Reference Guide

Revision B

McAfee Enterprise Security Manager

Data Source Configuration

Contents

1 Overview

This guide details how to configure data sources to send syslog data in the proper format to the McAfee® Enterprise Security Manager (McAfee ESM) Event Receiver.

McAfee Confidential - Do Not Redistribute Without Permission

The information in this document regarding McAfee or third-party products or services is provided for the education and convenience of McAfee customers only.

All information contained herein is subject to change without notice, and is provided *AS IS* without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

2 System requirements

Administrative level access

To configure each data source service, you must have appropriate administrative level access.

Required software

Each data source supports a specific version of McAfee ESM and some have additional requirements.

Vendor	Model	ESM Version	Data Source Requirements
A10 Networks	Load Balancer	8.4.2 and later	None
Accellion	Secure File Transfer	9.1.0 and later	None
Access Layers	Portnox	9.2.0 and later	None
Adtran	Bluesocket	9.1.1 and later	None
	NetVanta	9.2.0 and later	None
AirTight Networks	SpectraGuard	9.2.0 and later	None
Alcatel-Lucent	NGN Switch	9.0.0 and later	None
	VitalQIP	9.2.0 and later	None
Amazon	CloudTrail	9.5.1 and later	None
Apple, Inc	Mac OS X	9.1.0 and later	None
Arbor Networks	Pravail	9.1.0 and later	None
ArcSight	Common Event Format	9.2.0 and later	None
Aruba	ClearPass	9.5.0 and later	Aruba ClearPass 6.6.0 and later
Attivo Networks	BOTsink	9.5.0 and later	Attivo BOTsink 3.3 or later
Axway	SecureTransport	9.1.0 and later	None
Barracuda Networks	Spam Firewall	8.5.0 and later	None
	Web Application Firewall	9.1.0 and later	None
	Web Filter	8.5.0 and later	None
Bit9	Parity Suite	9.1.0 and later for Basic (RFC 3164) logs	None
		9.2.0 and later for CEF (ArcSight) formatted logs	None
Blue Coat Systems	Director	9.2.0 and later	None

Vendor	Model	ESM Version	Data Source Requirements
	ProxySG Access Log	8.3.0 and later	To use FTP, use an intermediary server running FTP services (such as FileZilla or vsftpd), which has sufficient storage to store the Access logs.
	Reporter	9.5.0 and later	Make sure that your API key has been generated before you add this Data Source.
BlueCat Networks	DNS/DHCP Server	9.1.0 and later	None
Blue Ridge Networks	BorderGuard	8.3.0 and later	None
Brocade	IronView Network Manager	9.2.0 and later	None
	VDX Switch	9.2.0 and later	None
Check Point	Check Point	9.2.0 and later	None
Cisco	IOS	8.2.0 and later	None
	IOS IPS	9.5.1 and later	None
	Meraki	9.4.1 and later	Supports multiple series of the devices from the Meraki line (for example, MR series and MX series).
	NX-OS	9.4.0 and later	None
	PIX ASA	9.0.0 and later	ASDM must be enabled and installed on the target device before you follow the configuration instructions included here. There are other methods to configure syslog. This is the only method covered in this document.
	Unified Computing System	9.0.0 and later	None
	Wireless LAN Controller	9.2.0 and later	None
Citrix	NetScaler	8.2.0 and later	None
	Secure Gateway	9.2.0 and later	None
Cluster Labs	Pacemaker	8.3.0 and later	None
Code Green	Data Loss Prevention	9.1.0 and later	None
Cooper Power Systems	Yukon IED Manager Suite	8.4.2 and later	None
	Cybectec RTU	9.4.0 and later	None
Corero	IPS	8.2.0 and later	None
CyberArk	Enterprise Password Vault	9.2.0 and later	None
	Privileged Identity Management Suite	9.2.0 and later	None
	Privileged Threat Analytics	9.5.0 or later	CyberArk PTA 3.1 or later
Damballa	Failsafe	9.1.0 and later	None
Dell	PowerConnect Switches	8.3.0 and later	None
	Aventail	8.3.0 and later	None

Vendor	Model	ESM Version	Data Source Requirements
	Sonic OS	8.2.0 and later	None
DG Technology - InfoSec	Mainframe Event Acquisition System (MEAS)	9.0.0 and later	None
Econet	Sentinel IPS	9.2.0 and later	None
EdgeWave	iPrism Web Security	8.3.0 and later	None
Enforcive	Cross-Platform Audit	9.4.0 and later	None
Entrust	IdentityGuard	8.5.0 and later	None
Extreme Networks	ExtremeWare XOS	9.2.0 and later	None
F5 Networks	Local Traffic Manager	8.3.0 and later	None
	FirePass SSL VPN	8.3.0 and later	None
Fidelis	XPS	9.1.0 and later	None
FireEye	Malware Protection System	9.0.0 and later	None
Fluke Networks	AirMagnet Enterprise	8.4.2 and later	None
Force10 Networks	FTOS	8.3.0 and later	None
Forcepoint	Websense	9.2.0 and later	None
ForeScout	CounterACT	8.4.0 and later for standard syslog	None
		9.0.0 and later for CEF formatted syslog	None
Fortinet	FortiGate UTM	8.5.0 and later	None
	FortiMail	9.4.0 and later	None
	FortiManager	9.1.0 and later	None
Fortscale	User and Entity Behavior Analytics (UEBA)	9.5.0 and later	Fortscale UEBA 2.7 and later
FreeRADIUS	FreeRADIUS	8.3.0 and later	None
Gigamon	GigaVUE	9.1.1 and later	None
Globalscape	Enhanced File Transfer (EFT)	9.4.1 and later	None
HBGary	Active Defense	9.0.0 and later	None
Hewlett-Packard	LaserJet Printers	8.3.0 and later	None
	3Com Switches	8.3.0 and later	None
	ProCurve	8.1.0 and later	None
HyTrust	Appliance	9.2.0 and later	None
IBM	Guardium	8.3.0 and later	None
	WebSphere Application Server	9.4.1 and later	None
Infoblox	NIOS	9.0.0 and later	None
InterSect Alliance	Snare For Windows	9.1.0 and later	None
Interset	Interset	9.5.1 and later	None
Juniper Networks	JUNOS Structured Data Format	9.1.1 and later	You must have System-Control level rights on JUNOS.

Vendor	Model	ESM Version	Data Source Requirements
	NetScreen	9.2.0 and later	None
	Network and Security Manager	9.2.0 and later	None
Kaspersky	Administration Kit	9.2.1 and later	None
Lastline	Enterprise	9.5.0 and later	None
Locum	RealTime Monitor	9.0.0 and later	None
LOGbinder	LOGbinder	9.2.0 and later	None
Lumension	LEMSS	9.2.0 and later	None
	Bouncer	8.2.0 and later for syslog	None
		9.2.0 and later for CEF	None
Malwarebytes	Breach Remediation	9.5.0 and later	None
	Management Console	9.5.0 and later	Malwarebytes Management Console 1.7
McAfee	Database Security	9.1.0 and later	None
	Email and Web Security 5.x.x	9.1.0 and later	None
	Email and Web Security 6.x.x and later	9.2.0 and later	None
	ePolicy Orchestrator	9.2.0 or later	McAfee ePolicy Orchestrator 4.6.0 or later.
	Firewall Enterprise	9.2.0 and later	None
	Network DLP Monitor	9.1.0 and later	None
	Network Security Manager	8.5.0a and later for sending data over syslog from IntruShield 6.x.x	None
		9.1.0 and later for sending data over syslog from McAfee Network Security Manager 6.x.x and later	None
		9.1.2 and later for pulling SQL data from McAfee Network Security Manager 6.x.x and later	None
	Network Threat Response	9.4.1 and later	McAfee Network Threat Response 4.0.0.5 or later
	Next Generation Firewall	9.2.0 and later	McAfee® Next Generation Firewall (McAfee NGFW) (version 7 of Stonesoft)
	UTM Firewall	9.2.0 and later	None
Microsoft	DNS	9.2.0 and later	None

Vendor	Model	ESM Version	Data Source Requirements
	Forefront Endpoint Protection 2010	9.3.2 and later	Database credentials with at least read-only rights to the information schema, the FEP data warehouse database, and the vwFEP_AM_NormalizedDetectionHistory. FEP Database server must have remote TCP connections enabled.
	Internet Authentication Service (IAS)	9.1.0 and later	None
	Internet Information Services (IIS)	9.2.0 and later	None
	Network Policy Server (NPS)	9.5.2 and later	None
	Office 365	10.1.0 or later	Administrative rights to the Microsoft Office Azure portal
	Windows DHCP Server	9.4.0 and later	None
	Windows Event Log WMI	9.2.1 or later for Microsoft Windows XP, Server 2003 or later 9.3.2 or later for Microsoft Windows 8.1, Server 2012-R2 or later	Administrative rights on the Windows device
Motorola	AirDefense	9.0.0 and later	None
NetFort Technologies	LANGuardian	8.5.0 and later	None
NetWitness	Spectrum	9.0.0 and later	None
Niara	Niara	9.5.0 and later	Niara 1.5 or later
Nortel Networks	Contivity	9.4.0 and later	None
	Passport 8000 Series Switch	8.3.0 and later	None
Novell	eDirectory	9.2.0 and later	None
	Identity and Access Management	9.1.0 and later	None
Oracle	Audit	9.2.1 and above	Oracle 9i, 10g, 11g, or 12c
	Internet Directory Server	9.4.1 and later	None
Palo Alto Network	PAN-OS	8.3.0 and later	None
PhishMe	Intelligence	9.5.0 and later	None
	Triage	9.5.1 or later	PhishMe Triage 2.0 or later
Proofpoint	Messaging Security Gateway	9.2.0 and later	None
Raytheon	SureView	9.0.0 and later	None
Raz-Lee Security	iSecurity Suite	9.2.0 and later	None
Red Hat	JBoss Application Server/ WildFly 8	9.4.1 and later	None

Vendor	Model	ESM Version	Data Source Requirements
RedSeal Networks	RedSeal 6	9.1.0 and later	None
ReversingLabs	N1000 Network Security Appliance	9.5.0 and later	None
RioRey	DDOS Protection	9.2.0 and later	None
Riverbed	Steelhead	8.3.0 and later	None
RSA	Authentication Manager	8.4.2 and later	None
SafeNet	Hardware Security Modules	9.4.1 and later	None
Skycure	Skycure Enterprise	9.4.0 and later	None
Skyhigh Networks	Cloud Security Platform	9.5.1 or later	Skyhigh Cloud Security Platform 2.2 or later Enterprise Connector for SkyHigh
Sophos	Web Security and Control	8.5.0 and later	None
Sourcefire	FireSIGHT Management Console - eStreamer	9.4.0 and later	None
SSH Communications Security	CryptoAuditor	9.4.1 and later	None
STEALTHbits	StealthINTERCEPT	9.4.0 and later	None
Symantec	Data Loss Prevention	9.1.0 and later	None
	Endpoint Protection	8.4.0 and later	None
	Messaging Gateway	9.1.0 and later	None
	PGP Universal Server	8.5.0 and later	None
	Web Gateway	8.3.0 and later	None
ThreatConnect	Threat Intelligence Platform	9.5.0 and later	ThreatConnect Threat Intelligence Platform version 3 or later
TippingPoint	SMS	9.2.0 and later	None
Tofino Security	Firewall LSM	8.4.0 and later	None
Topia Technology	Skoot	9.2.0 and later	None
TrapX Security	DeceptionGrid	9.5.0 and later	TrapX Security - DeceptionGrid version 5.x
Trend Micro	Deep Security	9.2.0 and later	None
	Deep Security Manager	9.2.0 and later	None
	OfficeScan	9.2.0 and later	None
Trustwave	Data Loss Prevention	9.2.0 and later	None
	Network Access Control	8.4.0 and later	None
Type80 Security Software	SMA_RT	9.4.0 and later	None
Unix	Linux	9.2.0 and later	None
Verdasys	Digital Guardian 6.1.2	9.2.0 and later	None
VMware	VMware	9.2.0 and later	None
	AirWatch	9.4.1 and later	None

Vendor	Model	ESM Version	Data Source Requirements
	vCenter Server	9.3.2 and later	None
Vormetric	Data Security Manager	9.2.0 and later	None
WatchGuard Technologies	Firebox	8.5.0 and later	None
Websense	Websense Enterprise	9.2.0 and later	None
WurldTech	OpShield	9.4.1 and later	Wurldtech Opshield (R1.7.1)
Xirrus	802.11abgn Wi-Fi Arrays	8.3.0 and later	None
ZeroFox	Riskive	9.2.0 and later	None
Zscaler	Nanolog Streaming Service	9.4.0 and later	None

3 Configuring McAfee data sources

Contents

McAfee Data Loss Prevention Monitor

Contents

Configure McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor)

Configure McAfee DLP Monitor to forward logs.

Task

1. In the **navigation pane**, expand **Application Security**, point to **Options**, then click **Logging Profiles**.
2. Above the **Logging Profiles** area, click **Create**.
3. For **Configuration**, select **Advanced**.
4. For **Profile Name**, type a unique name for the logging profile.
5. Select **Remote Storage**, then select **Reporting Server** for the **Type**.
6. If you do not want data to be logged locally while it is being logged remotely, deselect **Local Storage**.
7. For **Protocol**, select **UDP**.
8. For **Server IP**, type the IP address of the McAfee Event Receiver.

9 For **Server Port**, type **514** (the default port used for Syslog).

10 (Optional) To ensure that system logging takes place, even when the logging utility is competing for system resources, select **Guarantee Logging**.

11 (Optional) To log details about brute force attacks, DoS attacks, IP enforcer attacks, or web scraping attacks, select **Report Detected Anomalies**. Examples of log details can include start and end time, number of dropped requests, and attacking IP addresses.

12 Click **Create**.

Add McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	Network DLP Monitor
Data Format	Default
Data Retrieval	Syslog (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

McAfee DLP Monitor events to McAfee ESM fields

Log format

The expected format for this device is:

```
CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|deviceEventClassId|Name|Severity|
Extension
```

Log sample

This is a sample log from a McAfee DLP Monitor device:

```
<13>RTS: CEF:0|McAfee|iGuard|9.2|CNN wget|CNN wget|Medium|cs1=Policy for prevenct
cs1Label=policies cn1=2 cn1Label=MatchCount src=172.3.2.1 dst=172.1.2.3 spt=54399 dpt=1344
```

```
app=HTTP_Request cs3=HTTP_Header cs3Label=Content cs4=etl.1 cs4Label=partition_name
cn2=13291520 cn2Label=partition_offset cs5=2147484161 cs5Label=instance fsize=187 end=Jul 23
2012 13:47:13 suser= duser= cs2="" cs2Label=Subject fname=Unknown
```

Mappings

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

Log fields	McAfee ESM fields
request	URL
cs2	Subject
cs1	Object
fname	Filename
cs3	Object_Type
cn1	Message_Text
Name	Message
duser	Destination_Username
suser	Source User
cnt	Event Count
shost	Hostname
proto	Protocol
src	
spt	Source Port
smac	Source MAC
dst	Destination IP address
dpt	Destination Port
dmac	Destination MAC
app	Application
start, end, rt, tstamp, collection	First Time, Last Time

McAfee Database Security

Contents

Configure McAfee® Database Security

Task

1 Log on to McAfee® Database Security console.

2 Select **System** | **Interfaces** | **Syslog**.

3 Select **Use syslog**.

4 Configure the correct syslog host/port (IP address and port of the McAfee Event Receiver).

5 Select transport protocol.

6 Set syslog format to **CEF**.

7 Click **Save**.

Add McAfee Database Security

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	Database Security - CEF (ASP)
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device
Syslog Relay	Leave Default
Mask	Leave Default
Require Syslog TLS	Deselected
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

McAfee Database Security events to McAfee ESM fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a McAfee Database Security device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

McAfee Email and Web Security

Contents

Configure McAfee Email and Web Security 6.x.x or later (CEF)

Task

1. Open and log on to the Appliance Management Console.
2. Select **System** | **Logging** | **Alerting and SNMP** | **System Log Settings**.
3. Click **Enable system log events**.
4. To enable CEF format, select the Logging format **ArcSight**.
5. Select **Off-box system log** and click **Add Server**.
6. Add the McAfee Event Receiver IP address and port (default is 514).

Configure McAfee Email and Web Security 5.x.x (syslog)

Task

1. Open and log on to the Appliance Management Console.
2. Select **System** | **Logging** | **Alerting and SNMP** | **System Log Settings**.
3. Click **Enable system log events**.
4. To enable standard non-formatted syslog messages, select the Logging format **Syslog**.
5. Select **Off-box system log** and click **Add Server**.
6. Add the McAfee Event Receiver IP address and port (default is 514).

Add McAfee Email and Web Security

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	For Syslog, select **EWS v5 / Email Gateway Original Format - Legacy (ASP)**. For CEF, select **Email Gateway - CEF (ASP)**.
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the McAfee Event Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

McAfee Email and Web Security 6.x.x events to McAfee ESM fields

Log format (CEF)

The expected format for this device is:

```
|Device Vendor|Device Product|Signature ID|Name|Severtiy| act=<action> app=<application>
msg=<message> dst=<destination IP> dhost=<destination host> src=<source IP> dpt=<destination
port> spt=<source port> dmac=<destination MAC> smac=<source MAC> suser=<source user>
duser=<destination user> deviceDirection=<direction> sourceServiceName=<name> fsize=<file
size> rt=<reception time> cs1Label=virus-names cs1=<virus name> cs4Label=email-attachments
cs4=<attachment name> cs6Label=email-subject cs6=<email subject> cn3Label=
number-email-recipients cn3=<number of recipients> cn2Label=num-email-attachments
cn2=<number of attachments> cnt=<count>
```

Log sample (CEF)

This is a sample log from a McAfee Email and Web Security device:

```
Jan 1 01:23:45 bridge : CEF:0|McAfee|Email Gateway|7.0|12345|Email Status|5|act=service
app=smtp msg=Email blocked with SMTP Code 550 dvc= dst= dhost= src=1.2.3.4
shost=ext-server.std.dom suser=<sender@domain.com> duser=<recipient@domain.com>
deviceDirection=0 sourceServiceName= filePath=
fileId=a0b1_c2d3_e4f5a6b7_c8d9_e0f1_a2b3_c4d5e6f7a8b9 fsize=123 rt=1234567891011
flexNumber1=123 flexNumber1Label=reason-id cs4Label=email-attachments cs4=
cs5Label=master-scan-type cs5= cs6Label=email-subject cs6=WSTest mail
McafeeEmailgatewayOriginalSubject= McafeeEmailgatewayOriginalSender=
```

```
McafeeEmailgatewayOriginalMessageId= McafeeEmailgatewayEmailEncryptionType=
cn1Label=is-primary-action cn1= cn2Label=num-email-attachments cn2=0
cn3Label=number-email-recipients cn3=1
```

Mappings (CEF)

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

Log fields	McAfee ESM fields
Signature ID	Sid
Name	Message
Severity	Severity
sourceServiceName	Policy Name
email-subject	Message Text
virus-names	Threat Name
Device Vendor and Device Product	Category
email-attachments, dlpfile, imagefile	Filename
deviceDirection	Direction
fsize	Bytes Sent
number-email-recipients	Recipient Count
suser	From
duser	To
act	Device Action
app	Application
act	Command Name
dst	Destination IP
src	Source IP
dhost	Hostname
rt	First Time, Last Time
dpt	Destination Port
spt	Source Port
dmac	Destination MAC
smac	Source MAC
cnt	Event Count
msg	Reason

McAfee Email and Web Security 5.x.x events to McAfee ESM fields

Log format (syslog)

The expected format for this device is:

```
timestamp Application=<app> Event=<event> status=<status> User=<username> source=<source ip>
virusname=<Virus.Name> filename=http://example.com/example.exe from=<from> size=<size>
nrcpts=<number of recipients> to=<to> relay=<destination ip> subject=<email subject>
spamrules=<signature name>  attachment(s)=<name of attachment>
```

Log sample (syslog)

This is a sample log from a McAfee Email and Web Security device:

```
<22>Jan  1 01:23:45 mx1 Application=http, Event='Anti-virus engine detection', status='The
content was categorized as a Potentially Unwanted Program', User=user1@DOMAIN.LOCAL,
source=(192.0.2.10), msgid=1234_5678_a0b1c23_d4e5_f7a8_b9c0_d1e2f3a4b5v6,
virusname=Cookie-Adserver (Abc\123\123abc Element), filename= http://example.com/homepage;
```

Mappings (syslog)

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

Log fields	McAfee ESM fields
timestamp	First Time, Last Time
Application	Application
Event	Message
status	Reason
from	From
to	To
User	Source User
source	Source IP
relay	Destination IP
virusname	Threat Name
filename, attachment	Filename
spamrules	Signature Name
size	Bytes Sent
subject	Subject

McAfee ePolicy Orchestrator

McAfee® ePolicy Orchestrator® (McAfee® ePO™) can be added as a device on McAfee ESM. McAfee ePO applications are listed as child data sources in the McAfee ESM device tree. Once authenticated as a device, you can access some McAfee ePO functions from the McAfee ESM. If you don't need this enhanced integration functionality, you can add McAfee ePO as a data source on a McAfee Event Receiver.

Contents

Configure the Database Server user account

This task applies to device options and data source configuration options. Both require a McAfee ePO database user account, which enables the McAfee Event Receiver to collect the data from the McAfee ePO database.

Task

1 Log on to the McAfee ePO database server.

2 Start **SQL Server Management Studio** | **Enterprise Manager**.

3 Expand the **Console Root** node several times to view the items under the **Security** folder.

4 Right-click the **Logins** icon, then select **New Login**.

5 On the **General** page, do the following:

   a In**Login name**, enter a user name (such as, `epo`) that the McAfee Event Receiver uses to connect to the McAfee ePO database.

   b Select **SQL Server Authentication**, then enter and confirm a password.

   c From the **Default database** menu, select the McAfee ePO database from the **Database** drop-down list.

   If you leave the Default database as master, the McAfee Event Receiver fails to pull events.

6 Select the **User Mapping** page.

   a Select the database where the user's logon is mapped.

   b For **Database role membership**, select **db_datareader**.

7 Click **OK** to save.

8 Log off from the SQL Server Management Studio/Enterprise Manager.

Configure the application server user account

This task applies only to the device configuration option. The McAfee ESM user account must have rights that allow ESM to use enhanced integration features such as McAfee ePO tagging and actions, McAfee® Risk Advisor, and McAfee® Threat Intelligence Exchange (TIE).

Task

1 Log on to the McAfee ePO console using an account with the appropriate rights.

2 Select **Menu** | **Permission Sets** | **User Management**.

3 Create a named group by selecting **Actions** | **New**, then click **Save**.

4 Add rights so that the McAfee ESM account works properly. With the new group selected, scroll down to **Systems**, then select **Edit**.

5 In **Systems** , select these options, then click **Save**.

   a For **Actions**, select **Wake up agents, view Agent Activity Log**.

   b For **Tag use**, select **Apply, exclude, and clear tags**.

6 To assign users to the group, in the **User Management** section, select **Menu** | **Users**.

7 Select **New User** and define these options:

   a Enter the **New User** name.

   b Set the **Logon status** to **Enabled**.

c Set the **Authentication type** to **ePO authentication** and enter the password.

d Set the **Manually assigned permission sets** to **Selected permission sets** and **McAfee SIEM**, then click **Save**.

Differences in configuration options for ePolicy Orchestrator

Additional ESM features are available when McAfee ePO is configured as a device in ESM. This table lists most of the difference in features available for each configuration.

McAfee ePO connected as a device	McAfee ePO connected as a data source
McAfee ePO listed in the ESM device tree as a device	McAfee ePO listed in the ESM device tree as a data source
Associated McAfee ePO applications listed as child data sources under the device	N/A
Assign tags in McAfee ePO from ESM for source or destination IP addresses and events generated by alarms	N/A
Automatic enablement of McAfee® Threat Intelligence Exchange (TIE) reporting in ESM over McAfee® Data Exchange Layer (DXL), if a TIE server is connected to McAfee ePO	N/A
Enablement of McAfee® Risk Advisor data acquisition	N/A
Automatic enablement of ACE correlation rules for TIE and Risk Advisor	N/A
Automatic enablement of Alarms and Watchlists for TIE	N/A
Ability to query multiple McAfee ePO devices for custom reports or views in ESM	N/A

Add McAfee ePolicy Orchestrator as a data source

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	ePolicy Orchestrator (ASP)
Data Format	Default
Data Retrieval	SQL (Default)
Enabled	Check Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
User ID	The McAfee ePO database user name
Password	The McAfee ePO database password
Port	The McAfee ePO database port (default is 1433)
Database Name	The McAfee ePO database name
Database Instance	The database instance, if any

Add McAfee ePolicy Orchestrator as a device

After successfully logging on to the McAfee ESM console, you can add a McAfee ePO device via the Device wizard. You must have the user names and passwords, created previously, for the McAfee ePO Application Server and the McAfee ePO database server.

Task

1 From the device tree, select **Physical Display**, then click the **Add Device** icon from the **Action** toolbar.

2 In the **Add Device Wizard**, select **McAfee ePolicy Orchestrator (v4.6 or newer)**, then click **Next**.

3 Enter a name for the McAfee ePO device, then click **Next**.

   a Select the McAfee Event Receiver that connects to the McAfee ePO device.

   b Enter the application IP address of the McAfee ePO Application Server.

   c Enter the application port (default is 8443).

   d Enter the application user name for the McAfee ePO web interface.

   e Enter the application password for the McAfee ePO web interface.

   f When McAfee ePO is added on the ESM, the ESM can check for the presence of a Threat Intelligence Exchange (TIE) server. If one is present, the ESM begins listening and retrieving events from the Data Exchange Layer (DXL). To use this feature, select **Enable DXL**.

4 Test the McAfee Event Receiver's ability to connect to McAfee ePO by clicking **Connect**. When the connection is successful, click **Next**.

If the connection fails, verify the user credentials and that no firewall policies are blocking the connection between the McAfee Event Receiver and McAfee ePO.

Select **Require user authentication** only if each McAfee ePO user has a separate account for each device.

a Enter the database IP address of the McAfee ePO database server.

b Enter the database port (default is 1433).

c Enter the database user name.

d Enter the database password.

e Enter the database name.

f If using database instances, enter the database instance name.

5 Test the McAfee Event Receiver's ability to connect to the McAfee ePO database by clicking **Connect**. When the connection is successful, click **Next**.

If the connection fails, make sure that you are using the correct user credentials, and that no firewall policies are blocking the connection between the McAfee Event Receiver and McAfee ePO.

A status window appears while McAfee ePO is added as a device in ESM.

6 When McAfee ePO is successfully added, click **Finish**.

7 In the ESM device tree, expand the new McAfee ePO device.

a Confirm the connection to the McAfee ePO host

b Identify the McAfee products discovered by ESM as installed extensions in McAfee ePO.

Integrate McAfee ePolicy Orchestrator

McAfee Enterprise Security Manager can start McAfee ePO directly from its interface, allowing the user to view endpoint details stored in McAfee ePO.

This advanced integration assumes that McAfee ePO has been added as a device, and that the local network settings have been properly configured in Asset Manager. If the local network settings have already been configured, skip to section 6.2.

This configuration example assumes one McAfee ePO server with a local SQL database. In configurations where the McAfee ePO server is connected to a secondary SQL database server, contact McAfee support for assistance.

Tasks

- *Enable the ability to start ePolicy Orchestrator from ESM* on page 38
- *Start ePolicy Orchestrator from ESM to view details about Managed Assets* on page 39
- *Assign ePolicy Orchestrator tags from McAfee ESM* on page 39

Enable the ability to start ePolicy Orchestrator from ESM

Task

1 From the menu in the upper-right corner of the ESM, click the **Asset Manager** icon.

2 On the **Network Discovery** tab of the **Asset Manager** window, click **Local Network**.

3 Enter the IP addresses and optional subnets that make up the **Local Network**, then click **OK**.

McAfee ESM now allows the user to start McAfee ePO and view details specific to a managed endpoint.

Start ePolicy Orchestrator from ESM to view details about Managed Assets

Task

1. Select an event from the ESM views that contain source or destination IP addresses associated with a managed asset in McAfee ePO.
2. In the upper left of the component window, click the menu icon.
3. Select **Actions** | **View in ePO**from the expanded menu.
4. Select a McAfee ePO device (if applicable), then click **OK**.
   - If only one McAfee ePO device or data source appears on the system, the McAfee ePO interface starts.
   - If more than one McAfee ePO devices or data sources appear on the system, select the one you want to access. The McAfee ePO interface starts for that device.
   - If an event or flow is selected from a table component in ESM, with both a source IP address and destination IP address from the local network, the user must also select which IP address is used in the lookup. Once the IP address is identified, the McAfee ePO interface starts.
5. When prompted for authentication with McAfee ePO, enter the appropriate McAfee ePO credentials to log on.

   Once authenticated, the asset information window for McAfee ePO displays details related to the endpoint that you selected from the event in ESM.

Assign ePolicy Orchestrator tags from McAfee ESM

With viewing managed endpoints on the McAfee ePO server, McAfee ESM supports assigning ESM tags to assets and alarms directly from the console.

Task

1. Select an event from the ESM views that contain source or destination IP addresses associated with a managed asset in ESM.
2. In the upper left of the component window, click the menu icon.
3. From the expanded menu, select **Actions** | **ePO Tagging**.
4. Select a policy tag from the list, then click **Assign**.
5. (Optional) Once you assign an ESM tag to the endpoint, select **Wake up client**.
6. When finished, click **Close**.
7. (Optional) To access the ESM tagging options:
   a. Select an ESM device in the ESM device tree, then click the **Properties** icon above the device tree.
   b. To display the tagging options, select **ePO Tagging** from the left side of the **ePO Properties** window.

McAfee ePO device authentication problems

McAfee ePO authentication credentials must be added to ESM before using McAfee ePO tags or actions.

There are two types of authentication:

- Single global account — If the user belongs to a group that has access to a McAfee ePO device, the integration features can be used after entering the global credentials.
- Separate account for each device per user — The user must have permission to view the device in the ESM device tree.

Select a method of authentication to employ when using tags or actions. If the credentials are not found or are invalid, the user is prompted to enter valid credentials, which must be saved to allow future communication with the device.

Tasks

- *Configure separate account authentication* on page 40

Configure separate account authentication

Global account authentication is the default setting in ESM. You must configure separate account authentication.

1 Verify that **Require user authentication** is selected when adding the McAfee ePO device on the ESM, or when configuring its connection settings (see Add McAfee ePolicy Orchestrator as a device on page 37).

2 Enter the credentials on the ESM **options** page.

   a On the system navigation bar of the ESM console, click **options**, then click **ePO Credentials**.

   b Select a McAfee ePO device and click **Edit**.

   c Provide the user name and password for the selected device, then click **Test Connection**.

   d Click **OK** when the test passes.

McAfee Firewall Enterprise

Contents

Configure McAfee Firewall Enterprise

Task

1 From the McAfee Firewall Enterprise Admin Console, select **Monitor** | **Audit Management**, then click the **Firewall Reporter/Syslog** tab.

2 In the **Export audit to syslog servers** section, click **New** on the toolbar.

3 Enter the IP address of the McAfee Event Receiver where the logs are sent.

4 From the **Remote Facility** drop-down list, select a syslog facility to help identify the audit export.

5 (Optional) Click in the **Description** cell and type a description of the audit export entry.

6 Verify these settings from the advanced options, then press OK.

   - Port: 514
   - Format: SEF

7 Save the changes.

Add McAfee Firewall Enterprise

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	Firewall Enterprise (ASP)
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Mask	Default
Require Syslog TLS	Leave unchecked
Support Generic Syslogs	Default
Time Zone	Time zone of data being sent

McAfee Firewall Enterprise events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a McAfee Firewall Enterprise device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol

Log fields	McAfee ESM fields
Source	Source IP
Destination	Destination IP

McAfee Network Security Manager

Contents

Configure McAfee Network Security Manager 7.x.x

Task

1 Log on to the management interface as an administrator.

2 Click the **Configure** icon on the dashboard.

3 In the resource tree, click the **root node** (usually **My Company**).

4 Click the **Fault Notification** tab, then click **Syslog**.

5 Change these settings, then click **Save**:

- Enable Syslog Forwarder: **Yes**
- Server Name or IP address: **Enter the IP/Hostname of your Receiver**
- Port: **514**
- With Severity: **Informational and above**

6 Click **Edit**.

7 Insert this text into the **Message** field:

```
|$IV_SENSOR_ALERT_UUID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"|$IV_ATTACK_ID
$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|
$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|
$IV_DESTINATION_PORT$|$IV_CATEGORY$|$IV_SUB_CATEGORY$|$IV_DIRECTION$|$IV_RESULT_STATUS$|
$IV_DETECTION_MECHANISM$|$IV_APPLICATION_PROTOCOL$|$IV_NETWORK_PROTOCOL$|$IV_RELEVANCE$|
$IV_QUARANTINE_END_TIME$|$IV_MCAFEE_NAC_FORWARDED_STATUS$|$IV_MCAFEE_NAC_MANAGED_STATUS$|
$IV_MCAFEE_NAC_ERROR_STATUS$|$IV_MCAFEE_NAC_ACTION_STATUS$|$IV_SENSOR_CLUSTER_MEMBER$|
$IV_ALERT_ID$|$IV_ATTACK_COUNT|$|$IV_VLAN_ID$|$IV_LAYER_7_DATA$|$IV_VLAN_ID$|
$IV_PROTECTION_CATEGORY$|$IV_SOURCE_VM_NAME$|$IV_TARGET_VM_NAME$|$IV_SOURCE_VM_ESX_NAME$|
$IV_TARGET_VM_ESX_NAME$|$IV_PROXY_SERVER_IP$|
```

Make sure there are no newline characters entered in that field.

8 Click **Save**.

Configure McAfee Network Security Manager 6.x.x

Task

1 Log on to the management interface as an administrator.

2 Click the **Configure** icon on the dashboard.

3 In the resource tree, click the **root node** (usually **My Company**).

4 Select **Alert Notification** | **Syslog Forwarder**.

5 Change these settings, then click **Save**:

- Enable Syslog Forwarder: **Yes**
- Host IP Address/Hostname: **Enter the IP/Hostname of your Receiver**
- Port: **514**
- With severity level: **Informational and above**

6 Click **Edit**.

7 Insert this text into the **Message** field:

```
|$IV_SENSOR_ALERT_UUID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"|$IV_ATTACK_ID
$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|
$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|
$IV_DESTINATION_PORT$|$IV_CATEGORY$|$IV_SUB_CATEGORY$|$IV_DIRECTION$|$IV_RESULT_STATUS$|
$IV_DETECTION_MECHANISM$|$IV_APPLICATION_PROTOCOL$|$IV_NETWORK_PROTOCOL$|$IV_RELEVANCE$|
$IV_QUARANTINE_END_TIME$|$IV_MCAFEE_NAC_FORWARDED_STATUS$|$IV_MCAFEE_NAC_MANAGED_STATUS$|
$IV_MCAFEE_NAC_ERROR_STATUS$|$IV_MCAFEE_NAC_ACTION_STATUS$|$IV_SENSOR_CLUSTER_MEMBER$|
$IV_ALERT_ID$|$IV_ATTACK_COUNT$|$IV_VLAN_ID$|$IV_LAYER_7_DATA$|$IV_VLAN_ID$|
$IV_PROTECTION_CATEGORY$|$IV_SOURCE_VM_NAME$|$IV_TARGET_VM_NAME$|$IV_SOURCE_VM_ESX_NAME$|
$IV_TARGET_VM_ESX_NAME$|$IV_PROXY_SERVER_IP$|
```

Make sure there are no newline characters entered into that field.

8 Click **Save**.

Add McAfee Network Security Manager (syslog delivery)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	McAfee Network Security
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent

McAfee Network Security Manager (syslog) events to McAfee fields

Log format

The expected format for this device is:

```
<SyslogForarderType>:|SENSOR_ALERT_UUID|ALERT_TYPE|ATTACK_TIME|ATTACK_NAME|ATTACK_ID|
ATTACK_SEVERITY|ATTACK_SIGNATURE|ATTACK_CONFIDENCE|ADMIN_DOMAIN|SENSOR_NAME|INTERFACE|
SOURCE_IP|SOURCE_PORT|DESTINATION_IP|DESTINATION_PORT|CATEGORY|SUB_CATEGORY|DIRECTION|
RESULT_STATUS|DETECTION_MECHANISM|APPLICATION_PROTOCOL|NETWORK_PROTOCOL|RELEVANCE|
QUARANTINE_END_TIME|MCAFEE_NAC_FORWARDED_STATUS|MCAFEE_NAC_MANAGED_STATUS|
MCAFEE_NAC_ERROR_STATUS|MCAFEE_NAC_ACTION_STATUS|SENSOR_CLUSTER_MEMBER|ALERT_ID|ATTACK_COUNT|
VLAN_ID|LAYER_7_DATA|VLAN_ID|PROTECTION_CATEGORY|SOURCE_VM_NAME|TARGET_VM_NAME|
SOURCE_VM_ESX_NAME|TARGET_VM_ESX_NAME|PROXY_SERVER_IP|
```

Log sample

This is a sample log from a McAfee Network Security Manager device:

```
Oct  14 10:24:36 SyslogAlertForwarder: |1234567891234567891|Signature|2014-10-14 10:24:32
EST|"P2P: BitTorrent Meta-Info Retrieving"|0x32c020a0|Medium|catch-most|Low|Exmaple|
SENSR600A|3A-3B|123.234.128.64|24680|64.65.66.67|42356|PolicyViolation|
restricted-application|Inbound|Blocked|signature|N/A|udp|
```

Mappings

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

Log fields	McAfee ESM fields
ATTACK_TIME	firsttime, lasttime
ATTACK_NAME	Message
ATTACK_ID	Signature ID
ATTACK_SEVERITY	Severity
ADMIN_DOMAIN	Domain

Log fields	McAfee ESM fields
SENSOR_NAME	Hostname
INTERFACE	Interface
SOURCE_IP	Source IP
SOURCE_PORT	Source Port
DESTINATION_IP	Destination IP
DESTINATION_PORT	Destination Port
CATEGORY	Category
SUB_CATEGORY	Application
DIRECTION	Direction
RESULT_STATUS	Action
NETWORK_PROTOCOL	Protocol

Configure McAfee Network Security Manager 6.x.x or later (SQL pull)

Before setting up an NSM data source, you need to run the NSM-SEIM Configuration Tool as described here.

Once the configuration tool is run, you can set up the data source on the ESM.

Task

1. Download the configuration tool.
   a. Browse to the **McAfee Product Download** website.
   b. Enter the **customer grant number** that was provided to you in the **Download My Products** search box.
   c. Click **Search**. The product update files are located under the **MFE** | **product name** | **version** | **downloads** link.
   d. View the *Read the McAfee EULA* and agree to its terms before proceeding.
   e. Download the NSM-SEIMConfigurationTool files.
2. Run the NSM-SEIM Configuration Tool on the NSM server. The tool finds the default path to the NSM. If it does not locate it, browse to its location.
3. Enter the NSM SQL user, password, and database name that you entered for the installation of the NSM.
4. Enter the SEIM user name and password to be used on the data source and McAfee Event Receiver IP address where the data source is added. These are entered on the data source screen.

Add McAfee Network Security Manager to a device (SQL pull)

After successfully logging on to the McAfee ESM console, the data source needs to be added to a device in the ESM hierarchy:

Task

1. In the System Navigation Tree, select the **Local ESM node** or a group where you want to add the device.
2. Click the **Add Device** icon.
3. Select **Network Security Manager (v7.1.3 or newer)**, then click **Next**.
4. Enter a name that is unique in this group for the NSM device in the **Device Name** field, then click **Next**.
5. In the **Add Device Wizard**, select the McAfee Event Receiver to associate this device with.

6 Enter the credentials to log on to the NSM device's web interface/API, then click **Next**.

7 Enter the target IP address or URL.

8 Enter the target SSH port number. Ensure that it is valid to be used with the specified IP address.

9 Add the user name, password, and an optional database name for the device.

10 Click **Next**. The ESM tests device communication and reports on the status of the connection. You can open **System Properties** after successfully keying the device.

Add McAfee Network Security Manager (SQL pull)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	McAfee
Data Source Model	Network Security Manager – SQL Pull (ASP)
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
User Name	< User name set up on NSM for pulling from the database >
Password	< Password set up on NSM for pulling from the database>
Port	<Default is 3306>
Database Name	<Database name set up in the Configuration Tool>
Version	<Version of NSM>

McAfee Network Security Manager (SQL pull) events to McAfee fields

Log format

The expected format for this device is:

```
 creationTime=" date time " alertType="…" category="…" subCategory="…" detectionMethod="…"
attackId=" # " attackName="…" severity=" # " alertCount=" # " sourceIPAddr="…" sourcePort="
# " targetIPAddr="…" targetPort=" # " sourceUserId="…" destinationUserId="…"
```

Log sample

This is a sample of a log from the McAfee Network Security Manager device after SQL pull.

```
creationTime="2012-06-22 19:37:01" alertType="Signature" category="Exploit"
subCategory="Buffer Overflow" detectionMethod="Signature" attackId="4255775"
```

```
attackName="IRC: mIRC Userhost Buffer Overflow" severity="7" alertCount="1"
sourceIPAddr="6FA2A653" sourcePort="6667" targetIPAddr="550D1EC1" targetPort="1041"
sourceUserId="0" destinationUserId="0"
```

Mappings

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

Log fields	McAfee ESM fields
creationTime	firsttime, lasttime
alerttype	Object Type
category + subcategory	Subject
detectionMethod	Method
attackId	Signature ID
attackName	Message (smart learned if unknown)
severity	severity plus a zero appended
alertCount	Event Count
sourceIPAddr	Source IP
sourcePort	Source Port
targetIPAddr	Destination IP
targetPort	Destination Port
sourceUserId	Source Username
destinationUserId	Destination Username
result	Action
appName	Application

McAfee Network Threat Response

Contents

Configure McAfee Network Threat Response

Task

- A McAfee Network Threat Response API user name and password must be generated on the Network Threat Response Device. See the Network Threat Response documentation for instructions about how to set up the user name and password.

Add McAfee Network Threat Response

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**McAfee**
Data Source Model	**Network Threat Response (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
User ID	This is the user name generated in step 3.1.
Password	Password that was generated in step 3.1.
Sensor Groups	Click **Retrieve** to get a list of sensor groups from NTR. Select at least one sensor group to write out the data source.
Port	Leave as default of 8443.
Connect	Tests connection to data source.
Time Zone	Time zone of data being collected.

Associate sensor groups with McAfee Network Threat Response

After adding an NTR data source, you can add, edit, or remove sensor groups.

Task

1 Navigate to **Receiver Properties**.

2 Select the NTR data source.

3 Click **Clients**.

From this screen you can see the sensor groups associated with the NTR data source as well as add, edit, or remove them.

McAfee Network Threat Response events to McAfee fields

Mappings

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

NTR log fields	McAfee ESM fields
Eventtime	Firsttime
Eventtime	Lasttime
Sip	Source IP
Dip	Destination IP
Dport	Destination Port
Protocol	Application_Protocol
incidentId	Incident_ID
Filename	Filename
Size	File_Size
Host	Hostname
Behavior	Object
victimIP	Victim_IP
attackerIP	Attacker_IP
url	URL
incidentNTRURL	Device_URL
Reputation	Reputation_Name
Urlcategory	URL_Category
Enginelist	Engine_List
Dirtiness	Reputation_Name
fileType	File_Type
Sigcategory	Category
Sha1	Sha1
Md5	File_Hash
Incidentid	Incident_ID
Hostname	hostname
Sport	Source Port

McAfee Next Generation Firewall

Contents

Configure McAfee Next Generation Firewall

Task

1 Select **Monitoring** | **System Status**.

2 Expand the **Servers** branch.

3 Right-click the Log Server from which you want to forward log data, and select **Properties** to open the Log Server Properties.

4 Switch to the **Log Forwarding** tab.

5 Click **Add** to create a Log Forwarding rule. A new row is added to the table.

6 Configure the Log Forwarding rule to point to your McAfee ESM. Make sure that **Format** is set to **McAfee ESM**.

7 Click **OK**.

Add McAfee Next Generation Firewall

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**McAfee**
Data Source Model	**Next Generation Firewall – Stonesoft (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

McAfee Next Generation Firewall events to McAfee fields

Log sample

This is a sample log from a McAfee Next Generation Firewall (Stonesoft) device:

```
Timestamp="2013-11-21 00:00:00",LogId="1615132411",NodeId="10.1.0.2",Facility="Cluster
protocol",Type="Diagnostic",Event="Cluster protocol event",CompId="148",InfoMsg="p0 load: 3
(passed: 1111111 netload_factor: 2  all: 2222222 p: 19",ReceptionTime="2013-11-21
00:00:00",SenderType="Firewall",SituationId="2011",Situation="System_Cluster-Protocol-Event",
EventId="5809198281527719675"
```

Mappings

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

Log fields	McAfee ESM fields
ReceptionTime	firsttime/lasttime
NodeId	Device_IP.Device_IP
Facility	application
Type/AlertSeverity	severity
Situation/Event/SenderType : Facility	message
Action	action
Src	src_ip
Dst	dst_ip
Protocol	protocol
SrcPort/IcmpType	src_port
DstPort/IcmpCode	dst_port
SrcIF	Interface.Interface
AccTxBytes	Bytes_Sent.Bytes_Sent
AccRxBytes	Bytes_Received.Bytes_Received
Username/AuthName	src_username
Sendertype	objectname
Situation	sid

McAfee Risk Advisor

Contents

Integrate McAfee Risk Advisor

You can get McAfee Risk Advisor data from multiple McAfee ePO servers.

The data comes via a database query from the McAfee ePO SQL Server database. The database query returns an IP address reputation score list. Constant values for the low reputation and high reputation values are provided. All returned McAfee ePO and McAfee Risk Advisor reputation lists are merged in ESM, with duplicate IP addresses retaining the highest score. The merged reputation list is sent to McAfee ACE devices and used in scoring risk for **Source IP** and **Destination IP** fields.

When you add McAfee ePO to ESM, you are prompted to configure McAfee Risk Advisor data. When you click **Yes**, a data enrichment source and two ACE scoring rules (if applicable) are created and added to the policy.

For more information, see *Data Enrichment* and *Risk Correlation Scoring* in the *McAfee Enterprise Security Manager Product Guide*.

A risk correlation manager must be created to use the ACE scoring rules.

Enable McAfee Risk Advisor data acquisition

Task

1 From the ESM device tree, select the McAfee ePO device, then click the **Properties** icon just above the device tree.

2 Select **Device Management** from the left side of the **ePO Properties** window, then click **Enable** for **Enable MRA**.

A window shows that the MRA configuration process started, which means that MRA acquisition is enabled.

3 Click **OK**.

McAfee UTM Firewall

Contents

Configure McAfee UTM Firewall

Task

1 From the System menu, select **Diagnostics | System Log tab | Remote Syslog** tab.

2 Select **Enable Remote Logging**.

3 Enter the IP address or DNS host name for the McAfee Event Receiver in the **Remote Host** field.

4 Enter the **Remote Port** where the McAfee Event Receiver is listening for syslog messages. Typically, the default is **correct**.

5 Set the **Filter Level** to only send syslog messages at this level or higher.

6 (Optional) To force a more precise and standardized time stamp with every message, select **Include extended ISO date**. The date is prepended to syslog messages before being sent.

7 Click **Submit**.

Add McAfee UTM Firewall

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**McAfee**
Data Source Model	**UTM Firewall (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**Default**
Require Syslog TLS	Leave unchecked
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

McAfee UTM Firewall events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a McAfee UTM Firewall device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

Threat Intelligence Exchange

Contents

Integrate Threat Intelligence Exchange

Threat Intelligence Exchange (TIE) verifies the reputation of executable programs on endpoints. When Threat Intelligence Exchange events are generated in ESM, you can view their execution history and select which actions to take on the malicious data.

When a McAfee ePO device is added to the ESM, the ESM automatically checks for the presence of a TIE server. If one is present, the ESM begins listening and retrieving events from the Data Exchange Layer (DXL) (see Add McAfee ePolicy Orchestrator as a device on page 37).

When the TIE server is detected, these configurations are automatically added:

- TIE Watchlists
- TIEData Enrichment
- TIE Correlation Rules
- TIE Alarms

After configuration, ESM receives a visual notification, which includes a link to the summary of the changes.

A notification window appears if a TIE server is added to the McAfee ePO server after the device was added to the ESM.

TIE alarms

The ESM has two alarms that trigger when important Threat Intelligence Exchange events are detected.

- **TIE bad file threshold exceeded** triggers from the correlation rule, **TIE - Malicious file (SHA-1) found on increasing number of hosts**.
- **TIE unknown file executed** triggers from a specific TIE event and adds information to the **TIE data source IPs** watchlist.

TIE Content Pack

The TIE Content Pack is an optional installation that includes additional components to help in viewing and accessing TIE information based on events from correlation rules, alarms, reports, watchlists, and parsed log data.

This Content Pack includes some components that are automatically included on the discovery of a TIE server.

These additional components are included with the installation of the TIE Content Pack:

Correlation Rules

- TIE - GTI Reputation Changed from Dirty to Clean
- TIE - TIE Reputation Changed from Dirty to Clean

Views

- TIE View
- TIE Malicious File Watchlist View

Report

- TIE – Daily Overview

Watchlist

- TIE – Malicious Files Found

For details about this content pack, see KB84533.

TIE correlation rules

Six correlation rules are optimized for Threat Intelligence Exchange data, and are automatically added to a policy when TIE is detected.

- TIE - GTI reputation changed from clean to dirty
- TIE - Malicious file (SHA-1) found on increasing number of hosts
- TIE - Malicious file name found on increasing number of hosts
- TIE - Multiple malicious files found on single host
- TIE - TIE reputation changed from clean to dirty
- TIE - Increase in malicious files found across all hosts

TIE file execution history

Endpoint file execution history, reported as a list of IP addresses that have tried to execute a file, can be viewed for any TIE event.

You can select an applicable item in the ESM, then apply any of these actions:

- Create a watchlist.
- Add the information to a blacklist.
- Append the information to a watchlist.
- Export the information to a .csv file.
- Create an alarm.

TIE watchlist

The **TIE data source IPs** watchlist is added automatically in ESM, and maintains a list of systems that have triggered the **TIE unknown file executed** alarm.

The **TIE data source IPs** watchlist is a static watchlist with no expiration.

View TIE file execution history and set up actions

The Threat Intelligence Exchange execution history page displays a list of systems that have executed the file associated with the event selected in the ESM.

Before continuing, verify that a McAfee ePO device with an attached Threat Intelligence Exchange server is added to the ESM.

Task

1. From the ESM device tree, select the McAfee ePO device.
2. On the views drop-down list, select **Event Views** | **Event Analysis**.
3. Click the menu icon from a view component in ESM, then select **Actions** | **TIE Execution History**.
4. On the **TIE Execution History** page, view a list of the systems that have executed the file from the selected event.
5. To add this data to a workflow, click a system, click the **Actions** drop-down menu, then select an option to open its ESM page.
6. Set up the selected action (see the online Help for instructions).

