

McAfee Enterprise Security Manager Data Source Configuration Guide

Data Source: Malwarebytes Breach Remediation

April 2017

Table of Contents

- 1 Introduction 3
- 2 Prerequisites 3
- 3 Specific Data Source Configuration Details 4
 - 3.1 Malwarebytes Breach Remediation Configuration..... 4
 - 3.2 McAfee Event Receiver Configuration 4
- 4 Data Source Event to McAfee Field Mappings..... 5
 - 4.1 Log Format 5
 - 4.2 Log Sample..... 5
 - 4.3 Mappings..... 5
- 5 Appendix A – Generic Syslog Configuration Details..... 6
- 6 Appendix B – Troubleshooting..... 8

1 Introduction

This guide details how to configure Malwarebytes Breach Remediation to send syslog data in the proper format to the McAfee Event Receiver.

2 Prerequisites

McAfee Enterprise Security Manager Version 10.x and above.

In order to configure the Malwarebytes Breach Remediation syslog service, appropriate administrative level access is required to perform the necessary changes documented below.

3 Specific Data Source Configuration Details

3.1 Malwarebytes Breach Remediation Configuration

Please refer to your product documentation for instructions on sending syslog logs to a remote server. Use the McAfee Event Receiver IP address for the address of the remote server.

3.2 McAfee Event Receiver Configuration

After successfully logging into the McAfee ESM console, the data source will need to be added to a McAfee Event Receiver in the ESM hierarchy.

1. Select the desired McAfee Event Receiver.
2. Click the **Properties** icon.
3. From the Receiver Properties listing, select **Data Sources**.
4. Click **Add**.
OR
1. Select the desired McAfee Event Receiver.
2. Click the **Add Data Source** icon.

Data Source Screen Settings

1. Data Source Vendor – Malwarebytes
2. Data Source Model – Breach Remediation
3. Data Format – Default
4. Data Retrieval – SYSLOG (Default)
5. Enabled: Parsing/Logging/SNMP Trap – Parsing
6. Name – Name of data source
7. IP Address/Hostname – The IP address and host name associated with the data source device.
8. Syslog Relay – None
9. Mask – 32
10. Require Syslog TLS – Enable to require the Receiver to communicate over TLS.
11. Support Generic Syslogs – Do nothing
12. Time Zone – Time zone of data being sent.

Note – Refer to Appendix A for details on the Data Source Screen options

4 Data Source Event to McAfee Field Mappings

4.1 Log Format

The expected format for this device is as follows:

```
CEF:0|PRODUCT_VENDOR|PRODUCT_NAME|PRODUCT_VERSION|SIGNATURE
ID|NAME|SEVERITY|KEY=VALUE KEY=VALUE...
```

4.2 Log Sample

This is a sample log from a Malwarebytes Breach Remediation device:

```
CEF:0|Malwarebytes|Malwarebytes Malware
Remediation|1.0|1000|ScanStarted|1|act=Action cat=MalwareCategory
cs1=MalwareName cs1Label=MalwareName cs2=MalwareHash cs2Label=MalwareHash
cs3=SessionId cs3Label=SessionId cs4=MalwareClass cs4Label=MalwareClass
```

4.3 Mappings

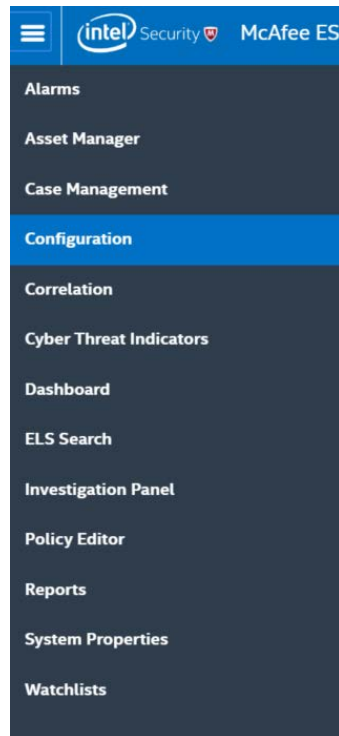
The table below shows the mappings between the data source and McAfee ESM fields.

