ForeScout

Syslog Messages Sent by CounterACT®

CounterACT Technical Note

Updated for Syslog Plugin 3.2.0

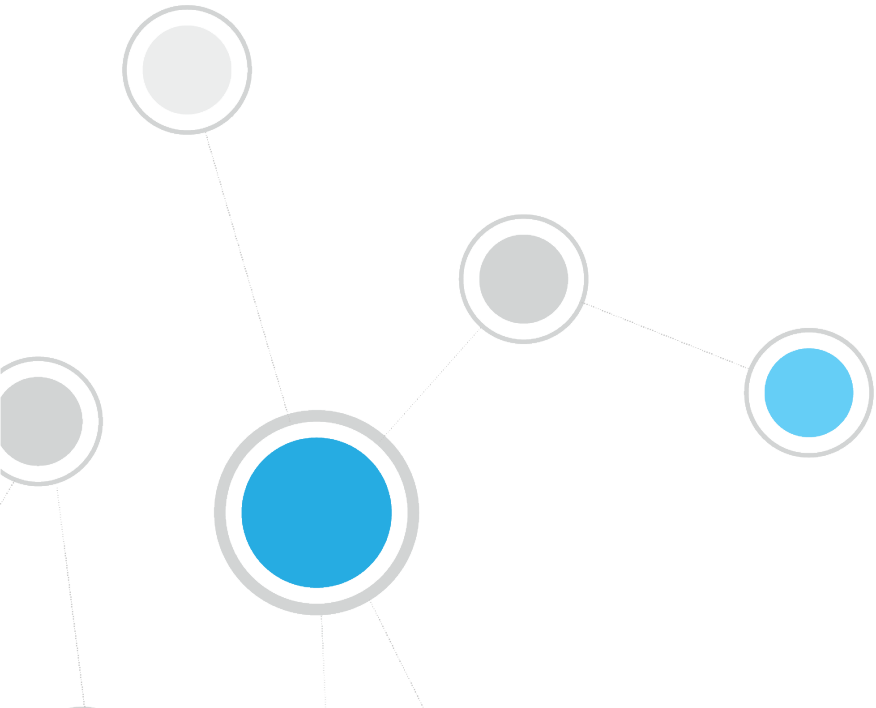


Table of Contents

About This Document

CounterACT® sends valuable information regarding its processes to one or more external Syslog servers. This information, in the form of Syslog (system log) messages, can be used for event aggregation, auditing, and further processing.

The Syslog Plugin configuration determines which Syslog server or servers receive CounterACT Syslog messages from each CounterACT device. Syslog Plugin configuration settings are set independently for each CounterACT device.

This document describes the different types of Syslog messages generated by CounterACT. Syslog messages can be generated by actions or by selected event types. The specific Syslog messages generated in your environment may vary based on the policy definitions and the events occurring in your system.

This document is intended as an aid to help you understand the different Syslog messages generated in your environment. It does not include all possible CounterACT Syslog messages.

In this document, the word *message* always refers to a Syslog message.

For more information on CounterACT Syslog message generation settings, see the *Syslog Plugin Configuration Guide*.

This document contains the following sections:

Notation Used in This Document

The following notation is used when describing the formats of Syslog messages.

Notation	Description	Example
Non-italicized bold text	Fixed text in all messages of the same type	**Source:**
ITALICIZED CAPITALIZED BOLD TEXT	Variable text in each message of the same type	***SOURCEIP***

Format of Syslog Messages

CounterACT generates Syslog messages that contain the following:

- ***PRIORITY_INFO***
  - Facility
  - Severity
- ***HEADER_INFO*** (Optional)

  - Timestamp
  - CounterACT device identifier
- ***MESSAGEID*[*PROCESSID*]:**
  - Message Identity
  - Process ID (in square brackets)
- ***MESSAGE_CONTENT***

Syslog messages are transmitted in the following format:

PRIORITY_INFO HEADER_INFO* MESSAGEID*[*PROCESSID*]: *MESSAGE_CONTENT

** - optional field*

The following is an example of a Syslog message that includes the optional fields:

```
Local5.Error Jul 28 13:09:06 10.10.1.10 ACTIONidentity[22835]: Potentially malicious running process found
```

Common Fields in All Syslog Messages

The following table describes the Syslog message fields.

Message Field	Description	For Action-Triggered Messages	For Event-Triggered Messages
PRIORITY_INFO	A combination of: ▪ *Facility* ▪ *Severity*	User-defined in the *Send Message to Syslog*, *Syslog Facility and Syslog Severity* fields. The default values are user-defined in the Syslog Plugin Configuration, *Default Action configuration* tab.	For Operating System messages, determined by the priority of the underlying message from the operating system. For all other messages, user-defined in the Syslog Plugin Configuration, *Send Events to*, *Facility and Severity* fields for each Syslog server.