4 Configuring 3rd-party data sources

Contents

- *CyberArk Enterprise Password Vault*
- *CyberArk Privileged Identity Management Suite (CEF)*
- *CyberArk Privileged Threat Analytics*
- *Damballa Failsafe*
- *Dell Aventail*
- *Dell PowerConnect Switches*
- *Dell SonicOS*
- *DG Technology - InfoSec MEAS*
- *Econet Sentinel IPS*
- *EdgeWave iPrism Web Security*
- *Enforcive Cross-Platform Audit*
- *Entrust IdentityGuard*
- *Extreme Networks ExtremeWare XOS*
- *F5 Networks FirePass SSL VPN*
- *F5 Networks Local Traffic Manager*
- *Fidelis XPS*
- *FireEye Malware Protection System*
- *Fluke Networks AirMagnet Enterprise*
- *Force10 Networks FTOS*
- *Forcepoint Websense*
- *ForeScout CounterACT*
- *Fortinet FortiGate*
- *Fortinet FortiMail*
- *Fortinet FortiManager*
- *Fortscale User and Entity Behavior Analytics (UEBA)*
- *FreeRADIUS*
- *Gigamon GigaVUE*
- *Globalscape Enhanced File Transfer*
- *HBGary Active Defense*
- *Hewlett-Packard 3Com Switches*
- *Hewlett Packard LaserJet Printers*
- *Hewlett-Packard ProCurve*
- *HyTrust Appliance*
- *IBM*
- *Infoblox NIOS*
- *InterSect Alliance Snare for Windows*
- *Interset*
- *Juniper Networks JUNOS Structured-Data Format*
- *Juniper Networks NetScreen*
- *Juniper Networks Network and Security Manager*
- *Kaspersky Administration Kit*
- *Lastline Enterprise*
- *Locum RealTime Monitor*
- *LOGbinder*
- *Lumension Bouncer*
- *Lumension LEMSS*
- *Malwarebytes Breach Remediation*
- *Malwarebytes Management Console*
- *Microsoft DNS*
- *Microsoft Forefront Endpoint Protection 2010*
- *Microsoft Internet Authentication Service (IAS)*
- *Microsoft Internet Information Services (IIS)*

- *Microsoft Network Policy Server (NPS)*
- *Microsoft Office 365*
- *Microsoft Windows DHCP*
- *Microsoft Windows Event Log WMI*
- *Motorola AirDefense*
- *NetFort Technologies LANGuardian*
- *NetWitness Spectrum*
- *Niara*
- *Nortel Networks Contivity*
- *Nortel Networks Passport 8000 Series Switches*
- *Novell eDirectory*
- *Novell Identity and Access Management*
- *Oracle Audit (SQL)*
- *Oracle Audit (syslog)*
- *Oracle Audit (XML)*
- *Oracle Unified Auditing (SQL)*
- *Oracle Internet Directory Server*
- *Palo Alto Networks PAN-OS*
- *PhishMe Intelligence*
- *PhishMe Triage*
- *Proofpoint Messaging Security Gateway*
- *Raytheon SureView*
- *Raz-Lee Security iSecurity Suite*
- *Red Hat JBoss Application Server/WildFly 8*
- *RedSeal Networks RedSeal 6*
- *ReversingLabs N1000 Network Security Appliance*
- *RioRey DDOS Protection*
- *Riverbed Steelhead*
- *RSA Authentication*
- *SafeNet Hardware Security Modules*
- *Skycure Enterprise*
- *Skyhigh Networks Cloud Security Platform*
- *Sophos Web Security and Control*
- *Sourcefire FireSIGHT Management Console*
- *SSH Communications Security CryptoAuditor*
- *STEALTHbits StealthINTERCEPT*
- *Symantec Data Loss Prevention*
- *Symantec Endpoint Protection*
- *Symantec Messaging Gateway*
- *Symantec PGP Universal Server*
- *Symantec Web Gateway*
- *ThreatConnect Threat Intelligence Platform*
- *TippingPoint SMS*
- *Tofino Firewall LSM*
- *Topia Technology Skoot*
- *TrapX Security DeceptionGrid*
- *Trend Micro Deep Security*
- *Trend Micro Deep Security Manager*
- *Trend Micro OfficeScan*
- *Trustwave Data Loss Prevention*
- *Trustwave Network Access Control*
- *Type80 Security Software SMA_RT*

A10 Networks Load Balancer

Contents

Configure A10 Networks Load Balancer

Task

1 Log on to the A10 Networks Load Balancer user interface (UI), then select **Config** | **System** | **Settings**.

2 In the menu bar, select **Log**, then, in the **Log Server** field, enter the IP address of your McAfee Event Receiver.

3 Ensure that **Log Server Port** is set to **514**, and leave all other settings at their default values.

4 Click **OK**.

Configure A10 Networks Load Balancer from the command line

Task

1 Log on to the command-line interface (CLI).

2 Type:

```
logging syslog 5
logging host IP address of McAfee Receiver port 514
```

Add A10 Networks Load Balancer

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	A10 Networks
Data Source Model	Load Balancer
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source.
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Default>
Mask	<Enable>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

A10 Networks Load Balancer events to ESM fields

Log format

The expected format for this device is:

```
SYSLOG Header [log source] message
```

ESM supports only standard logs from this device. However, custom logs generated by the AFLEX engine are not supported. Custom rules for this product can be created in the ESM, but how to create them is outside of the scope of this documentation.

Log sample

This is a sample log from an A10 Networks AX series load balancer device:

System log:

```
Oct 24 2014 01:02:03                    Error [SYSTEM]NTP server us.pool.ntp.org is not
reachable
```

AX log:

```
Oct 24 2014 04:05:06                    Error [AX] Unknown gzip error while decompressing
packet
```

Logging log:

```
Oct 24 2014 07:08:09                    Error [LOGGING]Send log email to
test.user@example.com failed.
```

Alternate delivery method:

```
<13>a10logd: [SYSTEM]<6> User "admin" with session ID 1 successfully saved the running
configuration
```

Mappings

This table shows the mappings between the data source and ESM fields.

Pre 9.2.0:

Log fields	ESM fields
Log Source	Application
Server Name	Domain
SLB server, NTP Server	Hostname
Error Type, Group Name, change	Object Name
Email "To" address	Destination Username
User	Source Username

9.2.0 and later:

Log fields	ESM fields
Log Source	Application
Server Name	Domain
SLB server, NTP Server	Hostname
Error Type, change	Object Name
Email "To" address	Destination Username
User	Source Username
Group Name	Group Name

A10 Networks Load Balancer troubleshooting

Standard logs from this device are supported by this data source, but custom logs generated by the AFLEX engine are not supported. Custom rules for this product can be created in the ESM, but that is outside of the scope of this documentation.

Accellion Secure File Transfer

Contents

Configure Accellion Secure File Transfer

Task

1 From the **Home** menu, select **Appliance**, then click **Configure**.

2 In the **Syslog Server** field, enter the IP address of the McAfee ESM, then click **Submit** to save and exit.

Add Accellion Secure File Transfer

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Accellion
Data Source Model	Secure File Transfer (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the McAfee Event Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent

Accellion Secure File Transfer events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device name> <application> <IP address> <user> <message> <destination user>
```

Log sample

This is a sample log from an Accellion Secure File Transfer device:

```
<123>1 2001-01-01T01:01:01-01:00 name0001 httpd - - - [12345]: (1.2.3.4) (User:username)
[Web] Sent password reset request to ldap user, user_id:example@example.com
```

Mappings

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

Log fields	McAfee ESM fields
Device Name	Hostname
Application	Application
IP Address	Source IP
User	Source Username
Destination User	Destination Username
Filename	Filename
From email	From
To email	To
Email subject	Subject

Access Layers Portnox

Contents

Configure Access Layers Portnox

See the Portnox documentation provided by Access Layers for information about how to set up the remote syslog service to send data to the ESM.

Add Access Layers Portnox

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Access Layers**
Data Source Model	**Portnox**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

Access Layers Portnox events to McAfee fields

Log format

The expected format for this device is:

```
date time,message
```

Log sample

This is a sample log from an Access Layers Portnox device:

```
01/01/2001 00:00:00,recieved trap from unauthorized source 192.0.2.1
```

Mappings

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

Log fields	McAfee ESM fields
Date, Time	First Time, Last Time
device IP, switch IP, trap device	Source IP
device mac, duplicate mac	Source MAC
received IP	Destination IP
device	Hostname
device action, port action	Command
port name	Object

Adtran Bluesocket

Contents

Configure Adtran Bluesocket

Task

1 Click **Logging**, select **Event History**, then click **Syslog Forwarding**.

2 Select the box next to **Syslog Forwarding**, then select the **Syslog Forwarding Priority Level**.

3 In the **Syslog Receiver IP Address** field, enter the IP address of your McAfee Event Receiver.

4 Pick a **Logging Facility** number between 0 and 9 (your preference), click **Apply**, then click **Save**.

Add Adtran Bluesocket

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Adtran**
Data Source Model	**Bluesocket (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**<Default>**
Time Zone	Time zone of data being sent.

AdTran Bluesocket events to McAfee fields

Log format

The expected format for this device is:

```
<pri>log_source:
event=event_type&loglevel=severity&obj=object&ipaddr=source_ip&name=name&msg=message&
```

Log sample

This is a sample log for an Adtran Bluesocket device:

```
<133>user_tracking:
event=user_logout_successful&loglevel=notice&obj=user&ipaddr=192.0.2.0&name=NAME3215&msg=user
: NAME213, role id: #, role name: Public-Access, vlan id: #, vlan name: Managed, mac:
FF:FF:FF:FF:FF:FF, ip: 192.0.2.1, hostname: , login time: 2015-01-01 00:00:00, session
duration: # hour, # minutes, ## seconds, sessionID: 00:11:22:33:44:FF:0000001111112222, tl.
bytes in:9999999, tl. bytes out: 99999999, tl. pkts in: 99999, tl. pkts out: 99999&
```

Mappings

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

Log fields	McAfee ESM fields
event	Event Subtype, Messsage
loglevel	Severity
obj	Object
ipaddr	Source IP
mac	Source MAC
session duration	Message_Text
log_source	Application
role id	Command
role name	Domain
login time	First Time, Last Time
name	Source Username
hostname	Hostname

Adtran NetVanta

Contents

Configure Adtran NetVanta

Task

1 Log on to your Adtran NetVanta device through a web browser, then click **Logging**.

2 Select the **Event History** checkbox, click the **Syslog Forwarding** tab, then select the **Syslog Forwarding** checkbox.

3 Select a **Syslog Forwarding Priority Level** between 0 and 5, with 0 reporting the most and 5 reporting only the most important events.

4 Enter the **McAfee Receiver** IP address in the **Syslog Receiver IP Address** section.

5 For the **Logging Facility**, enter a number between 0 and 9, then click **Save**.

Add Adtran NetVanta

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Adtran**
Data Source Model	**NetVanta**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

Adtran NetVanta events to McAfee fields

Log format

The expected format for this device is:

```
Date Time Device-Type Event-Source:Message
```

Log sample

This is a sample log from an Adtran NetVanta device:

```
<13>Dec 02 14:03:35 Switch OPERATING_SYSTEM:SESSION User password-only login OK on portal
TELNET 1 (10.19.243.125:2230)
```

Mappings

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

Log fields	McAfee ESM fields
portal, proto	Application
Portal IP, src	Source IP
Portal Port, Src	Source Port
dst	Destination IP
Dst	Destination Port
Device-Type	Hostname
Session ID	Session ID
Interface	Object
User	Source Username

AirTight Networks SpectraGuard

Contents

Configure AirTight Networks SpectraGuard

See the AirTight Networks SpectraGuard documentation for Remote Syslog setup using the IP address of your McAfee Event Receiver as the destination IP address.

Add AirTight Networks SpectraGuard

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	AirTight Networks
Data Source Model	SpectraGuard
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

AirTight Networks SpectraGuard events to McAfee fields

Log format

```
<Source Mac Address>SpectraGuard Version : Start/Stop: Source [SourceName] Source Status. :
Source IP://Domain/SubDomain : Date/Time : Severity : Message
```

Log sample

This is a sample log from an AirTight Networks SpectraGuard device:

```
<00:00:00:FF:FF:FF>SpectraGuard Enterprise v6.5 : Start: Client [Username] is active. :
192.0.2.1://AAAA/BBBBB: 2001-01-01T00:00:00+00:00 : High : 100 : 1 : 11 : 111: Closest
Sensor [AP1.5 Sensor-Examination & Certification-207]
```

Mappings

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

Log fields	McAfee ESM fields
Severity	Severity
Source Mac Address	Source MAC
Start/Stop	Event Sub Type
SourceName	Hostname
Domain	Domain
Source IP	Source IP
Date/Time	First Time, Last Time
SubDomain	Object

Alcatel-Lucent NGN Switch

Contents

Configure Alcatel-Lucent NGN Switch

Task

- To configure a syslog file, enter these commands on the command line:
  - `syslog <syslog-id>`
  - `description <description-string>`
  - `address <ip-address>`
  - `log-prefix log-prefix-string`
  - `port <port #>`
  - `level {emergency|alert|critical|error|warning|notice|inf|debug}`
  - `facility <syslog-facility>`

  The following is a syslog configuration example:

```
syslog 1
description "This is a syslog file."
address x.x.x.x
facility user
level warning
exit
```

Add Alcatel-Lucent NGN Switch

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Alcatel-Lucent**
Data Source Model	**NGN Switch (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do Nothing**
Time Zone	Time zone of data being sent.

Alcatel-Lucent NGN Switch events to McAfee fields

Log format

Thu Jun 13 03:39:36 MNT 2013::AUTHENTICATION::JohnSmith::
1371074976970::10.10.10.15(10.10.10.15:64575):::Attempt to log in:::Failed, no such user.

Mappings

Mappings using the provided log example.

Log fields	McAfee ESM fields
Category	AUTHENTICATION
Source User	JohnSmith
Source IP	10.10.10.15
Destination	64575

Alcatel-Lucent VitalQIP

Contents

Configure Alcatel-Lucent VitalQIP

Task

1 Log on to your Alcatel-Lucent VitalQIP device.

2 In the system configuration, set the IP address of your McAfee Event Receiver as a **Syslog Redirect Host**, then save your changes.

Add Alcatel-Lucent VitalQIP

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Alcatel-Lucent**
Data Source Model	**VitalQIP**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

Alcatel-Lucent VitalQIP events to McAfee fields

Log format

The expected format for this device is:

```
<pri>application[pid]: message
```

Log sample

This is a sample log from an Alcatel-Lucent VitalQIP device:

```
<14>/opt/qip/usr/bin/dhcpd[12345]: DHCP_RenewLease: Host=EXAMPLEHOST IP=10.11.12.13
MAC=0011223344AA Domain=example.com
```

Mappings

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

Log fields	McAfee ESM fields
Subnet, IP	Source IP
MAC	Source MAC
Host	Hostname
Domain	Domain

Amazon CloudTrail

Contents

Configure Amazon CloudTrail

Amazon Web Services (AWS) CloudTrail can send a notification each time a log file is written to the Amazon S3 bucket. AWS recommends using Amazon Simple Queue Service (SQS) to subscribe to event notifications for programmatically processing notifications. To receive timely notifications in ESM for new Amazon CloudTrail logs, configure an SQS queue on AWS that contains Simple Notification Service (SNS) push notifications when new log bundles are created in S3.

See Amazon documentation for details.

Add Amazon CloudTrail

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Amazon**
Data Source Model	**CloudTrail**
Data Format	**Default**
Data Retrieval	**API (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
AWS Access Key	The user name used to log on to AWS.
AWS Secret Key	The password used to log on to AWS.
SQS URL	The URL that points to the SQS queue provided by AWS.
SQS Visibility	The time that a message (log) stays hidden after it is requested. If the message is not deleted by the collector, it is restored after the timeout (default is 300 seconds).
SQS Poll Interval	The interval between collection requests (default is 300 seconds).
Connect	Performs a test connection to the AWS services. Make sure that this test runs successfully before moving on. If errors exist, collection might not work properly.

Amazon CloudTrail events to McAfee fields

Log sample

This is a sample log from an Amazon CloudTrail device:


```
{"Records": [{"awsRegion": "us-west-2","eventID":
"12ab34cd-f4d2-4222-ad86-ad4841234fed","eventName": "DescribeTags","eventSource":
"ec2.amazonaws.com","eventTime": "2015-06-20T11:26:18Z","eventType":
"AwsApiCall","eventVersion": "1.02","recipientAccountId": "12345","requestID":
"b3b56ade-2321-222e-9b4e-e7d30b142916","requestParameters": {"filterSet": {"items":
[{"name": "resource-type","valueSet": {"items": [{"value": "instance"}]}},{"name":
"key","valueSet": {"items": [{"value": "Name"}]}}]}},"responseElements":
null,"sourceIPAddress": "10.0.0.1","userAgent": "aws-sdk-java/1.9.8 Linux/
3.9.5-301.fc19.x86_64 Java_HotSpot(TM)_64-Bit_Server_VM/
20.13-b02/1.6.0_38-ea","userIdentity": {"accessKeyId": "ABC123","accountId": "12345","arn":
"arn:aws:iam::12345:user/someUserName","principalId": "principalID","type":
"IAMUser","userName": "someUserName"}}]}
```


Mappings

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

Log fields	McAfee ESM fields
awsRegion	Source_Zone
eventName	Message
eventTime	First Time, Last Time
userAgent	User_Agent
userIdentity/userName	Source User

Log fields	McAfee ESM fields
eventSource	Service_Name
sourceIPAddress	Source User, Host
requestId	Source GUID
eventID	Dest. GUID
eventType	Category
userIdentity/accountId	Source_UserID
recipientAccountId	Destination_UserID

Apple Mac OS X

Contents

Configure Apple Mac OS X

The syslog configuration is done on the command line. See your Apple Mac OS X product documentation for instructions on how to access and use the Terminal program.

Task

1 Open the Terminal program, then make a backup of the syslog.conf file:

```
$ cp /etc/syslog.conf /tmp/syslog.conf.bkp
```

2 Open the configuration file in a text editor, for example, `vi`:

```
$ sudo vi /etc/syslog.conf
```

3 Insert this line at the end of the syslog.conf file:

```
*.*  @x.x.x.x
```

where `x.x.x.x` is the IP address of your McAfee Event Receiver.

A port can also be specified by adding `:x` to the end of the IP address, where `x` is the port number. If no port is specified, default port 514 is used.

The line consists of a wildcard statement (`*.*`) and an action (`@x.x.x.x`) separated by tabs. It tells the syslog daemon to forward a copy of all (`*.*`) events to the specified IP address.

4 Click **Save**, click **Exit**, then restart the syslogd service with these two commands:

```
$ sudo launchctl unload /System/Library/LaunchDaemons/com.apple.syslogd.plist
```

```
$ sudo launchctl load /System/Library/LaunchDaemons/com.apple.syslogd.plist
```

5 Verify that the service is running:

```
$ ps -e | grep syslogd
```

Add Apple Mac OS X

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Apple Inc.
Data Source Model	Mac OS X (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent

Apple Mac OS X events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <hostname> <service> <message>
```

Log sample

Here is a sample log from an Apple Mac OS X device:

```
Jan 01 01:01:01 Example-Mac-mini.local com.apple.backupd[1234]: Backup completed
successfully.
```

Mappings

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

Log fields	McAfee ESM fields
Username	Source Username
“Run as” username (usually root)	Destination Username
IP Address	Source IP

Log fields	McAfee ESM fields
Remote IP Address	Destination IP
Port	Source Port
Service / Daemon	Application

Arbor Networks Pravail

Contents

Configure Arbor Networks Pravail

Refer to the Arbor Networks Pravail 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.

Add Arbor Networks Pravail

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Arbor Networks**
Data Source Model	**Pravail**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent.

Arbor Networks Pravail events to McAfee fields

Log format

The expected format for this device is:

```
Date Time Application: action Source IP Detection Type protocol/port (application)
destination IP URL: url
```

Log sample

This is a sample log from an Arbor Networks Pravail device:

```
<13>Oct 22 09:49:32 HTX-ARBOR-00 pravail: Blocked Host: Blocked host 192.0.2.1 at 09:49 by
TCP SYN Flood Detection using TCP/445 (MICROSOFT-DS) destination 192.0.2.2,URL: https://
example.com/folder/
```

Mappings

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

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
Action	Event Subtype
Source	Source IP
Destination	Destination IP
Detection Type	Message
Protocol	Protocol
Port	Source Port

ArcSight Common Event Format

Contents

Configure ArcSight Common Event Format

This data source can be used with devices that generate ArcSight Common Event Format (CEF)-formatted events. If McAfee Event Receiver doesn't support a specific vendor and model, this is a useful alternative.

Follow the directions for your vendor to enable ArcSight CEF-formatted events to be delivered to the McAfee Event Receiver. You might need administrative rights.

Add ArcSight Common Event Format

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ArcSight**
Data Source Model	**Common Event Format (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

ArcSight Common Event Format events to McAfee fields

Log format

The expected format for this device is:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
```

```
ID|Name|Severity|Extension
```

The format of the event is consistent, until Extension. At this point, there is no specific order of fields in CEF. The various key value pairs that follow can be arranged in any order based on the decisions of the vendor.

Log sample

This is a sample log from an ArcSight Common Event Format device:

```
2014-04-21T18:35:15.546Z 192.168.2.5 CEF:0|McAfee|ESM|9.4.0|277-2121969963|TCP_NC_MISS|2|
start=1398105379000 end=1398105379000 rt=1398105308000 cnt=1 eventId=4246692
nitroUniqueId=4246692 deviceExternalId=Live BlueCoat ProxySG
deviceTranslatedAddress=192.168.2.22 externalId=202857 cat=Web Policy nitroNormID=941621248
act=success proto=hopopt deviceDirection=0 dst=192.168.2.114 dpt=80 src=192.168.2.16
nitroTrust=2 nitroAppID=nFMAIN nitroObject_Type=Web_Advertisements sntdom=domain.com.tw
nitroMethod=GET duser=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR
1.1.4322; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648)
suser=johnsmith nitroURL=http://domain.com/somepath/index.html nitroQuery_Response=OBSERVED
nitroResponse_Code=200 nitroDevice_IP=192.168.2.11 nitroDevice_Port=8080
```

Mappings

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

Log fields	McAfee ESM fields
Signature ID	Signature ID
Name	Message
act	Event Subtype
dpt	Dest Port
dst	Dest IP
dmac	Dest Mac
cnt	Event Count
proto	Protocol
spt	Source Port
src	Source IP
smac	Source MAC
start	Firsttime
end	Lasttime
severity	Severity
dproc	Application
nitroCommandID	Command
sntdom	Domain
shost	Host
fname, spriv, nitroObjectID	Object
duser	Dest User
suser	Source User

Aruba ClearPass

Contents

Configure Aruba ClearPass

Task

1 Log on to the ClearPass Policy Manager, then navigate to **Administration Menu** | **External Servers** | **Syslog Export Filters**.

2 Copy the contents of Appendix C, paste it into a blank file, and save it as an XML file, for example, McAfee_SIEM_SyslogExportData.xml.

3 Change all instances of the text `change.me.receiver.ip` in the XML file to the IP address of the McAfee Event Receiver.

4 On the **Syslog Export Filters** page, select the **Import** link in the top right area of the page.

5 Click **Browse** to navigate to the XML file that you created.

This file sets up the needed syslog export filters and populates the syslog target IP address.

6 Navigate to the **Syslog Targets** page and verify that the IP address of the McAfee Event Receiver is in the host **Address** field.

See also

Aruba ClearPass Syslog export file contents on page 84

Add Aruba ClearPass

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Aruba**
Data Source Model	**ClearPass**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Aruba ClearPass events to McAfee fields

Log format

The expected format for this device is:

Session Log:

```
CEF.SignatureID CEF.EventName Severity duser dmac dpriv cs2 outcome rt dvc cat
```

Insight Log:

```
CEF.SignatureID CEF.EventName Severity dmac cs6 dst duser cs4 cs5 rt dvc cat
```

Audit Log:

```
 CEF.SignatureID CEF.EventName Severity rt cat duser dvc act
```

System Log:

```
CEF.SignatureID CEF.EventName Severity dvc deviceProcessName outcome rt cat
```

Log sample

This is a sample log from an Aruba ClearPass device:

Session Log:

```
<143>Aug 10 2016 15:18:04 172.20.21.100 CEF:0|Aruba Networks|ClearPass|6.6.1.84176|2006|
Guest Access|1|duser=bob dmac=784b877a4155 dpriv=[User Authenticated] cs2=UNKNOWN
cs2Label=System Posture Token outcome=[Allow Access Profile] rt=Aug 10 2016 15:16:51
dvc=172.20.21.100 cat=Session Logs
```

Insight Log:

```
<143>Aug 11 2016 14:59:50 172.20.21.100 CEF:0|Aruba Networks|ClearPass|6.6.1.84176|1009|
Endpoints|1|dmac=784b877a4155 cs6=Murata Manufacturing Co., Ltd.
cs6Label=Endpoint.MAC-Vendor dst=172.20.21.7 duser=bob cs3=Computer
cs3Label=Endpoint.Device-Category cs4=Linux cs4Label=Endpoint.Device-Family cs5=Linux
Computer cs5Label=Endpoint.Device-Name ArubaClearpassEndpointConflict=f
ArubaClearpassEndpointStatus=Known deviceCustomDate1=Aug 03 2016 14:31:54
deviceCustomDate1Label=Endpoint.Added-At rt=Aug 11 2016 14:56:52 dvc=172.20.21.100
cat=Insight Logs
```

Audit Log:

```
<143>Aug 01 2016 11:16:42 172.20.21.100 CEF:0|Aruba Networks|ClearPass|6.6.1.84176|3002|
Syslog Export Data|2|rt=Aug 01 2016 11:16:32 fname=Intel Radius Authenication cat=Audit
Records duser=admin dvc=172.20.21.100 act=REMOVE
```

System Log:

<

```
143>Aug 23 2016 16:57:39 172.20.21.100 CEF:0|Aruba Networks|ClearPass|6.6.1.84176|4009|
restart|1|dvc=172.20.21.100 deviceProcessName=Policy server outcome=Success rt=Aug 23 2016
16:55:23 cat=ClearPass System Events
```

Mappings

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

Log fields	McAfee ESM fields
deviceProcessName, destinationServiceName	Application
Cleint IP Address, dst, dvc	Source IP
Rt, start	First Time, Last Time
CEF.Severity	Severity
Dmac	Source Mac
Endpoint.MAC-Vendor	Object_Type
ArubaClearpassGuestVistorCompany	Domain
Dvchost	Hostname
requestMethod	Method
Duser	Source User
ArubaClearpassGuestVisitorName	Contact_Nickname
Outcome, reason	Message_Text
Endpoint.Device-Name	External_Device_Name
CEF.SignatureID	External_EventID
Endpoint.Device-Family	External_Device_Type
Cat	Subcategory
Src	Device_IP
Msg, CEF.EventName	Message
CEF.SignarureID	SID
Act, outcome	Action
ArubaClearpassOnbardEnrollmentDeviceVersion	Version
dpriv	Privileges

Aruba ClearPass Syslog export file contents

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Mon Aug 29 15:58:17 MDT 2016" version="6.6"/>
<DataFilter>
<DataFilter description="All Endpoints" name="[Endpoints]" qType="INSIGHT"
conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="" operator="EXISTS" columnName="MAC-Address" scope="Endpoint"/>
</conditionSets>
    </DataFilter>
<DataFilter description="All ClearPass Guest" name="[ClearPass Guest]" qType="INSIGHT"
conditionSetJoinType="OR">
<conditionSets conditionJoinType="OR">
<conditions value="" operator="EXISTS" columnName="Username" scope="Guest"/>
<conditions value="" operator="EXISTS" columnName="MAC-Address" scope="Guest"/>
</conditionSets>
</DataFilter>
<DataFilter description="All ClearPass System Events" name="[ClearPass System Events]"
qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="" operator="EXISTS" columnName="Source" scope="CppmSystemEvent"/>
</conditionSets>
</DataFilter>
<DataFilter description="All ClearPass Configuration Audit" name="[ClearPass Configuration
Audit]" qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
```

```
<conditions value="" operator="EXISTS" columnName="Action" scope="CppmConfigAudit"/>
</conditionSets>
</DataFilter>
<DataFilter description="All RADIUS Authentications " name="[RADIUS Authentications]"
qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="RADIUS" operator="EQUALS" columnName="Protocol" scope="Auth"/>
</conditionSets>
</DataFilter>
<DataFilter description="All RADIUS Failed Authentications" name="[RADIUS Failed
Authentications]" qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="RADIUS" operator="EQUALS" columnName="Protocol" scope="Auth"/>
</conditionSets>
<conditionSets conditionJoinType="AND">
<conditions value="0" operator="NOT_EQUALS" columnName="Error-Code" scope="Auth"/>
</conditionSets>
</DataFilter>
<DataFilter description="All session log requests" name="[All Requests]" qType="SESSION"
conditionSetJoinType="OR">
<conditionSets conditionJoinType="OR">
<conditions value="0" operator="NOT_EQUALS" columnName="Request-Id" scope="Common"/>
</conditionSets>
</DataFilter>
<DataFilter description="All TACACS Authentication " name="[TACACS Authentication]"
qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="" operator="EXISTS" columnName="Username" scope="Tacacs"/>
</conditionSets>
</DataFilter>
<DataFilter description="All TACACS Failed Authentication" name="[TACACS Failed
Authentication]" qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="0" operator="NOT_EQUALS" columnName="Error-Code" scope="Tacacs"/>
</conditionSets>
</DataFilter>
<DataFilter description="All WEBAUTH Authentication " name="[WEBAUTH Authentication]"
qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="WEBAUTH" operator="EQUALS" columnName="Protocol" scope="Auth"/>
</conditionSets>
</DataFilter>
<DataFilter description="All WEBAUTH Failed Authentications " name="[WEBAUTH Failed
Authentications]" qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="WEBAUTH" operator="EQUALS" columnName="Protocol" scope="Auth"/>
</conditionSets>
<conditionSets conditionJoinType="AND">
<conditions value="0" operator="NOT_EQUALS" columnName="Error-Code" scope="Auth"/>
</conditionSets>
</DataFilter>
<DataFilter description="All Application Authentications" name="[Application
Authentication]" qType="INSIGHT" conditionSetJoinType="AND">
<conditionSets conditionJoinType="AND">
<conditions value="Application" operator="EQUALS" columnName="Protocol" scope="Auth"/>
</conditionSets>
</DataFilter>
</DataFilter>
<SyslogTargets>
<SyslogTarget protocol="UDP" port="514" description="McAfee Receiver"
hostAddress="change.me.receiver.ip"/>
</SyslogTargets>
<SyslogExportConfigurations>
<SyslogExportData description="" name="McAfee ESM Application Authenication"
fieldGroupName="Application Authentication" enabled="true" filterName="[Application
Authentication]" exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Auth.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Protocol</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
```

```
<SyslogExportDataColumn>Auth.Login-Status</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Source</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Enforcement-Profiles</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Audit" fieldGroupName="" enabled="true"
exportEventFormat="CEF" exportTemplate="Audit Records">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM ClearPass Config Audit"
fieldGroupName="ClearPass Configuration Audit" enabled="true" filterName="[ClearPass
Configuration Audit]" exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>CppmConfigAudit.Name</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmConfigAudit.Action</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmConfigAudit.Category</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmConfigAudit.Updated-By</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmConfigAudit.Updated-At</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM ClearPass Guest" fieldGroupName="ClearPass
Guest" enabled="true" filterName="[ClearPass Guest]" exportEventFormat="CEF"
exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Guest.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Visitor-Name</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Visitor-Company</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Role-Name</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Enabled</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Created-At</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Starts-At</SyslogExportDataColumn>
<SyslogExportDataColumn>Guest.Expires-At</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM ClearPass System Events"
fieldGroupName="ClearPass System Events" enabled="true" filterName="[ClearPass System
Events]" exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmSystemEvent.Source</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmSystemEvent.Level</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmSystemEvent.Category</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmSystemEvent.Action</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmSystemEvent.Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Endpoint" fieldGroupName="Endpoints"
enabled="true" filterName="[Endpoints]" exportEventFormat="CEF" exportTemplate="Insight
Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Endpoint.MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.MAC-Vendor</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Device-Category</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Device-Family</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Device-Name</SyslogExportDataColumn>
```

```
<SyslogExportDataColumn>Endpoint.Conflict</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Status</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Added-At</SyslogExportDataColumn>
<SyslogExportDataColumn>Endpoint.Updated-At</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Failed Authenications"
fieldGroupName="Failed Authentications" enabled="true" filterName="[All Requests]"
exportEventFormat="CEF" exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Auth-Source</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Auth-Method</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.System-Posture-Token</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Enforcement-Profiles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Error-Code</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Alerts</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Guest Access" fieldGroupName="Guest
Access" enabled="true" filterName="[All Requests]" exportEventFormat="CEF"
exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Auth-Method</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.System-Posture-Token</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Enforcement-Profiles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Insight Radius Auth"
fieldGroupName="RADIUS Authentications" enabled="true" filterName="[RADIUS Authentications]"
exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Auth.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Protocol</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Login-Status</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Source</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Enforcement-Profiles</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Insight Radius Auth Failed"
fieldGroupName="RADIUS Failed Authentications" enabled="true" filterName="[RADIUS Failed
Authentications]" exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Auth.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Service</SyslogExportDataColumn>
```

```
<SyslogExportDataColumn>CppmErrorCode.Error-Code-Details</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmAlert.Alerts</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Logged in Users" fieldGroupName="Logged in
users" enabled="true" filterName="[All Requests]" exportEventFormat="CEF"
exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Framed-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Radius Accounting" fieldGroupName="RADIUS
Accounting" enabled="true" filterName="[All Requests]" exportEventFormat="CEF"
exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>RADIUS.Acct-Username</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-NAS-Port</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-NAS-Port-Type</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Calling-Station-Id</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Framed-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Session-Id</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Session-Time</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Output-Pkts</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Input-Pkts</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Output-Octets</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Input-Octets</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Service-Name</SyslogExportDataColumn>
<SyslogExportDataColumn>RADIUS.Acct-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM System" fieldGroupName="" enabled="true"
exportEventFormat="CEF" exportTemplate="System Events">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM TACACS Accounting" fieldGroupName="TACACS+
Accounting" enabled="true" filterName="[All Requests]" exportEventFormat="CEF"
exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>TACACS.Remote-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>TACACS.Acct-Flags</SyslogExportDataColumn>
<SyslogExportDataColumn>TACACS.Privilege-Level</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM TACACS Administration"
fieldGroupName="TACACS+ Administration" enabled="true" filterName="[All Requests]"
exportEventFormat="CEF" exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>TACACS.Remote-Address</SyslogExportDataColumn>
```

```
<SyslogExportDataColumn>TACACS.Privilege-Level</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM TACACS Authenication"
fieldGroupName="TACACS Authentication" enabled="true" filterName="[TACACS Authentication]"
exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Tacacs.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Remote-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Request-Type</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Auth-Source</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Enforcement-Profiles</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Privilege-Level</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM TACACS Failed Auth" fieldGroupName="TACACS
Failed Authentication" enabled="true" filterName="[TACACS Failed Authentication]"
exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Tacacs.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Remote-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Request-Type</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.NAS-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Tacacs.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmErrorCode.Error-Code-Details</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmAlert.Alerts</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM WebAuth" fieldGroupName="WEBAUTH"
enabled="true" filterName="[WEBAUTH Authentication]" exportEventFormat="CEF"
exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Auth.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Protocol</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.System-Posture-Token</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Login-Status</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Source</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Enforcement-Profiles</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
<SyslogExportData description="" name="McAfee ESM Web Authenication" fieldGroupName="Web
Authentication" enabled="true" filterName="[All Requests]" exportEventFormat="CEF"
exportTemplate="Session Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Common.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>WEBAUTH.Host-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Roles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.System-Posture-Token</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Enforcement-Profiles</SyslogExportDataColumn>
<SyslogExportDataColumn>Common.Request-Timestamp</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
```

```
<SyslogExportData description="" name="McAfee ESM WebAuth Fail Auth" fieldGroupName="WEBAUTH
Failed Authentications" enabled="true" filterName="[WEBAUTH Failed Authentications]"
exportEventFormat="CEF" exportTemplate="Insight Logs">
<SyslogServerNameList>
<string>change.me.receiver.ip</string>
</SyslogServerNameList>
<SyslogExportDataColumns>
<SyslogExportDataColumn>Auth.Username</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-MAC-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Host-IP-Address</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Protocol</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.System-Posture-Token</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmNode.CPPM-Node</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Login-Status</SyslogExportDataColumn>
<SyslogExportDataColumn>Auth.Service</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmErrorCode.Error-Code-Details</SyslogExportDataColumn>
<SyslogExportDataColumn>CppmAlert.Alerts</SyslogExportDataColumn>
</SyslogExportDataColumns>
</SyslogExportData>
</SyslogExportConfigurations>
</TipsContents>
```

Attivo Networks BOTsink

Contents

Configure Attivo Networks BOTsink

Task

1 In the BOTsink console, click the **Gear** icon, then select **Administration** | **Syslog**.

2 To configure a new syslog destination, click the **+ Server** icon, then fill in the required BOTsink fields:

- **Name** – Type a name that helps you identify the McAfee Event Receiver.
- **IP address** – Type IP address of the McAfee Event Receiver.
- **Port** – Type 514 or a server-side port.
- **Protocol** – Select User Datagram Protocol (UDP) or Transmission Control Protocol (TCP).
- **Enable** – Select to turn on syslog forwarding from the BOTsink Manager.

3 Click **Save.**

Add Attivo Networks BOTsink

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Attivo Networks**
Data Source Model	**BOTsink**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Attivo Networks BOTsink events to McAfee fields

Log format

The expected format for this device is:

```
<9>BotSink: Severity:[] Attacker IP:[] Target IP:[] Target OS:[] Description:[] Details:[]
Phase:[] Service:[]
```

Log samples

This is a sample log from a device:

```
<9> BotSink: Severity:[Medium] Attacker IP:[192.168.1.79] Target IP:[1.1.1.1] Target OS:
[CentOS 7.0] Description:[Telnet connection started] Details:[16/8/1@19:32:42: START: telnet
pid=122 from=1.1.1.1 ] Phase:[Access] Service:[TELNET]
```

Mappings

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

Log fields	McAfee ESM fields
Description	Message
Severity	Severity
Attacker IP	Attacker_IP, Hostname
Target IP	Victim_IP, Destination_Hostname
Target OS	Operating_System
Details	Message_Text
Phase	Threat_Category

Log fields	McAfee ESM fields
Service	Service_Name
Details (Access Log timestamp)	First Time, Last Time
Device	External_Device_Type
VLANID	vlan

Axway SecureTransport

Contents

Configure Axway SecureTransport

See the Axway Security Transport 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.

Add Axway SecureTransport

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Axway**
Data Source Model	**SecureTransport**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Axway SecureTransport events to McAfee fields

Log format

The expected format for this device is:

```
Weekday Date Time Version IP Filesize FilePath/FileName TransferType(s) Username
TransferProtocol
```

Log sample

This is a sample log from an Axway SecureTransport device:

```
Mon Jan 01 00:00:00 2001 514 192.0.2.0 100000000 /Folder/Folder/Folder/Folder/Folder/
CompressedFile.part1.rar a n o r oteupp ftp 0 *
```

Mappings

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

Log fields	McAfee ESM fields
Weekday Date Time	First Time, Last Time
Version	Version
IP	Source IP
Filesize	Message_Text
FilePath/FileName	Object
Username	Source Username
TransferProtocol	Application

Barracuda Spam Firewall

Contents

Configure Barracuda Spam Firewall

Task

1 In the web interface, go to **Advanced** | **Advanced Networking**.

2 In the **Syslog Configuration** section, enter the IP address of the McAfee Event Receiver in the **Mail Syslog** field.

3 In the **Port** field, enter the number where the McAfee Event Receiver is listening (default is 514).

4 Select **UDP** for the **Protocol**, then click **Add**.

Add Barracuda Spam Firewall

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Barracuda Networks
Data Source Model	Spam Firewall (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the McAfee Event Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Barracuda Spam Firewall events to McAfee fields

Log format

The expected format for this device is:

```
<event action> <hostname> <IP address> <time><username> <destination username> <spam score>
<event ID> <subject>
```

Log sample

This is a sample log from a Barracuda Networks Spam Firewall device:

```
<123>inbound/pass[1234]: example.com[192.0.2.1] 1234567890-a1b2c3d4e5f6-a7b8c9 978310861
978310861 SCAN - example@example.com example@example.com 1 2 34 SUBJ:=Email Subject
```

Mappings

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

Log fields	McAfee ESM fields
Host	Hostname
Spam Score	Spam_Score
Client IP	Source IP

Log fields	McAfee ESM fields
Username	Source Username
Destination Username	Destination Username
Email Subject	Subject
Action	Event_Class
Event ID	External_Event_ID
Queued as ID	Queue_ID
Bytes Received	Bytes_Received

Barracuda Web Application Firewall

Contents

Configure Barracuda Web Application Firewall

Task

1 Open a web browser and log on to your Web Application Firewall (WAF) device.

2 Click the **ADVANCED** tab and select **Export Logs**.

3 In the **Syslog** section, click **Add Syslog Server**, then fill in these fields:

- **Name**: A name for reference in the WAF.
- **IP Address**: The IP address of your McAfee Event Receiver.
- **Port**: The port number used for syslog on your McAfee Event Receiver (**514** by default).
- **Connection Type**: Most commonly **UDP**, the default in the McAfee Event Receiver.
- **Validate Server Certificate**: Select **No**.
- **Client Certificate**: Not needed when **Validate Server Certificate** is set to **No**.

4 Click **Add**.

Add Barracuda Web Application Firewall

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Barracuda Networks**
Data Source Model	**Web Application Firewall (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Barracuda Web Application Firewall events to McAfee fields

Log format

The expected format for this device depends on the log type:

System Logs:

```
Timestamp Module Name Log Level Event ID Message
```

Web Firewall Logs:

```
Timestamp Unit Name Log Type Severity Level Attack Description Client IP Client Port
Application IP Application Port Rule ID Rule Type Action Taken Follow-up Action Attack
Details Method URL Protocol Session ID User Agent Proxy IP Proxy Port Authenticated User
Referrer Attack ID Attack Group
```

Access Logs:

```
Timestamp Unit Name Log Type Application IP Application Port Client IP Client Port Login ID
Certificate User Method Protocol Host Version HTTP Status Bytes Sent Bytes Received Cache
Hit Time Taken Server Server Port Server Time Session ID Response Type Field Profile Matched
Field Protected Field WF Matched Field URL Query Referrer Cookie User Agent Proxy IP Proxy
Port Authenticated User Custom Header 1 Custom Header 2 Custom Header
```

Audit Logs:

```
Timestamp Unit Name Log Type Admin Name Client Type Login IP Login Port Transaction Type
Transaction ID Command Name Change Type Object Type Object Name Variable Old Value New Value
          Additional Data
```

Network Firewall Logs:

```
Unit Name Timestamp Log Type Severity Level Protocol Source IP Source Port Destination IP
Destination Port Action ACL Name Interface ACL Details
```

Log sample

This is a sample log from a device:

System Log:

```
Feb 3 15:09:02 wsf STM: LB 5 00141 LookupServerCtx = 0xab0bb600
```

Web Firewall Log:

```
2016-02-03 01:49:09.077 -0800 wafbox1 WF ALER SQL_INJECTION_IN_PARAM 192.0.2.0 39661
198.51.100.0 80 webapp1:deny_ban_dir GLOBAL LOG NONE [type="sql-injection-medium"
pattern="sql-quote" token="' or " Parameter="address" value="hi' or 1=1--"] POST 192.0.2.0/
cgi-bin/process.cgi HTTP REQ-0+RES-0 "Mozilla/5.0 (X11; U; Linux i686 (x86_64); en-US; rv:
1.8.1.20) Gecko/20081217 Firefox/2.0.0.20" 192.0.2.0 39661 User1 http:// 192.0.2.0/cgi-bin/
1.pl 11956 ATTACK_CATEGORY_INJECTION
```

Access Log:

```
2016-02-02 21:16:59.914 -0800 wafbox1 TR 192.0.2.0 80 198.51.100.0 37754 "-" "-" POST HTTP
192.0.2.0 HTTP/1.1 200 812 6401 0 198.51.100.0 80 0 SERVER DEFAULT PASSIVE VALID /cgi-bin/
process.cgi "-" http:// 192.0.2.0/cgi-bin/1.pl ys-grid_firewall_log-grid=o%3Acolumns%3Da
%253Ao%25253Aid%25253Ds%2525253Aiso_timestamp%25255Ewidth%25253Dn%2525253A38%255Eo%252
"Mozilla/5.0 (X11; U; Linux i686 (x86_64);en-US; rv:1.8.1.20) Gecko/20081217 Firefox/
2.0.0.20" 198.51.100.0 37754 User2 en-us,or;q=0.5 gzip,deflate
ISO-8859-15,utf-8;q=0.7,*;q=0.7
```

Audit Logs:

```
2016-02-02 21:08:53.861 -0800 wafbox1 AUDIT User3 GUI 192.0.2.0 0 CONFIG 17 - SET
web_firewall_policy default url_protection_max_upload_files "5" "6" "[]"
```

Network Firewall Log:

```
afbox1 2016-05-21 03:28:23.494 -0700 NF INFO TCP 192.0.2.0 52236 192.0.2.0 8000 DENY testacl
MGMT/LAN/WAN interface traffic:deny policy TCPFeb 3 15:09:02 wsf STM: LB 5 00141
LookupServerCtx = 0xab0bb600
```

Mappings

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

Log fields	McAfee ESM fields
Timestamp	First Time, Last Time
Attack Description	Message
Client IP	Source IP
Client Port	Source Port
Application IP	Destination IP
Application Port	Destination Port
Rule ID	Signature_Name
Rule Type	Object
Attack Details	Message_Text
Method	Application, Method
URL	URL
Protocol	Protocol, App_Layer_Protocol
User Agent	User_Agent

Log fields	McAfee ESM fields
Referrer	Referrer
User	Source Username
Bytes Sent	Bytes_Sent
Bytes Received	Bytes_Received
Cmd	Command
HTTP status	Query_Response
Version	Application_Protocol
Device Type	Object
ACL Name	Policy_Name
Interface	Interface

Barracuda Web Filter

Contents

Configuring Barracuda Web Filter

Task

1 From the admin interface, go to **Advanced** | **Syslog**.

2 Enter the IP address of the McAfee Event Receiver.

Add Barracuda Web Filter

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Barracuda Networks
Data Source Model	Barracuda Web Filter (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the McAfee Event Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Barracuda Web Filter events to McAfee fields

Log format

The expected format for this device is:

```
<device IP> <service> <time date> <source IP> <destination IP> <web domain> <action>
<service> <command> <application> <user>
```

Log sample

This is a sample log from a Barracuda Networks Web Filter device:

```
[192.0.2.1] <123>http_scan[12345]: 978310861 192.0.2.2 192.0.2.3 text/javascript http://
example.com/ 123 ABC ALLOWED CLEAN 2 1 1 0 1 (ldap0:internet_standardaccess) 1 CUSTOM-6 0 -
0 example.com search-engines-portals,CUSTOM-5,CUSTOM-6,CUSTOM-12345678901112 [ldap0:user]
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Hostname
Application	Application
Source IP	Source IP
Destination IP	Destination IP
Command	Command
Web Domain	Domain
Service	Object
User	Source Username

Log fields	McAfee ESM fields
Description	Message_Text
Subject	Subject

Bit9 Parity Suite

Contents

Configure Bit9 Parity Suite

Task

1 Navigate to the **System Configuration** page in the user interface.

2 On the **Configuration Options** list, select **Server Status**, click **Edit**, then select **Syslog enabled**.

3 In the **Syslog address** field, enter the IP address of your McAfee Event Receiver, then set the **Syslog port** to **514**.

4 Set **Syslog format**.

- For standard syslog formatted logs, set to **Basic (RFC 3164)**.
- For ArcSight CEF formatted logs, set to **CEF (ArcSight)**.

5 Click **Update** to save changes and exit.

Add Bit9 Parity Suite

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Bit9**
Data Source Model	Bit9 Parity Suite (ASP) for Basic (RFC 3164) logs Bit9 Parity Suite – CEF (ASP) for ArcSight CEF formatted logs
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

Bit9 Parity Suite Basic (RFC 3164) events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device name> <message>
```

Log sample

This is a sample log from a Bit-9 Parity Suite device:

```
<123>1 2001-01-01T01:01:01Z example.name.com Parity - - - Bit9 ParityServer event:
text="Computer from '192.0.2.1' changed its name from 'hostname1' to 'hostname2'."
event_type="Computer Management" event_subtype="Computer modified" hostname="hostname2"
username="exampleName" date="1/01/2001 01:01:01 PM"
```

Mappings

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

Log fields	McAfee ESM fields
hostname	Hostname
event_type	Application
ip_address	Source IP
Destination IP	Destination IP
Source MAC	Source MAC
Destination MAC	Destination MAC
CLI	Command
hostname	Domain

Log fields	McAfee ESM fields
Name, hash	Object
username	Source_Username
Destination Username	Destination_Username
process	Target_Process_Name
file_name	Destination_Filename
policy	Policy_Name
Description	Message_Text

Bit9 Parity Suite - CEF (ArcSight) events to McAfee fields

Log format

The expected CEF format for this device is:

```
<priority> <date> <hostname> CEF:<version>|<device vendor>|<device product>|<device version>|
<signature ID>|<name>|<severity>|<custom field label=label> <custom field value=value>…
```

Log sample

This is a sample CEF log from a Bit9 Parity Suite device:

```
<123>Jan 01 01:01:01 hostname CEF:0|Bit9|Parity|x.x.x|1234|New file on network|4|
externalId=123456 cat=value rt=Jan 01 01:01:01 UTC filePath=c:\\example.net
fname=example.net fileHash=a1b2c3d4e5f6 fileId=123456 dproc=c:\\example.exe dst=192.0.2.1
dhost=hostname duser=username dvchost=hostname msg=Server discovered new file example.net
cs1Label=rootHash cs1=hash cs2Label=installerFilename cs2=filename cs3Label=Policy cs3=policy
```

Mappings

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

Log fields	McAfee ESM fields
dhost	Hostname
installerFilename	Application
src	Source IP
dst	Destination IP
spt	Source Port
dpt	Destination Port
smac	Source MAC
dmac	Destination MAC
proto	Protocol
cnt	Event Count
fname	Filename
Policy	Object_Type
spriv	Object
suser	Source_Username
duser	Destination_Username

Log fields	McAfee ESM fields
externalId	End_Page
act	Event Subtype

Blue Coat Director

Contents

Configure Blue Coat Director

See the Blue Coat Director 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.

