Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for McAfee Web Gateway File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for McAfee Web Gateway File

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode. Updated device custom string mappings in access mappings tables.
05/16/2016	Removed "legacy" and reference to vendor's Common Event Format version.
02/15/2016	Updated link to Customer Alliance site. Marked this connector as legacy; for future version support, use the vendor’s Common Event Format version.
05/15/2015	Added information regarding version support with CEF Certified connector.
06/30/2014	Added support for 'AccessDenied' and 'FoundVirus' log types for v7.4.
05/15/2014	Added support for 7.4.
05/15/2013	Added configuration information for 7.2.
12/21/2012	Added support for 7.2 and updated event mappings.

Contents

SmartConnector for McAfee Web Gateway File

This guide provides information for installing the SmartConnector for McAfee Web Gateway File and configuring the device for event collection. McAfee Web Gateway version 6.8, 7.2, and 7.4 are supported.

Product Overview

The McAfee Secure Web Gateway is a Web security appliance solution that delivers comprehensive protection against web-born threats. Its McAfee filtering technologies block spyware, inappropriate Web content, phishing, known viruses, worms, and Trojans. McAfee Secure Web Gateway lets your business take advantage of Web 2.0 capabilities while remaining in control of enterprise security.

Configuration

Activities and events occurring in Web and email communication can be logged by McAfee Secure Web Gateway into various log files, such as the HTTP Access Log and the Security Log, for which event collection is supported by this connector.

Each of these logs contains a particular set of log file fields, which also can be customized. To customize the logs file field:

- For version 6.8, go to **Reporting -> Overall Reporting -> Log File Management -> Activate Log File tab.**
- For versions 7.2 and 7.4, go to **Policy -> Settings -> File System Logging.**

For complete information about Web Gateway log files, see the McAfee Web Gateway online help.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

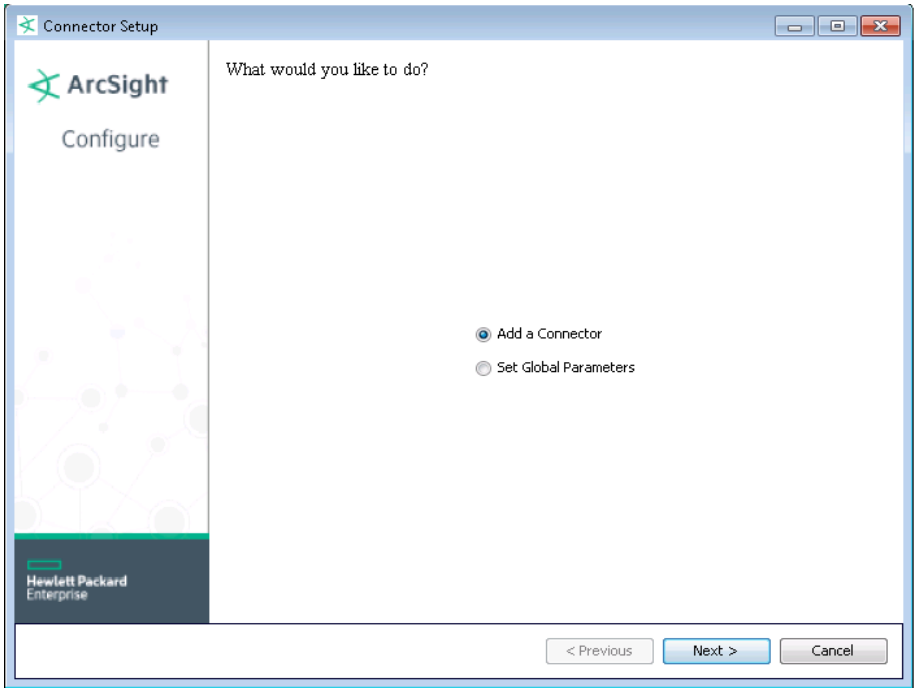
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the HPE SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting ‘Enabled’ to encrypt the fields identified in ‘Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