Log Fields	McAfee ESM Fields
CEF.EventName + CEF:Signature.ID	Msg
CEF:Severity	Severity
Act	Action
Cat	Threat_Category
MalwareName	Threat_Name
MalwareHash	Hash
SessionId	Session
MalwareClass	Event_Class
CommandLine	Command
deviceMacAddress	Source MAC
Dvchost	Host
filePath	File_Path
Msg	Message_Text
Suser	Source User

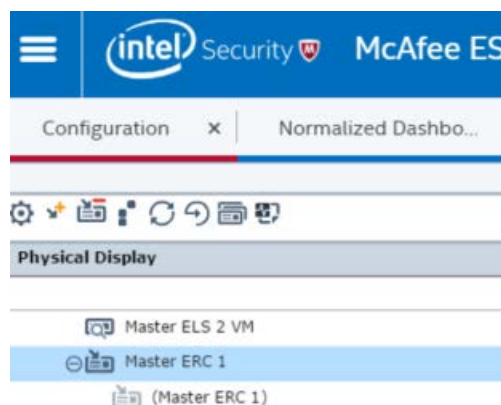
5 Appendix A – Generic Syslog Configuration Details

There are different options available when configuring a new data source. When some options are selected, additional parameters may appear. Most of these parameters are examined in more detail below. This section outlines the general options available in the **Add Data Source** configuration screen.

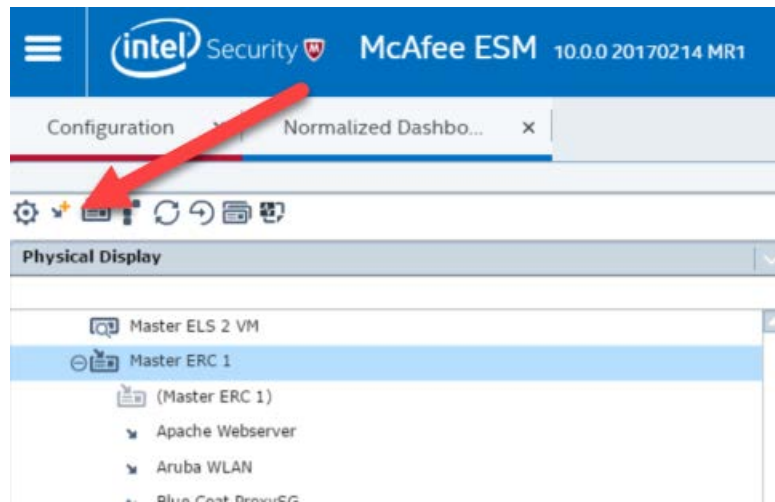
1. Select Configuration under the top left drop-down menu



2. To add a data source, in the system Tree, on the left of the console, expand your Local ESM by clicking the plus sign next to it and Click on your Event Receiver



3. Click the Add Data Source button in the top left corner of the console



Add Data Source configuration window is launched:

Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC ?

Data Source Vendor: A10 Networks

Data Source Model: Load Balancer

Data Format: Default

Data Retrieval: SYSLOG (Default)

Enabled: ☒ Parsing ☐ Logging ☐ SNMP Trap

Name:

IP Address:

Host Name: Look up

Syslog Relay: None

Mask: 0

Require syslog TLS: ☐

Port: 514

Support Generic Syslogs: Do nothing

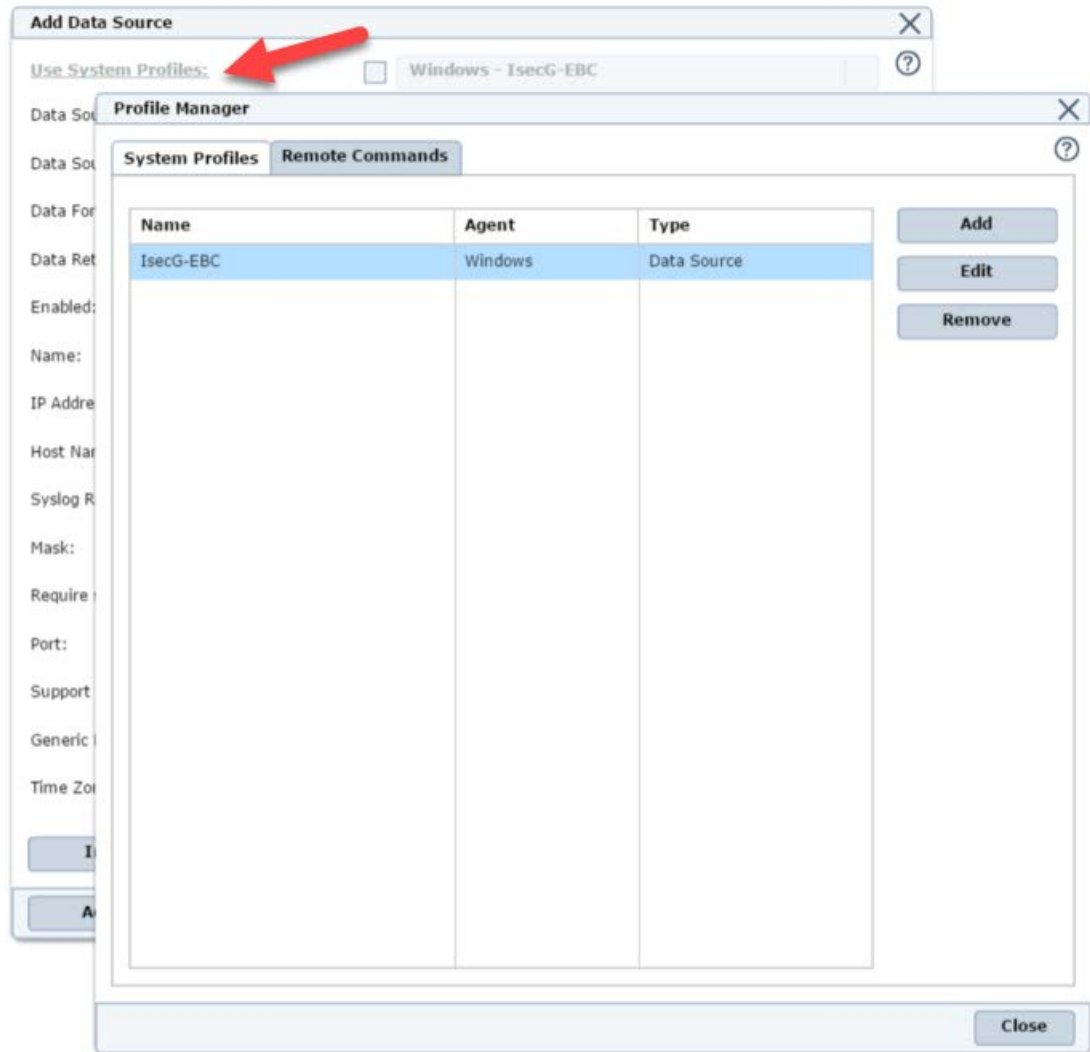
Generic Rule Assignment: User Defined 1

Time Zone: (GMT,00:00) Greenwich Mean Time

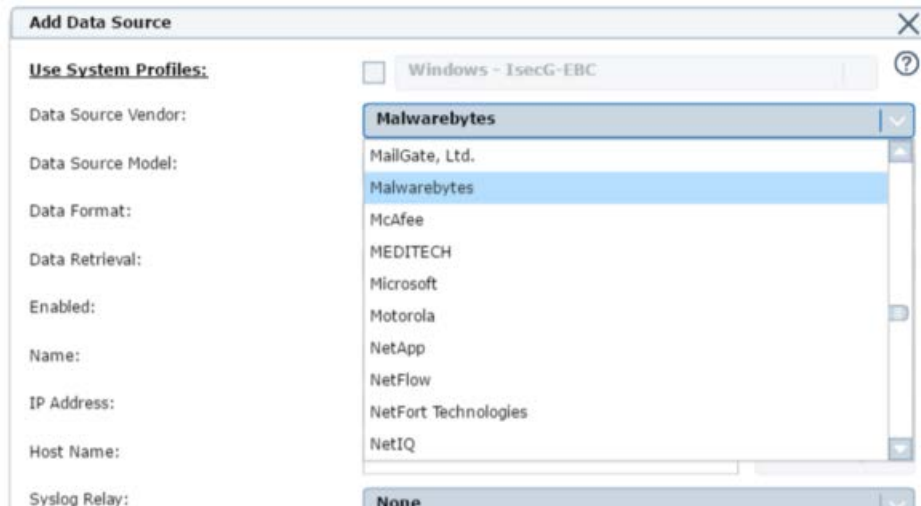
Interface Manage the network interface for the parent Receiver.

Advanced OK Cancel

4. Use System Profiles – System Profiles are a way to use settings that are repetitive in nature, without having to enter the information each time. An example is WMI credentials, which are necessary to retrieve Windows Event Logs if WMI is the chosen mechanism.



5. Data Source Vendor – List of all supported vendors.



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC

Data Source Vendor: **Malwarebytes**

Data Source Model: MailGate, Ltd.
