Technical Guide

UAMD Log & UAM Filter

Released: 2018-08-08
Doc Rev. No: R1

Table of Contents

1 Introduction

Universal access method (UAM) has become a popular method for network service providers, particularly Wi-Fi service providers, to grant or deny access to more network resources to users connected to the wired or wireless networks they manage. UAM involves presenting a web page in a browser to the connected users, so that the users can login to access more network resources.

UAM is also one of the authentication methods supported by the EWS controller, besides other authentication methods such as 802.1X authentication and auto login by the controller based on the MAC addresses and/or IP addresses of the devices used. Furthermore, the EWS controller also supports customization to the behavior of UAM through a UAM filter and provides UAMD log.

1.1 UAM Filter

If user agent strings in non-browser http requests from clients match any of the entries in the UAM Filter at least partially, these requests would be dropped. On modern devices, many applications may be running in the background and may attempt to access the Internet for updates or data synchronization, but these requests may be redirected without using a browser so that the login page cannot be displayed. The high frequency of these processes may overload the system CPU even before login, and with UAM filter, these requests can be dropped to help prevent unnecessary CPU workload for your system.

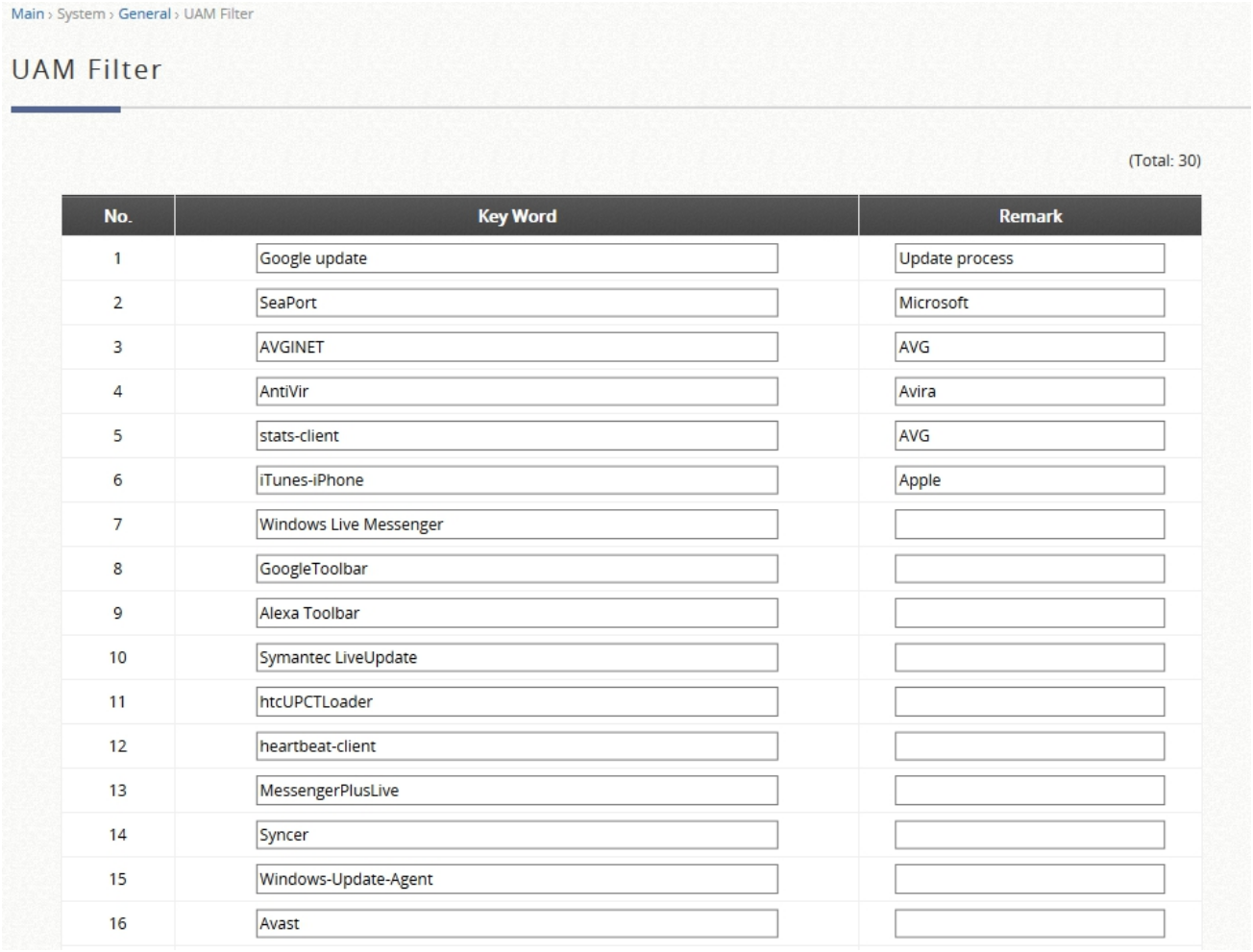
1.2 UAMD Log

In the UAMD log, UAM related outputs from the UAM daemon are displayed. The log can be displayed in one of the two formats – Extended Log Format and Common Log Format. ELF is a standardized text file format that is used by web servers when generating log files much like the CLF, but ELF files provide more information and greater flexibility.

2 Configurations

2.1 How to Configure UAM Filter

a. Go to *System > General > UAM Filter*, add the respective User Agent into the list to block unnecessary background applications attempting to have internet access for updates or synchronization, such as Antivirus “Avast”.


Main › System › General › UAM Filter

UAM Filter

