



ForeScout

CounterACT[®] Syslog Plugin

Configuration Guide

Version 3.2.1

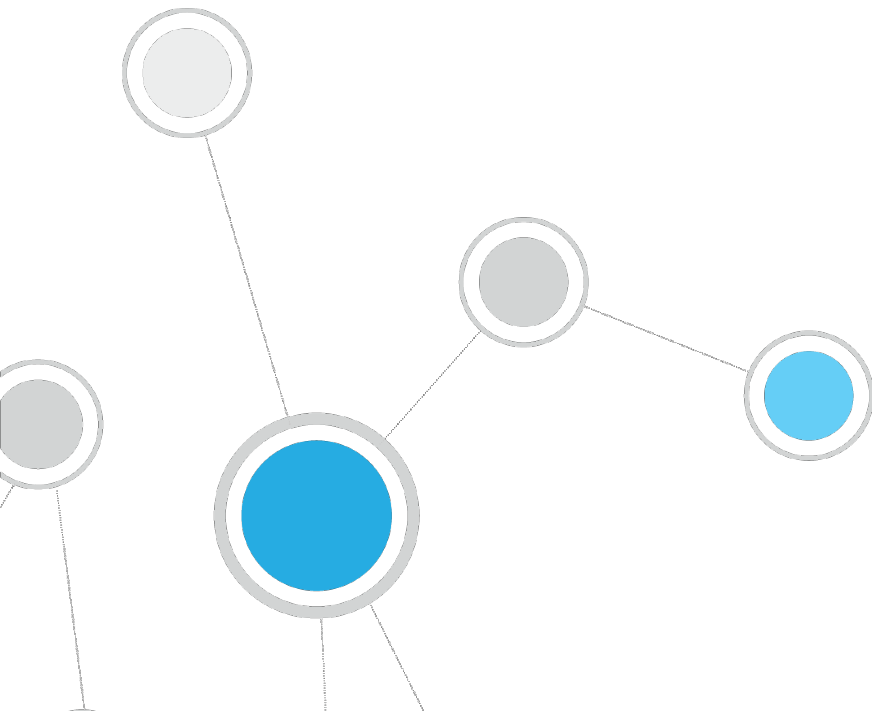


Table of Contents

About the Syslog Plugin	3
Multiple Destination Syslog Server Support.....	3
Receiving Event Messages	3
Sending Syslog Messages.....	4
Sending CounterACT Event Messages.....	4
Using Actions to Send Endpoint Messages	4
Open Integration with ControlFabric Technology.....	4
Requirements	5
Installation and Configuration	5
Installation	5
Configuration.....	6
Send Events To	6
Syslog Triggers	9
Default Action Configuration	13
Receive From.....	14
Testing the Configuration	15
Downloading and Configuring NTSyslog.....	16
Create Custom Syslog Policies.....	18
Send Message to Syslog Action	19
Working with Property Tags	20

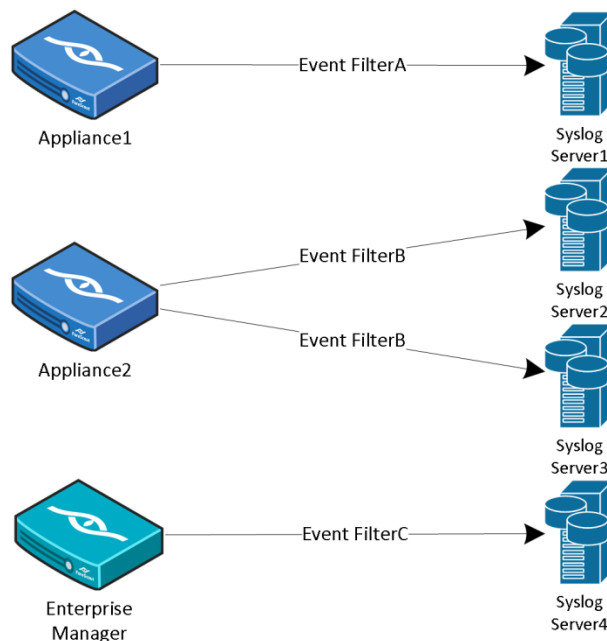
About the Syslog Plugin

The Syslog Plugin lets you send, receive and format messages to and from external Syslog servers. You can configure each CounterACT device to:

- Send all event messages to one or more Syslog servers.
- Receive messages from up to three manually configured Syslog servers.

Multiple Destination Syslog Server Support

The following diagram provides an example of communication from CounterACT devices to Syslog servers.



Receiving Event Messages

Receiving event messages from external Syslog servers allows CounterACT to gain visibility into events that cannot be obtained from analyzing traffic either because:

- Traffic is not visible to any of the deployed CounterACT Appliances.
- Traffic is encrypted.

Login events are recorded on Windows Domain Controllers. When these events are received by the Syslog Plugin, CounterACT knows immediately if an endpoint has been authenticated to the Domain Controller and which User and Domain Name were used for authentication. CounterACT parses the received messages, and updates the relevant host properties. This information is displayed in the Profile tab of the Console Details pane.

To receive messages from external Syslog servers, configure the [Receive From](#) plugin configuration tab.