Malwarebytes

Data Format: McAfee

Data Retrieval: MEDITECH

Enabled: Microsoft

Name: Motorola

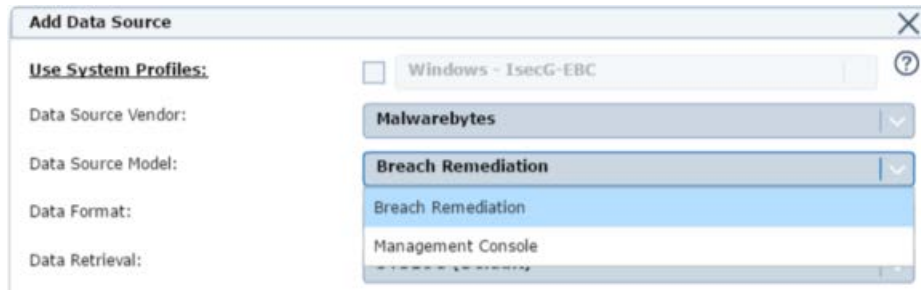
IP Address: NetApp

Host Name: NetFlow

Syslog Relay: NetFort Technologies
NetIQ

Syslog Relay: **None**

6. Data Source Model – List of all supported products for a vendor



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC

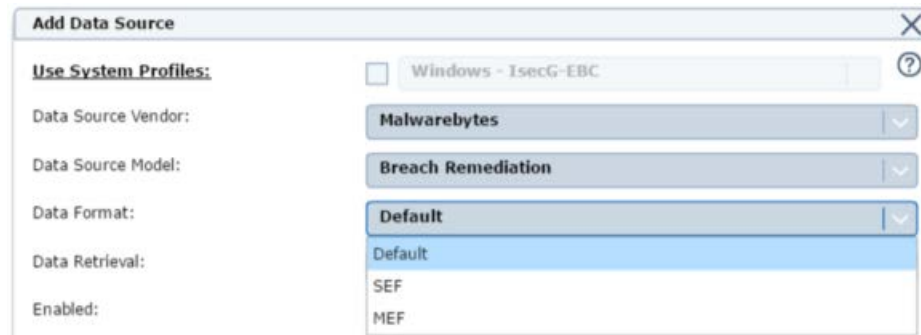
Data Source Vendor: **Malwarebytes**

Data Source Model: **Breach Remediation**

Data Format: Breach Remediation

Data Retrieval: Management Console

7. Data Format – The expected format of the received / collected data. Options are “Default”, “CEF”, and “MEF”. This should generally be left as Default for supported data sources, and is intended to be used for custom data sources.



