RSA NetWitness Platform

Event Source Log Configuration Guide



McAfee Web Gateway

Last Modified: Friday, February 14, 2020

Event Source Product Information:

Vendor: McAfee Event Source: Web Gateway Versions: 6.8.5, 7.x, 8.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

Additional Downloads:

- nicsftpagent.conf.mcafeewg1
- nicsftpagent.conf.mcafeewg2

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later Event Source Log Parser: mcafeewg Collection Method: File, Syslog Event Source Class.Subclass: Host.Web log To configure McAfee Web Gateway to work with RSA NetWitness Platform, complete one of the following:

- Configure Syslog Collection
- Configure File Collection

Configure Syslog Collection

To configure syslog collection, you must complete these tasks:

- I. Customize McAfee Web Gateway Logs
- II. Configure Syslog Collection for McAfee Web Gateway version 7.x or 8.x
- III. Configure RSA NetWitness Platform for Syslog Collection

Customize McAfee Web Gateway Logs

To customize McAfee Web Gateway logs for version 7.0 and later:

- 1. Open a browser and log on to the McAfee Web Gateway appliance with administrative credentials.
- 2. Click the Policy tab.
- 3. Click the Settings tab in the left menu.
- 4. Expand Engines > File System Logging.
- 5. Click Access Log Configuration.
- 6. In the File System Logging Settings window, ensure the settings are as follows:
 - a. In the Name of the log field, type:

access.log

- b. Select Enable log buffering and Enable header writing.
- c. In the Log header field, type:

```
#time_stamp src_ip auth_user server_name cache_status server_ip url_
port "method" "url" event protocol bytes_from_client bytes_from_
server user_agent "referrer " block_res
```

- 7. Click Save Changes.
- 8. From the File System Logging menu, click Found Viruses Log.
- 9. In the File System Logging Settings window, ensure the settings are as follows:

a. In the Name of the log field, type:

foundviruses.log

- b. Select Enable log buffering and Enable header writing.
- c. In the Log header field, type:

#time_stamp "auth_user" "src_ip" "virus_name" "url"

10. Click Save Changes.

Configure Syslog Collection for McAfee Web Gateway version 7.x

To configure Syslog Collection for McAfee Web Gateway version 7.x

- 1. Open a browser and log on to the McAfee Web Gateway appliance with administrative credentials.
- 2. Click on the **Configuration** tab.
- 3. On the left panel, click File Editor.
- 4. Expand the mwgappl folder, then click on the rsyslog.conf file
- 5. In the file, look for a line similar to the following:

*.info;mail.none;authpriv.none;cron.none /var/log/messages

Replace it with the line below:

*.info;daemon.!=info;mail.none;authpriv.none;cron.none -/var/log/messages

6. In the rsyslog.conf file, after the line that says local7.* /var/log/boot.log insert the following line:

daemon.info @**SA-IP_addr:**514

where *SA-IP_addr* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector

Note: This line should be inserted before the *# ####* begin forwarding rule *####* message. Refer to the McAfee Community docs for the correct amount of spacing needed.

7. Click Save Changes.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

- 1. In the NetWitness menu, select ADMIN > Services.
- In the Services grid, select a Log Decoder, and from the Actions menu, choose View > Config.
- 3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is mcafeewg.

Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

- 1. In the NetWitness menu, select ADMIN > Services.
- In the Services grid, select a Log Decoder, and from the Actions menu, choose View > System.
- 3. Depending on the icon you see, do one of the following:

- If you see [•] Start Capture</sup>, click the icon to start capturing Syslog.
- If you see [•] Stop Capture</sup>, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

- 1. In the NetWitness menu, select ADMIN > Services.
- In the Services grid, select a Remote Log Collector, and from the Actions menu, choose View > Config > Event Sources.
- 3. Select Syslog/Config from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

The Available Event Source Types dialog is displayed.

