# Table of Contents

### About the Syslog Plugin ................................................................. 3
- Multiple Destination Syslog Server Support ........................................ 3
- Sending Event Messages ........................................................................ 3
- Receiving Event Messages .................................................................... 3
- Sending Syslog Messages ...................................................................... 4
  - Sending CounterACT Event Messages ............................................... 4
  - Using Actions to Send Endpoint Messages ....................................... 4
- Requirements ..................................................................................... 5

### Configuration .................................................................................. 5
- Select an Appliance to Configure ......................................................... 5
- Send Events To .................................................................................. 6
  - Facility Values ................................................................................. 8
  - Severity Values ............................................................................... 9
- Syslog Triggers .................................................................................. 9
  - Including Header Information in All Message ................................... 9
  - Selecting Syslog Message Triggers .................................................. 10
- NAC Events ...................................................................................... 11
- Threat Protection ............................................................................... 11
- System Logs and Events .................................................................... 12
- User Operations ................................................................................ 12
- Operating System Messages ............................................................. 12
- Default Action Configuration .............................................................. 12
- Receive From ................................................................................... 13
- Verify That the Plugin Is Running ..................................................... 14
- Testing the Configuration .................................................................. 15

### Downloading and Configuring NTSyslog .......................................... 15

### Create Custom Syslog Policies ......................................................... 18
- Send Message to Syslog Action ........................................................... 19
- Working with Property Tags ............................................................... 20

### Core Extensions Module Information .............................................. 20

### Additional CounterACT Documentation .......................................... 21
- Documentation Downloads ............................................................... 21
- Documentation Portal ....................................................................... 22
- CounterACT Help Tools .................................................................... 22
About the Syslog Plugin

The Syslog Plugin is a component of the ForeScout CounterACT® Core Extensions Module. See Core Extensions Module Information for details about the module.

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 Home view.

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. See Additional CounterACT Documentation for information about accessing this document.

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.
Requirements
The following CounterACT products and software releases are required for the operation of this plugin:
- CounterACT version 8.0.
- An active Maintenance Contract for CounterACT devices is required.

Configuration
This section describes how to configure the Syslog Plugin.

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.

To configure the Syslog Plugin:
1. In the Modules pane, select Core Extensions > Syslog and then select Appliances. The Syslog - Appliances Installed dialog box opens.

2. Select any Appliance or the Enterprise Manager and select Configure. 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Address</td>
<td>Syslog server IP address or fully qualified domain name.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Syslog server port.</td>
</tr>
<tr>
<td>Server Protocol</td>
<td>Syslog messaging can use TCP or UDP. Select the protocol to be used for communicating with this Syslog server.</td>
</tr>
<tr>
<td>Use TLS</td>
<td>For some server types, you can instruct CounterACT to use TLS to encrypt communication with the Syslog server.</td>
</tr>
<tr>
<td>Soft-fail OCSP Requests</td>
<td>If CounterACT could not receive a response from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.</td>
</tr>
<tr>
<td>Message Identity</td>
<td>Free-text field for identifying the Syslog message.</td>
</tr>
<tr>
<td>Facility</td>
<td>Syslog message facility that is transmitted as part of the message Priority field. For valid values, see Facility Values.</td>
</tr>
<tr>
<td>Severity</td>
<td>Syslog message severity that is transmitted as part of the message Priority field. For valid values, see Severity Values.</td>
</tr>
</tbody>
</table>

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.