Add Blue Coat Director

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Blue Coat
Data Source Model	Director (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing.
Time Zone	Time zone of data being sent

Blue Coat Director events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <severity> <hostname> <user> <IP address> <message>
```

Log sample

This is a sample log from a Blue Coat Director device:

```
Jan 01 01:01:01 <cli.notice_minor> hostname cli[1234]: admin@192.0.2.2: Device exampleName:
attempting connection using ssh.
```

Mappings

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

Log fields	McAfee ESM fields
Device ID	Hostname
Destination Hostname	Destination_Hostname
IP Protocol	Protocol
IP Address	Source IP
Destination IP	Destination IP
Port	Source Port
Application	Application
Command	Command
Filename	Filename
Invalid IP	Object
User	Source Username
Destination User	Destination Username
URL List	URL

Blue Coat ProxySG

Contents

Create a custom log format

McAfee ESM requires a custom format for the Blue Coat Access Logs.

Task

1 Select **Configuration** | **Access Logging** | **Formats**, then click **New**.

2 Select a format type.

- **W3C Extended Log File Format (ELFF) string**
- **Custom format string** to use log-specific formats

3 Give the format a name, then type the format:

- If you selected **W3C Extended Log File Format (ELFF) string**, type this custom format:

```
date time time-taken c-ip cs-username cs-auth-group x-exception-id sc-filter-result
cs-categories cs(Referer) sc-status s-action cs-method rs(Content-Type) cs-uri-scheme
cs-host cs-uri-port cs-uri-path cs-uri-query cs-uri-extension cs(User-Agent) s-ip
sc-bytes cs-bytes
```

- If you selected **Custom format string**, enter the format for the supported custom string.

4 Click **Test Format** to make sure that there are no syntax errors.

5 Select **Log all headers** from the **Multiple-valued header policy** list, then click **OK**.

Tasks

- *Associating the custom log format with a custom log* on page 105
- *Associating the custom log to the Web Content Policy* on page 105

Associating the custom log format with a custom log

Task

1 Select **Configuration** | **Access Logging** | **Logs** | **Logs**, then click **New**.

2 Type a log name, select your custom log format from the drop-down list, then add a meaningful description.

3 Type the maximum size that the remote log file reaches before rolling over to a new file.

4 Enter a size for the **Early Upload** file, then click **OK**.

Associating the custom log to the Web Content Policy

Task

1 Select **Configuration** | **Policy** | **Visual Policy Manager** | **Launch**.

2 Once the Visual Policy Manager (VPM) has started, add a Web Content Layer or edit the existing one. This document describes adding a Web Content Layer.

3 In the VPM, select **Policy** | **Add Web Content Layer**, then enter a name for this new Web Content Layer.

4 Right-click the **Action** column, select **Set**, then select **New** | **Modify Access Logging**.

5 Select **Enable Logging to**, then, from the drop-down list, select the custom log you created.

6 Click **OK**, then click **Install Policy**.

Enable Access Logging globally

Task

1 Select **Configuration** | **Access Logging** | **General** | **Default Logging**.

2 Select **Enable Access Logging**, then click **Apply**.

Configure Syslog

Task

1 Select **Configuration** | **Access Logging** | **Logs** | **Upload Client**.

2 In the **Log** drop-down list, select the custom log that you created.

3 From the Client Type drop-down list, select **Custom Client**, then click **Settings**.

4 Fill in these fields:

- **Host** – Enter the IP address of the McAfee Event Receiver.
- **Port** – Enter `514`.
- **Use Secure Connections (SSL)** – Deselect.

5 Click **OK**.

6 Click **Apply** to return to the Upload Client tab.

7 For **Save the log file as**, select **text file**.

8 Leave the defaults for all other options.

9 Click the **Upload Schedule** tab.

10 Select **Upload Type**.

11 For **Upload the access log**, select **continuously** to stream the access logs to the McAfee Event Receiver.

12 Leave the default settings for all other options.

13 Click **OK**, then click **Apply**.

Add Blue Coat ProxySG (syslog)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Blue Coat Systems**
Data Source Model	**ProxySG Access Log (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**<Defaults>**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device
Syslog Relay	**<Enable>**
Mask	**<Default>**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	**<Default>**
Time Zone	Time zone of data being sent

Add Blue Coat ProxySG (FTP)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Blue Coat Systems**
Data Source Model	**ProxySG Access Log (ASP)**
Data Format	**Default**
Data Retrieval	**FTP File Source**
Enabled: Parsing/Logging/SNMP Trap	**<Defaults>**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Port	**21** (default for FTP)
Number of Lines per record	**<Default>**
Interval	**5 Minutes**
File Completion	**60 Seconds**
Delete processed files	Select to have the Receiver delete the files from the FTP Server after they are processed.
Path	Enter "/" (without quotation marks)
Wildcard expression	***.log.gz**
Username	The user name for the FTP client.
Password	The password for the FTP client.
Encryption	Leave deselected.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Blue Coat ProxySG events to McAfee fields

Log format

The expected format for this device is:

Access log event v6 log example:

```
date time time-taken c-ip cs-username cs-auth-group x-exception-id sc-filter-result
cs-categories cs(Referer) sc-status s-action cs-method rs(Content-Type) cs-uri-scheme
cs-host cs-uri-port cs-uri-path cs-uri-query cs-uri-extension cs(User-Agent) s-ip sc-bytes
cs-bytes x-virus-id
```

Access log event v5.4.6.1 log example:

```
date time c-ip c-port r-ip r-port x-cifs-uid x-cifs-tid x-cifs-fid x-cifs-method
x-cifs-server x-cifs-share x-cifs-path x-cifs-orig-path x-cifs-client-bytes-read
x-cifs-server-bytes-read x-cifs-bytes-written x-client-connection-bytes
x-server-connection-bytes x-server-adn-connection-bytes x-cifs-client-read-operations
x-cifs-client-write-operations x-cifs-client-other-operations x-cifs-server-operations
s-action x-cifs-error-code cs-username cs-auth-group s-ip
```

These log formats are supported custom formats:

nFMAIN log example:

```
nFMAIN Date=|$(date)|, Time=|$(time)|, Time-Taken=|$(time-taken)|, Source=|$(c-ip)|, Status=|
$(sc-status)|, Action=|$(s-action)|, IncomingBytes=|$(sc-bytes)|, OutgoingBytes=|$
(cs-bytes)|, Method=|$(cs-method)|, Scheme=|$(cs-uri-scheme)|, Username=|$(cs-username)|,
Supplier=|$(s-supplier-name)|, UserAgent=|$(cs(User-Agent))|, Result=|$(sc-filter-result)|,
Category=|$(sc-filter-category)|, Virus=|$(x-virus-id)|, DeviceIP=|$(s-ip)|, DevicePort=|$
(s-port)|, URL=|$(c-uri)|, DestinationIP=|$(r-ip)|, DestinationPort=|$(cs-uri-port)|
```

nFIM log example:

```
nFIM Date=|$(date)|, Time=|$(time)|, Time-Taken=|$(time-taken)|, Source=|$(c-ip)|, Username=|
$(cs-username)|, Protocol=|$(cs-protocol)|, Method=|$(x-im-method)|, User-Id=|$
(x-im-user-id)|, Client=|$(x-im-client-info)|, Buddy=|$(x-im-buddy-id)|, ChatRoom=|$
(x-im-chat-room-id)|, Action=|$(s-action)|, File=|$(x-im-file-path)|, FileSize=|$
(x-im-file-size)|, DeviceIP=|$(s-ip)|
```

nFSSL log example:

```
nFSSL Date=|$(date)|, Time=|$(time)|, Time-Taken=|$(time-taken)|, Source=|$(c-ip)|, Action=|$
(s-action)|, CertStatus=|$(x-rs-certificate-validate-status)|, Errors=|$
(x-rs-certificate-observed-errors)|, DestinationIP=|$(r-ip)|, DestinationPort=|$
(cs-uri-port)|, Supplier=|$(s-supplier-name)|, ClientCipher=|$
(x-rs-connection-negotiated-ssl-version)|, ClientCiphernegotiate=|$
(x-rs-connection-negotiated-cipher)|, CipherSize=|$
(x-rs-connection-negotiated-cipher-size)|, Category=|$(x-rs-certificate-hostname-category)|,
ServerCipher=|$(x-cs-connection-negotiated-ssl-version)|, ServernegotiatedCipher=|$
(x-cs-connection-negotiated-cipher)|, ServerCipherSize=|$
(x-cs-connection-negotiated-cipher-size)|, Device=|$(s-ip)|, IncomingBytes=|$(sc-bytes)|,
OutgoingBytes=|$(cs-bytes)|, Protocol=|$(cs-protocol)|, URL=|$(c-uri)|
```

nFSTREAM log example:

```
nFSTREAM Date=|$(date)|, Time=|$(time)|, Scheme=|$(cs-uri-scheme)|, DestinationPort=|$
(cs-uri-port)|, Status=|$(c-status)|, User-Agent=|$(cs(User-Agent))|, Hostexe=|$
(c-hostexe)|, Hostexever=|$(c-hostexever)|, Filesize=|$(filesize)|, Protocol=|$(transport)|,
Bytes1=|$(sc-bytes)|, Bytes2=|$(c-bytes)|, Device=|$(s-ip)|, Source=|$(x-client-address)|,
URL=|$(c-uri)|, Method=|$(cs-method)|
```

nFP2P log example:

```
nFP2P Date=|$(date)|, Time=|$(time)|, Source=|$(c-ip)|, Username=|$(cs-username)|, Protocol=|
$(cs-protocol)|, ClientType=|$(x-p2p-client-type)|, Bytes1=|$(x-p2p-client-bytes)|, Bytes2=|$
(x-p2p-peer-bytes)|, Action=|$(s-action)|, DestinationIP=|$(r-ip)|, DestinationPort=|$
(cs-uri-port)|, Device=|$(s-ip)|
```

Mappings

Access Log

Fields with * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
Date, Time	Firsttime, lasttime
c-ip	src_ip
cs-username	src_username
sc-filter-result	Query_Response.Query_Response*
cs-categories	Subject.Subject
sc-status	Action

Log fields	McAfee ESM fields
s-action	Message
cs-method	commandname
rs-Content-Type	application
cs-host	domain
cs-uri-port	src_port
cs-uri-path	URL.URL
	Job_Name.Job_Name*
cs-User-Agent	User_Agent.User_Agent*
s-ip	dst_ip

Access Log v5.4.6.1

Fields with * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
Date, Time	Firsttime, lasttime
c-ip	src_ip
s-action	Message
cs-bytes	Bytes_Sent.Bytes_Sent*
sc-bytes	Bytes_Received.Bytes_Received*
cs-method	Method.Method
cs-uri-scheme	
cs-host	domain
cs-uri-port	src_port
cs-uri-path	URL.URL
cs-username	src_username
rs(Content-Type)	application
cs(Referer)	Referer.Referer*
cs-User-Agent	User_Agent.User_Agent*
sc-filter-result	Action
cs-categories	Object_Type.Object_Type
x-virus-id	Object_Type.Object_Type
s-ip	dst_ip

nFMAIN

Fields with * indicate compatibility with version 9.2 and later only.

Log Fields	McAfee ESM Fields
nfMAIN	Application
Date, Time	Firsttime, lasttime
Source	src_ip
Status	Response_Code.Response_Code*
Action	Action

Log Fields	McAfee ESM Fields
IncomingBytes	Bytes_Received.Bytes_Received*
OutgoingBytes	Bytes_Sent.Bytes_Sent*
Method	Method.Method
Scheme	Protocol
Username	src_username
User-Agent	User_Agent.User_Agent*
Result	Query_Response.Query_Response*
Category	Category.Category*
Virus	Threat_Name.Threat_Name*
Device_IP	Device_IP.Device_IP*
DevicePort	src_port
URL	URL. URL
DestinationIP	dst_ip
DestinationPort	dst_port

nFIM

Fields with a * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
nFIM	Application
Date, Time	Firsttime, lasttime
Source	src_ip
Username	src_username
Protocol	Protocol
Method	Method.Method
Client	Client_Version.Client_Version*
Action	Action
File	Filename.Filename
DeviceIP	DeviceIP.DeviceIP*

nFSSL

Fields with * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
nFSSL	Application
Date, Time	Firsttime, lasttime
Source	src_ip
Action	Action
DestinationIP	dst_ip
DestinationPort	dst_port
Supplier	URL.URL
Category	Category.Category*

Log fields	McAfee ESM fields
DeviceIP	DeviceIP.DeviceIP*
IncomingBytes	Bytes_Received.Bytes_Received*
OutgoingBytes	Bytes_Sent.Bytes_Sent*
Protocol	Protocol

nFSTREAM

Fields with * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
nFSTREAM	Application
Date, Time	Firsttime, lasttime
DestinationPort	dst_port
Status	Response_Code.Response_Code*
Action	Action
User-Agent	User_Agent.User_Agent*
Hostexe	Client_Version.Client_Version*
Protocol	Protocol
Bytes1	Bytes_Received.Bytes_Received*
Bytes2	Bytes_Sent.Bytes_Sent*
Device	Device_IP.Device_IP*
Source	src_ip
URL	URL.URL
Method	Method.Method

nFP2P

Fields with * indicate compatibility with version 9.2 and later only.

Log fields	McAfee ESM fields
nFP2P	Application
Date, Time	Firsttime, lasttime
Source	src_ip
Username	src_username
Protocol	Protocol
ClientType	Message
Bytes1	Bytes_Received.Bytes_Received*
Bytes2	Bytes_Sent.Bytes_Sent*
Action	Action
DestinationIP	dst_ip
DestinationPort	dst_port
Device	Device_IP.Device_IP*

Configure FileZilla FTP Server

Before you begin
If you are using FTP, set it up first.

Task

1 Download the FileZilla FTP Server for Windows.

2 Install the FileZilla FTP server on your Windows Server and accept all default options.

3 Create a directory to store the BlueCoat ProxySG Access Logs, for example, `D:\BlueCoatLogs`.

A Filezilla server page opens.

4 Add users.

a Select **Edit** | **Users**.

b On the General page, click **Add** under Users, then type the FTP account name.

c In the account settings section, make sure that **Enable Account** is selected.

d Select **Password**, then type a password for the newly created proxysg user.

For security purposes, make sure that this password is complex.

e Click **Shared Folders**, then click **Add**.

f Navigate to the directory created previously, click **OK**, then give the user all file and all directory rights to the directory.

An *H* next to the directory indicates that this is the home directory for the user. If *H* doesn't appear, highlight the directory and click **Set as home dir**.

g Click **OK** to save the user.

The Filezilla FTP server is up and running and the proxysg user is ready to go.

Configure FTP Upload

Task

1 To configure access logs to upload their data to the FTP server, select **Configuration** | **Access Logging** | **Logs** | **Upload Client**.

2 In the Log drop-down list, select the custom log that you created earlier (see *Create a custom log format*).

3 From the Upload Client Type drop-down list, select **FTP Client**, then click **Settings**.

a Fill in these fields.

- **Host:** Enter the IP address of the Filezilla FTP server.
- **Port:** 21 is the default FTP port.
- **Path:** Enter a slash (`/`).
- **Username:** Enter `proxysg`, the user you created earlier (see *FileZilla FTP server configuration*).

b Click **Change Primary Password**, enter the password, then click **OK**.

c In the **Filename** field, type a name that contains text or specifiers.

The file name includes the log name, last octet of the proxy sg, month, day, hour, minute, and seconds.

d Since the Filezilla server is not configured for FTPS or SFTP, deselect **Use Secure Connections (SSL)**.

e Select **Local Time** to upload the local time file instead of using UTC.

f Click **OK**, then click **Apply** to return to the Upload Client Configuration page.

4 For **Save the log file as**, select **gzip file** to reduce the log file size.

The McAfee Event Receiver decompresses a gzipped log file and parses the logs that are in it.

5 Click the **Upload Schedule** tab, then, on the Log drop-down list, select the custom log you created.

6 Under Upload Type, select **periodically**.

7 Under Rotate the Log File, select **Every**, and enter `0` hours and `5` minutes.

The Blue Coat ProxySG uploads the access logs to the FTP server every 5 minutes.

8 Click **Apply**, then verify that the upload is successful.

a On the Upload Client tab, click **Test Upload**, and go to the FTP server (Filezilla Server).

b Verify that the user proxysg logged on and that a file named “main_upload_result” was uploaded to the FTP server.

Blue Coat ProxySG troubleshooting

Use these tips to troubleshoot your configuration if events do not appear in the ESM.

- Log on to the FTP server (FileZilla in this guide) and check the log, verifying the entries that state that the ProxySG has uploaded the log files.
- Make sure that logs state that the McAfee Event Receiver connected and downloaded the log files.
- Verify that port 514 is open on the McAfee Event Receiver. Your output will be similar.

```
netstat -an | grep 514
```

```
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp6       0      0 :::514                  :::*                    LISTEN
udp        0      0 0.0.0.0:514             0.0.0.0:*
udp6       0      0 :::514                  :::*
```

- Use tcpdump on the McAfee Event Receiver to verify receipt of syslog from the server. You can use a command like this to verify the receipt of data:

```
tcpdump -i eth0 source <remote host IP>
```

Blue Coat Reporter

Contents

Configure Blue Coat Reporter

Task

1 Click the **General Settings** tab, then, in the navigation pane, expand **Data Settings** and select **Cloud Download**.

2 Select **Enable Cloud Download**, then specify the directory where the Cloud access logs are being saved.

3 Specify the **Cloud API Username** and **Cloud API Password** to grant access, then click **Save**.

Add Blue Coat Reporter

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Blue Coat**
Data Source Model	**Reporter (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

Blue Coat Reporter events to McAfee fields

Log format

The expected format for this device is:

```
x-bluecoat-customer-id date time x-bluecoat-appliance-name time-taken c-ip cs-userdn
cs-auth-groups x-exception-id sc-filter-result cs-categories cs(Referer) sc-status s-action
cs-method rs(Content-Type) cs-uri-scheme cs-host cs-uri-port cs-uri-path cs-uri-query
cs-uri-extension cs(User-Agent) s-ip sc-bytes cs-bytes x-virus-id x-bluecoat-location-name
x-bluecoat-application-name x-bluecoat-application-operation r-ip x-cloud-drtr x-cloud-rs
cs(X-Requested-With)
```

Log sample

This is a sample log from a device:

```
5478 2016-01-05 05:03:05 "Device_Name" 30 203.0.113.0 DOMAIN\username "DOMAIN\Permitted,
DOMAIN\Domain Users" - OBSERVED "Unrated" http://www.example.com/webpage/ 200 TCP_NC_MISS
GET text/html;charset=UTF-8 http www.example.com 80 /webpage - - "Mozilla/5.0 (Windows NT
5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36" 192.0.2.0
1306 1040 - "ABCD" "-" "-" 198.51.100.0 - - -
```

Mappings

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

Log fields	McAfee ESM fields
date, time	First Time, Last Time
x-bluecoat-appliance-name	External_Device_Name
c-ip	Device_IP
cs-userdn	Domain, Source User
x-exception-id	Reason
sc-filter-result	Action
cs-categories	URL_Category
cs(Referer)	URL
sc-status	Response_Code, Action
s-action	Rule Message
cs-method	Request_Type
cs-uri-scheme	Protocol
cs-host	Web_Domain
cs-uri-port	Destination Port
cs(User-Agent)	User_Agent
s-ip	Source IP
sc-bytes	Bytes_Sent
cs-bytes	Bytes_Received
x-bluecoat-application-name	Application
r-ip	Destination IP

BlueCat DNS/DHCP Server

Contents

Configure BlueCat DNS/DHCP Server using Linux syslog

Task

1 Edit the **/etc/syslog.conf** file.

2 Add this line to the file:

```
*.*; @1.2.3.4:514
```

where `1.2.3.4` is the IP address of your McAfee Event Receiver and `514` is the default port for syslog.

3 Run the command:

```
service syslog restart
```

Configure BlueCat DNS/DHCP Server using the vendor documentation

See the documentation for BlueCat DNS/DHCP Server syslog setup provided by the manufacturer.

Add BlueCat DNS/DHCP Server

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**BlueCat Networks**
Data Source Model	**BlueCat DNS/DHCP Server**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

Blue Ridge Networks BorderGuard

Contents

Configure Blue Ridge Networks BorderGuard

See the BorderGuard documentation for instructions about sending syslog events to your McAfee Event Receiver.

Add Blue Ridge Networks BorderGuard

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Blue Ridge Networks
Data Source Model	BorderGuard (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing.
Time Zone	Time zone of data being sent

Blue Ridge Network BorderGuard events to McAfee fields

Mappings

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

Log fields	McAfee ESM fields
Domain	Domain
IPaddr	Source IP
External IP	Destination IP
Port	Source Port
External Port	Destination Port

Log fields	McAfee ESM fields
MACaddr	Source MAC
CN	Source Username

Brocade IronView Network Manager

Contents

Configure Brocade IronView Network Manager

Configure Brocade IronView Network Manager wired devices.

Task

1 Click the **Wired** tab on the Configuration Wizard panel, then click **New** on the toolbar.

2 Select the syslog receivers, then click **Next**.

3 On the Select Action page, click the action that you want to perform.

- **Add** a syslog receiver to the target devices.
- **Delete** the specified syslog receivers from the target devices.
- **Replace All** syslog receiver entries on the target devices with the entries in this payload configuration.
- **Clear All** syslog receiver entries from the target devices.

4 Click **Next**, then click **New** to add the syslog receivers.

5 Enter the IP address of the McAfee Event Receiver (syslog server), set the UDP port to **514**, then click **Add** to add it to the list of syslog receivers.

Each device can have up to six syslog receivers. All syslog receivers defined for a device receive the same data.

6 To change a syslog receiver, select it and click **Edit**, then make the changes and click **Update**.

7 To open the Deployment section of the wizard, click **Next**.

Add Brocade IronView Network Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Brocade**
Data Source Model	**IronView Network Manager (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

Brocade IronView Network Manager events to McAfee fields

Log format

The expected format for this device is:

```
DATE:SEVERITY:EVENTSOURCE: MESSAGE
```

Log sample

This is a sample log:

```
Jan 20 03:33:52:I:Security: running-config was changed from console
```

Mappings

This table shows the mappings between the data source and ESM fields.

Log fields	ESM fields
Object	Object
Source IP	Source IP
MAC Address	Source MAC
Destination IP	Destination IP
Source Port	Source Port
Destination Port	Destination Port
Host	Host
User	Source User
Application	Application

Brocade VDX Switch

Contents

Configure Brocade VDX Switch

The syslog configuration is done at the command line. See the Brocade VDX Switch product documentation for instructions about how to access and use the command line.

Task

1 Log on to the command line interface for the switch and enter this command:

```
> syslogdIpAdd "192.0.2.1"
```

Replace `"192.0.2.1"` with the IP address of the McAfee ESM.

2 To verify that the logging setting was added, enter this command:

```
> syslogdIpShow
```

This lists all configured remote syslog server IP addresses for the switch.

Add Brocade VDX Switch

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Brocade**
Data Source Model	**VDX Switch (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing.**
Time Zone	Time zone of data being sent.

Brocade VDX Switch events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device name> <log type> <time> <message ID> <severity> <class> <user> <role>
<IP> <interface> <application> <swname> <arg0> <arg1> <arg2>
```

Log sample

This is a sample log from a Brocade VDX Switch device:

```
<123>Jan 1 01:01:01 device name: [log@1234 value="AUDIT"][timestamp@1234
value="2001-01-01T01:01:01.123456"][tz@1234 value="TimeZone"][msgid@1234 value="msg123"]
[severity@1234 value="INFO"][class@1234 value="CLASS"][user@1234 value="user"][role@1234
value="admin"][ip@1234 value="192.0.2.2"][interface@1234 value="telnet"][application@1234
value="app"][swname@1234 value="1234"][arg0@1234 value="command" desc="Event Name"]
[arg1@1234 value="value" desc="Status"][arg2@1234 value=""show"" desc="string"] Event:
command, Status: show, User command: "show running-config interface 01".
```

Mappings

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

Log felds	McAfee ESMMcAfee ESM fields
Swname	Host
Application	Application
IP	Source IP
log type	Object
user	Source User
interface	Interface

Check Point

Contents

Enable the LEA service on the Check Point management server

Task

1 Use SSH to connect to the Check Point management server, then enter expert mode.

2 Open $FWDIR/conf/fwopsec.conf and edit the file according to the type of authentication you want to use.

- For authenticated and encrypted connection (recommended), specify:

```
lea_server auth_port 18184
```

```
lea_server auth_type sslca (or other supported method)
```

- For authenticated connection only, specify:

```
lea_server auth_port 18184
```

- For no authentication or encryption, specify:

```
lea_server port 18184
```

3 Run `cprestart`.

Create an OPSEC Application

Task

1 Log on to the Check Point user interface, then expand the OPSEC Applications tree node.

2 Right-click the **OPSEC Application** category, select **New OPSEC Application**, then enter a name for the OPSEC Application.

This name is used when creating the data source in the ESM.

3 In the **Host** field, select a host, then select the network object that represents the McAfee Event Receiver.

If the object does not exist, create one by clicking **New** and entering the IP address of the McAfee Event Receiver.

4 In the Client Entries section, select **LEA**, then click **Communication** near the bottom of the dialog box.

5 Enter and confirm your one-time password, then click **Initialize**.

The certificate is initialized and displays the message Initialized but trust not established.

6 Close the Communication dialog box.

7 On the OPSEC Application Process dialog box, click **OK**.

8 Perform an **Install DB** on the Check Point server.

Check Point best practices

Create your Check Point Data sources in a parent-child relationship.

Create your Primary CMA as the parent data source, then add your CLMs, Secondary CMAs, and Firewalls as children to the Primary CMA data source.

Adding the parent data source

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Check Point**
Data Source Model	**Check Point (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Name	User-defined name of the CMA
IP Address/Hostname	The IP address of the CMA
Event Collection Type	Select Audit and Log events.
Port	**18184 (Default)**

These settings are needed only if authentication or encryption is being used.

Option	Definition
Use Authentication	Type of authentication selected when creating the LEA connection.
Application Name	Name of the OPSEC Application created during Check Point setup.
Activation Key	One-time password created while creating the OPSEC application during Check Point setup.
Use Encryption	Select if using encryption.
Options (authentication only)	Advanced settings leave default unless having connection issues.
Connect (authentication only)	Tests the connection to the OPSEC LEA service and pulls the certificate.

Add child data sources

After the parent is successfully added, create the child data sources CLMs, Firewalls, and Secondary CMAs.

Task

1 Select the parent data source from the **Receiver Properties Data Sources** screen.

2 Select **Add Child Data Source**.

Child Data Source Screen Settings Log server / CLM and Secondary SMS / CMA

Option	Definition
Name	User-defined name of the CLM
IP Address/Hostname	IP address of the CLM
Device Type	Log Server / CLM or Secondary SMS / CMA
Event Collection Type	Select Audit and Log events.
Parent Report Console	User-defined name of the CMA that the CLM is managed by (preselected if creating a child data source).
Distinguished Name	For more information, see *Add a Check Point CLM or Secondary CMA* .

Child Data Source Screen Settings Security Device (Firewall)

Option	Definition
Name	User-defined name of the Security Device
IP Address	IP address of the Security Device
Device Type	Security Device
Parent Report Console	User-defined name of the CMA that the CLM is managed by (preselected if creating a child data source).

Add a Check Point CLM or Secondary CMA

Typically, the DN is required only to add the Check Point CLM as a data source. This task is needed when firewall logs are sent to a CLM instead of the CMA.

Task

1 Use SSH to connect to the CMA, then enter expert mode.

2 To show all DNs, run this command:

```
grep sic_name $FWDIR/conf/objects_5_0.C
```

3 Find the correct DN for the CLM.

Check Point events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a Check Point device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

Check Point troubleshooting

- If connection test fails, verify CMA IP address.
- If connection test fails, verify that the application name and one-time password are correct.
- If using encryption and connection test fails, click **Options** to change encryption until connection succeeds.
- If connection test fails, reinitialize trust in the Check Point user interface

Cisco IOS

Contents

Configure Cisco IOS

Task

1 Open a secure connection to the console of your Cisco IOS device, then go into enable mode.

```
Router> enable
```

Depending on your configuration, you might need to enter a password.

2 Once in enable mode, go into global configuration mode.

```
Router# configure terminal
```

```
Router(config)#
```

3 Enable the syslog message.

System messages are enabled by default. If logging is disabled, use this command to enable it or to ensure that it is on.

```
Router(config)# logging on
```

By default, this only logs to the console. Use this command to enable logging to send to a specific host, such as the McAfee Event Receiver. The host argument is the name or IP address of the host.

```
Router(config)# logging <host>
```

4 Enable time stamps for logs.

```
Router(config)# service timestamps log datetime localtime
Router(config)# service timestamps debug datetime localtime
```

5 Adjust the security level with this command.

```
Router(config)# logging trap <level>
```

Emergency	0	System unusable messages
Alert	1	Immediate action required messages
Critical	2	Critical condition messages
Error	3	Error condition messages
Warning	4	Warning condition messages
Notification	5	Normal but significant messages
Information	6	Informational messages

6 Save changes and exit:

a Close out of config mode.

```
Router(config)# exit
```

b Save changes.

```
Router# copy running-config startup-config
```

OR

```
Router# copy run start
```

c Exit from enable mode.

```
Router# disable
Router>
```

Add Cisco IOS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**IOS (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco IOS events to McAfee fields

Log format

The expected format for this device is:

```
Date Time: %Facility-Severity-mnemonic: Description SourceIP -> DestIP
```

Log sample

This is a sample log from a Cisco IOS device:

```
Jan 01 01:23:45.678: %SEC-6-IPACCESSLOGNP: list 99 denied 0 192.0.2.2 -> 192.0.2.3, 1 packet
```

Mappings

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

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
Facility	Application
SourceIP	Source IP
DestIP	Destination IP

Log fields	McAfee ESM fields
Protocol	Protocol
SourcePort	Source Port
DestPort	Dest Port
Interface	Interface
Source MAC	Source MAC
Error Code	Response Code
Bundle, Group	Group Name
category	Category

Configure Cisco IOS IPS

No special steps are required on the Cisco IPS device.

Add Cisco IOS IPS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Cisco
Data Source Model	IOS IPS (SDEE protocol)
Data Format	Default
Data Retrieval	API (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Port	443
Use SSL/TLS	Selected
URI	cgi-bin/sdee-server
Username	User name for logging on to the IPS
Password	Password for logging on to IPS
Interval	Choose the frequency you want to pull from the IPS

Cisco IOS IPS events to McAfee fields

Mappings

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

Log field	McAfee ESM fields
sd:hostId	Hostname
cid:initialAlert | sd:evIdsAlert/@eventId	External SessionID
sdIdsAlert/@severity	Severity
sd:time	First Time | Last Time
sd:signature/@description	Message Text
sd:attacker/sd:addr | sd:attacker/sd:ipv6Address	Source IP
sd:target/sd:addr | sd:target/sd:ipv6Address	Dest. IP
cid:interface	Interface
cid:protocol	Protocol
cid:summary	Event Count
@cid:version	Version
CVE	Vulnerability Reference
cid:appName	Application
cid:alertDetails	Message Text
cid:riskRatingValue	Reputation
sd:signature/@cid:type	Threat Category
sd:signature/@id	Incident_ID
cid:os/@type	Object
marsCategory	Threat_Name
sd:attacker/sd:addr/@cid:locality	Source Zone
sd:target/sd:addr/@cid:locality	Destination Zone

Cisco Meraki

Contents

Configure Cisco Meraki

Task

1 From the dashboard, navigate to **Network-wide** | **Configure** | **General**, then click **Add a syslog server**.

2 In the **Server IP** field, enter the IP address of the McAfee Event Receiver, and in the **Port** field, enter `514` (the default port for syslog).

3 Add the roles to the **Roles** field to enable logging for them.

Add Cisco Meraki

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**Meraki**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco Meraki events to McAfee fields

Mappings

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

Log fields	McAfee ESM fields
src	Source IP
dst	Destination IP
mac	Source Mac
request	Method
url	URL
protocol	Protocol
direction	Direction
DNS server	DNS_Server_IP
router	Device_IP
signature	Signature_Name
port changes	Old_Value, New_Value
time	First Time, Last Time

Log fields	McAfee ESM fields
group	Group_Name
client	Host
SSID	Wireless_SSID
radio number	External_Device_ID
reason	Reason
priority	Priority

Cisco NX-OS

Contents

Configure Cisco NX-OS

The syslog configuration is done at the command line. See your product documentation for instructions about how to access and use the CLI.

Task

1 Enter enable mode, then enter configuration mode:

```
> enable
```

```
# configure terminal
```

2 Configure a host where you want to send syslogs:

```
# logging server 192.0.2.1 6
```

where `192.0.2.1` is the IP address of your McAfee Event Receiver, and `6` is the severity level of the logs you want to send (`6` is all events, `2` is only critical and emergency events).

3 To confirm these settings, show remote syslog server configuration.

```
# show logging server
```

4 Save the configuration:

```
# copy running-config startup-config
```

Add Cisco NX-OS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**NX-OS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco NS-OX events to McAfee fields

Log Format

The expected format for this device is:

```
<timestamp> <hostname>: %<application>-<severity>-<message type>: <message>
```

Log sample

This is a sample log from a Cisco NX-OS device:

```
2001 Jan 01 01:01:01 EET: %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user
example_username from 192.0.2.2 - sshd[12345]
```

Mappings

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

Log fields	McAfee ESM fields
Host	Hostname
protocol	Protocol
IP address / sender	Source IP
IP address / target	Destination IP
Source Port / Port	Source Port
Destination / Port	Destination Port
MAC address / sender	Source MAC
MAC address / target	Destination MAC
Application	Application
file	Filename

Log fields	McAfee ESM fields
domain	Domain
user	Source User
remote user	Destination User
Interface, Port	Interface
Destination Interface	Interface_Dest
Timestamp	First Time, Last Time

Cisco PIX ASA

Contents

Configure Cisco PIX ASA

Task

1 Go to the ASDM Home window, then select **Configuration** | **Features** | **Properties** | **Logging** | **Logging Setup**.

2 To enable syslog, select **Enable logging**.

3 In the navigation tree under **Logging**, select **Syslog Servers**, then click **Add** to add syslog server.

4 In the **Add Syslog Server** dialog box, enter the syslog server details, then click **OK**.

Add Cisco PIX ASA

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**PIX/ASA/FWSM (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco PIX ASA events to ESM fields

Mappings

These ESM fields are used within the Cisco PIX ASA ruleset:

Log fields	ESM fields
Action	Application
Bytes_Sent	Command
Count	Destination_Hostname
Device_IP	Direction
Domain	Destination IP
Destination Mac	Destination Port
Destination User	Filename
Group_Name	Host
Interface_Dest	Interface
Rule Message	NAT_Details
Object	Object_Type
Policy_Name	Protocol
Reason	Session
Severity	Source IP
Source MAC	Source Port
Source User	Subject
URL	Username

Cisco Unified Computing System

Contents

Configure Cisco Unified Computing System

1 Log on to the Cisco Unified Computing System (UCS) Manager.

2 In the navigation pane, select the **Admin** tab, expand **Faults**, **Events** and **Audit Log**, then select **Syslog**.

3 In the right pane, enable **Remote Destination Server**, enter the IP address of the syslog server, then select the appropriate level and facility.

4 Click **Save Changes**.

Add Cisco Unified Computing System

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**Unified Computing System (ASP)**
Data Format	Default
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco Unified Computing System events to ESM fields

Log format

The expected format for this device is:

```
<date> <time>: %<facility>-<severity>-<mnumonic>: <description>
```

Log sample

This is a sample log from a Cisco Unified Computing System device:

```
<13>: 2012 Oct 10 21:37:25 EDT: %UCSM-5-DEVICE_SHARED_STORAGE_ERROR: [F0863][warning]
[device-shared-storage-error][sys/mgmt-entity-B] device FOX1616G2JC, error accessing
shared-storage
```

Mappings

This table shows the mappings between the data source and ESM fields.

Log fields	ESMfields
facility	Application
severity	Severity
server	Host

Cisco Wireless LAN Controller

Contents

Configure Cisco Wireless LAN Controller

Task

1. In the controller UI, select **Management** | **Logs** | **Config**, enter the IP address of the server where you want to send the syslog messages, then click **Add**.
2. In the **Syslog Level** field, select the severity level.

   The only messages sent to the syslog server are messages with severity equal to or less than the level you set.

3. In the **Syslog Facility** field, set the facility for outgoing syslog messages to the syslog servers.
4. By default, messages logs include information about the source file. To not include this information, deselect **File Info**.
5. To commit and save the changes, click **Apply**, then click **Save Configuration**.

Add Cisco Wireless LAN Controller

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cisco**
Data Source Model	**Wireless LAN Controller (ASP)**
Data Format	Default
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cisco Wireless LAN Controller events to McAfee fields

Log format

The expected format for this device is:

```
Host Time_Stamp: FACILITY-SEVERITY-MNEMONIC: Message-text
```

Log sample

This is a sample log from a Cisco Wireless LAN Controller device:

```
<180>ABCDE12345: *CDP Main: Nov 09 16:02:36.289: #LWAPP-4-AP_DUPLEX_MISMATCH: spam_api.c:
7755 Duplex mismatch discovered on GigabitEthernet0 (not full duplex), with ABCDE12345
FastEthernet0/1 (full duplex) for AP ABCDE12345
```

Mappings

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

Log fields	McAfee ESM fields
Computer, host	Host, Destination Host
Facility Code	Application
Severity Level	Severity

Log fields	McAfee ESM fields
CMD	Command
Domain	Domain
SSID	Wireless_SSID
Interface	Interface, Interface_Dest
MAC, Client, MAC-ID	Source Mac, Destination Mac, Old_Value
Remote IP	Device IP
Remote Port	Device Port
Username	Source User
SNMP Trap	SNMP_Item

Citrix NetScaler

Contents

Configure Citrix NetScaler

Task

1 In the **Configuration** utility, expand **System** | **Auditing**, then click **syslog**.

2 Click the **Servers** tab, then click **Add**.

   a In the **Name** field, enter the name of the syslog server (for example, `McAfee Event Receiver`), then select **syslog** from the **Auditing Type** list.

   b In the **IP Address** field, enter the IP address of the McAfee Event Receiver.

   c In the **Port** field, enter the port number used for syslog by the McAfee Event Receiver (default is 514).

   d In the **Log Levels** group, select **ALL** to send all logs to the McAfee Event Receiver.

   Individual levels can be selected as needed.

   e Click **Create**, then click **Close**.

3 Click the **Policies** tab to add audit policies, then click **Add**.

   a In the **Name** field, enter a name for the policy (for example, `McAfee ESM`).

   b Select **SYSLOG** in the **Auditing Type** list, then select the McAfee Event Receiver server name in the **Server** list.

   c Click **Create**, then click **Close**.

4 Click **Global Bindings**, click **Insert Policy**, and select the policy name that you created.

5 Click **OK**.

Add Citrix NetScaler

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Citrix**
Data Source Model	**NetScaler (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Citrix NetScaler events to McAfee fields

Log format

The expected format for this device is:

```
<date time zone> <device> <application> <message> <key-value pairs…>
```

Log sample

This is a sample log from a Citrix NetScaler device:

```
<12> 01/10/2001:01:01:01 GMT netscaler ABC-D : SSLVPN HTTPREQUEST 1234567 : Context
username@192.0.2.1 - SessionId: 12345- example.com User username : Group(s) groupname :
Vserver a1b2:c3d4:e5f6:a7b8:c9d0:e1f2:a3b4:c5d6:123 - 01/01/2001:01:01:01 GMT GET file/
path.gif - -
```

Mappings

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

Log Fields	McAfee ESM Fields
Host	Host
Protocol	Protocol

Log Fields	McAfee ESM Fields
Source	Source IP
Destination	Destination IP
Vserver IP	Device_IP
Source	Source Port
Destination	Destination Port
Vserver Port	Device Port
VPN Session	Session ID
Application	Application
Command	Command
Domain	Domain
Filename	Filename
User	Source User
URL	URL, Web_Domain
Nat_ip	NAT_Details

Citrix Secure Gateway

Contents

Configure Citrix Secure Gateway

Task

1 In the **Access Gateway Management Console**, click **Management** | **System Administration**, then click **Logging**.

2 Click **Remote Server Settings** | **Access Gateway Logging**, then enter the IP address of the McAfee Event Receiver in the **Server** field.

3 In the **Port** field, enter the port used to receive syslog by the McAfee Event Receiver (default is 514).

4 Under **Log Type**, select one or more types of logs to be sent to the McAfee Event Receiver.

5 (Optional) To change the frequency with which logs are sent or to send them manually, click **Management** | **System Administration** | **Logging** | **Access Gateway Logging** | **Log Settings**.

Add Citrix Secure Gateway

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Citrix
Data Source Model	Secure Gateway (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Port	514 (default)
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Citrix Secure Gateway events to McAfee fields

Log format

The expected format for this device is:

```
<data time> <severity> <message>
```

Log sample

This is a sample log from a Citrix Secure Gateway device:

```
[Mon Jan 01 01:01:01 2001] [error] SSL Library Error 47 on 1.2.3.4:123 with peer 4.5.6.7:456
An unclassified SSL network error occurred. (error code: 12345 error:12345678)
```

Mappings

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

Log Fields	McAfee ESM Fields
Username	Username
Protocol	Protocol
Source IP	Source IP
Destination IP	Destination IP
Source Port	Source Port
Destination Port	Destination Port
Time	First Time, Last Time

Cluster Labs Pacemaker

Contents

Configure Cluster Labs Pacemaker

Task

1 Open the `/etc/corosync/corosync.conf` configuration file using a text editor.

2 Edit the following lines, below the **Logging** section:

```
To_syslog: yes
```

```
Syslog_facility: daemon
```

3 Save your changes, close the file, then copy the file to all nodes.

Add Cluster Labs Pacemaker

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cluster Labs**
Data Source Model	**Pacemaker (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cluster Labs Pacemaker events to ESM fields

Log format

The expected format for this device is:

```
<priority><hostname>[<ID>]: [<service>/<name>] <Log ID> <message>…
```

Mappings

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

Log fields	ESM fields
Hostname	Host
PID, UUID	Object
Message	Message
Application, Node	Application
Node	Command
Username	Source User
Target Username	Destination user
Severity	Severity

Code Green Data Loss Prevention

Contents

Configure Code Green Data Loss Prevention

See the Code Green Data Loss Prevention product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add Code Green Data Loss Prevention

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Code Green**
Data Source Model	**Data Loss Prevention (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Code Green Data Loss Prevention events to McAfee fields

Log format

The expected format for this device is:

```
"<Date> <Time>",<Device Type>,<Hostname>,,,<IP address>,<Session ID>,<Severity>,<Message>
```

Log sample

This is a sample log from a Code Green Data Loss Prevention device:

```
"Jan 1, 2001 4:01:01 PM",Appliance,hostname,0,,,123456,Notice,Login Events,admin,
192.0.2.1,,Login completed by admin from 192.0.2.2
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Host
email domain	Domain
IP Address	Source IP
Destination IP	Destination IP
“changed port number to”	Source Port
“destination port”	Destination Port
Date, Time	First Time, Last Time
Session ID	Session ID
Severity	Severity

Log fields	McAfee ESM fields
Username	Source User
Device Type	Object

Cooper Power Systems Cybectec RTU

Contents

Configure Cooper Power Systems Cybectec RTU

See the Cooper Power Systems Cybectec RTU product documentation for instructions about sending syslog logs to a remote server. Use the McAfee Event Receiver IP address for the address of the remote server.

Add Cooper Power Systems Cybectec RTU

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cooper Power Systems**
Data Source Model	**Cybectec RTU (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**<Enable>**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cooper Power Systems Cybectec RTU events to McAfee fields

Log format

The expected format for this device is:

```
<timestamp> <device name> <log type> [<location>] <service>; <message type> <message>
```

Log sample

This is a sample log from a Cooper Power Systems Cybectec RTU device:

```
Jan 1 01:01:01 deviceName Security: [Example - Location] Security Service; MAINTENANCE:
"Admin" - Authenticated (EXAMPLEDOMAIN\admin; HOSTNAME)
```

Mappings

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

Log fields	McAfee ESM fields
Source	Hostname
PROTO	Protocol
SRC	Source IP
DST	Destination IP
SRC	Source Port
DST	Destination Port
Command	Command
Domain	Domain
Event	Object
Username	Source User
Service	Service Name
Message Type	Application
Point	Interface
Device	External_Device_Name
Value	New_Value

Cooper Power Systems Yukon IED Manager Suite

Contents

Configure Cooper Power Systems Yukon IED Manager Suite

See the Cooper Power Systems Yukon IED Manager Suite product documentation for instructions about sending syslog logs to a remote server. Use the McAfee Event Receiver IP address for the address of the remote server.

Add Cooper Power Systems Yukon IED Manager Suite

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Cooper Power Systems**
Data Source Model	**Yukon IED Manager Suite (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**<Enable>**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Cooper Power Systems Yukon IED Manager Suite events to McAfee fields

Log format

The expected format for this device is:

```
<Priority> <date> <time> <hostname> <server> <message>
```

Log sample

This is a sample log from a Cooper Power Systems Yukon IED Manager Suite device:

```
<123>Jan 01 01:01:01 HOSTNAME ApplicationServer: (Connection) Connection established with
DeviceName [HOSTNAME:Application Manager Server:1234]
```

Mappings

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

Log fields	McAfee ESM fields
Originating Host	Host
Protocol	Protocol
IP Address	Source IP

Log fields	McAfee ESM fields
Port	Source Port
Date, Time	First Time, Last Time
Priority	Severity
Connection status	Event Subtype
Server	Application
Domain	Domain
Destination Device	Object
User	Source User
To User	Destination User

Corero IPS

Contents

Configure Corero IPS

See the Corero IPS or Top Layer - Attack Mitigator IPS documentation for instructions about how to send syslog data to the McAfee Event Receiver.

Add Corero IPS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Corero
Data Source Model	Corero IPS (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Corero IPS events to McAfee fields

Log format

The expected format for this device is:

```
<date> <time> <device IP> <severity> <device name> <id> <pt> <prot> <cip> <cprt> <sip>
<sprt> <atck> <disp> <ckt> <src> <msg>
```

Log sample

This is a sample log from a Corero IPS device:

```
01-01-2001 01:01:01        192.0.2.1    auth.warn       IPS5500: id=123456 pt=ABC-DE
prot=TCP cip=192.0.2.2 cprt=12345 sip=192.0.2.3 sprt=12 atck=abc-123456 disp=abcde ckt=1
src=extern msg="Message: SynFlood - Connection From Malicious Source IP Address"
```

Mappings

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

Log fields	McAfee ESM fields
prot	Protocol
cip	Source IP
sip	Destination IP
cprt	Source Port
sprt	Destination Port
atck	Signature ID
msg	Message

CyberArk Enterprise Password Vault

Contents

Configure CyberArk Enterprise Password Vault

Syslog messages can be sent to multiple syslog servers in two different ways.

- One message can be sent to multiple servers by configuring an XSLT file.
- Multiple messages can be sent to different servers and formatted differently for each server by configuring multiple XSLT files, formats, and code-message lists. The code-message lists must be matched. They must contain the same number of items in the same order.

Task

1 In \PrivateArk\Server\DBParm.sample.ini, copy the SYSLOG section.

The .ini file contains these configuration values.

- **SyslogServerIP**—The IP addresses of the Syslog servers where messages are sent. Specify multiple values with commas.
- **SyslogServerProtocol**—Specifies the Syslog protocol that is used to send audit logs. Specify **TCP** or **UDP**. The default value is **UDP**.
- **SyslogServerPort**—The port used to connect to the Syslog server. The default value is **514**.
- **SyslogMessageCodeFilter**—Defines which message codes are sent from the Vault to McAfee ESM through the Syslog protocol. You can specify message numbers or ranges of numbers, separated by commas. Specify multiple values with pipelines. By default, all message codes are sent for user and safe activities.
- **SyslogTranslatorFile**—Specifies the XSL file used to parse CyberArk audit records data into Syslog protocol. Specify multiple values with commas.
- **DebugLevel**—Determines the level of debug messages. Specify **SYSLOG(2)** to include Syslog xml messages in the trace file.
- **UseLegacySyslogFormat**—Controls the format of the syslog message, and defines whether it is sent in a newer syslog format (RFC 5424) or in a legacy format. The default value is **No**, which enables working with the newer syslog format. Specify multiple values with commas.

2 In DBParm.ini, paste the **SYSLOG** section at the bottom of the file, then rename the file to `McAfee.xsl`.

3 Copy the relevant XSL translator file from the syslog subfolder of the server installation folder to the location specified in the SyslogTranslatorFile parameter in DBParm.ini.

During vault installation or upgrade, sample XSL files are copied to the **PrivateArk\Server\syslog** folder.

4 Make any needed changes to the XSL translator file relevant to ESM implementation.

5 **Stop** and **Start** the vault for the changes to take effect.

Add CyberArk Enterprise Password Vault

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**CyberArk**
Data Source Model	**Enterprise Password Vault (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

CyberArk Enterprise Password Vault events to McAfee fields

Log sample

Here is a sample log from a CyberArk Enterprise Password device:

```
Nov 05 15:08:51 VLT2PI "Cyber-Ark Vault 5.50.0074" 295 295 "NULL" 6 LOCALHOST\\SYSTEM
Retrieve password <username>=PasswordManager <action>=Retrieve password <msg>=, , Root\
\Groups\\RMAPSDBGroup, , PROD_RMAPS_OLA_DB, , , , CPM, , Retrieve password
```

Mappings

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

Log fields	McAfee ESM fields
username	src_username (ASP)
action	Msg (ASP)
fname	Filename.Filename (cef)
duser	dst_username (cef)
src	src_ip (cef)
cs1_Affected_User_Name	src_username (cef)
cs2_Safe_Name	Objectname (cef)

CyberArk Privileged Identity Management Suite (CEF)

Contents

Configure CyberArk Privileged Identity Management Suite (CEF)

Syslog messages can be sent to multiple syslog servers in two different ways:

- One message can be sent to multiple servers by configuring an XSLT file.
- Multiple messages can be sent to multiple syslog servers and formatted differently for each server by configuring multiple XSLT files, formats, and code-message lists. The code-message lists must be matched, meaning they must contain the same number of items in the same order.

Task

1 In \PrivateArk\Server\DBParm.sample.ini, copy the **SYSLOG** section.

The .ini file contains these configuration values.

- **SyslogServerIP** – The IP addresses of the syslog servers where messages are sent. Specify multiple values with commas.
- **SyslogServerProtocol** – Specifies the syslog protocol that is used to send audit logs. Specify **TCP** or **UDP**. The default value is **UDP**.
- **SyslogServerPort** – The port used to connect to the syslog server. The default value is **514**.
- **SyslogMessageCodeFilter** – Defines which message codes are sent from the vault to McAfee ESM through the syslog protocol. You can specify message numbers or ranges of numbers, separated by commas. Specify multiple values with pipelines. By default, all message codes are sent for user and safe activities.
- **SyslogTranslatorFile** – Specifies the XSL file used to parse CyberArk audit records data into syslog protocol. Specify multiple values with commas.
- **DebugLevel** – Determines the level of debug messages. Specify **SYSLOG(2)** to include syslog xml messages in the trace file.
- **UseLegacySyslogFormat** – Controls the format of the syslog message, and defines whether it is sent in a newer syslog format (RFC 5424) or in a legacy format. The default value is **No**, which enables working with the newer syslog format. Specify multiple values with commas.

2 In DBParm.ini, paste **SYSLOG** section at the bottom, then rename the file to `McAfee.xsl`.

3 Copy the relevant XSL translator file from the syslog subfolder of the server installation folder to the location specified in the SyslogTranslatorFile parameter in DBParm.ini.

During vault installation or upgrade, sample XSL files are copied to the **PrivateArk\Server\syslog** folder.

4 Make any needed changes to XSL translator file relevant to ESM implementation.

5 **Stop** and **Start** the vault for changes to take effect.

Add CyberArk Privileged Identity Management Suite (CEF)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**CyberArk**
Data Source Model	**Privileged Identity Management Suite - CEF**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

CyberArk Privileged Identity Management Suite CEF events to McAfee fields

Log sample

Here is a sample log from a CyberArk Privileged Identity Management Suite – CEF device:

```
Dec 14 09:49:33 PRODVAULT CEF:0|Cyber-Ark|Vault|6.0.0430|38|Failure: CPM Verify Password
Failed|7|act=CPM Verify Password Failed duser=PasswordManager fname=Root
\S-1-5-21-1147481723-1708746877-4547331-38808 src=10.7.3.171 cs1Label="Affected User Name"
cs1= cs2Label="Safe Name" cs2=Windows PCAdmin Accounts cs3Label="Location" cs3=
cs4Label="Property Name" cs4= cs5Label="Target User Name" cs5= cn1Label="Request Id" cn1=
msg=Failure. Failure Description: CACPM344E Verifying Password Safe: Windows PCAdmin
Accounts, Folder: Root, Object: S-1-5-21-1147481723-1708746877-4547331-38808 failed (try
#368). Code: 2101, Error: Error in verifypass to user IT28326D1L.hmcorp.local\pcadmin on
domain IT28326D1L.hmcorp.local(\\IT28326D1L.HMCORP.LOCAL). Reason: No network provider
accepted the given network path. (winRc\=1203). , address
\=IT28326D1L.hmcorp.local;retriescount\=368;username\=pcadmin;, Failure: CPM Verify Password
Failed
```

Mappings

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

Log fields	McAfee ESM fields
Fname	Filename.Filename
cs4_Database	Database_Name.Database_Name
Dhost	Destination_Hostname.Destination_Hostname
Spriv	Priviledged_User.Priviledged_User
externalId	Instance_GUID.Instance_GUID
cs1_Affected_User_Name	Destination_UserID.Destination_UserID
App	protocol
App	application
duser	dst_username
suser	src_username
cs2_Safe_Name	objectname
Dvc	src_ip
shost	src_ip
Src	src_ip

CyberArk Privileged Threat Analytics

Contents

Configure CyberArk Privileged Threat Analytics

Task

1 On the Privileged Threat Analytics (PTA) system, open the **/opt/tomcat/diamond-resources/default/systemparm.properties** configuration file using a text editor.

2 Copy the line that contains the `syslog_outbound` property, then close the file.

3 Open the **/opt/tomcat/diamond-resources/local/systemparm.properties** configuration file.

4 Paste the line you copied, then uncomment the `syslog_outbound` property and edit the parameters.

Use this example as a guide.