Sending Syslog Messages

Sending valuable information from CounterACT to one or more external Syslog servers allows the information to be used for event aggregation, auditing, and further processing. For a description of the contents of the different Syslog message types generated by CounterACT, refer to CounterACT Technical Notes: *Syslog Messages Sent by CounterACT*.

There are two types of messages that you can send to Syslog:

- [Sending CounterACT Event Messages](#)
- [Using Actions to Send Endpoint Messages](#)

Sending CounterACT Event Messages

You can configure the plugin to send ongoing messages about CounterACT system events from one CounterACT device to one or more Syslog servers using the configuration settings in the Syslog Plugin. See [Configuration](#).

Each CounterACT device receives unique event information from the network, and will only send events to Syslog that occurred within the network segment of the CounterACT device. This is important to consider when configuring which CounterACT devices send messages to Syslog servers.

CounterACT can be configured to send a message to the configured Syslog servers each time a new event of the following type occurs.

- [NAC Events](#)
- [Threat Protection](#)
- [System Logs and Events](#)
- [User Operations](#)
- [Operating System Messages](#)

Using Actions to Send Endpoint Messages

You can send customized messages to Syslog for specific endpoints using the *Send Message to Syslog* action, either manually or in CounterACT policies. Use the action to send messages based on policy results or at customizable intervals. See [Syslog Policy Actions](#).

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 Syslog 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](#).

Requirements

The following CounterACT products and software releases are required for the operation of this plugin:

- CounterACT version 7.0.0 and above

Installation and Configuration

This section describes how to install and configure the Syslog Plugin.

Installation

CounterACT is delivered with several bundled plugins, including this plugin.

New plugin functionality and supporting data may become available independently between major CounterACT version releases. This section describes how to install the plugin when a new plugin version becomes available between releases.

To install the plugin:

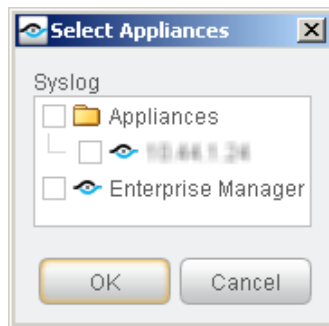
1. Navigate to the [Customer Support, Base Plugins](#) page and download the plugin `.fpi` file.
2. Save the file to the machine where the CounterACT Console is installed.
3. Log into the CounterACT Console and select **Options** from the **Tools** menu.
4. Select **Plugins**. The Plugins pane opens.
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.
9. Once the installation is complete, select **Close**. The plugin is listed in the Plugins pane.
10. Select the plugin and select **Start**. The Select Appliances dialog box opens.
11. Select the CounterACT Appliances on which to start the plugin. It is recommended to run the plugin on all Appliances in the environment.
12. Select **OK**. The plugin runs on the selected Appliances.
13. Select **Close**.

Configuration

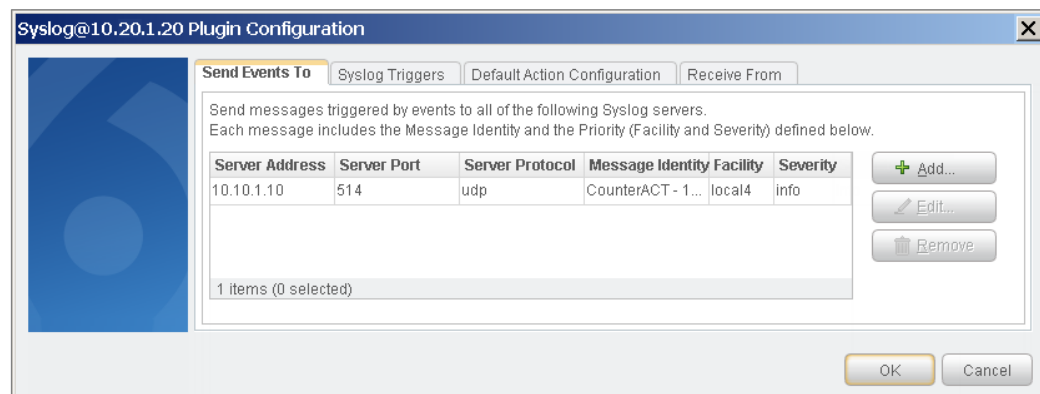
This section describes how to configure the plugin to ensure that the CounterACT device can properly communicate with Syslog servers.

To configure the Syslog Plugin:

1. In the Plugins pane, select **Syslog** and then select **Configure**. The Select Appliances dialog box opens.



2. Select any Appliance or the Enterprise Manager and select **OK**. You cannot configure multiple CounterACT devices simultaneously. The Configuration dialog box opens.

