



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Cisco Secure IPS SDEE SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2006 – 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

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

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

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

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

Contents

| | |
|--|----|
| Configuration Guide for Cisco Secure IPS SDEE SmartConnector | 5 |
| Product Overview | 6 |
| Configure the Sensor for SmartConnector Event Collection | 7 |
| Obtain the Authentication Certificate from the Sensor | 7 |
| On Windows | 7 |
| On RedHat Linux | 11 |
| Install the SmartConnector | 12 |
| Prepare to Install Connector | 12 |
| Install Core Software | 13 |
| Set Global Parameters (optional) | 14 |
| Select Connector and Add Parameter Information | 16 |
| Select a Destination | 17 |
| Complete Installation and Configuration | 17 |
| Access Advanced Parameters | 18 |
| Enable XQuery Processing | 18 |
| Change XML Replacing Characters | 18 |
| Run the SmartConnector | 19 |
| Device Event Mapping to ArcSight Fields | 20 |
| Alert Payload Mappings | 20 |
| Alert Log Mappings | 20 |
| Error Log Mappings | 21 |
| Status Log Mappings | 22 |
| Payload Support | 24 |

Turn Off SSL for Debugging or Troubleshooting25

Troubleshooting27

Send Documentation Feedback 29

Configuration Guide for Cisco Secure IPS SDEE SmartConnector

This guide provides information for installing the SmartConnector for Cisco Secure IPS SDEE and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

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

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Cisco IPS Sensors are network security appliances that detect unauthorized activity over the network, analyzing traffic in real time, letting users quickly respond to security breaches. When unauthorized activity is detected, the sensors can send alarms providing details of the activity and can control other systems, such as routers, to terminate the unauthorized session or sessions. Sensor installation requires seven simple addressing parameters and no special training. When the sensor is installed, it immediately begins monitoring as a promiscuous device by default.

This SmartConnector also can receive events from multiple Cisco IPS sensors through direct connection.

Configure the Sensor for SmartConnector Event Collection

The SmartConnector Installation and Configuration wizard will ask you for a set of parameters during the installation process. Using these parameters, the wizard configures the sensor to send event information to the ArcSight SmartConnector.



The following steps presume you have configured the IPS sensor to let the SmartConnector communicate with it. If you have not done so, see your vendor's documentation for information about the configuration of access lists or allowed hosts.

The SmartConnector can validate the Cisco IPS Sensor's authentication certificate. To operate in this configuration, first get the certificate from Cisco IPS Sensor and import it into the SmartConnector Java Runtime Environment before running the SmartConnector for Cisco IPS SDEE.

Obtain the Authentication Certificate from the Sensor

The following procedure is required only if you want the SmartConnector to validate the Cisco IPS sensor's authentication certificate.



If you want the connector to validate the certificate, remember to select 'true' for the SmartConnector's Certificate Validation parameter during connector installation.

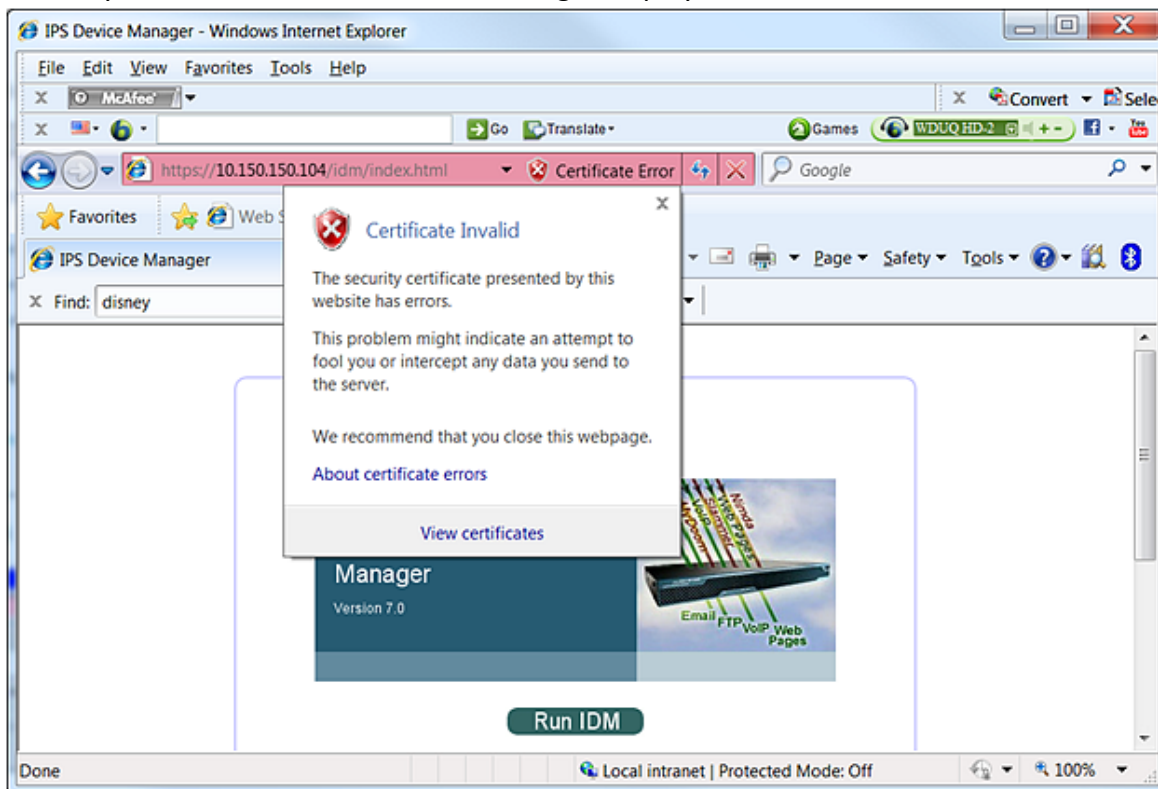
This section provides instructions for Microsoft Windows and Red Hat Linux for retrieving, importing, and verifying the authentication certificate. You will download and save the certificate file to a temporary location. During the SmartConnector installation process, you will be asked to copy this file to a SmartConnector subfolder.

