AlgoSec Security Management Suite

Syslog Reference Guide

View our most recent updates in our online ASMS Tech Docs.

Document Release Date: 23 March, 2020

Legal Notices

Specifications subject to change without notice.

Proprietary & Confidential Information

This document contains proprietary information. Neither this document nor said proprietary information shall be published, reproduced, copied, disclosed, or used for any purpose other than the review and consideration of this material without written approval from AlgoSec, 65 Challenger Rd., Suite 310, Ridgefield Park, NJ 07660 USA.

The software contains proprietary information of AlgoSec; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between AlgoSec and the client and remains the exclusive property of AlgoSec If you find any problems in the documentation, please report them to us in writing. AlgoSec does not warrant that this document is error-free.

Contents

ASMS Syslog message reference

ASMS can send monitoring messages using the syslog system, which is a standard for forwarding log messages in an IP network. ASMS can send syslog messages to local or remote servers, and External systems can read ASMS's monitoring messages and act up on their content.

Supported external syslog systems include SEIM (Security Information and Event Management) or SOC (Security Operations Center) systems, such as ArcSight, Check Point Eventia, CA eTrust, NetIQ, and so on.

This document provides descriptions of how to configure ASMS to generate and send Syslog messages, as well as references of the messages generated.

For more details, see:

- AFA Syslog messages
- FireFlow syslog messages
- AppViz Syslog messages
- Login and logout Syslog messages
- System metric notifications

AFA Syslog messages

AFA generates Syslog messages for analysis performed, policy changes detected, as well as user login and logout events across ASMS.

Configure Syslog message generation for each device you add to AFA.

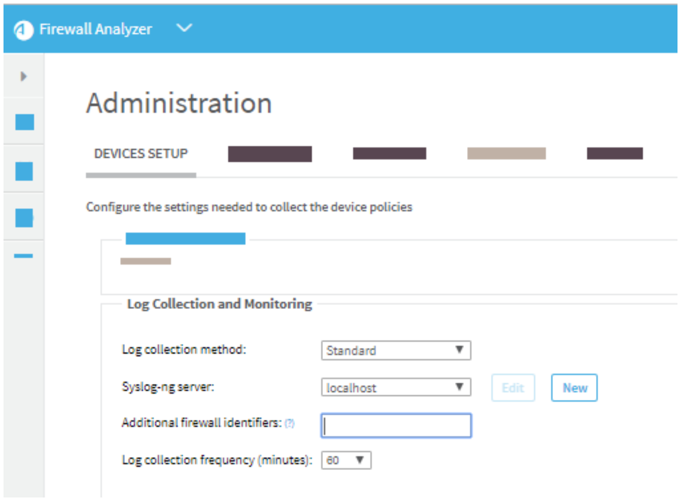
This topic includes:

- Configure Syslog messages for AFA
- Configure an external Syslog server for AFA messages
- AFA syslog message syntax
- AFA analysis syslog messages
- AFA policy change syslog messages

Configure Syslog messages for AFA

Configure AFA Syslog message logging in the AFA**Administration** area for each relevant device.

For example:



Configure the settings needed to collect the device policies

Log Collection and Monitoring

Log collection method: Standard

Syslog-ng server: localhost

Additional firewall identifiers: (?)

Log collection frequency (minutes): 60

Configure an external Syslog server for AFA messages

If, while defining **Log Collection and Monitoring** settings for your device, you add a remote Syslog server that's connected using the **root** user, AFA automatically performs the initial setup required.

However, if you want to collect logs from a Syslog server with a user other than **root**, you'll need to perform these steps yourself, or others if specified by your system.

Do the following:

1. Log in to the syslog-ng server as user **root**.
2. Run the following command:

   chmod o+x /home/<user>

3. On the syslog-ng server, open the following file for editing: **/etc/syslog-ng/syslog-ng.conf**.
4. Add the following line to the file:

   include "/home/<user>/algosec/syslog_processor/algosec_syslog-ng.conf";

   Where **<user>** is the name of the user connecting to the syslog-ng server.

   > **Note:** This is the user name you configured in the **SSH User Name** or **User Name** field when you specified the syslog-ng server. For details, see AFA Syslog messages.

5. Save your changes to the **syslog-ng.conf** file.
6. In AFA, in the **Syslog Server Settings** dialog, click **Test Connectivity** to ensure that the connection works.
7. Click **OK** and **Finish** to start the AFA installation process on the syslog-ng server.
8. Restart the syslog-ng server configuration. Run the following command as user **root**:

   service syslog-ng restart

Your syslog-ng server is now ready to use with a user other than **root**.

Note: If the following message appears: **Plugin module not found .. module='afsql'**, ensure that syslog server is installed and configured correctly.

Note: If you are working with a Check Point Eventia system, you must also install a plug-in before you can view AFA messages in Eventia. For more details, contact Check Point to obtain the plug-in.