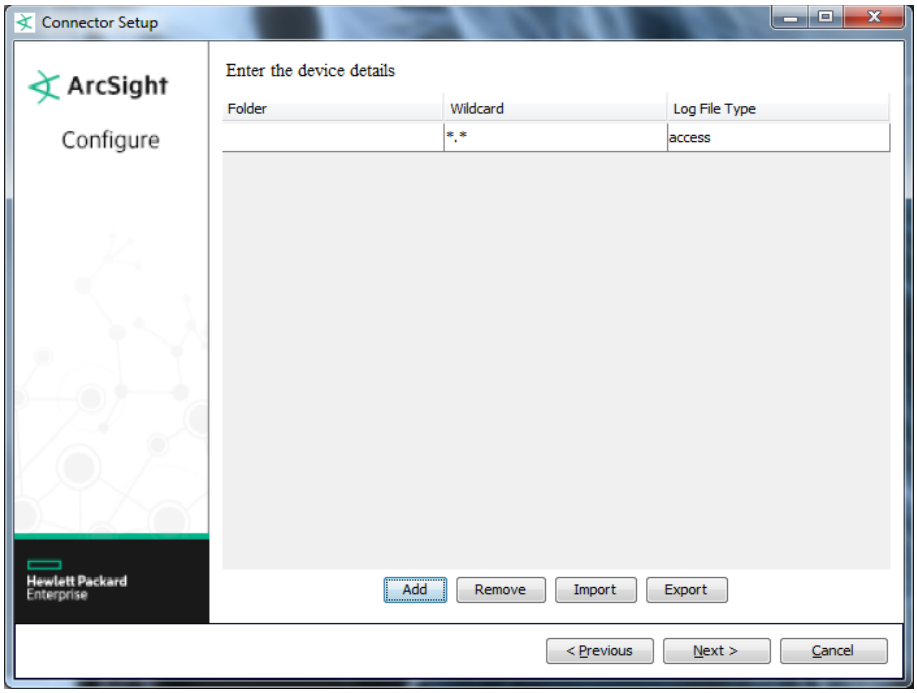
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **McAfee Web Gateway File** and click **Next**.

3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Folder where the log files are stored.
Wildcard	Wildcard that identifies the files to process. For example, if the access log file is 'access1003021405.log', use wild card 'access*.log'; if the security log file is 'security1003031515.log.gz', use wild card 'security*.log.gz'.
Log File Type	Select 'access,' 'security,' 'foundviruses,' or 'access_denied' for the type of log file.

Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Customize Text Qualifier (Optional)

This section is required only if your log files use " (double quotation mark) as the text qualifier and the " character also appears in in the logs .

The names of event fields for McAfee Web Gateway are defined in the first line of the log file as follows:

```
#src_ip_anonymous - auth_user_anonymous time_stamp "req_line" status_code
bytes_to_client "referer" "user_agent"
```

Note that some fields have the text qualifier " (double quotation) because the field in the real log may contain spaces:

```
0.0.0.2 - - [13/Feb/2010:00:21:43 +0000] "POST
http://www.arcsight.com/safebrowsing/downloads?client=navclient-auto-
ffox%26appver=3.6%26pver=2.2%26wrkey=AKEgNisVaDwd7BzRvEhUGBeT2YfCiZqZfWL5
F WIfoAapSEZfBmVn93phhNtJlrVW6onboaqQHo1KITyQaMoLssAg4H5rZl0NBg==
HTTP/1.1" 200 745 "" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US;
rv:1.9.2) Gecko/20100115 Firefox/3.6 (.NET CLR 3.5.30729)"
```

In the Access log event above, the last field is `"Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.2) Gecko/20100115 Firefox/3.6 (.NET CLR 3.5.30729)"` with several spaces inside. With the text qualifier, the ArcSight SmartConnector treats it as one field.

However, fields containing one or more double quotation marks (") in customer logs causes parsing problems. To solve the problem, you can change the default text qualifier " to another qualifier, such as $"$ (or other special characters that never appear in the logs).

The SmartConnector for McAfee Web Gateway File supports collection of events from both access and security logs. If the fields of the access log contain " rather than \", you should change the text qualifier. This applies to both access and security logs.