On Windows

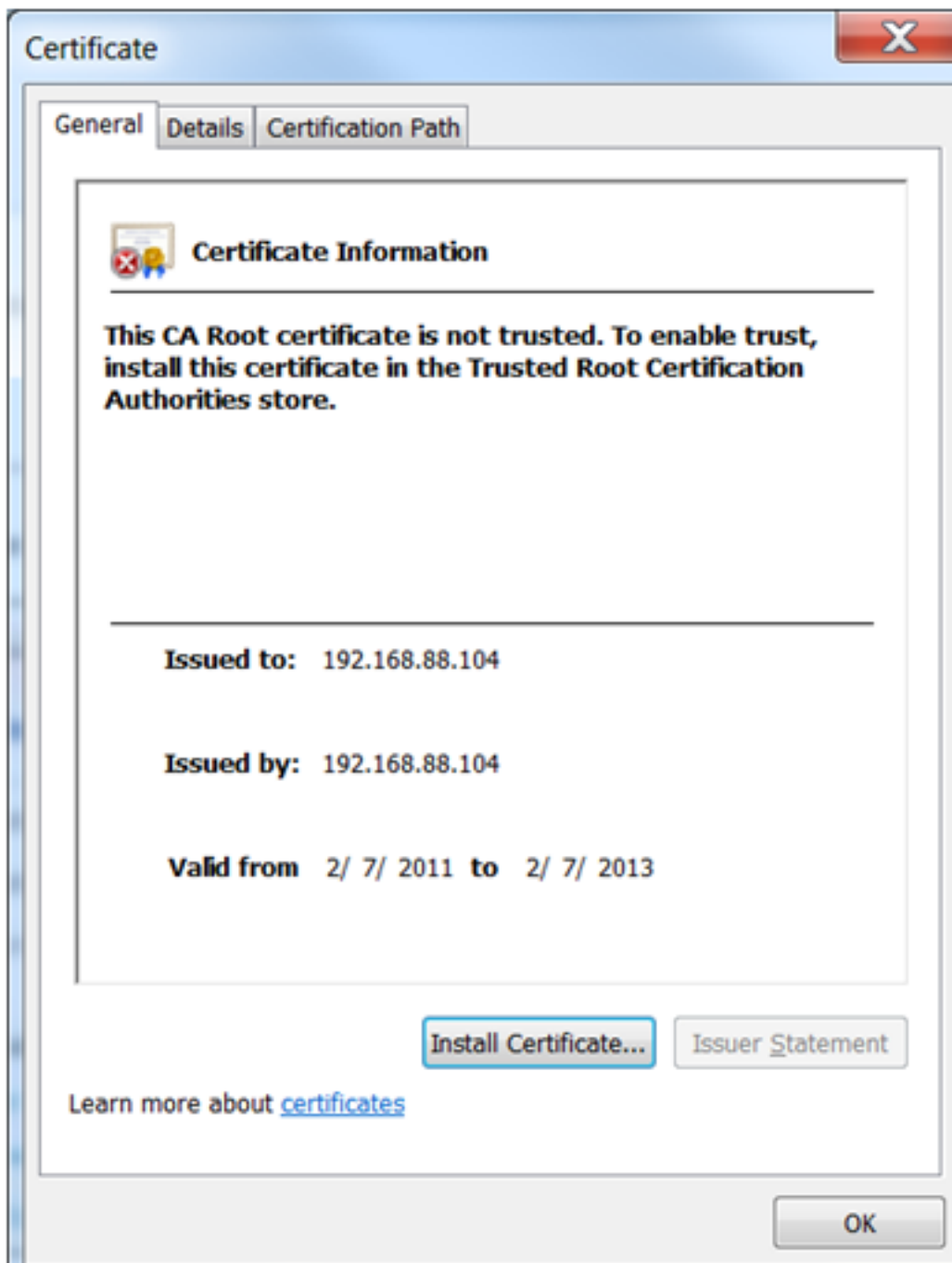
Microsoft Internet Explorer 7.0 or later is required.

