Micro Focus Security ArcSight Connectors

SmartConnector for McAfee Network Security Manager DB (Time-based)

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for McAfee Network Security Manager DB (Time-based)

June, 2018

Copyright © 2004 – 2017; 2018 Micro Focus and its affiliates and licensors.

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
12/19/2017	Added support for version 9.1.
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Added support for version 8.3. Updated configuration parameters and added global parameters. Removed support for versions 7.0 and 7.1.
06/30/2016	Updated MySQL JDBC driver information.
05/16/2016	Updated link for MySQL JDBC driver.
11/17/2015	Updated Device Product field mapping. Support ended for Network Security Manager versions 5.1, 6.0, and 6.1 due to end-of-life of product versions by vendor.
08/14/2015	Renamed this connector from McAfee Network Security Manager DB to McAfee Network Security Manager DB (Time-based).
06/30/2015	Added support for version 8.2.
09/30/2014	Added support for version 8.1.
05/15/2014	Added new mappings for Confidence, Signature Name and Signature ID for v7.5 and v8.0.
03/31/2014	Added support for version 8.0.

SmartConnector for McAfee Network Security Manager DB (Time-based)

This guide provides information for installing the SmartConnector for McAfee Network Security Manager DB (formerly McAfee IntruShield DB) and configuring the device for event collection. McAfee Network Security Manager versions 7.5, 8.0, 8.1, 8.2, 8.3, and 9.1 are supported.

This connector uses timestamp as the key field in the SQL query for events. Using timestamp as the key field resulted in a possible loss of events. HP recommends that you migrate to the SmartConnector for McAfee Network Security Manager DB (ID-based).

Product Overview

McAfee Network Security Manager is a network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Configuration

Because MySQL supports host-based access control, you may find it necessary to configure MySQL to allow connections from the host where the SmartConnector for McAfee Network Security Manager DB is running. Execute a command such as the following in a MySQL prompt to allow MySQL access:

```
GRANT SELECT ON NetworkSecurityMangerdb.* to
MySQLuser@'agenthost' identified by 'MySQLpassword';
```

Where the parameters are defined as follows:

Parameter	Description
NetworkSecurityManagerdb	The name of the database used by Network Security Manager (typically 'lf').
MySQLuser	The user that you created for the ArcSight SmartConnector to access the MySQL database.
AgentHost	The host name (or IP address) of the host running the ArcSight SmartConnector (for testing purposes, you could use %, which means 'any host').
MySQLPassword	The password of the user you created for the ArcSight SmartConnector.