- 5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
- 6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

After you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Configure File Collection

To configure File collection, you must complete these tasks:

- I. Customize McAfee Web Gateway
- II. Set up SFTP Agent
- III. Configure the RSA NetWitness Platform Log Collector for File Collection

Customize McAfee Web Gateway Logs

To customize McAfee Web Gateway logs for version 6.8.5:

- 1. Open a browser and log on to the McAfee Web Gateway appliance with administrative credentials.
- 2. Click the **Reporting** tab.
- 3. In the Overall Reporting section, click Log File Management.
- 4. To customize the HTTP Access logs, follow these steps:
 - a. In the HTTP Access Log section, click Customize HTTP Access Log.
 - b. In the HTTP Access Log field of the Log File Structure section, type:

```
time_stamp src_ip auth_user server_name cache_status server_ip url_
port "method" "url" event protocol bytes_from_client bytes_from_
server user_agent "referer" block_res
```

- c. Click Apply Changes.
- 5. To customize the HTTP Access Denied logs, follow these steps:
 - a. In the HTTP Access Denied Log section, click Customize HTTP Access Denied Log.
 - b. In the HTTP Access Denied Log field of the Log File Structure section, type:

```
time_stamp src_ip auth_user server_name cache_status server_ip url_
port "method" "url" event protocol bytes_from_client bytes_from_
server user_agent "referer" block_res
```

- c. Click Apply Changes.
- 6. To customize the security logs, follow these steps:

- a. In the Security Log section, click Customize Security Log.
- b. In the Security Log field of the Log File Structure section, type:

```
time_stamp "object_id" status_code media_type extension media_type_
status
```

- c. Click Apply Changes.
- 7. To customize the Found Viruses logs, follow these steps:
 - a. In the Found Viruses Log section, click Customize Found Viruses Log.
 - b. In the Found Viruses Log field of the Log File Structure section, type: time_stamp "virus_name" "file_name" "media_type" infected_status
 - c. Click Apply Changes.

To customize McAfee Web Gateway logs for version 7.0 and up:

- 1. Open a browser and log on to the McAfee Web Gateway appliance with administrative credentials.
- 2. Click the **Policy** tab.
- 3. Click the Settings tab in the left menu.
- 4. Expand Engines > File System Logging.
- 5. Click Access Log Configuration.
- 6. In the File System Logging Settings window, ensure the settings are as follows:
 - a. In the Name of the log field, type:

access.log

- b. Select Enable log buffering and Enable header writing.
- c. In the Log header field, type:

```
#time_stamp src_ip auth_user server_name cache_status server_ip url_
port "method" "url" event protocol bytes_from_client bytes_from_server
user_agent "referrer " block_res
```

- 7. Click Save Changes.
- 8. From the File System Logging menu, click Found Viruses Log.
- 9. In the File System Logging Settings window, ensure the settings are as follows:
 - a. In the **Name of the log** field, type:

foundviruses.log

- b. Select Enable log buffering and Enable header writing.
- c. In the Log header field, type:

#time stamp "auth user" "src ip" "virus name" "url"

10. Click Save Changes.

Set Up the SFTP Agent

To set up the SFTP Agent Collector, download the appropriate PDF from RSA Link:

- To set up the SFTP agent on Windows, see Install and Update SFTP Agent
- To set up the SFTP agent on Linux, see Configure SFTP Shell Script File Transfer

Configure the Log Collector for File Collection

Perform the following steps to configure the Log Collector for File collection.

To configure the Log Collector for file collection:

- 1. In the NetWitness menu, select ADMIN > Services.
- In the Services grid, select a Log Collector, and from the Actions menu, choose View > Config > Event Sources.
- 3. Select File/Config from the drop-down menu.

The Event Categories panel displays the File event sources that are configured, if any.

4. In the Event Categories panel toolbar, click +.

The Available Event Source Types dialog is displayed.