- 1 From Internet Explorer, enter the IP address of the IPS sensor (for example `https://1010.111.16`).

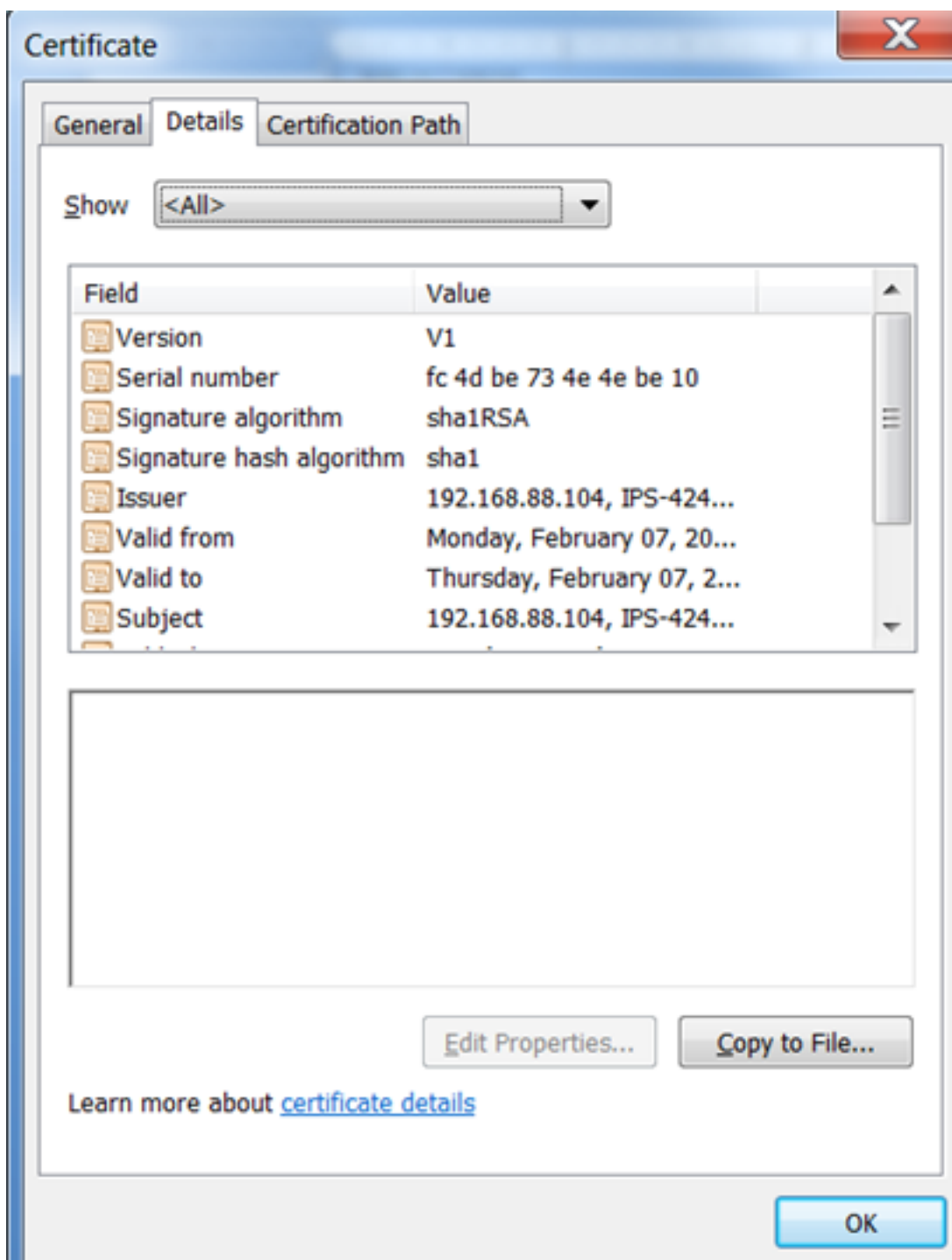
2 When the Certificate Error is displayed (as shown highlighted in pink below), click the arrow by **Certificate Error** and the following is displayed:



3 Click **View certificates**. When the Certificate Information is displayed, click **Install Certificate....**



4 Click the **Details** tab and click **Copy to File...** The Certificate Export Wizard is displayed.



5 Click **Next**, then, on the next window, select **Base-64 encode X.509 (.CER)**, which is used by the SmartConnector for Cisco IPS SDEE.

6 Click **Next**; on the next window enter a temporary location and a file name (for example, `ips40_sensor.cer`) for the new certificate. You will be asked to copy this file to a SmartConnector subfolder during the installation process.

- 7 Click **Next**, then, on the window displayed, click **Finish** to exit the wizard.