AFA syslog message syntax

AFA stores syslog messages locally, in the **/var/log/message** directory, in CEF (Common Event Format).

Each message starts with a standard syslog prefix, including the event date and time, and the AFA machine name. This prefix is followed by the CEF-standard, bar-delimited message format.

AFA syslog message headers have the following syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|<Event>|<Event>|<Severity>|
<Domain>|<Extension>
```

where:

- **<AFA-Version>** is the AFA version string. For example: **v6.1-b55**
- **<Event>** items are readable text that designates the message type.
- **<Severity>** is a number between **0-7** and varies by message.
- **<Domain>** is the domain name or **NONE**, if domains are not enabled.
- **<Extension>** items contain more details in a **parameter=value** format.

AFA analysis syslog messages

AFA generates syslog messages for each analysis run, as well as additional information and administrative syslog messages as needed.

The following table provides a basic description of the syslog messages generated for AFA analysis and links to more details below.

Message type	Description
Start and Start Refresh syslog messages	Indicate that an AFA analysis has begun
Findings syslog messages	Summarize the analysis results
End syslog messages	Indicate the completion of an analysis process, regardless of status
ReportData syslog messages	Provide details for a specific report
Info syslog messages	Contain additional details about report findings, such as changes in policies
Admin syslog messages	Indicate a situation that requires administrative attention

Tip: Both the **report** and **firewall** parameters appear in all syslog messages issued for a report being generated, and can be used to identify all related messages for the report.

Start and **Start Refresh** syslog messages

Start messages indicate that an AFA analysis has begun, identifying the unique job-name assigned.

If you are refreshing an existing report, the event name and ID is **Start Refresh** instead of **Start**.

Severity level: 1.

Syntax:

Start syslog messages have the following syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|Start|Start|1|<Domain>|
report=<report_name> firewall=<device_name>
```

Start messages include the following parameters:

- **report.** The name assigned to the new report. For example, **afa-3928**.
- **firewall.** The name of the device being analyzed.

Findings syslog messages

Findings messages summarize the analysis results, and are sent when the report is ready.

If a failure occurred and no report was generated, no message is sent.

Severity level: Depends on the status message. For details, see Severity.

Syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|Findings|Findings|<Domain>|
<Severity>|report=<report_name> firewall=<device_name> status=<status>
msg=<details>
```

Findings messages include the following parameters:

- **report.** The name assigned to the new report. For example, **afa-3928**.
- **firewall.** The name of the device being analyzed.
- **status.** A description of the status found, such as:

Status	Description	Severity
No changes	The device policy has not changed since the previous analysis.	1
Changes	Changes in the device policy were detected, but no new risk items were flagged.	3
New risks	Changes in the device policy were detected, and additional risk items were flagged. This is the most sever status code that AFA produces.	5

Status	Description	Severity
Manual run	The report was initiated manually, and is not scheduled. This may occur when an administrator is testing a new configuration or scenario.	1

- **msg.** A short, free-text summary of any risks found. For example: **1 high, 2 medium**.

End syslog messages

End messages are always sent when an analysis process completes, regardless of the status.

Severity level: Depends on the analysis status. For details, see AFA analysis syslog messages.

Syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|End|End|<Severity>|<Domain>|
report=<report_name> firewall=<device_name> status=<status>
url=<report URL>
```

End messages include the following parameters:

- **report.** The name assigned to the new report. For example, **afa-3928**.
- **firewall.** The name of the device being analyzed.
- **status.** One of the following:

Status	Description	Severity
Success	Analysis completed successfully.	1
Failure	Analysis failed to complete.	7

- **url**. The URL of the report generated. For example: **url=https://192.168.2.8/~sally/algosec/php/Login.php?type\=firewall&report\=sally-570**

> **Tip:** This URL contains equal signs (**=**) and leading backslashes (\). Before using this URL as a hyperlink, you'll need to strip out the backslashes.

ReportData syslog messages

ReportData syslog messages are sent for each new report generated, and contain details about the report's contents.

Severity level: 0

Syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|ReportData|ReportData|
<Domain>|0|report=<report_name> firewall=<device_name> {<report data>}
```

ReportData messages include the following parameters:

- **report.** The name assigned to the new report. For example, **afa-3928**.
- **firewall.** The name of the device being analyzed.
- **report data**. Includes details from the report for the device analyzed, such as the number of risks of various severity, security rating scores, number of duplicate objects, number of covered rules, and so on. For details, see Sample ReportData message.

Info syslog messages

Info messages contain additional details about report findings, including a list of any detected risks, changes in the policy, and so on.

Severity: 0

Syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-Version>|Info|Info|0|<Domain>|
report=<report_name> firewall=<device_name> msg=<details>
```

Info messages include the following parameters:

- **report.** The name assigned to the new report. For example, **afa-3928**.
- **firewall.** The name of the device being analyzed.
- **msg**. Contains the additional details.

