Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Sourcefire Defense Center eStreamer

Configuration Guide

August 15, 2017

Configuration Guide

SmartConnector for Sourcefire Defense Center eStreamer

August 15, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
08/15/2017	Replaced "arcsight connectorsetup" command with "runagentsetup".
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2016	Added support for eStreamer version 5.4.0.
05/16/2016	Added reference to CEF certified version of this product for latest version support.
06/30/2015	Corrected misplaced mappings (BugtraqId and CVEId).
03/31/2015	Added support for eStreamer 5.3.1.
02/16/2015	Added Record Type additional data mapping and updated mapping for Device Receipt Time for RNA and Intrusion mappings; updated Source Host Type and Destination Host Type additional data mappings for RNA only mappings.
08/15/2014	Added support for malware and file events; enhanced policy violation event Name mapping.
06/30/2014	Added support for version 5.3.
02/14/2014	Removed "3.1 or lower" option from the "Request intrusion events" options. Stated that passwords are required when using PKCS12 certificates.

Contents

SmartConnector for Sourcefire Defense Center eStreamer

This guide provides information for installing the SmartConnector for Sourcefire Defense Center eStreamer (formerly Sourcefire Management Console) and configuring the device for event collection. Collection of Intrusion, RNA, and Policy Violation events from the following Sourcefire eStreamer versions is supported: 4.9, 4.9.1, 4.10, 4.10.1, 5.0.2, 5.1.0, 5.1.1, 5.2, 5.3, 5.3.1, and 5.4.0. Malware and file event collection is supported in versions 5.1.1 through 5.4.0.

For support of latest versions of this product, use the SmartConnector for ArcSight CEF Cisco FireSIGHT Syslog. For CEF mappings, see the configuration guide for the CEF Certified connector available from the vendor. (https://www.protect724.hpe.com/docs/DOC-13799).

Product Overview

Sourcefire Defense Center eStreamer is a management platform for intrusion detection deployments, especially for large distributed enterprise networks. Sourcefire Defense Center incorporates policy management, data aggregation, correlation, and reporting into a single centralized solution to make the most of a distributed sensor infrastructure.

Configuration

This section provides instructions for configuring the Defense Center eStreamer to send events to the ArcSight SmartConnector. The basic steps include:

- Adding an eStreamer client and creating an authentication certificate
- Selecting event types to be sent to the SmartConnector

For complete information, see "Configuring eStreamer" in the *Sourcefire System eStreamer Integration Guide*.

Create a Client and Authentication Credentials

eStreamer Version 5

Before eStreamer can send events to the connector, you must add the connector to the eStreamer server's peers database. You also must copy the authentication certificate generated by the eStreamer server to the client.

To add an eStreamer client:

1. Log in as a user with Admin access and select **Local -> Registration -> eStreamer** tab.
2. Click **Create Client**. The Create Client window is displayed.
3. In the **Hostname** field, enter the IP address of the host running the SmartConnector.

If you use a host name, the host input server must be able to resolve the host to an IP address.

4 Type a password in the **Password** field. Java Development Kit (JDK) 6 requires a password for PKCS 12 certificates.

5 Click **Save**. The eStreamer server lets the client computer access port 8302 on the Defense Center and creates an authentication certificate to use during client-server authentication.

6 Click the download icon next to the certificate (pkcs12) file and save the certificate file to the directory used by your client computer for SSL authentication.

Unless you are installing the connector in FIPS-enabled mode, you will need the path and name of the pkcs12 file and the password for the eStreamer client you created in this section for the parameter entry fields 'SSL Keystore file path and name' and 'SSL Keystore password' during SmartConnector installation.

7 Use `KeyMan` or other third party software to open the `<ip>.pkcs12` file and highlight and open each certificate (there are two certificates). For the key, also set the flag "trust as an addressbook certificate." Save the file to the same file name.

8 Download and save the **pkcs12** file to `user/agent/sourcefire/<ip>.pkcs12`; you will refer to that location during the connector installation process.

The client now can connect to the Defense Center. You do not need to restart the Defense Center or eStreamer service.

eStreamer Version 4

To add an Event Streamer client:

1 Select **Operations -> Configuration -> eStreamer**.

2 Navigate to **eStreamer/Clients**.

3 Click **Create Client**. The **Create Client** page displays, asking for Hostname and Password (optional).

4 In the **Hostname** field, enter the IP address or hostname of the client (connector) device.

5 Enter a password in the **Password** field.

6 Click **Save**. The Defense Center now allows host access to port 8302 on the eStreamer client and creates an authentication certificate to use during client-server authentication. The eStreamer Client page is re-displayed. The location of the certificate is displayed in the eStreamer Clients table after successful client creation.

