Forescout
Syslog Messages
Technical Note

Updated for Syslog Plugin 3.5
Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Resources page on the Forescout website for additional technical documentation: https://www.forescout.com/company/resources/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2019 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.
# Table of Contents

**About This Document .................................................................** 4  
Notation Used in This Document ......................................................... 4

**Format of Syslog Messages .................................................................** 4  
Common Fields in All Syslog Messages .................................................. 5

**Optional Fields in All Messages .................................................................** 6  
Include timestamp and CounterACT device identifier in all messages ........... 6

**Syslog Messages Generated by Actions .................................................................** 7  
Action Message Fields ........................................................................ 7

**Syslog Messages Generated by Events .................................................................** 8  
General Settings ................................................................................... 10  
Only send messages generated by the "Send Message to Syslog" action ...... 10  
NAC Events ....................................................................................... 10  
Include NAC policy logs ...................................................................... 11  
Include NAC policy match/unmatch events ............................................ 12  
Threat Protection ................................................................................. 13  
Include bite events ........................................................................... 13  
Include scan events .......................................................................... 14  
Include lockdown events .................................................................... 15  
Include block events ......................................................................... 15  
Include email worm events ................................................................ 16  
System Log and Events ....................................................................... 17  
Include system uptime events ............................................................... 17  
Include system log events ................................................................. 17  
Include system status messages .......................................................... 18  
Include Forescout application status messages ...................................... 19  
User Operation ................................................................................... 21  
Include user operations ................................................................. 21  
Operating System Messages .................................................................. 22  
Include operating system messages .................................................... 22

**Additional Forescout Documentation .................................................................** 24  
Documentation Downloads ............................................................... 24  
Documentation Portal ........................................................................ 25  
Forescout Help Tools ........................................................................ 25
About This Document

The Forescout® solution 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 Forescout 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 the Forescout platform. 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 Forescout Syslog messages.

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

For more information on Forescout Syslog message generation settings, see the *Forescout Core Extensions: Syslog Plugin Configuration Guide*.

This document contains the following sections:

- Format of Syslog Messages
- Optional Fields in All Messages
- Syslog Messages Generated by Actions
- Syslog Messages Generated by Events

### Notation Used in This Document

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

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-italicized bold text</td>
<td>Fixed text in all messages of the same type</td>
<td>Source:</td>
</tr>
<tr>
<td><strong>ITALICIZED CAPITALIZED BOLD TEXT</strong></td>
<td>Variable text in each message of the same type</td>
<td>SOURCEIP</td>
</tr>
</tbody>
</table>