  For example: **Start data collection** or **Summary: <risk-level> <count> <risk code> <title>**

Admin syslog messages

Admin messages indicate a situation that requires administrative attention.

Severity: 7

Syntax:

```
CEF:0|AlgoSec|Firewall Analyzer|<AFA-
Version>|Admin|Admin|7|<Domain>|msg=<details>
```

Admin messages include the following parameters:

- **msg**. Contains details about the situation. For example: **Low disk space** or **Over 95% of the disk space is in use**

Sample AFA syslog messages

The following examples show syslog messages as they would look in the local **/var/log/messages** file.

- Sample normal report message sequence, no changes found
- Sample normal report message sequence, manual run
- Sample ReportData message
- Sample analysis failure message, manual run
- Sample admin message
- Sample admin message, High Availability clusters

Each message occupies a single line in the file.

Sample normal report message sequence, no changes found

```
May 15 17:00:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Start|Start|1|NONE|report=sally-570 firewall=ALGO_CLMay 15 17:00:02
algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Info|Info|0|NONE|
report=sally-570 firewall=ALGO_CL msg=Start data collectionMay 15
17:00:28 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Findings
|Findings|1|NONE|report=sally-570 firewall=ALGO_CL status=No changesMay
15 17:00:38 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|End|
End|1|NONE|report=sally-570 firewall=ALGO_CL status=Success url=
https://192.168.2.8/~sally/algosec/php/Login.php?type\=firewall&report
\=sally-570
```

Sample normal report message sequence, manual run

```
May 15 17:06:07 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Start|Start|1|NONE|report=sally-572 firewall=192_168_2_52May 15
17:06:08 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Info|
Info|0|NONE|report=sally-572 firewall=192_168_2_52 msg=Start data
collectionMay 15 17:06:51 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|
v6.1-b55|Findings|Findings|1|NONE|report=sally-572 firewall=192_168_2_52
 status=Manual run msg=1 suspected high risks, 1 medium risks.
May 15 17:06:51 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Info|Info|0|NONE|report=sally-572 firewall=192_168_2_52 msg=Summary:
susp_high 1 F08 Insecure external access to router 2May 15 17:06:51
algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Info|Info|0|
NONE|report=sally-572 firewall=192_168_2_52 msg=Summary: medium 2
R01 "From somewhere to Any allow Any service" rules 2May 15
17:06:56 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|End|
End|1|NONE|report=sally-572 firewall=192_168_2_52 status=Success
url=https://192.168.2.8/~sally/algosec/php/Login.php?type\=
firewall&report\=sally-572
```

Sample ReportData message

```
CEF:0|AlgoSec|Firewall Analyzer|v2018.1.800-b281|ReportData|ReportData|
0|NONE|report=afa-12345 firewall=QWERTYUIOPOIU01 {"NERC Level":"Fair",
"Number of Low Risks":"4","Device IP":"10.20.140.551","ISO27001 Level":
"Fair","NIST_800-41 Level":"Fair","NERC Score":"70","SOX Level":"Fair",
"SOX Score":"66","PCI Score":"65","GLBA Score":"73","NIST_800-53 Score"
:"70","BASEL Level":"Fair","Number of Unused Rules":null,"NIST_800-171
Score":"72","Number of Medium Risks":"9","Device Groups":[],"ASD_ISM
Score":"62","Number of High Risks":"0","HIPAA Level":"Fair","Number
of Duplicate Objects":"206","Number of Special Case Rules":"6",
"Security Rating Score":"86","Number of Disabled Rules":"4","GLBA
Level":"Fair","NIST_800-53 Level":"Fair","ISO27001 Score":"68","TRM
Level":"Fair","TRM Score":"74","PCI Level":"Fair","Device Brand":
"Check Point","HIPAA Score":"73","NIST_800-171 Level":"Fair","GDPR
Level":"Fair","Domain Name":0,"ASD_ISM Level":"Fair","Highest Risk
Level":"Suspected_High","Number of Covered Rules":"3","Rule Count":
"100","Number of Suspected High Risks":"2","Device Id":"QWERTYUIOPOIU01",
"GDPR Score":"68","Report Date":"20190622T224914+0300","NIST_800-41
Score":"62","BASEL Score":"66"}
```

Sample analysis failure message, manual run

```
May 16 11:14:01 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Start|Start|1|NONE|report=sally-577 firewall=afrMay 16 11:14:01
algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Info|Info|0|
NONE|report=sally-577 firewall=afr msg=Start data collectionMay 16
11:14:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Info|
Info|0|NONE|report=sally-577 firewall=afr msg=Data collection failed
May 16 11:14:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
End|End|7|NONE|report=sally-577 firewall=afr status=Failure
url=https://192.168.2.8/~sally/algosec/php/Login.php?type\=
firewall&report\=sally-577
```

