

# Logging and Debug

## Feature Overview and Configuration Guide

### Introduction

AlliedWare Plus™ has a comprehensive debugging and logging facility in various protocols and components. This guide describes how to start and stop debugging and logging.

### Products and software version that apply to this guide

This guide applies to all AlliedWare Plus products, running version **5.4.4** or later.

Feature support and implementation varies between products. To see whether a product supports a particular feature or command, see the following documents:

- The [product's Datasheet](#)
- The product's [Command Reference](#)

These documents are available from the above links on our website at [alliedtelesis.com](http://alliedtelesis.com).

Most features described in this document are supported from AlliedWare Plus 5.4.4 or later. These features are available in later releases:

- Log type triggers are available from 5.4.7-2.1 onwards. See "[Activating Configuration Scripts with Log Message Triggers](#)" on page 21
- External logging is available from 5.4.7-1.1 onwards. See "[External logging](#)"
- The commands **copy buffered-log** and **copy permanent-log** are available from 5.4.7-1.1 onwards
- The **exclude** filter option is available from 5.4.4-4.13 onwards. See "[Configuring filters to exclude messages from logging messages in the CLI](#)" on page 19.
- From version 5.5.2-1.1 onwards, logging and debugging can be VRF-aware when configured.
- Provided that you have version 2.16.0 of the Device GUI or later installed on your device, you can access the Logging feature from the Device GUI.



# Contents

Introduction .....	1
Products and software version that apply to this guide .....	1
Debugging .....	3
Displaying debug on a terminal .....	3
Turning off debugging .....	4
Logging .....	4
Buffered logs.....	7
Permanent logs.....	8
Terminal logs .....	9
Console logs .....	10
Host logs (for syslog) .....	11
Email logs.....	13
External logging .....	14
Configuring log filters .....	16
Configuring filters in the Device GUI.....	16
Configuring filters to include logging messages in the CLI .....	18
Configuring filters to exclude messages from logging messages in the CLI.....	19
Restoring default settings .....	20
Activating Configuration Scripts with Log Message Triggers .....	21
Configuring a log message trigger.....	21
Regular expressions in log type triggers.....	22

## Debugging

Many protocols have debug commands which log protocol-specific information. For example, using the **debug mstp protocol** command results in the device writing all debugging messages generated by the MSTP algorithm to the logging system.

On using a debug command, the protocol continues to generate output until the **no** parameter is used with the command.

### Displaying debug on a terminal

To display debug output on the terminal:

#### Step 1: Turn on the debug options by using the relevant debug command

```
awplus#debug <protocol> <parameter>
```

#### Step 2: Run the terminal monitor command

```
awplus#terminal monitor
```

#### Sample Output

This is a sample output of the **debug rsvp events** command displayed on the terminal:

```
awplus#terminal monitor

Dec  2 16:41:49 localhost RSVP[6518]: RSVP: RSVP message sent to 10.10.23.60/32
via interface vlan2

Dec  2 16:41:57 localhost RSVP[6518]: RSVP: Received an RSVP message of type RSVP
Reservation from 192.168.0.60 via interface vlan2

Dec  2 16:41:57 localhost RSVP[6518]: RSVP: Received a RESV message from
10.10.23.60/32
```

The debug output will only come to the console while the terminal monitor mode is enabled.

Terminal monitor mode is disabled by the command:

```
awplus#terminal no monitor
```

Additionally, it is possible to enable terminal monitor mode for a specified number of seconds, after which it is automatically disabled. For example, to enable terminal monitor mode for just 30 seconds, use the command:

```
awplus#terminal monitor 30
```

## Turning off debugging

To turn off debugging, use the **no debug** or **undebug** command. When a protocol is specified with the **no debug** or **undebug** commands, debugging is stopped for the specified protocol.

- For example, to turn off STP debug (for STP, RSTP and MSTP), use the command:

```
awplus(config)#no debug mstp
```

- To turn off AMF debug, use the command:

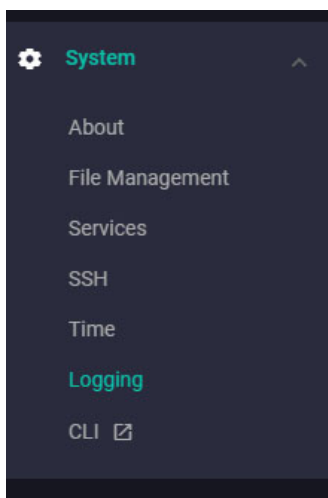
```
awplus(config)#no debug atmf
```

- To stop all debugging, use the **all** parameter with these commands.

```
awplus#undebug all
```

## Logging

Protocols generate important debugging messages by default, and send them to the logging system. Log messages can be filtered based on: the program that generated the message, the severity level of the message, the type of facility that generated the message, and substrings within the message text.



