



# **McAfee Enterprise Security Manager**

## **Data Source Configuration Guide**

Data Source: *Fortinet FortiGate UTM*

December 30, 2013



**Important Note:**

The information contained in this document is confidential and proprietary.  
Please do not re-distribute without permission.

## Table of Contents

|     |   |   |
|-----|---|---|
| 1   | Introduction                                      | 4 |
| 2   | Prerequisites                                     | 4 |
| 3   | Specific Data Source Configuration Details        | 5 |
| 3.1 | FortiGate UTM Configuration                       | 5 |
| 3.2 | McAfee Receiver Configuration                     | 5 |
| 4   | Appendix A - Generic Syslog Configuration Details | 7 |
| 5   | Appendix B - Troubleshooting                      | 7 |



## **1 Introduction**

This guide details how to configure FortiGate UTM version 4.0 and higher to send syslog data in the proper format to the ESM.

## **2 Prerequisites**

McAfee Enterprise Security Manager Version 8.5.0 and above.

In order to configure the FortiGate UTM Syslog service, appropriate administrative-level access is required to perform the necessary changes documented below.

### 3 Specific Data Source Configuration Details

#### 3.1 FortiGate UTM Configuration

Note – Space-delimited logs are the preferred format; however, we do support the comma-separated logs as well.

##### Command Line Interface (CLI)

Enter the following commands

```
config log syslogd setting
    set csv disable
    set facility <Facility Name>
    set port 514
    set reliable disable
    set server <IP Address of Receiver>
    set status enable
end
```

Note - If you already have a syslog server configured in the FortiGate UTM, you can still add up to a total of three syslog servers in the configuration by changing the first line to “config log syslogd2 setting” or “config log syslogd3 setting”.

**(For more information refer to the “FortiOS™ Handbook Logging and Reporting for FortiOS 5.0” under the section “Advanced Logging”).**

##### Through the Fortigate Management Console:

1. Go to **Log&Report > Log Config > Log Setting**
2. Mark the **Syslog** checkbox.
3. Expand the **Options** section to set any custom logging options
4. Then enter the following information in the corresponding fields:
  - a. Name/IP: **Enter the hostname or IP address of the Receiver**
  - b. Port: **514**
  - c. Level: **Desired level of logging (ex. 6 - Information)**
  - d. Facility: **Leave at the default value**
  - e. Enable CSV: **Leave this box unchecked**
5. Click **Apply**

#### 3.2 McAfee Receiver Configuration

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

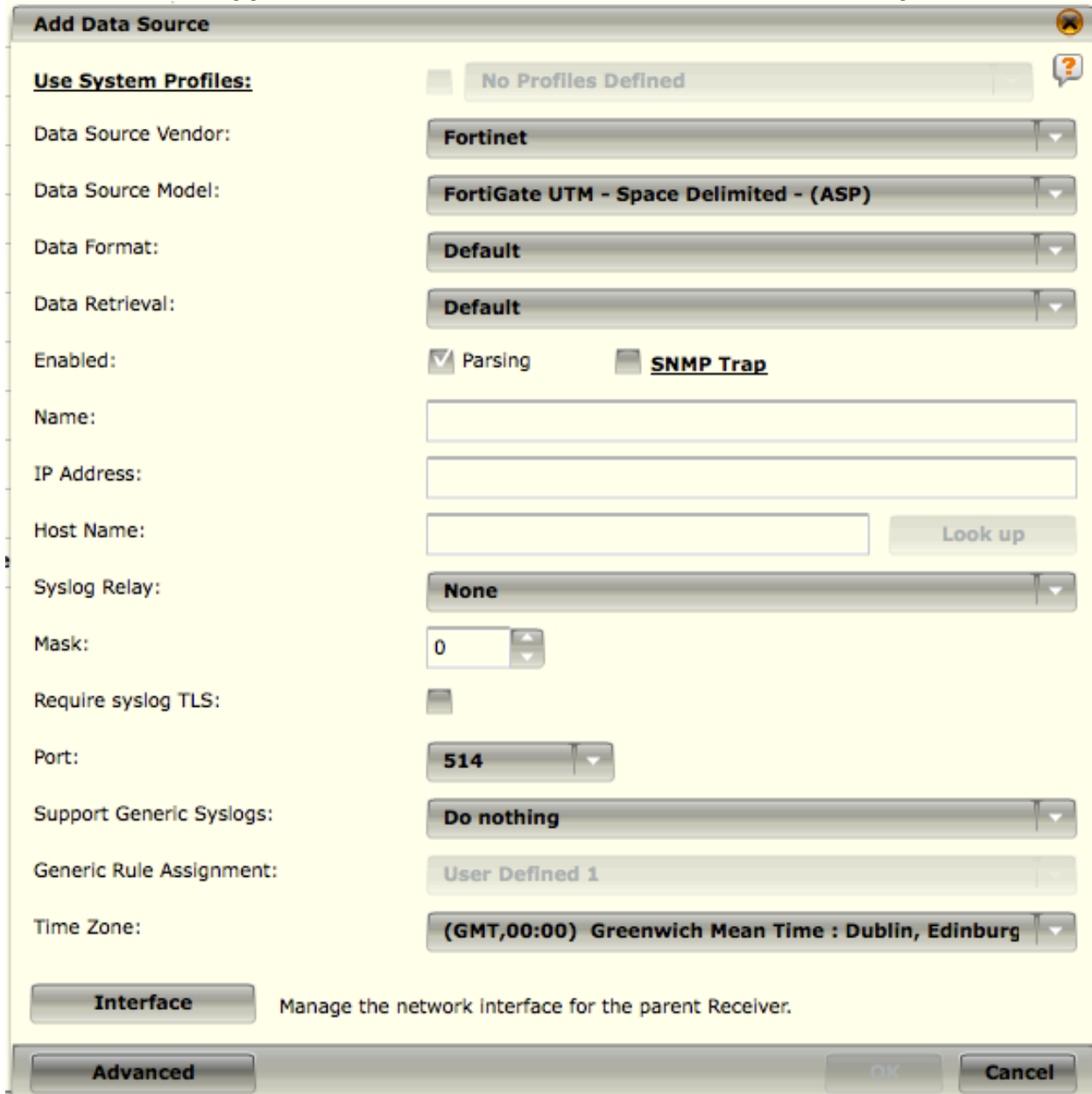
1. Select the Receiver you are applying the data source setting to.
  2. Select the Receiver properties.
  3. From the Receiver Properties listing, select “Data Sources”.
  4. Select “Add Data Source”.
- OR
1. Select the Receiver you are applying the data source setting to.
  2. After selecting the Receiver, select the “Add Data Source” icon.