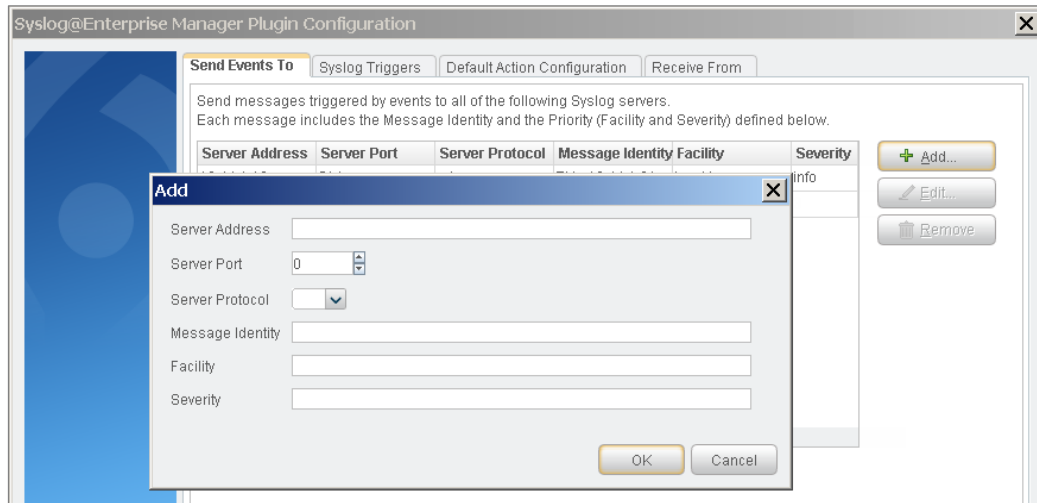


3. See the following sections to complete the information in each tab:
 - [Send Events To](#)
 - [Syslog Triggers](#)
 - [Default Action Configuration](#)
 - [Receive From](#)
4. When the configuration is complete, select **OK**.

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:

- the details CounterACT needs to communicate with the server
- the *Facility*, *Severity*, and *Message Identity* values to be included in all event messages



To configure CounterACT to send event messages to Syslog servers:

1. In the *Send Events To* tab, do one of the following:
 - To define a Syslog server not in the table, select **Add**.
 - To modify the definition of an existing server, select it in the table and select **Edit**.
2. Specify the following information for the server:

Server Address	Syslog server IP address or fully qualified domain name.
Server Port	Syslog server port.
Server Protocol	Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this Syslog server.
Message Identity	Free-text field for identifying the Syslog message.
Facility	Syslog message facility that is transmitted as part of the message Priority field. For valid values, see Facility Values .
Severity	Syslog message severity that is transmitted as part of the message Priority field. For valid values, see Severity Values .

3. Select **OK**. The updated server definition appears in the table.
4. (Optional) To delete a server, select it in the table and select **Remove**.

Facility Values

The Syslog message facility must be one of the values in the following table.

Facility Value	IETF Facility Description
kern	kernel messages
kernel	
user	user-level messages
mail	mail system
daemon	system daemons
system	
auth	security/authorization messages
syslog	messages generated internally by syslogd
internal	
lpr	line printer subsystem
printer	
news	network news subsystem
uucp	UUCP subsystem
cron	clock daemon
clock	
authpriv	security/authorization messages
security2	
ftp	FTP daemon
FTP	
NTP	NTP subsystem
audit	log audit
alert	log alert
clock2	clock daemon
local0	local use 0
local1	local use 1
local2	local use 2
local3	local use 3
local4	local use 4
local5	local use 5
local6	local use 6
local7	local use 7

If the facility value is not valid, it is set to **local5**.

Severity Values

The Syslog message severity must be one of the values in the following table.

Severity Value	IETF Severity Description
emergency	system is unusable
emerg	
alert	action must be taken immediately
critical	critical conditions
crit	
error	error conditions
err	
warning	warning conditions
notice	normal but significant condition
informational	informational messages
info	
debug	debug-level messages

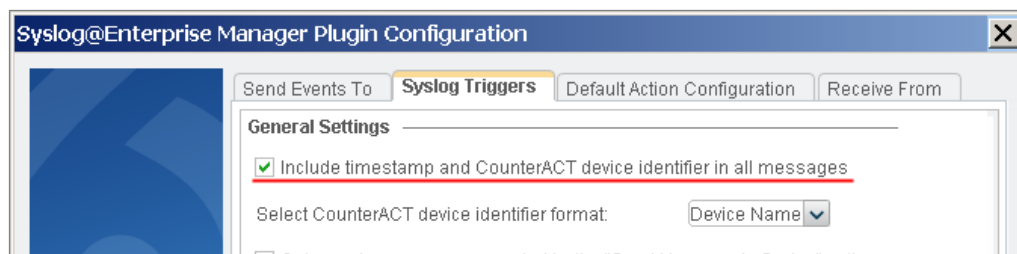
If the severity value is not valid, it is set to **error**.

Syslog Triggers

Configure the settings in the *Syslog Triggers* tab.

Including Header Information in All Message

The *Syslog Triggers* tab contains a setting that applies to all Syslog messages sent from the CounterACT device.