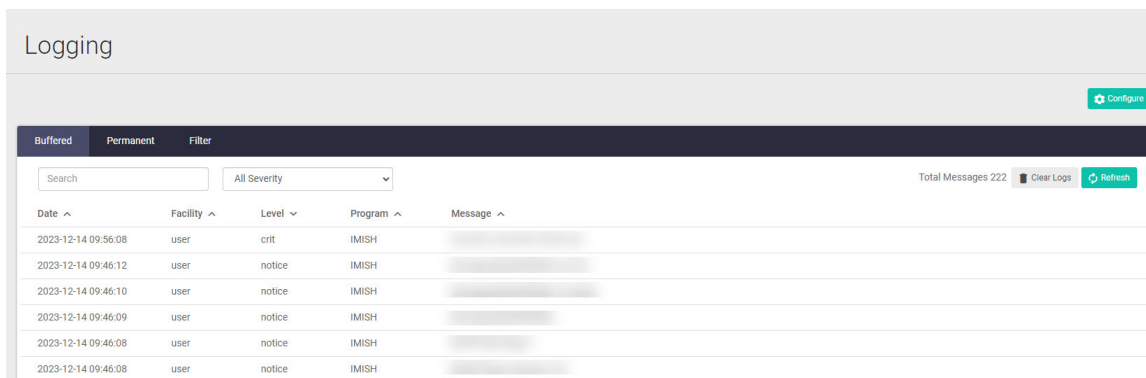
From version 2.16.0 onwards of the Device GUI, you can access the logs of the device you are configuring by clicking on **System > Logging** on the left-hand menu.

Feature locations in the Device GUI may change depending on your Device GUI version. To access the latest Logging features, we recommend you update to version 2.16.0 or later.

Navigate to the following pages to read about specific log types:

- ["Buffered logs" on page 7](#)
- ["Permanent logs" on page 8](#)
- ["Terminal logs" on page 9](#)
- ["Console logs" on page 10](#)
- ["Host logs \(for syslog\)" on page 11](#)
- ["Email logs" on page 13](#)
- ["External logging" on page 14](#)

Clicking on the Logging menu item will take you to the Logging page, where you can view and configure logging settings for your device.



### Log message format

Log messages generated by AlliedWare Plus show information in the following format:

`<date> <time> <facility>.<severity> <hostname> <program>[<pid>]: <message>`

Table 1: Elements in log messages

ELEMENT	DESCRIPTION
<code>&lt;date&gt; &lt;time&gt;</code>	The date and time when the log message was generated, according to the device’s clock.
<code>&lt;facility&gt;</code>	The facility assigned for the message.
<code>&lt;severity&gt;</code>	The severity level of the message, indicating its importance.
<code>&lt;hostname&gt;</code>	The device’s hostname, as configured by the <b>hostname</b> command (default: awplus).
<code>&lt;program&gt;</code>	Within the modular operating system, the particular program that generated the message. Some programs correspond to particular features (e.g., MSTP, EPSR), while others correspond to internal functions in the operating system (e.g. kernel).
<code>&lt;pid&gt;</code>	The process ID (PID) of the current instance of the software program that generated the message. A particular process ID does not always correspond to the same program. Some log messages, such as kernel messages, may not include a process ID.
<code>&lt;message&gt;</code>	The specific content of the log message. This may include some variable elements, such as interface names, and some strings that are fixed.

These are the severity levels for log messages:

SEVERITY IN MESSAGE	SEVERITY LEVEL	MEANING
emerg	0	Emergency: system is unusable; operation severely impaired.
alert	1	Alert: action must be taken immediately; operation has been or could be affected.
crit	2	Critical: critical conditions; issue that requires manager attention, possible problem.
err	3	Error: error conditions; issue that may require manager attention.
warning	4	Warning: warning conditions; normal notification of an event, not serious or particularly important.

SEVERITY IN MESSAGE	SEVERITY LEVEL	MEANING
notice	5	Notice: normal but significant condition; useful information, can be ignored during normal operation.
info	6	Informational: informational messages; generally unimportant everyday events.
debug	7	Debug: debug-level messages; extremely detailed (possibly high-volume) debugging information. Debug messages are only generated when debugging for a particular feature is enabled using the debug commands for that feature.

### Changing the time format in log messages

For versions 2.16.0 onwards, clicking on the **Configure** button will open the date-time format settings that the logs will display in. Note that although this is a feature that displays in the Device GUI, the change you make only applies to viewing logs in the CLI.

For versions earlier than 2.16.0, the Configure button displays the filters tab. For information about the filters tab, see "[Configuring filters in the Device GUI](#)" on page 16.