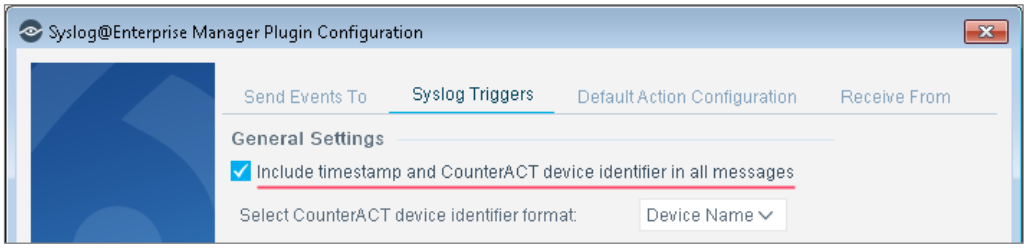
Message Field	Description	For Action-Triggered Messages	For Event-Triggered Messages
HEADER_INFO (Optional)	A combination of: ▪ *Timestamp* (date and time) transmitted by CounterACT to the Syslog server ▪ *CounterACT device identifier* of the device sending the message	Only included when **Include timestamp and CounterACT device identifier in all messages** is selected in the Syslog Plugin Configuration, *Syslog Triggers* tab. In the Syslog Plugin Configuration, *Syslog Triggers* tab, the user defines the *CounterACT device identifier* format: ▪ Device name, if resolved ▪ Device IP address	
MESSAGEID	*Message Identity*	*Message Identity* is user-defined in the *Send Message to Syslog, Message Identity* field. The default value is user-defined in the Syslog Plugin Configuration, *Default Action configuration* tab.	*Message Identity* is user-defined in the Syslog Plugin Configuration, *Message Identity* field for each Syslog server.
[*PROCESSID*]:	*Process ID* of the CounterACT process sending the message	The internal application *Process ID* is enclosed in square brackets and followed by a colon.	
MESSAGE_CONTENT	Unique text for each message type.	User-defined text in the *Send Message to Syslog* action.	One or more additional message fields. For format details, see the message content description in this document for each event type.

Some Syslog servers may display additional information, such as:

- The date the Syslog server received the message.
- The time the Syslog server received the message.
- The IP address from which the Syslog server received the message.

Optional Fields in All Messages

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



Include timestamp and CounterACT device identifier in all messages

When selected, all syslog messages include:

- A timestamp
- The device name or IP address of the CounterACT device sending the message

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

If Device Name is selected but cannot be resolved, the CounterACT device IP address is included in its place.

Syslog Messages Generated by Actions

Customized Syslog action messages for specific endpoints are triggered by the *Audit, Send Message to Syslog* action either manually or based on CounterACT policy detections. Each action sends a single message to a single Syslog server.

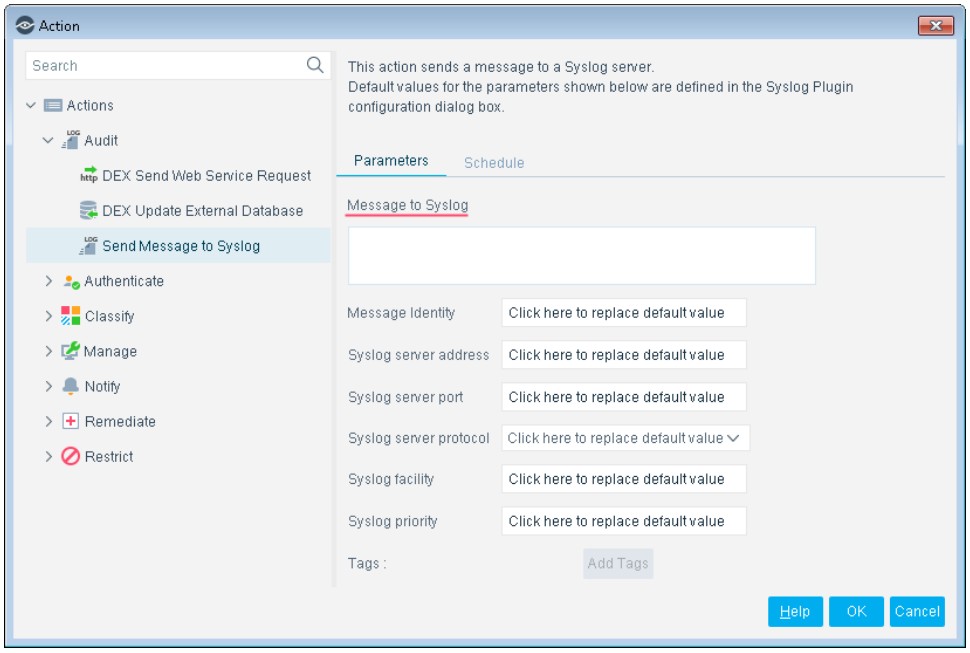
Syslog messages can be sent at customizable intervals when one of the following is defined:

- A scheduled recurrence in the *Send Message to Syslog* action.
- A time-based recheck schedule in a policy.

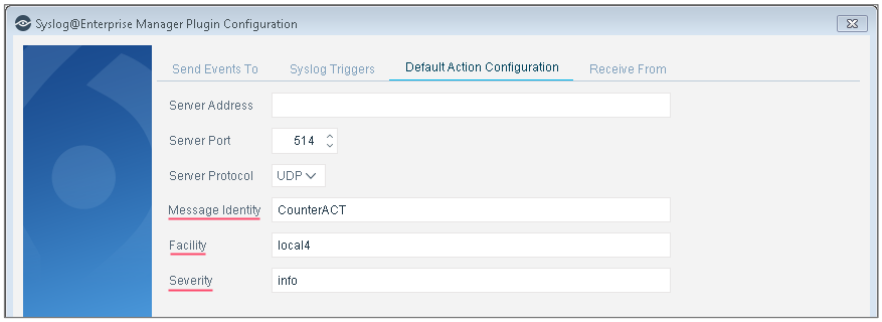
Action Message Fields

In messages generated by actions:

- The *Message content* value is always taken from the *Send Message to Syslog, Message to Syslog* action parameter, which may include property tags. When the message is generated, each tag is replaced by the current data value of the host property.



- The *Syslog Facility*, *Syslog Severity*, and *Message Identity* values are each taken from:
  - The *Send Message to Syslog* action parameters, if a value is provided.
  - The Syslog Plugin Configuration, *Default Action configuration* tab, if a value is not provided in the action.



See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

MESSAGE_CONTENT

Sample Message Generated by an Action

The following is an example of a Syslog message that includes the optional fields:

`Potentially malicious running process found`

In the sample message, the message defined by the user in the *Send Message to Syslog* action was simply:

`Potentially malicious running process found`

For more information about the Syslog message fields, see Format of Syslog Messages.

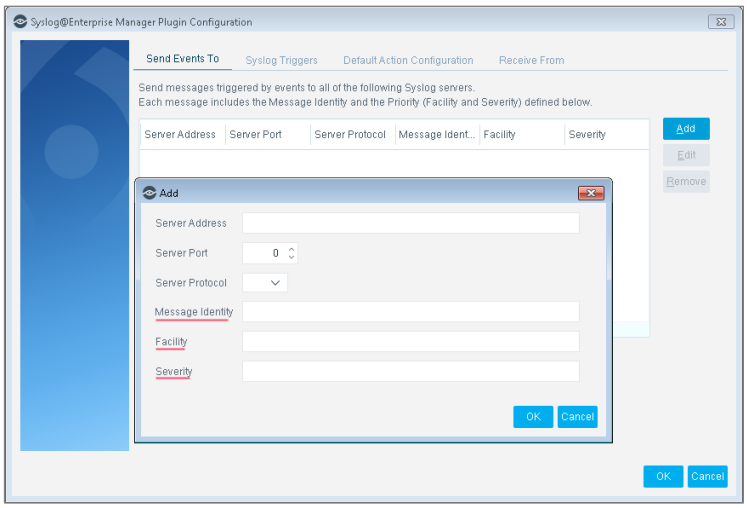
Syslog Messages Generated by Events

CounterACT generates Syslog messages depending on events occurring in the system.

Each CounterACT device receives unique event information from the network. Syslog messages are only sent for events 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.

The *Message content* of each message is dependent on the type of event.

The details of each Syslog server and the *Facility*, *Severity*, and *Message Identity* values to be included in all event messages are defined in the Syslog Plugin Configuration, *Send Events To* tab. All event messages are sent to all Syslog servers defined in the tab.