Sample admin message

```
May 16 11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin
|Admin|7|NONE|msg=Low disk space on the AFA server (under 200 MB)May 16
11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|
7|NONE|msg=Backup of AFA configuration failedMay 16 11:24:02 algosec-dev5
CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=Low disk
space on AlgoSec server
```

Sample admin message, High Availability clusters

```
May 16 11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin
|Admin|7|NONE|msg=AlgoSec HA - Service started on PrimaryMay 16 11:24:02
algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|
msg=AlgoSec HA - Service stopped on PrimaryMay 16 11:24:02 algosec-dev5
CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=AlgoSec
HA - Service started on SecondaryMay 16 11:24:02 algosec-dev5 CEF:0|
AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=AlgoSec HA
 - Service stopped on SecondaryMay 16 11:24:02 algosec-dev5 CEF:0|
AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=AlgoSec HA
 - Secondary is downMay 16 11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall
Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=AlgoSec HA - Secondary is up
May 16 11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Admin|Admin|7|NONE|msg=AlgoSec HA - Version mismatch errorMay 16
11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|
Admin|7|NONE|msg=AlgoSec HA - Split brain errorMay 16 11:24:02
algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|
NONE|msg=AlgoSec HA - Sync too slowMay 16 11:24:02 algosec-dev5
CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=
AlgoSec HA - Manual hand-over performedMay 16 11:24:02 algosec-dev5
CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=
AlgoSec HA - appliance manually removed from HA clusterMay 16
11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Admin|Admin|7|NONE|msg=AlgoSec HA - HA parameters setMay 16
11:24:02 algosec-dev5 CEF:0|AlgoSec|Firewall Analyzer|v6.1-b55|
Admin|Admin|7|NONE|msg=AlgoSec HA - Primary appliance initialized
successfully by secondaryMay 16 11:24:02 algosec-dev5 CEF:0|
AlgoSec|Firewall Analyzer|v6.1-b55|Admin|Admin|7|NONE|msg=AlgoSec
HA - Secondary appliance initialized successfully by primary
```

AFA policy change syslog messages

Each time AFA detects a change via real-time monitoring, a log entry is created in the **/var/log/messages** directory.

Tip: AFA can also send syslog messages to a remote server. Configure the remote server in the AFA**Administration** area. For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

Changes to host groups, services, or applications

When changes are made to a host group, service, or application, one message summarizing everything added, deleted, or changed since the last monitoring is logged for each group type.

For example:

```
msg=History Services : added : 0 changed : 0 deleted : 0
```

Changes to rules

When changes are made to rules, one message is logged each time a rule is added, changed, or removed. The rule ID is specified in the message.

For example:

```
msg=History Rules : Rule 30 has been added
```

FireFlow syslog messages

FireFlow automatically sends Syslog messages for all history items, including changes made to change requests, comments, and replies, as well as for each status update in a FireFlow change request.

No additional configuration is required to save FireFlow Syslog messages locally.

This topic includes:

- FireFlow syslog message syntax
- FireFlow syslog message examples
- Configure an external syslog server for FireFlow messages

FireFlow syslog message syntax

FireFlow automatically writes messages to the local syslog daemon using the **local0** ID.

These messages are located in the **/var/log/messages** directory, which requires **root** permissions to access.

All FireFlow syslog messages start with a standard syslog prefix, including the event date and time, and the FireFlow machine name.

This prefix is followed by a CEF standard bar-delimited message, using the following syntax:

```
CEF:0|DeviceVendor|DeviceProduct|DeviceVersion|ID|Name|Severity|Extension
```

where:

- **DeviceVendor** is always set to **AlgoSec**.
- **DeviceProduct** is always set to **FireFlow**.
- **DeviceVersion**. Indicates the FireFlow version string. For example **v1.1-b13**.
- **Name** / **ID**. Both indicate the message type, and is equal to eachother.

- **Severity**. Indicates the messages severity, as a number between 0-10.
- **Extension**. Detailed message information in the following format:

  ```
  ticket=<ticketID> by_user=<user> msg=<message>
  ```

  Where:

  - **ticketId** is the change request ID.
  - **user** is the user or the email address of the requestor, including the FireFlow system.
  - **message** is a description of the event that triggered the message.

Configure an external syslog server for FireFlow messages

To forward FireFlow's Syslog messages to a remote Syslog server instead of saving them locally, do the following:

1. Log in to the FireFlow machine as user root, and open the **/etc/syslog.conf** file for editing.
2. Add the following line to the file:

   local0.*@<SyslogServer>

   where **<SyslogServer>** is the name or IP address of the remote syslog server.