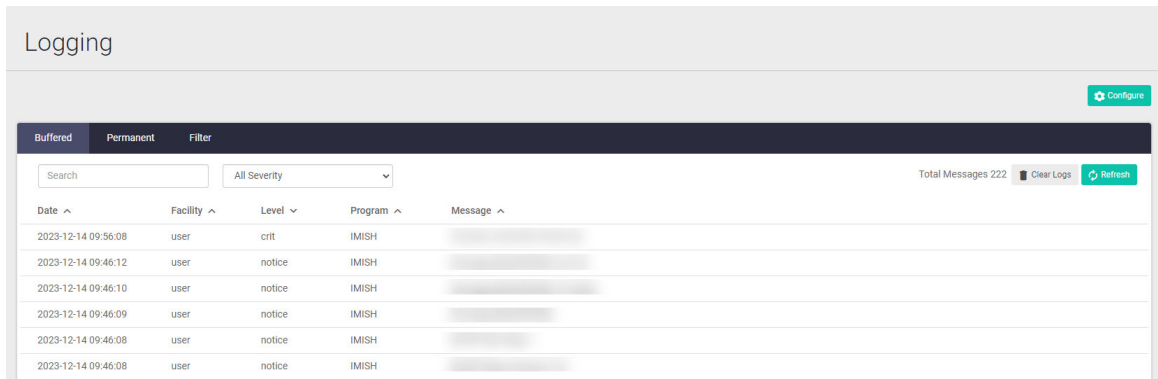
Alternatively, you can use the following command to change the date format to the ISO standard. The ISO date format is `<YYYY-MM-DD>T<hh:mm:ss><timezone-designator>`, which is a compliant of RFC3164. The syslog tools that support RFC3164 format will be able to separate out the correct date information of the input syslog message.

```
awplus(config)#log date-format iso
```

Use the command **log data-format default** to undo this change and set the date format to default.

## Buffered logs

When you first click on the **Logging** page on a device, you are met with the Buffered logs tab. This shows you the events that have been logged from your device that are not saved when the device reboots. A buffered log is a file stored in RAM on the device, and because it is stored in RAM its content does not survive a reboot of the device.



- The buffered log is enabled by default and has a filter to include messages with a severity level of 'notice' and above.
- A device can only have one instance of the buffered log.
- You can clear logs by clicking the Clear Logs button,
- or refresh logs by clicking the Refresh button.

From this page, you can also search for specific logs, and filter logs by severity. You can also change the order in which logs appear by clicking on the arrow next to the header on the table you wish to sort from.

The Buffered tab includes logs with a severity level of 'notice' and above by default.

### Buffered log commands

The buffered log can be enabled or disabled using the commands:

```
awplus#configure terminal
awplus(config)#log buffered
awplus(config)#no log buffered
```

Additional filters can be added and removed using the commands:

```
awplus(config)#log buffered {exclude|facility|level|msgtext|program|size}
awplus(config)#no log buffered {exclude|facility|level|msgtext|program|size}
```

The following log buffered commands are available:

Table 2:

COMMAND	DESCRIPTION
show log	Display the entire contents of the buffered log.
show log tail	Display the 10 most recent entries in the buffered log.
show log tail <10-250>	Display a specified number of the most recent entries in the buffered log.
show log config	Display the configuration of all log outputs.
log buffered size	Specify the amount of memory the buffered log may use.
clear log	Remove the contents of the buffered log and permanent log.
clear log buffered	Remove the contents of the buffered log only.
copy buffered-log	Copy the contents of the buffered log to a destination file in a different external or internal location. This command is available from 5.4.7-1.1 onwards.
default log buffered	Restore the buffered log to its default configuration.

## Permanent logs

Clicking on the Permanent tab will show you all of the permanent logs that are stored on your device.

Date	Facility	Level	Program	Message
2023-12-14 09:56:08	user	crit	IMISH	
2023-12-14 09:46:08	user	warning	IMI	
2023-12-14 09:25:44	kern	err	kernel	
2023-12-14 09:25:41	kern	warning	kernel	
2023-12-14 09:25:41	kern	warning	kernel	
2023-12-14 09:25:34	daemon	err	pppd	

You can filter through this list by clicking the arrow next to the header on the table you wish to sort from. A permanent log is a file stored in NVS on the device, unless the device has no NVS, in that case it is stored in Flash.

Permanent logs are retained when the device reboots.

The Permanent tab includes logs with a severity level of ‘warning’ and above by default.

On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

A device can only have one instance of the permanent log. The permanent log is enabled by default and has a filter to include messages with a severity level of “warning” and above.



## Permanent log commands

The permanent log can be enabled or disabled using the commands:

```
awplus#configure terminal
awplus(config)#log permanent
awplus(config)#no log permanent
```

The following log permanent commands are available:

COMMAND	DESCRIPTION
show log permanent	Display the entire contents of the permanent log.
show log permanent tail	Display the 10 most recent entries in the permanent log.
show log permanent tail <10-250>	Display a specified number of the most recent entries in the permanent log.
show log config	Display the configuration of all log outputs.
log permanent size	Specify the amount of memory the permanent log may use.
clear log	Remove the contents of the buffered log and permanent log.
clear log permanent	Remove the contents of the permanent log only.
copy permanent-log	Copy the contents of the permanent log to a destination file in a different external or internal location. This command is available from 5.4.7-1.1 onwards.
default log permanent	Restore the permanent log to its default configuration.

## Terminal logs

Terminal logging displays all log messages on the console as they occur. By default this includes messages at **informational** and **debugging** severity level. It can be useful for troubleshooting but can also result in large numbers of messages displaying on the console.