```
syslog_outbound=[{"host": "<SIEM_IP>", "port": 514, "format": "<FORMAT>",
"protocol": "UDP"}]
```

where `<SIEM_IP>` is the IP address of the McAfee Event Receiver and `<FORMAT>` is the `CEF`.

5 Save and close the file, then restart CyberArk PTA.

Add CyberArk Privileged Threat Analytics

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**CyberArk**
Data Source Model	**Privileged Threat Analytics - CEF (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

CyberArk Privileged Threat Analytics events to McAfee fields

Log sample

This is a sample log from a device:

```
CEF:0|CyberArk|PTA|3.1|21|Suspected credentials theft|9|duser=jessica
dst=fileserver4.orgdomain.com cs2Label=eventID cs2=647864b993dcfc92f014fe7a
deviceCustomDate1Label=detectionDate deviceCustomDate1=1421021802000 cs3Label=link
cs3=https://1.1.1.1/incidents/647864b993dcfc92f014fe7a
```

Mappings

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

Log fields	McAfee ESM fields
CustomDate1	Firsttime, Lasttime
Src, sip	Source IP
Dst, dip	Destination IP
severity	severity
Vaultuser	Source Username
url	link

Log fields	McAfee ESM fields
eventID	External Session ID
duser	Destination Username
Src_host	Hostname
eventname	Message
Dst_host	Destination Hostname
CEF.SignatureID	Sid, External Event ID

Damballa Failsafe

Contents

Configure Damballa Failsafe

Task

1. Log on to the **Damballa Failsafe Management Console**, then navigate to **Setup** | **Integration Settings**.
2. Click the **Syslog** tab, then select **Enable Publishing to Syslog**.
3. In the **Syslog Hostname** field, enter the IP address of the McAfee Event Receiver, then select **Enable Syslog Header**.
4. In the **Syslog Facility** and **Syslog Severity** drop-down lists, select the facility and severity of events to send to the McAfee Event Receiver.
5. Leave the **Syslog Port** field blank for the default port of 514, then click **Save**.

Add Damballa Failsafe

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Damballa**
Data Source Model	**Failsafe (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Damballa Failsafe events to McAfee fields

Log format

The expected format for this device is:

```
CEF:<version>|<device vendor>|<device product>|<device version>|<signature ID>|<name>|
<severity>|<key=value> <key=value> <key=value>…
```

Log sample

This is a sample log from a Damballa Failsafe device:

```
CEF:0|Damballa|Failsafe|5.0.3|Convicted Host|Evidence|10|app=DNS cat=DNS Query cfp1=123
cfp1Label=Asset Risk Factor cfp2=123 cfp2Label=Incident Severity cn1=100 cn1Label=Threat
Conviction Score cn2=52 cn2Label=Local Severity cs1=name cs1Label=Threat Name cs2=name
cs2Label=Industry Name cs3=example.com cs3Label=KB Link cs4Label=Connection Status
cs6=example.com cs6Label=Asset Detail Link destinationDnsDomain=example.com dst=192.0.2.1
dvchost=name externalid=1234567 in=0 out=0 proto=UDP rt=978310861 src=192.0.2.2
start=978310861
```

Mappings

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

Log fields	McAfee ESM fields
shost	Host
proto	Protocol
src	Source IP
dst	Destination IP
spt	Source Port
dpt	Destination Port

Log fields	McAfee ESM fields
smac	Source MAC
dmac	Destination MAC
start, end, rt, tstamp, collection	First Time, Last Time
cs4	Event Subtype
cn1, cn2, Severity (CEF header)	Severity
cnt	Event Count
externalid	Session ID
app	Application
cat	Object_Type
cs1, fname, spriv	Object
destinationDnsDomain, sntdom	Domain
suser	Source User
duser	Destination User
request	URL
Signature ID (CEF Header) +Name (CEF Header)	Message
msg	Message_Text
cs2	Threat_Name

Dell Aventail

Contents

Configure Dell Aventail

Task

1 Log on to the **Aventail Management Console**, then click **Monitoring** | **Logging**.

2 Click the **Configure Logging** tab, then set the logging levels in the **Aventail service level** section.

3 In the **Syslog configuration** section, enter these settings:

- **Server** *n*: The IP address of the McAfee Event Receiver
- **Port**: 514
- **Protocol**: UDP

4 Click **Save**, then click **Pending Changes** to apply the new settings.

Add Dell Aventail

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Dell
Data Source Model	Aventail
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Dell Aventail events to McAfee fields

Mappings

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

Before 9.2.0:

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
Hostname	Host
Severity	Severity
Src	Source IP, Source Port
User	*Source User, Domain
Dest	Destination IP, Destination Port
Command, rule	Command
Duration	Elapsed_Time
Session ID	Session ID
status	Event Subtype

Log fields	McAfee ESM fields
Variable, cleanup, attribute, file, assigned to, Client OS, Client OS Version, policy	Object
access to	Object, Destination IP, Destination Port

*** Data from log is reconstructed in a more human readable format**

9.2.0 and later:

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
Hostname	Host
Severity	Severity
Src	Source IP, Source Port
User	*Source User, Domain
Dest	Destination IP, Destination Port
Command, rule	Command
SrcBytes	Bytes_Sent
DstBytes	Bytes_Received
Duration	Elapsed_Time
Session ID	Session ID
status	Event Subtype
Variable, cleanup, attribute	Object
access to	Destination_Hostname, Destination IP, Destination Port
file	Filename
assigned to	Destination_Zone
Client OS, Client OS Version	Operating_System
policy	Policy_Name

*** Data from log is reconstructed in a more human readable format**

Dell PowerConnect Switches

Contents

Configure Dell PowerConnect Switches

Task

1 Using a web browser, log on to the Dell PowerConnect Switch.

2 Navigate to **System** | **Logs** | **Remote Log Server**, then click **Add** to add a server.

3 In the **Log Server** field, enter the IP address of the McAfee Event Receiver.

4 In the **UDP Port** field, enter the port used on the McAfee Event Receiver to receive syslog (default is **514**).

5 In the **Severity** section, select the severity of logs to be sent to the McAfee Event Receiver, then click **Apply Changes**.

Add Dell PowerConnect Switches

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Dell
Data Source Model	PowerConnect Switches (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent

Dell PowerConnect Switches events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device IP> <application> <message number> <message>
```

Log sample

This is a sample log from a Dell PowerConnect Switches device:

```
JAN 01 01:01:01 192.0.2.1-1 TRAPMGR[123456789]: service(123) 1234 %% An invalid user tried
to login through Web from 192.0.2.2
```

Mappings

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

Log fields	McAfee ESM fields
Application	Application
IP Protocol	Protocol
IP Address	Source IP
Destination IP Address	Destination IP
Login Method	Object
User	Username
Date Time	First Time, Last Time
Severity	Severity

Dell SonicOS

Contents

Configure Dell SonicOS

Task

1 Log on to the web interface, then select **Log** | **Automation** from the navigation menu.

2 In the **Syslog Servers** section, click **Add**, then, in the **Name or IP Address** field, enter the IP address of your McAfee Event Receiver.

3 In the **Port** field, enter **514** (the default port for syslog), then click **OK**.

4 In the **Syslog Format** list, select **Default**, then click **Apply**.

Add Dell SonicOS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Dell**
Data Source Model	**SonicOS**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Dell SonicOS events to McAfee fields

Log format

The expected format for this device is:

```
<pri>id=id sn=serial_number time="date time" fw=IP_Address pri=priority c=Message_Category
m=Message_ID msg="IPS_Message" sid=IPS_Signature_ID extra_fields…
```

Log sample

This is a sample log from a SonicWall device:

Standard Event:

```
<129>id=firewall sn=0012ABCD3456 time="2014-01-10 12:11:10 UTC" fw=123.45.56.1 pri=1 c=32
m=608 msg="IPS Detection Alert: ICMP Destination Unreachable (Port Unreachable)" sid=310
ipscat=ICMP ipspri=3 n=323984 src=192.168.0.12:53:X1: dst=10.10.0.88:6045:X4:
```

Mappings

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

Management Event:

Log fields	McAfee ESM fields
id	Application
mgmtip	Source IP
m	Signature ID
time	First Time, Last Time

Standard Event:

Log fields	McAfee ESM fields
pri	Severity
m	Siganture ID
msg	Message, *Signature_Name
c	**Event_Class
Category	Category
bytesRx	Bytes_Received
bytesTx	Bytes_Sent
usr	Source User
src	Source IP, Source Port
dst	Destination IP, Destination Port
proto	Protocol, Application
“from machine”, Host	Host
FQDN	Domain
time	First Time, Last Time

*** Only available in ESM 9.2.0 and later ** Values are converted to their text equivalent**

DG Technology - InfoSec MEAS

Contents

Configure DG Technology - InfoSec MEAS

See the DG Technology – InfoSec Mainframe Event Acquisitions System (MEAS) product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add DG Technology - InfoSec MEAS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**DG Technology - InfoSec**
Data Source Model	**Mainframe Event Acquisitions System (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

DG Technology - InfoSec MEAS events to McAfee fields

Log format

The logs follow the CEF logging format. In addition to the regular CEF formatted key-value pairs, additional keys can be found in the msg="" key-value pair. Here is the CEF logging format:

```
CEF:Version|INFOSEC-DGTECH|MEAS|MeasServer Version|Signature ID|Name|Severity|extensions
```

Log sample

This is a sample log from a MEAS device:

```
Jan 1 00:00:00 HOST1 CEF:0|INFOSEC-DGTECH|MEAS|#.##.##|###|SIGNATURE NAME|1|act=log
shost=HOST1 suid=USER1 src=192.0.2.1 msg="MEASType\=###-### UID\=< UserID > SID\=<HOST1> TYPE
\=<CMND> Text\=<TSS.ADD(UserID2).PSUS> sproc\=HOST1..log"
```

Mappings

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

Log fields	McAfee ESM fields
act	Event Subtype
Attempts Rejects Failures	Session_Status
CAT	Catalong_Name
Cmd	FTP_Command
cnt	Event Count
DEPT	Organizational_Unit
dmac	Destination MAC
dproc	Application

Log fields	McAfee ESM fields
dprot	Access_Resource
dpt	Destination Port
dst	Destination IP
duid, Duid	Destination_UserID
FileType	File_Type
fname	Destination_Filename
fname	Filename
host	Host
jobname, sproc	Mainframe_Job_Name
Jobtype	Job_Type
LPort	Source Port
LUName	Logical_Unit_Name
MEASType (XXX-YYY)	External_EventID(XXX)/External_SubEventID(YYY)
MEASType (XXX-YYY)	Signature ID (396-XXX99YYY)
name	Rule_Name
Number.of.Bytes	*Bytes_Sent
pgname	Application
Plan	DB2_Plan_Name
proto	protocol
Reason	Reason
Return Code	Response_Code
RPort	Destination Port
severity	severity
shost	LPAR_DB2_Subsystem
smac	Source MAC
src	Source IP
sntdom	Domain
SQLSTMT	SQL_Statement
start, end ,rt, tstamp, collection	First Time, Last Time
Step/Stepname	Step_Name
StepCount	Step_Count
suid	Source_UserID
suser	Source User
Test, Text	Message_Text
TYPE	Command
VOLS	Volume_ID

Econet Sentinel IPS

Contents

Configure Econet Sentinel IPS

See your Econet Sentinel IPS documentation for information about sending syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Some versions of Sentinel IPS have different setup methods for remote syslog than other versions of the same product. See the corresponding documentation for your version of Sentinel IPS.

Add Econet Sentinel IPS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Econet**
Data Source Model	**Sentinel IPS**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Econet Sentinel IPS events to McAfee fields

Log format

The expected format for this device is:

```
Timestamp | Src | Src Port | Dst | Dst Port | Severity | Attack Description
```

Log samples

This is a sample log from a Econet Sentinel IPS device:

```
2013-10-30 16:27:17.772624|192.168.2.2|8080|192.168.2.1|80|1|VNC Aggressive SCAN attempt
```

Mappings

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

Log fields	McAfee ESM fields
Timestamp	First Time, Last Time
Src Port	Source Port
Source	Source IP
Dst	Destination IP
Dst Port	Destination Port
Severity	Severity
Attack Description	Message

EdgeWave iPrism Web Security

Contents

Configure EdgeWave iPrism Web Security

Task

1 Log on to the iPrism Web Security configuration web console, then click **System Settings** | **Event Logging**.

2 Select **Enable event logging using Syslog**, then, in the **Syslog Host** field, enter the IP address of the McAfee Event Receiver.

3 In the **Syslog Port** field, enter **514**, then click **Save** and **Activate Changes**.

Add EdgeWave iPrism Web Security

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**EdgeWave**
Data Source Model	**iPrism Web Security (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

EdgeWave iPrism Web Security events to McAfee fields

Log format

The expected format for this device is:

```
<priority> <date> <time> <device> <type> <protocol> <time> <action> <IP> <profile> <user>
<bandwidth> <URL> <rating> <duration> <method> <status> <mime>
```

Log sample

This is a sample log from an EdgeWave iPrism Web Security device:

```
<123>Jan 01 01:01:01 iprism: WEB http 978310861 P 192.0.2.1 Block-User domain\username 123
http://example.com/sub web search 0 HTTPGET 200 image/gif
```

Mappings

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

Log fields	McAfee ESM fields
Rating	Message
Action	Event Subtype
IP	Source IP
Protocol	Application
Web Domain	Domain
Mime	Object
User	Source User

Enforcive Cross-Platform Audit

Contents

Configure Enforcive Cross-Platform Audit

See the Enforcive Cross-Platform Audit 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.

Add Enforcive Cross-Platform Audit

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Enforcive**
Data Source Model	**Cross-Platform Audit**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Enforcive Cross-Platform Audit events to McAfee fields

Log format

The expected format for this device is:

```
<pri> CEF:0|Enforcive|ES CPA|version|eventID|EventDesc|Severity|app=appname cat=category
act=action cs1=cs1string cs1Label=cs1Label dhost=DestHost end=timestamp duser=DestUser
dproc=destinationProcess src=SourceIP dst=DstIP msg=Event Description:Message
```

Log sample

This is a sample log from an Enforcive Cross-Platform Audit device:

```
<110> CEF:0|Enforcive|ES CPA|8.2|SIN00F0000|FTP_SERVER-FTP LOGON|3|app=System i -
Application Audit cat=FTP_SERVER act=FTP LOGON cs1=Warning cs1Label=event status dhost=DES
THOST end=2001-02-03-12.34.56.123456 duser=DestUser dproc=123456/FTPGUEST/QTFTP123456
src=192.0.2.0 dst=203.0.113.0 msg=Event Description:User is unauthorized to ftp
```

Mappings

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

Log fields	McAfee ESM fields
EventID	Signature ID
EventDesc	Rule Message
Severity	Severity
cat	Category
Act	Event Subtype
Dhost	Destination_Hostname
end, start, rt	First Time, Last Time
duser	Destination User
src	Source IP
dst	Destination IP
Application	Application
Event Status	Status
Dproc	Target_Process_Name
Message	Message_Text

Entrust IdentityGuard

Contents

Configure Entrust IdentityGuard

Task

1 In the **Entrust Identity Guard Properties Editor**, click **System Logging Appenders** from the **Table of Contents**.

2 In the **SYSTEM_SYSLOG Host Name** field, enter the IP address of the McAfee Event Receiver.

3 To specify a port other than the standard syslog UDP port, add a colon and the port number at the end of the IP address (for example, `192.0.2.1:514`).

4 Click **Validate** | **Save**.

Add Entrust IdentityGuard

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Entrust**
Data Source Model	**IdentityGuard (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Entrust IdentityGuard events to McAfee fields

Log format

The expected format for this device is:

```
<Priority> <Date> <Time> <IP> <Log Type> <Severity> <Log ID> <Domain> <User> <Message>
```

Log samples

This is a sample log from an Entrust Identity Guard device:

```
<123>Jan 1 01:01:01 196.0.2.1 Audit Writer] [INFO ] [IG.AUDIT] [AUD3003] [DOMAIN/user] One
time password with index 4 created for user DOMAIN/user. Expiry Date: 2001-01-01 01\:01\:01
```

Mappings

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

Log fields	McAfee ESM fields
Date, Time	First Time, Last Time
Description	Message
IP	Source IP

Log fields	McAfee ESM fields
Description	Action
Application Name	Application
Domain	Domain
User	Source User

Extreme Networks ExtremeWare XOS

Contents

Configure Extreme Networks ExtremeWare XOS

The syslog configuration is done at the command line. See the Extreme Networks ExtremeWare XOS product documentation about how to access and use the command line.

Replace `<ip_address>` with the McAfee Event Receiver IP address. Replace `<vr_name>` with the virtual router name. Replace `<local0 ... local7>` with the local level you want to send to the McAfee Event Receiver.

```
configure syslog add <ip_address>:514 vr <vr_name> <local0 ... local7>
```

```
enable log target syslog <ip_address>:514 vr <vr_name> <local0 ... local7>
```

```
configure log target syslog <ip_address>:514 vr <vr_name> <local0 ... local7> DefaultFilter
severity Debug-Data
```

```
configure log target syslog <ip_address>:514 vr <vr_name> <local0 ... local7> match Any
```

```
configure log target syslog <ip_address>:514 vr <vr_name> <local0 ... local7> format
timestamp seconds date Mmm-dd event-name none process-slot priority tag-name
```

Add Extreme Networks ExtremeWare XOS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Extreme Networks**
Data Source Model	**ExtremeWare XOS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Extreme Networks ExtremeWare XOS events to McAfee fields

Log formats

The expected format for this device is:

```
<PRI> DATE TIME APPLICATION: MESSAGE
```

Log samples

These are sample logs from an device:

```
<123> Jan 01 01:01:01 AAA: MSM-A: Login failed for user Bob through ssh (192.0.2.0/24) <123>
Jan 01 01:01:02 AAA: MSM-A: User Bob logout from ssh (192.0.2.0/24) <123> Jan 01 01:01:03
AAA: MSM-A: Login passed for user Bob through ssh (192.0.2.0/24)
```

Mappings

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

Log fields	McAfee ESM fields
Severity	Severity
Action	Action
Application	Application
Source MAC	Source MAC
Username	Source User
Source IP	Source IP
Source Port	Source Port
Destination IP	Destination IP
Destination Port	Destination Port

Log fields	McAfee ESM fields
Message	Rule Message
Object	Object

F5 Networks FirePass SSL VPN

Contents

Configure F5 Networks FirePass SSL VPN

Task

1. Log on to the F5 Networks FirePass Admin Console, then navigate to **Device Management** | **Maintenance** | **Logs**.
2. In the **System Logs** menu, select **Enable Remote Log Server**, and verify that **Enable Extended System Logs** is deselected.
3. In the **Remote Host** field, type the IP address of the McAfee Event Receiver.
4. In the **Log Level** drop-down list, select **Information**.
5. In the **Kernel Log Level** drop-down list, select **Information**, then click **Apply System Changes** to save.

Add F5 Networks Firepass SSL VPN

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**F5 Networks**
Data Source Model	**Firepass SSL VPN (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

F5 Networks Firepass SSL VPN events to McAfee fields

Log formats

The expected format for this device is:

```
<priority> <log type>[<log id>]: [<user>@<domain>] <message> <key> = <value>…
```

Log sample

This is a sample log from an F5 Networks FirePass SSL VPN device:

```
<123>security[12345]: [support@exampleDomain] User exampleUser logged on from 192.0.2.1 Sid
=1a2b3c
```

Mappings

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

Log fields	McAfee ESM fields
hostname	Host
domain	Domain
Source IP, from	Source IP
Destination IP, to	Destination IP
Source Port, from	Source Port
Destination Port, to	Destination Port
session	Session ID
Access menu	Message
group	Command
Sid	Object

Log fields	McAfee ESM fields
User	Source User
account	Destination User
Email	To
Backup filename	Destination_Filename
Email Subject	Subject

F5 Networks Local Traffic Manager

Contents

Configure F5 Networks Local Traffic Manager

Syslog settings are configured through the command line. See the F5 Networks Local Traffic Manager product documentation for steps to access the command line interface.

Task

1 Log on to the command line of the F5 Local Traffic Manager.

2 At the tmsh prompt, add a syslog server using this command format:

```
modify /sys syslog remote-servers add {<server name> {host <server IP address>
remote-port <port number>}}
```

Example:

```
modify /sys syslog remote-servers add {server{host 10.1.1.1 remote-port 514}}
```

3 Save the configuration:

```
save /sys config
```

Add F5 Networks Local Traffic Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**F5 Networks**
Data Source Model	**Local Traffic Manager – LTM (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**<default>**
Time Zone	Time zone of data being sent.

Fidelis XPS

Contents

Configure Fidelis XPS

See the Fidelis XPS/CommandPost product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add Fidelis XPS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Fidelis**
Data Source Model	**Fidelis XPS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Fidelis XPS events to McAfee fields

Log format

The expected format for this device is:

```
<action> <alert UUID> <compression> <destination address> <destination port> <filename>
<from> <group> <policy> <protocol> <rule> <sensor IP> <sensor name> <severity>  <source
address> <source port> <subject> <summary> <time> <to> <user>
```

Log sample

This is a sample log from a Fidelis XPS device:

```
alert aabbccdd-eeff-1122-3344-5566778899aa 0 192.0.2.1 123 <n/a> <n/a> default POLICY TLS
Expired SSL Certificate 127.0.0.1 sensor1 Medium 192.0.2.2 456 <n/a> Invalid SSL certificate
detected from 192.0.2.3 2001-01-01 01:01:01 <n/a> <n/a>
```

Mappings

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

Log fields	McAfee ESM fields
rule	Message
proto	Protocol
srcaddr	Source IP
dstaddr	Destination IP
srcport	Source Port
dstpor	Destination Port
severity	Severity
time	First Time, Last Time

Log fields	McAfee ESM fields
filename	Filename
from	From
to	To
subject	Subject
user	Source User
"Fidelis XPS"	Application

FireEye Malware Protection System

Contents

Configure FireEye Malware Protection System

Configure the syslog using the command line. See your product documentation about how to access and use the command line interface.

Task

1 To enter configuration mode, enter the following commands :

```
enable
configure terminal
```

2 Activate rsyslog notifications:

```
fenotify rsyslog enable
```

3 Add a new remote SIEM server:

```
fenotify rsyslog trap-sink <SIEM-name>
```

Replace `<SIEM-name>` with a short name without spaces to identify the server.

4 Specify the IP address for the new remote server:

```
fenotify rsyslog trap-sink <SIEM-name> address <IP-address>
```

Replace `<SIEM-name>` with the name created in step 3.

Replace `<IP-address>` with the IP address of the McAfee Event Receiver.

5 Set the event format:

```
fenotify rsyslog trap-sink <SIEM-name> prefer message format cef
```

Replace `<SIEM-name>` with the name you created.

6 Save the configuration:

```
write memory
```

Add FireEye Malware Protection System

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**FireEye**
Data Source Model	**FireEye Malware Protection System – CEF (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

FireEye Malware Protection System events to McAfee fields

Log format

The expected format for this device is:

```
CEF:<version>|<device vendor>|<device product>|<device version>|<signature ID>|<name>|
<severity>|<key=value> <key=value> <key=value>…
```

Log sample

This is a sample log from a FireEye Malware Protection System device:

```
CEF:0|FireEye|MPS|6|AB|infection-match|1|rt=Jan 01 2001 01:01:01 src=192.0.2.1 cn2Label=sid
cn2=123 shost=example.com proto=tcp dvchost=name dst=192.0.2.2 spt=123 dvc=192.0.2.3
smac=00:11:22:33:44:55 cn1Label=vlan cn1=1 dpt=123 externalId=1234 cs4Label=link
cs4=example.com dmac=66:77:88:99:00:AA cs1Label=sname cs1=name
```

Mappings

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

Log fields	McAfee ESM fields
shost, dvchost	Host
cn2	Protocol
src	Source IP
dst	Destination IP
spt	Source Port
dpt	Destination Port
smac	Source MAC
dmac	Destination MAC
cn1	VLAN
rt	First Time, Last Time
cnt	Event Count
severity (CEF header)	Severity
cs1	Message
msg	Application
cs2	Command
cat	Object
cs4	URL
cs3	Operating_System
filepath	File_Path
filehash	File_Hash
act	Event Subtype

Fluke Networks AirMagnet Enterprise

Contents

Configure Fluke Networks AirMagnet Enterprise

Task

1 From the **AirMagnet Policy Notification List**, select **Syslog** to open the **Syslog Notification** dialog box.

2 In the **Notification Name** field, enter a unique notification name.

3 In the **Generation** drop-down list, select an interval to generate notifications.

4 In the **Syslog server name** field, enter the fully qualified domain name (FQDN) or IP address of the McAfee Event Receiver.

5 In the **Facility code** drop-down list, select the type of messages you want to send.

6 In the **Protocol** area, select **UDP**, then enter the port used on the McAfee Event Receiver for receiving syslog (default is **514**).

7 Click **OK** to save and close.

Add Fluke Networks AirMagnet Enterprise

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Fluke Networks
Data Source Model	AirMagnet Enterprise (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Fluke Networks AirMagnet Enterprise events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device name> <message> <sensor> <location> <description> <source MAC> <SSID>
```

Log sample

This is a sample log from a Fluke Networks AirMagnet Enterprise device:

```
<123>Jan 01 01:01:01 deviceName deviceName Alert: Rogue AP by MAC address (ACL) from sensor
SensorName, Location: location, Description: , Source MAC: A1:B2:C3:D4:E5:F6, Channel: 123
```

Mappings

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

Log fields	McAfee ESM fields
SSID	Host
Sensor	Object
Source MAC	Source MAC
Destination MAC	Destination MAC

Force10 Networks FTOS

Contents

Configure Force10 Networks FTOS

Configure the syslog at the command line. See your product documentation for instructions about how to access and use the command line.

Task

1 Log on to the command line and enter these commands:

```
logging 192.0.2.1
```

Replace `192.0.2.1` with the IP address of the McAfee Event Receiver.

2 To confirm that the logging settings updated successfully, check the running configuration:

```
show running-config logging
```

3 Save changes:

```
copy running-config startup-config
```

Add Force10 Networks FTOS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Force10 Networks**
Data Source Model	**FTOS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Force10 Networks FTOS events to McAfee fields

Log format

The expected format for this device is:

```
<date> <time> %<hostname> %<service>-<severity>-<log type>: <message>
```

Log sample

This is a sample log from a Force10 Networks FTOS device:

```
Jan 01 01:01:01: %HOSTNAME %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable password
authentication success on vty0 ( 192.0.2.1 )
```

Mappings

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

Log Fields	McAfee ESM Fields
User	Source User
Service	Application
IP Address	Source IP
Severity	Severity

Forcepoint Websense

Contents

- *Forcepoint Websense events to McAfee fields*

Configure Forcepoint Websense

After you install or enable Websense Multiplexer, activate and configure McAfee ESM integration on **TRITON - Web Security**. Follow this procedure for each Policy Server instance in your deployment.

Task

1. Navigate to **Settings** | **General** | **SIEM Integration** and select **Enable SIEM integration for this Policy Server**.
2. Provide the IP address or host name of the system hosting McAfee ESM, then provide the communication port to use for sending McAfee ESM data.
3. Specify the transport protocol (UDP or TCP) to use when sending data to McAfee ESM, then select the McAfee ESM format to determine the syntax of the string used to pass log data to the integration.
4. From the available options, select the CEF format, then click **OK** to cache your changes.
5. To implement the changes, click **Save** and **Deploy**.

When the changes are saved, Websense Multiplexer connects to Filtering Service and distributes the log data to both Log Server and the selected McAfee ESM integration.

Add Forcepoint Websense

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

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

Option	Definition
Data Source Vendor	**Forcepoint**
Data Source Model	**Websense - CEF, Key Value Pair (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Forcepoint Websense events to McAfee fields

Log format

```
The expected format for this device is Common Event Format (CEF).
```

Log sample

This is a sample log from a Websense device:

```
<13>Mar 06 12:55:48 192.0.2.1 CEF:0|Forcepoint|Security|7.7.0|9|Transaction permitted|1|
act=permitted app=http dvc=192.0.2.2 dst=192.0.2.3 dhost=test.host.com dpt=80 src=192.0.2.4
spt=2209 suser=LDAP://192.0.2.4 OU\\=User,DC\\=example,DC\\=com/sanitized
destinationTranslatedPort=51101 rt=1362603348000 in=727 out=554 requestMethod=GET
requestClientApplication=Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/
4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET CLR
1.1.4322; .NET4.0C; InfoPath.2; .NET4.0E) reason=- cs1Label=Policy cs1=role-8**Test
Standard ,role-8**Test Standard  cs2Label=DynCat cs2=0 cs3Label=ContentType cs3=text/
plain;charset\\=UTF-8 cn1Label=DispositionCode cn1=1026 cn2Label=ScanDuration cn2=1
request=http://test.host.com/path
```

Mappings

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

Log Fields	McAfee ESM fields
act	Action
severity	Severity
cat	Category
suser, suid	Source User
src	Source IP
dst	Dest. IP
dpt	Dest. Port
spt	Source IP
destinationTranslatedPort	Nat_Details
requestMethod	Method
request	URL
in	Bytes_Received
out	Bytes_Sent
cn2_ScanDuration	Elapsed_Time
fname	Filename
cat	Category
msg	Rule Message | Description
sourceServiceName	Service_Name
request	URL
dhost	Web_Domain
app	Protocol
dst	Dest. IP
dpt	Dest. Port

Log Fields	McAfee ESM fields
src	Source IP
spt	Source Port
suser	Source User
Cn1_DispositionCode	Signature ID
Timestamp	First Time | Last Time
EventID	External_EventID

ForeScout CounterACT

Contents

Configure ForeScout CounterACT

To configure CounterACT to send syslog events to the McAfee Event Receiver, you must install a plug-in for CounterACT.

Task

1 From the ForeScout website, download the ForeScout plug-in for integration with the McAfee ESM.

2 In the CounterACT software, click **Options** from the toolbar, then click **Plugins**.

3 Click **Install** and navigate to the plug-in file that you downloaded, then click **Install**.

The plug-in appears in the **Plugins** list.

4 Select the **McAfee ESM** plug-in, then click **Configure**.

5 Select the devices that need to be configured to send events to the McAfee Event Receiver, then click **OK** to open the **Configuration** window.

6 In the **Server Address** field, enter the IP address of the McAfee Event Receiver.

7 In the **Syslog Port** field, enter `514`, then click **OK** to save and exit.

Add ForeScout CounterACT

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ForeScout**
Data Source Model	**CounterACT (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

ForeScout CounterACT events to McAfee fields

Log format

The expected format for this device is:

```
<Priority> <device name>[<event ID>]: <log type> <source IP> <rule> <policy> <match>
<category> <details> <reason> <added>
```

Log sample

This is a sample log from a ForeScout CounterACT device:

```
<123>CounterACT[12345]: NAC Policy Log: Source: 192.0.2.1, Rule: Policy "AntiVirus
Compliance" , Match: "AV Not Running:Match", Category: Not Compliant, Details: Host
evaluation changed from "AV Not Installed:Match" to "AV Not Running:Match" due to
condition . Reason: Property update: AntiVirus Installed: Added: AV Software.
```

Mappings

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

Log fields	McAfee ESM fields
Event ID	Session ID
to, User	Source User
from, Source	Source IP
Destination	Destination IP
Destination	Destination Port
Policy	Application
command	Command
CPU usage, Uptime (in seconds)	Object

Configure ForeScout CounterACT for CEF

ForeScout CounterACT does not generate events in CEF format. Use the ArcSight SmartConnector to send CEF formatted logs to the McAfee Event Receiver.

See the ArcSight product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add ForeScout CounterACT for CEF

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ForeScout**
Data Source Model	**CounterACT CEF (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

ForeScout CounterACT for CEF events to McAfee fields

Log Format

The expected format for this device is:

```
<priority> <device name> <event ID> CEF:<version>|<device vendor>|<device product>|<device
version>|<signature ID>|<name>|<severity>|<key=value> <key=value> <key=value>...
```

Log Sample

This is a sample log from a ForeScout CounterACT device:

```
<123>CounterACT[1234]: CEF:0|ForeScout Technologies|CounterAct|6|NONCOMPLIANCE|host is not
compliant|5|cs1Label=Compliancy Policy Name cs2Label=Compliancy Policy Subrule Name
cs3Label=Host Compliancy Status cs4Label=Compliancy Event Trigger cs1=VirusScan Status
cs2=VirusScan Updated cs3=no cs4=Periodical dst=192.0.2.1 dmac=aa:bb:cc:dd:ee:ff
duser=username dhost=hostname dntdom=DOMAIN dvc=192.0.2.2 dvchost=host rt=978310861000
```

Mappings

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

Log fields	McAfee ESM fields
shost, dvchost	Host
Dpt	Protocol
src, dvc	Source IP
Dst	Destination IP
Spt	Source Port
Dpt	Destination Port
smac	Source MAC
dmac	Destination MAC
rt, start, end, tstamp, collection	First Time, Last Time
Cnt	Event Count
Name (CEF Header)	Message
Severity (CEF Header)	Severity
dproc	Application
sntdom	Domain
fname, spriv	Object
suser	Source User
duser	Destination User
request	URL
Compliance Status, cs1	Message_Text
filePath	Subject

Fortinet FortiGate

Contents

Configure Fortinet FortiGate using the command line interface

The preferred format is space-delimited logs, but you can also use comma-separated logs.

Task

- Enter these 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
```

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, see *FortiOS™ Handbook Logging and Reporting for FortiOS 5.0* under the section, *Advanced Logging*.

Configure Fortinet FortiGate UTM through the Management Console

The preferred format is space-delimited logs, but you can also use comma-separated logs.

Task

1 Go to **Log&Report** | **Log Config** | **Log Setting**, then select **Syslog**.

2 Expand the **Options** section to set any custom logging options, then enter this information in the corresponding fields:

- **Name/IP**—Enter the host name or IP address of the McAfee Event Receiver.
- **Port**—Set the port to **514**.
- **Level**—Set the level of logging.
- **Facility**—Leave the default value.
- **Enable CSV**—Leave this box deselected.

3 Click **Apply**.

Add Fortinet FortiGate UTM

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Fortinet
Data Source Model	FortiGate UTM – Space Delimited – (ASP)
Data Format	Default
Data Retrieval	Default
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	Default
Require Syslog TLS	Leave unchecked
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Fortinet FortiGate UTM events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a Fortinet FortiGate UTM device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

Fortinet FortiMail

Contents

Configure Fortinet FortiMail

Task

1 Go to **Log and Report** | **Log Settings** | **Remote Log Settings**.

The **Remote Log Settings** tab is displayed.

Table 4-1 Option definitions

Option	Definition
Enabled	Select to enable remote storage on the server.
ID	Displays the remote host ID.
Server	Displays the IP address of the syslog server.
Port	Displays the port on the syslog server.
Level	Displays the minimum severity level for logging.
Facility	Displays the facility identifier that the FortiMail unit uses to identify itself.

2 Select **Enabled** to allow logging to a remote host, then, in **Profile name**, enter a profile name.

3 In **IP**, enter the IP address of the syslog server where FortiMail stores the logs.

4 In **Port**, enter `514` for syslog (default is UDP).

5 In **Level**, select the severity level that a log message must equal or exceed to be recorded to this location.

6 In **Facility**, select the facility identifier that the FortiMail unit uses to identify itself when sending log messages.

7 To easily identify log messages from the FortiMail unit, enter a unique facility identifier, then verify that no other network devices use the same facility identifier.

8 Enable **CSV format** to send log messages in comma-separated value (CSV) format.

9 In **Logging Policy Configuration**, enable the types of logs that you want to record to this storage location, then click **Create**.

Add Fortinet FortiMail

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Fortinet**
Data Source Model	**Fortimail**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Fortinet FortiMail events to McAfee fields

Log sample

Here are sample logs from a device.

Statistics:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=Admin pri=Critical user=admin ui=192.0.2.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=syst
```

Config:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=config pri=information user=admin ui=203.0.113.0 module=unknown submodule=unknown
msg="changed settings for 'log setting local'"
```

System:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=System pri=Warning user=admin ui=203.0.113.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=system
submodule=interface msg="DNS: Connection timed out. No servers could be reached."
```

Update:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=Update pri=Warning user=admin ui=203.0.113.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=system
submodule=interface msg="Update result: virusdb:<yes|no>, avengine:<yes|no>, spamdb:<yes|
no>, asengine:<yes|no>
```

SMTP:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=SMTP pri=Warning user=admin ui=203.0.113.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=system
submodule=interface msg= “Starting flgrptd”
```

Admin:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=Admin pri=Critical user=admin ui=203.0.113.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=system
submodule=interface msg=“User <user_name> login successfully from {GUI(<ip_address>) |
console|SSH(<ip_address>)|telnet(<ip_address>)}”
```

HA:

```
date=2015-08-09 time=10:30:31 device_id=FE100C3909600504 log_id=0004001036 type=event
subtype=ha pri=notice user=ha ui=ha action=none status=success msgs=“monitord: main loop
starting, entering MASTER mode”
```

Webmail:

```
date=2015-08-09 time=12:42:48 device_id=FE100C3909600504 log_id=0000000920 type=event
subtype=Webmail pri=Warning user=admin ui=203.0.113.0 module=unknown submodule=unknown
user=<user_ name> ui={console|SSH(<ip_address>)|telnet(<ip_address>)} module=system
submodule=interface msgs=“User <user_name> from <IP address> logged in.”
```

Antivirus:

```
date=2015-07-24 time=17:07:42 device_id=FE100C3909600504 log_id=0100000924 type=virus
subtype=infected pri=information from="syntax@www.ca" to="user2@1.ca" src=203.0.113.0
session_id="q6OL7fsQ018870-q6OL7fsR018870" msg="The file inline-16-69.dat is infected with
EICAR_TEST_FILE."
```

Antispam:

```
date=2015-07-20 time=14:33:26 device_id=FE100C3909600504 log_id=0300000924 type=spam
pri=information session_id="q6KIXPZe008097-q6KIXPZf008097" client_name="[203.0.113.0]"
dst_ip="203.0.113.1" endpoint="" from="syntax@www.ca" to="user1@1.ca" subject="Email with
wd, excel, and rtf test" msg="Detected by BannedWord test"
```

Encryption:

```
date=2015-08-09 time=10:45:27 device_id=FE100C3909600504 log_id=0400005355 type=encrypt
pri=information session_id="q79EiV8S007017-q79EiV8T00701700001474" msg="User user1@1.ca read
secure message, id:'q79EiV8S007017-q79EiV8T00701700001474', sent from: 'user2@2.ca', subject:
'ppt file'"
```

Mappings

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

Log fields	McAfee ESM fields
Date/Time	First Time, Last Time
dst_ip	Destination IP

Log fields	McAfee ESM fields
Src	Source IP
Pri	Severity
client_name	Domain, Source IP
session_id	Message_ID
user	Source User, Destination User
To	To
from	From
direction	Direction
domain	Domain
virus	Threat_Name
subject	Subject
log_id	External_EventID
device_id	External_SessionID
mailer	Application
Dictionary	Category
hash	File_Hash
File	Filename
clientname, host	Host
interface	Interface
group	Group_Name
message	Message_Text, Rule Message
Pid	PID
daemon	Process_Name
proto	Protocol
reason	Reason
System White List	Reputation_Server_IP
Score	Spam_Score
URL	URL
alias	User_Nickname

Fortinet FortiManager

Contents

Configure Fortinet FortiManager

Task

1 Go to **System Settings** | **Advanced** | **Syslog Server**.

2 Select **Create New** to open the **New Syslog Server** window.

3 Fill in the **Name**, for example, McAfee ESM.

4 Fill in the **IP address** or **FQDM** of the McAfee Event Receiver.

5 Enter the **Port** number. The default is 514.

Add Fortinet FortiManager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Fortinet
Data Source Model	FortiManager (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Fortinet FortiManager events to McAfee fields

Log format

The expected format for this device is:

```
date=<date> time=<time> devicename=<devicename> deviceID=<deviceID> logID=<logID>
type=<type> subtype=<subtype> priority=<priority> user=<user> message=<message>
firmware=<firmware> type=<type> version=<version>
```

Log sample

This is a sample log from a Fortinet FortiManager device:

```
<123>date=2001-01-01time=12:01:01,devname=device,device_id=ABC123,
log_id=0123456789,type=example,subtype=example,pri=example,user=username; msg="Message Text;
firmware=12345678; type=ABCD1234; version=1.0
```

Mappings

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

Log fields	McAfee ESM fields
timestamp	First Time, Last Time
user	Source User
pri, level	Severity
devname	Host
log_id	Object
subtype	Application

Fortscale User and Entity Behavior Analytics (UEBA)

Contents

Configure Fortscale User and Entity Behavior Analytics (UEBA)

Task

1 From the main **Fortscale** interface, navigate to **System Configuration** | **System** | **Alert Forwarding via Syslog**.

2 Toggle **Enable Forwarding** to **Yes**.

3 For **Forwarding Type**, select **Alerts**.

4 In the **IP** field,enter the IP address for the McAfee Event Receiver.

5 In the **Port** field, type the port where the McAfee Event Receiver is listening. Default is **514**.

6 Under **Selective Forwarding: Alert Severity**, check which alert severities to forward.

7 Under **Selective Forwarding: User Tags**, check which tags to filter for forwarded events.

8 Click **Apply**.

Add Fortscale User and Entity Behavior Analytics (UEBA)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Fortscale**
Data Source Model	**Fortscale UEBA**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Fortscale User and Entity Behavior Analytics (UEBA) events to McAfee fields

Log format

The expected format for this device is:

```
<PRI>DATE TIME HOSTNAME -: KEY: VALUE KEY: VALUE KEY: VALUE…
```

Log sample

This is a sample log from a device:

```
<123>Jan 01 01:01:01 demo.fortscale.com -: Alert URL: https://demo.fortscale.dom Alert Name:
data_exfiltration_normalized_username_daily Start Time: 978336061 End Time: 978336061 Entity
Name: someName Entity Type: User Severity: Critical Alert Status: Open Comment:
```

Mappings

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

Log fields	McAfee ESM fields
Alert URL	URL
Alert Name	Message

Log fields	McAfee ESM fields
Start Time	First Time, Last Time
Entity Name	Source User, External_Device_Name
Entity Type	Object_Type
Severity	Severity
Alert Status	Status
Comment	Message_Text

FreeRADIUS

Contents

Configure FreeRADIUS

Task

1 In the **/etc/freeradius/radius.conf** file, make these changes:

```
logdir = syslog
Log_destination = syslog
log {
destination = syslog
syslog_facility = daemon
stripped_names = no
auth = yes
auth_badpass = no
auth_goodpass = no
}
```

2 Make this addition to **/etc/syslog.conf**:

```
# .=notice will log only authentication messages (L_AUTH)
example1.=notice @10.10.3.21
# .=err will log only module errors for radius
example1.=err @10.10.3.21
```

where 10.10.3.21 is the IP address or host name of the McAfee Event Receiver, and “example1” is the facility to be used with FreeRADIUS in the next step.

3 Set up FreeRadius to run with these options:

```
-l syslog
-g example1
```

where “example1” is the facility name that you have chosen to use.

Add FreeRADIUS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	FreeRADIUS
Data Source Model	FreeRADIUS (ASP)
Data Format	Default
Data Retrieval	Default
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Unchecked
Support Generic Syslogs	Default
Time Zone	Time zone of data being sent

FreeRADIUS events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a FreeRADIUS device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

Gigamon GigaVUE

Contents

Configure Gigamon GigaVUE

The syslog configuration is done at the command line. See your product documentation for instructions about how to access and use the command line.

Task

- From the command line, enter:

```
config syslog_server host 192.0.2.1
```

  where 192.0.2.1 is the IP address of the McAfee Event Receiver.

Add Gigamon GigaVUE

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Gigamon
Data Source Model	GigaVUE (ASP)
Data Format	Default
Data Retrieval	Syslog (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Gigamon GigaVUE events to McAfee fields

Log format

```
<priority>Original Address=<IP address> <date time> <hostname> <application> <message>
```

Log samples

This is a sample log from a Gigamon GigaVUE device:

```
<123>Original Address=192.0.2.1 Jan  1 01:01:01 hostname application: Packet Drop port 12
drop 123 packets
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Host
Application	Application
Original Address	Source IP
Interface Port Number	Object
Date Time	First Time, Last Time

Globalscape Enhanced File Transfer

Contents

Configure Globalscape Enhanced File Transfer

Before you begin

See the Globalscape Enhanced File Transfer (EFT) documentation for configuration instructions. Specific details can be located in the **EFT Logging and Visibility** | **Log Format, Type, and Location** section. Ensure that the default logging settings are used for proper parsing.

The McAfee Collector is used to send the Globalscape logs to McAfee ESM. See the McAfee Collector documentation for configuration help.

Task

1. In the administration interface, connect to EFT, then click the **Server** tab.
2. Click the **Server** node, set the log level to **Diagnostic**, then select **Generic log tail** for the client.
3. In the right pane, click the **Logs** tab.
4. In **Log File Settings** folder in which to save log files box, type the path to the directory in which to save this server's log files. To browse for a path, click the folder icon.
5. In the Log file format list, click W3C Extended, Microsoft IIS, NCSA Common, or No Logging.

   The McAfee Collector is used to send the Globalscape logs to McAfee ESM. See the McAfee Collector documentation.

6. Under the McAfee Collector, set the log level to Diagnostic.
7. Select Generic log tail for the client.

   If a Host ID is used, you must use this same Host ID when creating the data source on the McAfee Event Receiver.

8. Verify that the client is enabled, then apply the changes.

Add Globalscape Enhanced File Transfer

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Globalscape**
Data Source Model	**Enhanced File Transfer (EFT)**
Data Format	**Default**
Data Retrieval	**McAfee Event Format (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Host ID	Name of the host ID in the McAfee Collector, if a Host ID was entered.
Use encryption	Checked if encryption was selected in the McAfee Collector.

Globalscape Enhanced File Transfer events to McAfee fields

Log format

The expected format for this device is:

```
computer timestamp IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log samples

This is a sample log from a <Product Name> device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
timestamp	First Time, Last Time
c-ip	Source IP
c-port	Source Port
cs-username	Source User
cs-method	Command
cs-uri-stem	Message_Text
sc-bytes	Bytes_from_Server
cs-bytes	Bytes_from_Client
s-name	Destination_Hostname
s-port	Destination Port

HBGary Active Defense

Contents

Configure HBGary Active Defense

Task

1. Log on to the Active Defense Management Console.
2. Navigate to **Settings** | **Alerts**.
3. In the **Alerts** window, click **Add Route** to open the Router Editor.
4. Enter a name to identify the McAfee Event Receiver into **Route Name**.
5. In the **Settings** area, enter the IP address of the McAfee Event Receiver into the **Host** field.
6. In the **Port** field, enter **514** (the default port for syslog).
7. In the **Events** area, select the events to be sent to the McAfee Event Receiver.
8. Click **OK** to save and exit.

Add HBGary Active Defense

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**HBGary**
Data Source Model	**ActiveDefense (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Dafault)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

HBGary Active Defense events to McAfee fields

Log format

The expected format for this device is:

```
<priority> <date> <time> <hostname> <process>[ID]:LEEF:<version>|<vender>|<product>|
<version>|<event ID>| <key>=<value> <key>=<value> <key>=<value> …
```

Log samples

This is a sample log from a HBGary Active Defense device:

```
<123> 2001-01-01T01:01:01Z hostname process[1234]:LEEF:1|HBGary|Active Defense|1.2.3|Login|
sev=0 user=admin dstHost=hostname dst=192.0.2.1 message=Logged In
```

Mappings

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

Log fields	McAfee ESM fields
srcHost	Host
Event ID	Application
src	Source IP
dst	Destination IP
message	Message
result	Event Subtype
sev	Severity

Hewlett-Packard 3Com Switches

Contents

Configure Hewlett-Packard 3Com Switches

See the product documentation for information about how to send syslog events to a remote syslog server or McAfee ESM.

Add Hewlett-Packard 3Com Switches

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Hewlett-Packard
Data Source Model	3Com Switches (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Hewlett-Packard 3Com Switches events to McAfee fields

Log format

The expected format for this device is:

```
<device IP> <date time> <application> <message> <username> <source IP> <object>
```

Log samples

This is a sample log from a Hewlett-Packard 3Com Switch device:

```
[192.0.2.1] <123>Jan  1 01:01:01 1234 1234G %%10VTY/5/VTY_LOG(l):- 1 - TELNET user username
in group failed to login from 192.0.2.2(a1b2-c3d4-e5f6) on interface.
```

Mappings

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

Log fields	McAfee ESM fields
Application	Application
Command	Command
Source IP Address	Source IP
MAC Address	Source MAC
User	Source User
Task	Object

Hewlett Packard LaserJet Printers

Contents

Configure Hewlett Packard LaserJet Printers

See documentation for information about how to send syslog events to a remote syslog server or McAfee ESM. Configure the printer to send syslog events to the IP address of the McAfee Event Receiver.