### Format of Syslog Messages

The generated Syslog messages 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]: MESSAGECONTENT
```

* - 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Description</th>
<th>For Action-Triggered Messages</th>
<th>For Event-Triggered Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRIORITY_INFO</strong></td>
<td>A combination of:</td>
<td>User-defined in the Send Message to Syslog, Syslog Facility and Syslog Severity fields.</td>
<td>For Operating System messages, determined by the priority of the underlying message from the operating system.</td>
</tr>
<tr>
<td></td>
<td>- Facility</td>
<td>The default values are user-defined in the Syslog Plugin Configuration,** Default Action configuration** tab.</td>
<td>For all other messages, user-defined in the Syslog Plugin Configuration,** Send Events to, Facility and Severity** fields for each Syslog server.</td>
</tr>
<tr>
<td></td>
<td>- Severity</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>HEADER_INFO</strong></td>
<td>(Optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A combination of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Timestamp (date and time) transmitted to the Syslog server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- CounterACT device identifier of the device sending the message</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only included when Include timestamp and CounterACT device identifier in all messages is selected in the Syslog Plugin Configuration,** Syslog Triggers** tab.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Syslog Plugin Configuration,** Syslog Triggers** tab, the user defines the CounterACT device identifier format:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Device name, if resolved</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Device IP address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Syslog Messages

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Description</th>
<th>For Action-Triggered Messages</th>
<th>For Event-Triggered Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>MESSAGEID</td>
<td>Message Identity</td>
<td>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.</td>
<td>Message Identity is user-defined in the Syslog Plugin Configuration, Message Identity field for each Syslog server.</td>
</tr>
<tr>
<td>[PROCESSID]:</td>
<td>Process ID of the Forescout process sending the message</td>
<td>The internal application Process ID is enclosed in square brackets and followed by a colon.</td>
<td></td>
</tr>
<tr>
<td>MESSAGE_CONTENT</td>
<td>Unique text for each message type.</td>
<td>User-defined text in the Send Message to Syslog action.</td>
<td>One or more additional message fields. For format details, see the message content description in this document for each event type.</td>
</tr>
</tbody>
</table>

Some Syslog servers may display additional information, such as:
- The date when the Syslog server received the message.
- The time when 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.

![Syslog Plugin Configuration](image)

**Include timestamp and CounterACT device identifier in all messages**

When selected, all syslog messages include:

---

Updated for Syslog Plugin 3.5

---
- 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 Forescout 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**

The Forescout platform 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 the source IP address 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: ADDITIONALDETAILS.

Sample NAC Policy Log Messages

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

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


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

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Last Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message title</td>
<td>NAC Policy Log:</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td>Source:</td>
<td>Source: 10.20.3.40</td>
<td>Source: followed by the endpoint IP address on which the policy event occurred.</td>
</tr>
</tbody>
</table>
Syslog Messages

Updated for Syslog Plugin 3.5

### Syslog Messages Technical Note

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Last Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details: ADDITIONAL_DETAILS</td>
<td>Details: Host evaluation changed from &quot;Manageable Windows:Unmatched&quot; to &quot;Domain Current:Pending&quot; due to condition. Reason: Host added to group &quot;Windows&quot; because it matches rule &quot;1.1 Primary Classification--&gt;Windows&quot;. Duration: less than a second</td>
<td>Details: followed by the event details, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ Event type (For example, &quot;Host evaluation changed&quot; followed by details of the change)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>▪ If the event is of type &quot;Host evaluation changed&quot;, then the following is also included:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- &quot;Reason:&quot; followed by the reason for the event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- &quot;Duration:&quot; followed by the length of time taken to evaluate the policy.</td>
</tr>
</tbody>
</table>

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 Primary 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 Primary 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 Primary Classification-->Windows". Duration: less than a second

**NAC Policy Log:** Source: <IP address>, Rule: Policy "1.1 Primary 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Last Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message title</td>
<td>NAC Policy Log:</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td><strong>Source</strong>: SOURCEIP</td>
<td>Source: 10.20.3.123</td>
<td>Source: followed by the endpoint IP address on which the NAC event occurred.</td>
</tr>
<tr>
<td><strong>Rule</strong>: POLICY_NAME</td>
<td>Rule: Policy &quot;1.1 Primary Classification&quot;</td>
<td>Rule: followed by the NAC policy name.</td>
</tr>
<tr>
<td><strong>Match</strong>: MATCH_OR_UNMATCH</td>