Install the SmartConnector

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

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

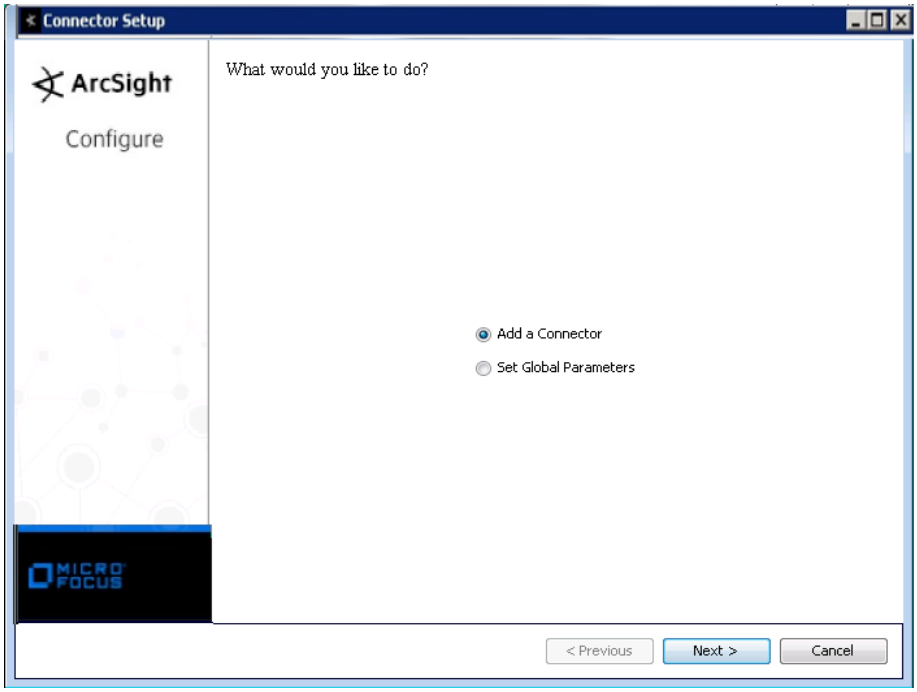
Install Core Software

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 Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus 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:



Download MySQL JDBC Driver

1. Click **Cancel** to leave the configuration wizard at this point.
2. The following steps are required when you use the MySQL JDBC driver, required for Connector Appliance/ArcSight Management Center and Linux systems.

   A. For connector versions 7.2.4 and later, download the latest MySQL JDBC Driver from:

   http://dev.mysql.com/downloads/connector/j

   For connector versions 7.2.3 and earlier, download the MySQL 5.0.8 JDBC Driver from:

   https://dev.mysql.com/downloads/connector/j/5.0.html

   Install the driver.

   B. For software connectors, copy the appropriate jar file to `$ARCSIGHT_HOME\current\user\agent\lib`, where `$ARCSIGHT_HOME` refers to the connector install folder, such as `c:\ArcSight\SmartConnectors`. For Connector Appliance/ArcSight Management Center users, see "Add a JDBC Driver to the Connector Appliance/ArcSight Management Center" later in this guide.

   C. From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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.

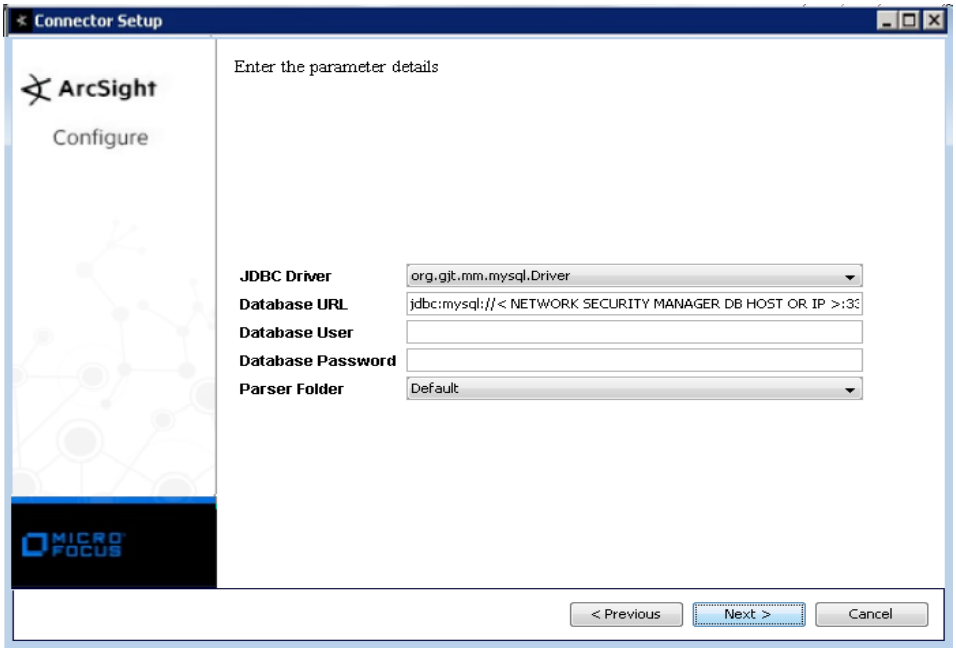
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 Network Security Manager DB (Time-based)** and click **Next**.