Add Hewlett Packard LaserJet Printers

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Hewlett-Packard
Data Source Model	LaserJet Printers (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Hewlett Packard LaserJet Printers events to McAfee fields

Log format

The expected format for this device is:

```
<severity> <hostname> <message>
```

Log sample

This is a sample log from a Hewlett-Packard LaserJet Printers device:

```
<13> printer: paper out
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Host

Hewlett-Packard ProCurve

Contents

Configure Hewlett-Packard ProCurve

The syslog configuration is performed at the command line. See the ProCurve documentation provided by Hewlett-Packard for more information about how to access and use the command line interface.

Task

- Enter this command to add a syslog server:

  ```
  logging <ip_address>
  ```

  Replace <ip_address> with the IP address of the McAfee Event Receiver.

Add Hewlett-Packard ProCurve

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

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

Option	Definition
Data Source Vendor	**Hewlett-Packard**
Data Source Model	**ProCurve (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Hewlett-Packard ProCurve events to McMcAfee ESM fieldsAfee fields

Log format

The expected format for this device is:

```
<date time> <device name> <message>
```

Log sample

This is a sample log from a Hewlett-Packard ProCurve device:

```
Jan 01 01:01:01 procurve.com/ procurve.com ABC_1234, Interface ethernet 1/01, state up
```

Mappings

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

Log fields	McAfee ESM fields
Application	Application
IP Protocol	Protocol
Source IP	Source IP
Destination IP	Destination IP
Source IP	Source Port
Destination Port	Destination Port
Action / State	Event Subtype

HyTrust Appliance

Contents

Configure HyTrust Appliance

Task

1. Open the HyTrust Appliance application.
2. Navigate to **Configuration** | **Logging**.
3. Select **Capture** from the **Logging Level** drop-down list.
4. In the **HTA Logging Aggregation** field, select **External**.
5. Select **Proprietary** in the **Logging Aggregation Template Type** field.
6. In the **HTA Syslog Servers** field, type the IP address or host name and port number of the McAfee Event Receiver, using this format:

   ```
   IPaddress:port
   ```

   -or-

   ```
   hostname:port
   ```

7. Ensure **Encrypt Syslog** is empty.
8. Click **Apply**.

Add HyTrust Appliance

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**HyTrust**
Data Source Model	**Appliance (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	leave default (32)
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

HyTrust Appliance events to McAfee fields

Log format

The expected format for this device is:

```
<PRI> Date HTA-FQDN Facility:Error_Type : HTA-log-message-code Source: src_ip Msg
```

Log sample

This is a sample log from a HyTrust Appliance device:

```
<174>Feb 15 19:17:44 hta3a.testdrive.hytrust.com local5:INFO : ARC0005I Job scheduled to run
Feb 15, 2012 7:17:44 PM on 10 1.652.04.1 0 is started at Feb 15, 2012 7:17:44 PM.
```

Mappings

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

Log fields	McAfee ESM fields
HTA-log-message-code	Message_ID.Message_ID

IBM

Contents

Configure IBM Guardium

Task

1 From the Guardium CLI command line, enter this command:

```
store remote log add daemon.* 192.168.2.1 tcp
```

where 192.168.2.1 is the IP address of the McAfee Event Receiver.

2 Log on to the Guardium UI with admin permissions.

3 Select the **Administration Console** tab.

4 Navigate to **Configuration** and select **Global Profile.**

5 In the **Message Template** text area, enter one of these options.

- Standard syslog format:

```
<pri>Date Time Username Application[pid]: Alert based on rule ID
                    ruleDescription|Category:
                    category|Classification:
                    classification|Severity
                    severity|Rule #
                    ruleID [ruleDescription ]|Request Info: [Session start:
                    sessionStart]|Server Type:
                    serverType|Client IP
                    clientIP|ServerIP:serverIP|Client PORT:
                    clientPort|Server Port:
                    serverPort|Net Protocol:netProtocol|DB Protocol:
                    DBProtocol|DB Protocol Version:
                    DBProtocolVersion|DBUser:
                    DBUser|Application User Name
                    AppUserName|Source Program:
                    SourceProgram|Authorization Code:
                    AuthorizationCode|Request Type:
                    requestType|Last Error:
                    lastError|SQL:
                    SQLString|To add to baseline:
                    addBaselineConstruct
```

- CEF format:

```
CEF:0|IBM|Guardium|7.0|%%ruleID|%%ruleDescription|5|rt=%%receiptTimeMills cs1=%
%severity cs1Label=Severity cs2=%%serverType cs2Label=Server Type cs3=%%classification
cs3Label=Classification cat=%%category app=%%DBProtocol cs4=%%DBProtocolVersion
cs4Label=DB Protocol Version suser=%%AppUserName sproc=%%SourceProgram act=%
%requestType start=%%sessionStartMills externalId=%%violationID duser=%%DBUser dst=%
%serverIP dpt=%%serverPort src=%%clientIP spt=%%clientPort proto=%%netProtocol msg=%
%SQLString
```

Add IBM Guardium

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**IBM**
Data Source Model	**Guardium**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

IBM Guardium events to McAfee fields

Log format

The expected syslog format for this device is:

```
<pri>Date Time Username Application[pid]: Alert based on rule ID ruleDescription|Category:
category|Classification: classification|Severity severity|Rule # ruleID [ruleDescription ]|
Request Info: [Session start: sessionStart]|Server Type: serverType|Client IP clientIP|
ServerIP:serverIP|Client PORT: clientPort|Server Port: serverPort|Net Protocol:netProtocol|
DB Protocol: DBProtocol|DB Protocol Version: DBProtocolVersion|DBUser: DBUser|Application
User Name AppUserName|Source Program: SourceProgram|Authorization Code: AuthorizationCode|
Request Type: requestType|Last Error: lastError|SQL: SQLString|To add to baseline:
addBaselineConstruct
```

The expected CEF format for this device is:

```
CEF:0|IBM|Guardium|8.0|%%ruleID|%%ruleDescription|5|rt=%%receiptTimeMills cs1=%%severity
cs1Label=Severity cs2=%%serverType cs2Label=Server Type cs3=%%classification
cs3Label=Classification cat=%%category app=%%DBProtocol cs4=%%DBProtocolVersion cs4Label=DB
Protocol Version suser=%%AppUserName sproc=%%SourceProgram act=%%requestType start=%
%sessionStartMills externalId=%%violationID duser=%%DBUser dst=%%serverIP dpt=%%serverPort
src=%%clientIP spt=%%clientPort proto=%%netProtocol msg=%%SQLString
```

Log sample

This is a sample syslog log from an IBM Guardium device:

```
<13>Jan 01 01:01:01 usr123456 guard_sender[0001]: Alert based on rule ID log full sql - US
DBAs Oracle#012Category:   Classification:    Severity INFO  #012Rule # 20251 [log full
sql - US DBAs Oracle ]#012Request Info: [ Session start: 2001-01-01 01:01:01 Server Type:
ORACLE Client: 192.0.2.1 (DEVICENAME1000) Server: 192.0.2.1 (DEVICENAME1000) Client PORT:
0001 Server Port: 0 Service Name: SERVICEOAX1111 Net Protocol: NetProtocolName Protocol:
ProtocolName Protocol Version: 9.99 User: sys#012Application User Name  :PU=SYS#012Source
Program: Application Authorization Code: 0 Request Type: BIND_DATA Last Error: #012SQL:
begin sys . command_name . Command_Name ( l0row_id => 11111 , l0row_stamp => 22222222 ,
row_id => 11111 , row_stamp => 22222222 , txt => 'backup piece handle=/Filepath/ recid=11111
stamp=22222222' , sameline => 0.00 ) ; end ;#012 To add to baseline:
```

This is a sample CEF log from an IBM Guardium device:

```
<13>Jan  1 01:01:01 usr123456 guard_sender[0001]: CEF:0|IBM|Guardium|8.0|20322|log full
sql - US DBAs MSSQL|5|rt=1420074061000 cs1=INFO cs1Label=Severity cs2=MS SQL SERVER
cs2Label=Server Type cs3= cs3Label=Classification cat= app=TDS cs4=8.0 cs4Label=DB Protocol
Version suser= sproc= act=SQL_RPC start=1420074061000 externalId=123456789 duser=user2
dst=10.10.10.10 dpt=1234 src=10.10.10.11 spt=1234 proto=TCP msg= [ISDB].[dbo].
[sp_ISDB_Obj_AD_AuditEvents_Insert] 'user2','usr123456','Logoff','AMC'
```

Mappings

This table shows the mappings between the data source and McAfee ESM.

Log fields	McAfee ESM
Application	Application
Severity	Severity
ClientIP	Source IP
ClientPort	Source Port
ServerIP	Destination IP
ServerPort	Destination Port
DB user	Source User
Application User	Destination User
Net Protocol	Protocol
Category	Category
Server	Destination_Hostname
ExternalID	External_EventID
Partition	File_Path
Time, Start, Session Start	First Time, Last Time
Host	Host
msg	Message_Text, Rule Name, SQL_Statement
ObjectID	Object
PID	PID
Rule #	Policy_ID
Rule Name	Policy_Name
sproc	Process_Name
Act, Request Type	Request_Type

Log fields	McAfee ESM
SID	Signature ID
SQL	SQL_Statement

Configure IBM Websphere Application Server

By default, basic logging is enabled in IBM WebSphere Application Server. However, you can also change the log level settings to produce higher and lower volumes of logs based on the log severity level (for example, fatal, severe, warning, detail, and all).

All logging levels are supported. For more information about how to change the log level settings, see the product documentation provided by IBM for your version of WebSphere Application Server.

Add IBM Websphere Application Server

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**IBM**
Data Source Model	**WebSphere Application Server**
Data Format	**Default**
Data Retrieval	**SCP**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Port	22
Number of lines per record	1
File copy timeout	30
Login timeout	30
Interval	5
File Completion	15 seconds
Delete processed files	Select to delete processed logs.
Path	The path to the log files. In Linux, UNIX, AIX, and Solaris, the default path is: "/opt/IBM/WebSphere/AppServer/profiles/**name_of_profile**/logs/**server1**" In Windows, the default path is: "C:\IBM\WebSphere\AppServer\profiles**name_of_profile**\logs**server1**" where "**name_of_profile**" is the profile name of the IBM InfoSphere Information Server instance, and "**server1**" is the instance name of the application server.
Wildcard expression	System*.log
Username	The logon for the computer that runs the server (a user name with sufficient permissions on the server running IBM WebSphere Application Server).
Password	The password for the specified user name.
Time Zone	Time zone of data being sent.
Support Generic Syslogs	**Do nothing**

5 Test the connection. If the test returns "test connection successful", the device is configured correctly.

IBM Websphere Application Server events to McAfee fields

Log format

Here is the basic logging format listed in the IBM documentation. The advanced logging format and tracing logs are not currently supported. The expected format for this device is:

```
<timestamp><threadId><shortName><eventType>[className][methodName]<message>
```

Log sample

This is a sample log from an IBM Websphere Application Server device:

```
[5/25/15 23:24:25:123 EDT] 00000001 BatchSensorCo I   CWLRB5903I: BatchSensorComponent
initialized successfully.
```

Mappings

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

Log fields	McAfee ESM fields
timestamp	First Time, Last Time
threadId	External_SessionID
shortname	Message (modified by data source rules)
shortname (hashed)	Signature ID
eventType	Severity
classname	External_Application
methodName	Method
Set by DSR	Event Subtype

IBM Websphere Application Server supported facilities

These facilities are currently supported, and provide more descriptive information when parsed by the McAfee ESM.

```
ACIN, ACWA, ADFS, ADMC, ADMN, ADMR, ASYN, CHFW, CNTR, CSCP, CWLDD, CWLRB, CWLRS, CWNEN,
CWOAU, CWPKI, CWPMI, CWRCB, CWRLS, CWSCT, CWSID, CWSIU, CWWJP, CWXRS, DYNA, FFDC, HMGR,
I18N, IVTL, NMSV, OBPL, PLGC, RASD, SCHD, SECJ, SESN, SRVE, STUP, TCPC, TRAS, UTLS, WACS,
WAR, WKSP, WMSG, WSSC, WSVR, WSWS, WTRN
```

Infoblox NIOS

Contents

Configure Infoblox NIOS

Task

1 Do one of the following:

- From the **Grid** perspective, click **grid** | **Edit** | **Grid Properties**
- From the **Device** perspective, click **hostname** | **Edit** | **Device Properties**

2 In the **Grid** or **Device** editor, click **Monitoring**, then define these options.
   - **Enable external syslog server**: Select this to enable the Infoblox device to send messages to the specified syslog server.
   - **Syslog Server Group**: To define one or more syslog servers click **Add**, enter the following, then click **OK**:
     - **Server Address**: Enter the IP address of the syslog server.
     - **Connection Type:** Specify whether the device uses TCP or UDP to connect to the external syslog server.
     - **Port:** Specify the destination port number (standard port is 514).
     - **Out Interface:** Specify the interface where the device sends syslog messages to the syslog server.
     - **Severity Filter:** Select a filter from the drop-down list.
     - **Message Source:** Specify which syslog messages the device sends to the external syslog server:
       - **Internal:** Device sends the syslog messages that it generates.
       - **External:** Device sends the syslog messages that it receives from other devices, such as syslog servers and routers.
       - **Any:** Device sends both internal and external syslog messages.
     - **Copy audit log messages to syslog:** Select the Infoblox device to include audit log messages with the messages it sends to the syslog server. This function can be helpful to monitor administrative activity on multiple devices from a central location.
     - **Audit Log Facility:** Select the facility where you want the syslog server to sort the audit log messages.
3 Click the **Save** icon to save your settings.

Add Infoblox NIOS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.
2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Infoblox**
Data Source Model	**NIOS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Configure Syslog for a grid member

Task

1 From the Grid perspective, click **+** (for *grid*) -> **+** (for **Members**) -> *member* -> **Edit** -> **Member Properties**.

2 In the *Grid Member* editor, click **Monitoring**, then define these options.

- **Override grid syslog settings:** Select to override grid-level syslog settings and apply member-level settings.
- **Enable external syslog server:** Select to enable the Infoblox device to send messages to a specified syslog server.
- **Syslog Server Group:** To define one or more syslog servers, click **Add**, enter the following, and then click **OK**:
  - **Server Address:** Type the IP address of a syslog server.
  - **Connection Type:** Specify whether the device uses TCP or UDP to connect to the external syslog-server.
  - **Port:** Specify the destination port number.
  - **Out Interface:** Specify the interface where the device sends syslog messages to the syslog server.
  - **Severity Filter:** Choose a filter from the drop-down list.
- **Message Source:** Specify which syslog messages the device sends to the external syslog server:
  - **Internal:** The device sends the syslog messages that it generates.
  - **External:** The device sends the syslog messages that it receives from other devices.
  - **Any:** The device sends both internal and external syslog messages.
- **Enable syslog proxy:** Select to enable the device to receive syslog messages from other devices, such as syslog servers and routers, then forward these messages to an external syslog server.
- **Enable listening on TCP:** Select if the device uses TCP to receive messages from other devices.
  - **Port:** Enter the port number where the device receives syslog messages from other devices.

- **Proxy Client Access Control:** Click **Add**, enter the following in the *Access Control* Item dialog box, then click **OK:**
  - **IP Address option:** Select **IP Address** to add the IP address of a device, or select **Network** to add the network address of a group of devices.
    - **Address:** Enter the IP address of the device or network.
    - **Subnet Mask:** If you entered a network IP address, you must also enter its subnet mask.

3 Click the **Save** icon to save your settings.

InterSect Alliance Snare for Windows

Contents

Configure InterSect Alliance Snare for Windows

Task

1 In the Windows Start menu, navigate to the **Intersect Alliance** folder in the programs listing, then open **Snare for Windows**. The open-source version of the software includes *Open Source* in the title. This opens your default browser and takes you to a web interface running on the local host.

2 In the upper left, click **Network Configuration**.

3 In the **Destination Snare Server address** field, enter the IP address of your McAfee Event Receiver.

4 In the **Destination Port** field, enter the port number used for sending syslog to your McAfee Event Receiver *(default is 514).*

5 Select **Enable SYSLOG Header?** to have syslog headers included with events.

6 (Optional) If using the Enterprise version of Snare, you can use the Coordinated UTC feature. This changes the time stamps in the logs to UTC. If you enable this feature, you must set the time zone for this data source in McAfee ESM to Greenwich Mean Time.

7 Click **Change Configuration** when done.

Add InterSect Alliance Snare for Windows

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**InterSect Alliance**
Data Source Model	**Snare for Windows (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent (Greenwich Mean Time if using the Coordinated Universal Time feature in Snare).

The Open Source version of Snare does not support coordinated UTC. Events delivered by Snare, contain time stamps based on the time zone of the localhost from which they were sent. For coordinated UTC support, use the Enterprise version of Snare for Windows.

InterSect Alliance Snare for Windows events to McAfee fields

Log format

```
Hostname Event Log Type Criticality SourceName Snare Event Counter DateTime EventID
SourceName UserName SIDType EventLogType ComputerName CategoryString DataString
ExpandedString MD5 Checksum
```

Log samples

This is a sample log from Snare for Windows:

```
Test_Host MSWinEventLog 0 Security 3027 Fri May 24 09:30:43 2013 593
Security Administrator User Success Audit EXAMPLE Detailed
Tracking A process has exited:Process ID: 656 User Name:
Administrator Domain: EXAMPLE Logon ID: (0x0,0x6C52)
```

Mappings

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

Log fields	McAfee ESM fields
Hostname, Caller Machine Name, Caller Workstation, Client Name, from Workstation, Source Workstation, Target Server Name, User Workstations, Workstation Name	Host
Criticality	Severity
Source, Client Address, Source Network Address, Network Address	Source IP
Source Port	Source Port

Log fields	McAfee ESM fields
Destination	Dest. IP
SourceName	Application
Logon Type	Logon_Type
Domain, Caller Domain, Domain Name, Member ID, New Domain, Primary Domain, Supplied Realm Name, Target Domain, User Domain, Account Domain	Domain
Authentication Package Name, Authentication Package, Logon Process Name, Process Name, Service Name	Application
Object Name, Group Name, Target Account Name, Program	Object
UserName, User Name, Caller User Name, Client User Name, Logon Account, Account Name, UserID	Source User
New Account Name, Member Name, Target Account Name, Account Name	Destination User
Failure Code	Command
NtLogon	Session_Status
Logon Type	Logon_Type
EventID and SourceName	Signature ID
EventLogType	Event Subtype

Interset

Contents

Configure Interset

With a fully configured and working Interset and McAfee ESM solution, this information is required.

- Familiarity with configuring Flume using Ambari. See the Configure Data Ingest documentation.
- The tenant ID in Interset that contains the data to send to the McAfee Event Receiver ESM (for example, 0).
- The name (FQDN or IP address) and port of the McAfee Event Receiver.

Task

1 In Apache Ambari, create the Flume Export Configuration Group.

2 Configure the system so that events are sent as Syslog to the McAfee Event Receiver.

a Copy the esmSyslog.conf file from the /opt/interest/export/conf-templates folder to a local system, and make these substitutions:

- On each line, change the tenant ID <TID> to the appropriate tenant ID (for example, 0).
- Change the ESM McAfee Event Receiver location <ESM Syslog Receiver Port> with the port number of the McAfee Event Receiver.
- Replace any other system variables, such as <ZOOKEEPER_HOST>, with appropriate values.

b Upload and save the new esmSyslog.conf file to Ambari for processing.

3 Repeat step 2 with esmStorySyslog.conf, located in the same template folder, to also send high risk stories to the McAfee Event Receiver. By default, only stories with a risk score greater than 75 are sent. To change this behavior, change the value in the following line as needed:

```
interset_auth_events_<TID>_esm.sources.kafkaSource.interceptors.scoreChecker.toCompare =
riskScore:greaterThan:75
```

Add Interset

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Interset**
Data Source Model	**Interset**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Integrate Interset

An integration feature enables additional details involving Interset events displayed in the McAfee ESM.

This integration feature only works with events that contain the URL custom type. Ensure that the data source has been configured and that the data source has been added to the McAfee Event Receiver before completing these steps.

Task

1 In the McAfee ESM console, select an ESM on the left side, then click the **Properties** icon.

2 From the **System Properties** menu, select **Custom Settings**.

3 Near the bottom of **Custom Settings**, click **Device Links**.

4 In the **Custom Device Links** window, select the Interset device that you previously added, then select **Edit**.

5 In the **Edit URL** window, click the **arrow** directly to the right of the blank URL field. Select **Custom Types** | **URL**.

Once selected, a value is automatically entered in the previously blank **URL** section.

6 The **Custom Device Links** window now displays the CustomType value. Select **OK**.

7 Select an event that contains the URL custom type, then select the **Launch Device URL** icon (an image of the Earth).

Once the **Launch Device URL** is selected, a browser window displays a logon prompt for your Interset device. Once logged on, additional details about the selected Interset event in the ESM are displayed.

Interset events to McAfee fields

Log sample

This is a sample log from an device:

```
On Jan 21, 2016 8:00:00 AM, user543 told a Story with a Risk Score of 88. See 'https://
analytics.example.com/investigator#/?
t=story&type=story&ts=1414746760&te=1417392000&state=stories' for details. It was very
unusual for user543 to take from the projects /project0871, /project0156, /project0589, /
project0473, /project0821, /project0221, /project0369. user543 mooched from the project /
project0263. user543 took from the inactive projects /project0833, /project0821, /
project0852. user543 took significantly more from the project /project0822 than others.
```

Mappings

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

Log fields	McAfee ESM fields
/timestamp, /clienteventtime, /_time, Time	First Time, Last Time
Username, /sourceuseridname, /user, /src_user	Source User
Message Details	Message_Text
Risk Score	Reputation, Severity
URL	URL
/appidname	Application
/eventuuid	UUID
/sourcemachineidname, /src	Host
/sourceip, /src, /ip	Source IP
/eventtype, /signature_id	Job_Type, SID
/fileidpath	Destination_Filename
/sourcepath	Filename
/contactip, /dest	Destination IP, Destination_Hostname
/action	Action, Rule Message
/dvc	External_Device_ID
/src_port	Source Port
/vendor	External_Device_Type
/project	Category
/size	File_Size

Juniper Networks JUNOS Structured-Data Format

Contents

Configure Juniper Networks JUNOS Structured-Data Format

JUNOS supports logging in standard Junos format and structured-data format. We recommend the structured-data format.

Structured-data format includes more information without significantly increasing log size. It also makes it easier for automated applications to extract information from a message. This format complies with Internet draft-ietf-syslog-protocol-23 (https://tools.ietf.org/html/draft-ietf-syslog-protocol-23).

These instructions apply to any JUNOS device running 10.3 or later. Some examples are EX, M, MX, PTX, QFX, QFabric, and T series systems.

Here is a basic setup example of sending logs to a remote syslog host:

```
[edit system]
syslog {
host <HOSTNAME/IP ADDRESS of McAfee Event Receiver> {
facility SEVERITY;
structured-data {
brief;
}
}
    }
```

Here is a basic setup example of sending logs to a log file:

```
[edit system]
syslog {
file <Path/Filename> {
facility SEVERITY;
structured-data {
brief;
}
}
  }
```

More options can be specified for log outputs. See the *JUNOS System Log Messages Reference* document to learn more.

Task

1 To configure the system to log system messages, add a **syslog** statement at the [edit system] hierarchy level.

2 To log in structured-data format, include a **structured-data** statement for each logging output.

Add Juniper Networks JUNOS Structured-Data Format

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Juniper Networks**
Data Source Model	**JUNOS – Structured-Data Format (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Juniper Networks JUNOS Structured-Data Format events to McAfee fields

Log format

The expected format for this device is:

```
<priority> version timestamp hostname process processID TAG [junos@2636.platform
variable-value-pair1=”value” message-text]
```

Log samples

This is a sample log from a JUNOS structured-data format device:

```
<165>1 2007-02-15T09:17:15.719Z router1 mgd 3046 UI_DBASE_LOGOUT_EVENT
[junos@2636.1.1.1.2.18 username="regress"]
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Hostname
Service-name	Application

Log fields	McAfee ESM fields
Source-address	Source IP
Destination-address	Destination IP
Nat-destination-address	Nat Details Nat Address
Source-port	Source Port
Destination-port	Destination Port
Nat-source-address	Nat Details Nat Address
Nat-source-port	Nat Details Nat Port
Packet-incoming-interface	Interface
Source-zone-name	Source Zone
Destination-zone-name	Destination Zone
Bytes-from-client	Bytes from client
Bytes-from-server	Bytes from server
Policy-name	Policy name
Elapsed-time	Elapsed time
Attack-name	Threat name
Protocol-id	Protocol
Session-id	Session
Reason	Object name
Username	Source Username

Juniper Networks NetScreen

Contents

Configure Juniper Networks NetScreen using the command-line interface

Task

- To configure Juniper Networks NetScreen using the command line, type the following commands:

```
Set syslog config <ip_address> <security_facility> <local_faciltiy>
Set syslog config <ip_address> port 514
Set syslog config <ip_address> log all
Set syslog enable
```

Add Juniper Networks NetScreen

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Juniper Networks**
Data Source Model	**NetScreen/IDP (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Juniper Networks NetScreen events to McAfee fields

Log format

The expected format for this device is:

```
<PRI>HOSTNAME: NetScreen device_id=HOSTNAME []EVENT_DESCRIPTION: MESSAGE (DATE TIME)
```

Log sample

This is a sample log from a device:

```
<123>JNHOST: NetScreen device_id=JNHOST [Root]system-warning-00515: Admin user BobJ has
logged on via SSH from 192.0.2.1:1234 (2001-01-01 01:01:01)
```

Mappings

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

Log fields	McAfee ESM fields
src, ip address	Source IP
src_port, port, icmp_type	Source Port
dst	Dest. IP

Log fields	McAfee ESM fields
dst_port, icmp_code	Dest. Port
proto	Protocol
src_zone	Source Username, Source_Zone
dst_zone	Dest Username, Destination_Zone
device_id	Host
Service	Application
Sent	Bytes_sent
Rcvd	Bytes_received
reason	Reason
domain	domain
start_time	First Time
start_time	Last Time
Severity	Severity
Session id	Session ID
policy id	Command
src-xlated ip	NAT Address
src-xlated ip (port)	NAT Port
policy id	Policy Name
deviceId	External_Device_ID
application	Application

Juniper Networks Network and Security Manager

Contents

Configure Juniper Networks Network and Security Manager

Task

1 From the **Network and Security Manager** application, go to **Action Manager** | **Action Parameters.**

2 Fill in **Syslog Server IP** with the IP address of the McAfee Event Receiver.

3 Select the **Syslog Facility** you want to send the events as.

4 Click **OK** to save.

Add Juniper Networks Network and Security Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Juniper Networks**
Data Source Model	**Network and Security Manager – NSM (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Juniper Networks Network and Security Manager events to McAfee fields

Log format

The expected format for this device is:

```
<Priority> <Date Time> <hostname> <message>
```

Log sample

This is a sample log from a Juniper Networks Network and Security Manager device:

```
<123>Jan  1 01:01:01 192.0.2.1 20010101, 1234, 2001/01/01 01:01:01, 2001/01/01 01:01:01,
domain.Name, 0, deviceName, 192.0.2.2, info, cmd, (NULL), (NULL), 192.0.2.3, 3, 192.0.2.4,
4, (NULL), (NULL), 192.0.2.5,50, 192.0.2.6, 6, protocol, SYSTEM, 0, unknown, none, 0, 0, not
applicable, informational, no,details, admin, file, (NULL), 0, 0, 0, 0, 0, 0, 0, 0, no, 0,
Not Set, service
```

Mappings

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

Log fields	McAfee ESM fields
Device Name	Host
Protocol	Protocol
Src Addr	Source IP
Dst Addr	Destination IP
Src Port	Source Port
Dst Port	Destination Port
Action	Action
Time Received	First Time, Last Time
Severity	Severity
Subcategory	Application
Bytes Out	Bytes_Sent
Bytes In	Bytes_Received
Details	Command
Device Domain	Domain
User	User
Nat Src Addr, Nat Src Port	NAT_Details
Policy	Policy_Name

Kaspersky Administration Kit

Contents

Configure Kaspersky Administration Kit

See your product documentation for instructions about sending log events to a remote server. Use the McAfee Event Receiver IP address for the IP address of the remote server.

Add Kaspersky Administration

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Kaspersky**
Data Source Model	**Administration Kit – SQL Pull (ASP)**
Data Format	**Default**
Data Retrieval	**SQL (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
User ID	User name of the Kaspersky database
Password	Password of the Kaspersky database
Port	1433
Database Name	Database name
Poll frequency	How often you want to pull logs.
Time Zone	Time zone of data being sent.

Kapersky Administration Kit events to McAfee fields

Log sample

This is a sample log from a Kaspersky Administration Kit device:

```
event_id="4164828" nIpAddress="167772161" domain_name="DOMAIN" hostname="HOSTNAME"
group_name="GROUPNAME" rise_time="2013-09-16 09:22:52.257" registration_time="2013-09-16
09:22:57.840" severity="1" task_display_name="Update_KBDOM-SRV_KAV6.0 MP4" description=""
product_name="KAVFS6" product_version="6.0.4.0" product_display_version="6.0.4.1611"
event_type="KLPRCI_TaskState" string_1="" string_2="" string_3="" string_4="" string_5=""
string_6="" string_7="" string_8=""
```

Mappings

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

Log fields	McAfee ESM fields
rise_time	First Time, Last Time
severity	Severity
product_name	Application
domain_name	Domain
hostname	Hostname
product_version	Version
event_type	Event_Class
nIpAddress	src_ip
File_Path*	File_Path
Threat_Name*	Threat_Name
task_display_name	Job_Name

Log fields	McAfee ESM fields
objectname*	objectname
URL*	URL
Message_Text*	Message_Text
Process_Name*	Process_Name
Category*	Category
PID*	PID

*Keys are found in string_ or in the description field

Lastline Enterprise

Contents

Configure Lastline Enterprise

See Lastline Enterprise product documentation for instructions on how to send syslog logs to a remote server.

Before you begin

Configuring this data source requires:

- McAfee ESM version 9.5.0 or later
- Administrative level access to configure syslog service to send logs
- McAfee Event Receiver IP address for the address of the remote server

1. From the Lastline portal, click **Admin**.
2. Click **Syslog**.
3. Click the **Integration** tab.
4. Create a syslog destination by selecting the sensors to log, time zone, IP address/port for the McAfee Event Receiver, host name, and log format message (CEF).
5. Enable the notification option.
6. Set the default configuration to log all categories with no delay between logs and no maximum limit per day.
7. Optionally, limit the volume of messages by category, minimum severity level, rate, and maximum daily volume.

Add Lastline Enterprise

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Lastline
Data Source Model	Enterprise
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address	IP address associated with the data source device
Hostname	Host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Require McAfee Event Receiver to communicate over TLS
Support generic syslogs	Do nothing
Time Zone	Time zone of data being sent

Lastline Enterprise events to McAfee fields

Log format

The expected format for this device is as follows:

```
<Date-Time> <CEF Version> <Device Vendor> <Device Product> <Device Version> <Signature ID>
<Name> <Severity> <Key-Value Pairs>
```

Log sample

This is a sample log from a Lastline Enterprise device:

```
May 20 13:20:56 mcafeecef CEF:0|Lastline|Enterprise|7.3|signature-match|IDS Signature Match|
4|act=LOG cat=drive-by/Fiesta EK cn1=45 cn1Label=impact cn2=6052 cn2Label=IncidentId cn3=100
cn3Label=IncidentImpact cnt=1 cs1=d6aeef2b:20fbe7df:13acfcd2 cs1Label=detectionId
cs2=https://user.lastline.com/event#/3999999999/677777777/78888?event_time\\=2017-05-20
cs2Label=EventDetailLink cs3=http://example.com/
asp9gg3/0040e4c25360c1ec435c460d570f5a0602080b0407045807040107425506075061531
cs3Label=EventUrl deviceExternalId=3888888888:688888888 dpt=80 dst=203.0.113.0 end=May 20
2017 13:16:16 UTC externalId=74444 proto=TCP src=192.0.2.0 start=May 20 2017 13:16:16 UTC
```

Mappings

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

Log fields	McAfee ESM fields
name - category	Rule Name
severity	Severity
EventUrl	URL
EventDetailLink	Device_URL
IncidentId	Incident_ID
act	Action
cat	Threat_Category, Category, Subcategory
cnt	Count
detectionId	File_ID
dhost	Destination_Hostname
dpt	Destination Port
dst	Destination IP
start, rt, end	First Time, Last Time
externalId	External_EventID
fileHash	File_Hash
fileSHA1	SHA1
fname	Filename
fileType	Object
proto	Protocol
src	Source IP
spt	Source Port
deviceType	Sensor_Type
deviceExternalId	External_Device_Type
dvchost	Host
smac	Source Mac
msg	Message_Text

Locum RealTime Monitor

Contents

Configure Locum RealTime Monitor

See documentation for information about how to send syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add Locum RealTime Monitor

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Locum**
Data Source Model	**RealTime Monitor (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Locum RealTime Monitor events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device IP> <device> <time> <status> <message>
```

Log sample

This is a sample log from a Locum RealTime Monitor device:

```
<123>Jan 01 01:01:01 192.0.2.1 RealTime_Monitor 01:01 VALIDATION: 1234 Usercode example
validated for example (by FTP/SERVER/FOR/"192.0.2.2")
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Host
Protocol	Protocol
Device IP	Source IP

Log fields	McAfee ESM fields
UC	Destination IP
Application	Application
Object	Object Type
Object	Object
Task	Command
User	Source User
Usercode	Destination User
Database Name	Database_Name
Description	Message_Text

LOGbinder

Contents

Configure LOGbinder

Task

1 Open the LOGbinder Configurator.

2 Select the **Output** section, then select your preferred logging method. McAfee ESM currently supports the CEF format and the Syslog-Generic format for all types.

3 Double-click the selected logging method and fill in the required syslog information.

Add LOGbinder

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**LOGbinder**
Data Source Model	**LOGbinder**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

LOGbinder events to McAfee fields

Log format (Sharepoint)

The expected formats for this device is:

Syslog

```
syslogTimestamp syslogHost signatureID LOGbinder SP|deviceVersion|type|eventTimestamp|
message|name="key1" label="Key 1" value="value1"|name="key2" label="Key 2" value="value2"|…
```

CEF

```
CEF:version|LOGbinder|SP|deviceVersion|signatureID|message key1=value1 key2=value2…
```

Log format (Exchange)

The expected format for this device is:

Syslog

```
syslogTimestamp syslogHost signatureID LOGbinder EX|deviceVersion|type|eventTimestamp|
message|name="key1" label="Key 1" value="value1"|name="key2" label="Key 2" value="value2"|…
```

CEF

```
CEF:version|LOGbinder|EX|deviceVersion|signatureID|message key1=value1 key2=value2…
```

Log format (SQL)

The expected format for this device is:

Syslog

```
syslogTimestamp syslogHost signatureID LOGbinder SQL|deviceVersion|type|eventTimestamp|
message|name="key1" label="Key 1" value="value1"|name="key2" label="Key 2" value="value2"|…
```

CEF

```
CEF:version|LOGbinder|SQL|deviceVersion|signatureID|message key1=value1 key2=value2…
```

Log sample (Exchange)

This is a sample log from a LOGbinder EX device:

Syslog

```
Jan 01 01:01:01 192.0.2.1 25190 LOGbinder EX|2.0|success|2015-01-01T01:01:01.0000001-00:00|
New-AdminAuditLogSearch Exchange cmdlet issued|name="occurred" label="Occurred"
value="1/1/2015 1:01:01 AM"|name="cmdlet" label="Cmdlet" value="New-AdminAuditLogSearch"|
name="performedby" label="Performed By" value="testUser"|name="succeeded" label="Succeeded"
value="Yes"|name="error" label="Error" value="n/a"|name="originatingserver"
label="Originating Server" value="DEV1 (198.51.100.1)"|name="objectmodified" label="Object
Modified" value="AuditLogSearch\\f8376002-c01c-45e3-ad9c-0c1dd7cfe780"|name="parameters"
label="Parameters" value="Name: StartDate, Value: [1/1/2015 1:01:01 AM]Name: EndDate, Value:
[9/6/2013 6:55:00 PM]Name: StatusMailRecipients, Value: [test@test.com]Name: Name, Value:
[8e41b65d-46ee-4f41-9e4d-f8996c19ce04]"|name="properties" label="Modified Properties"
value="n/a"|name="additionalinfo" label="Additional Information" value="CmdletParameters/
Parameter/Name\= [StartDate]; CmdletParameters/Parameter/Value\= [1/1/2015 1:01:01 AM];
CmdletParameters/Parameter/Name\= [EndDate]; CmdletParameters/Parameter/Value\= [1/1/2015
1:01:06 AM]; CmdletParameters/Parameter/Name\= [StatusMailRecipients]; CmdletParameters/
Parameter/Value\= [test@test.com]; CmdletParameters/Parameter/Name\= [Name];
CmdletParameters/Parameter/Value\= [8e41b65d-46ee-4f41-9e4d-f8996c19ce04]"|name="support"
value="For more information, see http://www.ultimatewindowssecurity.com/securitylog/
encyclopedia/event.aspx?eventid=25190"
```

CEF

```
Jan 01 01:01:01 192.0.2.1 CEF:0|LOGbinder|EX|3.0|25190|New-AdminAuditLogSearch Exchange
cmdlet issuedrt=1/1/2015 1:01:01 AM act=Error suser=testUser outcome=Yes
msg=New-AdminAuditLogSearch Exchange cmdlet issued dvchost=DEV1 fname= AuditLogSearch\
\f8376002-c01c-45e3-ad9c-0c1dd7cfe780 filePermission=n/a cs4=n/a cs4Label=Modified
Properties cs3= name="additionalinfo" label="Additional Information" value="CmdletParameters/
Parameter/Name\= [StartDate]; CmdletParameters/Parameter/Value\= [1/1/2015 1:01:01 AM];
CmdletParameters/Parameter/Name\= [EndDate]; CmdletParameters/Parameter/Value\= [1/1/2015
1:01:06 AM]; CmdletParameters/Parameter/Name\= [StatusMailRecipients]; CmdletParameters/
Parameter/Value\= [test@test.com]; CmdletParameters/Parameter/Name\= [Name];
CmdletParameters/Parameter/Value\= [8e41b65d-46ee-4f41-9e4d-f8996c19ce04]"
cs3Label=Additional Info reason=For more information, see http://
www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=25190
```

Log sample (SharePoint)

This is a sample log from a LOGbinder SP device:

Syslog

```
Jan 01 01:01:01 192.0.2.1 65 LOGbinder SP|5.1|success|2015-01-01T01:01:01.0000001-00:00|Item
declared as a record|name="occurred" label="Occurred"
value="2015-01-01T01:01:01.0000001-00:00"|name="site" label="Site" value="testSite"|
name="user" label="User" value="testUser"|name="objecturl" label="Object URL" value="\
\testSite\place\thing\"|name="support" value="For more information, see http://
www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=65"
```

CEF

```
Jan 01 01:01:01 192.0.2.1 CEF:0|LOGbinder|SP|5.1|65|Item declared as a
recordrt=2015-01-01T01:01:01.0000001-00:00 request=testSite duser=testUser filePath=\
\testSite\place\thing\ reason=For more information, see http://
www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=65
```

Log sample (SQL)

This is a sample log from a LOGBinder SQL device:

SQL

```
Jan 01 01:01:01 192.0.2.1 24000 LOGbinder SQL|2.0|failure|2015-01-01T01:01:01.0000001-00:00|
SQL audit event|name="occurred" label="Occurred" value="1/1/2015 1:01:01.0000000 AM"|
name="action_id" label="Action" value="RWC"|name="succeeded" label="Succeeded" value="False"|
name="permissionbitmask" label="Permission bitmask" value="16"|name="iscolumnpermission"
label="Is column permission" value="False"|name="sessionid" label="Session ID" value="78"|
name="serverprincipalid" label="Server Principal ID" value="2"|name="databaseprincipalid"
label="Database Principal ID" value="1"|name="targetserverprincipalid" label="Target Server
Principal ID" value="0"|name="targetdatabaseprincipalid" label="Target Database Principal
ID" value="0"|name="objectid" label="Object ID" value="n/a"|name="classtype" label="Class
Type" value="n/a"|name="sessionserverprincipalname" label="Session Server Principal Name"
value="LB\\Administrator"|name="serverprincipalname" label="Server Principal Name" value="LB\
\Administrator"|name="serverprincipalsid" label="Server Principal SID" value="n/a"|
name="databaseprincipalname" label="Database Principal Name"
value="2015-01-01T01:01:01.0000001"|name="targetserverprincipalname" label="Target Server
Principal Name" value="dbo"|name="targetserverprincipalsid" label="Target Server Principal
SID" value="n/a"|name="targetdatabaseprincipalname" label="Target Database Principal Name"
value="n/a"|name="serverinstancename" label="Server Instance Name" value="n/a"|
name="databasename" label="Database Name" value="DEV2"|name="schemaname" label="Schema Name"
value="master"|name="objectname" label="Object Name" value="n/a"|name="statement"
label="Statement" value="n/a"|name="additionalinformation" label="Additional Information"
value="REVOKE ALTER ON XML SCHEMA COLLECTION::[dbo].[$(SchemaCollectionName)] TO [$
(UserName2)] CASCADE"|name="support" value="For more information, see http://
www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=24000"
```

CEF

```
Sep 23 15:46:10 host CEF:0|LOGbinder|SQL|2.0|24000|SQL audit eventrt=1/1/2015
1:01:01.0000000 AM cfp1=RWA cfp1Label=Action oldFileId=False filePermission=16 fileHash=N/A
dpid=78 suid=1 cn3=1 cn3Label=Database Principal ID cn1=1 cn1Label=Target Server Principal
ID cn2=0 cn2Label=Target Database Principal ID fileId=n/a cfp2=n/a cfp2Label=Class Type
duser=LB\\Administrator suser=n/a spriv=n/a cs2=2015-01-01T01:01:01.0000001
cs2Label=Database Principal Name cs4=n/a cs4Label=Target Server Principal Name cs3=1
cs3Label=Target Server Principal SID cs5=0 cs5Label=Target Database Principal Name
deviceExternalId=n/a filePath=n/a cs6=master cs6Label=Schema Name fname=n/a cs1=n/a
cs1Label=Statement reason=n/a reason=For more information, see http://
www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=24000
```

Mappings (Exchange)

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

Log fields	McAfee ESM fields
Signature ID	Signature ID
rt | occurred	First Time | Last Time
src | ClientIPAddress	Source IP
cmdlet	Command
oldFileId | folderid	Filename
deviceHostName | dvchost | originatingserver	Host
fname | objectmodified	Object
suser | performedby	Source User
suid	Security_ID
sproc | clientprocess	Process_Name
performedlogonType	Logon Type

Log fields	McAfee ESM fields
mailboxguid	Instance GUID
itemsubject	Subject

Mappings (Sharepoint)

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

Log fields	McAfee ESM fields
Signature ID	Signature ID
rt | occurred	First Time | Last Time
fname | fileName | objecttitle	Filename
site | request	Object
user | duser | requestedby | membername | administratorname	Destination User
suser | user	Source User
objecturl | filepath	URL
source | filepath	File_Path
newauditpolicy	Policy_Name

Mappings (SQL)

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

Log fields	McAfee ESM fields
Signature ID	Signature ID
rt | occurred	First Time | Last Time
cfp1 | action_id	Device_Action
FileId | succeeded	Action
duser | sessionserverprincipalname	Destination User
dpid | sessionid	Session ID
schemaname	Database_Name
memberdomainname	Domain
targetobjectname	Object
suser | member | targetobjectname	Source User
deviceExternalId | server	External_Device_ID

Lumension Bouncer

Contents

Configure Lumension Bouncer

See documentation for information about how to send syslog events to a syslog server or McAfee ESM.

Add Lumension Bouncer

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Lumension**
Data Source Model	**Bouncer (ASP)** or **Bouncer – CEF (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Lumension Bouncer (CEF) events to McAfee fields

Log format

The expected format for this device is:

```
BouncerMgr CEF:0|Lumension|BOUNCER|<version>|<event type>|<event name>|<severity>|
<key>=<value> <key>=<value> <key>=value>
```

Log sample

This is a sample log from a Lumension Bouncer device:

```
BouncerMgr CEF:0|Lumension|BOUNCER|6.2|1234|Execute of file denied|1|
EndpointName=exampleName EventClass=Endpoint EventID=1234 CauseID=Executing
IPAddress=192.0.2.1 TargetFileName=\Device\HarddiskVolume1\file.exe TargetPath=\Device
\HarddiskVolume1\ TargetSHA=ABCDEF12344567890ABCDEF1234567890ABCDEF TargetSize=12345678
TargetSID=S-1-5-21-1234567890-123456789-1234567890-123 TargetCertSubject=VeriSign Class 3
Code Signing 2001 TargetCertSHA=ABCDEF123445677890ABCDEF1234567890ABCD TargetCertSize=1234
Timestamp=2001-01-01 01:01:01
```

Mappings

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

Log fields	McAfee ESM fields
EndpointName	Host
IPAddress	Source IP
Timestamp	First Time, Last Time
Event wName	Action
Severity	Severity
TargetApp, AppName	Application
TargetPath	Filename
TargetFileName	Object
TargetUser	Destination User
AskReason	Message_Text
CauseID	Subject
EventClass	Event Class
Event Type	External_Event_ID

Events Lumension Bouncer (syslog) events to McAfee fields

Log format

The expected format for this device is:

```
BouncerMgr CEF:0|Lumension|BOUNCER|<version>|<event type>|<event name>|<severity>|
<key>=<value> <key>=<value> <key>=value>
```

Log sample

This is a sample log from a Lumension Bouncer device:

```
Jan 01 01:01:01 hostname Manager:John Client:192.168.1.1 EventID: 123456 Level: 1 Count:78
EventCause: 90 AppName: appName ManagedName:name Pathname:name
```

Mappings

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

Log fields	McAfee ESM fields
IpProto	Protocol
SrcAddr	Source IP
DstAddr	Destination IP
SrcPort	Source Port
DstPort	Destination Port
AppName	Application
Manager	Source User
Client	Destination User

Lumension LEMSS

Contents

Configure Lumension LEMSS

See the Lumension LEMSS product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add Lumension LEMSS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Lumension**
Data Source Model	**Lumension LEMSS**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Lumension LEMSS events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <severity> <deviceIP> <date time> <HostName> <ApplicationName> <ProcessName>
<Message ID> <User> <UserName> <DeviceType> <DeviceName> <VolumeLabel> <StrongID> <Filename>
<Other> <Reason> <UniqueID> <ModelID>
```

Log sample

This is a sample log from a Lumension LEMSS device:

```
01-01-2001 01:01:01 System.Info 192.0.2.1 1 2001-01-01T01:01:01Z app MEDIUM-INSERTED
[EventLog@12345 User="S-1-2-34-1234567890-1234567890-12345678-1234" UserName="DOMAIN\\user"
DeviceType="Removable" DeviceName="Generic Flash Disk USB Device, Disk drive, (Standard disk
drives)" StrongID="a1b1c3d4e5f6a1b1c3d4e5f6a1b1c3d4" Reason="ENCRYPTED"
UniqueID="a1b1c3d4e5f6a1b1c3d4e5f6a1b1c3d4e5f6a1b1"
ModelID="a1b1c3d4e5f6a1b1c3d4e5f6a1b1c3d4e5f6a1b1"]
```

Mappings

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

Log fields	McAfee ESM fields
HostName	Hostname
ApplicationName	Application
DeviceIP	Source IP
ProcessName	Command
UserName	Domain, Source User
VolumeLabel	
Version	Version
DeviceName	External_Device_Name
DeviceType	External_Device_Type
Filename	Directory
Reason	Reason

Malwarebytes Breach Remediation

Contents

Configure Malwarebytes Breach Remediation

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

Add Malwarebytes Breach Remediation

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Malwarebytes**
Data Source Model	**Breach Remediation**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Malwarebytes Breach Remediation events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|PRODUCT VENDOR|PRODUCT NAME|PRODUCT VERSION|SIGNATURE ID|NAME|SEVERITY|KEY=VALUE
KEY=VALUE…
```

Log sample

This is a sample log from a 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
```

Mappings

This table 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

Log fields	McAfee ESM fields
deviceMacAddress	Source MAC
Dvchost	Host
filePath	File_Path
Msg	Message_Text
Suser	Source User

Malwarebytes Management Console

Contents

Configure Malwarebytes Management Console

Syslog settings can be accessed from the Admin Module.

Task

1 Open the Admin Module.

2 Switch to the **Syslog Settings** tab.

3 By default, logging to an external Syslog server is disabled. Click **Change** to open the settings dialog box.

4 Select **Enable Syslog** and fill in the appropriate configuration fields.

- Address: <IP address of the McAfee Event Receiver>
- Port: **514**
- Protocol: **UDP**
- Specify Facility number (ranges from 0–23).
- Specify Severity number (ranges from 0–7).
- Payload Format: **CEF**

Add Malwarebytes Management Console

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Malwarebytes**
Data Source Model	**Management Console**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Malwarebytes Management Console events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|VENDOR|PRODUCT|VERSION|CATEGORY|MESSAGE|SEVERITY|deviceExternalId=externalid
dvchost=hostname deviceDnsDomain=domain deviceMacAddress=mac_address dvc=device_ip
rt=TIMESTAMP cs1Label=KEY cs1=VALUE…
```

Log sample

This is a sample log from a Malwarebytes Management Console device:

```
CEF:0|Malwarebytes|MBMC|1.7.0.3208 MBAM:1.80.2.1012 DB:913030101 MBAE:1.08.2.1189|DETECTION|
Exploit ROP attack quarantined|5|deviceExternalId=d6961b91-6098-48c4-a64eff75c9e5550e
dvchost=PC-WIN123 deviceDnsDomain=WORKGROUP deviceMacAddress=00-00-00-00-00-00
dvc=192.0.2.10 rt=Jan 01 2016 01:01:01 -00:00 cn1=1 cn1Label=ObjectTypeScanned cs6=
cs6Label=ObjectScanned cat=DETECTION cn2=1 cn2Label=Action act=QUARANTINE outcome=success
suser=jdoe cs5=data cs5Label=Data msg=Attacked application: C:\\Users\\jdoe\\Desktop\
\iexplore.exe; Parent process name: explorer.exe; Layer: Protection Against OS Security
Bypass; API ID: 453; Address: 0x76F5FE07; Module: ; AddressType: ; StackTop: 0x002F0000;
StackBottom: 0x002ED000; StackPointer: ; Extra: fname=Internet Explorer filePath=C:\\Users\
\jdoe\\Desktop\\iexplore.exe sourceServiceName=MBAE cs1= cs1Label=Payload cs2=
cs2Label=PayloadChecksum cs3= cs3Label=PayloadUrl cs4= cs4Label=PayloadProc
```

Mappings

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

Log fields	McAfee ESM fields
Message	Message
suser	Source Username
dst	Destination IP
src	Source IP

Log fields	McAfee ESM fields
act	Device_Action
Action	Action / Subtype
deviceMacAddress	Source Mac
rt	First Time, Last Time
PayloadProc	Application
ObjectScanned	Object
dvchost	Hostname
Severity	Severity
fname	Filename
filePath	File Path
deviceExternalId	Source GUID
ObjectTypeScanned	Object Type
dvc	Device IP, Source IP (Fallback)
sourceServiceNam	Service Name
PayloadUrl	URL

Microsoft DNS

Contents

Configure Microsoft DNS

Task

1. Open the **Domain Name System Microsoft Management Console** (DNS MMC) snap-in.
2. Click **Start** | **Programs** | **Administrative Tools**, then select **DNS**.
3. From the DNS Server, right-click the server and select the **Properties** submenu.
4. Click the **Debug Logging** tab, then select **Log packets debugging**.
5. Ensure that the **Incoming**, **UDP**, **Queries/Transfer**, and **Request** checkboxes are selected.
   File location is: *systemroot\System32\Dns\Dns.log*
6. Configure McAfee Collector to tail the log and send to the McAfee Event Receiver.

Add Microsoft DNS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Microsoft
Data Source Model	DNS
Data Format	Default
Data Retrieval	MEF
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Host ID	Host ID associated with the McAfee Collector log tail configuration if applicable
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Microsoft Windows DNS events to McAfee fields

Log sample

```
9/3/2010 2:06:38 PM 1720 PACKET  02306B10 UDP Rcv 127.0.0.1       be06   Q [0001   D
NOERROR] A     (3)www(9)sonystyle(3)com(0)
9/3/2010 2:06:38 PM 1720 PACKET 06569C90 UDP Snd 10.0.0.30 6068 Q [0001 D NOERROR] A
(3)www(9)sonystyle(3)com(0)
```

Microsoft Forefront Endpoint Protection 2010

Contents

Configure Microsoft Forefront Endpoint Protection 2010

No configuration is needed on the FEP application to allow data collection from McAfee ESM, which collects data by connecting directly to the data warehouse database.

Add Microsoft Forefront Endpoint Protection 2010

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Forefront Endpoint Protection 2010 (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
User ID	The database user ID.
Password	The password associated with the User ID.
Port	The TCP port that the database is listening on. The default port is 1433.
Database Name	The name of the database that contains the vwFEP_AM_NormalizedDetectionHistory view, typically prefaced with **FEPDW_***.

Microsoft Forefront Endpoint Protection 2010 events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a Microsoft Forefront Endpoint Protection 2010 device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol

Log fields	McAfee ESM fields
Source	Source IP
Destination	Destination IP

Microsoft Internet Authentication Service (IAS)

Contents

Configure Microsoft Internet Authentication Service (IAS)

This file supports multiple modes of data delivery. This data source supports all file delivery methods (SCP, HTTP, FTP, SFTP, NFS, and CIFS/Windows File Share). Additional setup steps might be required on the IAS server to allow data to be sent to the McAfee Event Receiver using these methods.

The recommended method for data delivery is to use the McAfee Collector to send the logs over syslog. These agents can send only the logs that haven't yet been sent, eliminating duplicates.

See the documentation for the method you choose to use.

Configure Microsoft IAS (Formatted ASP)

Task

1. Open Internet Authentication Service.
2. Click **Remote Access Logging** in the console tree.
3. Right-click **Local File** in the details pane, then click **Properties**.
4. Enable the logging you want, then click **Apply**.
5. Click the **Log File** tab.
6. In the **Directory** field, enter the path for log file storage. If you are not using the McAfee Collector, make sure that the path is accessible to the McAfee Event Receiver.

   The default path is systemroot/System32/LogFiles.
7. Under **Format**, select **IAS**.
8. To create a log file at specific intervals, select the interval that you want to use.
9. Click **Apply**, then click **OK**.