Select **Include timestamp and CounterACT device identifier in all messages** to include in all Syslog messages:

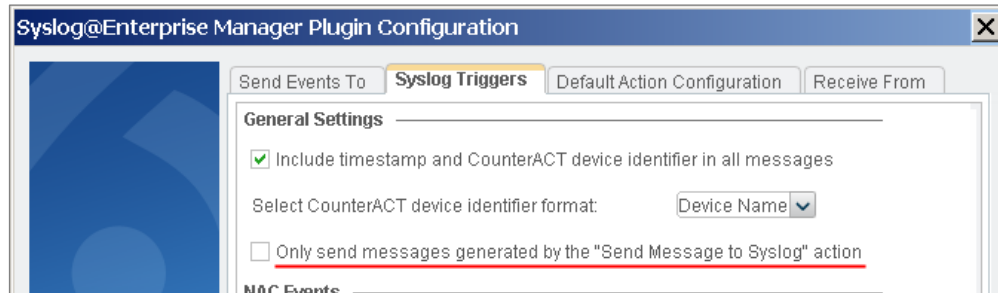
- a timestamp
 - the device name or IP address of the CounterACT device sending the message
- 📖 *If Device Name is selected but cannot be resolved, the CounterACT device IP address is included in its place.*

These fields comply with the RFC 3164 specification for BSD Syslog.

Selecting Syslog Message Triggers

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

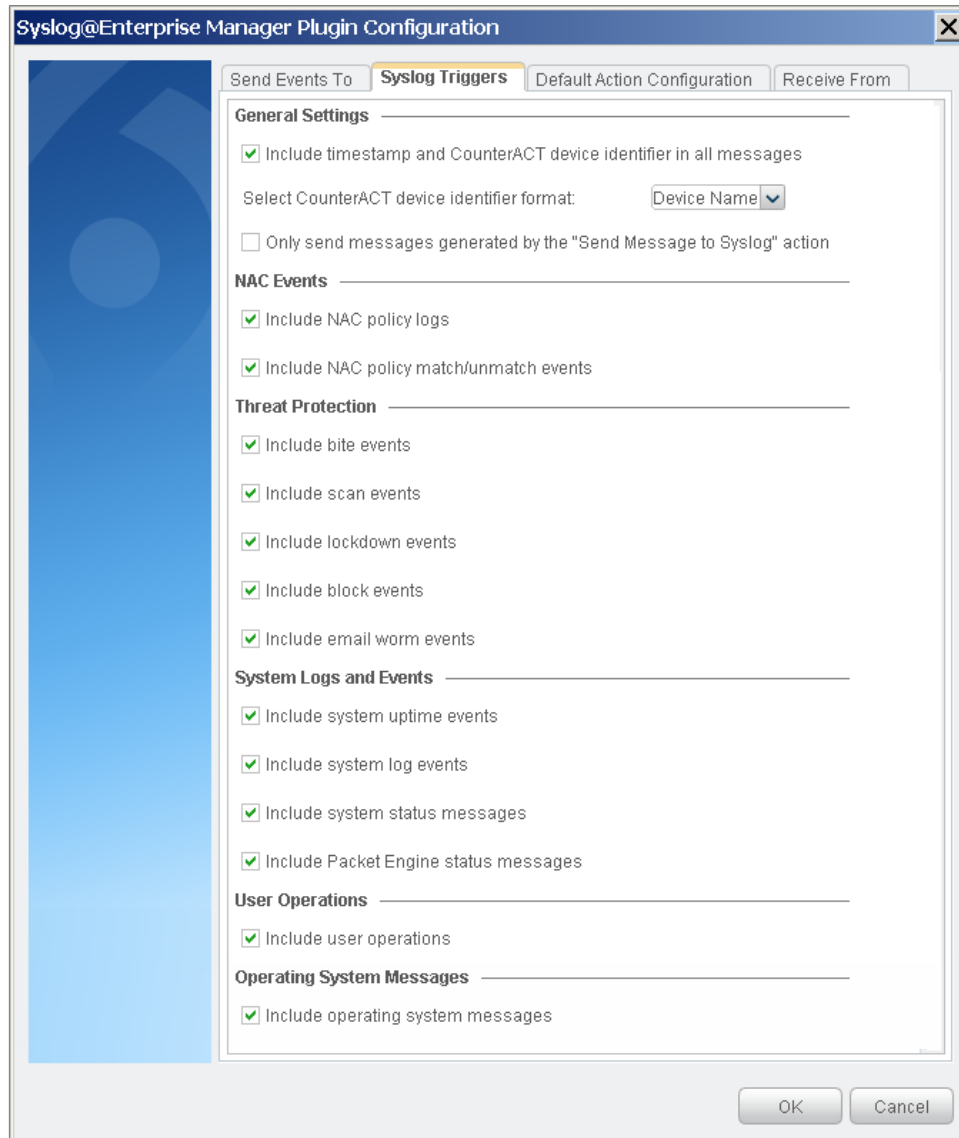
To enable Syslog messages to be generated by events and not only by policies, the **Only send messages generated by the "Send Message to Syslog" action** checkbox must *not* be selected.



If the **Only send messages generated by the "Send Message to Syslog" action** checkbox is not selected, you can select options in the tab to define which event types trigger Syslog messages.

You can select event triggers from the following categories:

- [NAC Events](#)
- [Threat Protection](#)
- [System Logs and Events](#)
- [User Operations](#)
- [Operating System Messages](#)



NAC Events

These event messages contain information on all policy event logs.