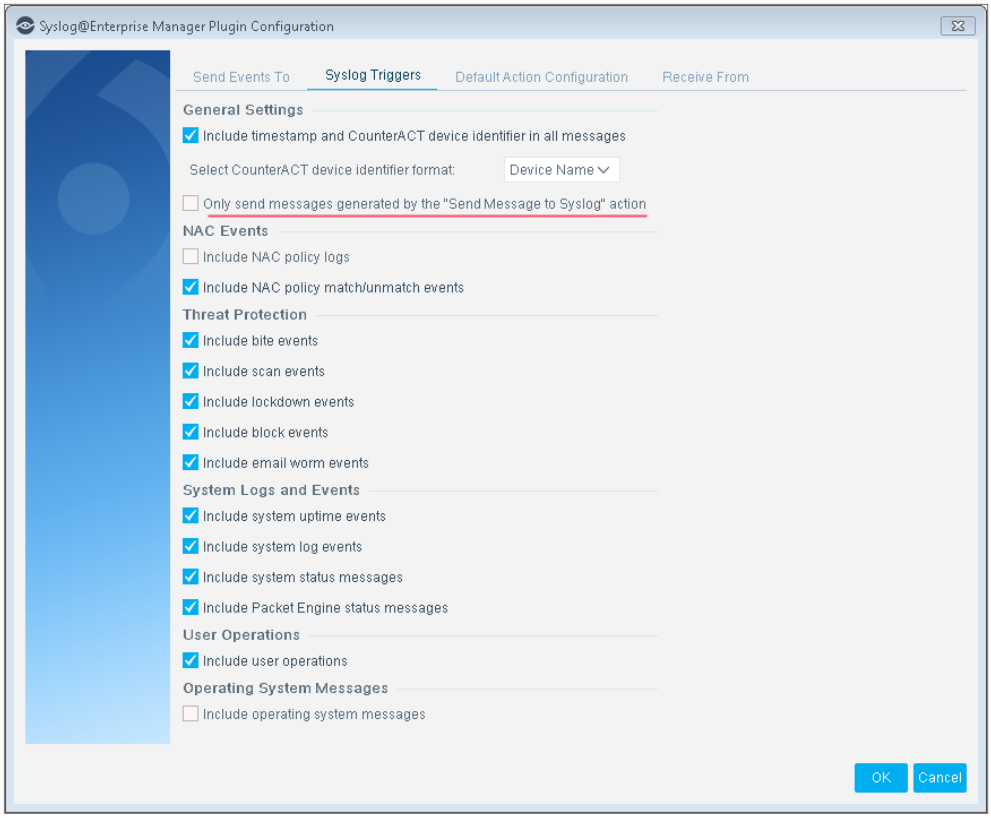
Operating System messages include the priority of the underlying message from the operating system and not the priority defined in the plugin configuration.

The CounterACT device sends a Syslog event message if the event type that occurred is selected in the Syslog Plugin Configuration, *Syslog Triggers* tab. A message is sent each time a new event of a selected type occurs.

This section describes the following *Syslog Triggers* settings:

- General Settings
- NAC Events
- Threat Protection
- System Log and Events

- User Operation
- Operating System Messages



General Settings

Configure general settings for Syslog messages.

Only send messages generated by the "Send Message to Syslog" action

When selected:

- Syslog messages are generated when triggered by the *Audit, Send Message to Syslog* action only.
- Syslog messages are not triggered by any event, even if the event type is selected in this tab.

To enable Syslog messages to be generated by events, ensure that this checkbox is ***not*** selected.

NAC Events

These messages contain information, such as source IP and policy name, about NAC policy events.

Include NAC policy logs

When selected, a Syslog message is generated whenever an endpoint policy event occurs.

The log displays information about endpoints as they are detected, and it is continuously updated as the policy is evaluated for the endpoint.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

NAC Policy Log: Source: *SOURCEIP*, Rule: *MANUAL_OR_POLICY* , Details: *ADDITIONAL_DETAILS*.

Sample NAC Policy Log Messages

NAC Policy Log: Source: <IP address>, Rule: Policy "1.1 Asset Classification" , Details: Host cleared from policy. Status was "Windows:Match". Reason: Host removed.

NAC Policy Log: Source: <IP address>, Rule: Policy "1.1 Asset Classification" , Details: Evaluated new host. Status is "Windows:Pending" due to condition

NAC Policy Log: Source: <IP address>, Rule: Policy "1.1 Asset Classification" , Details: Host evaluation changed from "Windows:Pending" to "Windows:Match" due to condition . Reason: Property update: Network Function "Windows Machine" learned (first time). Duration: less than a second

NAC Policy Log: Source: <IP address>, Rule: Policy "Manageable Windows" , Details: Host evaluation changed from "Manageable Windows:Unmatched" to "Domain Current:Pending" due to condition . Reason: Host added to group "Windows" because it matches rule "1.1 Asset Classification-->Windows". Duration: less than a second

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Last Sample Message	Description
Message title	NAC Policy Log:	Identifies the type of event message.
Source: *SOURCEIP*	Source: 10.20.3.40	**Source:** followed by the endpoint IP address on which the policy event occurred.
Rule: *MANUAL_OR_POLICY*	Rule: Policy "Manageable Windows"	**Rule:** followed by **Manual** or the NAC policy name.