On RedHat Linux

- 1 To obtain the certificate on RedHat Linux, enter the following:

```
/usr/bin/openssl s_client -connect 10.0.111.16:443 > openssl_output.txt
```

- 2 Edit **openssl_output.txt** using your preferred editor. Copy the Server certificate:

```
-----BEGIN CERTIFICATE-----
MIICHjCCAYcCCOmRUSHwwM2YMA0GCSqGSIb3DQEBBQUAMFQxCzAJBgNVBAYTA1VT
MRwwGgYDVQQKEExNDaXNjbyBTeXN0ZW1zLCBJbmMuMREwDwYDVQQLEWhJRFRMTNDIx
MDEUMBIGA1UEAxMLMTAuMCA4xMDAuMTgwHhcNMDYwMTIzMtK0OTA5WhcNMDgwMTI0
MTk0OTA5WjBUMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ21zY28gU31zdGVtcywg
SW5jLjJERMA8GA1UECXMISURTLTQyMTAxFDASBgNVBAMTCzEwLjAuMTAwLjE4MIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvNOLNyUcnMaVa8DHBkL5TeR2X0+Ja
zVLk44D4x1epwY+IqyZnAQs2FS+nWCvQ+u7Xai/wC7Vs95UmtuEMSMGL3aRRfavY
lCuxIt0hrI/PPScxMhWGPv05R1YsFeQ//XZTrcq0q/yoi0bzQM/bx0ayReM/dS0P
5EoIPJxGrjx8CQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABdspBcM5+5ve5Ie0Q+f
NIm/CvFQc/e2KMfRuGouw5zwH1hAeHBeT7zGq0uklCtGu9t/EwYtYkbJV/HemrJo
Te0HuyH4FUSlN7Kdvg1IwrxbtT7FEQicwe/zcq86h7IehZRp4IbdXTE6+e1r6kw0
LCe+YZMwTTzfheki6UEz/eVg
-----END CERTIFICATE-----
```

- 3 Copy this selection into a new file (for example, `ips40_sensor.cer`) and save in a temporary location. You will import this certificate to the connector Local Java Runtime Environment during the SmartConnector installation and configuration process.

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 OpenText SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the OpenText 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 Complete installing the SmartConnector core component.

The following steps are for importing the sensor certificate to the connector's Local Java Run Environment; this example is for Windows systems. If you are making use of Linux or Unix, change the command to reflect your \$ARCSIGHT_HOME and change \ to /.

A Click **Cancel** to exit the configuration wizard.

B From \$ARCSIGHT_HOME\current\user\agent, create a ciscoids subdirectory; copy the certificate file you obtained during sensor configuration (for example, ips40_sensor.cer) and save it into this subdirectory.

C From \$ARCSIGHT_HOME\current\bin, execute the **keytool** application to import the ips40_sensor.cer certificate obtained by following the steps in the previous section. Enter this **keytool** command on a single line.

```
arcsight agent keytool -import -alias ips40_10_0_111_16 -file  
<\user\agent\ciscoids\ips40_sensor.cer> -store clientcerts
```

where <\user\agent\ciscoids\ips40_sensor.cer> is the path to and name of the sensor certificate file.

D Following the prompts, answer **yes** for the prompt **Trust this certificate?**

```
Owner: CN=10.0.111.16, OU=IDS-IDS-4210, O="Cisco Systems, Inc.", C=US
Issuer: CN=10.0.111.16, OU=IDS-IDS-4210, o="Cisco Systems, Inc.", C=US
Serial number: 26fb5b6a69e0bca7
Valid from: Tue May 06 17:26:31 PDT 2003 until: Fri May 06
17:26:31 PDT 2005
Certificate fingerprints:
MD5: 14:BB:6A:6E:92:15:4E:7A:0A:40:EE:04:23:33:AE:EF
SHA1:
99:94:7E:30:43:53:A6:2A:DA:76:12:21:6A:C5:F3:09:E5:68:A8:36
Trust this certificate? [no]: yes
Certificate was added to keystore
```

E Verify the imported certificate by entering the following command from \$ARCSIGHT_HOME\current\bin:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate (alias=ids40_10_0_111_16) is displayed in the list:

```
Keystore type: jks
keystore provider:SUN
Your keystore contains 12 entries:
ids40_10_0_111_16, Fri May 09 18:37:11 PDT 2003,
trustedCertEntry,
Certificate fingerprint (MD5):
14:BB:6A:6E:92:15:4E:7A:0A:40:EE:04:23:33:AE:EF
```

F From \$ARCSIGHT_HOME/current/bin, double-click 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:

| Parameter | Setting |
|-------------------|--|
| FIPS mode | Select 'Enabled' 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 'Disabled'. |
| Remote Management | Select 'Enabled' 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 'Disabled'. |

| Parameter | Setting |
|---------------------------------|--|
| Remote Management Listener Port | The remote management device will listen to the port specified in this field. The default port number is 9001. |
| Preferred IP Version | When 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. The initial setting is IPv4. |

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

| Parameter | Setting |
|------------------------------|--|
| Format Preserving Encryption | Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector. |
| Format Preserving Policy URL | Enter the URL where the OpenText SecureData Server is installed. |
| Proxy Server (https) | Enter the proxy host for https connection if any proxy is enabled for this machine. |
| Proxy Port | Enter the proxy port for https connection if any proxy is enabled for this machine. |
| Format Preserving Identity | The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData. |
| Format Preserving Secret | Enter the secret configured for OpenText SecureData to use for encryption. |
| Event Fields to Encrypt | Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited. |