You will make a change in two places: the SmartConnector parser file and through the McAfee Web Gateway Device.

SmartConnector

1 After completing connector installation, go to `$ARCSIGHT_HOME/current/user/agent/fcp` and create the following subdirectory:

```
mcafee_webgateway_file
```

2 In the `mcafee_webgateway_file` subfolder, create the following files:

```
mcafee_webgateway_file_access.sdkfilereader.properties
mcafee_webgateway_file_security.sdkfilereader.properties
```

3 Add the following line to each file, then save and close the files.

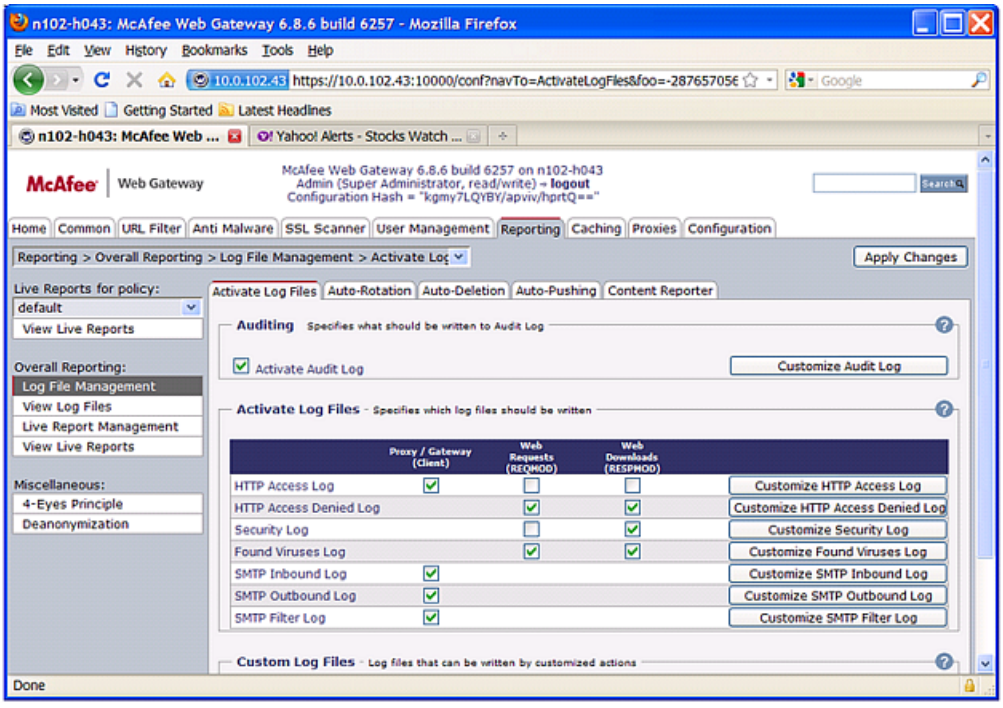
```
text.qualifier=$"$
```

McAfee Web Gateway, v6.8