FireFlow syslog message examples

The following code shows examples of FireFlow syslog messages:

```
Jul 13 00:13:42 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=requestor@company.com msg=Ticket created

Jul 13 00:13:42 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=FireFlow_System msg=Outgoing email recorded

Jul 13 00:38:32 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Taken

Jul 13 00:38:32 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Status changed from 'new' to 'plan'
```

```
Jul 13 00:38:40 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Change Source 1.1.1.1 added

Jul 13 00:38:41 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Change Destination 3.3.3.3 added

Jul 13 00:38:41 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Change Service smtp added

Jul 13 00:38:41 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Change Action allow added

Jul 13 00:38:57 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=ned msg=Status changed from 'plan' to 'check'

Jul 13 00:48:52 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=FireFlow_System msg=Firewall Last Report afa-3 added

Jul 13 00:48:52 localhost CEF:0|AlgoSec|FireFlow|v1.1-b13|Log|Log|0|
ticket=1 by_user=FireFlow_System msg=Firewall Last Report Date
2009-07-13 04:47:32 added
```

AppViz Syslog messages

AppViz generates Syslog messages for each change detected in a AppViz application.

This topic includes:

- Configure AppViz Syslog messages
- AppViz Syslog message syntax

Configure AppViz Syslog messages

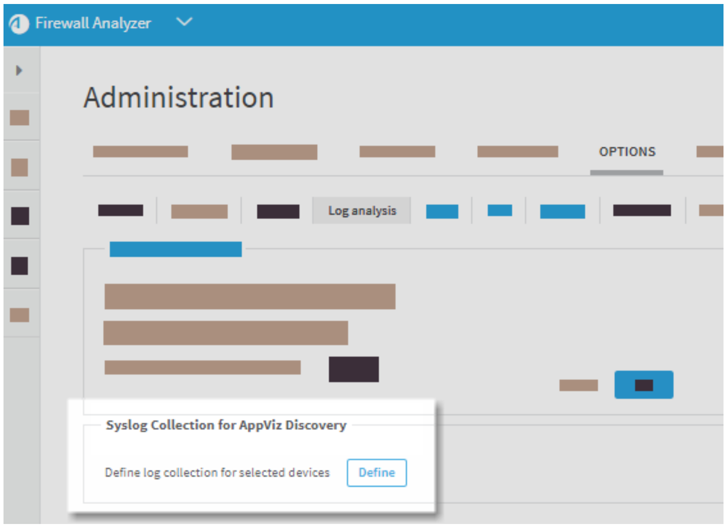
Configure ASMS to send Syslog messages for AppViz events from the AFA**Administration** area. For example, you may want to define Syslog message collection before starting a Traffic Logs Discovery process.

Do the following:

1. Click your username in the toolbar and select **Administration**.
2. On the **General** tab, under **Define Syslog Collection**, click **Define**.

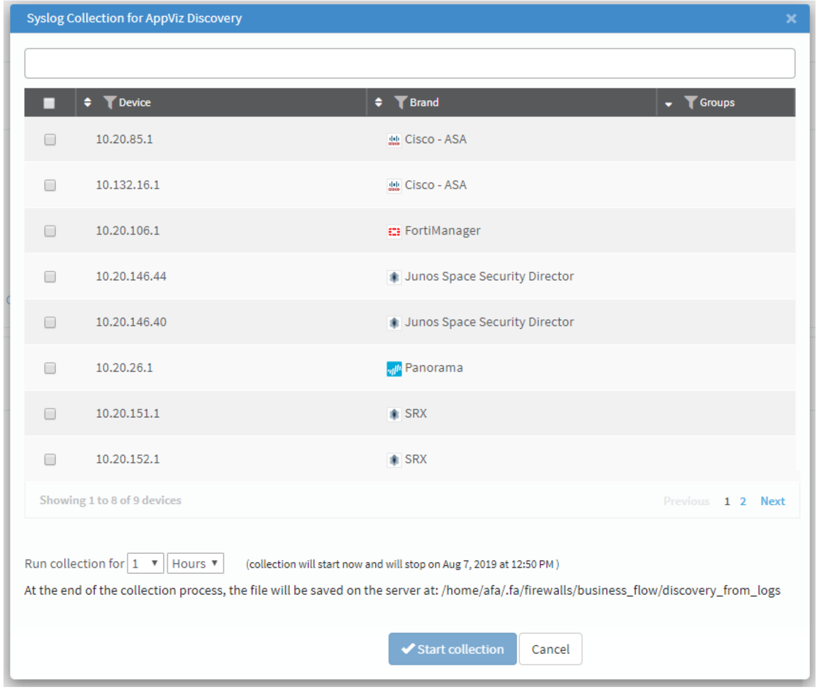
   A new tab opens to the **Log analysis** tab of the AFA**Administration** area.
3. In the **Log analysis** tab, under **Syslog Collection for AppViz Discovery**, click **Define**.

   For example:


Firewall Analyzer
Administration
OPTIONS
Log analysis
Syslog Collection for AppViz Discovery
Define log collection for selected devices
Define

A **Syslog Collection for AppViz Discovery** dialog opens displaying all devices configured for AppViz.