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 proceed with "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 **Cisco Secure IPS SDEE** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

| Parameter | Description |
|-------------------------------|--|
| Cisco IPS Sensor Event Types | Specify event types to retrieve. evAlert, evIdsAlert, evError, and evStatus types are filled in by default. If your appliance uses SDEE, select evError, evStatus, and evIdsAlert, or any subset of the three event types. If your appliance uses CIDE (a Cisco extension to SDEE), select evError, evStatus, and evAlert, or any subset of those three event types. |
| Enable Certificate Validation | Specify whether the SmartConnector is to enable the validation of the sensor's certificate for the client. Certificate validation is enabled (true) by default. |
| Enable Hostname Validation | Specify whether the SmartConnector is to enable the validation of the sensor's hostname. Hostname validation is enabled (true) by default. |
| Enable Payload Sampling | Set this option to true to enable payload sampling, thus making payload available for the device for selected events through the Console. Because event payloads are relatively large, ArcSight does not store them by default. |

- 4 Enter the device details.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

| Parameter | Description |
|----------------|---|
| Sensor Host IP | Enter the Cisco IPS Sensor's IP Address. |
| Port | Enter the Cisco IPS Port. |
| User | Enter the Cisco IPS user name. |
| Password | Enter the password for the Cisco IPS user. |
| Event Severity | Specify the event severity to retrieve (by default, the severity is set to Informational plus low, medium, and high). |

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*.

Access Advanced Parameters

After SmartConnector installation, you can change the connector's advanced parameters by editing the `agent.properties` file found at `$ARCSIGHT_HOME\current\user\agent`.

Enable XQuery Processing

To enable xquery processing:

- 1 Access advanced parameters as described above.
- 2 Locate the `usexquery` parameter and change the default value of `false` to `true`.
- 3 Save the file and restart the connector for your changes to take effect.

Change XML Replacing Characters

To use '[' and ']' in place of '<' and '>' in connector processing:

- 1 Access advanced parameters as described above.
- 2 Locate the `changexmlreplacingcharacters` parameter and change the default value of `false` to `true`.
- 3 Save the file and restart the connector for your changes to take effect.

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.

Alert Payload Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------|-----------------------|
| Device Custom String 5 | triggerPacket |
| Device Custom String 6 | eventId |
| Device Event Class ID | sigId |

Alert Log Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|--|
| Agent (Connector) Severity | High = high; Medium = medium; Low = informational, low |
| Base Event Count | baseCount |
| Destination Address | victimAddr |
| Destination Port | victimPort |
| Device Action | One of ('Denied', 'Permitted') |
| Device Custom IPv6 Address 2 | attackerIPv6Addr (Source IPv6 Address) |
| Device Custom IPv6 Address 3 | victimIPv6Addr (Destination IPv6 Address) |
| Device Custom Number 1 | Risk Rating Value |
| Device Custom Number 2 | interfaceGroup |
| Device Custom Number 3 | vlan |
| Device Custom String 1 | Signature version |
| Device Custom String 2 | subSigId |
| Device Custom String 3 | fromAttacker |
| Device Custom String 4 | fromVictim |
| Device Custom String 5 | One of(signature or marsCategory) |

| ArcSight ESM Field | Device-Specific Field |
|--------------------------|-------------------------------------|
| Device Custom String 6 | payloadSample |
| Device Event Category | 'evAlert' |
| Device Event Class ID | sigId |
| Device Host Name | hostId |
| Device Inbound Interface | interface |
| Device Payload ID | ipLogId |
| Device Process Name | appName |
| Device Product | 'Cisco Intrusion Prevention System' |
| Device Receipt Time | time |
| Device Severity | severity |
| Device Vendor | 'CISCO' |
| External ID | eventId |
| Message | alertDetails |
| Name | sigName |
| Reason | globalCorrelationRiskDelta |
| Request Context | interfaceContext |
| Source Address | attackerAddr |
| Source Port | attackerPort |
| Transport Protocol | protocol |
| Type | 'AGGREGATED' |

Error Log Mappings

| ArcSight ESM Field | Device-Specific Field |
|----------------------------|---|
| Agent (Connector) Severity | High = fatal, Medium = error, Low = warning |
| Device Custom String 1 | HostId |
| Device Event Category | 'evError' |
| Device Host Name | hostId |
| Device Process Name | appName |
| Device Product | 'Cisco Intrusion Prevention System' |

| ArcSight ESM Field | Device-Specific Field |
|---------------------|-----------------------|
| Device Receipt Time | time |
| Device Severity | severity |
| Device Vendor | 'CISCO' |
| External ID | eventId |
| Message | errorMessage |
| Name | errorName |