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



Parameter	Description
JDBC/ODBC Driver	Accept the default org.gjt.mm.mysql.Driver
Database URL	Enter the database URL or accept the default jdbc:mysql://<NETWORK SECURITY MANAGER DB HOST or IP>:3306/lf, replacing <NETWORK SECURITY MANAGER DB HOST or IP> with the database host's name or IP address.
Database User	Login name assigned to access the database
Database Password	Password assigned to access the database
Parser Folder	You can specify whether to enable optional 'payload sampling' or 'typespecificdata' or both. When 'payload sampling' is selected during the installation process, retrieved payload is stored as part of the events. When 'type-specific-data' is selected during the installation process, the IP addresses involved in Host Sweep types of alerts are mapped to Device Custom String 6; Device Custom String 1 contains a count of the number of IP addresses involved in the alert.

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*.

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.

Payload Support

Payload refers to the information carried in the body of an event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload may also be forensically significant.

You can retrieve, preserve, view, or discard payloads for the McAfee Network Security Manager DB SmartConnector using the ArcSight Console. Because event payloads are relatively large, ArcSight does not store them by default. Instead, you can request payloads from devices for selected events through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console.

Payloads are downloaded and stored only on demand; you must configure Network Security Manager to log these packets. By default, 256 bytes of payload will be retrieved.

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

Locate Payload-Bearing Events

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view. In an ArcSight Console Viewer panel grid view, right-click a column header and choose **Add Column < Device > Payload ID**. Look for events showing a Payload ID in that column.

Retrieve Payloads

In a Viewer panel grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab, then click **Retrieve Payload**.

Preserve Payloads

In a grid view, right-click an event with an associated payload, select **Payload**, then **Preserve**. Alternatively, in the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discard Payloads

In a grid view, right-click an event with an associated payload and select **Payload**, then **Discard Preserved**. You also can use the Event Inspector: In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Discard Preserved Payload**.

Save Payloads to Files

In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Save Payload**. In the **Save** dialog box, navigate to a directory and enter a name in the **File name** text field. Click **Save**.

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.

NSM 9.x Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity); Medium = Medium (Device Severity); Low = Low (Device Severity)
Application Protocol	PROTOCOL_ID
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom Number 3	EXECUTABLE_CONFIDENCE
Device Custom String 1	PACKET_LOG_TYPE
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME

ArcSight ESM Field	Device-Specific Field
Device Severity	One of (ATTACK_SEVERITY, low)
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	SOURCE_USER_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 9.x Payload Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity), Medium = Medium (Device Severity), Low = Low (Device Severity)
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom Number 1	PACKETLOGID
Device Custom Number 3	EXECUTABLE_CONFIDENCE
Device Custom String 1	PACKETLOGTYPE (PACKET_LOG_TYPE)
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	One of (ATTACK_SEVERITY, Low)
Device Vendor	'McAfee'

ArcSight ESM Field	Device-Specific Field
Event Outcome	resultSetValue (100=Success, 300=Failure)
External Id	ALERT_ID
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	SOURCE_USER_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 9.x Payload Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTNATION_DNS_ID
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	PACKETLOGID ('PACKETLOGID')
Device Custom Number 2	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
External ID	ALERT_ID
Source DNS Domain	SOURCE_DNS_DOMAIN
Source User Id	SOURCE_USER_ID

NSM 9.x Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
Source DNS Domain	SOURCE_DNS_DOMAIN
Source User Id	SOURCE_USER_ID

NSM 8.x Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity); Medium = Medium (Device Severity); Low = Low (Device Severity)
Application Protocol	PROTOCOL_ID
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom Number 3	EXECUTABLE_CONFIDENCE
Device Custom String 1	PACKET_LOG_TYPE
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	One of (ATTACK_SEVERITY, low)
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	SOURCE_USER_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 8.x Payload Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity), Medium = Medium (Device Severity), Low = Low (Device Severity)
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom Number 1	PACKETLOGID
Device Custom Number 3	EXECUTABLE_CONFIDENCE
Device Custom String 1	PACKETLOGTYPE (PACKET_LOG_TYPE)
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	One of (ATTACK_SEVERITY, Low)
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
External Id	ALERT_ID
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	SOURCE_USER_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 8.x Payload Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTNATION_DNS_ID
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	PACKETLOGID ('PACKETLOGID')
Device Custom Number 2	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
External ID	ALERT_ID
Source DNS Domain	SOURCE_DNS_DOMAIN
Source User Id	SOURCE_USER_ID