##### Data Source Screen Settings


1. Data Source Vendor – Fortinet
2. Data Source Model – FortiGate UTM – Space Delimited – (ASP)
3. Data Format – Default

4. Data Retrieval – Default
5. Name – Name of data source
6. IP Address/Hostname – The IP address and host name associated with the data source device.
7. Syslog Relay – None
8. Mask – Default
9. Require Syslog TLS – Leave unchecked
10. Support Generic Syslogs – Do Nothing
11. Time Zone – Time zone of data being sent.

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



**Add Data Source**

Use System Profiles: ☐ No Profiles Defined 

Data Source Vendor: **Fortinet**

Data Source Model: **FortiGate UTM - Space Delimited - (ASP)**

Data Format: **Default**

Data Retrieval: **Default**

Enabled: ☒ Parsing ☐ **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: **User Defined 1**

Time Zone: **(GMT,00:00) Greenwich Mean Time : Dublin, Edinburg**

**Interface** Manage the network interface for the parent Receiver.

**Advanced** **OK** **Cancel**

## 4 Appendix A - Generic Syslog Configuration Details

Once you select the option to add a data source, you are taken to the “Add Data Source” menu. The general options for adding a data source are shown. As you select different options, additional parameters may show. Each of these parameters will be examined in more detail.

1. 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.
2. Data Source Vendor – List of all supported vendors.
3. Data Source Model – List of supported products for a vendor.
4. Data Format – “Data Format” is the format the data is in. Options are “Default”, “CEF”, and “MEF”.

Note – If you choose CEF it will enable the generic rule for CEF and may not parse data source-specific details.

5. Data Retrieval – “Data Retrieval” allows you to select how the Receiver is going to collect the data. Default is over syslog.
6. Enabled: Parsing/Logging/SNMP Trap – Enables parsing of the data source, logging of the data source, and reception of SNMP traps from the data source. If no option is checked, the settings are saved to the ESM, but not written to the Receiver or utilized. Default is to select “Parsing”.
7. Name – This is the name that will appear in the Logical Device Groupings tree and the filter lists.
8. IP Address/Hostname – The IP address and host name associated with the data source device.
9. Syslog Relay – “Syslog Relay” allows data to be collected via relays and bucketed to the correct data source. Enable syslog relay on relay sources such as Syslog-NG.
10. Mask – Enables you to apply a mask to an IP address so that a range of IP addresses can be accepted.
11. Require Syslog TLS – Enable to require the receiver to communicate over TLS.
12. Support Generic Syslog – “Generic Syslog” allows users to select “Parse generic syslog” or “Log ‘unknown syslog event’”. Both these options will create an alert for an auto-learned syslog event if there is no parsing rule.
13. Time Zone - If syslog events are sent in a time zone other than GMT, you need to set the time zone of the data source so the date on the events can be set accordingly.
14. Interface – Opens the receiver interface settings to associate ports with streams of information.
15. Advanced – Opens advanced settings for the data source.

## 5 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 you see errors saying events are being discarded because the “Last Time” value is more than one hour in the future, or the values are incorrect, you may need to adjust the “Time Zone” setting.