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC

Data Source Vendor: **Malwarebytes**

Data Source Model: **Breach Remediation**

Data Format: **Default**

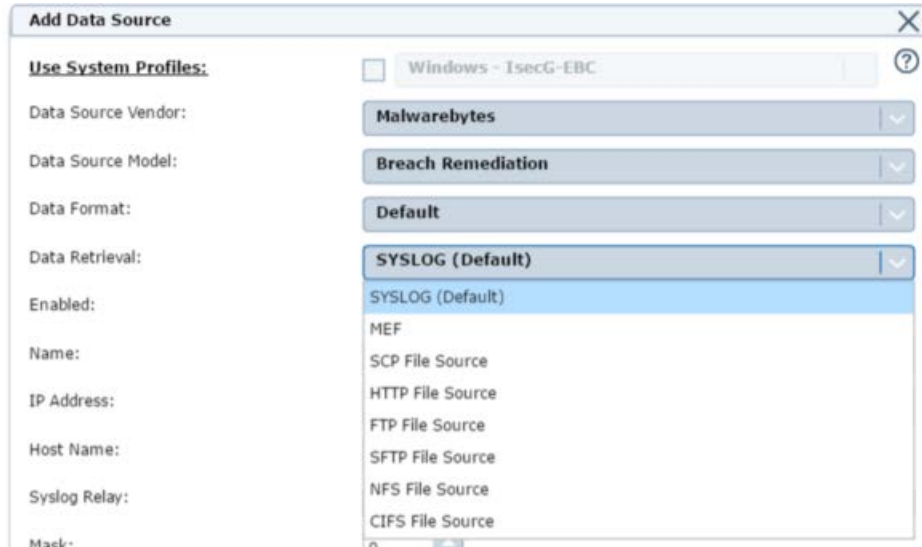
Data Retrieval: Default

Enabled: SEF

MEF

Note – If CEF is selected, the generic CEF parsing rule will be enabled and rolled into policy for that data source. If selected on supported CEF data sources, the generic parsing rule may override existing parsing rules that are designed to parse data source specific details. This will result in degraded reporting for the specific data source.

8. Data Retrieval – The expected collection method used by the Receiver to collect the data. The default is generally syslog. It is expected that this option will be changed to match the needs in a specific user's environment. The data will need to remain in the expected format, otherwise the parsing rules may not parse the events.



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC ?

Data Source Vendor: **Malwarebytes**

Data Source Model: **Breach Remediation**

Data Format: **Default**

Data Retrieval: **SYSLOG (Default)**

Enabled: **SYSLOG (Default)**

Name: MEf

IP Address: SCP File Source

Host Name: HTTP File Source

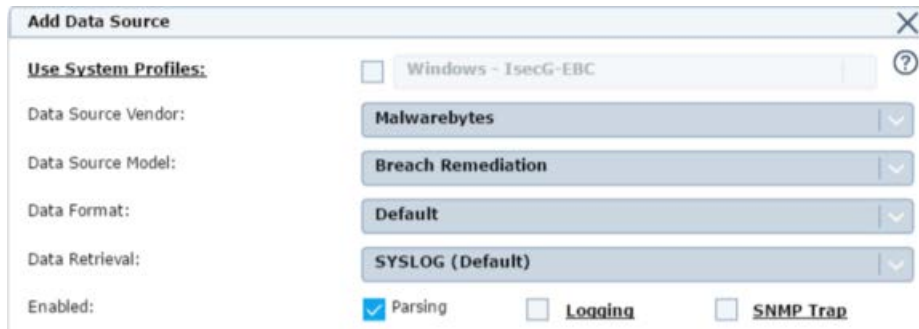
Syslog Relay: FTP File Source

Mask: SFTP File Source

NFS File Source

CIFS File Source

9. Enabled: Parsing/Logging/SNMP Trap – Parsing enables the data source to pass events to the parser. Logging enables the data source to pass raw event data to the Enterprise Log Manager (ELM). SNMP enables reception of SNMP traps for select data sources. If none of the options are checked, the settings are saved to the ESM, but effectively disables the data source. The default is generally Parsing.