The terminal log can be enabled using the commands:

```
awplus#configure terminal
awplus(config)#debug <protocol> [<parameter>]
awplus(config)#exit
awplus#terminal monitor
```

To turn off terminal logging use the command:

```
awplus#terminal no monitor
```

From 5.4.8-0.2 onwards, you can also use the command:

```
awplus#no terminal monitor
```

To limit the terminal monitor output, use the following commands:

1. First remove the default filter:

```
awplus(config)#no log monitor level debugging
```

2. Then add a filter that describes the messages you wish to see, for example OSPF:

```
awplus(config)#log monitor program ospf
```

COMMAND	DESCRIPTION
default log terminal	Restores the default settings for log messages sent to the terminal when a <b>log terminal</b> command is issued. By default all messages are sent to the console when a <b>log terminal</b> command is issued.
terminal (filter)	Creates a filter to select messages to be sent to all consoles when the <b>log terminal</b> command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

## Console logs

This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the device's main console port. Terminal log and console log **cannot** be set at the same time. If console logging is enabled then the terminal logging is turned off.

The console log can be enabled or disabled using the commands:

```
awplus#configure terminal
```

```
awplus(config)#log console
```

```
awplus(config)#no log console
```

The following log console commands are available:

COMMAND	DESCRIPTION
<code>default log console</code>	Restores the default settings for log messages sent to the terminal when a <b>log console</b> command is issued. By default all messages are sent to the console when a <b>log console</b> command is issued.
<code>console (filter)</code>	Creates a filter to select messages to be sent to all consoles when the <b>log console</b> command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.
<code>log console exclude</code>	Removes the contents of the buffered log (and permanent log if it exists).
<code>show log config</code>	Displays information about the logging system. This includes the configuration of the various log destinations, buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each of these destinations.

## Host logs (for syslog)

A host log sends log messages to a remote syslog server. A device may have many syslog hosts configured.

The host log can be enabled or disabled using the commands:

```
awplus#configure terminal
awplus(config)#log host <ipv4-addr>
awplus(config)#log host <ipv6-addr>
awplus(config)#no log host <ipv4-addr>|<ipv6-addr>
```

where: *<ipv4-addr>* or *<ipv6-addr>* is the IP address of the remote syslog server.

You can also create a secure log destination using the **secure** parameter and specify the SSL certificates by **log trustpoint** command. It is only available for IPv4 hosts. For more information about how to create a trustpoint, refer to the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#).

If a remote syslog server resides within a named VRF, it can be enabled or disabled with the VRF parameter:

```
awplus#configure terminal
awplus(config)#log host <ipv4-addr>|<ipv6-addr> vrf <name> [secure]
awplus(config)#no log host <ipv4-addr>|<ipv6-addr> vrf <name>
```

For more details on VRFs, see the [VRF-lite Feature Overview and Configuration Guide](#)

**Example** The following configuration example shows for a named VRF called 'red':

```
ip vrf red 1
```

The following configuration example shows for a remote host '10.38.201.1' in VRF 'red' with a filter for debug messages:

```
log host 10.38.201.1 vrf red
log host 10.38.201.1 vrf red level debugging
```

A hostname also can be used in place of an IPv4 or IPv6 address, but only for hosts not within a VRF:

```
awplus(config)#log host <name> [secure]
```

**Note:** The 'Extended Key Usage' field should be configured in the certificates, and the purpose should be correct during the certificate validation between clients (clientAuth) and server (serverAuth), or the SSL connection will not be established

```
awplus#configure terminal
awplus(config)#log trustpoint <trustpoint-name>
awplus(config)#log host <ipv4-addr> [secure]
```

There are no default filters associated with host outputs when they are created. Filters can be added and removed using various parameters of the **log host** command.

It is not possible to view the log messages sent to this type of output as they are not retained on the device. They must be viewed on the remote device.

The other host log commands are:

COMMAND	DESCRIPTION
show log config	Displays the configuration of all log outputs.
log host time	Adjust the time information in messages to a time zone other than the one configured on this device.
default log host <ip-address>	Restores the device default settings for log sent to a remote syslog server.
log facility	Specifies an outgoing syslog facility. This determines where the syslog server will store the log messages. (Available with 5.4.6-0.1 and later.)
log host source	Specifies a source interface or IP address for the device to send syslog messages from. This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses. (Available with 5.4.6-0.1 and later.)
log host startup-delay	Changes the delay between the device booting up and it attempting to connect to remote log hosts. This delay period allows time for network connectivity to the remote host to be established. During this period, the device buffers log messages and sends them once it has connected to the remote host. You can change the delay period and the number of messages buffered.

## Email logs

An email log sends log messages to an email address. A device may have many email logs configured.

The email log can be enabled or disabled using the commands:

```
awplus#configure terminal
awplus(config)#log email <email-address> {exclude|facility|level|msgtext|
program|time}
awplus(config)#no log email <email-address> {exclude|facility|level|
msgtext|program|time}
```

where *<email-address>* is the destination email address.

It is not possible to view the log messages sent to this type of output as they are not retained on the device. They must be viewed by the email recipient.