(Total: 30)

No.	Key Word	Remark
1	Google update	Update process
2	SeaPort	Microsoft
3	AVGINET	AVG
4	AntiVir	Avira
5	stats-client	AVG
6	iTunes-iPhone	Apple
7	Windows Live Messenger	
8	GoogleToolbar	
9	Alexa Toolbar	
10	Symantec LiveUpdate	
11	htcUPCTLoader	
12	heartbeat-client	
13	MessengerPlusLive	
14	Syncer	
15	Windows-Update-Agent	
16	Avast	

In addition, if for some special reason the network administrators would like to prevent the web sheet on mobile devices from showing, the following entries may be added to the UAM Filter.

2.2 How to Enable and Interpret Messages in UAMD Log

a. Go to *Status > Logs and Reports> UAMD Log* and select ELF format to get more detailed information. Below is a table from different browsers/OS. Please keep in mind that it is important to make sure that you have enabled authentication in the Service Zone(s) to properly gather the information in the UAMD Log.

Browser	OS	User Agent
Firefox	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Chrome	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

		(KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Internet Explorer	Windows 10	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Safari	MAC OS X	Mac OS X: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3.8

b. Below is an example from UAMD Log to determine what Browser and Operating System is used.

10.29.139.119 [13/Oct/2017:17:31:03 +0800] "GET /redirect HTTP/1.1" ***Host: www.msftconnecttest.com*** *"User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36"*

10.29.139.119 [13/Oct/2017:18:32:12 +0800] "GET /success.txt HTTP/1.1" ***Host: detectportal.firefox.com*** *"User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0"*

Breakdown: Client IP Address [Timestamp] "GET /_____ HTTP/1.1" **Host:** _____ "User Agent:_____ "

c. If you have properly added the correct keyword into the UAM Filter, you will see the following request rejected by the EWS controller

10.29.139.40 [13/Oct/2017:09:31:12 +0800] "GET /iavs9x/servers.def.vpx HTTP/1.1" ***Host: r5525652.iavs9x.u.avast.com*** *"User-Agent: avast! Antivirus (instup)" [reject]*

3 Remarks

Please contact Edgecore's Technical Support Team at ecwifi@edge-core.com for additional inquiries.