NAC policy logs	Endpoint policy events. The log displays information about endpoints as they are detected and is continuously updated as the policy is evaluated for the endpoint.
NAC policy match/unmatch events	Policy evaluation change events.

Threat Protection

These event messages contain information on intrusion-related activity, including bite events, scan events, lockdown events and manual events. These messages can be triggered when the Syslog Plugin runs on an Appliance but not when it runs on an Enterprise Manager.

Bite events	Indicates that an endpoint has tried to gain access to your network using a system mark.
Scan events	Indicates that an endpoint has performed a specific probe a defined number of times within a defined time period. By default, when an endpoint initiates three probes within one day, CounterACT considers this activity a scan.
Lockdown events	Indicates that a malicious event has been detected by another Appliance.
Block events	Indicates that CounterACT has blocked packets from the source from going through to the specified destination (host + service).
Email worm events	Indicates that CounterACT has identified email worm anomalies sent over email.

System Logs and Events

These event messages contain information about the CounterACT system events.

System uptime events	Indicates the amount of time the CounterACT service has been running.
System log events	Indicates certain CounterACT activities detected by the system. For example, successful and failed user login operations. (Messages sent to the Event Viewer)
System status messages	Indicates memory, swap and CPU usage statistics.
Packet Engine status messages	Indicates the status of the CounterACT service that monitors and injects SPAN port traffic. If it is down, many CounterACT features will not work.

User Operations

These event messages are generated when a user operation takes place, and they are included in the Audit Trail.

User operations	Indicates that the user made a configuration change such as updating policies, stopping or starting the device, or updating user passwords.
------------------------	---

Operating System Messages

These event messages are generated by the operating system.

Operating system messages	Indicates an event of relevance at the level of the operating system. This is useful, for example, if you want to monitor the health of an Appliance or Enterprise Manager by sending the events to a SIEM.
----------------------------------	---

Filter Operating System Messages by Severity

You can filter operating system messages sent by CounterACT to the Syslog server according to severity level.

To filter these messages:

1. Run the following command:

```
fstool set_property
config.oslog_severity_filter.value={severity_level}
```

For example, `fstool set_property config.oslog_severity_filter.value=crit`

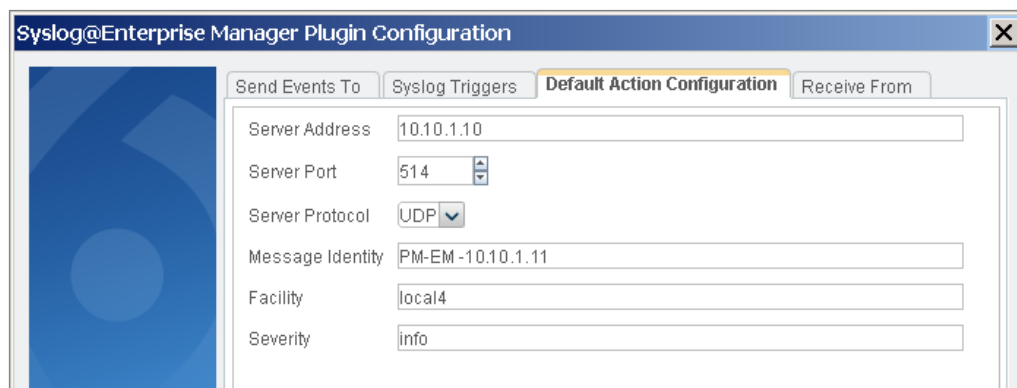
The following severity levels are available:

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

2. Restart the Syslog Plugin for the change to take effect.

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. See [Send Message to Syslog Action](#) for details.



Specify the following values:

Server Address	Syslog server IP address or fully qualified domain name.
Server Port	Syslog server port.

Server Protocol	Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this server.
Message Identity	Free-text field for identifying the Syslog message.
Facility	Syslog message facility that is transmitted as part of the message Priority field. For valid values, see Facility Values .
Severity	Syslog message severity that is transmitted as part of the message Priority field. For valid values, see Severity Values .

Receive From

This tab allows you to define:


- up to three Syslog agents from which the plugin may receive Syslog messages
- which ports the plugin will use to listen for messages being sent from the defined Syslog agents

The screenshot shows the 'Syslog@10.20.1.20 Plugin Configuration' dialog box with the 'Receive From' tab selected. The dialog has four tabs: 'Send Events To', 'Syslog Triggers', 'Default Action Configuration', and 'Receive From'. The 'Receive From' tab contains the following configuration options:

- 1st Syslog Source:** Source Type (dropdown menu with '<Select Type>' selected), IP Address (text field with '0 . 0 . 0 . 0').
- 2nd Syslog Source:** Source Type (dropdown menu with '<Select Type>' selected), IP Address (text field with '0 . 0 . 0 . 0').
- 3rd Syslog Source:** Source Type (dropdown menu with '<Select Type>' selected), IP Address (text field with '0 . 0 . 0 . 0').
- Ports for Incoming Syslog Messages:** UDP Port (spin box with '514'), TCP Port (spin box with '0').


At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

For each Syslog agent, define its source type and its IP address. Currently, the only source type supported is NTSyslog security log. You must download and configure NTSyslog on an organizational domain controller to work with the *Receive From* feature. See [Downloading and Configuring NTSyslog](#).