Status Log Mappings

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|---|
| Agent (Connector) Severity | High = false; Low = true, Unknown |
| Bytes In | One of (ipLogBytesCaptured, ipLogAddedIpLogBytesCaptured, ipLogCompletedIpLogBytesCaptured, ipLogStartedIpLogBytesCaptured) |
| Destination Address | One of (ipLogAddedIpLogAddr, ipLogCompletedIpLogAddr, ipLogStartedIpLogAddr) |
| Destination Host Name | One of (shunEntryAddedInfoDestAddr, shunEntryRemovedInfoDestAddr) |
| Destination Port | One of (shunEntryAddedInfoDestPort, shunEntryRemovedInfoDestPort) |
| Destination Process Name | One of (appName, executionStatusChangeApplication) |
| Destination User Name | One of (clockChangedUser, shutdownUser) |
| Device Action | loginActionAttributeAction |
| Device Custom IPv6 Address 3 | One of (ipLogStartedIPv6Addr, ipLogAddedIPv6Addr) (Destination IPv6 Address) |
| Device Custom String 1 | HostId |
| Device Event Category | 'evStatus' |
| Device Event Class ID | One of ((descriptionParentNode, descriptionParentNode, resultParentNode) |
| Device Host Name | hostId |
| Device Outbound Interface | One of (netInterfaceAddedInterface, netInterfaceRemovedInterface) |
| Device Process Name | appName |
| Device Product | 'Cisco Intrusion Prevention System' |
| Device Receipt Time | time |

| ArcSight ESM Field | Device-Specific Field |
|---------------------|---|
| Device Severity | One of (cmdStatus, 'Unknown') |
| Device Vendor | 'CISCO' |
| Event Outcome | shutdownSuccessful |
| External ID | eventId |
| Message | One of (syslogMessage,cmdDescription, applicationStoppedReason, executionStatusChangeDescription, globalCorrUpdateCompletedDescript, globalCorrUpdateStartedDescript, rebootDescription,softwareUpgradeCompletedDescription, softwareUpgradelnitiatedDescription, deniedAttckLstClrByUsrDescript, controlTransRespDataCompWarning, statusDescription,shutdownDescription) |
| Name | One of (statusDescription, descriptionParentNode, resultParentNode) |
| Source Host Name | One of (cmdHostId, loginActionUserAddress, shunEntryAddedInfoSourceAddr, shunEntryRemovedInfoSourceAddr, denyAttackerCompletedAddress, denyAttackerStartedAddress) |
| Source Port | One of (loginActionPort, shunEntryAddedInfoSourcePort, shunEntryRemovedInfoSourcePort) |
| Source Process Name | cmdAppName |
| Source User ID | One of (loginActionUserName, cmdUser, rebootUser) |
| Start Time | One of (ipLogBeginTime, ipLogCompletedIpLogBeginTime, ipLogStartedIpLogBeginTime) |

Payload Support

Payload support is available with this SmartConnector. *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.

You can retrieve, preserve, view, or discard payloads using the ArcSight ESM 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.

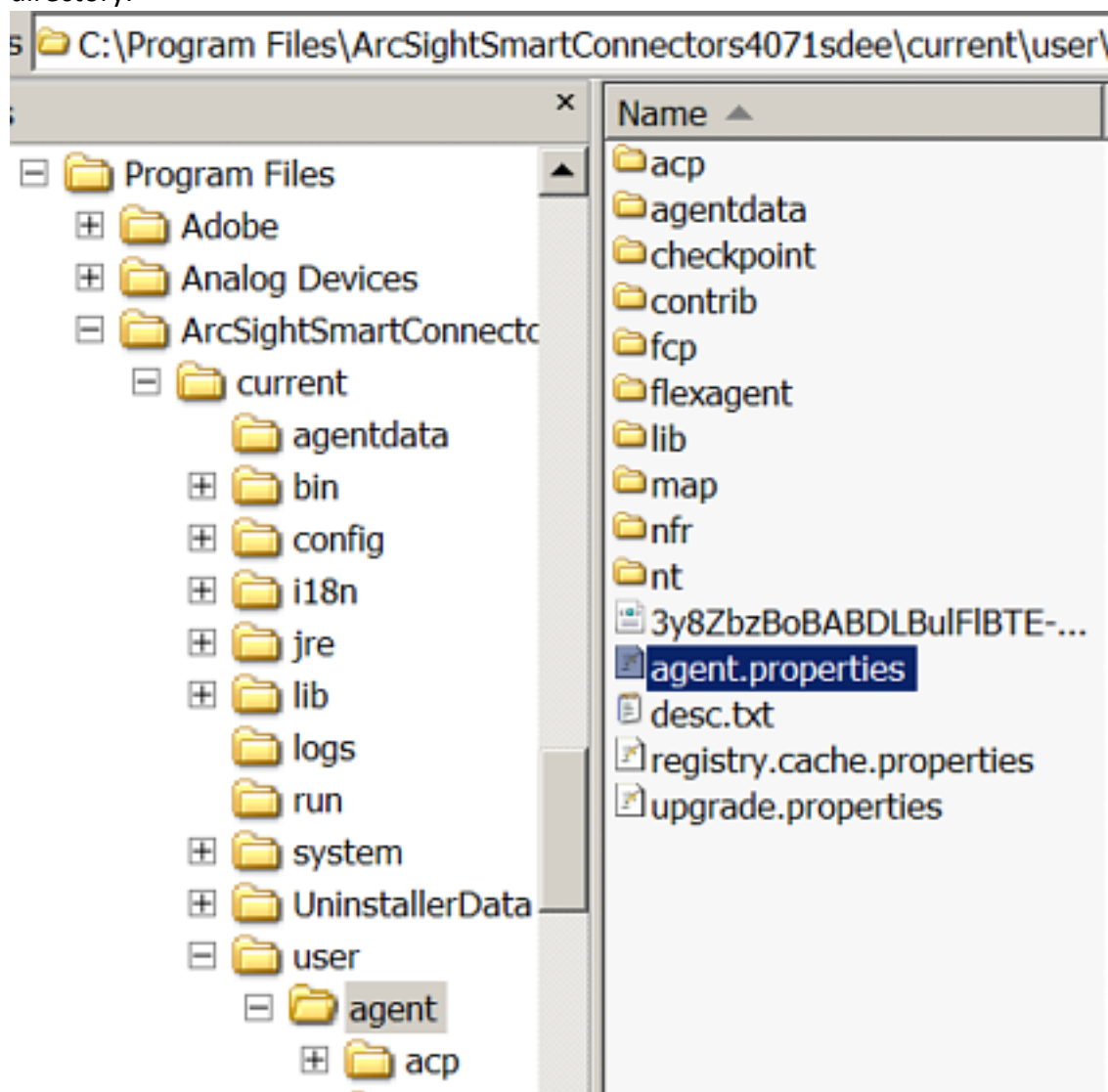
Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