The other email log commands are:

COMMAND	DESCRIPTION
show log config	Displays the configuration of all log outputs.
log email time	Adjusts the time information in messages to a time zone other than the one configured on this device.
default log email <email-address>	Restores the device’s default settings for log messages sent to an email address.

**Note:** An email server and “from” address must be configured on the device in order for email logs to work:

- mail from <email-address>
- mail smtp <ip-address> |<domain-name>

Where the **<email-address>** is the “From” field on the sent email, and the **<ip-address>** or **<domain-name>** is the email’s destination SMTP server. Specifying the server by using its domain name is only available from software version 5.4.7-1.1 onwards.

Email logs are sent in batches of approximately 20 messages and have the subject line “Log messages”.

- For more information about email and mail, see the [Mail \(SMTP\) Feature Overview and Configuration Guide](#).

## External logging

External logging sends syslog messages to a file on a USB memory device or SD card. It is available from software version 5.4.7-1.1 onwards.

External logging can be enabled or disabled using the commands:

```
awplus#configure terminal
awplus(config)#log external <filename>
```

For example, to save messages to a file called “messages.log” in a directory called “log” on a USB stick, use the command:

```
awplus(config)#log external usb:/log/messages.log
```

If the file does not already exist on the memory device, it (and any specified subdirectory) will be automatically created. If the file already exists, messages are appended to it.

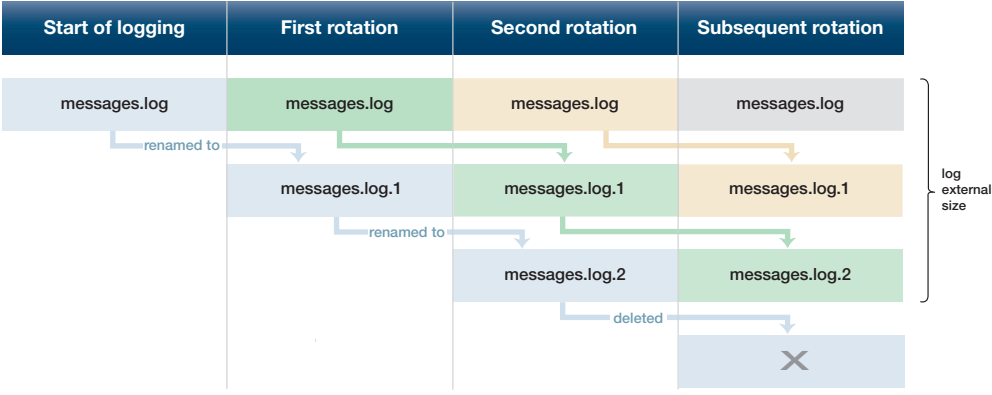
We strongly recommend using ext3 or ext4 as the file system on the external memory device. These file systems have a lower risk of file corruption occurring if the switch or firewall loses power.

You should also unmount the memory device before removing it from the switch or firewall, to avoid corrupting the log file. To unmount the device, use the **unmount** command.

If you are using this on a VCStack, each stack member needs to have its own external memory device. Enabling or disabling external logging enables or disables it on all stack members.

The other external log commands are:

COMMAND	DESCRIPTION
show log config	Displays the configuration of all log outputs. This lets you see if the external logging is functioning by checking that the status is enabled.
show log external	Displays the contents of the external log.
log external size <50-4194304>	Configures the total amount of size that the external log is permitted to use, in kilobytes. The maximum possible depends on the memory device’s file system. The default maximum size is 50 kBytes. Note that if you are rotating between multiple files, this is the maximum size of all files, not of each individual file. For example, if you are rotating between 2 files (log external rotate 1), each file will have a maximum size of 25 kBytes by default.
log external rotate <0-255>	Configures the number of files that the external log can rotate through. For example, the diagram below shows how setting rotate to 2 makes the device rotate through 3 files. The default is 1, which rotates between the initial file and 1 additional file (e.g. messages.log and messages.log.1). Note that if you set rotate to 0, and the external log file becomes full, then the device deletes the full log file and creates a new (empty) file of the same name to save messages into. For this reason, we recommend setting rotate to at least 1.

COMMAND	DESCRIPTION
	
<pre>clear log external</pre>	Delete the external log file.
<pre>default log external</pre>	Restores the device's default settings for external logging.

## Configuring log filters

You can create a filter to select messages to be sent to each of the log output types. You can filter on the priority/severity level of the message, the program that generated the message, the logging facility used, a sub-string within the message, or a combination of some or all of these.