 *Received messages are not stored by CounterACT.*

To configure Syslog sources:

1. Select **NTSyslog security log** from the **Source type** field and enter the domain controller **IP address** for each source you list.
2. Enter the **UDP Port** and/or **TCP Port** used for listening for incoming Syslog messages.
 - By default, **UDP Port** is set to 514.
 - By default, **TCP Port** is set to 0 and is not used.

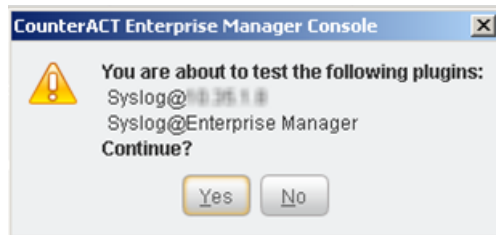
 *A port cannot be used for listening for Syslog messages when its value is set to 0.*

Testing the Configuration

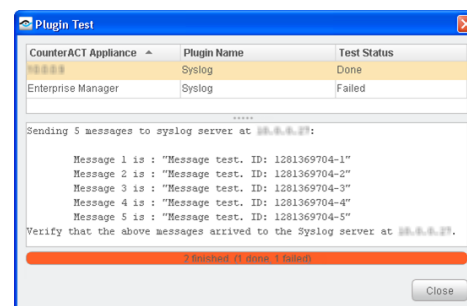
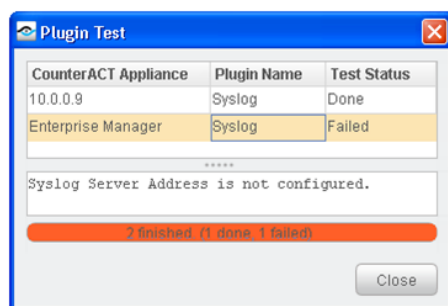
Use the test option to verify that CounterACT can communicate with the Syslog servers defined in the plugin configuration *Send Events To* tab.

To test the plugin configuration:

1. Select Syslog from the Plugin pane and then select **Test**. A confirmation message appears identifying CounterACT devices on which the test will be performed.



2. Select **Yes** to begin the plugin test. The Plugin Test dialog box displays information about each CounterACT device tested, as well as a number of test messages.



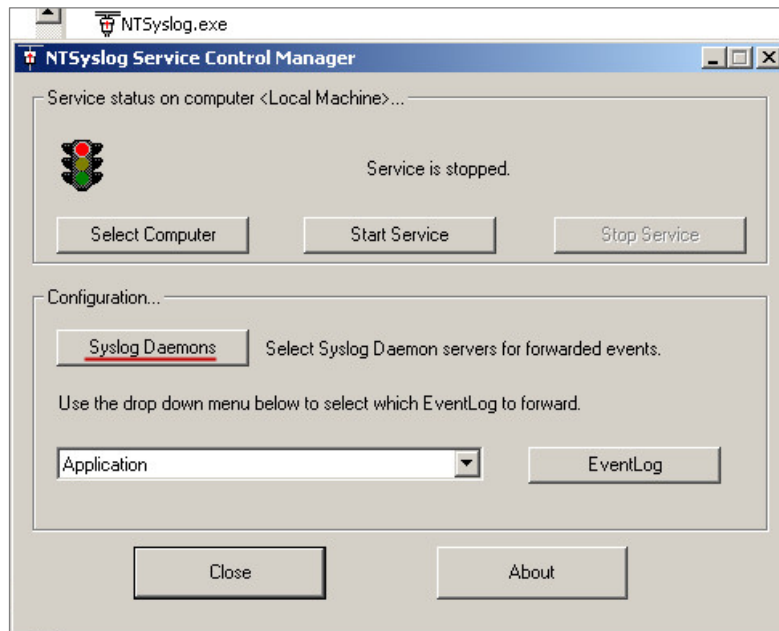
3. Verify that the Syslog servers received the messages displayed in the dialog box.

Downloading and Configuring NTSyslog

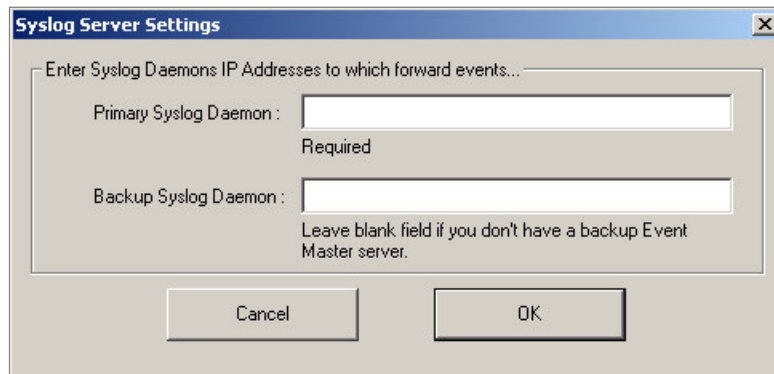
NTSyslog is a tool that sends Active Directory security logs to CounterACT if the Syslog Plugin is configured to receive messages. See [Receive From](#) to configure the plugin to receive messages.