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.

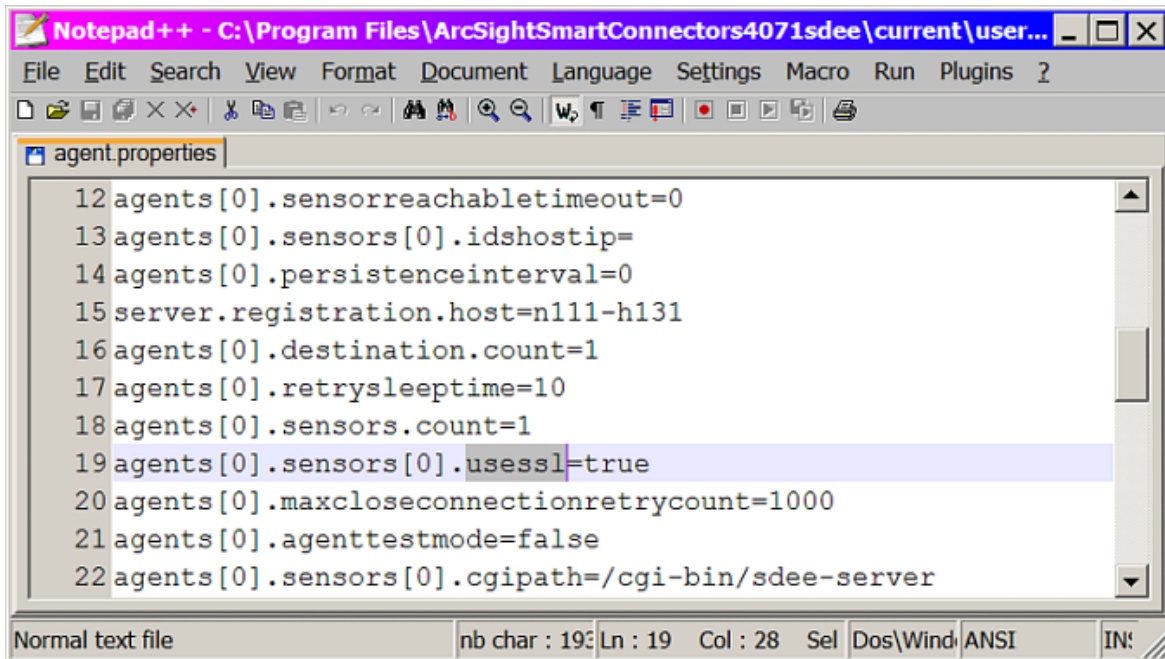
Turn Off SSL for Debugging or Troubleshooting

An advanced option named `usessl` has been added to turn off SSL for debugging/troubleshooting purposes. The value of this option is true by default. To change the value of this parameter:

- 1 After connector installation, locate the `$ARCSIGHT_HOME\current\user\agent` directory.



- 2 Open `agent.properties` to edit.
- 3 Locate the `usessl` parameter and set its value to false.