For example the command syntax for the permanent log is:

```
log permanent [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
```

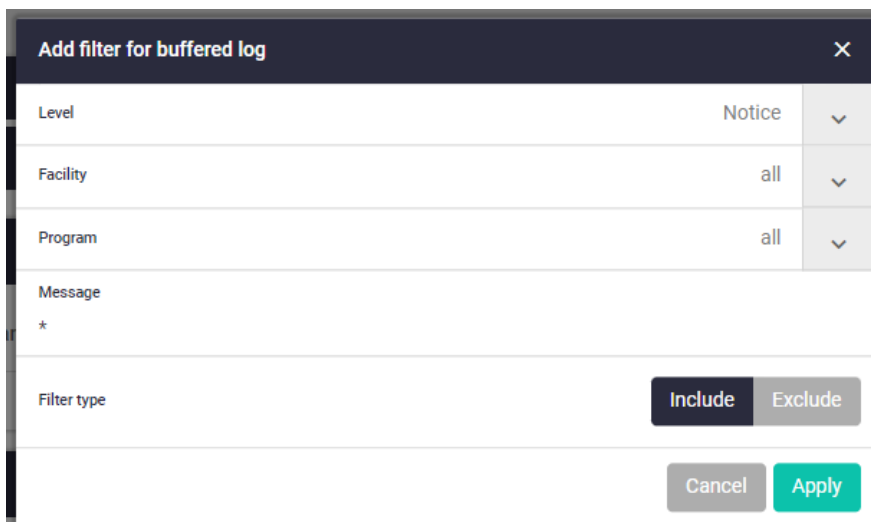
## Configuring filters in the Device GUI

The Local filters tab provides the filter settings for the Buffered and Permanent log tabs. You can add new filters or change the default log filters from this page.



- To add a log filter, click **+ New Filter** next to the log you wish to filter.

For example, clicking **+ New Filter** next to the Buffered log filter table will display the Add filter dialogue box.



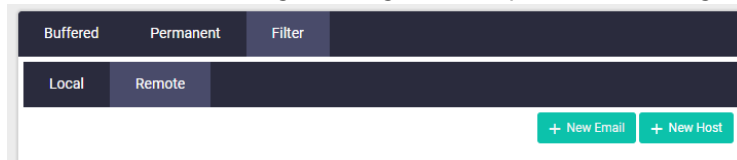
You can filter by Level, Facility, Program, Message, and choose to either include or exclude logs of this type.



## Remote filters

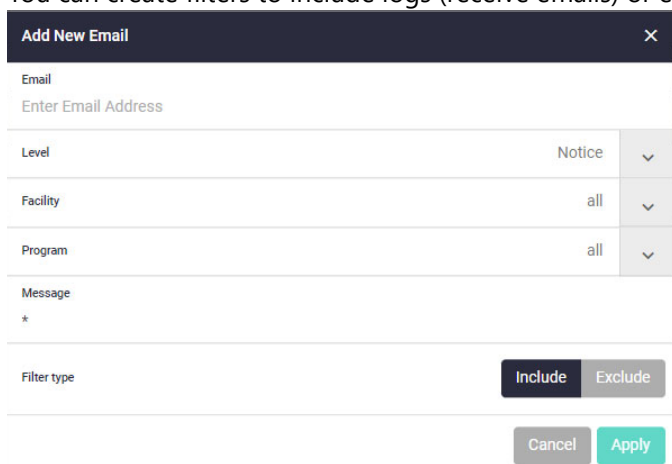
The Remote log filters tab enables you to filter specific log notifications to an email or host (syslog server) of your choice.

For example, you can create a list of separate filters in order of importance, so you only receive notifications for warning level logs with a specific text string.



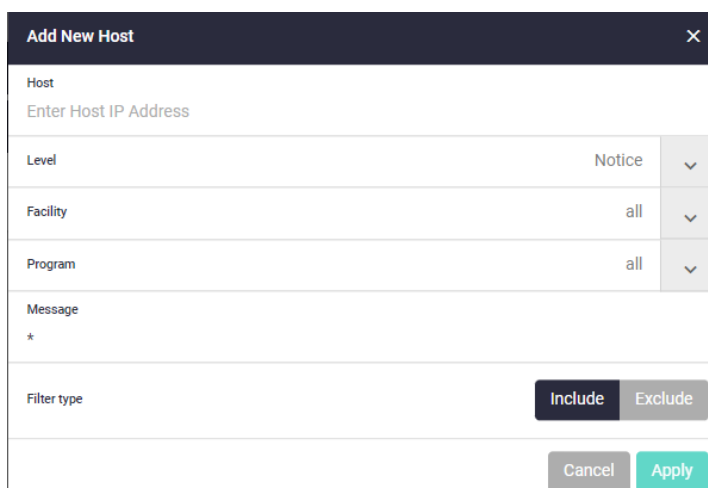
- To specify which log messages to receive emails about, click **+ New Email**.

You can create filters to include logs (receive emails) or exclude logs (don't receive emails).



- To specify which log messages to send to a host (syslog server) click **+ New Host**.

You can create filters to include logs (receive notifications), or exclude logs (don't receive notifications).



## Configuring filters to include logging messages in the CLI

Here are two examples of configuring filters to include messages into different types of logging output:

1. To save all messages in the buffered log if they are generated by EPSR and have a severity of **informational** or higher, use the following commands:

```
awplus#configure terminal
awplus(config)#log buffered level informational program epsr
```

2. To save a **specific part(s)** of messages in the buffered log.

For example:

To filter **only** the OSPF message (**SEND[Hello]: To 224.0.0.5 via vlan1:172.16.101.2, length 44**) to appear on the console, or in "show log", use the following command:

```
awplus(config)#log buffered program ospf msgtext To 224.0.0.5 via
vlan1:172.16.101.2, length 44
```

Figure 1 below shows some unfiltered OSPF debug output, but by using the filter to include only the "SEND[Hello]..." text, we get the filtered output shown in Figure 2.