Unless you are installing the connector in FIPS-enabled mode, you will need the path and name of the pkcs12 file and the password for the eStreamer client you created in this section for the parameter entry fields 'SSL Keystore file path and name' and 'SSL Keystore password' during SmartConnector installation.

7 Use `KeyMan` or other third party software to open the `<ip>.pkcs12` file and highlight and open each certificate (there are two certificates). For the key, also set the flag "trust as an addressbook certificate." Save the file to the same file name.

8 Download and save the **pkcs12** file to a temporary location; you will copy this file to a SmartConnector subfolder during the connector installation process.

The client now can connect to the Defense Center. You do not need to restart the eStreamer service.

Configure Event Types to be Sent

eStreamer Version 5

To configure the types of events the eStreamer server can transmit:

1 Log in as a user with Admin access and select **System -> Local -> Registration**.

2 Click the **eStreamer** tab. The eStreamer Event Configuration menu is displayed.

3 Select the check boxes next to the types of events you want eStreamer to forward to the connector. Possible selections include Discovery Events, Correlation and White List Events, Impact Flag Alerts, Intrusion Events, Intrusion Event Packet Data, User Activity, and Intrusion Event Extra Data.

4 Click **Save**.

Your settings are saved and the events you selected are forwarded to eStreamer clients when requested.

eStreamer Version 4

To configure the types of events transmitted by eStreamer through Defense Center:

1 Select **Operations > Configuration > eStreamer**.

2 Navigate to **eStreamer/Clients**.

3 In the **Select Event** column under **eStreamer Event Configuration**, select the check boxes that represent the types of events you want eStreamer to forward to requesting clients. You can select any or all of the following:

Version 4
RNA Events
Compliance Events
Impact Flag Alerts
Intrusion Events
Intrusion Packet Data
RUA Events

4 Click **Save**. Your settings are saved and the events you selected are forwarded to eStreamer clients when requested.

Install the SmartConnector

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

Prepare to Install Connector

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

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

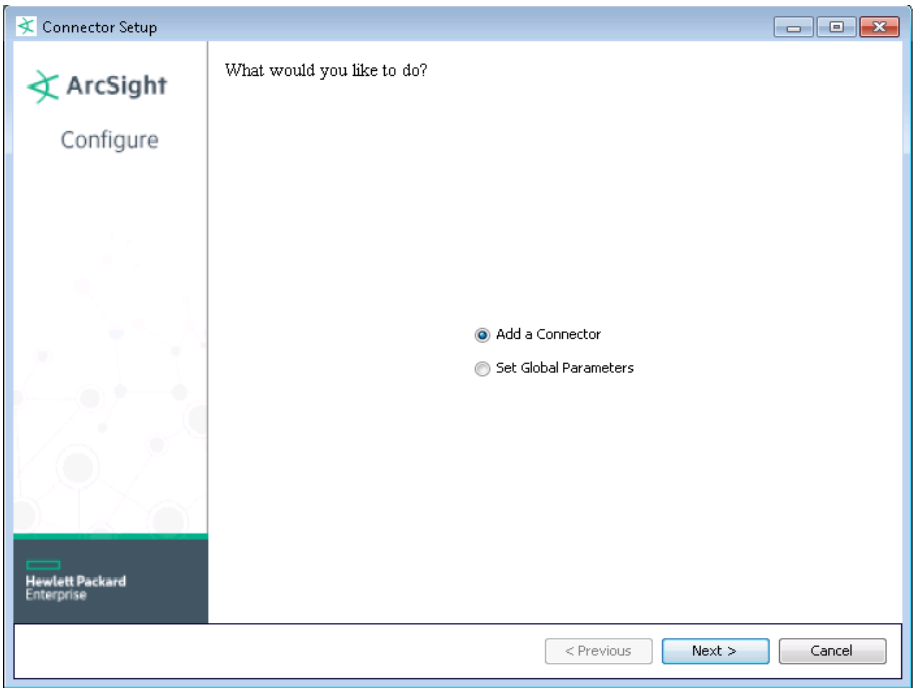
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Next, you will need to download and save the certificate and authentication files for this SmartConnector.