Message Field	Value in Last Sample Message	Description
Details: ***ADDITIONAL_DETAILS***	Details: Host evaluation changed from "Manageable Windows:Unmatched" to "Domain Current:Pending" due to condition . Reason: Host added to group "Windows" because it matches rule "1.1 Asset Classification-->Windows". Duration: less than a second	**Details:** followed by the event details, including: ▪ Event type (For example, “Host evaluation changed” followed by details of the change) ▪ If the event is of type “Host evaluation changed”, then the following is also included: - “Reason:” followed by the reason for the event. - “Duration:” followed by the length of time taken to evaluate the policy.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include NAC policy match/unmatch events

When selected, a Syslog message is generated whenever a policy evaluation change event occurs. These event logs are similar to the NAC policy logs, but focus solely on endpoints matching and unmatching policy rules.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

NAC Policy Log: Source: *SOURCEIP*, Rule: *POLICY_NAME* , Match: *MATCH_OR_UNMATCH*, Category: *CATEGORY*, Details: *ADDITIONAL_DETAILS* . Reason: *CHANGE*. Duration: *DURATION_MIN_SEC*

Sample NAC Policy Match/Unmatch Event Messages

NAC Policy Log: Source: <IP address>, Rule: Policy "Manageable Windows" , Match: "Domain Current:Pending", Category: N/A, Details: Host evaluation changed from "Manageable Windows:Pending" to "Domain Current:Pending" due to condition . Reason: Host group membership by MAC address resolved - not in any group; Host added to group "Windows" because it matches rule "1.1 Asset Classification-->Windows". Duration: less than a second

NAC Policy Log: Source: <IP address>, Rule: Policy "Manageable Windows" , Match: "Manageable Windows:Pending", Category: N/A, Details: Host evaluation changed from "Domain Current:Pending" to "Manageable Windows:Pending" due to groups filter . Reason: Host removed from group "Windows" because it no longer matches rule "1.1 Asset Classification-->Windows". Duration: 24 seconds

NAC Policy Log: Source: <IP address>, Rule: Policy "Manageable Windows" , Match: "Domain Current:Pending", Category: N/A, Details: Host evaluation changed from "Manageable Windows:Unmatched" to "Domain Current:Pending" due to condition . Reason: Host added to group "Windows" because it matches rule "1.1 Asset Classification-->Windows". Duration: less than a second

NAC Policy Log: Source: <IP address>, Rule: Policy "1.1 Asset Classification" , Match: "Windows:Match", Category: Classifier, Details:

Host evaluation changed from "Windows:Pending" to "Windows:Match" due to condition . Reason: Property update: Network Function "Windows Machine" learned (first time). Duration: 5 minutes and 29 seconds

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Last Sample Message	Description
Message title	NAC Policy Log:	Identifies the type of event message.
Source: ***SOURCEIP***	Source: 10.20.3.123	**Source:** followed by the endpoint IP address on which the NAC event occurred.
Rule: ***POLICY_NAME***	Rule: Policy "1.1 Asset Classification"	**Rule:** followed by the NAC policy name.
Match: ***MATCH_OR_UNMATCH***	Match: " Windows:Match"	**Match** or **Unmatch:** followed by the sub-rule name and the match status.
Category: ***CATEGORY***	Category: Classifier	**Category:** followed by the policy category type, or “N/A” if no category is assigned.
Details: ***ADDITIONAL_DETAILS***	Details: Host evaluation changed from "Windows:Pending" to "Windows:Match" due to condition	**Details:** followed by the host evaluation change details.
Reason: ***CHANGE***	Reason: Property update: Network Function "Windows Machine" learned (first time)	**Reason:** followed by what caused the policy matching change.
Duration: ***DURATION_MIN_SEC***	Duration: 5 minutes and 29 seconds	**Duration:** duration of policy evaluation.

For more information about the Syslog message fields, see Format of Syslog Messages.

Threat Protection

These messages contain information on intrusion-related activity, including bite events, scan events, lockdown events and manual events.

