Enterprise Manager Plugin Configuration
Send Events To
Syslog Triggers
Default Action Configuration
Receive From

Server Address:
Server Port: 514
Server Protocol: UDP
Message Identity: CounterACT
Facility: local4
Severity: info

Figure 7

Specify the following values:

1. **Server Address**: Mention EventTracker installed host IP address.
2. **Server Port**: Mention syslog server(default 514) port.
3. **Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
4. **Message Identity**: Free-text field for identifying the syslog message.
5. **Facility**: (Optional) Syslog message facility that is transmitted as part of the message priority field. If the facility value is not mentioned, it is set to **local5**.
6. **Severity**: Mention severity as **Info.**

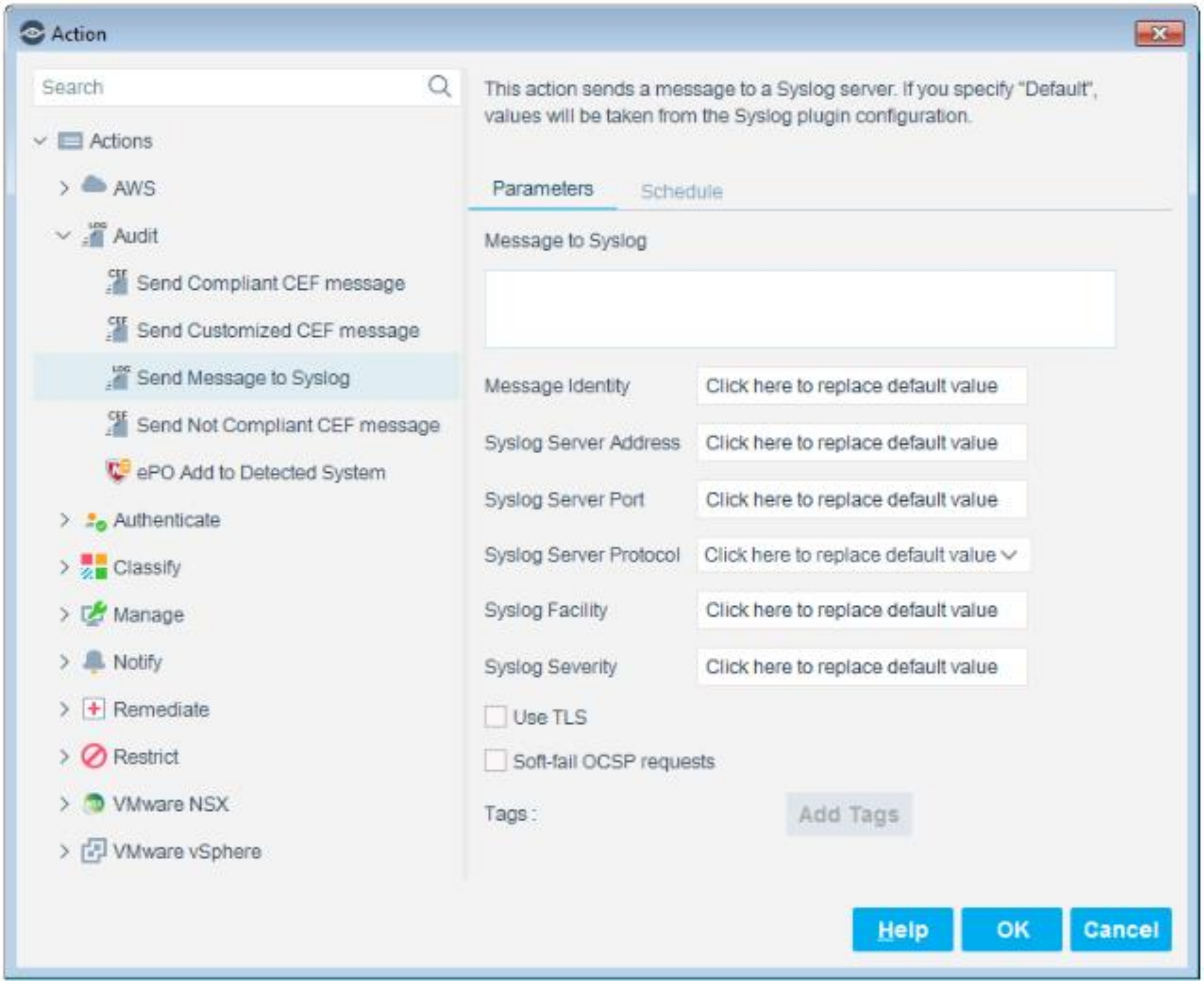
Using actions to send endpoint messages

Send Message to syslog:

The Send Message to syslog action is used by the syslog plugin to send a message to the syslog server. This message overrides syslog plugin configuration options.

1. In the **Policy Manager**, select a policy and select **Edit**. The **Policy Properties** dialog box opens.
2. Next to the **Main Rule** section select **Edit**. The Policy Conditions dialog box opens.
3. Next to the **Actions** section select **Add**. The Action dialog box opens.
4. In the left pane expand the Audit folder.

5. Select **Send Message to syslog**.



This action sends a message to a Syslog server. If you specify "Default", values will be taken from the Syslog plugin configuration.

Message to Syslog

Message Identity	Click here to replace default value
Syslog Server Address	Click here to replace default value
Syslog Server Port	Click here to replace default value
Syslog Server Protocol	Click here to replace default value
Syslog Facility	Click here to replace default value
Syslog Severity	Click here to replace default value

□ Use TLS

□ Soft-fail OCSP requests

Tags :

Figure 8

6. Specify the following or use **Default** where applicable to apply the default configuration.

- **Message to syslog**: Type a message to send to the syslog server when the policy is triggered.
- **Message Identity**: Free-text field for identifying the syslog message.
- **Syslog Server Address**: Provide EventTracker installed host IP address.
- **Syslog Server Port**: Set syslog port number (default is 514).
- **Syslog Server Protocol**: Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
- **Syslog Facility:** (Optional) Syslog message facility that is transmitted as part of the message Priority field. If the facility value is not mentioned, it is set to **local**.
- **Syslog Priority:** Mention severity as **Info.**
  Tags: Mention tag as ForeScout CounterAct.