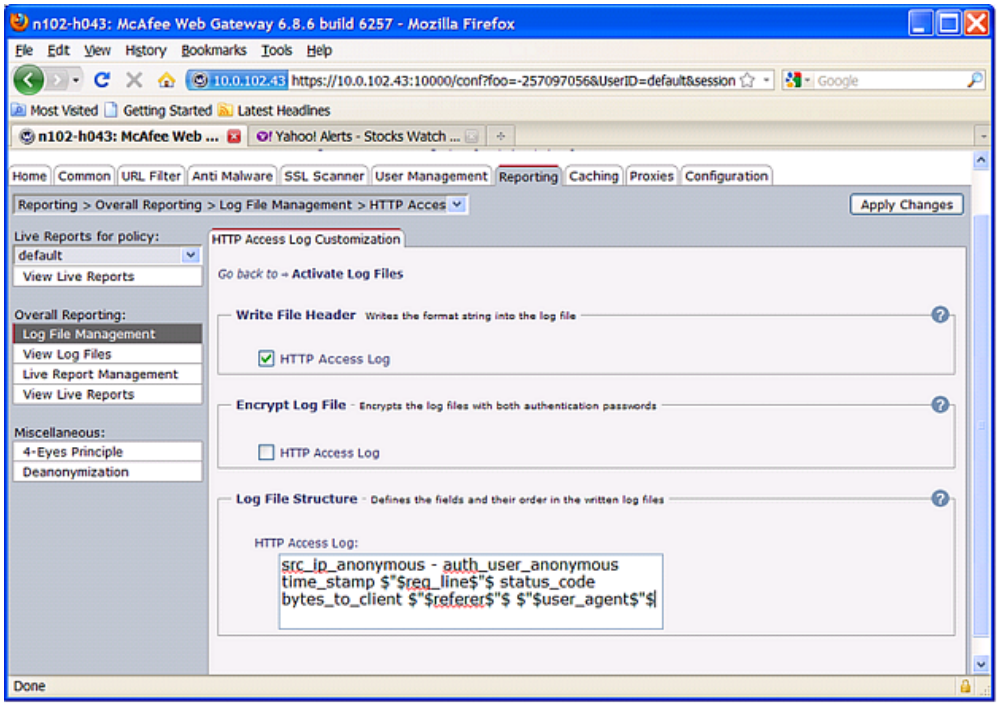
1 Log in to the Web Gateway device.

2 Select the **Reporting** tab, then select **Log File Management**.

3 To make this change to the access log, click **Customize HTTP Access Log**.



4 Make the changes as shown in the following figure.



5 Click **Apply Changes** to save the change. The default text qualifier " changes to $"$.

6 Check new access logs and make sure $"$ is the new text qualifier in the first line and other lines.

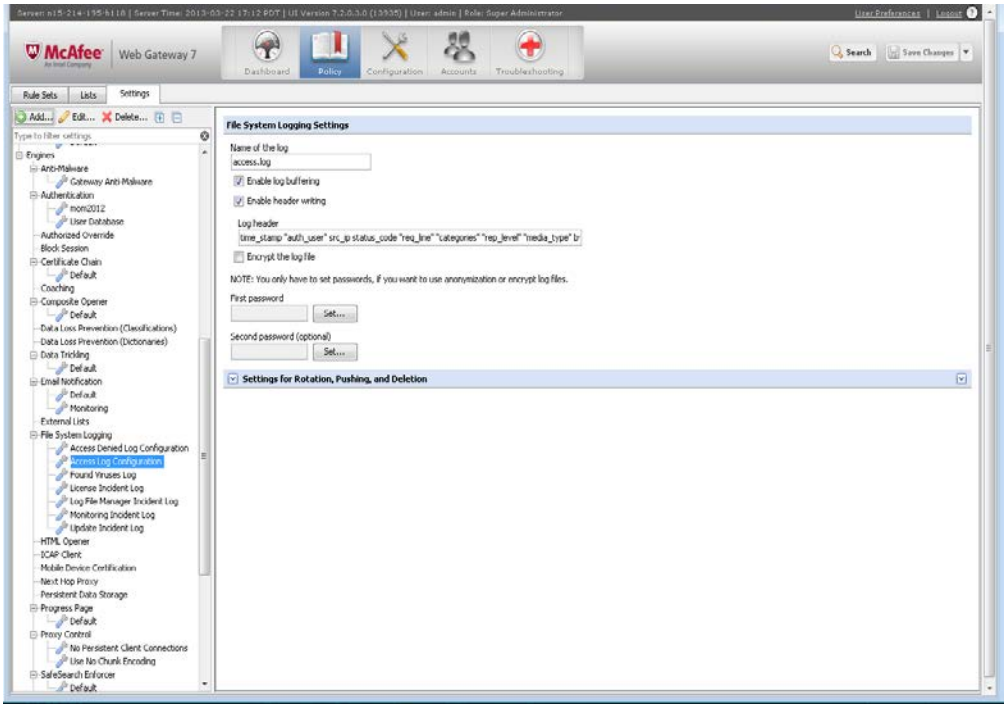
7 Repeat this procedure from step 3, substituting the **Customize HTTP Security Log** for the access log.