For example:



☐	Device	Brand	Groups
☐	10.20.85.1	Cisco - ASA	
☐	10.132.16.1	Cisco - ASA	
☐	10.20.106.1	FortiManager	
☐	10.20.146.44	Junos Space Security Director	
☐	10.20.146.40	Junos Space Security Director	
☐	10.20.26.1	Panorama	
☐	10.20.151.1	SRX	
☐	10.20.152.1	SRX	

Showing 1 to 8 of 9 devices

Run collection for 1 ▾ Hours ▾ (collection will start now and will stop on Aug 7, 2019 at 12:50 PM)

At the end of the collection process, the file will be saved on the server at: /home/afa/.fa/firewalls/business_flow/discovery_from_logs

4. Select the devices you want to collect data from.

> **Tip:** Enter all or part of an IP address in the search bar at the top to filter the devices shown, or use the sort and filter buttons in the grid header.

5. Below the grid, define how long you want to run log collection for, and then click **Start collection**.

Once configured, AppViz syslog messages are collected in the **/home/afa/.fa/firewalls/business_flow/discovery_from/logs** directory.

AppViz Syslog message syntax

AppViz generates Syslog messages only for changes detected in AppViz applications. Each message has the following syntax:

```
CEF:0|AlgoSec|BusinessFlow|ReportData|ReportData|0|NONE|{<change details>}
```

Where **<change details>** are details about the application change detected.

Severity level: 0

For example:

```
CEF:0|AlgoSec|BusinessFlow|ReportData|ReportData|0|NONE|{"Revision ID":"5",
"Application ID":"5","Name":"Payroll","Revision status":"PENDING",
"Lifecycle phase":"Testing","Connectivity status":"None","Number of flows
":"1","Number of blocked flows":"0","Number of unscanned servers":"3",
"Change requests":{"Id":["4"],"Opened date":["20190807T175653+0300"],
"Requestor":["administrator"],"Status":["OPEN"]},"Part of critical
process":false,"Pci application":false,"Created":"20190807T175550+0300"}
```

Login and logout Syslog messages

Each time a user logs in or out of ASMS, a log entry is created in the **/var/log/messages** directory. This includes internal logins, such as when FireFlow opens a session to run a traffic simulation query in AFA.

This topic includes:

- Login and logout syslog message contents
- Login and logout syslog event reference
- Sample login and logout Syslog messages

Login and logout syslog message contents

Syslog entries for login and logout events include the following details:

- **Date and time**
- **ASMS build version**
- **Event name**, such as **"Successful login"**. For details, see Login and logout syslog event reference.
- **Severity level**: 0
- **The domain ID**. When domains are disabled, this will appear as `NONE`.
- **The username**.
- **The IP address of the browsing computer**. Internal events do not include the IP address, because it will always be the **localhost**.

Login and logout syslog event reference

The following table lists basic login and logout events that generate Syslog messages. Your system may generate additional messages depending on your configuration.

Message	Description
Internal Connection	Internal connection event

Message	Description
Internal Connection - Manual logout	Internal connection event related to a manual logout
Internal Connection - Session expired logout	Internal connection event related to a logout due to a session expiration
Internal Connection - Successful login	Internal connection event related to a successful login
Login Failed - System Error	Log in failed because of a system error.
Manual logout	User manually logged out
Session Expired	User session expired and user is logged out
Successful login	Successful login occurred
Unsuccessful login	Log in failed because of invalid input. Additional details about the failure are included in the message.

Sample login and logout Syslog messages

Successful login event

```
Mar  2 09:29:56 localhost : CEF:0|AlgoSec|Suite|afa Wed Feb 22 09:56:46
IST 2017|Successful login|Successful login|0|NONE|user=admin
IP=192.168.201.1
```

Unsuccessful login because of user input

```
Mar  2 09:36:22 localhost : CEF:0|AlgoSec|Suite|afa Wed Feb 22 09:56:46
IST 2017|Unsuccessful login|Unsuccessful login|0|NONE|user=admina
IP=192.168.201.1
```

Unsuccessful login because of a system error

```
Feb  5 16:15:59 afa-4-126 : CEF:0|AlgoSec|Suite|v6.11.0-b390|Login Failed
 - System Error|Login Failed - System Error|0|NONE|user=admin
IP=192.168.3.216
```

Internal login

```
Mar  2 09:45:30 localhost : CEF:0|AlgoSec|Suite|v6.11.0-b495|Internal
Connection|Internal Connection|0|NONE|user=FireFlow_batch
```

Manual logout

```
Mar  2 09:36:13 localhost : CEF:0|AlgoSec|Suite|afa Wed Feb 22 09:56:46
IST 2017|Manual logout|Manual logout|0|NONE|user=admin IP=192.168.201.1
```

Session Expired

```
Jan 29 19:26:35 localhost : CEF:0|AlgoSec|Suite|v6.11.0-b310|Session
Expired|Session Expired|0|NONE|user=admin IP=192.168.201.1
```

Note: By default, timeout occurs after the session is inactive for 5 hours.

