Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

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

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for McAfee Network Security Manager DB (Time-based)

This guide provides information to install the SmartConnector for McAfee Network Security Manager DB (formerly McAfee IntruShield DB) and to configure the device for event collection.

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

This guide provides a high level overview of ArcSight SmartConnectors.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

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 might 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';
```

The following table describes the parameters:

Parameter	Description
NetworkSecurityManagerdb	The name of the database used by Network Security Manager (typically 'lf').
MySQLuser	The ArcSight user created 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 indicates any host).
MySQLPassword	The password for the database user.

Downloading the JDBC Driver

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.

Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar to mssql-jdbc-9.4.0.jre8.jar.
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)

- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

For more information and to download the MS SQL Server JDBC Driver, see aa937724

Installing the SmartConnector

The following sections provide instructions to install and configure the SmartConnector.

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy the jar file associated with the version of the driver that you downloaded earlier to `$ARCSIGHT_HOME/current/user/agent/lib`
5. (Optional) To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin directory`.

   An example of The JDBC driver download path for SQL JDBC driver is:

   - For version 4.0 for 32-bit environment is `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll`
   - For 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`

Note: If you are upgrading the SmartConnector, you must copy the authentication file to $ARCSIGHT_ HOME\jre\bin again after update, as the upgrade process overwrites the $ARCSIGHT_HOME\jre\bin directory.

6. To add JDBC Driver to ArcMC or Connector Applicance, see Adding JDBC Driver to the Connector Appliance/ArcSight Management Center.
7. Browse to `ARCSIGHT_HOME/current/bin` and double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.
9. Select **McAfee Network Security Manager DB (Time-based)** from the Type drop-down list, then click **Next**.
10. Specify the followin 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`. Replace <NETWORK SECURITY MANAGER DB HOST or IP> with the database host's name or IP address. You can replace 'lf', with the real database name in your environment.
Database User	Enter the name of the database user.
Database Password	Enter the Password for the database user.
Parser Folder	Optionally, you can specify one of the following parameters: **Payload Sampling:** When Payload Sampling is selected during the installation process, retrieved payload is stored as part of the events. **Type Specific Data:** 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. **Type Specific Data and Payload Sampling:** This option enables both payload sampling and Type Specific Data. **Default:** This option disables both payload sampling and Type Specific Data options.

11. Select a destination and configure parameters.
12. Specify a name for the connector.
13. 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.

14. Select whether you want to run the connector as a service or in the standalone mode.
15. Complete the installation.
16. Run the SmartConnector.

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

Adding JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the required containers, as follows:

1. From the Connector Appliance/ArcSight Management Center, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the `.jar` file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (for example, `JDBCdriver`). Click **Next**.
10. Click **Done** to complete the process. The newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
12. Select one or more containers into which you want to upload the driver, then click **Next**.
13. Click **Done** to complete the process.

14. Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.

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	sensorAlertUUID(SENSOR_ALERT_UUID)
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

ArcSight ESM Field	Device-Specific Field
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, NULL Attack Name in product DB)
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

ArcSight ESM Field	Device-Specific Field
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	sensorAlertUUID
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, NULL Attack Name in product DB)
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)

ArcSight ESM Field	Device-Specific Field
Device Vendor	'McAfee'
Event Outcome	resultSetValue (100=Success, 300=Failure)
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, NULL Attack Name in product DB)
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)

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)
External Id	ALERT_ID
File Hash	FILEHASH
File Name	FILENAME
Name	one of (ATTACK_NAME, NULL Attack Name in product DB)
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

ArcSight ESM Field	Device-Specific Field
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

ArcSight ESM Field	Device-Specific Field
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
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
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
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)

ArcSight ESM Field	Device-Specific Field
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

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.

The connector displays the following error "com.mysql.jdbc.exceptions.jdbc4.MySQLNonTransientConnectionException: No operations allowed after connection closed.

Make sure your JDBC driver is up to date with the latest version, compatible with the version of the database as recommended by MySQL. MySQL database administrator should go to the my.cnf file and increase the wait_timeout parameter. By default, MySQL sets this value to "28800" seconds. If this value is modified, revert the changes to default value to restore connectivity with the Database server.

"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

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for McAfee Network Security Manager DB (Time-based) SmartConnector (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!