To download and configure NTSyslog:

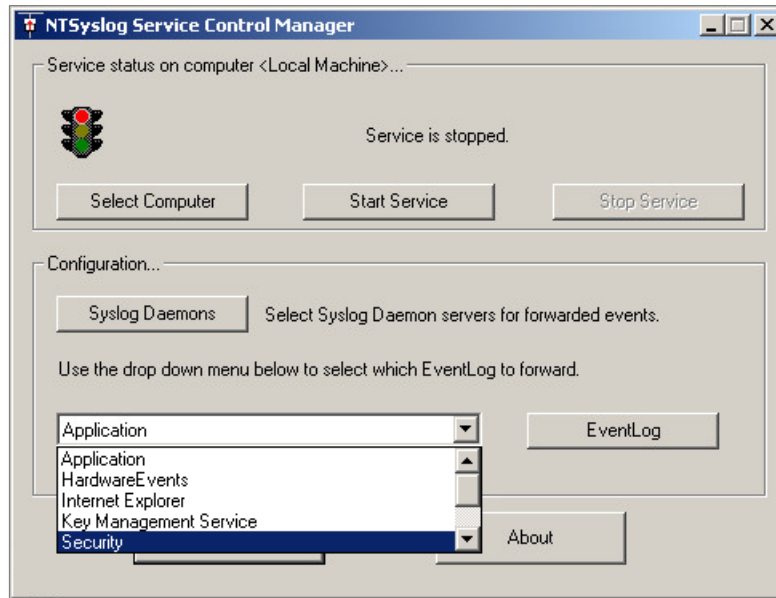
1. Install NTSyslog to your organizational Domain Controller. Use <http://sourceforge.net/projects/ntsyslog/> or download from another location.
2. Open the NTSyslog Service Control Manager.



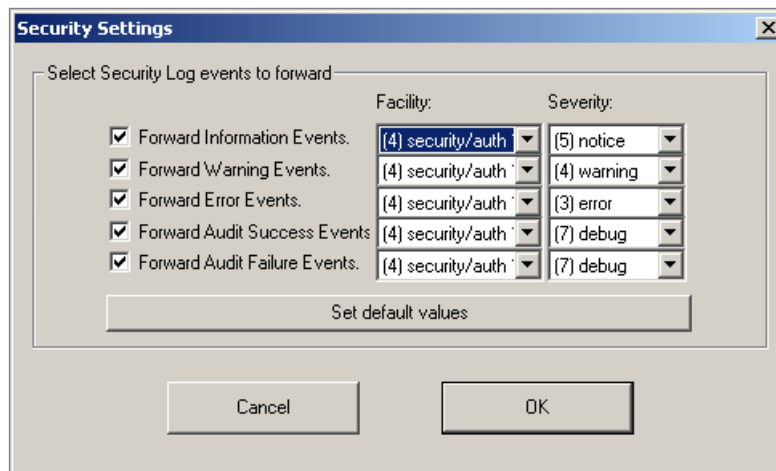
3. Select **Syslog Daemons**.



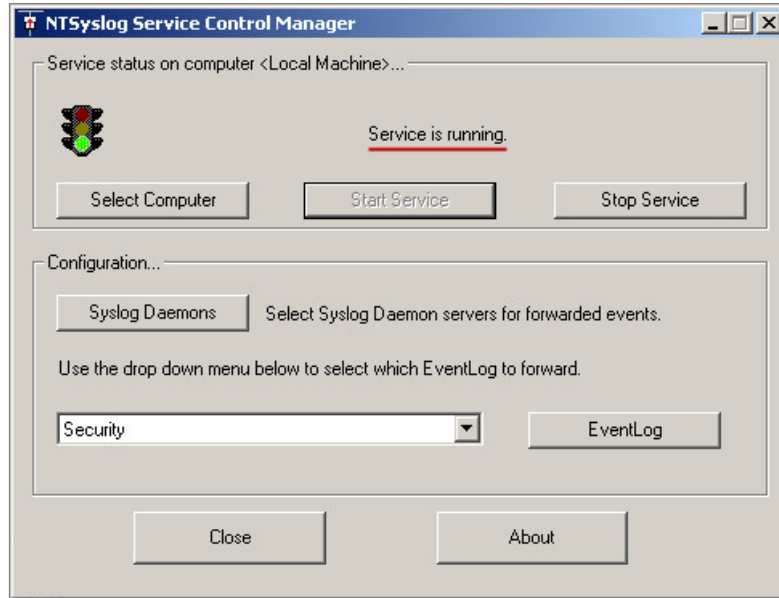
4. In the **Primary Syslog Daemon** field, enter the IP address of the CounterACT device to which traffic must be sent, and select **OK**.



5. In the NTSyslog Service Control Manager **EventLog** dropdown menu, select **Security**, and then select **EventLog**. Ensure that all events are selected.



6. Select **OK**.
7. Select **Start Service**, and verify that the *Service is running* message appears in the NTSyslog Service Manager dialog box.




Create Custom Syslog Policies

CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. You can use a policy to instruct CounterACT to apply the [Send Message to Syslog Action](#) to endpoints that match conditions based on reported endpoint properties.