Figure 1: Unfiltered section of debug

```
awplus#12:11:03 x930 OSPF[1893]: IFSM[vlan1:172.16.101.2]: Hello timer expire
12:11:03 x930 OSPF[1893]: SEND[Hello]: To 224.0.0.5 via vlan1:172.16.101.2,length 44
12:11:03 x930 OSPF[1893]: -----
12:11:03 x930 OSPF[1893]: Header
12:11:03 x930 OSPF[1893]:   Version 2
12:11:03 x930 OSPF[1893]:   Type 1 (Hello)
12:11:03 x930 OSPF[1893]:   Packet Len 44
12:11:03 x930 OSPF[1893]:   Router ID 9.9.9.9
12:11:03 x930 OSPF[1893]:   Area ID 0.0.0.0
12:11:03 x930 OSPF[1893]:   Checksum 0xd87a
12:11:03 x930 OSPF[1893]:   AuType 0
12:11:03 x930 OSPF[1893]: Hello
12:11:03 x930 OSPF[1893]:   NetworkMask 255.255.0.0
12:11:03 x930 OSPF[1893]:   HelloInterval 10
12:11:03 x930 OSPF[1893]:   Options 0x2 (-|-|-|-|-|E|-)
12:11:03 x930 OSPF[1893]:   RtrPriority 1
12:11:03 x930 OSPF[1893]:   RtrDeadInterval 40
12:11:03 x930 OSPF[1893]:   DRouter 172.16.101.2
12:11:03 x930 OSPF[1893]:   BDRouter 0.0.0.0
12:11:03 x930 OSPF[1893]:   # Neighbors 0
12:11:03 x930 OSPF[1893]: -----
```

Figure 2: Filtered section of debug

```
awplus#debug ospf all
awplus#clear log
awplus#show log
  <date> <time> <facility>.<severity> <program[<pid>]>: <message>
  -----
2016 Nov 20 12:14:09 user.notice x930 IMISH[676]: show log
2016 Nov 20 12:14:14 user.info   x930 OSPF[1893]: SEND[Hello]: To 224.0.0.5 via
vlan1:172.16.101.2, length 44
```

The filter has put a specific debug message into the log, without you having to turn on terminal monitor, and without flooding the console or log with unneeded debug messages.

## Configuring filters to **exclude** messages from logging messages in the CLI

With version 5.4.4-4.13 and later you can drop unwanted log messages. For example, you can drop low priority log messages that are overfilling the log files. Use this with caution, to avoid dropping important messages.

To configure the device to drop logs, specify the level, program, facility, or message text you want to drop, and use the **exclude** parameter to specify to drop them. The **exclude** parameter option is available for all types of log output with version 5.4.4-4.13 and later. For example, the syntax for the buffered log is:

```
log buffered exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]
```

**Example** Consider a situation where you often see log messages such as the following, which are harmless, but may be frustrating:

```
CoreSw EXFX[3101]: DBG:exfx_rxtx_rxInvalidPktPrint 358: Invalid packet RX'ed dmac
001e.67a7.0501 smac eccd.6d7b.3d92 ethertype 0800
CoreSw EXFX[3101]: DBG:exfx_rxtx_rxInvalidPktPrint 358: Invalid packet RX'ed dmac
001e.67a7.0501 smac eccd.6d7b.3d92 ethertype 0800
CoreSw EXFX[3101]: DBG:exfx_rxtx_rxPktSourceSet 339: Packet RX'ed with no ifindex srcDevNum 1
srcPortNum 61 vlan 1 cpuCode 473
```

You can filter these out by either filtering on the message text, or filtering on the program EXFX combined with level of “error”:

- Filtering on the message text:

You can filter out these messages by specifying the message text. The following examples use a **msgtext** filter to exclude logs from both the permanent log (**show log permanent**), and the buffered log (**show log**).

```
awplus(config)#log permanent exclude msgtext exfx_rxtx_rxInvalidPktPrint
awplus(config)#log permanent exclude msgtext exfx_rxtx_rxPktSourceSet
```

```
awplus(config)#log buffered exclude msgtext exfx_rxtx_rxInvalidPktPrint
awplus(config)#log buffered exclude msgtext exfx_rxtx_rxPktSourceSet
```

Note that if you only base your filter on the message text, you will filter logs containing the specified text from all programs and severity levels.