RSA RESPOND INVESTIGAT	E MONITOR CONFIGURE ADMIN
Hosts Services Event So	urces Endpoint Sources Health & Well
A Change Service	- Log Collector Config ©
General Remote Collectors F	Files Event Sources Event Destinations Settin
File 💙 Config	~
Event Categories Sc	Available Event Source Types
+ -	Name ^
Name	acf2
	acf2tvm
	apache
	apachetomcat
	artart
	artie
	artrequest
	bluecoat_eim
	Cancel OK

5. Select the correct type from the list, and click **OK**.

Select webgateway from the Available Event Source Types dialog.

The newly added event source type is displayed in the Event Categories panel.

Note: The image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

RSA RES	POND	INVESTI	GATE M	DNITOR C	ONFIGURE	ADMIN		ō 🗘 🗕	admin 🎯 🤅	
Hosts	Servic	es Event	t Sources	Endpoint S	ources He	alth & Wellne	ess Syste	m Security		
📥 Change S	ervice		ANCE20485 - L	og Collector	Config 🛞					
General	Remote	e Collectors	Files	Event Sources	Sources Event Destinations Settings			Appliance Service Configuration		
File		✓ Config		~			E Ev	ent Source Config	uration Guides	
Event Categories		Sources								
+ -			+ - 🗷	Limport Source	e 🖄 Export Sour					
Name		File Directory		Address	Event Filter	File Spec	File Encoding	Enabled		
☑ apache			apache_logs		127.0.0.1	127.0.0.1		UTF-8	true	
	270 4	of 1							ltoms 4 . 4 of	

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

The Add Source dialog is displayed.

Note: Again, the image below uses **Apache** as an example only. Your screen will look different, depending on which Event Source type you are configuring.

Add Source				
Basic				^ ^
File Directory *	homeapache			
Address	127.0.0.1			
File Spec	^.*s			
File Encoding	UTF-8			
Enabled				
Advanced				
Ignore Encoding Conversion Errors	V			
File Disk Quota	10		٥	
Sequential Processing				
Save On Error				
Save On Success				
Eventsource SSH Key				
Debug	Off		~	1
Manage/Error Files				
Error Files Size		Megabyte	\sim	U.
Error Files Count		\diamond		
Error Files Reduction		\$		
Manage Saved Files				
OK Saved Files Size		Megabyte	\sim	
Saved Files Count		\diamond		
Saved Files Reduction		Ô		
el	Add Source Basic File Directory * Address File Spec File Spec File Encoding Enabled © Advanced Ignore Encoding Conversion Errors File Disk Quota Sequential Processing Save On Success Eventsource SSH Key Debug Manage/Error Files Error Files Size Error Files Size Saved Files Size Saved Files Size Saved Files Size Saved Files Size Saved Files Size	Add Source Basic File Directory* homeapache Address File Directory* homeapache Address File Spec A+*\$ File Encoding UTF-8 Enabled Conversion Errors File Disk Quota 10 Sequential Processing Save On Success Eventsource SSH Key Debug Off ManageError Files Error Files Count Saved Files Count Saved Files Count Eventsource Saved Files Count Eventsource Saved Files Count Eventsource Saved Files Count EventSaved Count	Add Source Basic File Directory* homeapache Address 127.0.0.1 File Spec A.*5 File Encoding UTF-8 Enabled Conversion Errors File Disk Quota 10 Sequential Processing Save On Error Save On Success Eventsource SSH Key Debug Off ManageError Files Error Files SIXE Error Files SIXE Error Files SIXE Error Files SIXE Error Files Count Error Files SIXE Saved Files Count Error Files Count Error Files SIXE Saved Files Count Error Files Count Saved Files Count Error Files Count Error Files Count Saved Files Count Examples Count Ex	Add Source

- 7. Add a File Directory name, modify any other parameters that require changes, and click **OK**.
- 8. Stop and Restart File Collection. After you add a new event source that uses file collection, you must stop and restart the NetWitness File Collection service. This is necessary to add the key to the new event source.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.