Include bite events

When selected, a Syslog message is generated whenever an endpoint tries to gain access to your network using a system mark.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

EVENT_TYPE*. Source: *SOURCEIP*, Destination: *DESTINATIONIP*:*PORT

Sample Bite Event Message

`Port bite. Source: 120.10.1.23. Destination: 130.20.3.45:139`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
EVENT_TYPE	Port bite.	Identifies the type of event message.
Source: *SOURCEIP*	Source: 120.10.1.23.	**Source:** followed by the endpoint IP address on which the threat event was detected.
Destination: *DESTINATIONIP*:*PORT*	Destination: 130.20.3.45:139	**Destination:** followed by the IP address and port which the threat attempted to access.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include scan events

When selected, a Syslog message is generated whenever an endpoint performs 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.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

EVENT_TYPE*. Source: *SOURCEIP

Sample Scan Event Message

`Scan event. Source: 106.101.1.23.`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
EVENT_TYPE	Scan event.	Identifies the type of event message.
Source: *SOURCEIP*	Source: 106.101.1.23.	**Source:** followed by the endpoint IP address on which the threat event was detected.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include lockdown events

When selected, a Syslog message is generated whenever a malicious event is detected by another Appliance.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

EVENT_TYPE*. Source: *SOURCEIP

Sample Lockdown Event Message

`Manual event. Source: 10.10.1.123`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
EVENT_TYPE	Manual event.	Identifies the type of event message.
Source: *SOURCEIP*	Source: 10.10.1.123.	**Source:** followed by the endpoint IP address on which the threat event was detected.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include block events

When selected, a Syslog message is generated whenever CounterACT blocks packets from the source from going through to the specified destination (host and service).

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

EVENT_TYPE*. Host: *SOURCEIP*, Target: *DESTINATIONIP*, *Time TIME_IN_EPOCH*, Service: *PORT/PROTOCOL*, Is Virtual Firewall blocking rule: *TRUE_FALSE*, Reason: *BLOCK_TYPE

Sample Block Event Message

`Block Event: Host: 10.10.2.123, Target: 10.20.3.234, Time 1469975529, Service: 23/TCP, Is Virtual Firewall blocking rule: false, Reason: Port block`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
EVENT_TYPE	Block event.	Identifies the type of event message.
Host: *SOURCEIP*	Host: 10.10.2.123,	**Host:** followed by the IP address of the source blocked by CounterACT from sending packets.

Message Field	Value in Sample Message	Description
Target: ***DESTINATIONIP***	Target: 10.20.3.234,	**Target:** followed by the IP address of the endpoint which was blocked from receiving the packets.
Time: ***TIME_IN_EPOCH***	Time 1469975529,	**Time:** followed by the Unix epoch time.
Service: ***PORT/PROTOCOL***	Service: 23/TCP,	**Service:** followed by the service port/protocol.
Virtual firewall blocking rule status	Is Virtual Firewall blocking rule: false,	**Is Virtual Firewall blocking rule:** followed by **`true`** or **`false`**.
Reason: ***BLOCK_TYPE***	Reason: Port block	**Reason:** followed by the block type.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include email worm events

When selected, a Syslog message is generated whenever CounterACT identifies email worm anomalies sent over email.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

EVENT_TYPE. Source: SOURCEIP. Details: DETAILS

Sample Email Worm Event Message

`Mail Infection Attempt. Source: 10.10.1.123. Details: mail_from=sender@from.com,mail_to=recipient@to.com,mail_subject=Check out this report`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
EVENT_DESCRIPTION	Mail Anomaly Sender Mail Anomaly Server Mail Anomaly Amount Mail Anomaly Attachment Mail Anomaly Recipient Mail Infection Attempt	Describes the type of email worm event.
Source: ***SOURCEIP***	Source: 10.10.1.123.	Intruder IP address

Message Field	Value in Sample Message	Description
Details: ***DETAILS***	mail_from=sender@from.com,mail_to=recipient @to.com,mail_subject=Check out this report	**Details:** Comma-separated list of key-value pairs containing metadata of the malicious email. Optional fields are mail_from, mail_to, mail_subject and mail_attachment

System Log and Events

These messages contain information about CounterACT system events.

Include system uptime events

When selected, a Syslog message is generated every hour to show the amount of time the CounterACT service has been running.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

Uptime *NUM_SECONDS* seconds

Sample System Uptime Event Message

`Uptime 1902057 seconds`

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
Uptime *NUM_SECONDS* seconds	Uptime 1902057 seconds	Identifies the type of event message: **Uptime** followed by the number of seconds the service has been running.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include system log events

When selected, a Syslog message can be generated when the log is written to show certain CounterACT activities detected by the system. For example, successful and failed user login operations. (Messages sent to the Events Viewer.)