Add Microsoft IAS (Formatted ASP)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Internet Authentication Service – Formatted (ASP)**
Data Format	**Default**
Data Retrieval	The chosen method of data delivery (SCP, HTTP, FTP, SFTP, NFS, or CIFS/ Windows File Share)
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft IAS (formatted ASP) events to McAfee fields

Log format

The expected format for this device is:

```
NAS-IP-Address, User-Name, Record-Date, Record-Time, Service-Name, Computer-Name,
AttributeNumber1, ValueForAttributeNumber1, AttributeNumber2, ValueForAttributeNumber2,
AttributeNumber3, ValueForAttributeNumber3…
```

Log sample

This is a sample log from a Microsoft IAS device:

```
192.0.2.1,client,01/01/2012,00:00:00,UAS,CLIENTCOMP,44,2666,25,311 1 172.1.1.1 01/00/2012
00:00:00 2665,8153,0,8111,0,4130,server.example.com/Domain Users/service/folder/client,
4294967206,14,4294967207,2,6,2,28,14400,7,1,4149,VPN_Allow_user,
4120,0x0049532D48455243554C4553,4127,4,4154,Microsoft Routing and Remote Access Service
Policy,4155,1,4129,Domain\user.name,4136,2,4142,0
```

Mappings

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

Log fields	McAfee ESM fields
Client	Domain
User-Name	Username
Date and Time	Firsttime/Lasttime
Service-Name	Application
Computer-Name (Radius/AD Server IP)	Destination IP
NP-Policy-Name	Object name
Packet-type	Action
Framed-IP-Address	Source IP
NAS-ID	External Device Name
NAS-IP-Address	Device IP
Called-Station-ID	Destination MAC
Calling-Station-ID	Source MAC
Application	Application
Reason-Code	Reason
Connection-Info	Message_Text

Configure Microsoft IAS (database compatible)

Task

1 Open Internet Authentication Service.

2 Click **Remote Access Logging** in the console tree.

3 In the details pane, right-click **Local File**, then click **Properties**.

4 Enable the type of logging you want, then click **Apply**.

5 Click the **Log File** tab.

6 Enter the path for log file storage in the **Directory** field. If you are not using the McAfee Collector, make sure that the path is network accessible to the McAfee Event Receiver.

The default path is systemroot/System32/LogFiles.

7 Click **Database-compatible** for the **Format** parameter.

8 To create a log file at specific intervals, select the interval that you want to use.

9 Click **Apply**, then click **OK**.

Add Microsoft IAS (Database Compatible)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Internet Authentication Service – Database Compatible**
Data Format	**Default**
Data Retrieval	The chosen method of data delivery (SCP, HTTP, FTP, SFTP, NFS, or CIFS/ Windows File Share)
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft IAS (database compatible) events to McAfee fields

Log format

The expected format for this device is:

```
"ComputerName"," ServiceName", Record-Date, Record-Time, Packet-Type," User-Name","
Fully-Qualified-Distinguished-Name"," Called-Station-ID"," Calling-Station-ID",
Callback-Number, Framed-IP-Address," NAS-Identifier"," NAS-IP-Address",NAS-Port,
Client-Vendor,"Client-IP-Address"," Client-Friendly-Name", Event-Timestamp, Port-Limit,
NAS-Port-Type,Connect-Info,Framed-Protocol,Service-Type,Authentication-Type,"Policy-Name",Rea
son-Code,"Class",Session-Timeout,Idle-Timeout,Termination-Action,EAP-Name,Acc-Status-Type,Ac
c-Delay-Time,Acc-Input-Octets,Acc-Output-Octets,Acc-Session-ID,Acc-Authentic,Acc-Input-Packet
,Acc-Output-packet,acc-terminate-Cause,acc-multi-ssn-ID,acc-link-Count,Acc-Interim-Interval,t
unnel-type,tunnel-medium-type,tunnel-client-endpoint,tunnel-server-endpoint,Acc-tunnel-conn,t
unnel-pvt-group-ID,"tunnel-assignment-id",Tunnel-Preference,MS-acc-auth-type,MS-acc-EAP-Type,
MS-RAS-Version,MS-RAS-Vendor,MS-CHAP-Error,MS-CHAP-Error,MS-CHAP-Domain,MS-MPPE-Encryption-Ty
pes,MS-MPPE-Encryption-Policy,"Proxy-Policy-Name:MSG",Provider-Type,Provider-Name,Remote-Serv
er-IP,MS-RAS-CLient-Name,MS-RAS-Client-Version
```

Log sample

This is a sample log from a Microsoft IAS device:

```
"TestHost","IAS",01/01/2016,00:00:00,4,"EXAMPLE
\Test.User",,"192.0.2.1","192.0.2.2",,"192.0.2.2","TestIdentifier","192.0.2.1",
1,9,"192.0.2.1","TestClient",,,,,,,,0,,,,,,1,,,,,1,,,,,,,,13,6,,,,"110",,,,,,,,,,"Use
Windows authentication for all users",,,,,
"TestHost","IAS",01/01/2016,00:00:001,"EXAMPLE\Test.User","EXAMPLE
\Test.User","0F-0F-0F-0F-0F-0F:EXAMPLE-Host","0A-0A-0A-0A-0A-0A",,,"TestIdentifier","192.0.2.
1",1,9,"192.0.2.1","TestClient",,,19,,,,11,,0,,,,,,,,,,,,,,,,,13,6,,,,"190",,,,,,,,,,"NAP
802.1X (Wireless)",1,,,,
```

Mappings

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

Log fields	McAfee ESM fields
Client	Domain
username	Source User
Record-Date+Record-Time	First Time, Last Time
IAS	Application
Hostname	Host
Policy-Name	Policy_Name
Packet-type	Event Subtype
Tunnel-client-endpoint address	Source IP
Reason-Code	Reason
Packet-Type+99+Reason-Code	Signature ID
ComputerName	Destination Host
ServiceName	Service_Name
Event-Timestamp	First Time, Last Time
Domain, FQ-Domain, MS-CHAP-DOMAIN	Domain
User-Name, FQ-Distinguished-Name	Source User
Called-Station-ID	Destination MAC
Class (IP Address)	Destination IP
NAS-Identifier	External_Device_ID
NAS-IP-Address, Client-IP-Address	Device_IP
Calling-Station-ID	Source MAC
Framed-IP-Address	Source IP
Calling-Station-ID (IP Address)	Source IP
Connect-Info	Message_Text
Acct-Session-Id	Session

Microsoft Internet Information Services (IIS)

Contents

Configure Microsoft IIS

Task

1 Open the Internet Information Services (IIS) Manager (found in **Administrative Tools** in the Control Panel).

2 Select the **Logging** option.

3 Select a log format. W3C format is the default, but IIS and NCSA are also supported. If using the W3C format, you must select all fields.

4 Make a note of where the logs are being saved, or change the location as needed.

5 Finish the logging setup by configuring the McAfee Collector to tail the IIS logs and send to the McAfee Event Receiver.

Add Microsoft IIS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Internet Information Services (ASP)**
Data Format	**Default**
Data Retrieval	**MEF**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft IIS events to McAfee fields

Log format

The expected formats for this device are:

WC3

```
date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port
cs-username c-ip cs-version cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status
sc-substatus sc-win32-status sc-bytes cs-bytes time-taken
```

NCSA

```
Remote_host_address Remote_log_name User_name [Date/time Greenwich mean time (GMT) offset]
"Request and protocol version" Service_status_code Bytes_sent
```

IIS

```
Client_IP_address, User_name, Date, Time, Service_and_instance, Server_name, Server_IP,
Time_taken, Client_bytes_sent, Server_bytes_sent, Service_status_code, Windows_status_code,
Request_type, Target_of_operation, Parameters,
```

Advanced Logging

```
date time cs-uri-stem cs-uri-query s-contentpath sc-status s-computername cs(Referer)
sc-win32-status sc-bytes cs-bytes W3WP-PrivateBytes cs-username cs(User-Agent) time-local
TimeTakenMS sc-substatus s-sitename s-ip s-port RequestsPerSecond s-proxy cs-version
c-protocol cs-method cs(Host) EndRequest-UTC date-local CPU-Utilization cs(Cookie) c-ip
BeginRequest-UTC
```

Log sample

The following are samples of possible logs from the Microsoft IIS device:

WC3

```
2011-04-14 14:58:36 MS_ISS_1 name 127.0.0.1 GET /exampletest - 80 - 127.0.0.1 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+WOW64;+Trident/4.0;+SLCC2;+.NET+CLR
+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729) - - 127.0.0.1 404 4 2 109 398 2
```

NCSA

```
172.21.13.45 - Microsoft\fred [08/Apr/2001:17:39:04 -0800] "GET /scripts/iisadmin/ism.dll?
http/serv HTTP/1.0" 200 3401
```

IIS

```
172.16.255.255, anonymous, 03/20/01, 23:58:11, MSFTPSVC, SALES1, 172.16.255.255, 60, 275, 0,
0, 0, PASS, /Intro.htm, -,
```

Advanced Logging

```
2014-11-16 22:56:55.379 /index.html - "C:\inetpub\wwwroot\index.html" 200 "WIN2008R2-1" - 0
339 39 - - - 15:56:55.379 4 0 "DEFAULT WEB SITE" 10.50.14.9 80 - - "HTTP/1.0" "http" GET
"10.50.14.9" 2014-11-16 22:56:55.379 2014-11-16 - - 10.50.14.8 2014-11-16 22:56:55.375
```

Mappings

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

WC3 Log fields	McAfee ESM fields
Date Time (two fields)	FirstTime,LastTime
s-ip	Destination IP
cs-method	Command
cs-uri-stem	Object
s-port	Destination Port
cs-username (domain section)	Domain
cs-username	Source User
c-ip	Source IP
cs(User-Agent)	Application
cs-host	Hostname
sc-status	sid
sc-status(first number)	Action

IIS log fields	McAfee ESM fields
Client IP	Source IP
User name	Source User
Date Time (two fields)	FirstTime, LastTime
Server Name	Hostname
Server IP	Destination IP
Clients bytes sent	Bytes_from_Client
Server bytes sent	Bytes_from_Server
Service Status Code	sid
Service Status Code (first number)	action
Request Type	Command
Target of Operation	Object

NCSA Log fields	McAfee ESM fields
Remote Host Address	Source IP
User name	Source User
Date Time (two fields)	FirstTime, LastTime
Request and protocol version (first part)	Command
Request and protocol version (second part)	Object
Request and protocol version (third part)	Protocol
Service Status Code	sid
Service Status Code (first number)	action
Bytes Sent	Bytes_Sent

Advanced logging	McAfee ESM fields
Date Time (two fields)	FirstTime,LastTime
s-ip	Destination IP
cs-method	Command
cs-uri-stem	Object
s-port	Destination Port
cs-username (domain section)	Domain
cs-username	Source User
c-ip	Source IP
cs(User-Agent)	User_Agent
cs-host	Hostname
sc-status	sid
sc-status(first number)	Action
sc-bytes	Bytes_from_Server
cs-bytes	Bytes_from_Client
protocol	Application_Protocol

Install Microsoft IIS Advanced Logging

Task

1 Download the Advanced Logging extension for IIS. At the time of this documentation, it was available at: http://www.iis.net/downloads/microsoft/advanced-logging

2 Run AdvancedLogging.exe to start the Web Platform Installer.

Once loaded, the installer displays a window to install Advanced Logging.

3 Select **Install**.

4 When the installer displays the licensing information, select **I Accept**.

The remaining phases complete the installation automatically.

5 Click **Finish** to exit the Advanced Logging installation.

6 Click **Exit** to exit the Web Platform Installer.

Advanced Logging is now installed.

Configure Microsoft IIS Advanced Logging

Task

1 Open the Internet Information Services (IIS) Manager.

2 Under **Connections**, select the server.

3 Click the **Advanced Logging** icon.

4 When the installer displays the licensing information, select **I Accept**.

The remaining phases complete the installation automatically.

5 From the **Advanced Logging** menu, click **Enable Advanced Logging** on the right.

6 In the **Name column**, click the name of the server hosting the site to change the menu options on the right.

7 Select **Edit Log Definition**.

8 From the **Log Definition** menu, scroll down to **Selected Fields**, then click **Select Fields**.

9 In **Select Logging Fields**, select every field in the **ID** column. Scroll down to select all fields, then press **OK**.

10 From the **Internet Information Services (IIS) Manager** window, click **Apply**.

11 Done.

Microsoft Network Policy Server (NPS)

Contents

Configure Microsoft Network Policy Server (NPS)

Multiple modes of data delivery are supported for this file. All file delivery methods (SCP, HTTP, FTP, SFTP, NFS, and CIFS/Windows File Share) are supported with this data source. Additional setup might be required on the NPS server to allow data to be sent to the McAfee Event Receiver using these methods.

The recommended method for data delivery is to use the McAfee Collector to send the logs over Syslog. These agents have the added benefit of being able to send only the logs that haven't yet been sent, eliminating duplicates.

See the respective delivery method documentation for the method you chose to use.

Configure Microsoft NPS (Database Compatible)

Task

1. Open the Network Policy Server or the NPS Microsoft Management Console (MMC) snap-in.
2. In the console tree, click **Accounting**.
3. In the details pane under **Log File Properties**, click **Change Log File Properties**.

   For Server 2008, click **Configure Local file Logging** under **Local File Logging** in the details pane.
4. In **Log File Properties**, enable the type of logging you want, then click **Apply**.
5. Click the **Log File** tab.
6. Enter the path for log file storage in the **Directory** field. If you are not using the McAfee Collector, make sure that the path is accessible to the McAfee Event Receiver.

   The default path is systemroot/System32/LogFiles.
7. From the **Format** menu, select **ODBC (Legacy)**.

   For platforms earlier than Server 2008 R2, select **IAS** in the **Format** field.
8. To create a log file at specific intervals, select the interval that you want to use.
9. Click **Apply**, then **OK**.

Add Microsoft NPS (Database Compatible)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Internet Authentication Service – Database Compatible**
Data Format	**Default**
Data Retrieval	The method chosen in step 3.2.2.
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft NPS (database compatible) events to McAfee fields

Log format

The expected format for this device is:

```
"ComputerName"," ServiceName", Record-Date, Record-Time, Packet-Type," User-Name","
Fully-Qualified-Distinguished-Name"," Called-Station-ID"," Calling-Station-ID",
Callback-Number, Framed-IP-Address," NAS-Identifier"," NAS-IP-Address",NAS-Port,
Client-Vendor,"Client-IP-Address"," Client-Friendly-Name", Event-Timestamp, Port-Limit,
NAS-Port-Type,Connect-Info,Framed-Protocol,Service-Type,Authentication-Type,"Policy-Name",Rea
son-Code,"Class",Session-Timeout,Idle-Timeout,Termination-Action,EAP-Name,Acc-Status-Type,Ac
c-Delay-Time,Acc-Input-Octets,Acc-Output-Octets,Acc-Session-ID,Acc-Authentic,Acc-Input-Packet
,Acc-Output-packet,acc-terminate-Cause,acc-multi-ssn-ID,acc-link-Count,Acc-Interim-Interval,t
unnel-type,tunnel-medium-type,tunnel-client-endpoint,tunnel-server-endpoint,Acc-tunnel-conn,t
unnel-pvt-group-ID,"tunnel-assignment-id",Tunnel-Preference,MS-acc-auth-type,MS-acc-EAP-Type,
MS-RAS-Version,MS-RAS-Vendor,MS-CHAP-Error,MS-CHAP-Error,MS-CHAP-Domain,MS-MPPE-Encryption-Ty
pes,MS-MPPE-Encryption-Policy,"Proxy-Policy-Name:MSG",Provider-Type,Provider-Name,Remote-Serv
er-IP,MS-RAS-CLient-Name,MS-RAS-Client-Version
```

Log sample

These are log samples from a Microsoft IAS device:

```
"TestHost","IAS",01/01/2016,00:00:00,4,"EXAMPLE
\Test.User",,"192.0.2.1","192.0.2.2",,"192.0.2.2","TestIdentifier","192.0.2.1",
1,9,"192.0.2.1","TestClient",,,,,,,,0,,,,,,1,,,,,1,,,,,,,,13,6,,,,"110",,,,,,,,,,,"Use
Windows authentication for all users",,,,,
```

```
"TestHost","IAS",01/01/2016,00:00:001,"EXAMPLE\Test.User","EXAMPLE
\Test.User","0F-0F-0F-0F-0F-0F:EXAMPLE-Host","0A-0A-0A-0A-0A-0A",,,"TestIdentifier","192.0.2.
1",1,9,"192.0.2.1","TestClient",,,19,,,,11,,0,,,,,,,,,,,,,,,,,13,6,,,,"190",,,,,,,,,,,"NAP
802.1X (Wireless)",1,,,,
```

Mappings

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

Log fields	McAfee ESM fields
Client	Domain
username	Source User
Record-Date+Record-Time	First Time, Last Time
IAS	Application
Hostname	Host
Policy-Name	Policy_Name
Packet-type	Event Subtype
Tunnel-client-endpoint address	Source IP
Reason-Code	Reason
Packet-Type+99+Reason-Code	Signature ID
ComputerName	Destination Host
ServiceName	Service_Name
Event-Timestamp	First Time, Last Time
Domain, FQ-Domain, MS-CHAP-DOMAIN	Domain
User-Name, FQ-Distinguished-Name	Source User
Called-Station-ID	Destination MAC
Class (IP Address)	Destination IP
NAS-Identifier	External_Device_ID
NAS-IP-Address, Client-IP-Address	Device_IP
Calling-Station-ID	Source MAC
Framed-IP-Address	Source IP
Calling-Station-ID (IP Address)	Source IP
Connect-Info	Message_Text
Acct-Session-Id	Session

Configure Microsoft NPS (Formatted ASP)

Task

1 Open Network Policy Server (NPS) or the NPS Microsoft Management Console (MMC) snap-in.

2 Click **Accounting** in the console tree.

3 In the details pane under **Log File Properties**, click **Change Log File Properties**.

For Server 2008, click **Configure Local file Logging**.

4 On the **Log File Properties** page, enable the logging you want, then click **Apply**.

5 On the **Log File** tab, enter the path for log file storage in the **Directory** field. If you are not using the McAfee Collector, make sure that the path is accessible to the McAfee Event Receiver.

The default path is systemroot/System32/LogFiles.

6 From the **Format** drop-down list, select **IAS (Legacy)**.

For platforms earlier than Server 2008 R2, select **IAS** in the **Format** field.

7 To create a log file at specific intervals, select the interval that you want to use.

8 Click **Apply**, then click **OK**.

Add Microsoft NPS (Formatted ASP)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Network Policy Server**
Data Format	**Default**
Data Retrieval	The method chosen in step 3.1.2.
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft NPS (formatted ASP) events to McAfee fields

Log format

The expected format for this device is:

```
NAS-IP-Address, User-Name, Record-Date, Record-Time, Service-Name, Computer-Name,
AttributeNumber1, ValueForAttributeNumber1, AttributeNumber2, ValueForAttributeNumber2,
AttributeNumber3, ValueForAttributeNumber3…
```

Log sample

This is a sample log from a Microsoft IAS device:

```
192.0.2.1,client,01/01/2012,00:00:00,UAS,CLIENTCOMP,44,2666,25,311 1 172.1.1.1 01/00/2012
00:00:00 2665,8153,0,8111,0,4130,server.example.com/Domain Users/service/folder/client,
4294967206,14,4294967207,2,6,2,28,14400,7,1,4149,VPN_Allow_user,
4120,0x0049532D48455243554C4553,4127,4,4154,Microsoft Routing and Remote Access Service
Policy,4155,1,4129,Domain\user.name,4136,2,4142,0
```

Mappings

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

Log fields	McAfee ESM fields
Client	Domain
User-Name	Username
Date and Time	Firsttime/Lasttime
Service-Name	Application
Computer-Name (Radius/AD Server IP)	Destination IP
NP-Policy-Name	Object name
Packet-type	Action
Framed-IP-Address	Source IP
NAS-ID	External Device Name
NAS-IP-Address	Device IP
Called-Station-ID	Destination MAC
Calling-Station-ID	Source MAC
Application	Application
Reason-Code	Reason
Connection-Info	Message_Text

Configuring Microsoft NPS (XML ASP)

DTS Compliant (XML) logging is not available on platform earlier than Server 2008 R2.

Task

1. Open the Network Policy Server or the NPS Microsoft Management Console (MMC) snap-in.
2. In the console tree, click **Accounting**.
3. In the details pane under **Log File Properties**, click **Change Log File Properties**.
4. In the Log File Properties window, enable the logging you want, then click **Apply**.
5. Click the **Log File** tab.
6. Enter the path for log file storage in the **Directory** field. If you are not using the McAfee Collector, make sure that the path is accessible to the McAfee Event Receiver.

   The default path is systemroot/System32/LogFiles.
7. From the **Format** drop-down list, select **DTS Compliant**.
8. To create a log file at specific intervals, select the interval that you want to use.
9. Click **Apply**, then click **OK**.

Add Microsoft NPS (XML ASP)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Internet Authentication Service – XML (ASP)**
Data Format	**Default**
Data Retrieval	The method chosen in step 3.3.2.
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft NPS (XML ASP) events to McAfee fields

Log format

The expected format for this device is:

```
<Event><Timestamp data_type="VALUE"> VALUE </Timestamp><Computer-Name data_type="VALUE">
VALUE </Computer-Name><Event-Source data_type="VALUE"> VALUE </Event-Source><Class
data_type="VALUE"> VALUE </Class><Session-Timeout data_type="VALUE"> VALUE </
Session-Timeout><Fully-Qualifed-User-Name data_type="VALUE"> VALUE \userName</
Fully-Qualifed-User-Name><SAM-Account-Name data_type="VALUE"> VALUE \userName</
SAM-Account-Name><Client-IP-Address data_type="VALUE"> VALUE </
Client-IP-Address><Client-Vendor data_type="VALUE"> VALUE </
Client-Vendor><Client-Friendly-Name data_type="VALUE"> VALUE </
Client-Friendly-Name><Proxy-Policy-Name data_type="VALUE"> VALUE </
Proxy-Policy-Name><Provider-Type data_type="VALUE"> VALUE </Provider-Type><Packet-Type
data_type="VALUE"> VALUE </Packet-Type><Reason-Code data_type="VALUE"> VALUE </Reason-Code></
Event>
```

Log sample

This is a sample log from a Microsoft IAS device:

```
<Event><Timestamp data_type="4">01/01/2012 00:00:00.000</Timestamp><Computer-Name
data_type="1">S0020222</Computer-Name><Event-Source data_type="1">IAS</Event-Source><Class
data_type="1">311 1 192.0.2.10 01/01/2012 00:00:00 2</Class><Session-Timeout
data_type="0">30</Session-Timeout><Fully-Qualifed-User-Name data_type="1">COMPANY\userName</
Fully-Qualifed-User-Name><SAM-Account-Name data_type="1"> COMPANY\userName</
SAM-Account-Name><Client-IP-Address data_type="3">192.0.2.1</
```

```
Client-IP-Address><Client-Vendor data_type="0">0</Client-Vendor><Client-Friendly-Name
data_type="1">clientComputer</Client-Friendly-Name><Proxy-Policy-Name data_type="1">Secure
Wireless Connections</Proxy-Policy-Name><Provider-Type data_type="0">1</
Provider-Type><Packet-Type data_type="0">11</Packet-Type><Reason-Code data_type="0">0</
Reason-Code></Event>
```

Mappings

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

Log fields	McAfee ESM fields
User-Name	Domain
User-Name	Username
Date and Time	Firsttime/Lasttime
Calling Station ID	Source MAC
Computer-Name	Destination_Hostname
Called Station ID	Destination MAC
Policy Name	Message
Framed-IP-Address	Source IP
Client-IP-Address	Device IP
Class	Destination IP
NAS-IP-Address	Device IP
NAS-Identifier	External Device ID
Reason-Code	Reason

Microsoft Office 365

Contents

Configure Microsoft Office 365

Sending logs from Microsoft Office 365 using API requires access to the Microsoft Office Azure portal with administrator rights.

Before you begin

Configuring this data source requires:

- McAfee ESM version 10.1.0 or later
- Access to the Microsoft Office Azure portal with administrator rights

Task

1 In the Microsoft Azure portal, navigate to **Azure Active Directory**. If **Azure Active Directory** is not visible in the left menu, click **More Services** then search for it.

2 From the Active Directory submenu, click the **Properties** tab.

3 Copy the **Directory ID** value to use as the **Tenant ID** when setting up McAfee ESM for the Microsoft Office 365 data source.

4 Navigate to **App registrations**.

5 To add an application, click **New application registration**.

   a Name the application.

   b Select the **Web app/API** type.

   c In **Sign-on URL** , enter `http://localhost:1234`

   d Click **Create** at the bottom of the screen.

6 Select the newly created application.

7 Copy and save the **Application ID** to use as the **Client ID** when setting up McAfee ESM for the Microsoft Office 365 data source.

8 To allow McAfee ESM to have permission to pull event data, click **Required permissions**.

   a Click **Add** at the top of the screen.

   b From **Add API Access**, click **Select an API**.

   c Search for and select **Office 365 Management APIs**. Then click **Select** at the bottom of the screen.

   d In **Required Permissions**, select **Office 365 Management APIs**.

   e Enable all delegated permissions then click **Save** at the top of the screen.

   f Work with your administrator to grant the application new permissions by clicking **Grant Permissions** at the top of the screen.

9 To set up a security key, do the following:

   a Click **Keys** on the application settings.

   b Enter a key description and select a duration.

   c Click **Save**.

   d On the next screen, save the secret key value to a secure location for future reference.

The secret key value does not appear again. McAfee ESM requires the secret key to set up the Microsoft Office 365 data source.

10 To get collected data for Microsoft Office 365 subscriptions to specific content types, use a tool that can send API POST and GET comments. Starting a subscription requires an access token to call the subscription API.

   a For the POST URL, enter `https://login.microsoftonline.com/"insert tenant id here"/oauth2/token`

   b For POST raw body of the request, enter `grant_type=client_credentials&client_id="insert client id here"&client_secret="insert secret key here"&resource=https://manage.office.com`

c In the header, set **Key** to `'Content-Type'` and the value to `'application/x-www-form-urlencoded'`

d Send the post results in JSON and retrieve the access token from the response to use in the next request.

For information about access tokens, see https://msdn.microsoft.com/en-us/office-365/get-started-with-office-365-management-apis#requesting-access-tokens-from-azure-ad.

11 To start subscriptions, do the following:

a For the POST URL, enter `https://manage.office.com/api/v1.0/"insert tenant id here"/activity/feed/subscriptions/start?contentType="insert desired subscription content type"`

b In the header, set **Key** to `'Authorization'` and the value `'bearer "insert accesss token here"'`

JSON indicates that the content type is enabled.

As of June 12, 2017, content types are Audit.AzureActiveDirectory, Audit.Exchange, Audit.SharePoint, Audit.General, and DLP.All. For information about starting subscriptions, see https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference#start-a-subscription.

12 To verify which content types are subscribed, do the following:

a For the GET URL, enter `https://manage.office.com/api/v1.0/"insert tenant id here"/activity/feed/subscriptions/list`

b In the header, set **Key** to `'Authorization'` and the value to `'bearer "insert accesss token here"'`

JSON returns with a list of all content types that are enabled.

For information about listings subscriptions, see https://msdn.microsoft.com/en-us/office-365/office-365-management-activity-api-reference#list-current-subscriptions.

Add Microsoft Office 365

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Microsoft
Data Source Model	Office 365
Data Format	Default
Data Retrieval	API
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Tenant ID	Tenant ID
Client Key	Client key
Client Secret Key	Client secret key
Use proxy	Proxy, if required by installation
Support Generic Syslogs	Do nothing
Time Zone	Time zone of the data being sent

Microsoft Office 365 events to McAfee fields

Log format

The expected format for this device is:

```
<Date-Time> <Id> <Operation> <OrganizationId> <RecordType> <ResultStatus> <UserKey>
<UserType> <Version><Workload> <UserId> <ClientIPAddress> <ClientInfoString> <Client>
<ExternalAccess> <InternalLogonType> <LogonType> <LogonUserSid><MailboxGuid>
<MailboxOwnerSid> <MailboxOwnerUPN> <OrganizationName> <OriginatingServer> <Item>
```

Log sample

This is a sample Microsoft Office 365 log:

```
{"CreationTime":"2000-01-01T22:00:04","Id":"00000000-0000-0000-0000-000000000000","Operation"
:"Create","OrganizationId":"00000000-0000-0000-0000-000000000000","RecordType":
2,"ResultStatus":"Succeeded","UserKey":"0000A0AA0A0000A0","UserType":2,"Version":
1,"Workload":"Exchange","UserId":"S-1-5-21-0000000000-0000000000-0000000000-0000000","ClientIPAddress":
00.00.0000.010;","ExternalAccess":false,"InternalLogonType":0,"LogonType":
1,"LogonUserSid":"S-1-5-21-0000000000-0000000000-0000000000-0000000","MailboxGuid":"0000000
0-0000-0000-0000-000000000000","MailboxOwnerSid":"S-1-5-21-0000000000-0000000000-0000000000-2
026015","MailboxOwnerUPN":"user1@example.com","OrganizationName":"server.example.com","Origin
atingServer":"NEWSERVER (00.01.0000.001)\r\n","Item":{"Attachments":"newfile.xls
(000000)","Id":"AAAAAAAAAAAA/
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA","ParentFo
lder":{"Id":"AAAAAAAAAAAA/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA","Path":"\\My
Folders\\Personal Folders - 2000\\Jan 2000"},"Subject":"AA00: RTF - AAA "}}
```

Mappings

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

Log fields	McAfee ESM fields
CreationTime	first time, last time
ResultStatus	action
Workload	application
ClientIP, ClientIPAddress, ActorIpAddress	source IP address
Operation	sid, msg, sigid
UserId, MailboxOwnerUPN	user name
RecordType	request type
ua, UserAgent	user agent
AzureActiveDirectoryEventType	attribute type
UserType	authentication type
ObjectID	URL
ItemType	object type
OrganizationName	domain
Subject	subject
ExternalAccess	access privileges
ClientApplication	process name
ChannelGuid	instance GUID

Microsoft Windows DHCP

Contents

Configure Microsoft Windows DHCP

Enable DHCP server audit logging.

Task

1 Open the DHCP Microsoft Management Console (MMC) snap-in.

2 In the console tree, select the DHCP server that you want to configure.

For Server 2008 and later, expand the navigation tree and select **IPv4** or **IPv6**.

3 From the **Action** menu, select **Properties**.

4 On the **General** tab, select **Enable DHCP audit logging**, then click **OK**.

5 (Optional) Click the **Advanced** tab and enter the logging path in the **Audit log file path**.

By default, the location of DHCP audit logs is **%windir%\System32\dhcp**.

Add Microsoft Windows DHCP

This data source supports multiple modes of data delivery, including SCP, HTTP, FTP, SFTP, NFS, and CIFS/ Windows File Share. Additional setup might be required on the DHCP server to allow sending data to the McAfee Event Receiver using these methods.

The recommended method for data delivery is to use the McAfee Collector. These agents have the added benefit of being able to send only the logs that haven't yet been sent, eliminating duplicates.

See the respective delivery method documentation for setup and usage information.

Configure McAfee Collector for Microsoft Windows DHCP

This data source supports multiple modes of data delivery.

Option	Definition
Name	A unique name
Host ID	Optional – A unique host ID
Data Source IP	IP Address of data source
Log Directory	Enter path to DHCP audit log files.
Log File	Enter `Dhcp*.log` to gather all DHCP audit logs.
Tail Mode	Beginning of file
Multi-line Events	Unchecked
Event Delimiter	None
Event Delimiter is a Regex	None
Max Lines Per Max Event	1
Enabled	Checked

Add Microsoft Windows DHCP

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Microsoft**
Data Source Model	**Windows DHCP (ASP)**
Data Format	**Default**
Data Retrieval	**MEF**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Use encryption	Enable to require the Receiver to communicate over TLS.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Microsoft Windows DHCP events to McAfee Fields

Log format

For platforms earlier than Windows Server 2008: the expected format for this device is:

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address,
```

The expected format for this device is as follows for Windows Server 2008 and 2008 R2

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name,
TransactionID,QResult,Probationtime,CorrelationID,
```

The expected format for this device is as follows for Windows Server 2012 and above:

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name,
TransactionID,QResult,Probationtime,
CorrelationID,Dhcid,VendorClass(Hex),VendorClass(ASCII),UserClass(Hex),UserClass(ASCII),Relay
AgentInformation,DnsRegError
```

Log sample

This is a sample log from a Windows Server 2003 DHCP device:

```
35,01/01/01,01:01:01,DNS update request failed,192.0.2.1,sampleHost,000000000000,
```

This is a sample log from a Windows Server 2008 DHCP device:

```
10,01/01/01,01:01:01,Assign,192.0.2.10,sampleHost1,000000000000,,17739,0,,,
```

This is a sample log from a Windows Server 2012 R2 DHCP device:

```
10,01/01/01,01:01:01,Assign,192.0.2.20,sampleHost2,
000000000000,,3096562285,0,,,,0x4D53465420352E30,MSFT 5.0,,,,0
```

Mappings

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

Log Fields	McAfee ESM Fields
ID	Sid
IP Address	Source IP
Host Name	Host
MAC Address	Source MAC
Date + Time	First Time, Last Time
TransactionID	Session ID
User Name	Source User
QResult	Return_Code
VendorClass(ASCII)	External_Device_Name
DnsRegError	DNS – Response_Code

Microsoft Windows Event Log WMI

Contents

Configure Microsoft Windows Event Log WMI

Use Microsoft Windows Event Log WMI to pull events directly using the McAfee Event Receiver.

Task

1 Do one of the following:

- For Windows XP, Server 2003, or later, create a user account added to the Administrators group.
- For Windows 8.1 or Server 2012 R2, use the Administrator user account or create a user account and add it to the Administrators, Distributed COM Users, and Event Log Readers groups.

2 If using the second option, configure the data source to use RPC.

Add Microsoft Windows Event Log WMI

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Use System Profiles	System Profiles are a way to use settings that are repetitive in nature, without having to enter the information each time.
Data Source Vendor	**Microsoft** (set by default if using profile)
Data Source Model	**Windows Event Log** WMI (set by default if using profile)
Data Format	**Default**
Data Retrieval	**Default**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
NetBIOS Name	The NetBIOS name (host name) associated with the data source device
Username	The user name of the account being connected to on the data source device
Password	The password of the account being connected to on the data source device
Event Logs	The names of the Windows event logs to be collected
Interval	How long the Receiver waits before checking for new data
Use RPC	Use RPC – Whether to use Remote Procedure Calls (RPC) to connect to the data source device
Connect	Tests the connection to the data source device

Microsoft Windows Event Log events to McAfee fields

Log format

The expected format for this device is:

```
<dsip>(%s)||<Log File>(%s)||<Record Number>(%u)||<Source Name>(%s)||<Event ID>(%d)||<Windows
Version>(%d)||<Time Generated>(%u)||<Event Type>(%u)||<Computer Name>(%s)||<User>(%s)||
<Category>(%s)||<Number of Insertion Strings>(%d)||<Insertion Strings>(%s)||<Message>(%s)
```

Log sample

This is a sample log from a WMI data source:

```
10.33.146.158||System||164812||NtServicePack||4377||52||1387354608||3||MYOFFICEPC||MYDOMAIN
\MyUserName||||2||Windows Server 2003||KB2892076||Windows Server 2003 Hotfix KB2892076 was
installed.
```

Motorola AirDefense

Contents

Configure Motorola AirDefense

Task

1 Log on to the AirDefense user interface. The dashboard opens by default.

2 From the **Tools** menu, select **Configuration**. By default, the **User Preferences** section is displayed.

3 Click the **Notification Manager** tab.

4 To add a syslog destination, click **Add**.

5 In the **Create Notification** window, select **Syslog** as the type, and enter the IP address of the syslog server.

6 (Optional) Set the default intervals for the notification system, and enable or disable all syslog notifications. To log everything, all syslog notifications must be enabled.

Add Motorola AirDefense

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Motorola**
Data Source Model	**AirDefense**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Time Zone	Time zone of data being sent.

Motorola AirDefense events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a Motorola AirDefense device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log Fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

NetFort Technologies LANGuardian

Contents

Configure NetFort Technologies LANGuardian

Task

1 From the LANGuardian web interface, navigate to the **Configuration** page.

2 In the **System** section, click **Configuration,** set theIP address and SNMP collectors of the system.

3 On the **Configuration** page, find the field named **[Beta] Splunk Syslog Collector**.

4 Enter the IP address of the McAfee Event Receiver, then click **Save**.

Add NetFort Technologies LANGuardian

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**NetFort Technologies**
Data Source Model	**LANGuardian (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

NetFort Technologies LANGuardian events to McAfee fields

Log format

The expected format for this device is:

```
<priority> <date> <time> LANGuardian event[<event ID>]: sen_id=<ID> app_id=<ID> src_ip=<IP
address> dest_ip=<IP address> host=<web host> uri=<URI>
```

Log sample

This is a sample log from a NetFort Technologies LANGuardian device:

```
<123>Jan 01 01:01:01 LANGuardian event[1234]: sen_id=1 app_id=1 src_ip=192.0.2.1
dest_ip=192.0.2.2 host=example.example.com uri=/directory/directory2/file
```

Mappings

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

Log fields	McAfee ESM fields
date, time	First Time, Last Time
appname	Application
src_ip	Source IP
dest_ip	Destination IP
host	Domain
from_addr, username	Source User
to_addr	Destination User
subject, database	Object
smb_action	Command

NetWitness Spectrum

Contents

Configure NetWitness Spectrum

Task

1 Browse to System settings **Syslog Auditing**.

2 Select **CEF** from the drop-down list.

3 Enter the IP address/host name and port of McAfee Event Receiver.

Add NetWitness Spectrum

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**NetWitness**
Data Source Model	**Spectrum CEF (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

NetWitness Spectrum events to McAfee fields

Log sample

```
Jun 1 18:28:57 NWAPPLIANCE12921 CEF:0|NetWitness|Spectrum|1.1.5.6|Suspicious Event|Detected
suspicious network event ID 69933879 session ID 201323609982|2|static=69.0 nextgen=35.0
community=2.0 sandbox=N/R file.name=exe file.size=420.00 KB (430,080 bytes)
```

```
file.md5.hash=220e976618d1e2e3e2525833a1e288b1 com.netwitness.event.internal.id=201323609982
com.netwitness.event.internal.uuid=564e2120-68e2-44c4-b512-01cf4ca63fd5 country.dst.code=US
city.dst=New York org.dst=The Nasdaq Omx Group payload=910876 packets=758 country.dst=United
States time=Sat Jun 01 17:15:00 EDT 2013 tcp.srcport=49528
com.netwitness.event.internal.source=http://159.79.148.225:50103/sdk filetype=x86 pe
latdec.dst=40.7082 eth.src=00:17:DF:4B:6C:00 tcp.flags=25 ip.proto=6 ip.src=10.85.0.32
tcp.dstport=80 eth.dst=00:1D:70:83:1B:80 lifetime=0 did=us01nwdecod02 sessionid=201323609982
HomeNet.src=HomeNet medium=1 size=952612 content=application/x-msdownload
longdec.dst=-74.0132 rid=121375362485 eth.type=2048 ip.dst=198.55.130.62 service=80 ...
```

Mappings

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

Log Fields	McAfee ESM fields
file.name	Destination_Filename.Destination_Filename
filetype	File_Type.FileType
threat.category	Category.Category
File.md5.hash	File_Hash.File_Hash
domain.dst	domain
ip.proto	protocol
host	hostname
ip.src	src_ip
ip.dst	dst_ip
tcp.srcport	src_port
tcp.dstport	dst_port
eth.src	src_mac
eth.dst	dst_mac
sessionid	sessionid
time	firsttime/lasttime

Niara

Contents

Configure Niara

Task

1 Set up Forwarding.

   a From the Niara Analyzer Interface, navigate to **System Configuration** | **Syslog Destinations**.

   b Fill in the **Parameter Description**, for example, `McAfee ESM`.

   c In the **Syslog Destination** field, enter the IP address or host name of the McAfee Event Receiver.

d Set the protocol (default is **UDP**).

e Set the port (default is **514**).

2 Set up Notification.

a From the Niara Analyzer Interface, navigate to **System Configuration** | **Security Alerts/Emails**.

b Click **Add New**.

c Select **Enable Alert Syslog Forwarding**.

d Leave the default values for **Query**, **Severity**, and **Confidence**.

e For **Sending Notification**, select **As Alerts are produced**.

f For **TimeZone**, set as your local time zone.

Add Niara

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Niara**
Data Source Model	**Niara**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Niara events to McAfee fields

Log format

The expected format for this device is:

```
DATE TIME HOSTNAME KEY=VALUE KEY=VALUE KEY=VALUE…
```

Log sample

This is a sample log from a device:

```
Jan  1 01:01:01 example.hostname msg_type=alert detection_time="2001-01-01 01:01:01 -01:00"
alert_name=BitTorrent alert_type="P2P Application" alert_category="Policy Violation"
alert_severity=40 alert_confidence=40 attack_stage=Infection user_name=unknown
src_host_name=unknown src_ip=192.0.2.1 dest_ip=192.0.2.2 description="IP Address 192.0.2.1
downloaded BitTorrent application on Jan 01, 2001"
alert_id="bittorrent&192.0.2.1&BitTorrent&example.com"
```

Mappings

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

Log fields	McAfee ESM fields
detection_time	First Time, Last Time
alert_name	Message
alert_type	Threat_Name
alert_category	Threat_Category
alert_severity	Severity
alert_confidence	Confidence
user_name	Source Username
src_host_name	Host
src_ip	Source IP
dest_ip	Destination IP
description	Description
alert_id	Message_Text

Nortel Networks Contivity

Contents

Configure Nortel Networks Contivity

Task

- In the command line interface (CLI), enter these commands:
  - **`enable`** *`password`* where *`password`* is your administrative password.
  - **`config t`**
  - **`logging`** *`ip address`* **`facility-filter all level all`** where *`ip address`* is the IP address of the McAfee Event Receiver.
  - **`exit`**

Add Nortel Networks Contivity

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Nortel Networks**
Data Source Model	**Contivity (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

Nortel Networks Contivity events to McAfee fields

Log sample

This is a sample log from a Nortel Contivity device:

```
<131> 272 06/18/2014 10:33:00 tEvtLgMgr 0 : tIsakmp [03] No proposal chosen in message from
10.10.3.21
<134> 272 06/18/2014 10:33:00 tEvtLgMgr 0 : Security [06] Session: IPSEC[uname] attempting
login
```

Mappings

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

Log fields	McAfee ESM fields
Usernames	Source Username
First IP address	Source IP
Second IP address	Destination IP
Groups	Group_Name
File names	Filename
Message type	Category

Severity map

Each log that contains the following severity format (in brackets) is mapped according to the following sample and table:

```
<134> 272 06/18/2014 10:33:00 tEvtLgMgr 0 : Security [06] Session: IPSEC[uname] attempting
login
```

The following table shows the conversion from the severity level in the Nortel log to the severity level recorded in the ESM:

Nortel severity	McAfee ESM severity
01	99 (Emergency)
02	75 (Critical)
03	60 (Error)
04	50 (Warning)
05	25 (Alert)
06	10 (Debug)
07	10 (Informational)

Nortel Networks Passport 8000 Series Switches

Contents

Configure Nortel Networks Passport 8000 Series Switches

This syslog configuration is done at the command line. See your product documentation for instructions about how to access and use the command line.

Task

1 At the command line, enter this command:

```
config sys syslog host <ID>
```

where *<ID>* is the ID of the host that is sending syslog events. The ID can be a number from 1–10.

2 Specify where to send syslog events:

```
address <IP address>
```

where *<IP address>* is the IP address of the McAfee Event Receiver.

3 Specify the facility:

```
host <ID> facility local0
```

Replace *<ID>* with the ID used in **Step 1**.

4 Enable the host:

```
host enable
```

5 Specify the severity level:

```
host <ID> severity info
```

Replace <*ID*> with the ID used in **Step 1**.

6 Enable the host to send syslog events:

```
state enable
```

Add Nortel Networks Passport 8000 Series Switches

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Nortel Networks**
Data Source Model	**Passport 8000 Series Switches (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Nortel Networks Passport 8000 Series Switches events to McAfee fields

Log format

The expected format for this device is:

```
<device> <date time> <log type> <severity> <message> <id> <port number> <MAC address>
```

Log sample

This is a sample log from a Nortel Networks Passport 8000 Series Switch device:

```
<123>DEVICE [01/01/01 01:01:01] SNMP INFO Spanning Tree Topology Change(StgId=123,
PortNum=1234, MacAddr=a1:b2:c3:d4:e5:f6)
```

Mappings

This table shows the mappings between the data source and McAfee ESM.

Log fields	McAfee ESM
Application	Application
User	Source User
IP Address	Source IP
Station	Source MAC
Interface	Object

Novell eDirectory

Contents

Configuring Novell eDirectory

See the Novell eDirectory product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add Novell eDirectory

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Novell**
Data Source Model	**eDirectory (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Novell eDirectory events to McAfee field mappings

Log format

The expected format for this device is:

```
<date time> <device name> <account> <domain> <user ID source> <domain ID> <SysAddr>
<SysName> <target CN> <target O> <action> <Event ID> <event class> <category> <severity>
```

Log sample

This is a sample log from a Novell eDirectory device:

```
Jan 01 01:01:01 eDirectory : INFO {"Source" : "eDirectory","Observer" : {"Account" :
{"Domain" : "ExampleDomain","Name" : "CN=ExampleName,O=domain"},"Entity" : {"SysAddr" :
"192.0.2.1","SysName" : "name"}},"Initiator" : {"Account" : {"Domain" :
"domain"}},"Target" : {"Data" : {"Name" : "CN=name,O=domain"}},"Action" : {"Event" : {"Id" :
"1.2.3.4","Name" : "name","CorrelationID" : "eDirectory","SubEvent" : "category"},"Time" :
{"Offset" : 1359410152},"Log" : {"Severity" : 1},"Outcome" : "1","ExtendedOutcome" : "1234"}}
```

Mappings

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

Log fields	McAfee ESM fields
SysName	Hostname
SysAddr	Source IP
NetAddress	Destination IP, Destination Port
Attribute Name	Object
Account: Name: CN	Source User
Target: Name: CN	Destination User
Account: Name: O, Target: Name: O	Domain

Log fields	McAfee ESM fields
Event: Name	Event_Class
Event ID	Signature_Name
Subevent	Category
ClassName	Target_Class
Privileges	Message_Text

Novell Identity and Access Management

Contents

Configure Novell Identity and Access Management

Task

1 From the application, select **Auditing** | **Novell Auditing**.

2 In the **Sever** field, enter the IP address or the FQDN of the McAfee ESM.

3 In the **Port** field, enter the listening port (default is 514).

4 Under **Management Console Audit Events**, specify the events you want to send.

5 Click **OK**.

Add Novell Identity and Access Management

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Novell**
Data Source Model	**Identity and Access Management – IAM (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent.

Novell Identity and Access Management events to McAfee field mappings

Log format

The expected format for this device is:

```
<date time> <device IP> <device name> <date time> device name> <application> <hostname>
<Source IP> <User Identifier> <URL>
```

Log sample

This is a sample log from a Novell Identity and Access Management device:

```
<123>Jan 01 01:01:01 192.0.2.1 Novell Access Manager\AG\URL Acc:[wMon, 01 Jan 2001 01:01:01
+0100] [Novell Access Manager\AG\URL Access]: AMDEVICEID#hostname:
AMAUTHID#3authorizationID: AMEVENTID#eventID: Source IP Address: [192.0.2.2] User
Identifier: [cn=12345678,ou=unit,O=domain] Accessed URL [https://example.com]
```

Mappings

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

Log fields	McAfee ESM fields
AMDEVICEID	Hostname
Application	Application
Source ID Address, Remote Client IP Addr	Source IP
User Identifier, cn	Username
URL	URL

Oracle Audit (SQL)

Contents

Configure Oracle Audit (SQL)

Task

1 Enter db as the AUDIT_TRAIL parameter.

Example:

```
ALTER SYSTEM SET AUDIT_TRAIL=db;
```

2 Restart the service for the change to take effect.

3 Enable auditing for the appropriate tables.

Add Oracle Audit (SQL)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Oracle**
Data Source Model	**Oracle Audit – SQL Pull (ASP)**
Data Format	**Default**
Data Retrieval	**SQL (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address associated with the data source device.
User ID	User ID with access to Audit DB
Password	Password for user
Port	Database port (default is 1521)
Database SID	SID for Audit DB
Poll Frequency	Enter a polling frequency in seconds
Time Zone	Time zone of data being sent.

Oracle Audit (SQL) events to McAfee fields

Log format

The expected format for this device is:

```
AUDIT_TYPE="" SESSION_ID="" PROXY_SESSIONID="" STATEMENTID="" ENTRYID=""
EXTENDED_TIMESTAMP="" GLOBAL_UID="" DB_USER=" " CLIENT_ID="" ECONTEXT_ID="" EXT_NAME=""
OS_USER="" USERHOST="" OS_PROCESS="" TERMINAL="" INSTANCE_NUMBER="" OBJECT_SCHEMA=""
OBJECT_NAME="" POLICY_NAME="" NEW_OWNER="" NEW_NAME="" ACTION="" STATEMENT_TYPE=""
AUDIT_OPTION="" TRANSACTIONID="" RETURNCODE="" SCN="" COMMENT_TEXT="" SQL_BIND=""
SQL_TEXT="" OBJ_PRIVILEGE="" SYS_PRIVILEGE="" ADMIN_OPTION="" OS_PRIVILEGE="" GRANTEE=""
PRIV_USED="" SES_ACTIONS="" LOGOFF_TIME="" LOGOFF_LREAD="" LOGOFF_PREAD="" LOGOFF_LWRITE=""
LOGOFF_DLOCK="" SESSION_CPU="" OBJ_EDITION_NAME="" DBID=""
```

Log sample

This is a sample log from an Oracle Audit device:

```
AUDIT_TYPE="Standard Audit" SESSION_ID="1" PROXY_SESSIONID="0" STATEMENTID="1" ENTRYID="1"
EXTENDED_TIMESTAMP="2015-01-01 00:00:00.000" GLOBAL_UID="" DB_USER="QA" CLIENT_ID=""
ECONTEXT_ID="" EXT_NAME="" OS_USER="root" USERHOST="exampleUser" OS_PROCESS="1000:1000"
TERMINAL="unknown" INSTANCE_NUMBER="0" OBJECT_SCHEMA="" OBJECT_NAME="" POLICY_NAME=""
NEW_OWNER="" NEW_NAME="" ACTION="100" STATEMENT_TYPE="LOGON" AUDIT_OPTION=""
TRANSACTIONID="0013000D00AAFF2" RETURNCODE="0" SCN="0" COMMENT_TEXT="Authenticated by:
DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=192.0.2.1)(PORT=37063))" SQL_BIND=""
SQL_TEXT="" OBJ_PRIVILEGE="" SYS_PRIVILEGE="" ADMIN_OPTION="" OS_PRIVILEGE="NONE" GRANTEE=""
PRIV_USED="CREATE SESSION" SES_ACTIONS="" LOGOFF_TIME="" LOGOFF_LREAD="0" LOGOFF_PREAD="0"
LOGOFF_LWRITE="0" LOGOFF_DLOCK="" SESSION_CPU="0" OBJ_EDITION_NAME="" DBID="1234567890"
```

This is a sample log from an Oracle Unified Audit device