- Filtering on program **EXFX** and level **error**, as well as specifying the message text:

Specifying the program and level as well as the message text ensures you only exclude the messages you actually intend to. We recommend using this instead of a filter that only specifies the message text, in case logs from other programs contain the same message text.

```
awplus(config)#log permanent exclude level errors program EXFX msgtext
exfx_rxtx_rxInvalidPktPrint
awplus(config)#log permanent exclude level errors program EXFX msgtext
exfx_rxtx_rxPktSourceSet
```

## Restoring default settings

The following commands will restore logging configuration to defaults for each logging destination. This will undo and remove all filters for the specified destination. This is useful if there are a lot of log filters configured. Alternatively, you can remove specific configuration by using the standard **no** configuration command.

COMMAND	DESCRIPTION
default log buffered	Restores the buffered log stored in RAM to its default configuration. By default the size of the buffered log is 50 kB and it accepts messages with a severity level of notifications and above.
default log permanent	Restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with a severity level of warnings and above.
default log host <ip-addr>	Restores the device default settings for logs sent to a remote syslog server. By default no filters are defined for remote syslog servers. This command also restores the remote syslog server time offset value to local (no offset).
default log console	Restores the console log to its default configuration. By default all messages are sent to the console when a log console command is issued.
default log email	Restores the email log to its default configuration. By default no filters are defined for email addresses.
default log external	Restores the external log to its default configuration. By default, the size of the external log is 50 kB, it rotates through 1 additional file, and it accepts messages with a severity level of notices and above.

# Activating Configuration Scripts with Log Message Triggers

This feature is supported from AlliedWare Plus version 5.4.7-2.1.

You can configure a trigger to activate a configuration script when a particular string is generated in log messages of severity level notice or higher. The log message string can be filtered by including regular expressions (PCRE).

This section describes the general steps to configure a trigger to activate by a log message, and some simple syntax and examples for using regular expressions to match log messages for triggers.

## Configuring a log message trigger

### Step 1: Create a command script

Create a command script with the commands you would like executed when the trigger conditions are met. Either create a script on a PC then load it onto your device using the **copy (URL)** command, or create the command script directly on the device using the CLI, using the command:

```
awplus#edit [<filename>]
```

Note that any command executed by the script will generate a log message with level notice, and will include '[SCRIPT]' before the command string. Therefore, if something in the script matches the configured log message trigger string, it will retrigger indefinitely.

### Step 2: Enter the trigger configuration mode

You must be in Global Configuration mode to reach Trigger Configuration mode; use the command:

```
awplus#configure terminal
```

To create a trigger and enter its configuration mode, use the command:

```
awplus(config)#trigger <1-250>
```

### Step 3: Set the trigger type to log

The trigger type determines how the trigger is activated. To set the trigger to activate if a particular string is generated in a log message, use the command:

```
awplus(config-trigger)#type log <log-message-string>
```

Regular expressions (PCRE) are fully supported in the log message string ("[Regular expressions in log type triggers](#)" on page 22). Triggers are only activated by log messages of severity level notice (5) or higher. Log type triggers are limited to activating at most once per second.

### Step 4: Add the scripts to the trigger

You can add up to five scripts to the trigger. When a trigger is activated, it executes the scripts in sequence, with the lowest numbered script activated first. The first script runs to completion before the next script begins. To add a script, use the command:

```
awplus(config-trigger)#script <1-5> <filename>
```

**Step 5: Specify a description for the trigger**

Specify a description for the trigger, so that you can easily identify the trigger in show commands and log output. Use the command:

```
awplus(config-trigger)#description <description>
```

**Step 6: Verify the trigger's configuration**

To check the configuration of the trigger, use the command:

```
awplus(config-trigger)#show trigger [<1-250>|counter|full]
```

Triggers can also be configured to activate only on particular days, particular times during the day, for a limited number of repetitions, and for other types of events.

For more information about configuring triggers, see the [Triggers Feature Overview and Configuration Guide](#) and the 'Trigger Commands' chapter in the Command Reference for your device.

**Regular expressions in log type triggers**

Log type triggers fully support regular expressions using PCRE (Perl-Compatible Regular Expression) syntax. The following table shows some of the common syntax elements.

Syntax	Description
.	Use for any character.
\d	Use for any number.
*	Use for 0 or more occurrences of the preceding element.
+	Use for 1 or more occurrences of the preceding element.
()	Use parentheses for grouping.
	Use to separate alternatives (or).
[]	Use brackets to enclose a set of characters.

**Examples** Regular expressions can be used in the log message string to select a log messages to activate a script. The following examples show possible log type triggers using regular expressions.

To activate a trigger when a log message includes:

- a port identifier followed by a 'failed' message, use the command:

```
awplus(config-trigger)# type log port.+ failed
```

- a 'joined' message from any stack member:

```
awplus(config-trigger)# type log Stack member \d has joined
```

- a 'joined' message from a set of specific stack members (1, 2 or 3), use the command:

```
awplus(config-trigger)# type log Stack member [1-3] has joined
```

- a message mentioning an interface including either 'failed' or 'succeeded', use the command:

```
awplus(config-trigger)# type log Interface [a-z]* {succeeded|failed}
```

C613-22059-00 REV J



**NETWORK SMARTER**

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895

**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830

**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

[alliedtelesis.com](http://alliedtelesis.com)

© 2024 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.