A Click **Cancel** to exit the wizard at this point. Next, create a `sourcefire` folder at the following location:

```
$ARCSIGHT_HOME/current/user/agent/
```

B Locate the `<ip>.pkcs12` authentication file you created earlier and saved in a temporary location. Copy this file (`<ip>.pkcs12`) to the `sourcefire` directory also.

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

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

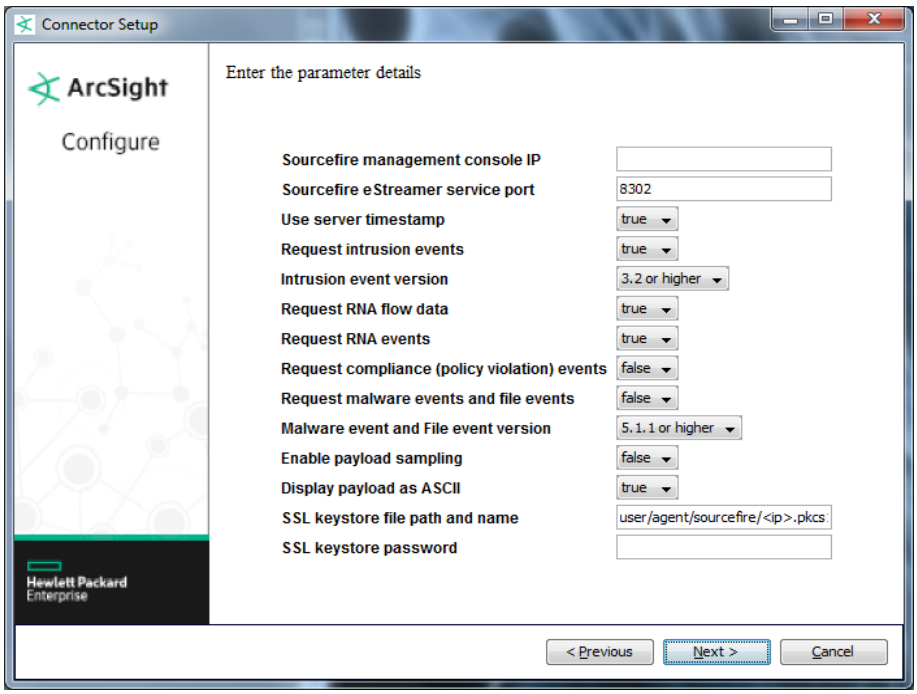
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.

Global Parameter	Setting
Preferred IP Version	If both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is IPv4.

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

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Sourcefire Defense Center eStreamer** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Sourcefire management console IP	Enter the IP address of the Sourcefire Management Console.
Sourcefire eStreamer service port	Enter the port number of the eStreamer service. The default value is '8302'.
Use server timestamp	The default selection for this parameter is 'true'. This feature is available for eStreamer version 4.8 and later versions.
Request intrusion events	Select 'true' to request intrusion events. The default value is true.

Parameter	Description
Intrusion event version	Specify which version of intrusion events to collect. For Sourcefire versions 4.x, use the "3.2 or higher" option. For Sourcefire version 5.x, use the "5.0" or "5.1.1" option for the best results. Contact Sourcefire for version compatibility information for the "3.2 or higher" option, referencing that bit 6 is set in the request flag.
Request RNA flow data	Select 'true' to request RNA flow events. The default value is true. (In Sourcefire version 5.x, these are known as "connection events.")
Request RNA events	Select 'true' to collect RNA events. The default value is true. (In Sourcefire version 5.x, "RNA" was renamed "Discovery.")
Request compliance (policy violation) events	Select 'true' to request policy violation data. The default value is 'false.' (In Sourcefire version 5.x, these are known as "correlation event".)
Request malware events and file events	Select 'true' to request malware and file events data. The default value is 'false.'
Malware event and file event version	Accept the default version (5.1.1 or higher).
Enable payload sampling	Select 'true' or 'false.' When set to 'true,' the first 1022 bytes of the payload associated with intrusion events are retrieved and sent in the deviceCustomString1 fields of the event. The default value is 'false'.
Display payload as ASCII	Select 'true' to display payload as ASCII; select 'false' for payload to be displayed in hexadecimal. The default value is 'true'.
SSL Keystore file path and name	This parameter is not seen when you are installing the connector in FIPS-enabled mode. Set the file path of the pkcs12 file generated earlier in this guide relative to the connector installation directory. The default value is user/agent/sourcefire/<ip>.pkcs12.
SSL Keystore password	The password for the above authentication credentials. This parameter is not seen when you are installing the connector in FIPS-enabled mode.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