```
          AUDIT_TYPE="Standard Audit" SESSION_ID="1" PROXY_SESSIONID="0" STATEMENTID="1"
ENTRYID="1" EXTENDED_TIMESTAMP="2015-01-01 00:00:00.000" ACTION_NAME "ALTER USER"
GLOBAL_UID="" CLIENT_PROGRAM_NAME="sqlplus@hostname" DB_USER="TESTUSER" CLIENT_ID=""
EXT_NAME="" OS_USER="root" USERHOST="exampleUser" OS_PROCESS="1000:1000" TERMINAL="unknown"
DBID="1234567890" AUTHENTICATION_TYPE="(TYPE=(OS));(CLIENT ADDRESS=((ADDRESS=(PROTOCOL=tcp)
(HOST=127.0.0.1)(PORT=54526))))" INSTANCE_NUMBER="0" OBJECT_SCHEMA="" OBJECT_NAME=""
POLICY_NAME="" NEW_NAME="" AUDIT_OPTION="" TRANSACTIONID="0013000D00AAFF2" RETURNCODE="0"
SCN="0" COMMENT_TEXT="Text comment on the audit trail entry, if any" SQL_BIND=""
SQL_TEXT="SELECT SYS_CONTEXT('USERENV','CDB_NAME'), SYS_CONTEXT('USERENV','CON_NAME') FROM
SYS.DUAL" OBJ_PRIVILEGE="" SYS_PRIVILEGE="" ADMIN_OPTION="" PRIV_USED="CREATE SESSION"
UNIFIED_AUDIT_POLICIES="ORA_SECURECONFIG, ORA_SECURECONFIG"
```

Mappings for DBA_COMMON_AUDIT_TRAIL

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

Log fields	McAfee ESM fields
RETURNCODE	Action, Return_Code
AUDIT_TYPE	Category
DBID	Database_ID
OS_USER	Destination User
EXTENDED_TIMESTAMP	First Time, Last Time
USERHOST	Host
STATEMENT_TYPE	Action, Rule Message
OBJECT_NAME	Object

Log fields	McAfee ESM fields
POLICY NAME	Policy Name
COMMENT_TEXT	Protocol, Source IP, Source Port
SQL_TEXT	SQL_Statement
SESSION_ID	Session_ID
ACTION	SID
DB_USER	Source User

Mappings for UNIFIED_AUDIT_TRAIL

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

Log fields	McAfee ESM fields
RETURN_CODE	Action, Return_Code
AUDIT_TYPE	Category
DBID	Database_ID
OS_USERNAME	Destination User
EVENT_TIMESTAMP	First Time, Last Time
USERHOST	Host
ADDITIONAL_INFO	Message_Text
OBJECT_NAME	Object
OBJECT_SCHEMA	Database_Name
AUTHENTICATION_TYPE	Protocol, Source IP, Source Port
FGA_POLICY_NAME	Policy_Name
SESSIONID	Session_ID
ACTION_NAME	SQL_Command, sid
CLIENT_PROGRAM_NAME	Application
UNIFIED_AUDIT_POLICIES	Rule_Name
DBUSERNAME	Source User
SQL_TEXT	SQL_Statement
SYSTEM_PRIVILEGE_USED	Command

Oracle Audit (syslog)

Contents

Configure Oracle Audit (syslog)

Task

1 Enter OS as the AUDIT_TRAIL parameter.

Example:

```
ALTER SYSTEM SET AUDIT_TRAIL=OS;
```

2 Edit the initsid.ora configuration file and enter the facility and priority in the AUDIT_SYSLOG_LEVEL parameter.

Example:

```
AUDIT_SYSLOG_LEVEL=facility.priority
```

3 Log on to the server with the syslog configuration file, `/etc/syslog.conf`, with root permissions.

4 Add the audit file location to `syslog.conf`

5 Restart the syslog logger (example: `/etc/rc.d/init.d/syslog restart`).

6 Restart the database instance (example: `CONNECT SYS / AS SYSOPER`).

Add Oracle Audit (syslog)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Oracle**
Data Source Model	**Oracle Audit (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address associated with the data source device
Syslog Relay	None
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Oracle Audit (syslog) events to McAfee fields

Log format

The expected format for this device is as follows:

```
<Priority Number>Process Name[]: LENGTH: '' ACTION:[] SQLTXT DATABASE USER:[] PRIVILEGE:[]
CLIENT USER:[] CLIENT TERMINAL:[] STATUS:[] DBID:[]
```

Log sample

This is a sample log from an Oracle Audit device:

```
<133>Oracle Audit[8435]: LENGTH : '317' ACTION :[168] 'select decode(status, 'OPEN', 1, 0),
decode(archiver, 'FAILED', 1, 0), decode(database_status, 'SUSPENDED', 1, 0)
into :status, :archstuck, :dbsuspended from v$instance' DATABASE USER:[1] '/' PRIVILEGE :[6]
'SYSDBA' CLIENT USER:[6] 'oracle' CLIENT TERMINAL:[0] '' STATUS:[1] '0' DBID:[10]
'1234567890'
```

Mappings

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

Log fields	McAfee ESM fields
STATUS, RETURNCODE	Action
DBID	Database_ID
CLIENT USER, OS$USERID	Destination User
EXTENDEDTIMESTAMP	First Time, Last Time
USERHOST	Host
Message	Message
OBJ$NAME, OBJECTNAME	Object
POLICY NAME	Policy Name
PRIVILEGE	Privileged_User
PROTOCOL	Protocol
RETURNCODE, STATUS	Return_Code
Session ID	Session ID
Signature ID	Signature ID
HOST	Source IP
PORT	Source Port
DATABASE USER, USERID	Source User
SQL TEXT, ACTION	SQL_Statement

Oracle Audit (XML)

Contents

Configure Oracle Audit (XML)

Task

1. Enter XML as the AUDIT_TRAIL parameter.

   Example: `ALTER SYSTEM SET AUDIT_TRAIL=XML;`

2. Restart the service for the change to take effect.
3. Enable auditing for the appropriate tables.
4. Optionally, change the directory in which audit trail files are written.

   Example: `ALTER SYSTEM SET AUDIT_FILE_DEST = '/audit_trail' DEFERRED;`

5. Navigate to the file destination you set, and open the XML once it is generated. Ensure that the audit trail is being written inside that file.

Add Oracle Audit (XML)

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Oracle**
Data Source Model	**Oracle Audit – XML File Pull (ASP)**
Data Format	**Default**
Data Retrieval	**File (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address associated with the data source device.
Port	22
Number of lines per record	1
File copy timeout	1 second
Login timeout	1 second
Interval	15 minutes
File Completion	60 Seconds
Delete processed file	Unchecked
Path	Path to file
Wildcard expression	Wild card for log file (example: *.log)
Username	Device user name
Password	Device password
Transfer compression	Unchecked
Time Zone	Time zone of data being sent.

Events Oracle Audit (XML) events to McAfee fields

Log format

The expected format for this device is:

```
<AuditRecord><Audit_Type></Audit_Type><Session_Id></Session_Id><StatementId></
StatementId><EntryId></EntryId><Extended_Timestamp></Extended_Timestamp><DB_User></
DB_User><Userhost></Userhost><OS_Process></OS_Process><Terminal></
Terminal><Instance_Number></Instance_Number><Returncode></Returncode><Scn></
Scn><OSPrivilege></OSPrivilege><DBID></DBID> <Sql_Text></Sql_Text></AuditRecord>
```

Log sample

This is a sample log from an Oracle Audit device:

```
<AuditRecord><Audit_Type>0</Audit_Type><Session_Id>0</Session_Id><StatementId>0</
StatementId><EntryId>0</EntryId><Extended_Timestamp>2015-01-01T00:00:00.0000000</
Extended_Timestamp><DB_User>/</DB_User><Userhost>HOST.COMPANY.COM</
Userhost><OS_Process>12345</OS_Process><Terminal>UNKNOWN</Terminal><Instance_Number>2</
Instance_Number><Returncode>0</Returncode><Scn>0</Scn><OSPrivilege>NONE</
OSPrivilege><DBID>1234567890</DBID> <Sql_Text>select count(*), null, null from sys.default</
Sql_Text> </AuditRecord>
```

Mappings

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

Log fields	McAfee ESM fields
STATUS, RETURNCODE	Action
DBID	Database_ID
CLIENT USER, OS$USERID	Destination User
EXTENDEDTIMESTAMP	First Time, Last Time
USERHOST	Host
Message	Message
OBJ$NAME, OBJECTNAME	Object
POLICY NAME	Policy Name
PRIVILEGE	Privileged_User
PROTOCOL	Protocol
RETURNCODE, STATUS	Return_Code
Session ID	Session ID
Signature ID	Signature ID
HOST	Source IP
PORT	Source Port
DATABASE USER, USERID	Source User
SQL TEXT, ACTION	SQL_Statement

Oracle Unified Auditing (SQL)

Configure Oracle Unified Auditing (SQL)

Oracle 12c introduced Unified Auditing. Previously, separate audit trails were kept for individual components. The Unified Audit trail combines all auditing into a single audit trail. By default, Oracle 12c is in “Mixed Mode” and all log data is written to both the traditional locations and the new location. Once Unified Auditing is explicitly enabled, all audit data are stored in the new location exclusively.

Task

1 Verify whether Unified Auditing is enabled.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';
```

2 If this query returns the following, Unified Auditing has not been enabled.

```
PARAMETER  VALUE
------------------ ----------
Unified Auditing FALSE
```

3 To enable Unified Auditing in Oracle 12c, first shut down your Oracle databases and listeners that are associated to the Oracle Home.

4 Next, relink the Oracle executable to support Unified Auditing by doing the following:

Unix/Linux:

```
cd $ORACLE_HOME/rdbms/lib
```

```
make -f ins_rdbms.mk uniaud_on ioracle
```

Windows:

```
cd %ORACLE_HOME%\bin
```

```
mv orauniadu12.dll.dbl orauniaud12.dll
```

5 Start your Oracle databases and listeners associated to the Oracle Home.

6 Both ORA_SECURECONFIG and ORA_LOGON_FAILURES polices are enabled by default and can be configured as needed.

7 Enable auditing for the appropriate table(s).

Oracle Internet Directory Server

Contents

Configuring Oracle Internet Directory Server

Task

1 Log on to the Oracle Directory Manager as administrator.

2 In the **Navigator** pane, expand the **server** listing and select a server instance.

3 Click the **Debug Flags** tab.

4 Select **Debug Flags**.

5 Click **Save**.

Logs are stored in:

```
%ORACLE_HOME%/ldap/log
```

Add Oracle Internet Directory Server

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Oracle**
Data Source Model	**Internet Directory Server**
Data Format	**Default**
Data Retrieval	**MEF** (McAfee Event Format)
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Oracle Internet Directory Server events to McAfee fields

Log format

The expected format for this device is:

```
[Timestamp][ServerType][ThreadIdentifier][Severity][FunctionName][Hostname][PID][ThreadID] :
[[
BEGIN
ConnectionID MessageID OperationID OperationName ConnectionIP ConnectionDomain
Trace information
END
]]
```

Log sample

This is a sample log from an Oracle Internet Directory Server device:

LDAP Audit Logs:

```
[2015-06-09T20:07:18+00:00] [OID] [TRACE:16] [] [OIDLDAPD] [host: example.oraclecloud.com]
[pid: 29238] [tid: 8] ServerWorker (REG):[[
BEGIN
ConnID:10578 mesgID:1 OpID:0  OpName:bind ConnIP:192.168.2.2 ConnDN:Anonymous
INFO : gslfbidbDoBind * Version=3 BIND dn="cn=orcladmin" method=128
                  ConnId = 10578, op=0, IpAddr=10.10.10.10
2015-06-09T20:07:18 * INFO:gsleswrASndResult OPtime=2112 micro sec RESULT=0 tag=97
```

```
nentries=0
END
]]
```

System Logs:

```
[2015-06-09T20:13:56+00:00] [OID] [NOTIFICATION:16] [] [OIDLDAPD] [host:
example.oraclecloud.com] [pid: 29238] [tid: 0] Main:: Shutting down ... detaching shared
memory
```

Mappings

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

Log fields	McAfee ESM fields
Timestamp	First Time, Last Time
OperationName	Message
ConnectionIP	Source IP
ConnectionDomain	Domain
PID	PID
ConnectionID	External_Session_ID
OperationID	External_Event_ID

Configure McAfee Collector for Oracle Internet Directory Server

To configure the McAfee Collector to send events, edit the McAfee Collector configuration file.

Task

1 Open the configuration file at /opt/McAfee/siem/mcafee_siem_collector.conf.

2 Edit these values:

a Set `rec_ip` to the IP address of the McAfee Event Receiver.

b Set `rec_port` to `8082`.

c Set `rec_encrypt` to `0`.

d Set `type` to `filetail`.

e Set `ft_dir` to the folder that contains the Oracle Internet Directory Server logs.

f Set `ft_filter` to a wildcard expression that matches the log files.

g Set `ft_delim` to the following regular expression:

```
\x5b\d{4}\x2d\d{2}\x2d\d{2}T(?:\d{2}\x3a){2}\d{2}(?:\x2b|\x2d)\d{2}\x3a\d{2}\x5d
```

h Set `ft_delim_end_of_event` to `0`.

i Set `ft_start_top` to `1`.

3 Save and close the file.

Palo Alto Networks PAN-OS

Contents

Configure Palo Alto Networks PAN-OS

See your version of *PAN-OS Administrator's Guide* for the complete steps to set up a syslog server within the product.

Add Palo Alto Networks PAN-OS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Palo Alto Networks**
Data Source Model	**Palo Alto Firewalls (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Palo Alto Networks PAN-OS events to McAfee field mappings

Log format

The expected format for this device is:

Traffic Logs:

```
FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source
IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination
User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress
Interface, Log Forwarding Profile, FUTURE_USE, Session ID, Repeat Count, Source Port,
Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes,
```

```
Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE_USE,
Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Packets
Sent, Packets Received.
```

Threat Logs:

```
FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source
IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination
User, Application, Virtual System, Source Zone, Destination Zone, Ingress Interface, Egress
Interface, Log Forwarding Profile, FUTURE_USE, Session ID, Repeat Count, Source Port,
Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action,
Miscellaneous, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags,
Source Location, Destination Location, FUTURE_USE, Content Type
```

Log sample

This is a sample log from a Palo Alto PANOS device:

```
2001/01/01 01:01:01,0004A100455,THREAT,vulnerability,148,2001/01/01 01:01:01,
192.168.0.1,192.168.0.2,0.0.0.0,0.0.0.0,p-Main-Outbound-2,,,web-browsing,vsys1,firewall,irout
er,ethernet1/3,ethernet1/1,p-WeaselUrlLogging-Local4-NCR,2001/01/01
01:01:01,65534,1,80,1433,0,0,0x0,tcp,alert,"",HTTP JavaScript Obfuscation
Detected(31825),any,low,
```

Mappings

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

Log fields	McAfee ESM fields
Generation Time	First Time, Last Time
Source IP	Source IP
Destination IP	Destination IP
Rule Name	Signature_Name
Source User	Source User
Subtype, Application	Application
Hostname	Host
Inbound Interface	Interface
Source Zone	Source_Zone
Destination Zone	Destination_Zone
Message	Message_Text
Category	Category
Outbound Interface	Interface_Dest
Bytes Sent	Bytes_Sent
Bytes Received	Bytes_Received
Domain	Domain
NAT	NAT_Details
Direction	Direction
File Path	File_Path
MAC	Source MAC
Command	Command
Event ID	Event_Class

Log fields	McAfee ESM fields
External Host	External_Hostname
OS	Operating_System
Protocol	Protocol
URL	URL
Session ID	Session ID

PhishMe Intelligence

Contents

Configure PhishMe Intelligence

Task

1. Make sure that you have a recent version of Python installed, and the python-requests library.
2. Acquire the PhishMe Python scripts and configure the config.ini file with the PhishMe API credentials.
3. To execute the script, use the command:

```
python phishme_to_mcafee.py”
```

   - If you need a proxy to connect to PhishMe, change the `[proxy]:use` value to `True` and fill out your proxy information in the following two fields.
   - Verify that any absolute paths are correct for your operating system.
   - To send Indicators of Compromise (IOCs) to McAfee ESM via CEF, set `[output-cef]:use` to `True` and provide a host name/IP address and port where you want to send CEF events.
   - For Cyber Threat Feeds, set up the McAfee ESM integration to output STIX files to a directory: set `[output-stix]:use` to `True` and provide the directory where you want to write the files.

Add PhishMe Intelligence

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**PhishMe**
Data Source Model	**Intelligence**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

PhishMe Intelligence events to McAfee field mappings

Log format

The expected format for this device is:

```
CEF:0|PhishMe|Intelligence|1.0|deviceEventClassId|name|Severity|URL/Domain externalID
category Malware Family First Published Brand Infrastructure Type ThreatHQ URL T3 Report URL
```

Log sample

This is a sample log from a device:

```
CEF:0|PhishMe|Intelligence|1.0|watchlist_url|Watchlist URL|10|cs4Label=Malicious URL
cs4=https://www.example.com/s/5rnzwnpnvlpqppf/modulo2.dat externalId=5879 cat=/ImpactRating/
Major cs1Label=Malware Family cs1=JAR Downloader deviceCustomDate1Label=First Published
deviceCustomDate1=1461106012435 cs2Label=Brand cs2=Generic Malware Threat
cs3Label=Infrastructure Type cs3=Location from which a payload is obtained cs5Label=ThreatHQ
URL cs5=https://www.example.com/p42/search/default?m\=5879 cs6Label=T3 Report URL
cs6=https://www.example.com/api/1/activethreatreport/5879/html
```

Mappings

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

Log fields	McAfee ESM fields
CEF.Event Name	Rule Message
CEF.Severity	Severity
externalId	External_EventID
Cat	Subcategory
dst	Destination IP
fname	File_Path

Log fields	McAfee ESM fields
fileHash	File_Hash
Malware Family	Threat_Name
T3 Report URL / Active Threat Report	Device_URL
Malicious URL	URL
Malicious Email	From
First Published	First Time, Last Time
Watchlist Domain	Object

PhishMe Triage

Contents

Configure PhishMe Triage

Task

1 Make sure you have a recent version of Python installed, and the python-requests library.

2 Acquire the PhishMe Python scripts and configure the config.ini file with the PhishMe API credentials.

3 To execute the script, use this command:

```
python phishme_to_mcafee.py”
```

- If a proxy is needed to connect to PhishMe, change the `[proxy]:use` value to `True` and fill out your proxy information in the following two fields.
- Verify that any absolute paths are correct for your operating system.
- To send Indicators of Compromise (IOCs) into McAfee ESM via CEF, set `[output-cef]:use` to `True` and provide a host name/IP address and port where you want to send CEF events.
- For Cyber Threat Feeds, set up McAfee ESM integration to output STIX files to a directory; set `[output-stix]:use` to `True` , and provide the directory where you want to write the files.

Add PhishMe Triage

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**PhishMe**
Data Source Model	**Triage**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

PhishMe Triage events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|PhishMe|Triage|2.0|Rule ID|Event|Severity|start rt Time Message Reported duser suser
cat Recipe Name Highest Priority Rule Matched - Priority Level Highest Priority Rule Matched
- Rule Name Report URL Subject
```

Log sample

This is a sample log from a device:

```
<13>Jan 1 01:01:01 phishme-triage Triage: I, [2016-01-01T20:10:51.914471 #62969] INFO -- :
CEF:0|PhishMe|Triage|2.0|1|Recipe Match|3|start=JAN 1 2016 01:01:01 rt=JAN 01 2016 01:01:01
deviceCustomDate1=JAN 01 2016 01:01:01 deviceCustomDate1Label=Time Message Reported
duser=user@example.com suser=user2@example.com cat=Crimeware cs1= cs1Label=Recipe Name cn1=4
cn1Label=Highest Priority Rule Matched - Priority Level cs2=Test_Rule cs2Label=Highest
Priority Rule Matched - Rule Name cs3=https://203.0.113.0/reports/1 cs3Label=Report URL
cs4=Review Documents cs4Label=Subject
```

Mappings

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

Log fields	McAfee ESM fields
start	First Time, Last Time
duser	Destination User
suser	Source User
cat	Threat_Category
Recipe Name	Policy_Name
Report URL	Device_URL

Log fields	McAfee ESM fields
Subject	Subject
Highest Priority Rule Matched – Rule Name	Rule_Name
Highest Priority Rule Matched – Priority Level	Priority
Rule ID, Event	Rule Message
Severity	Severity

Proofpoint Messaging Security Gateway

Contents

Configure Proofpoint Messaging Security Gateway

See *Proofpoint Messaging Security Gateway 7.2* for instructions about sending syslog event to a remote server. Use the McAfee Event Receiver IP address for the address of the remote server.

Add Proofpoint Messaging Security Gateway

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Proofpoint**
Data Source Model	**Messaging Security Gateway (ASP)**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Proofpoint Messaging Security Gateway events to McAfee fields

Log format

Filter log format provided by Proofpoint:

```
date Loglevel s=<External SessionID> mod=<Application> cmd=Command file=<File Name>
```

Log samples

This is a sample log from a Proofpoint Message Security Gateway device:

```
[2015-06-17 16:51:00.354586 -0700] rprt s=1v3jen000d m=1 x=1v3jen000d-1
omime=text/plain oext=txt corrupted=0 protected=0 size=159 virtual=0 a=0
mod=mail cmd=attachment id=0 file=text.txt mime=text/plain type=txt
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Hostname
Instancename	Severity
Serivcename|mod|module	Application
Timestamp	Firsttime | Lasttime
cmd	Command
ip	Source IP
Eid	Event Class
Session-id (s=)	External Session ID
Rule	Rule Name
File	Filename
Definitions	Object
Sudo=yes	Privileged User
Evt	Reason
Stage	Job Name
To	Destination User
Delay	Elapsed Time
port	Device Port

Raytheon SureView

Contents

Configure Raytheon SureView

See documentation for information about how to send CEF events through syslog to a remote server or McAfee ESM, and use the IP address of the McAfee Event Receiver for the address of the remote server.

Add Raytheon SureView

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Raytheon**
Data Source Model	**SureView (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

Raytheon SureView events to McAfee field mappings

Log format

The expected format for this device is:

```
CEF:<version>|<device vendor>|<device product>|<device version>|<signature ID>|<name>|
<severity>|<key=value> <key=value> <key=value>…
```

Log sample

This is a sample log from a Raytheon SureView device:

```
CEF:0|Raytheon|SureView|6.6|{1A2B3C4D-5E6F-1A2B-3C4D-5E6F1A2B3C4D}:1234|SIEM Notification3|1|
Event ={1A2B3C4D-5E6F-1A2B-3C4D-5E6F1A2B3C4D} fired at 1/1/01 1:1:01 PM coming from HOSTNAME
```

Mappings

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

Log fields	McAfee ESM fields
coming, AgentLabel, shost	Host
proto	Protocol
src	Source IP
dst	Destination IP
spt	Source Port
dpt	Destination Port
smac	Source MAC
dmac	Destination MAC
cnt	Event Count
dproc	Application
sntdom	Domain
fname, spriv	Object
UserLabel, suser	Source User
duser	Destination User
act	Event Subtype

Raz-Lee Security iSecurity Suite

Contents

Configure Raz-Lee Security iSecurity Suite

Use the command line interface (CLI) to configure your IBM iSeries (or AS/400) system.

Task

1 Log on to your IBM iSeries (or AS/400) system from the command line.

2 Type **STRAUD** and press **Enter**.

3 From the audit menu, select **System** | **Configuration**.

4 From the **System Configuration Menu**, select **SYSLOG** | **Definitions**.

- Set the value of **Send SYSLOG message** to **Yes**.
- Set the value of **Destination address** to the IP address of your McAfee Event Receiver.
- Set the value of **Facility to use** to your preferred facility level.
- Set the value of **Severity range to auto send** to your preferred severity range.

5 Save your changes.

Add Raz-Lee Security iSecurity Suite

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Raz-Lee Security**
Data Source Model	**iSecurity Suite**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

Raz-Lee Security iSecurity Suite events to McAfee fields

Log format

The expected format for this device is:

```
Timestamp   IP   MsgID   Object   File   User   Command   Job
```

The expected format for this device depends on the logged event.

Log sample

This is a sample log from a Raz-Lee Security iSecurity Suite device:

```
2016-03-01 03:31:47 Local6.Notice  192.0.2.0 AU RAZLEE Audit: MCA0100 *SECURITY Authority of
*N/*N *SOCKET /tmp/.ct_mc_0_srt929381427ac5388 changed for user profile *PUBLIC or
authorization list . Type of command used RPL. Access code (A-Added R-Removed N-None).
Authorities marked by Y were changed: OBJOPUY-Y OBJLOIS-Y *OBJOPR-Y *AUTLMGT- *AUTL- *READ-Y
*ADD- *UPD- *DLT- *EXCLUDE- *EXECUTE-Y *OBJALTER-Y *OBJREF-Y. Job 6784/QSYS/QYUSCMPOIU.
DLO , folder , on behalf of Office user . Personal status changed . QOpenSyys/'root' object .
```

Mappings

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

Log fields	McAfee ESM fields
Timestamp	First Time, Last Time
IP	Source IP
File	Filename
Program, Rcvr	Application
Object	Object
Source Port	Source Port
Dest Port	Destination Port
User	Source User
New User	Destination User
Job	Mainframe_Job_Name
CMD/Command	Command
Debug Message	Message_Text
Destination Host	Destination_Hostname
Group	Group_Name
Msg ID	Message_ID
Token Type	Authentication_Type
Library	Facility
Job Type/IPC Type	Job_Type
Renamed	New_Value
Device	External_Device_Name

Red Hat JBoss Application Server/WildFly 8

Contents

Configure Red Hat JBoss Application Server

By default, logs are stored locally in the installation directory for JBoss.

In a standalone system, that file is located in this directory: <INSTALL_PATH>/standalone/log/server.log

If JBoss is installed in a managed domain, the files are located in this directory: <INSTALL_PATH>/domain/servers/<SERVER_NAME>/log/server.log

Where <INSTALL_PATH> is the directory where JBoss was installed and <SERVER_NAME> is the server instance to be monitored.

Syslog is not natively supported for logging on to JBoss. You can retrieve these files using a file-pull method (for example SCP or SFTP) through the McAfee Event Receiver or Collector. You can also use a syslog program to send the information from the files directly to the McAfee Event Receiver. See the relevant product documentation for more information.

Configure WildFly 8

Task

- From the command line, run these commands:

```
/subsystem=logging/syslog-handler=syslog:add(syslog-format=RFC5424, level=INFO)
/subsystem=logging/root-logger=ROOT:add-handler(name=syslog)
/subsystem=logging/
syslog-handler=syslog:write-attribute(name=hostname,value="<ReceiverIpAddress>")
```

  where the <ReceiverIPAddress> is the IP address of the McAfee Event Receiver.

Add Red Hat JBoss Application Server/WildFly 8

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

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

Option	Definition
Data Source Vendor	**Red Hat**
Data Source Model	**JBoss / WildFly v8**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Red Hat JBoss Application Server/WildFly 8 events to McAfee fields

Log format

The expected format for this device, which is the default logging format, is:

```
Date Time Severity Class Thread LogID: Message
```

It is defined by the following string:

```
%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p [%c] (%t) %s%E%n
```

Log sample

This is a sample log from a Red Hat WildFly 8 device:

```
2017-05-15 02:22:20,825 INFO [org.jboss.as.server.deployment] (MSC service thread 1-3)
JBAS015876: Starting deployment of "fiveseries.war"
```

The expected format for the server.log is:

```
2017-02-16 21:53:19,520 INFO [org.jboss.as] (Controller Boot Thread) JBAS015961: Http
management interface listening on http://127.0.0.1:9990/management
```

```
2014-02-16 21:53:19,523 INFO [org.jboss.as] (Controller Boot Thread) JBAS015951: Admin
console listening on http://127.0.0.1:9990
```

```
2017-02-16 21:53:19,525 INFO [org.jboss.as] (Controller Boot Thread) JBAS015874: WildFly
8.0.0.Final \"WildFly\" started in 38820ms - Started 305 of 361 services (93 services are
lazy, passive or on-demand)
```

Mappings

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

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
LogID	Signature ID, External_EventID
Class	Target_Class
Severity	Severity

RedSeal Networks RedSeal 6

Contents

Configure RedSeal Networks RedSeal 6

See documentation for information about how to send syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add RedSeal Networks RedSeal 6

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**RedSeal Networks**
Data Source Model	**RedSeal 6 (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

RedSeal Networks RedSeal 6 events to McAfee fields

Log format

The expected format for this device is:

```
<date> - <key>=<value> | <key>=<value> | <key>=<value>…
```

Log sample

This is a sample log from a RedSeal Networks RedSeal 6 device:

```
Jan 01 1:01:01 - EventAction=Violation | EventDate=Jan 01, 2001 1:01:01 PM PDT |
EventName=BestPracticesCheckEvent | DeviceVendor=RedSeal Networks, Inc. |
DeviceProduct=RedSeal 6 | DeviceVersion=6.0.0 | RedSealServerName=example.net |
RedSealServerIPAddress=192.0.2.1 | EventSeverity=MEDIUM | HostName=hostname |
HostRedSealID=1a2b3c4d5e6f1a2b3c4d5e6f1a2b3c4d | Message=The SSH system service allows
protocol version 1 | CheckName=SSH Version 1 Enabled | FirstSeenDate=Jan 01, 2001 1:01:01 PM
PDT | LastSeenDate= Jan 01, 2001 1:01:01 PM PDT | FileLines=config:123 | Description="
```

Mappings

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

Log fields	McAfee ESM fields
HostName	Host
PrimaryService	Protocol
PrimaryIp	Source IP
RedSealServerIPAddress	Destination IP
EventAction	Application
PolicyName	Command
RedSealServerName	Domain
CheckName	Object
AttackDepth, Exposure, ServicesCount, VulnerabilityCount, Risk, DownstreamRisk, Confidence	URL
Message	Message_Text
OperatingSystem	Version
EventAction	Event Subtype
EventSeverity, Value	Severity

ReversingLabs N1000 Network Security Appliance

Contents

Configure ReversingLabs N1000 Network Security Appliance

See your product documentation for instructions about sending logs to a remote server. Use the McAfee Event Receiver IP address for the IP address of the remote server.

Add ReversingLabs N1000 Network Security Appliance

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ReversingLabs**
Data Source Model	**N1000 Network Security Appliance**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

ReversingLabs N1000 Network Security Appliance events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|deviceVendor|deviceProduct|deviceVersion|sig|eventName|severity|key value pairs
```

Log sample

This is a sample log from a ReversingLabs N1000 device:

```
CEF:0|ReversingLabs|N1000|1.0.0.0|detection|Threat detection|0|deviceDirection=0 proto=tcp
app=HTTP spt=8080 cn1=38974 dpt=50953 cs1=suspicious cn1Label=occurrence cs3=CERTIFICATE
dst=192.0.2.1 src=192.0.2.2 cs2Label=detectionName cs1Label=classification
cs3Label=detectionReason cs2=Win32.Certificate.Invalid start=2016-01-01 01:01:01.0+00:00
fileHash=01010101010101010101010101010101
```

Mappings

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

Log fields	McAfee ESM fields
start	First Time, Last Time
CEF Severity	Severity
proto	Protocol
app	Application
spt	Source Port
dpt	Destination Port
occurrence	Count

Log fields	McAfee ESM fields
classification	Event_Class
detectionName	Threat_Name
detectionReason	Category
deviceDirection	Direction
CEF DeviceProduct	External_Device_Type
filehash	File_Hash
fname	Filename
fsize	File_Size
fileType	File_Type
fileHash	File_Hash
oldFileHash	Parent_File_Hash
requestMethod	Method
dvc	Device_IP
dvchost	External_Device_Name
request	URL
act	Status

RioRey DDOS Protection

Contents

Configure RioRey DDOS Protection

See your product documentation for instructions about sending syslog events to a remote server. Use the McAfee Event Receiver IP address for the IP address of the remote server.

Add RioRey DDOS Protection

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**RioRey**
Data Source Model	**DDOS Protection**
Data Format	**SYSLOG (Default)**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

RioRey DDOS Protection events to McAfee fields

Log format

The expected format for this device is:

```
TimeStamp Host %EventSource: Message
```

Log sample

This is a sample log from a RioRey DDOS Protection device:

```
2014-01-01 01:01:01+00:00 abc-123 %SYSTEM: %ACD: AlarmInfoGet -> sysAlrm was
normal_ylw_off_red_off now normal_ylw_on_red_off
```

Mappings

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

Log fields	McAfee ESM fields
TimeStamp	First Time, Last Time
DeviceName	Hostname
EventSource	Application
Message	Message
was <Old_Value> now <New_Value>	Old_Value, New_Value
Victim IP	Victim_IP
Command	Command
Application	Application
Destination IP	Destination IP

Log fields	McAfee ESM fields
Source IP	Source IP
Threat	Threat_Category

Riverbed Steelhead

Contents

Configure Riverbed Steelhead using the Management Console

Task

1 From the Steelhead Management Console, click the **Setup** tab.

2 Click **Logging** to expand the logging menu.

3 Click **Remote Log Servers**.

4 In the **Add Remote Syslog Server** section, fill in the **Server IP** field with the IP address of the McAfee Event Receiver.

5 From the drop-down list, select a value for **Minimum Severity** of events to send to the McAfee Event Receiver.

6 Click **Add Server**.

7 Click **Save**.

Configure Riverbed Steelhead using the command line

This documentation assumes that you are already logged on to the command line interface (CLI) with administrative privileges. See the product documentation from Riverbed Steelhead for more information about how to access and use the command line interface.

Task

1 Set up remote logging.

```
logging <ip-address>
```

Replace <ip-address> with the IP address of the McAfee Event Receiver.

2 (Optional) Set the minimum severity of the events being sent.

```
logging <ip-address> trap <log level>
```

Where <ip-address> is the IP address of the McAfee Event Receiver, and <log level> is one of these settings:

Setting	Definition
`emerg`	Emergency
`alert`	Alert
`critical`	Critical
`err`	Error
`warning`	Warning
`notice`	Notice (default)
`info`	Informational

Add Riverbed Steelhead

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Riverbed**
Data Source Model	**Steelhead (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

Riverbed Steelhead events to McAfee fields

Log format

The expected format for this device is:

```
<priority><hostname>[<ID>]: [<service>/<name>] <Log ID> <message>…
```

Log sample

This is a sample log from a Riverbed Steelhead device:

```
<13>hostname[1234]: [splice/name.INFO] 1234567 {- -}  sock 123 id 123456 client
192.0.2.1:12345 server 192.0.2.2:56789 remote inner port 1234 trpy TRPY_NONE
```

Mappings

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

Log fields	McAfee ESM fields
hostname	Host
service	Application
Server, Client	Source IP
Remote	Destination IP
Server, Client	Source Port
Remote	Destination Port
Log ID	Session ID
Command	Command
host	Domain
module	Object
user	Source User

RSA Authentication

Contents

Configure RSA Authentication Manager 8 and later from the Security Console

Task

1 In the **RSA Authentication Manager Security Console**, navigate to **Setup** | **System Settings**.

2 In the **Basic Settings** section, select **Logging**.

3 Select the instance where you want to collect logs, then click **Next**.

4 In the **Log Levels** section:

   a Set **Administrative Audit Log** to **Success**

   b Set**Runtime Audit Log** to **Success**

   c Set **System Log** to **Warning**.

5 In **Log Data Destination**, set all three fields to **Save to remote database and internal Syslog at the following hostname or IP address**, and enter the host name or IP address of the McAfee Event Receiver.

6 Click **Save** to save changes.

Configure RSA Authentication Manager 7.1 SP2 or later for Linux

Task

1 Edit this file with a text editor: /usr/local/RSASecurity/RSAAuthenticationManager/utils/resources/ims.properties

2 Edit or add these lines in that file:

```
ims.logging.audit.admin.syslog_host = 192.0.2.1
ims.logging.audit.admin.use_os_logger = true
ims.logging.audit.runtime.syslog_host = 192.0.2.1
ims.logging.audit.runtime.use_os_logger = true
ims.logging.system.syslog_host = 192.0.2.1
ims.logging.system.use_os_logger = true
```

where 192.0.2.1 is the IP address of the McAfee Event Receiver.

3 Save and close the file.

4 Edit this file with a text editor: /etc/syslog.conf

5 Add this line:

```
*.* @192.0.2.1
```

where 192.0.2.1 is the IP address of the McAfee Event Receiver.

6 Restart the syslog daemon:

```
service syslog restart
```

Configure RSA Authentication Manager 7.1 SP2 or later for Windows

Task

1 Edit this file with a text editor: \Program Files\RSASecurity\RSAAuthenticationManager\utils\Resources\ims.properties

2 Edit or add these lines in the file:

```
ims.logging.audit.admin.syslog_host = 192.0.2.1
ims.logging.audit.admin.use_os_logger = true
ims.logging.audit.runtime.syslog_host = 192.0.2.1
ims.logging.audit.runtime.use_os_logger = true
ims.logging.system.syslog_host = 192.0.2.1
ims.logging.system.use_os_logger = true
```

where 192.0.2.1 is the IP address of the McAfee Event Receiver.

3 Save and close the file.

4 Restart the RSA Authentication Manager by navigating to **Start** | **Administrator Tools** | **Computer Management** | **Services and Applications** | **Services**.

5 Select **RSA Authentication Manager**.

6 Click **Restart**.

7 Open the **Authentication Manager Security Console** and select **Setup** | **Instances**.

8 Right-click the server instance and select **Logging**.

9 In the **Log Data Destination** section, select **Send system messages to OS system log**.

Add RSA Authentication Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**RSA**
Data Source Model	**Authentication Manager (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

RSA Authentication Manager events to McAfee fields

Mappings

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

Log fields	McAfee ESM fields
Date Time	First Time, Last Time
Severty	Severity
1st listed IP Address	Source IP
2nd listed IP Address	Destination IP
Event ID	Signature ID

SafeNet Hardware Security Modules

Contents

Configure SafeNet Hardware Security Modules

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

Add SafeNet Hardware Security Modules

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**SafeNet**
Data Source Model	**Hardware Security Modules (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

SafeNet Hardware-Security-Modules events to McAfee fields

Log format

The expected format for this device is:

```
firsttime hostname application: [firsttime] INFO src_ip [-] payctrlusr ID Crypto payctrlprd:
1 [op#1 ENCRYPTSTANDARD] - [action] [-]
```

Log sample

This is a sample log from a device:

```
<142>Apr 4 09:39:04 test.box.com testBox: [2016-04-04 09:39:04] INFO 172.0.0.1 [-]
payctrlusr 0 Crypto payctrlprd:3100660 [op#1 ENCRYPT AES] - [Success] [-]
```

Mappings

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

Log fields	McAfee ESM fields
firsttime	First Time, Last Time
hostname	Host
src_ip	Source IP
action	Event SubType
key name	Object
application	Application

Skycure Enterprise

Contents

Configuring Skycure Enterprise

Task

1. From the **Skycure Management Console**, go to **Dashboard** | **Configuration** and select **Configuration** next to **SIEM Integration**.
2. In the **IP Address** field, enter the IP address of the McAfee Event Receiver.
3. In the **Port** field, enter `514` (the default port for syslog).
4. In the **Protocol** field, select **UDP** from the drop-down list.
5. In the **Format** field, select **McAfee ESM** from the drop-down list.
6. Click **Save**.

Add Skycure Enterprise

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Skycure**
Data Source Model	**Skycure Enterprise**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Skycure Enterprise events to McAfee fields

Log format

The expected format for this device is:

```
<priority> <date> <time> <host> CEF:0|Skycure|Skycure|<version>|<event type>|<event name>|
<severity>|<key>=<value> <key>=<value> <key>=value>
```

Log sample

This is a sample log from a Skycure Enterprise device:

```
<123>Jan 01 2001 01:01:01 ip-192-0-2-1 CEF:0|Skycure|Skycure|1.0|suspicious_app_removed|
Suspicious App Removed|0|duid=123456789 duser=user@example.com msg=app was removed from
device #123456789 shost=ip-192-0-2-1 end=2001-01-01 01:01:01 UTC
```

Mappings

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

Log fields	McAfee ESM fields
shost	Host
Severity	Severity
EVENT_NAME	Message
end	First Time, Last Time
hotspot/ SSID	Object
User	Source User
duser	Destination User
version	Version

Log fields	McAfee ESM fields
duid	External_Device_Name
from	Old_Value
to	New_Value

Skyhigh Networks Cloud Security Platform

Contents

Configure Skyhigh Networks Cloud Security Platform

Task

1. From the Skyhigh Enterprise Connector interface, go to **Enterprise Integration** | **SIEM Integration**.
2. Change the value of **SIEM Server** to **ON**.
3. Select **Common Event Format (CEF)**.
4. Set the **Syslog Protocol** value to **UDP**.
5. For the **Syslog Server** value, enter the IP address of the McAfee Event Receiver.
6. For the **Syslog Port** value, type `514`.
7. Change the value for **Send Shadow service Anomalies to SIEM** to **All Anomalies**.
8. Change the value for **Send Sanctioned service Incidents to SIEM** to **All Incidents**.
9. Click **SAVE**.

Add Skyhigh Networks Cloud Security Platform

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Skyhigh Networks**
Data Source Model	**Cloud Security Platform**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to Communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Skyhigh Networks Cloud Security Platform events to McAfee fields

Log format

The expected format for this device is:

```
<PRIORITY>DATE TIME HOSTNAME CEF:0|DEVICE VENDOR|DEVICE PRODUCT|DEVICE VERSION|SIGNATURE ID|
NAME|SEVERITY|KEY=VALUE KEY=VALUE KEY=VALUE…
```

Log sample

This is a sample log from Cloud Security Platform:

```
<14>Jan 01 01:01:01 example.hostname CEF:0|Skyhigh|Anomalies|123|Service Category Based Data
Transfer|Download|5|start=2001-01-01 01:01:01.0 suser=exampleUser dst=example riskLevel=Low
anomalyType=Service Category
```

Mappings

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

Log fields	McAfee ESM fields
severity	Severity
start	First Time, Last Time
destinationHost	Destination Hostname
suser (if IP address)	Source IP
suser	Source Username
Direction	Direction
serviceName	Service_Name
response	Subtype

Log fields	McAfee ESM fields
riscValue	Reputation_Score
DeviceValue	Operating_System

Sophos Web Security and Control

Contents

Configure Sophos Web Security and Control

Task

1. From the web interface for Sophos Web Security and Control, navigate to **Configuration** | **System** | **Alerts** | **Monitoring**.
2. Click the **Syslog** tab.
3. Make sure that **Enable syslog transfer of web traffic** is selected.
4. In the **Hostname/IP** field, type in the IP address or host name of the McAfee Event Receiver.
5. In the **Port** field, enter the standard syslog port of **514**.
6. In the **Protocol** drop-down list, select **UDP**.
7. Click **Apply** to save the settings.

Add Sophos Web Security and Control

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Sophos**
Data Source Model	**Web Security and Control (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Sophos Web Security and Control events to McAfee fields

Log format

The expected format for this device is:

```
h=<remote host> u=<remote user> s=<HTTP status> X=<connection status> t=<timestamp>
T=<request time microseconds> Ts=<request time seconds> act=<action> cat=<URI category>
rsn=<reason> threat=<threat name> type=<MIME type> ctype=<content type> sav-ev=<engine
version> sav-dv=<data version> uri-dv=<URI list version> cache=<cache> in=<data in bytes>
out=<data in bytes> meth=<HTTP request method> ref=<HTTP referrer> ua=<User-Agent> req=<HTTP
request> dom=<web domain> filetype=<filetype category> rule=<policy rule ID> filesize=<size
of file> axtime=<time for access check> fttime=<time for file-typing> scantime=<scan time>
src_cat=<internal use> labs_cat=<internal use> dcat_prox=<internal use> target_ip=<resolved
IP> labs_rule_id=<internal use> reqtime=<request queue time> adtime=<Active Directory time>
ftbypass=<internal use>
```

Log sample

This is a sample log from a Sophos Web Security and Control device:

```
h=192.0.2.1 u="domain\\user" s=123 X=+ t=978310861 T=12345 Ts=0 act=1 cat="0x2300000123"
rsn=- threat="-" type="-" ctype="text/html" sav-ev=- sav-dv=- uri-dv=- cache=MISS in=123
out=123 meth=GET ref="-" ua="details" req="GET http://www.example.com/" dom="example.com"
filetype="-" rule="-" filesize=- axtime=0.000123 fttime=- scantime=- src_cat="-"
labs_cat="-" dcat_prox="-" target_ip="192.0.2.2" labs_rule_id="-" reqtime=- adtime=-
ftbypass=-
```

Mappings

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

Log fields	McAfee ESM fields
u	Source User
dom	Domain

Log fields	McAfee ESM fields
h	Source IP
target_ip	Destination IP
req	URL
threat	Object
rsn	Command
cat	Severity
act	Event Subtype

Sourcefire FireSIGHT Management Console

Contents

Configure Sourcefire FireSIGHT Management Console 5.x and later

Task

1. Log on to the FireSIGHT Management console (Defense Center).
2. Browse to **System > Local > Registration**.
3. Click **Create Client**.
4. Enter the IP address or host name of the McAfee Event Receiver and, as needed, a password to secure the certificate.
5. Save the new client settings.
6. Download the new client's certificate, which is used when creating the data source on McAfee ESM.
7. The McAfee Event Receiver currently pulls Discovery (RNA) and Intrusion Events. To allow it to collect both event types, select these options:
   - Discovery Events
   - Intrusion Events
   - Intrusion Event Packet Data
   - Intrusion Event Extra Data
8. Click **Save**.

Configure Sourcefire FireSIGHT Defense Center 4.10

Task

1 Log on to the Defense Center console.

2 Browse to **Operations** | **Configuration** | **eStreamer**.

3 Click **Create Client**.

4 Enter the IP address or host name of the McAfee Event Receiver and, as needed, a password to secure the Certificate.

5 Save the new Client settings.

6 Download the Certificate by clicking the link.

7 The McAfee Event Receiver currently pulls RNA and Intrusion Events. To allow it to collect both event types, select these options:

- RNA Events
- Intrusion Events
- Intrusion Event Packet Data
- Intrusion Event Extra Data

Add Sourcefire FireSIGHT Management Console - eStreamer

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Sourcefire**
Data Source Model	**FireSIGHT Management Console - eStreamer**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Port	**Default**
Collect Flows	Checked
Upload	This allows the user to upload and validate the certificate that was downloaded in the previous section.
Connect	Test the connection to the data source after the Certificate is downloaded.

Sourcefire FireSIGHT Management Console - eStreamer events to McAfee fields

Log format

The expected format of this device is the JavaScript Object Notation (JSON) format. The logs are similar to this sample:


```
{"Record Type": 104,"Record": "Intrusion Event 4.9 - 4.10.x","Server Timestamp":
1403652492,"Detection Engine": {"ID": 5,"Name": "xxx.yyy.zzz.com"},"Event ID": 153511,"Event
Second": 1402658492,"Event Microsecond": 68241,"Rule ID": {"Generator ID": 134,"Rule ID":
3,"Rule Revision": 1,"Rendered Signature ID": 3,"Message Length": 24,"Rule UUID":
0x11112222111122221111222211112222,"Rule Revision UUID":
0x11114444ssssaaaaa1111222233333221,"Message": "PPM_EVENT_PACKET_ABORTED"},"Generator ID":
134,"Rule Revision": 1,"Classification ID": {"Classification ID": 1,"Name":
"not-suspicious","Description": "Not Suspicious Traffic","UUID":
0x11111111112222222222333333333344},"Priority ID": {"ID": 3,"Name": "low"},"Source IPv4
Address": 1111333344,"Destination IPv4 Address": 1111222233,"Source Port/ICMP Type":
16615,"Destination Port/ICMP Code": 25,"IP Protocol ID": 6,"Impact Flags": 7,"Impact":
2,"Blocked": 0,"Reserved": 0,"VLAN ID": 0,"Pad": 0,"is_src_mac":
0xaa22113344dd,"is_dest_mac": 0x1122ddaa3344,"is_sigid": 2278188368}
```


Mappings

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

Log fields	McAfee ESM fields
Detection Engine, Detection Engine.Name, Sensor_Name	Sensor_Name
Detection Engine.Type, Sensor_Type	Sensor_Type
Detection Engine.UUID, Sensor_UUID	Sensor_UUID
Event Second, First/Last Seen, First/Last Used	First Time, Last Time
is_xforward, is_srcipv6, Source IPv4 Address, SourceIPv6	Source IP
is_destipv6, Destination IPv4 Address, DestinationIPAddress, DestinationIPv6	Destination IP
Is_src_port, Source Port/ICMP Type, SourcePort	Source Port
Is_dest_port, Destination Port/ICMP Code, DestinationPort	Destination Port
Is_src_mac, SourceMAC	Source Mac
Is_dest_mac, DestinationMAC	Destination Mac
Priority ID, Severity	Severity
Network Protocol, Host Type, ID, Attribute ID, Source Type, Protocol, Custom Product, Application	Application
Action, Blocked	Event Subtype
Bytes Sent	Bytes_Sent
Bytes Received	Bytes_Received
Drop User Product, Drop	Command
Protocol	Protocol
VLAN ID, Source VLAN ID	VLAN
EventCount	Event Count
Classification ID, Host Type, Source Type	Object
Domain, Version, Custom Version, Service Version	Domain
NetBIOS Name, CVE ID, Custom Vendor, Service Vendor name, Hostname	Host

Log fields	McAfee ESM fields
Source ID.Name, Username	Source User
Generator ID	External_EventID
Rule ID	External_SubEventID
Intrusion Policy ID	Policy_ID
UUID	UUID

Sourcefire FireSIGHT Management Console - eStreamer supported events

This is a list of all supported events from Defense Center.

- Record Type 7 - Intrusion Event
- Record Type 10 - New Host
- Record Type 11 - New TCP Service
- Record Type 12 - New UDP Service
- Record Type 13 - New Network Protocol
- Record Type 14 - New Transport Protocol
- Record Type 15 - New Client Application
- Record Type 16 - TCP Service Information Update
- Record Type 17 - UDP Service Information Update
- Record Type 18 - Operating System Update Message
- Record Type 19 - Host Timeout
- Record Type 20 - Host IP Address Reused
- Record Type 21 - Host Deleted: Host Limit Reached
- Record Type 22 - Hops Change
- Record Type 23 - TCP Port Closed
- Record Type 24 - UDP Port Closed
- Record Type 25 - TCP Port Timeout
- Record Type 26 - UDP Port Timeout
- Record Type 27 - MAC Information Change
- Record Type 28 - Additional MAC Detected for Host
- Record Type 29 - Host IP Address Changed
- Record Type 30 - Host Last Seen
- Record Type 31 - Host Identified as Router/Bridge
- Record Type 34 - VLAN Tag Information Update
- Record Type 35 - Client Application Timeout

- Record Type 37 - User Set Valid Vulnerabilities 4.0
- Record Type 38 - User Set Invalid Vulnerabilities 4.0
- Record Type 42 - NetBIOS Name Change
- Record Type 44 - Host Dropped: Host Limit Reached
- Record Type 45 - Update Banner Message
- Record Type 46 - Host Attribute Add
- Record Type 47 - Host Attribute Update
- Record Type 48 - Host Attribute Delete
- Record Type 51 - TCP Service Confidence Update
- Record Type 52 - UDP Service Confidence Update
- Record Type 71 - Flow/Connection Statistic
- Record Type 74 - User Set Operating System
- Record Type 78 - User Delete Address
- Record Type 80 - User Set Valid Vulnerabilities
- Record Type 81 - User Set Invalid Vulnerabilities
- Record Type 82 - User Host Criticality
- Record Type 83 - Host Attribute Set Value
- Record Type 84 - Host Attribute Delete Value
- Record Type 85 - User Add Hosts
- Record Type 86 - User Add Service
- Record Type 88 - User Add Protocol
- Record Type 89 - Host Service Data for RNA 4.9.0.x
- Record Type 92 - User Identity Dropped: User Limit Reached
- Record Type 93 - User Removed Change Event
- Record Type 94 - New User Identity
- Record Type 95 - User Login
- Record Type 101 - New OS Event
- Record Type 102 - Identity Conflict System Message
- Record Type 103 - Identity Timeout
- Record Type 104 - Intrusion Event
- Record Type 105 - Intrusion Event
- Record Type 107 - Client Application Messages
- Record Type 112 - Correlation Event
- Record Type 150 - Intrusion Policy

- Record Type 207 - Intrusion Event
- Record Type 208 - Intrusion Event

SSH Communications Security CryptoAuditor

Contents

Configure SSH Communications Security CryptoAuditor

Task

1 Log on to the web interface for CryptoAuditor as administrator.

2 Navigate to **Settings** | **External Services** | **External Syslog Servers** | **Add Syslog Server**.

   a Enter the IP address of the McAfee Event Receiver and port 514 (the default port for syslog).

   b Save and apply the changes.

3 Navigate to **Settings** | **Alerts** | **Add Alert Group**.

   a Enter a name for the group in the **Name** field.

   b In the **External Syslog server** drop-down list, select the IP address of the McAfee Event Receiver.

   c Save and apply the changes.

   d Under **Requests**, click the **+** icon next to each alert you want to add them to the newly created alert group.

   e Save and apply the changes.

Add SSH Communications Security CryptoAuditor

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**SSH Communications Security**
Data Source Model	**CryptoAuditor**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

SSH Communications Security CryptoAuditor events to McAfee fields

Log format

The expected format for this device is:

```
<facility>dateTime hostname CEF:0|Vendor|Product|Version|sigId|severity|rt=date
outcome=action
```

Log sample

This is a sample log from a CryptoAuditor device:

```
<189>Aug 18 16:17:47 auditor CEF:0|SSH|CryptoAuditor|1.5.2|4050|Admin_login|4|rt=Aug 18 2015
16:17:47 outcome=failure
```

Mappings

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

Log fields	McAfee ESM fields
sigID	Signature ID
rt	First Time, Last Time
externalID	External_EventID
src	Source IP
spt	Source Port
shost	Host
duser	Destination User
dst	Destination IP
dpt	Destination Port

Log fields	McAfee ESM fields
dhost	Destination_Hostname
outcome	Event Subtype
severity	Severity
msg	Rule Message
suser, SshAuditorAdminname	Source User
SshAuditorReason	Reason
SshAuditorRule	Policy_Name

STEALTHbits StealthINTERCEPT

Contents

Configure STEALTHbits StealthINTERCEPT

Task

1 Log in to StealthINTERCEPT.

2 Open the Administration Console.

3 From the menu bar, select **Configuration** | **Alerts**.

4 Click the **SIEM** tab and click **Configure** in the **SI System Alerting** window.

5 Enter the IP address of the Receiver in the **Host Address** field.

6 In the **Port** field, enter `514`.

7 From the **Mapping File** drop-down lists, select the **McAfee ESM SIEM** format.

8 Click **Events** and select the event types that you want for SIEM reporting.

9 Click **OK** to apply the new configuration.

Add STEALTHbits StealthINTERCEPT

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**STEALTHbits**
Data Source Model	**StealthINTERCEPT**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

STEALTHbits StealthINTERCEPT events to ESM fields

Log format

The expected LEEF Log format for this device is:

```
LEEF:1.0|Device Vendor|Device Product|Device Version|Signature
ID|Key value pairs
```

The expected CEF format for this device is:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Key value pairs
```

Log sample

This is a sample log from a device:

```
Oct 01 16:14:03 2008R264BITSRVR CEF:0|STEALTHbits|StealthINTERCEPT|3.1.262.1|Active
DirectoryuserObject ModifiedFalseTrue|Lockdown Disabled Users OU|3|rt=2014-10-01
10:14:02.258 sntdom=2008R264BITDOM suser=CN\=Administrator,CN\=Users,DC\=2008R264BitDomain,DC
\=com src=LDAP:[192.0.2.1]:5545 duser=CN\=DisabledUser2,OU\=Disabled OU,DC
\=2008R264BitDomain,DC\=com shost=2008R264BITDOM\2008R264BITSRVR msg=Policy_Name= Lockdown
Disabled Users OU Object_Class= user Success= False Blocked= True Attribute_Name=
userAccountControl New_Attribute_Value= Password is not required, Normal account
Old_Attribute_Value= Account is disabled, Password is not required, Normal account
Operation= Change Attribute
```

```
Sep 19 15:26:08 2008R264BITSRVR LEEF:1.0|STEALTHbits|StealthINTERCEPT|3.1.233.1|Active
DirectoryuserObject ModifiedFalseTrue|cat=Object Modified    devTimeFormat=yyyy-MM-dd
HH:mm:ss.SSS    devTime=2014-09-19 09:26:07.400    SettingName=Protected OU Lockdown
domain=2008R264BITDOM    usrName=NT AUTHORITY\ANONYMOUS LOGON    src=192.0.2.1
dst=192.0.2.2    DistinguishedName=CN=Brad,OU=ProtectedOU,DC=2008R264BitDomain,DC=com
AffectedObject=Brad    ClassName=user    OrigServer=2008R264BITDOM\2008R264BITSRVR
Success=False    Blocked=True    AttrName=lastLogonTimestamp    AttrNewValue={ 2014-09-19
09:26:07.4001154Z UTC }    AttrOldValue=    Operation=Change Attribute
```

Mappings

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

Log fields	McAfee ESM fields
CEF Event Message	Message
CEF Severity	Severity
Rt	First Time, Last Time
suser	Source User
shost	Hostname
src	Source IP, Source Port
Policy_Name	Policy_Name
Blocked	Action / Event Subtype
Success	Action / Event Subtype (Fallback)
Old_Attribute_Value	Old_Value
New_Attribute_Value	New_Value, Filename (when applicable)
Attribute_Name	Attribute_Type
duser	Object, Filename (when applicable)
Object_Class	Object_Type

Symantec Data Loss Prevention

Contents

Configure Symantec Data Loss Prevention

For successful integration of Symantec Data Loss Prevention with McAfee ESM, you must first enable syslog functionality. Once syslog is enabled, you must also add Response Rules in the Symantec Data Loss Prevention user interface.