System metric notifications

ASMS tracks various system metrics that trigger notifications when thresholds are exceeded. These notifications can be triggered as syslog messages, or events in the issues center.

AFA admins can modify the thresholds for each metric and the types of notifications triggered.

For more details, see the *AlgoSec Firewall Analyzer Administrator Guide*.

- Configure system notifications
- System notifications enabled by default

Configure system notifications

This procedure describes how to configure the **json** file that determines how and which AFA system notifications are sent.

Do the following:

1. Open a terminal and log in as user **afa.**
2. Browse to an open the **/data/algosec-ms/config/watchdog_configuration.json** file for editing.

   The **watchdog_configuration.json** file includes the following properties:

Property	Description
metrics	An array that specifes AFA metrics. For more details, see Metric element.

Property	Description
actions	An array of possible actions to take upon a metric status change. Supported actions include: - **publish_syslog** - **publish_issues_center** **Note:** While all metrics can trigger syslog messages, only some can trigger messages in the AFA issues center. For more details, see System notifications enabled by default .
metricsActions	An array of objects that each define when a specific status change triggers an action. For more details, see MetricsAction.

3. Modify the **json** file as needed, and save your changes.

Metric element

The **Metric** element in the **watchdog_configuration.json** file has the following properties:

Property	Description
enabled	Boolean. Determines whether the metric is enabled.
name	String. Read-only. A unique name for the metric. For details, see System notifications enabled by default.
description	String. A description of the metric. For details, see System notifications enabled by default.

Property	Description
frequency	A **frequency** object, which specifies the frequency for checking the metric. Each frequency object includes the following properties: • **value**. Integer. Determines how often the metric is checked. 0 = the metric is checked every time the collection service runs. • **unit**. String. One of the following time units: SECOND MINUTE HOUR DAY **Default** = 10 SECONDS.
hostTypes	Array. List of appliances that check the metric. One of the following: • **MASTER** • **SLAVE** • **REMOTE_MANAGER** If you do not have a distributed architecture, this is always defined as [**MASTER**].
thresholdPolicy	An **options** object that specifies the metric's thresholds. The **options** object is an array of objects that each specify a threshold for a specific status. For more details, see Options object and Threshold sample configuration.

Options object

Each options object includes the following properties:

Property	Description
status	String. Determines the status of the metric if the threshold is met. One of the following: - **PASS** - **FAIL** - **WARNING**
type	String. Determines the type of result returned by the metric collection. One of the following: - **STRING** - **INTEGER** - **FLOAT** - **BOOLEAN**
condition	String. The comparison operator to use on the metric collection result. One of the following: - **EQ (=)** - **LT (<)** - **LTE (<=)** - **GT (>)** - **GTE (>=)** - **NOT (!=)**
value	A type specified in the type property. The value to compare to the metric collection result. Set the value to zero (**0**) to cause the status to change if the threshold is met even once.

Property	Description
timeCondition	A **timeCondition** object, which determines a time period for which the threshold must be met in order for the metric status to change. The **timeCondition** object includes the following properties: • **value**. Integer. Determines how often the metric is checked. 0 = the metric is checked every time the collection service runs. • **unit**. String. One of the following time units: SECOND MINUTE HOUR DAY

Threshold sample configuration

The example below defines actions to take for PASS and FAIL statuses:

- The metric status will change to **PASS** if the result is **OK** for more than **1 minute**.
- The metric status will change to **FAIL** if the result is not **OK** even once.

```
"thresholdPolicy": {
 "options": [
  {
   "status": "PASS",
   "type": "STRING",
   "condition": "EQ",
   "value": "OK",
   "timeCondition": {
    "value": 1,
    "unit": "MINUTE"
   }
  },
 {
  "status": "FAIL",
  "type": "STRING",
  "condition": "NOT",
  "value": "OK",
  "timeCondition": {
   "value": 0,
   "unit": "MINUTE"
  }
 }
 ]
}
```

MetricsAction

The **MetricsAction** element is an array that defines the statuses available for the threshold definition.

For example, the code sample shown above defines actions for the **PASS** and **FAIL** statuses, but not for **WARNING** statuses. In this scenario, the WARNING status should be disabled in the MetricAction array.

The **MetricsAction** array includes the following properties:

Property	Description
metric	String. Defines name of the metric, as stated in the metric's object in the metrics array.
action	String. The name of the action, as stated in the action's object in the actions array.
pass	Boolean. Determines whether the action should be triggered when the metric's status changes to **pass**.
warning	Boolean. Determines whether the action should be triggered when the metric's status changes to **warning**.
fail	Boolean. Determines whether the action should be triggered when the metric's status changes to **fail**.

System notifications enabled by default

Some AFA messages can be triggered as syslog or Issues Center messages, and others can be triggered as syslog messages only.