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

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

eStreamer Intrusion and RNA Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Additional data	RecordType
Device Event Category	One of (EventCategory, ClassificationName, ClassificationId)
Device Event Class ID	GeneratorId or GeneratorId plus RuleId
Device External ID	One of (SensorId, DetectionEngineId, EventDetectionEngineId)
Device Product	'Sourcefire Management Console eStreamer'
Device Receipt Time	One of (EventSecond, ServerTimestamp)
Device Severity	One of (EventPriority, Priority, PriorityName, PriorityId, Priorityid, 'Low')
Device Vendor	'Sourcefire'

eStreamer Intrusion or RNA Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Additional data	IcmpCode = EventDestinationPort if transport EventProtocol is: ICMP,1
Additional data	IcmpType = EventSourcePort if EventProtocol is: ICMP,1
Destination Address	One of (EventDestinationIp, ResponderIp, DestinationIpAddress, Ip, Ip1, IpAddress)
Destination Port	One of (EventDestinationPort, ResponderPort, Port, Port1, TCPServicePort, UDPServicePort, TCP1ServicePort, UDP1ServicePort)
Device Custom IPv6 Address 2	EventSourceIpV6 (Source IPv6 Address)
Device Custom IPv6 Address 3	One of (EventDestinationIpV6, IpAddressV6) (Destination IPv6 Address)
Device Event Class ID	All of ('PV:', RuleId, ':', PolicyId) if RecordType = 8,36,65,97; All of("RNA:",EventType,":",EventSubtype)if RecordType = 54,109,110,123; All of (GeneratorId, RuleId) or All of ('RNA:', EventType, EventSubtype) if RecordType = 1,7,207,208,400;All of("PV:",RecordType,":",RuleId,":",PolicyId)if RecordType =112
Device Payload ID	One of(SensorId, DetectionEngineId), EventId, One of(ServerTimestamp, EventSecond))
Message	Description
Name	POLICY VIOLATION if RecordType = 8,36,65,97; METADATA if RecordType = 54,109,110,123; one of(EventName,RuleMessage,'Intrusion Event Record') if RecordType = 1,7,104,105,207,208,400; All of (POLICY VIOLATION, CorrelationRuleName, CorrelationPolicyName) if RecordType = 112
Source Address	One of (EventSourceIp, InitiatorIp, SourceIpAddress, InitiatorIpAddress, UsrLoginIPAddress)
Source Port	One of (EventSourcePort, InitiatorPort)
Source User ID	One of (SourceUserId, UsrLoginId)
Source User Name	One of (UsrLoginUsrNm, User)
Transport Protocol	One of (EventProtocol, Protocol, ProtocolName, TransportProtocol, TransportProtocol1, FlowProtocol)

eStreamer Intrusion Only Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High, high, 1; Medium = Medium, medium, 2; Low = Low, low, 3, 0, 4, 5
Device Action	One of (ImpactFlags, EventImpactFlags, RuleAction, Action("1=Detect", "2=Block", "3=Malware Cloud Lookup", "4=Malware Block", "5=Malware Whitelist"))
Device Custom Date 1	One of (ServerTimestamp, LastUsed)
Device Custom Date 2	HostLastSeen
Device Custom Number 2	One of (FingerprintId, FingerprintUuid)
Device Custom Number 3	BlockType
Device Custom String 1	payload
Device Custom String 2	Fingerprint
Device Custom String 6	One of (RenderedSignatureId, RuleId)
External ID	One of (EventId, ComplianceEventId)

ArcSight ESM Field	Device-Specific Field
Name	One of (EventName, RuleMessage, IOCEventType, EventDescription, FileAnalysisStatus, Disposition ("0=", "1=Clean", "2=Unknown", "3=Malware", "4=Unavailable", "5=Custom Signature"), "METADATA")
Request Client Application	One of(payloadHTTPUserAgent, ClientApplicationId, ApplicationId, WebApplicationId)
Request Context	payloadHTTPReferer
Request URL Host	payloadHTTPHost