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

If the facility value is not valid, it is set to **local5**.
Core Extensions Module: Syslog Plugin

Severity Values

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

<table>
<thead>
<tr>
<th>Severity Value</th>
<th>IETF Severity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emergency</td>
<td>system is unusable</td>
</tr>
<tr>
<td>emerg</td>
<td>action must be taken immediately</td>
</tr>
<tr>
<td>alert</td>
<td>critical conditions</td>
</tr>
<tr>
<td>critical</td>
<td>critical conditions</td>
</tr>
<tr>
<td>crit</td>
<td>error conditions</td>
</tr>
<tr>
<td>error</td>
<td>warning conditions</td>
</tr>
<tr>
<td>err</td>
<td>normal but significant condition</td>
</tr>
<tr>
<td>warning</td>
<td>informational messages</td>
</tr>
<tr>
<td>notice</td>
<td>info</td>
</tr>
<tr>
<td>informational</td>
<td>informational messages</td>
</tr>
<tr>
<td>info</td>
<td>debug-level messages</td>
</tr>
</tbody>
</table>

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 *Include only messages generated by the "Send Message to Syslog" action* checkbox must *not* be selected.

If the *Include only 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.

<table>
<thead>
<tr>
<th>NAC policy logs</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC policy match/unmatch events</td>
<td>Policy evaluation change events.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Bite events</th>
<th>Indicates that an endpoint has tried to gain access to your network using a system mark.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan events</td>
<td>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.</td>
</tr>
</tbody>
</table>
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. |

**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:

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

**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.
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.

**Verify That the Plugin Is Running**

After configuring the plugin, verify that it is running.

**To verify:**

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

## 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. In the **Modules** pane, select **Core Extensions > Syslog** 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/](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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message to Syslog</td>
<td>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.</td>
</tr>
<tr>
<td>Message Identity</td>
<td>Free-text field for identifying the Syslog message.</td>
</tr>
<tr>
<td>Syslog Server Address</td>
<td>Syslog server IP address or fully qualified domain name.</td>
</tr>
<tr>
<td>Syslog Server Port</td>
<td>Syslog UDP port number.</td>
</tr>
<tr>
<td>Syslog Server Protocol</td>
<td>Syslog messaging can use TCP or UDP. Select the protocol used to communicate with this server.</td>
</tr>
<tr>
<td>Syslog Facility</td>
<td>Syslog message facility that is transmitted as part of the message Priority field. For valid values, see Facility Values.</td>
</tr>
<tr>
<td>Syslog Severity</td>
<td>Syslog message severity that is transmitted as part of the message Priority field. For valid values, see Severity Values.</td>
</tr>
<tr>
<td>Use TLS</td>
<td>For some server types, you can instruct CounterACT to use TLS to encrypt communication with the Syslog server.</td>
</tr>
</tbody>
</table>
Soft-fail OCSP Requests

If CounterACT could not receive a response from the OCSP Responder, the certificate is considered valid. By default, hard-fail is applied.

Tags

To add property tags, see Working with Property Tags

---

**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.

---

**Core Extensions Module Information**

The Syslog plugin is installed with the CounterACT Core Extensions Module.

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

- Advanced Tools Plugin
- CEF Plugin
- DHCP Classifier Plugin
- DNS Client Plugin
- DNS Enforce Plugin
- DNS Query Extension Plugin
- Device Classification Engine
- External Classifier Plugin
- Flow Analyzer Plugin
The Core Extensions Module is a ForeScout Base Module. Base Modules are delivered with each CounterACT release.

Components listed above are released and rolled back with the Core Extensions Module.

Refer to the *CounterACT Core Extensions Module Guide* for more module information, for example module requirements, upgrade and rollback instructions. See Additional CounterACT Documentation for information about how to access the module guide.

**Additional CounterACT Documentation**

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

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

**Documentation Downloads**

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

*Software downloads are also available from these portals.*

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

**Product Updates Portal**

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.
To access the Product Updates Portal:
2. Select the CounterACT version you want to discover.

Customer Portal
The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:
2. Select Downloads or Documentation.

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

Notes: If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT 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.

CounterACT Administration Guide
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 Modules.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
**Identifying Your Licensing Mode in the Console**

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options > Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.

Contact your ForeScout representative if you have any questions about identifying your licensing mode.
Legal Notice

© 2018 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.

2018-04-10 09:21