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

Log: *LOG_MESSAGE*. Details: *DETAILS*. Severity: *SEVERITY_LEVEL*

Sample System Log Event Message

Log: Database vacuumed. Details: Reduced database size by 0MB Elapsed time was 5 minutes. Severity: Information

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
Log: *LOG_NAME*	Log: Database vacuumed.	Identifies the type of event message: **Log:** followed by the system log message.
Details: *DETAILS*	Details: Reduced database size by 0MB Elapsed time was 5 minutes.	**Details:** followed by more information.
Severity: *LOG_SEVERITY*	Severity: Information	**Severity:** followed by the severity level, such as **Error** or **Information**.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include system status messages

When selected, a Syslog message is generated every hour to show memory, swap and CPU usage statistics.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

System statistics: CPU usage: *CPU_USAGE%*, Available memory : *UNUSEDMEM_KB*, Used memory: *USEDMEM_KB*, Available swap: *UNUSEDSWAP_KB*, Used swap: *USEDSWAP_KB*

Sample System Status Message

System statistics: CPU usage: 12%, Available memory : 2071272 KB, Used memory: 2113736 KB, Available swap: 4194296 KB, Used swap: 87232 KB

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
Message title	System statistics:	Identifies the type of event message.
CPU usage: *CPU_USAGE%*	CPU usage: 12%	**CPU usage:** followed by the percent of CPU used.
Available memory : *MEM_AVAIL* KB	Available memory : 2071272 KB	**Available memory:** followed by amount of available memory, in KB.

Message Field	Value in Sample Message	Description
Used memory: *MEM_USED* KB	Used memory: 2113736 KB	**Used memory:** followed by amount of used memory, in KB.
Available swap: *SWAP_AVAIL* KB	Available swap: 4194296 KB	**Available swap:** followed by amount of available swap space, in KB.
Used swap: *SWAP_USED* KB	Used swap: 87232 KB	**Used swap:** followed by amount of used swap space, in KB.

For more information about the Syslog message fields, see Format of Syslog Messages.

Include Packet Engine status messages

When selected, a Syslog message is generated every hour to show the status of the CounterACT Application.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

Application status: *APP_STATUS*;Connected clients: *CLIENTS*; Recovery EM:* *RECOV_EM; Engine status:* *ENG_STATUS** ;Attacked Services: *SERVICES_NUM*;Installed Plugins: *PLUGINS***

** - optional field*

Sample Packet Engine Status Message

```
Application status: CounterACT Appliance is running;Connected clients:
admin@ta-user1-w7.abc.forescout.com;Engine status: Ready ;Attacked
Services: 0;Installed Plugins: Hardware WatchDog, Switch, User Directory,
Reports, CounterACT 7.0.0 Service Pack, Syslog, CounterACT Infrastructure
Update Pack, HPS - Inspection Engine, DNS Client, HPS Vulnerability DB,
Technical Support, Macintosh/Linux Property Scanner, NBT Scanner;;
```

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
Application status: *APP_STATUS*	Application status: CounterACT Appliance is running	**Application status:** followed by the CounterACT device type (Appliance or an Enterprise Manager), and status (if it is running).
Connected clients: *CLIENTS*	Connected clients: admin@ta-user1-w7.abc.forescout.com	**Connected clients:** followed by the user IDs and host names of the CounterACT Consoles or Enterprise Manager connected to the device.

Message Field	Value in Sample Message	Description
Recovery EM: ***RECOV_EM***		**Recovery EM:** followed by IP address of the recovery Enterprise Manager. Only if a recovery Enterprise Manager is defined. For Appliances only; this field is not sent out in messages from the Enterprise Manager.
Engine status: ***ENG_STATUS***	Engine status: Ready	**Engine status:** followed by the status. For Appliances only; not for Enterprise Managers.
Attacked Services: ***SERVICES_NUM***	Attacked Services: 0	**Attacked Services:** followed by the number of attacked services detected via the CounterACT Threats capability.
Installed Plugins: ***PLUGINS***	Installed Plugins: Hardware WatchDog, Switch, User Directory, Reports, CounterACT 7.0.0 Service Pack, Syslog, CounterACT Infrastructure Update Pack, HPS - Inspection Engine, DNS Client, HPS Vulnerability DB, Technical Support, Macintosh/Linux Property Scanner, NBT Scanner	**Installed Plugins:** followed by a comma-separated list of installed CounterACT plugins.