The following table lists the notifications enabled in AFA by default:

Metric names	Description	Syslog	Issues Center
suite_disk_space_available	**Available disk space in root partition** Notifications triggered: • **Fail** if < 5% • **Warning** if >=5% and < 10% • **Pass** if >10%	✔	✔
suite_nas_disk_space_available	**Available disk space in NAS partition** Notifications triggered: • **Fail** if < 5% • **Warning** if >=5% and < 10% • **Pass** if >10%	✔	✔
suite_data_disk_space_available	**Available disk space in data partition** Notifications triggered: • **Fail** if < 5% • **Warning** if >=5% and < 10% • **Pass** if >10%	✔	✔
suite_open_file_descriptors	**Open file descriptors** Notifications triggered: **Warning** if more than 4000 for the last 5 minutes.	✔	✔
suite_memory_available	**Available memory** Notifications triggered: **Warning** if less than 10% for the last 3 hours.	✔	✔
suite_cpu_usage	**CPU usage** Notifications triggered: **Warning** if 90% or more for the last 16 hours.	✔	✔

Metric names	Description	Syslog	Issues Center
The following: - **suite_ logstash_ service** - **suite_crond_ service,** - **suite_ elasticsearch_ service,** - **suite_httpd_ service** - **suite_kibana_ service,** - **suite_metro_ service** - **suite_mongo_ service,** - **suite_ postgresql_ service** - **suite_tomcat_ service**	**Essential linux daemons** Notifications triggered: - **Fail** if down - **Pass** if up	✔	✕
The following: - **afa_shallow_ health_check** - **abf shallow health check** - **aff_shallow_ health_check**	**Java processes health checks - shallow** Notifications triggered: - **Fail** if doesn't work for 20 seconds - **Pass** if works for 30 seconds	✔	✕

Metric names	Description	Syslog	Issues Center
The following: - **afa_deep_ health_check** - **abf deep health check** - **aff_deep_ health_check**	**Java processes health checks - deep** Notifications triggered: - **Fail** if at least one item fails for 10 minutes - **Pass** (immediately) if everything works	✔	✖
hadr_db_ replication_health	**Database replication health check**, between primary and secondary nodes in a cluster Relevant only when HA/DR and/or distributed architecture is enabled. Notifications triggered: - **Fail** if replication failed - **Pass** if replication succeeded	✔	✖
dfs_connectivity_ health_check	**Distributed file system health check** Notifications triggered: - **Fail** if down - **Pass** if up	✔	✖
suite_dist_ elements_ connection_health	**Connection health check** between central manager and load slaves / remote agents in a distributed architecture Relevant only when HA/DR and/or distributed architecture is enabled. Notifications triggered: - **Fail** if down for 2 minutes - **Pass** if up for 1 minute	✔	✖

Metric names	Description	Syslog	Issues Center
suite_cyberark_ aim_service	**Status of the CyberArk AIM service running on the ASMS host** Notifications triggered: • **Fail** if down • **Pass** if up	✔	✖
cyberark_ connectivity_ health_check	**Connection health check between ASMS and CyberArk vault** Notifications triggered: • **Fail** if check failed • **Pass** if check succeeded	✔	✔
Analysis	**Analysis results** Notifications triggered: • **Fail** if a device analysis failed • **Pass** if a device analysis succeeded **Note:** Always retrieved, even if this metric is disabled in the configuration file.	✔	✖
Monitor	**Monitoring results** Notifications triggered: • **Fail** if a device monitoring cycle failed • **Pass** if a device monitoring cycle succeeded **Note:** Always retrieved, even if this metric is disabled in the configuration file.	✔	✖

Metric names	Description	Syslog	Issues Center
Log Collection	**Traffic log collection results** Notifications triggered: • **Fail** if a device traffic log collection failed • **Pass** if a device traffic log collection succeeded **Note:** Always retrieved, even if this metric is disabled in the configuration file.	✔	✖
suite_traffic_logs_ folder_size	**Size of the traffic log collection folder** Notifications triggered: • **Pass** if the **/home/afa/.fa/syslog** folder size is lesser than or equal to **4000 Mbs** • **Warning** if the **/home/afa/.fa/syslog** folder size is greater than **4000 Mbs** • **Fail** if the **/home/afa/.fa/syslog** folder size is larger than **8000 Mbs**	✔	✔
Audit logs	**Audit log collection results** Notifications triggered: • **Fail** if a device audit log collection failed • **Pass** if a device audit log collection succeeded **Note:** Always retrieved, even if this metric is disabled in the configuration file.	✔	✖

Metric names	Description	Syslog	Issues Center
Scheduled Backup	**System backup service** Notifications triggered: - **Fail** if a scheduled backup failed - **Pass** if a scheduled backup succeeded **Note:** Always retrieved, even if this metric is disabled in the configuration file.	✔	✖

Send us feedback

Let us know how we can improve your experience with the Syslog Reference Guide.

Email us at: techdocs@algosec.com

Note: For more details not included in this guide, see the online ASMS Tech Docs.