The screenshot shows a Notepad++ window with the title bar 'Notepad++ - C:\Program Files\ArcSightSmartConnectors4071sdee\current\user...'. The menu bar includes File, Edit, Search, View, Format, Document, Language, Settings, Macro, Run, and Plugins. The toolbar contains various icons for file operations and editing. The text area shows the contents of the 'agent.properties' file, with the following lines:

```
12 agents[0].sensorreachbletimeout=0
13 agents[0].sensors[0].idshostip=
14 agents[0].persistenceinterval=0
15 server.registration.host=n111-h131
16 agents[0].destination.count=1
17 agents[0].retrysleeptime=10
18 agents[0].sensors.count=1
19 agents[0].sensors[0].usessl=true
20 agents[0].maxcloseconnectionretrycount=1000
21 agents[0].agenttestmode=false
22 agents[0].sensors[0].cgipath=/cgi-bin/sdee-server
```

The line 'agents[0].sensors[0].usessl=true' is highlighted in blue. The status bar at the bottom indicates 'Normal text file', 'nb char : 193', 'Ln : 19', 'Col : 28', 'Sel', 'Dos\Wind', 'ANSI', and 'IN:'.

- 4 Save your change and exit the file.
- 5 Restart the connector for your changes to take effect.

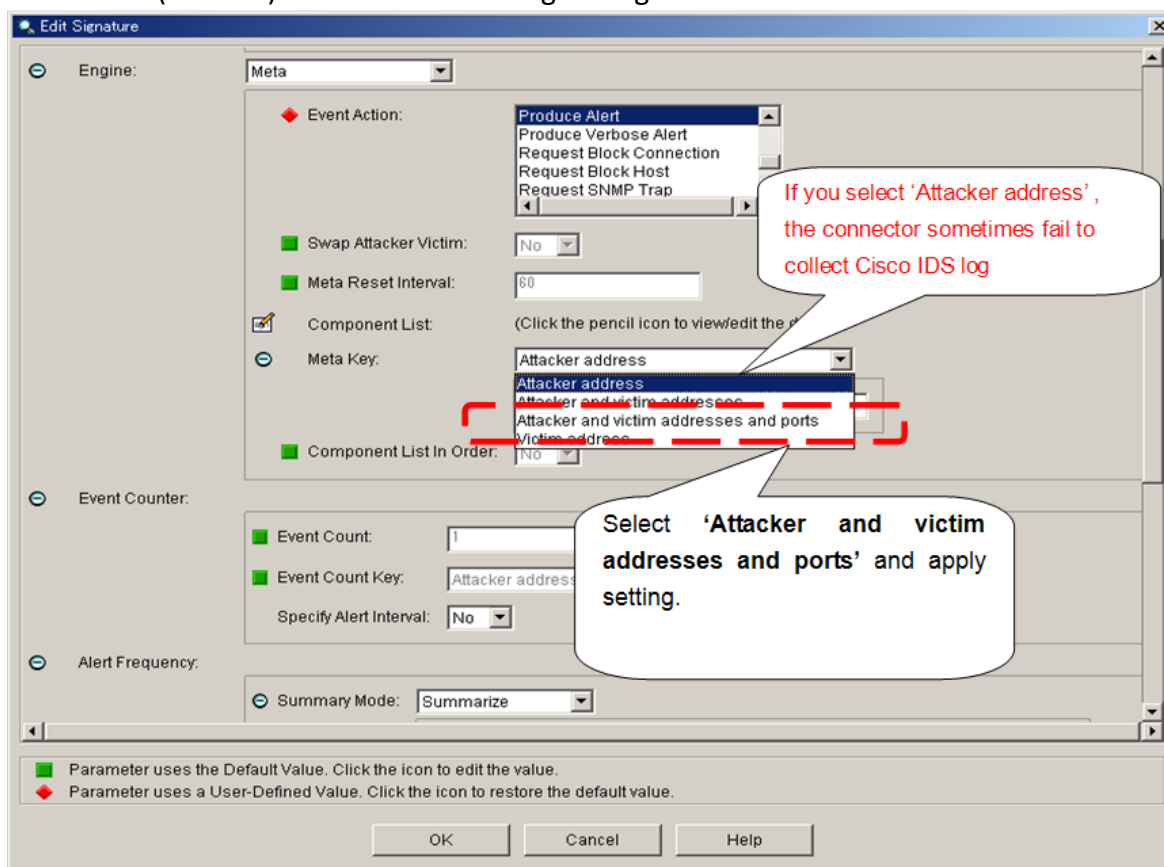
Troubleshooting

How can I see the raw events received from the SDEE device?

Set the value of the `traceallxml` parameter to true in `$ARCSIGHT_HOME/current/user/agent/agent.properties` and restart the connector. From the console, enable tracing for the SDEE sensor in which you are interested and retrieve the trace.

Why does the connectotr5s sometimes fail to collect the Cisco IDS log?

Try selecting Attacker and victim addresses and ports in the Meta Key section of the Cisco IDS Edit Signature panel and apply. If you select only Attacker address in this section, the connector sometimes fails to collect the log. If you set 'Attacker and victim addresses and ports' in Meta Key, target address and attacker/target port information is added in the original log. If addr and port have no value, the value '0' (port) or '0.0.0.0' (address) are added in the original log.



please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to

receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive events.

Send Documentation Feedback

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

**Feedback on Configuration Guide for Cisco Secure IPS SDEE SmartConnector
(SmartConnectors 8.4.3)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!