McAfee Web Gateway, v7.2/v7.4

1 Log into the Web Gateway device.

2 Go to **Policy -> Settings -> File System Logging.**.

3 To change the access log, click **Access Log Configuration**.



4 Check the **Enable Header Writing** check box.

5 Make the following changes in the Log Header field:

- Change "req_line" to $"$req_line$"$
- Change "user_agent" to $"$user_agent$"$
- Add $"$referer$"$

6 Click **Save Changes**. The default text qualifier " changes to $"$.

7 Check new access logs and make sure $"$ is the new text qualifier in the first line and other lines.

8 Repeat this procedure from step 3 to customize other logs.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

McAfee Web Gateway HTTP Access Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
additionaldata.Application_name	application_name
additionaldata.Rep_level	rep_level
additionaldata.X_Attribute_header	attribute
Agent (Connector) Severity	0, 400 - 599 = High; 300 - 399 = Medium; 100 - 299 = Low
Bytes In	bytes_from_client
Bytes Out	bytes_to_client
Destination Address	server_ip
Device Custom Number 1	Block Reason ID
Device Custom String 1	virus_name
Device Custom String 2	elapsed_time
Device Custom String 4	Reason
Device Custom String 5	block reason
Device Custom String 6	categories
Device Event Category	'Access Log'
Device Event Class ID	status_code
Device Product	'Web Gateway'
Device Receipt Time	time_stamp (dd/MMM/yyyy:HH:mm:ss z)
Device Severity	status_code
Device Vendor	'McAfee'
File Type	media_type
Message	req_line
Name	Name
Request Client Application	user_agent
Request Context	referer
Request Method	request method (such as Post, Get, Head)
Request URL	the URL that was requested
Source Address	One of (src_ip, src_ip_anonymous)
Source User Name	One of (auth_user, auth_user_anonymous)

McAfee Web Gateway HTTP Access Denied Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
additionaldata.App_rep_level	app_rep_level
additionaldata.Application_name	application_name
additionaldata.Rep_level	rep_level

ArcSight ESM Field	Device-Specific Field
additionaldata.Tba_3	tba_3
Bytes In	bytes_from_client
Bytes Out	bytes_to_client
Destination Address	dst_ip
Device Custom Number 1	Block Reason ID
Device Custom Number 2	Reputation
Device Custom String 1	Virus Name
Device Custom String 2	Antimalware Infected
Device Custom String 3	HTTP Version
Device Custom String 5	Block Reason
Device Custom String 6	Categories
Device Event Category	'Access Denied Log'
Device Event Class ID	status_code
Device Product	'Web Gateway'
Device Receipt Time	time_stamp (dd/MMM/yyyy:HH:mm:ss z)
Device Vendor	'McAfee'
File Type	media_type
Message	req_line
Reason	status_code
Request Client Application	user_agent
Source Address	src_ip
Source Host Name	system_hostname
Source User Name	auth_user

McAfee Web Gateway Virus Found Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Virus Name
Device Event Category	'Found Viruses Log'
Device Event Class ID	Malware Found
Device Product	'Web Gateway'
Device Receipt Time	time_stamp (dd/MMM/yyyy:HH:mm:ss z)
Device Vendor	'McAfee'
Message	virus_name
Name	Malware Found
Request URL	url
Source Address	src_ip
Source User Name	auth_user

McAfee Web Gateway Security Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	0, 400 - 599 = High; 300 - 399 = Medium; 100 - 299 = Low
Application Protocol	The request protocol

ArcSight ESM Field	Device-Specific Field
Device Action	media_type_status
Device Custom String 2	FileExt
Device Custom String 3	HTTP Version
Device Custom String 4	Reason
Device Event Category	'Security Log'
Device Event Class ID	status_code
Device Product	'Web Gateway'
Device Receipt Time	time_stamp (dd/MMM/yyyy:HH:mm:ss z)
Device Severity	status_code
Device Vendor	'McAfee'
File Type	media_type
Message	object_id
Name	Name
Request Method	The HTTP method that was requested
Request URL	The URL that was requested
Source User Name	auth_user