eStreamer RNA Only Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Additional data	AttributeAddress
Additional data	AttributeCategory
Additional data	AttributeId
Additional data	AttributeItem
Additional data	AttributeName
Additional data	AttributeType (0=attribute with text blob as value, 1=attribute with value in range, 2=attribute with a list of possible values, 3=attribute with a URL as value, 4=attribute with binary blob as value)
Additional data	AttributeUuid
Additional data	AutoAssignedIpFlag
Additional data	BLOBBlockLength
Additional data	BLOBBlockType
Additional data	Blocked
Additional data	BlockReason (0=Intrusion event not dropped, 1=Intrusion event was dropped (inline mode, drop when inline is set), 2=The packet that triggered the event would have been dropped, if the intrusion policy had been applied to a detection engine using an inline interface set)
Additional data	Confidence
Additional data	DataTypeName
Additional data	DescriptionClean
Additional data	DestinationCriticality (0=None, 1=Low, 2=Medium, 3=High)
Additional data	DestinationHostType (0=Host, 1=Router, 2=Bridge, 3=NAT Device, 4=Load Balancer)
Additional data	DestinationOsFingerprintUuid
Additional data	DestinationServiceId
Additional data	DestinationVlanId
Additional data	Encoding
Additional data	EventDataType
Additional data	EventDefinedMask
Additional data	EventExtraData
Additional data	EventMicrosecond
Additional data	Flag
Additional data	GenericListBlockLength
Additional data	GenericListBlockType
Additional data	GenScanResult

ArcSight ESM Field	Device-Specific Field
Additional data	GenScanResultClean
Additional data	GenScanResultSubType
Additional data	GenScanResultSubTypeClean
Additional data	HostVulnerability
Additional data	HostVulnerabilityId
Additional data	InvalidFlags
Additional data	PayloadDataBlocks
Additional data	RangeStartingValue
Additional data	RangeEndingValue
Additional data	RnaHostVulnerability
Additional data	ScanResult
Additional data	ScanType
Additional data	ServiceBanner
Additional data	ServiceConfidence
Additional data	ServiceHits
Additional data	ServiceId
Additional data	ServiceInformation
Additional data	ServiceSubtype
Additional data	ServiceVendorName
Additional data	ServiceVersion
Additional data	SignatureGeneratorId
Additional data	SourceCriticality (0=None, 1=Low, 2=Medium, 3=High)
Additional data	SourceHostType (0=Host, 1=Router, 2=Bridge, 3=NAT Device, 4=Load Balancer)
Additional data	SourceId
Additional data	SourceOsFingerprintUuid
Additional data	SourceServiceId
Additional data	SourceType
Additional data	SourceVlanId
Additional data	ThirdPartyScanHostVulnerability
Additional data	UserProductDataBlocks (UsrPrdDtBlk)
Additional data	Vulnerability
Additional data	VulnerabilityName
Additional data	VulnerabilityNameClean
Additional data	VulnerabilityType
Agent (Connector) Severity	High = High, high, 1, Medium = Medium, medium, 2, Low = Low, low, 3, 0, 4, 5
Application Protocol	One of (NetworkProtocol, NetworkProtocol1, ApplicationProtocolId)
Bytes In	One of (BytesReceived, PacketsReceived)
Bytes Out	One of (BytesSent, PacketsSent)
Destination Mac Address	One of (Mac1Mac, Mac, MacChange, MacRange, MacAddress)
Destination Service Name	One of (ServiceName, SubServiceName, ServiceName1, TCPServiceName, TCP1ServiceName, UDPServiceName, UDP1ServiceName)
Destination User ID	One of (destinationUserId, DestinationUserId, UserId)

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	BugtraqId
Device Custom String 3	Host Type
Device Custom String 4	One of (ClientApplicationName, ClientApplicationName_list)
Device Custom String 5	CVEId
End Time	LastPacketTimestamp
File Type	FileType
Message	VulnerabilityId
Reason	One of (AccessControlRuleReason, RuleReason)
Source User ID	One of (SourceUserId, UsrLoginId)
Source User Name	One of(UsrLoginUsrNm, User)
Start Time	FirstPacketTimestamp

eStreamer Malware and File Events Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Additional data	ClientApplicationUrl
File Create Time	FileTimestamp
File Hash	One of (SHAHash, FileSHAHash, ParentFileSHAHash)
File Name	One Of(FileName, ParentFileName, FileNameOrDisposition)
File Path	FilePath
File Size	FileSize
Request URL	URI

Payload Sampling

Many customers use ArcSight for security event analysis, including investigating the packet records data that triggered the security event. In ArcSight terms, these packet records are called *payload*. Payload refers to the information carried in the body of an event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload may also be forensically significant. ArcSight supports two ways to retrieve payload from Sourcefire eStreamer: Payload Sampling and On-Demand Payload.