Task

1 For Windows – Go to the directory \Vontu\Protect\config.

   For Linux – Go to the directory /opt/Vontu/Protect/config.

2 Open the file Manager.properties for editing.

3 Edit these three lines:

```
#systemevent.syslog.host=
#systemevent.syslog.port=
#systemevent.syslog.format=
```

a Remove the symbol '#' from these the beginning of each line.

b Set the value for `systemevent.syslog.host=` to the IP address of the McAfee Event Receiver.

c Set the value for `systemevent.syslog.port=` to the port where the McAfee Event Receiver is listening (default is 514).

d Set the value for `systemevent.syslog.format=` to `[{0}] {1} - {2}`.

The three original lines should now look similar to this:

```
systemevent.syslog.host=192.0.2.1
systemevent.syslog.port=514
systemevent.syslog.format=[{0}] {1} - {2}
```

4 Save these changes and restart the Vontu Server (Symantec Data Loss Prevention server).

Configure Symantec Data Loss Prevention for common event format (CEF)

Task

1 Log on to the Symantec DLP server with the appropriate permissions.

2 Navigate to **Manage** | **Policies** | **Response Rules** | **Add Response Rule**.

3 Select **Automated Response** in the new window, then click **Next**.

4 Configure the rule by completing these fields.

a **Rule Name** – Enter a rule name.

b **Description** – Enter a description for the rule name.

5 In the **Actions** section, click the drop-down list and select **Log to a Syslog Server**.

6 Click **Add Action**.

7 Configure the actions by completing these fields.

a **Host** – Enter the IP address of the remote log collector.

b **Port** – Enter `514`.

c **Message** – Enter the following:

```
CEF:0|Symantec|DLP|12.5.0|ruleID|$POLICY$|5|BLOCKED=$BLOCKED$ INCIDENT_ID=
$INCIDENT_ID$ INCIDENT_SNAPSHOT=$INCIDENT_SNAPSHOT$ MATCH_COUNT=$MATCH_COUNT$
PROTOCOL=$PROTOCOL$ RECIPIENTS=$RECIPIENTS$ SENDER=$SENDER$ SUBJECT=$SUBJECT$
SEVERITY=$SEVERITY$ FILE_NAME=$FILE_NAME$
```

Symantec Data Loss Prevention CEF events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|Symantec|DLP|12.5.0|ruleID|$POLICY$|5|BLOCKED=$BLOCKED$ INCIDENT_ID=$INCIDENT_ID$
INCIDENT_SNAPSHOT=$INCIDENT_SNAPSHOT$ MATCH_COUNT=$MATCH_COUNT$ PROTOCOL=$PROTOCOL$
RECIPIENTS=$RECIPIENTS$ SENDER=$SENDER$ SUBJECT=$SUBJECT$ SEVERITY=$SEVERITY$ FILE_NAME=
$FILE_NAME$
```

Log sample

This is a sample log from a Symantec DLP (Vontu DLP) device:

```
<13>Sep 5 08:22:01 data.example.com CEF:0|Symantec|DLP|12.5.0|ruleID|Policy|5|BLOCKED=Passed
INCIDENT_ID=204529 INCIDENT_SNAPSHOT=https://main.example.com/Path/Address MATCH_COUNT=3
PROTOCOL=SMTP RECIPIENTS=email@example.com SENDER=sender@example.com SUBJECT=Sensitive Data
(attachment included) SEVERITY=1:High FILE_NAME=myfile.xml
```

Mappings

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

Log fields	McAfee ESM fields
POLICY	Policy_Name, Message
BLOCKED	Event Subtype
INCIDENT_ID	Incident_ID
INCIDENT_SNAPSHOT	URL
MATCH_COUNT	Count
PROTOCOL	Application_Protocol
RECIPIENTS	Destination IP, To_Address
SENDER	Source IP, From_Address
SUBJECT	Subject
SEVERITY	Severity
FILE_NAME	Filename

Add Symantec Data Loss Prevention

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Symantec**
Data Source Model	**Symantec Data Loss Prevention (ASP)**
Data Format	**(Default)**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Symantec Data Loss Prevention events to McAfee fields

Log format

The expected format for this device is:

```
<pri>Date Time Application: sessionNumber|[HostName]|Message|Source|E-MailAddress|WebAddress|
```

Log sample

This is a sample log from a Symantec Data Loss Prevention (Vontu) device:

```
<20>Jan 01 01:01:01 admin Incident: 12345|US_GBM_COLLECT_BUSINESS_SOURCECODE|192.168.2.1|
HTTP incident| https://main.website.com/folder/thing.do=12345|http://main.website.com/
aspfile.asp
```

Mappings

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

Log fields	McAfee ESM fields
Application	Application
SessionNumber	Session ID
Source	Source IP
Hostname	Host
Message	Message
E-mailAddress	To
WebAddress	URL

Symantec Endpoint Protection

Contents

Configure Symantec Endpoint Protection

Task

1. Log on to the Symantec Endpoint Protection Manager Console as administrator.
2. Navigate to **Admin** | **Servers** | **Local Site** | **Configure External Logging**, then select any **Update Frequency**.
3. Select **Enable Transmission of Logs to a Syslog Server**.
4. In the **Syslog Server** field, enter the IP address of the McAfee Event Receiver.
5. In the **Destination Port** field, enter the port used for receiving syslog on the McAfee Event Receiver (default is 514).
6. In the **Log Facility** field, enter any facility number according to your preference.
7. On the **Log Filter** tab, select any of the files you want to export.
8. Click **OK** to save and exit.

Add Symantec Endpoint Protection

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Symantec
Data Source Model	Endpoint Protection (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	<Defaults>
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	<Enable>
Mask	<Default>
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	<Default>
Time Zone	Time zone of data being sent

Symantec Endpoint Protection events to McAfee fields

Log format

The expected format for this device is:

```
<date> [<device IP>] <date> SymantecServer <hostname>: <message>
```

Log sample

This is a sample log from a Symantec Endpoint Protection device:

```
Jan 01 01:01:01 [192.0.2.1] Jan 01 01:01:01 SymantecServer servername:,Category: 1,Symantec
AntiVirus,Symantec Endpoint Protection services startup was successful.
```

Mappings

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

Log fields	McAfee ESM fields
Hostname	Host
Client Hostname	Destination_Hostname
Protocol	Protocol
IP	Source IP
Remote IP	Destination IP
Port	Source Port
Remote Port	Destination Port
MAC	Source MAC
Remote MAC	Destination MAC
Session	Session ID

Log fields	McAfee ESM fields
Application name	Application
Command	Command
Domain	Domain
Occurrences	Count
File	Filename
User	Source User
Rule	Rule_Name
Source	Detection_Method
Operating System	Operating_System
Remote File Path	File_Path
Application type	Category
Risk Name	Threat_Name
Application hash	File_Hash
Management Server	Management_Server

Symantec Messaging Gateway

Contents

Configure Symantec Messaging Gateway

Task

1 Log on to the **Symantec Message Gateway Control Center** as administrator.

2 Navigate to **Administration** | **Settings** | **Logs**, then select the **Remote** tab.

3 Select **Enable Syslogs for the following host**, then select the host to send syslog data from.

4 In the **Host** field, enter the IP address of the McAfee Event Receiver.

5 Enter the port where the McAfee Event Receiver is listening (default is **514**).

6 Set the **Protocol** field to **UDP**.

7 Set the **Component Remote Log Levels** to the level you want.

8 Select **Enable Message Logs** so that message logs are sent to the McAfee Event Receiver.

9 Set the **Message log facility** to the level you want.

10 Save changes.

Add Symantec Messaging Gateway

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Symantec**
Data Source Model	**Symantec Message Gateway**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Events Symantec Messaging Gateway events to McAfee fields

Log format

The expected format for this device is:

```
<pri> Date Time Application: [Hostname] (Severity.Reference.Number): [EventIDNumber] <Source
Username> <Destination Username> SrcIP|SrcPort|DstIP|DstPort| Message Filepath/Filename
```

Log sample

This is a sample log from a Symantec Message Gateway device:

```
<23>Jan 1 01:01:01 antispam conduit: [Brightmail] (INFO:1234.12345678): [12345] Spamhunter
module: loaded rulefile /data/rules (file ver 1, type 1; module ver 1): 100000 rules loaded.
```

Mappings

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

Log fields	McAfee ESM fields
Application	Application
Hostname	Hostname

Log fields	McAfee ESM fields
Severity	Severity
EventIDNumber	Signature ID
Filepath/Filename	Filename
Source Username	Source User
Destination Username	Destination User
SrcIP	Source IP
DstIP	Destination IP
Message	Message_Text

Symantec PGP Universal Server

Contents

Configure Symantec PGP Universal Server

Task

1. Log on to the Symantec PGP Universal Server Device with a web browser.
2. Click **Settings**.
3. Select **Enable External Syslog**.
4. Set the **Protocol** to **UDP**.
5. Set the **Hostname** to the IP address of the McAfee Event Receiver.
6. Set the **Port** to **514** (the default port for receiving syslog on the McAfee Event Receiver).
7. Click **Save**.

Add Symantec PGP Universal Server

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Symantec**
Data Source Model	**PGP Universal Server**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Symantec PGP Universal Server events to McAfee fields

Log format

The expected format for this device is:

```
Date Time service[pid]: Message CLIENT USER from
```

Log sample

This is a sample log from a Symantec PGP Universal Server device:

```
2001/01/01 01:23:45 -00:00 NOTICE pgp/admin[2002]: Administrator [UNAUTHENTICATED USER] from
192.0.2.2 Using Passphrase login successfully for Administrator "admin_bt" from 192.0.2.1
```

Mappings

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

Log fields	McAfee ESM fields
Service	Severity/Application
Message	Command
Client	Source IP
User	Source User
From	Destination IP

Symantec Web Gateway

Contents

Configure Symantec Web Gateway

Task

1 Log on to your Symantec Web Gateway device through a web browser.

2 Navigate to **Administration** | **Configuration** | **Syslog**.

3 Set the **Syslog Server** value to the IP address of the McAfee Event Receiver.

4 Set **Facility** according to your preference.

5 Save changes.

Add Symantec Web Gateway

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Symantec**
Data Source Model	**Symantec Web Gateway (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Symantec Web Gateway events to McAfee fields

Log format

The expected format for this device is:

```
<pri>Alert type: [Alert Name] (Description), (Host), (Detection Type), (Threat Name),
(Threat Category), (Severity), (Threat Description)
```

Log sample

This is a sample log from a Symantec Web Gateway device:

```
<185>Symantec Web Gateway Alert: [Alert Name - Name] (Description: Alert events sent to
syslog), (Count: 1), (Host: 192.0.2.1), (Detection Type: 1), (Threat Name: Instant Buzz),
(Threat Category: Adware), (Severity: 1), (Threat Description: Instant Buzz is an adware
application which installed as an Internet Explorer advertising toolbar. It changes a user's
Internet Explorer settings unexpectedly and delivers targeted advertisements to the user.)
```

Mappings

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

Log fields	McAfee ESM fields
Host	Host, Source IP
Threat Name	Message
Threat Type	Application
Severity	Severity

ThreatConnect Threat Intelligence Platform

Contents

Configure ThreatConnect Threat Intelligence Platform

See the ThreatConnect Threat Intelligence Platform product documentation for setup instructions about sending Remote Syslog to an external server. Use the McAfee Event Receiver's IP address as the destination IP address and port 514 as the destination port.

Add ThreatConnect Threat Intelligence Platform

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ThreatConnect**
Data Source Model	**Threat Intelligence Platform**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

ThreatConnect Threat Intelligence Platform events to McAfee fields

Log format

The expected format for this device is:

```
CEF:0|threatconnect|threatconnect|<version>|<event class id>|<name>|<severity>|<key value
pairs>
```

Log sample

This is a sample log from a device:

```
CEF:0|threatconnect|threatconnect|3|14936758|McAfee ESM Demo Source Email|8|
cs5Label=Indicator cs3=This is one bad dude. cs2=McAfee ESM Demo Source
cs5=superduperbadguy@evil.com cs4=https://app.threatconnect.com/auth/indicators/details/
emailaddress.xhtml?
```

Mappings

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

Log fields	McAfee ESM fields
cat	sid
CEF.Severity	Severity
Confidence	Confidence
cat	Category
CEF.SignatureID, spid	External_EventID
Indicator, oldFileHash	Threat_Name
fileHash	New_Value
ThreatConnect URL	Device_URL

Log fields	McAfee ESM fields
cfp1	Reputation_Score
cfp2	Device_Confidence
deviceCustomDate1	firsttime,lasttime

TippingPoint SMS

Contents

Configure TippingPoint SMS

Task

1 From the **Device Configuration** screen, select **Server Properties** | **Management tab**.

2 At the bottom of the page, find **Remote Syslog for Events**:

- For a new configuration, click **New**.
- For an existing configuration, click **Edit**.

3 Enter the IP address for the McAfee Event Receiver.

4 Enter `514` for the port.

5 For **Alert Facility**, select **None**.

6 For **Block Facility**, select **None**.

7 For **Delimiter**, select **Tab**.

8 Click **Apply** to save changes.

Add TippingPoint SMS

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**TippingPoint**
Data Source Model	**SMS (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do Nothing**
Time Zone	Time zone of data being sent.

TippingPoint SMS events to McAfee fields

Log format

The expected format for this device is:

```
<Syslog category> Action Type Severity Policy UUID Signature UUID Signature Name Signature
Number Signature Protocol Source Address Source port Destination Address Destination Port
Hit Count Source Zone Name Destination Zone Name Incoming Physical Port VLAN ID Device Name
Tipping Point Taxonomy ID – Category Id assigned to Signature Event timestamp in Milliseconds
```

Log sample

This is a sample log from a TippingPoint SMS device:

```
<34> 8 4 00000002-0002-0002-0002-000000001026 00000001-0001-0001-0001-000000001026 1026:
HTTP: cgiwrap Vulnerability 1026 http 1.2.3.4 49725 2.3.4.5 80 1 1-1A 1-1B 2 0 TESTHOST
17107965 1406251768046 1117542384
```

Mappings

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

Log fields	McAfee ESM fields
Action Type	Event Subtype
Severity	Severity
Signature UUID	External_EventID
Signature Name	Message
Signature Number	Signature ID
Signature Protocol	Protocol
Source Address	Source IP

Log fields	McAfee ESM fields
Source Port	Source Port
Destination Address	Destination IP
Destination Port	Destination Port
Hit Count	Count
Source Zone Name	Interface
Source Destination Name	Interface_Dest
Device Name	Host
Event timestamp in milliseconds	First Time, Last Time

Tofino Firewall LSM

Contents

Configure Tofino Firewall LSM

Task

1. Ensure that the **Event Logger Module** is installed on the Tofino Firewall LSM.
2. Open the Tofino Configurator tool.
3. Under **Package Explorer**, navigate to the **Event Logger** and select it.

   The right frame refreshes with the configuration settings for the Event Logger.
4. Set the **Syslog Server IP Address** to the IP address of the McAfee Event Receiver.
5. Set the **Destination Port** to the port set up on the McAfee Event Receiver for receiving syslog (default is 514).
6. Set the **Lowest Priority Logged** according to your preference.

Add Tofino Firewall LSM

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Tofino**
Data Source Model	**Tofino Firewall LSM**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Tofino Firewall LSM events to McAfee fields

Log format

The expected format for this device is:

```
Firewall Name and Version: Message
```

Log sample

This is a sample log from a 3.1 Tofino Security – Tofino Firewall LSM Configuration device:

```
Tofino Firewall LSM: MAC_SRC=00:11:22:33:44:55 MAC_DST=55:44:33:22:11:00 IP_SRC=192.168.1.2
IP_DST=192.168.2.1 PROTO=FTP PORT_SRC=21 PORT_DST=11111
```

Mappings

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

Log fields	McAfee ESM fields
PORT_DST	Destination Port
PROTO	Protocol
DST_MAC	Destination Mac
DST_IP	Destination IP
SRC_MAC	Source Mac
SRC_IP	Source IP
SRC_PORT	Source Port

Topia Technology Skoot

Contents

Configure Topia Technology Skoot

See documentation for information about how to send syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add Topia Technology Skoot

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Topia Technology
Data Source Model	Skoot (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Topia Technology Skoot events to McAfee fields

Log format

The expected format for this device is:

```
<severity> <date> User=<username;
workspaceGUID=<GUID>;workspaceName=<name>;action=<action>;fileId=<IDnumber>;fileName=<filenam
e>;status=<action>
```

Log sample

This is a sample log from a Topia Technology Skoot device:

```
INFO 2001-01-01 01:01:01,001 -
User=user@domain.com;workspaceGUID=a1b2c3d4-e5f6-a1b2-c3d4-e5f6a1b2c3d4;workspaceName=Example
Name;action=fileupload;fileId=12;fileName=fileName.png;status=Success
```

Mappings

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

Log fields	McAfee ESM Fields
cat	sid
CEF.Severity	Severity
Confidence	Confidence
cat	Category
CEF.SignatureID, spid	External_EventID
Indicator, oldFileHash	Threat_Name
fileHash	New_Value
ThreatConnect URL	Device_URL
cfp1	Reputation_Score
cfp2	Device_Confidence
deviceCustomDate1	First Time, Last Time

TrapX Security DeceptionGrid

Contents

Configure TrapX Security DeceptionGrid

Task

1 Open up the device management screen and click the **Configuration** tab.

2 Edit the Syslog server property.

3 In the **Configure Syslog Service Settings** window, select **Enable Syslog Service**.

4 In the **Syslog server configuration IP** field, enter the IP address of the McAfee Event Receiver.

5 Click **Apply**.

Add TrapX Security DeceptionGrid

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**TrapX Security**
Data Source Model	**DeceptionGrid**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

TrapX Security DeceptionGrid events to McAfee fields

Log format

The expected format for this device is:

```
<PRI>DATE TIME HOSTNAME DATE: TIME HOSTNAME MESSAGE
```

Log sample

This is a sample log from a device:

```
<123>Jan 01 01:01:01 localhost 20010101-1: 01:01.001 localhost connections['tcp' :
978310861 : '192.0.2.1' : 123 : '192.0.2.1' : 456]: 123
```

Mappings

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

Log fields	McAfee ESM fields
Source IP	Source IP
Destination IP	Destination IP
Source Port	Source Port

Log fields	McAfee ESM fields
Destination Port	Destination Port
Protocol	Protocol
app	Application
class	Threat_Category
Hash	File_Hash

Trend Micro Deep Security

Contents

Configure Trend Micro Deep Security

Follow the documentation for the version of Deep Security you have installed.

Add Trend Micro Deep Security

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Trend Micro**
Data Source Model	**Deep Security**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Hostname	The host name of the device
Syslog Relay	**None**
Mask	**32**
Port	**514**
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Trend Micro Deep Security events to McAfee fields

Log format

The expected format for this device is:

```
date time hostname CEF:0|Device Vendor|Device Product|Device Version|Signature ID|Name|
Severity|Extension|...
```

Log sample

This is a sample log from a Trend Micro Deep Security device:

```
Jan 01 01:01:01 SampleServer CEF:0|Trend Micro|Deep Security Manager|8.0.1046|600|User
Signed In|3|src=1.2.3.4 suser=admin target=admin msg=User signed in from
fe80:0:0:0:2d02:6060:bebe:fd41
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP
suser	Source User
duser	Destination User
msg	Message
dmac	Destination MAC
dpt	Destination Port
dst	Destination IP
proto	Protocol
smac	Source MAC
spt	Source Port
src	Source IP
Time	First Time, Last Time
TrendMicroDsFrameType	Application
shost	Host
request	URL
Host ID	Server_ID

Trend Micro Deep Security Manager

Contents

Configure Trend Micro Deep Security Manager

Follow the documentation for the version of Deep Security Manager you have installed.

Add Trend Micro Deep Security Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Trend Micro**
Data Source Model	**Deep Security Manager**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Host Name	The host name of the device
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	**514**
Support Generic Syslogs	**<Default>**
Time Zone	Time zone of data being sent.

Trend Micro Deep Security Manager events to McAfee fields

Log format

The expected format for this device is:

```
Date time CEF:0|Company|Product|Version|EventID|Title|#|Message
```

Log sample

This is a sample log from a Trend Micro – Deep Security Manager device:

```
<134>Jan 01 00:00:00 AAAA01 CEF:0|Trend Micro|Deep Security Manager|8.0.0000|999|Contact by
Unrecognized Client|6|src=10.0.0.1 suser=System msg=A connection to Deep Security Manager
was initiated by a client not identifiable as a managed computer: 10.0.0.1:5500. Either the
client is not a managed Deep Security component, or a secure communication channel could not
```

```
be established.
```

Trend Micro OfficeScan events to McAfee fields

Log format

The expected format for this device is:

```
<computer name> <domain> <device name> <epoch time> <threat name> <infected file> <file
location>
```

Log sample

This is a sample log from a Trend Micro OfficeScan device:

```
COMPUTERNAME Domain  1 Device.Name 978310800 Threat_Name ~filename.tmp  C:\Users\filelocation
\  0 0 0
```

Mappings

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

Log fields	McAfee ESM fields
Computer Name	Host
Domain	Domain
Device Name	Object
URL	URL
Infected Filename	Destination_Filename
Operating System	Operating_System
Location	File_Path
Threat Name	Threat_Name
GUID	Instance_GUID
Time	First Time, Last Time
IP Address	Source IP
Port	Source Port

Trend Micro OfficeScan

Contents

Configure Trend Micro OfficeScan

See documentation for information about how to send syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add Trend Micro OfficeScan

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Trend Micro**
Data Source Model	**OfficeScan (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Trustwave Data Loss Prevention

Contents

Configure Trustwave Data Loss Prevention

See documentation for information about how to send CEF-formatted syslog events to a syslog server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add Trustwave Data Loss Prevention

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Trustwave
Data Source Model	Data Loss Prevention
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Trustwave Data Loss Prevention events to McAfee fields

Log format

The expected format for this device is:

```
<date time> < host > CEF:<version>|<device vendor>|<device product>|<device version>|
<signature ID>|<name>|<severity>|rt=<receipt time> scr=<source IP> dst=<destination IP>
sport=<source port> dport=<destination port> app=<application> shost=<source host>
dhost=<destination host>  externalId=<external ID>
```

Log sample

This is a sample log from a **Trustwave Data Loss Prevention** device:

```
Jan 1 01:01:01 abcde12345 CEF:0|Trustwave|DLP|8.14|sigid|name|5|rt=978310861000
src="192.0.2.0" dst="5.6.7.8" sport=1234 dport=5678 app="appname" shost="198.51.100.0"
dhost="example.com" externalId="a1b2c3d4-e5f6-a7b8-c9d0-e1f2a3b4c5d6"
```

Mappings

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

Log fields	McAfee ESM fields
dhost	Host
suser	Source User
duser	Destination User
cs6	Domain
app	Application
src	Source IP
dst	Destination IP

Log fields	McAfee ESM fields
sport	Source Port
dport	Destination Port
proto	Protocol
smac	Source MAC
dmac	Destination MAC
cnt	Event Count
shost	Object
fname	File_Path
externalId	Message_Text

Trustwave Network Access Control

Contents

Configure Trustwave Network Access Control

See documentation for information about how to send syslog events to a remote server or McAfee ESM. Use the IP address of the McAfee Event Receiver for the IP address of the remote server.

Add Trustwave Network Access Control

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Trustwave
Data Source Model	Network Access Control (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Trustwave Network Access Control events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <device IP> <state> <date> <device name> <action> <priority> <hostname>
```

Log sample

This is a sample log from a Trustwave Network Access Control device:

```
Jan 01 01:01:01 [1.2.3.4] Jan 01 01:01:01 applianceReady: Date=2001/01/01
01:01:01,ReportingAppliance=device,Action=applianceReady,Priority=critical,SourceAppliance=ho
stname
```

Mappings

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

Log fields	McAfee ESM fields
Source Appliance	Host
Priority	Severity
Managed Device	Source MAC
Domain	Domain
IP Address	Source IP
Action	Message

Type80 Security Software SMA_RT

Contents

Configure Type80 Security Software SMA_RT

See the Type80 Security Software SMA_RT product documentation for setup instructions about sending syslog data to a remote server. Use the IP address of the McAfee Event Receiver as the destination IP address and port 514 as the destination port.

Add Type80 Security Software SMA_RT

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Type80 Security Software**
Data Source Model	**SMA_RT (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Type80 Security Software SMA_RT events to McAfee fields

Log format

The expected format for this device is:

```
<date time> <IP address> <device name> <date time> <severity> <object> <user> <group> <name>
<terminal name>
```

Log sample

This is a sample log from a Type80 Security Software SMA_RT device:

```
Jan 01 01:01:01 192.0.2.0 DEVICE |||2001010101010101|||||YELLOW ALERT |ABC12345
USER(username) GROUP(groupname) NAME(name) terminalname
```

Mappings

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

Log fields	McAfee ESM fields
Terminal name	Hostname
Object	Object
IP Address	Source IP
Terminal Address	Destination IP
User	Username
Name	Source Username
Group	Group_Name

Unix Linux

Contents

Configure Unix Linux

Task

1 Edit the /etc/syslog.conf file.

2 Add this line to the file:

```
*.*; @<ip_address>:514
```

where <ip_address> is the IP address of your McAfee Event Receiver, and 514 is the default port for syslog/.

3 Run this command:

```
service syslog restart
```

Add Unix Linux

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Unix**
Data Source Model	**Linux**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Verdasys Digital Guardian

Contents

Configure Verdasys Digital Guardian

Task

1 Log on to the Digital Guardian Management Console.

2 Select **Workspace** | **Data Export** | **Create Export**.

   a From the **Data Sources** list box, select **Alerts** or **Events** as the data source.

   b From the **Export type list** box, select **ArcSight CEF**.

   c From the **Type** list box, select **UDP** or **TCP** as the transport protocol.

   d In the **Server Name** field, type the IP address of your ArcSight server.

   e In the **Port** field, type `514`.

   f From the **Syslog Severity Level** list box, select a severity level.

   g Select **Is Active**.

3 Click **Next**.

4 From the list of available fields, select the **Alert** or **Event** fields for your data export.

5 Select a criteria for the fields in your data export, then click **Next**.

6 Select a group for the criteria, then click **Next**.

7 Click **Test Query**, then click **Next**.

8 Save the data export.

Add Verdasys Digital Guardian

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Verdasys**
Data Source Model	**Digital Guardian**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**<Defaults>**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time Zone – Time zone of data being sent.

Verdasys Digital Guardian events to McAfee fields

Log sample

```
Jan 01 2014 01:01:01 APPSERVER.domain.com CEF:0|Verdasys|Digital Guardian|6.1.2.0464|File
Write|File Write|10|cat=alerts msg=File DG_AgentUTCDate=10/13/2013 sproc=updates.exe
deviceProcessName=updates.exe dvchost=workgroup/username-PC shost=workgroup/username-PC dst=
cs1=[APT-TEST01] - Processes Creating Binaries cs1Label=Rule cs2=False cs2Label=WasBlocked
suser=username-PC\\hostname fname=836d52c28e6cc389f3eaa0d46bbcecff.txt
DG_SourceDriveType=CDROM
```

Mappings

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

Log fields	McAfee ESM fields
DG_SourceDriveType	Object_Type
fname	Filename

Log fields	McAfee ESM fields
Custom field: Rule	Rule_Name
Custom field: WasBlocked	Process_Name

VMware

Contents

Configure VMware

See the specific product documentation of VMware for instructions about sending syslog events.

Add VMware

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**VMware**
Data Source Model	**VMware (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

VMware events to McAfee fields

Log sample

This is a sample log from a VMware device:

```
<166>Jan 1 12:34:56 Hostd: [2015-01-01 12:34:56.123 ABCD1234 severity service] Example
Message
```

Mappings

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

Log fields	McAfee ESM fields
User	Source User
IP Address	Source IP
Virtual Machine Name	Object
Destination	Destination IP
Host	Hostname
Application	Application
Command	Command
Changed Filename	Destination Filename
Method	Method
Severity	Severity
File	Filename

VMware AirWatch

Contents

Configure VMware AirWatch

Task

1 Log on to Admin Console and navigate to **Groups** | **Settings** | **All Settings** | **System** | **Enterprise Integration** | **Syslog**.

2 Enter the host name or IP address of the McAfee Event Receiver in the **Host Name** field.

3 Select **UDP** for **Protocol**.

4 Enter `514` in the **Port** field.

5 Select **UserLevelMessages** for **Syslog Facility**.

6 For **Event Types Logged**, select **Console** and **Device**.

7 Enter **Airwatch** in the **Message Tag** field.

8 Make sure that the **Message Content** field follows the default format.

Add VMware AirWatch

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**VMware**
Data Source Model	**AirWatch**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

VMware AirWatch events to McAfee fields

Log format

The expected format for this device is:

```
AirWatch Syslog Details are as follows Event Type: {EventType}Event: {Event}User:
{User}Event Source: {EventSource}Event Module: {EventModule}Event Category:
{EventCategory}Event Data: {EventData}
```

Log sample

This is a sample log from a device:

```
<101> October 11 11:12:22 AirWatch AirWatch Syslog Details are as follows Event Type:
DeviceEvent: SecurityInformationUser: sysadminEvent Source: Event Module: DevicesEvent
Category: DeliveryEvent Data: 747
```

Mappings

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

Log fields	McAfee ESM fields
EventType	Event_Class
Event	Message
User	Source User
EventSource	Subcategory
EventModule	Category
EventCategory	Message_Text
Application	Filename
Method	Method
Destination User	Destination User
OS Version	Version
OS	Operating_System
Status	Status
Device Type	External_Device_Type
Session	External_SessionID
Event Source	Object_Type

VMware vCenter Server

Contents

Configure VMware vCenter Server

Task

1 Log on to the vSphere web client.

2 Browse to the vCenter Server where you want to collect events.

3 Select **Manage** | **Permissions** | **Add Permission**.

4 Add minimum read-only permission to a user, then select **Propagate to children**.

Use an existing permission if one was created.

Add VMware vCenter Server

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**VMware**
Data Source Model	**vCenter Server (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	
Name	User-defined name of data source
IP Address/Hostname	The IP address associated with vCenter Server.
Username	User name associated with the read-only permission
Password	Password associated with the user name
Port	Default is 443
Use SSL	Selected by default

VMware vCenter Server events to McAfee fields

Log format

The expected format for this device is:

```
computer date time IP protocol source destination original client IP source network
destination network action status rule application protocol bytes sent bytes sent
intermediate bytes received bytes received intermediate connection time connection time
intermediate username agent session ID connection ID
```

Log sample

This is a sample log from a VMware vCenter Server device:

```
SC-CHPROXY 2012-01-25 00:00:02 TCP 192.168.1.2:45678 10.10.10.78:443 192.168.1.5 Local Host
Internal Establish 0x0 - HTTPS 0 0 0 0 - - - - 255594 1555999
```

Mappings

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

Log fields	McAfee ESM fields
Computer	Hostname
IP Protocol	Protocol
Source	Source IP
Destination	Destination IP

Vormetric Data Security Manager

Contents

Configure Vormetric Data Security Manager

Task

1 From the DSM product, select **Log** | **Syslog** and add the required information.

2 Select **Syslog Enabled** via **System** | **General Preferences** on the **System** tab.

3 Configure the Syslog server for DSM logging for each domain.

Add Vormetric Data Security Manager

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Vormetric**
Data Source Model	**Data Security (ASP)**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Defaults**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

Vormetric Data Security Manager events to McAfee fields

Log format

The expected format for this device is not available.

Log sample

These are sample logs from a Vormetric Data Security device:

```
<30>1 2013-06-29T18:44:42.420Z 10.10.10.1 vee-FS 0 CGP2601I [CGP@21513 sev="INFO" msg="Audit
access" cat="[AUDIT]" pol="aria256_on_host" uinfo="cfd,uid=100,gid=10{staff}" sproc="/opt/
```

```
VRTSfssdk/5.0/src/vxfsio/cache/obj64/cache_advisory" act="write_app" gp="/vor/guard"
filePath="/symtest" key="aria256_on_host" denyStr="PERMIT" showStr="Code (1M)"]

<14> Jan 06 05:31:03 cpu.mydom.com CEF:0|Vormetric, Inc.|dsm|5.2.0.1|DAO0048I|update host|3|
cs4Label=logger cs4=DAO spid=4322 rt=1388986263954 dvchost=cpu.mydom.com suser=USER_1
shost=test_cpu
```

Mappings

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

Log fields	McAfee ESM fields
filePath	Destination_Filename
cat	Category
url	URL
Message ID	Signature ID
sev	Severity
msg, Action	Message
user, suser, admin, uinfo	Source User
shost	Host, Source IP
dvchost	Destination_Hostname
sproc, Process	Application
act	Event Subtype, Command
denyStr	Event Subtype
spt	Source Port
count	Event Count
cs1_policy, policy, pol	Policy_Name, Command
“faked as USERNAME” from suser	User_Nickname
showStr, reason	Reason
rt	First Time, Last Time
key	Registry_Key
Res	Object

WatchGuard Technologies Firebox

Contents

Configure WatchGuard Technologies Firebox

Task

1 From the **Fireware** web interface, go to **System** | **Logging**.

2 Click the **Syslog Server** tab.

3 Select **Enable Syslog output to this server** and enter the IP address of the McAfee Event Receiver in the adjacent textbox.

4 In the **Settings** section, use the drop-down lists to select the syslog facility for each type of log message.

5 Click **Save**.

Add WatchGuard Technologies Firebox

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**WatchGuard Technologies**
Data Source Model	**Firebox and X Series (ASP)**
Data Format	**Default**
Data Retrieval	**SYSLOG (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent

WatchGuard Technologies Firebox events to McAfee fields

Log format

The expected format for this device is:

```
<priority> <time> <date> <hostname> (<time> <date>) <process>[<process id>]: <key>=<value>
<key>=<value> <key>=<value>…
```

Log sample

This is a sample log from a WatchGuard Technologies Firebox device:

```
<123>Jan 01 01:01:01 HOSTNAME (2001-01-01T01:01:01) http-proxy[1234]: msg_id="1A2B-3C4D"
Allow 1-Trusted 6-External tcp 192.0.2.1 192.0.2.2 12345 67890 msg="ProxyAllow: HTTP Request
URL match" proxy_act="Outgoing HTTP Proxy" rule_name="Default"
dstname="download.example.com" arg="arguments" (HTTP-proxy-Out)
```

Mappings

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

Log fields	McAfee ESM fields
Host, server	Host
protocol	Protocol
source IP	Source IP
destination IP	Destination IP
source port	Source Port
destination port	Destination Port
mac	Source MAC
destination mac	Destination MAC
message	Message
msg_id	Message_ID
action	Event Subtype
socket ID, process ID, pid,	Session ID
VLAN ID	VLAN
Severity	Severity
date, time	First Time, Last Time
application	Application
domain	Domain
filename	Filename
detail name	Object
Authentication Method	Method
src_user	Source User
interface	Interface
external interface	Interface_Destination
domain name, GET	URL
Group	Group_Name
member	External_Device_Name
member	External_Device_ID
diagnostic file location	External_Device_Type
session number	External_Session_ID
Cluster ID	External_Event_ID
Proxy Action	Device_Action

Log fields	McAfee ESM fields
Ruleset	Rule_Name
Task UUID	UUID
path	File_Path
Policy Name	Policy_Name
Service	Service_Name

Websense Enterprise SQL Pull

Contents

Configure Websense Enterprise SQL Pull

Task

1 Make sure that you have the credentials for a user with the necessary permissions to the database.

2 Make sure that you have your database's open port and IP address to set up the McAfee Event Receiver.

Add Websense Enterprise SQL Pull

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Websense**
Data Source Model	**Websense Enterprise – SQL Pull**
Data Format	**Default**
Data Retrieval	**SQL (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Instance Name	Enter the database Instance Name.
User ID/Password	User ID and password to log on to the database.
Port	**1433**
Database Name	Name of database.
Time Zone	Time zone of data being sent.

Websense Enterprise SQL Pull events to McAfee fields

Log format

The log format is specific to this data source.

Log sample

This is a sample log from a Websense Enterprise - SQL Pull device:

```
record_number="100000034293" first_time="1323776050" last_time="1323776050"
ip_src="10.0.2.231" ip_dst="10.0.66.80" dport="80" protocol="HTTP" command="Miscellaneous:"
domain="10.0.66.80" username_src="10.0.2.231" username_dst="Samuel" sig_desc="Custom URL,
category permitted" Url.Url="10.0.66.80" source_server_ip_int="10.0.2.231"
disposition_code="1028" bytes_sent="601" bytes_received="749" action="Permitted"
```

Mappings

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

Log fields	McAfee ESM fields
action	Action
protocol	Protocol
ip_src	Source IP
ip_dst	Dest. IP
	First Time | Last Time
dport	Dest. Port
username_src	Source User
username_dst	Destination User
Url.Url	URL
domain	Domain

Log fields	McAfee ESM fields
sig_desc	Rule Message
disposition_code	Signature ID
bytes_sent	Bytes_Sent
bytes_received	Bytes_Received
Command	Category

WurldTech OpShield

Contents

Configure WurldTech OpShield

Task

1. In top right corner of the interface, hover over **username**.
2. When the menu appears, select **Configuration**.
3. Go to Syslog Settings and Syslog servers.
4. Select **Enable**.
5. From the **Protocol** menu, select **UDP** or **TCP**.
6. Enter the IP address of the McAfee Event Receiver in the **IP Address** field.
7. Set Port to **514** or another port as needed.
8. Select the logging level you want.
9. Click **Save**.

Add WurldTech OpShield

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1. Select a McAfee Event Receiver.
2. Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Wurldtech**
Data Source Model	**OpShield**
Data Format	**Default**
Data Retrieval	**Syslog (Default)**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Enter the desired name for the data source.
IP Address/Hostname	Enter the IP address and host name (optional) associated with OpShield.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Unchecked
Support Generic Syslogs	**Do nothing**
Time Zone	Select the time zone offset applicable to the data being sent.

WurldTech OpShield events to McAfee fields

Mappings

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

Log fields	McAfee ESM fields
Channel	Category
Incident Type	Subcategory
NGFW Device Name	Device Name
Source IP	Source IP
Destination IP	Destination IP
protocol	Protocol, Application
Source Port	Source Port
Destination Port	Destination Port
signatureName	Policy Name
class	Event_Class
methodName	Method
privilege	Access_Privileges
errorMessage	Message_Text
incidentAction	Device_Action, Action
deviceSN	External_Device_ID

Xirrus Wi-Fi Arrays

Contents

Configure Xirrus Wi-Fi Arrays

The syslog configuration is done at the command line. See your product documentation for more information about how to access and use the command line.

Task

1 At the command line, turn on syslog:

```
syslog enable
```

2 Send syslog to the McAfee Event Receiver:

```
syslog primary x.x.x.x level 7
```

Where x.x.x.x is the IP address of the McAfee Event Receiver, and 7 is the severity level of the logs that are to be sent.

3 (Optional) If a primary server has already been defined, syslog can be sent to a secondary server:

```
syslog secondary x.x.x.x level 7
```

Where x.x.x.x is the IP address of the McAfee Event Receiver, and 7 is the severity level of the logs that are sent.

Add Xirrus Wi-Fi Arrays

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	Xirrus
Data Source Model	802.11abgn Wi-Fi Arrays (ASP)
Data Format	Default
Data Retrieval	SYSLOG (Default)
Enabled: Parsing/Logging/SNMP Trap	Parsing
Name	Name of data source
IP Address/Hostname	IP address and host name associated with the data source device
Syslog Relay	None
Mask	32
Require Syslog TLS	Enable to require the Receiver to communicate over TLS
Support Generic Syslogs	Do nothing
Time Zone	Time zone of data being sent

Xirrus 802.11abgn Wi-Fi Arrays events to McAfee fields

Log format

The expected format for this device is:

```
<device IP> <severity> <data> <time> <station MAC> <message>
```

Log sample

This is a sample log from a Xirrus 802.11abgn Wi-Fi Array:

```
[1.2.3.4] <15>Jan 01 01:01:01: info    : Station a1:b2:c3:d4:e5:f6, EAP Response packet
(type PEAP) received
```

Mappings

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

Log fields	McAfee ESM fields
Client Name	Host
SSID	Domain
VLAN ID / packet type / Manufacture	Object
Username	Source User
Station MAC	Source MAC
Source IP Address	Source IP
Source Port	Source Port
Destination IP Address	Destination IP

ZeroFox Riskive

Contents

Configure ZeroFox Riskive

See Riskive Documentation to enable syslog messages.

Add ZeroFox Riskive

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**ZeroFox**
Data Source Model	**Riskive**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**<Defaults>**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**<Default>**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**<Default>**
Time Zone	Time zone of data being sent.

ZeroFox Riskive events to McAfee fields

Log sample

This is a sample log from a Riskive device:

```
<133> Sep 20 16:02:19 2013 ZF1.0 192.168.0.3 5232117c1004db252d6479db:
AlertPriority="MEDIUM" AlertType="CONTENT_ALERT" AlertName="ZeroFoxContent" URL="http://
example.com/" IP="1.2.3.4" Score="0.0" Percentile="0"
Headers="Cache-Control:no-store,no-cache,must-revalidate,post-check=0,pre-check=0,Connection:
 Keep-Alive,Content-Type:text/html;charset=UTF-8,Date:Thu,12Sep201318:06:36GMT,Expires:Thu,
19Nov198108:52:00GMT,Keep-Alive:timeout=3,max=100,Pragma:no-cache,Server:Apache/
2.2.15(CentOS),Set-Cookie:app=2zf6bb1itfj47jbvb4tra3jdt7;expires=Thu,
26-Sep-201318:06:36GMT;path=/,X-Powered-By:PHP/5.3.3" DNS="name:example.com.,type:A,ttl:
```

```
300,address:1.2.3.4,target:;name:example.com.,type:NS,ttl:21600,address:,target:
03.dnsv.jp.;name:example.com.,type:NS,ttl:21600,address:,target:
04.dnsv.jp.;name:example.com.,type:NS,ttl:21600,address:,target:
01.dnsv.jp.;name:example.com.,type:NS,ttl:21600,address:,target:02.dnsv.jp." ASNumber="9371"
AsBlock="1.2.0.0/16"
```

Mappings

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

Log fields	McAfee ESM fields
URL	URL.URL
URL	Web_Domain.Web_Domain
DNS	DNS_Name.DNS_Name
Percentile	Severity
AlertPriority	Severity
IP	src_ip
Headers	Firsttime / Lasttime

ZScaler Nanolog

Contents

Configure ZScaler Nanolog

Use the Zscaler NSS admin portal for the configuration.

Task

1 Navigate to **Policy** | **Administration** | **Configure Nanolog Streaming Service**.

2 Click **Add Feed**, and type a name for the feed.

3 From the **NSS Name** list, select the Zscaler NSS system.

4 From the **Status** list, select **Enabled**.

5 Enter the IP address of the McAfee Event Receiver in the **SIEM IP** field.

6 Enter **514** in the **TCP Port** field.

7 Use the default CSV format for the **Feed Output Type** and **Feed Output Format**.

8 Click **Done** to save changes.

Add ZScaler Nanolog

After successfully logging on to the ESM console, you must add the data source to a McAfee Event Receiver in the ESM hierarchy.

Task

1 Select a McAfee Event Receiver.

2 Click the **Properties** icon.

3 From the **Receiver Properties** listing, select **Data Sources**.

4 Click **Add**.

Option	Definition
Data Source Vendor	**Zscaler**
Data Source Model	**Nanolog Streaming Service**
Data Format	**Default**
Data Retrieval	**Default**
Enabled: Parsing/Logging/SNMP Trap	**Parsing**
Name	Name of data source
IP Address/Hostname	The IP address and host name associated with the data source device.
Syslog Relay	**None**
Mask	**32**
Require Syslog TLS	Enable to require the Receiver to communicate over TLS.
Support Generic Syslogs	**Do nothing**
Time Zone	Time zone of data being sent.

ZScaler Nanolog events to McAfee fields

Log format

The expected format for this device is:

```
"%s{time}","%s{login}","%s{proto}","%s{url}","%s{action}","%s{appname}","%s{appclass}","%d{re
qsize}","%d{respsize}","%d{stime}","%d{ctime}","%s{urlclass}","%s{urlsupercat}","%s{urlcat}",
"%s{malwarecat}","%s{threatname}","%d{riskscore}","%s{dlpeng}","%s{dlpdict}","%s{location}","
%s{dept}","%s{cip}","%s{sip}","%s{reqmethod}","%s{respcode}","%s{ua}","%s{referer}"
```

Log sample

This is a sample log from a Zscaler Nanolog Streaming Service device:

```
"Mon Jan 01 01:01:01 2001","example","HTTP","1.2.3.4/","Allowed","General Browsing","General
Browsing","123","321","78","78","General Surfing","Miscellaneous","Miscellaneous or
Unknown","Clean Transaction","None","0","None","None","Example","Default
Department","4.3.2.1","1.2.3.4","head","403 - Forbidden","example ua","None"
```

Mappings

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

Log fields	McAfee ESM fields
time	First Time, Last Time
login	Source User
url	URL
reqsize	Bytes_from_Client
respsize	Bytes_from_Server
urlclass – urlsupercat – urlcat	URL_Category
malwarecat	Threat_Category
threatname	Threat_Name
riskscore	Reputation_Score
cip	Source IP
sip	Destination IP
reqmethod	Command
ua	User_Agent

A Generic syslog configuration details

Different options are available when configuring a new data source. When some options are selected, additional parameters might appear.

This section outlines the general options available in the **Add Data Source** configuration screen and provides details.

Table A-1 Option definitions

Option	Definition
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 needed to retrieve Windows Event Logs if WMI is the chosen mechanism.
Data Source Vendor	List of all supported vendors.
Data Source Model	List of supported products for a vendor.
Data Format	The expected format of the received / collected data. Options are **Default**, **CEF**, and **MEF**. Generally, this option is left as Default for supported data sources; it is intended to be used for custom data sources.  If **CEF** is selected, the generic CEF parsing rule is enabled and rolled into policy for that data source. If selected on supported CEF data sources, the generic parsing rule might override existing parsing rules that are designed to parse data source-specific details. This results in degraded reporting for the specific data source.
Data Retrieval	The expected collection method used by the McAfee Event Receiver to collect the data. The default is generally syslog. Typically, this option is changed to match the needs in a specific user's environment. The data needs to remain in the expected format, otherwise the parsing rules cannot parse the events.
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 McAfee 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 McAfee ESM, but effectively disables the data source. The default is **Parsing**.
Name	This is the name that appears in the Logical Device Groupings tree and the filter lists.
IP Address/ Hostname	The IP address and host name associated with the data source device.
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.
Mask	Allows a mask to be applied to an IP address so that a range of IP addresses can be accepted.
Require Syslog TLS	When enabled, requires the McAfee Event Receiver to communicate over TLS.

Table A-1 Option definitions *(continued)*

Option	Definition
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 McAfee ESM handles unparsed logs. **Parse generic syslog** creates an event for every unique unparsed event collected. **Log unknown** creates a single generic event and increment the count for every unparsed event. **Do nothing** ignores unparsed events. Use **Parse generic syslog** sparingly as it can negatively impact McAfee Event Receiver and McAfee ESM performance when there is a high incoming rate of unparsed logs. If unparsed events must be reported in McAfee ESM, use the **Log unknown** option; otherwise, leave the setting as **Do nothing**.
Time Zone	Set based on the time zone used in the log data. Generally, it is the time zone where the actual data source is located.
Interface	Opens the McAfee Event Receiver interface settings to associate ports with streams of information.
Advanced	Opens advanced settings for the data source.

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 McAfee Event 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 might need to be adjusted.

When creating custom ASP rules, the **Key** and **Value** table located in the **Parsing** tab displays 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 in the **Field Assignment** tab by dragging and dropping the key onto the wanted field.

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