<td>Match: &quot;Windows:Match&quot;</td>
<td>Match or Unmatch: followed by the sub-rule name and the match status.</td>
</tr>
<tr>
<td><strong>Category</strong>: CATEGORY</td>
<td>Category: Classifier</td>
<td>Category: followed by the policy category type, or &quot;N/A&quot; if no category is assigned.</td>
</tr>
<tr>
<td><strong>Details</strong>: ADDITIONALDETAILS</td>
<td>Details: Host evaluation changed from &quot;Windows:Pending&quot; to &quot;Windows:Match&quot; due to condition</td>
<td>Details: followed by the host evaluation change details.</td>
</tr>
<tr>
<td><strong>Duration</strong>: DURATION_MIN_SEC</td>
<td>Duration: 5 minutes and 29 seconds</td>
<td>Duration: duration of policy evaluation.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>EVENT_TYPE</code></td>
<td>Port bite.</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td><strong>Source:</strong> SOURCEIP</td>
<td>Source: 120.10.1.23.</td>
<td>Source: followed by the endpoint IP address on which the threat event was detected.</td>
</tr>
<tr>
<td><strong>Destination:</strong> DESTINATIONIP:PORT</td>
<td>Destination: 130.20.3.45:139</td>
<td>Destination: followed by the IP address and port which the threat attempted to access.</td>
</tr>
</tbody>
</table>

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, the Forescout platform 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>EVENT_TYPE</code></td>
<td>Scan event.</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td><strong>Source:</strong> SOURCEIP</td>
<td>Source: 106.101.1.23.</td>
<td>Source: followed by the endpoint IP address on which the threat event was detected.</td>
</tr>
</tbody>
</table>

For more information about the Syslog message fields, see [Format of Syslog Messages](#).
Include lockdowm 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT_TYPE</td>
<td>Manual event.</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td>Source: SOURCEIP</td>
<td>Source: 10.10.1.123.</td>
<td>Source: followed by the endpoint IP address on which the threat event was detected.</td>
</tr>
</tbody>
</table>

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

Include block events

When selected, a Syslog message is generated whenever the Forescout platform 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:


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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVENT_TYPE</td>
<td>Block event.</td>
<td>Identifies the type of event message.</td>
</tr>
</tbody>
</table>
### Syslog Messages Technical Note

#### Message Field | Value in Sample Message | Description
--- | --- | ---
Host: **SOURCEIP** | Host: 10.10.2.123, | Host: followed by the IP address of the source blocked by the Forescout platform from sending packets.
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 the Forescout platform 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.
**SOURCEIP** | Source: 10.10.1.123. | Intruder IP address
System Log and Events

These messages contain information about Forescout system events.

Include system uptime events

When selected, a Syslog message is generated every hour to show the amount of time the Forescout 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>Uptime 1902057 seconds</td>
<td>Identifies the type of event message: Uptime followed by the number of seconds the service has been running.</td>
</tr>
</tbody>
</table>

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 Forescout platform 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.

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

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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message title</td>
<td>System statistics:</td>
<td>Identifies the type of event message.</td>
</tr>
<tr>
<td><strong>CPU usage:</strong> CPU_USAGE%</td>
<td>CPU usage: 12%</td>
<td>CPU usage: followed by the percent of CPU used.</td>
</tr>
<tr>
<td><strong>Available memory:</strong> MEM_AVAIL KB</td>
<td>Available memory: 2071272 KB</td>
<td>Available memory: followed by amount of available memory, in KB.</td>
</tr>
</tbody>
</table>
### Syslog Messages

#### Technical Note

**Message Field** | **Value in Sample Message** | **Description**
--- | --- | ---
**Used memory:** \textit{MEM\_USED KB} | Used memory: 2113736 KB | **Used memory:** followed by amount of used memory, in KB.
**Available swap:** \textit{SWAP\_AVAIL KB} | Available swap: 4194296 KB | **Available swap:** followed by amount of available swap space, in KB.
**Used swap:** \textit{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 Forescout application status messages

When selected, a Syslog message is generated every hour to show the status of the Forescout 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:** \textit{APP\_STATUS}; Connected clients: \textit{CLIENTS}; Attacked Services: \textit{SERVICES\_NUM}; Recovery EM: \textit{*RECOV\_EM*}; Engine status: \textit{*ENG\_STATUS*}; Installed Plugins: \textit{PLUGINS}

* - optional field

#### Sample Packet Engine Status Message from a Managed Appliance


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

**Message Field** | **Value in Sample Message** | **Description**
--- | --- | ---
**Application status:** \textit{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).
<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connected clients:</strong></td>
<td><strong>CLIENTS</strong></td>
<td><strong>Connected clients:</strong> followed by the user ID and host name of the Forescout Console or Enterprise Manager connected to the device.</td>
</tr>
<tr>
<td></td>
<td>Connected clients:</td>
<td><strong>Connected clients:</strong> <a href="mailto:admin@HR-user.mycompany.com">admin@HR-user.mycompany.com</a></td>
</tr>
<tr>
<td>Attacked Services:</td>
<td><strong>SERVICES_NUM</strong></td>
<td><strong>Attacked Services:</strong> followed by the number of attacked services detected via the Threats capability. For Enterprise Managers only. This field is not sent out in messages from Appliances.</td>
</tr>
<tr>
<td></td>
<td>Attacked Services: 0</td>
<td></td>
</tr>
<tr>
<td>Recovery EM:</td>