- **Payload Sampling** allows up to 1022 bytes of the payload to be retrieved and displayed as ASCII characters in a custom string field for ***each*** intrusion event. An option is also provided to display up to 511 bytes in hexadecimal format. By default, the payload sampling feature is not enabled due to its potentially large storage requirements. To enable payload sampling, select **true** for the Enable payload sampling parameter during connector installation.

- **On-Demand Payload Retrieval** lets you retrieve the entire payload if the payload is still held on the device. For some intrusion events, the Sourcefire eStreamer API returns a packet record different from the one requested by ArcSight, resulting in some inconsistency in the on-demand payload retrieval support. This has been discovered with eStreamer 4.0 and later versions. When the retrieval fails, ArcSight sends an error message: “Retrieval failed: The agent was unable to retrieve the payload from the security device.”

In order to enable collection of HTTP requests for parsing in your payload, set the `samplepayload.parseHTTPheaders` option in the SmartConnector setup to 'true' as described in the *Enable Parsing of HTTP Requests* procedure in the next section.

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

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

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Configure payload retention periods on each originating Sourcefire device.

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

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

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

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

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

Enable Parsing of HTTP Requests

If payload sampling is enabled and `samplepayload.parseHTTPheaders` is set to `true`, any events containing HTTP requests in their payloads are parsed as follows.

HTTP Header	Device-Specific Field	ESM Field
"Host:"	payloadHTTPHost	Request URL Host
"Referer:"	payloadHTTPReferer	Request Context
"User-Agent:"	payloadHTTPUserAgent	Request Client Application

The default value of the `samplepayload.parseHTTPheaders` option is `false`. To set this value to `true`, after connector installation, edit the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Locate the `samplepayload.parseHTTPheaders` and change the **Value** from false to true. Save the file and restart the connector for your change to take

effect. To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

Troubleshooting

Why didn't the ArcSight SmartConnector connect to eStreamer?

If the ArcSight SmartConnector fails to communicate with eStreamer, make sure eStreamer is running on the correct port (by default, it is port 8302). SSH to the Sourcefire Defense Center and use the following command:

```
netstat -a | grep 8302
```

I am getting so many RNA events; how can I filter out some of them effectively?

There are multiple ways to filter out events. You can use the SmartConnector filtering feature to filter out unexpected events in general. This SmartConnector also supports a device level filtering feature that will filter out events more effectively. To control filtering, you can modify these parameters, found in the `agent.properties` file (located at: `$ARCSIGHT_HOME\current\user\agent`).

```
agents[0].request.flow.data=true
agents[0].request.flow.data.version=rna
agents[0].request.rna.event=true
agents[0].request.rna.event.version=4.10
```

Why doesn't Sourcefire Defense Center provide the Sensor IP address?

Sourcefire events do not contain the correct Sensor IP address as the device address in the ArcSight event. Instead, the Sourcefire Defense Center's IP address is used as the device address regardless of which sensor generated the event.

The Sourcefire Defense Center does provide a Sensor ID. The Sensor ID can be used to derive the correct sensor address to be mapped to the device address field in each Sourcefire event. This can be accomplished by updating the `map.0.properties` file in the `$ARCSIGHT_HOME\current\user\agent\map\` directory with the following entries:

```
event.deviceExternalId,set.event.deviceAddress,set.event.deviceHostName
1,1.1.1.1,HOSTNAME01
2,1.1.1.2,HOSTNAME02
```

Manager Receipt Time	Device Address	Device Host Name	Device External ID	End Time	Device Vendor	Priority	Attacker Address	Name	Target Address	Device Product
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:43	Sourcefire	4	192.168.1.100		192.168.8.244	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:43	Sourcefire	4	192.168.1.100		192.168.8.217	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:43	Sourcefire	4	192.168.1.100		192.168.8.216	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:43	Sourcefire	4	192.168.1.100		192.168.8.246	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:43	Sourcefire	7	192.168.1.191		192.168.8.2	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:29:33	Sourcefire	9	192.168.8.2		192.168.4.2	Sourcefire Management Console eStreamer
17 Jun 2013 15:30:21 PDT	1.1.1.2	HOSTNAME02	2	5/21 15:32:44	Sourcefire	9	192.168.8.2		192.168.4.2	Sourcefire Management Console eStreamer