NSM 8.x Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTNATION_DNS_ID
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
Source DNS Domain	SOURCE_DNS_DOMAIN
Source User Id	SOURCE_USER_ID

NSM 7.5 Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity); Medium = Medium (Device Severity); Low = Low (Device Severity)
Application Protocol	PROTOCOL_ID
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	Destination_User_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom String 1	PACKET_LOG_TYPE

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	One of (ATTACK_SEVERITY, low)
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	Source_User_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 7.5 Payload Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High (Device Severity), Medium = Medium (Device Severity), Low = Low (Device Severity)
Base Event Count	ATTACK_COUNT
Destination Address	TARGET_IP
Destination DNS Domain	DESTINATION_DNS_DOMAIN
Destination Port	TARGET_PORT
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Address	SENSOR_IP
Device Custom IPv6 Address 1	SENSOR_IP (Device IPv6 Address)
Device Custom IPv6 Address 2	SOURCE_IP (Source IPv6 Address)
Device Custom IPv6 Address 3	TARGET_IP (Destination IPv6 Address)
Device Custom Number 1	PACKETLOGID
Device Custom String 1	PACKETLOGTYPE (PACKET_LOG_TYPE)
Device Custom String 2	ALERT_ID
Device Custom String 3	resultSetValue ('ACTION_CODE')
Device Custom String 4	IV_ADMIN_DOMAIN
Device Custom String 5	port_name ('MONITORING_PORT')
Device Direction	DIRECTION

ArcSight ESM Field	Device-Specific Field
Device Event Category	CATEGORY
Device Event Class ID	ATTACKIDREF
Device Host Name	SENSOR_NAME
Device Inbound Interface	INTERFACE
Device Product	'Network Security Manager'
Device Receipt Time	ATTACK_TIME
Device Severity	One of (ATTACK_SEVERITY, low)
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
External Id	ALERT_ID
Name	one of (ATTACK_NAME, Severe network attack)
Source Address	SOURCE_IP
Source DNS Domain	SOURCE_DNS_DOMAIN
Source Port	SOURCE_PORT
Source User Id	SOURCE_USER_ID
Transport Protocol	NETWORK_PROTOCOL_ID

NSM 7.5 Payload Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTNATION_DNS_ID
Destination User Id	DESTINATION_USER_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	PACKETLOGID ('PACKETLOGID')
Device Custom Number 2	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
External ID	ALERT_ID
Source DNS Domain	SOURCE_DNS_DOMAIN
Source User Id	SOURCE_USER_ID

NSM 7.5 Type Specific Data Mappings

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DESTNATION_DNS_ID
Destination User Id	Destination_User_ID
Device Action	resultSetValue (200=Unknown, 400=Suspicious, 999=Blocked, 888=Set to block)
Device Custom Number 1	IP_COUNT_KEY ('IP_COUNT')
Device Custom String 6	TYPE_SPECIFIC_DATA_KEY ('TYPE_SPECIFIC_DATA')
Event Outcome	resultSetValue (100=Success, 300=Failure)
Source DNS Domain	SOURCE_DNS_DOMAIN

ArcSight ESM Field	Device-Specific Field
Source User Id	SOURCE_USER_ID

Troubleshooting

Why does the ArcSight SmartConnector experience a loss of events?

The SmartConnector for McAfee Network Security Manager DB experiences a loss of events because it only compatible with time-based events. Try installing the SmartConnector for McAfee Network Security Manager DB (ID-based). It supports version NSM 7.5 and ID-based events.

"When I use the latest MySQL JDBC driver, the connector does not receive events."

Connector versions 7.2.4 and later use the latest MySQL JDBC driver. For connector versions 7.2.3 and earlier, you will need the MySQL 5.0.8 JDBC Driver, which you can download from:

https://dev.mysql.com/downloads/connector/j/5.0.html