<td><strong>RECOV_EM</strong></td>
<td><strong>Recovery EM:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>Recovery EM: 10.1.1.1</td>
<td></td>
</tr>
<tr>
<td>EM connection status</td>
<td>EM connection status:</td>
<td><strong>Connection status:</strong> followed by connection status of the Appliance to the Enterprise Manager. This field is not sent out in messages from the Enterprise Manager.</td>
</tr>
<tr>
<td></td>
<td>Connected</td>
<td></td>
</tr>
<tr>
<td>Assigned hosts</td>
<td>Assigned hosts: 799</td>
<td><strong>Assigned hosts:</strong> followed by the number of hosts assigned to this Appliance. This field is not sent out in messages from the Enterprise Manager.</td>
</tr>
<tr>
<td>Engine status:</td>
<td><strong>ENG_STATUS</strong></td>
<td><strong>Engine status:</strong> followed by the Packet Engine status. For Appliances only. In messages from the Enterprise Manager, this field is reported for each connected Appliance</td>
</tr>
<tr>
<td></td>
<td>Engine status: Ready</td>
<td></td>
</tr>
<tr>
<td>Installed Plugins:</td>
<td><strong>PLUGINS</strong></td>
<td><strong>Installed Plugins:</strong> followed by a comma-separated list of installed Forescout plugins.</td>
</tr>
<tr>
<td></td>
<td>Installed Plugins: DNS Query Extension, Wireless, IoT Posture Assessment Library, HPS Inspection Engine, ...</td>
<td></td>
</tr>
<tr>
<td>Message Field</td>
<td>Value in Sample Message</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connected CounterACT Appliances:</td>
<td></td>
<td>Connected CounterACT Appliances: followed by a comma-separated list of Appliances and their Packet Engine statuses. For Enterprise Managers only. This field is not sent out in messages from Appliances.</td>
</tr>
</tbody>
</table>

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 Forescout 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 session SESSION_ID changed ITEM_CHANGED. Details: MESSAGE_CONTENT**

#### Sample User Operation Message

User admin changed Configuration. Details: Policy: '1.1 Primary Classification'
- Sub-Rule changes:
  - Sub-Rule Linux\Unix
  - Old Condition: Network Function: Unix Server/Workstation, Linux Desktop/Server

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
- 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 Primary 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.

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Final Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User USER session</strong></td>
<td>User admin changed Enterprise Manager Console.</td>
<td>Includes:</td>
</tr>
<tr>
<td><strong>SESSION_ID</strong></td>
<td></td>
<td>• user name (admin)</td>
</tr>
<tr>
<td><strong>changed</strong></td>
<td></td>
<td>• what the user changed. This may be one of:</td>
</tr>
<tr>
<td><strong>ITEM_CHANGED</strong></td>
<td></td>
<td>- ‘Configuration’, if the change is to the general Forescout configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Plugin name followed by ‘Configuration’</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Device name (for example, in the final message, “Enterprise Manager Console”</td>
</tr>
</tbody>
</table>

Details: 

**MESSAGE_CONTENT**

Details: Logout from <IP address> by host <IP address> : Logout succeeded

Details of the change. For example:

• Login to or out of the Forescout Console
• Started/Paused policies
• Changes to the configuration or 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](http://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/sal 1 1)

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

<table>
<thead>
<tr>
<th>Message Field</th>
<th>Value in Sample Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRIORITY_INFO</strong></td>
<td>Facility: Cron Severity: Info</td>
<td>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.</td>
</tr>
<tr>
<td><strong>HEADER_INFO</strong></td>
<td>Jul 28 13:40:01 user1-em1 CROND[27644]</td>
<td>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.</td>
</tr>
</tbody>
</table>
| **MESSAGE_CONTENT** | (root) CMD (/usr/lib/sa/sal 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](#).
Additional Forescout Documentation

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

- Documentation Downloads
- Documentation Portal
- Forescout Help Tools

Documentation Downloads

Documentation downloads can be accessed from the Forescout Resources Page, or one of two Forescout portals, depending on which licensing mode your deployment is using.

- Per-Appliance Licensing Mode – Product Updates Portal
- Flexx Licensing Mode – Customer Portal

Software downloads are also available from these portals.

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Resources Page

The Forescout Resources Page provides links to the full range of technical documentation.

To access the Forescout Resources Page:
- Go to https://www.forescout.com/company/resources/, select Technical Documentation and search for documents.

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:
- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Portal

The Downloads page on the Forescout Customer Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, 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.
To access documentation on the Forescout Customer Portal:
- Go to https://Forescout.force.com/support/ and select Downloads.

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

If your deployment is using Flexx Licensing Mode, you may not have received credentials to access this portal.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/ and use your customer support credentials to log in.

Forescout Help Tools
Access information directly from the Console.

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

Forescout Administration Guide
- Select Forescout Help from the Help menu.

Plugin Help Files
- After the plugin is installed, select Tools > Options > Modules, select the plugin and then select Help.

Online Documentation
- Select Online Documentation from the Help menu to access either the Forescout Resources Page (Flexx licensing) or the Documentation Portal (Per-Appliance licensing).