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC ?

Data Source Vendor: **Malwarebytes**

Data Source Model: **Breach Remediation**

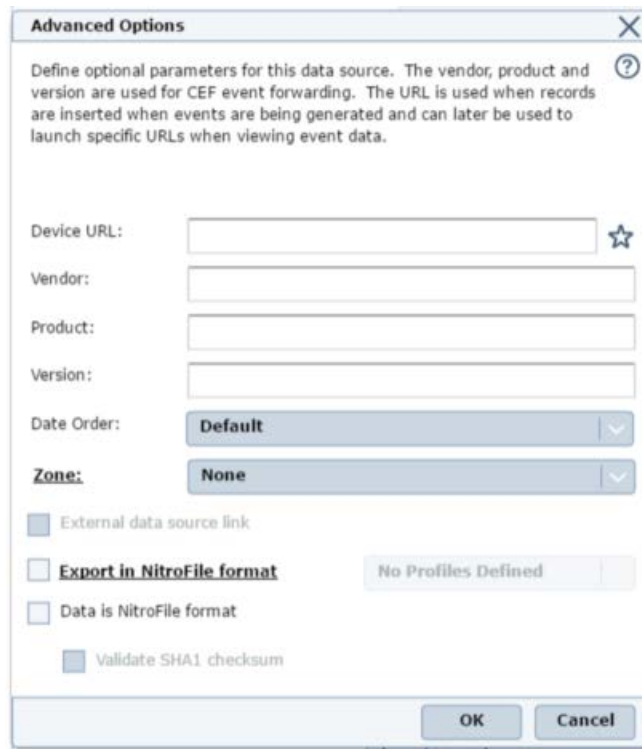
Data Format: **Default**

Data Retrieval: **SYSLOG (Default)**

Enabled: ☒ **Parsing** ☐ **Logging** ☐ **SNMP Trap**

10. Name – This is the name that will appear in the Logical Device Groupings tree and the filter lists.
11. IP Address/Hostname – The IP address and host name associated with the data source device.

12. Syslog Relay – Allows data to be collected via relays with the option to group events under specific data sources based on syslog header details. Enable syslog relay on relay sources such as Syslog-NG.



Advanced Options [X] [?]

Define optional parameters for this data source. The vendor, product and version are used for CEF event forwarding. The URL is used when records are inserted when events are being generated and can later be used to launch specific URLs when viewing event data.

Device URL: ☆

Vendor:

Product:

Version:

Date Order: **Default** ▼

Zone: **None** ▼

☐ External data source link

☐ **Export in NitroFile format** No Profiles Defined

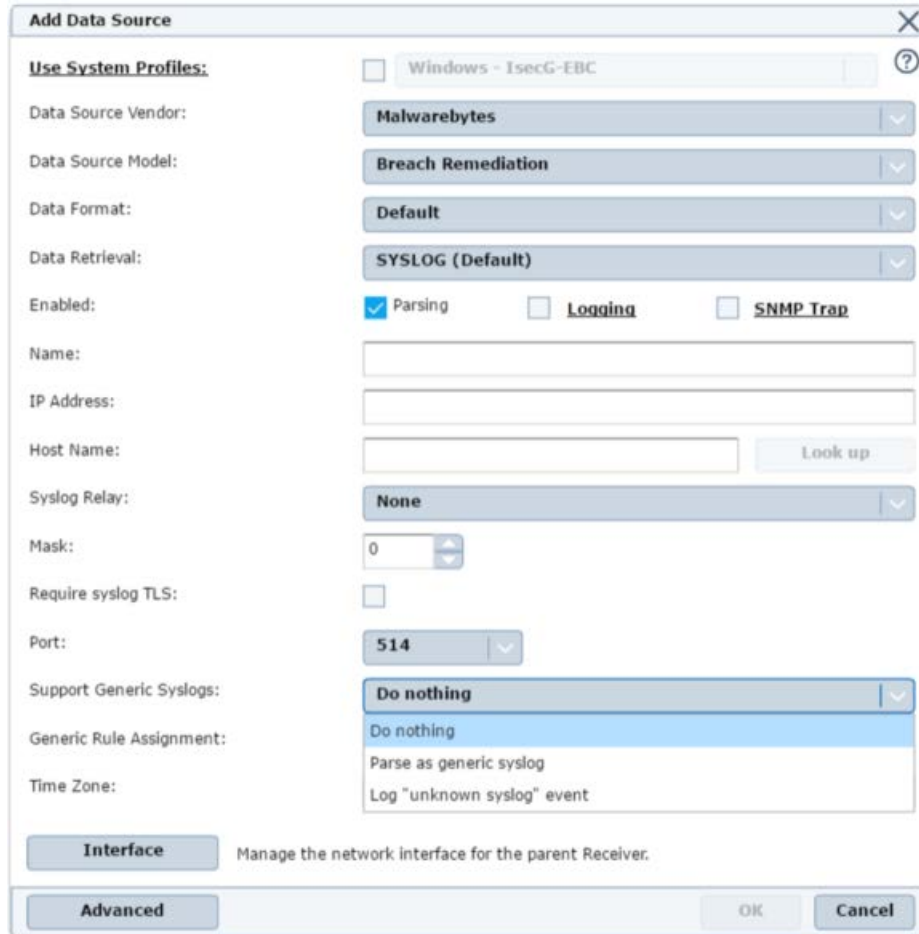
☐ Data is NitroFile format

☐ Validate SHA1 checksum

OK Cancel

13. Mask – Allows a mask to be applied to an IP address so that a range of IP addresses can be accepted.
14. Require Syslog TLS – Enable to require the receiver to communicate over TLS.
15. Port: UDP port for communication

16. Support Generic Syslog – Allows users to select one of the following options: **Parse generic syslog**, **Log unknown syslog event**, or **Do nothing**. These options control how the ESM handles unparsed logs. **Parse generic syslog** will create an event for every unique unparsed event collected. **Log unknown** will create a single generic event and increment the count for every unparsed event. **Do nothing** will ignore unparsed events. The **Parse generic syslog** option should be used sparingly as it can negatively impact the performance of the Receiver and ESM in cases where there is a high incoming rate of unparsed logs. It is recommended that the **Log unknown** option be used if unparsed events need to be reported in ESM, otherwise it is recommended to leave the setting as **Do nothing**.



Add Data Source

Use System Profiles: ☐ Windows - IsecG-EBC

Data Source Vendor: **Malwarebytes**

Data Source Model: **Breach Remediation**

Data Format: **Default**

Data Retrieval: **SYSLOG (Default)**

Enabled: ☒ Parsing ☐ Logging ☐ SNMP Trap

Name:

IP Address:

Host Name: **Look up**

Syslog Relay: **None**

Mask:

Require syslog TLS: ☐

Port: **514**

Support Generic Syslogs: **Do nothing**

Generic Rule Assignment: **Do nothing**

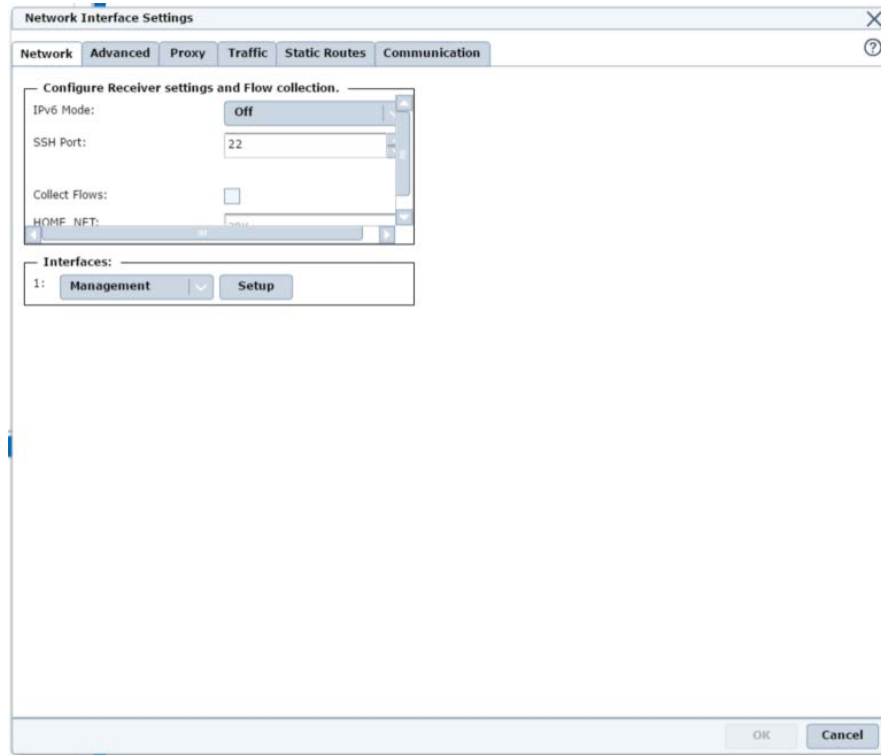
Time Zone:

Interface Manage the network interface for the parent Receiver.


Advanced

OK **Cancel**

17. Generic Rule Assignment – Grayed out since no generic rules are required.
18. Time Zone – This should be set based on the time zone used in the log data. Generally, it is the time zone where the actual data source is located.
19. Interface – Opens the receiver interface settings to associate ports with streams of information.



20. Advanced – Opens advanced settings for the data source.



The 'Advanced Options' dialog box is used to configure parameters for a data source. It includes a title bar with a close button (X) and a help icon (?). The main text area contains instructions: 'Define optional parameters for this data source. The vendor, product and version are used for CEF event forwarding. The URL is used when records are inserted when events are being generated and can later be used to launch specific URLs when viewing event data.' Below this, there are several input fields: 'Device URL' with a star icon, 'Vendor', 'Product', and 'Version'. There are also two dropdown menus: 'Date Order' set to 'Default' and 'Zone' set to 'None'. At the bottom, there are four checkboxes: 'External data source link', 'Export in NitroFile format' (which is checked), 'Data is NitroFile format', and 'Validate SHA1 checksum'. To the right of the 'Export in NitroFile format' checkbox is a button labeled 'No Profiles Defined'. At the very bottom are 'OK' and 'Cancel' buttons.

Advanced Options [X] [?]

Define optional parameters for this data source. The vendor, product and version are used for CEF event forwarding. The URL is used when records are inserted when events are being generated and can later be used to launch specific URLs when viewing event data.

Device URL: [] ☆

Vendor: []

Product: []

Version: []

Date Order: **Default** [v]

Zone: **None** [v]

☐ External data source link

☒ **Export in NitroFile format** [No Profiles Defined]

☐ Data is NitroFile format

☐ Validate SHA1 checksum

[OK] [Cancel]

6 Appendix B – Troubleshooting

If a data source is not receiving events, verify that the data source settings have been written out and that policy has been rolled out to the Receiver.

If there are errors saying events are being discarded because the **Last Time** value is more than one hour in the future, or the values are incorrect, the **Time Zone** settings for the data source or ESM may need to be adjusted.

When creating custom ASP rules, the **Key** and **Value** table located within the **Parsing** tab will display potential field mappings based on the log text entered in the **Sample Log Data** section. None of the data from the **Key** and **Value** table is populated by default. Actual field assignments are set within the **Field Assignment** tab by dragging and dropping the key onto the desired field.

When analyzing parsed event details, fields on the **Custom Types** tab will not be present if the data intended to be captured for that specific field is absent from the received logs.