For more information about the Syslog message fields, see Format of Syslog Messages.

User Operation

These messages are generated when a user operation takes place in the CounterACT Console. These are the same messages sent to the Audit Trail log.

Include user operations

When selected, a Syslog message is generated whenever the user makes a configuration change such as updating policies, stopping or starting the Appliance, changing plugin configuration, or updating user credentials.

See Format of Syslog Messages for the full syntax of Syslog messages. The ***MESSAGE_CONTENT*** part of these Syslog messages is composed as follows:

User USER changed ITEM_CHANGED. Details: MESSAGE_CONTENT

Sample User Operation Message

```
User admin changed Configuration. Details: Policy: '1.1 Asset
Classification'
Sub-Rule changes:
Sub-Rule Linux\Unix
Old Condition:
 Network Function: Unix Server/Workstation, Linux Desktop/Server
New Condition:
 Network Function: Unix Server/Workstation, Linux Desktop/Server  OR  Open
Ports: 22/TCP
```

```
User admin changed HPS Inspection Engine Configuration. Details: Edited the
following Enterprise Manager: :
 Endpoint Remote Inspection method: Previous Value:wmi_only Current
Value:wmi_with_fall_back
```

```
User admin changed Configuration. Details: Change field lists definition to
Lists
MaaS360 Software Installed -> Application Name: MaaS360 Unauthorized Mobile
Applications
NetBIOS Domain: Corporate domain names, Corporate domain names_1
VMware Server Product ID: ESXi Server List
Windows Applications Installed -> Name: sqlserver
Windows Services Running: Microsoft virtual services
```

```
User admin changed Configuration. Details: Paused Network Integrity rules:
1.1 Asset Classification
```

```
User admin changed Enterprise Manager Console. Details: Logout from <IP
address> by host <IP address> : Logout succeeded
```

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Final Sample Message	Description
User USER changed ITEM_CHANGED	User admin changed Enterprise Manager Console.	Includes: ▪ user name (admin) ▪ what the user changed. This may be one of: - 'Configuration', if the change is to the general CounterACT configuration - Plugin name followed by 'Configuration' - Device name (for example, in the final message, "Enterprise Manager Console"

Message Field	Value in Final Sample Message	Description
Details: MESSAGE_CONTENT	Details: Logout from <IP address> by host <IP address> : Logout succeeded	Details of the change. For example: ▪ Login or out of the CounterACT Console ▪ Started/Paused policies ▪ Changes to configuration of CounterACT or any installed plugins ▪ Changes to policies Note that each user event has a specific format for the details section as can be seen from the above examples.

For more information about the Syslog message fields, see Format of Syslog Messages.

Operating System Messages

The rsyslog system (refer to www.rsyslog.com) generates and determines the format of messages containing information about events of relevance at the level of the operating system.

Include operating system messages

When selected, a Syslog message is generated for relevant operating system events.

All Syslog messages generated by the operating system use the configuration defined in **`/etc/rsyslog.conf`**. This file dictates that all log messages to the following operating system log files are sent to Syslog:

- /var/log/messages
- /var/log/secure
- /var/log/maillog
- /var/log/cron
- /var/log/spooler
- /var/log/boot.log

Syslog messages are sent in the following format:

PRIORITY_INFO HEADER_INFO*: *MESSAGE_CONTENT

Sample Operating System Message

```
Cron.Info    Jul 28 13:40:01 user1-em1 CROND[27644]: (root) CMD
(/usr/lib/sa/sa1 1 1)
```

The following table describes the various fields comprising the content of these Syslog messages.

Message Field	Value in Sample Message	Description
PRIORITY_INFO	Facility: Cron Severity: Info	The Facility and Severity will be exactly as sent by the operating system, and will not be overwritten based on the configuration of the *Send Events To* tab of the Syslog Plugin.
HEADER_INFO	Jul 28 13:40:01 user1-em1 CROND[27644]	Header information will be exactly as sent by the operating system. This always includes a timestamp and hostname, and depending on the message destination, may also include the process name and process ID of the process logging the message.
MESSAGE_CONTENT	(root) CMD (/usr/lib/sa/sa1 1 1)	Session log message mapped from one of the following: ▪ **/var/log/messages** ▪ **/var/log/secure** ▪ **/var/log/maillog** ▪ **/var/log/cron** ▪ **/var/log/spooler** ▪ **/var/log/boot.log**

For more information about the Syslog message fields, see Format of Syslog Messages.

Legal Notice

2018-04-10 13:20

Legal Notice

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

2018-04-10 13:20