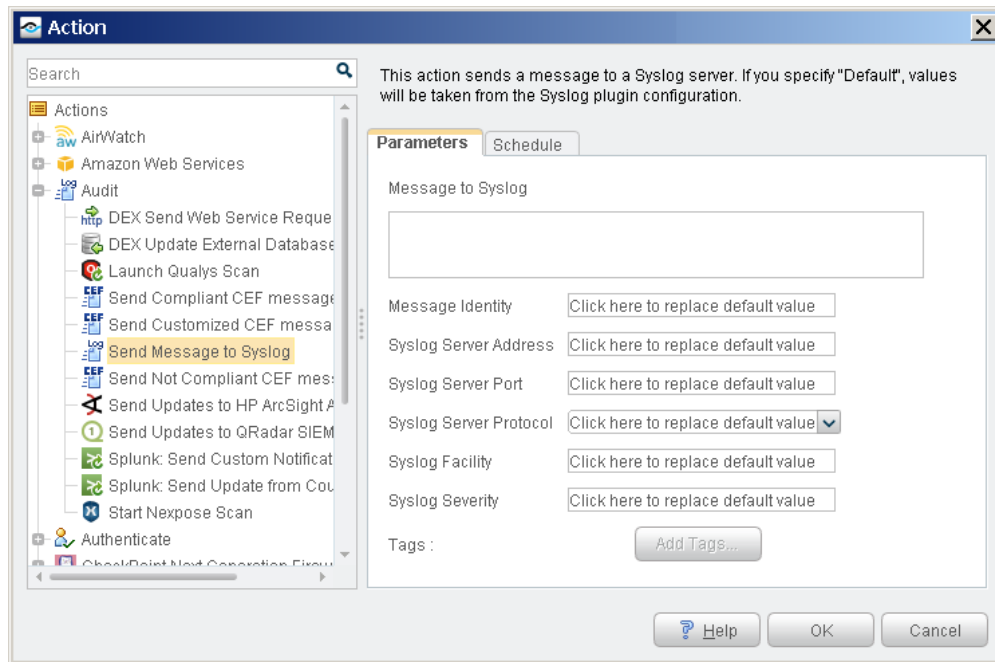
To create a custom policy:

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
3. Select **Add** to create a policy.

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

Send Message to Syslog Action

Use the *Audit, Send Message to Syslog* action to send a Syslog message to an external Syslog server.

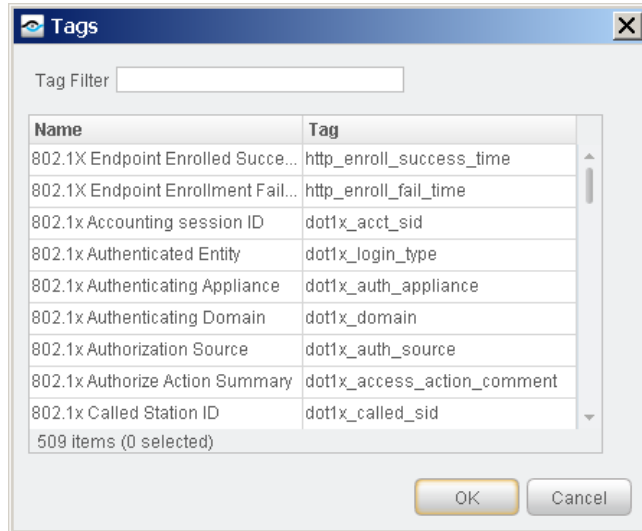


Specify the following configuration fields for the Syslog message, or accept the default values that were defined during plugin configuration. See [Default Action Configuration](#).

Message to Syslog	The text message that is sent to the Syslog server. You can use property tags to include endpoint data values. See Working with Property Tags .
Message Identity	Free-text field for identifying the Syslog message.
Syslog Server Address	Syslog server IP address or fully qualified domain name.
Syslog Server Port	Syslog UDP port number.
Syslog Server Protocol	Syslog messaging can use TCP or UDP. Select the protocol used to communicate with this server.
Syslog Facility	Syslog message facility that is transmitted as part of the message Priority field. For valid values, see Facility Values .
Syslog Severity	Syslog message severity that is transmitted as part of the message Priority field. For valid values, see Severity Values .

Working with Property Tags

You can add current values of host properties to the message. Select **Add Tags** to insert a placeholder that is populated with the actual value of the host property when the message is generated.



Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2018. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is another valid written agreement executed by you and ForeScout that governs the ForeScout products and services:

- If you have purchased any ForeScout products or services, your use of such products or services is subject to your acceptance of the terms set forth at <http://www.forescout.com/eula/>;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at <http://www.forescout.com/activecare-maintenance-and-support-policy/>;
- If you are evaluating ForeScout's products, your evaluation is subject to your acceptance of the applicable terms set forth below:
 - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: <http://www.forescout.com/evaluation-license/>.
 - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: <http://www.forescout.com/beta-test-agreement/>.
 - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at <http://www.forescout.com/nfr-license/>.

Send comments and questions about this document to: documentation@forescout.com

2018-10-03 11:07