Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Tripwire IP360 File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Tripwire IP360 File

October 17, 2017

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Added new configuration parameters to support SSL certification validation and hostname validation.
08/30/2016	Added support for version 7.5.
11/17/2015	Added support for version 7.4. Removed support for versions 6.4, 6.5, 6.6, 6.8, and 7.0.
02/16/2015	Added field mappings for Device Event Class ID, Device Severity, and Agent (Connector) Severity.
11/14/2014	Added support for version 7.0. Changed vendor name from 'nCircle' to 'Tripwire' and product name from 'Vulnerability Scanner' to 'IP360'.
08/15/2013	Added field mappings.

Contents

SmartConnector for Tripwire IP360 File

This guide provides information for installing the SmartConnector for Tripwire IP 360 File and configuring the device for event collection. XML3 log format is supported for Tripwire Device Profiler versions 7.4 and 7.5. This connector was formerly known as the nCircle Scanner XML3 File connector.

Product Overview

Tripwire IP360 is an enterprise-class vulnerability and risk management system that enables organizations to measure, manage, and reduce their network security risk. IP360 gathers detailed intelligence about the endpoint devices on the network, and uses reporting and analytics to prioritize vulnerabilities and provide a comprehensive view of network risk.

The ASPL XML Folder

The ASPL XML folder contains static information about all the possible vulnerabilities, operating systems, and applications of which Tripwire is aware. This changes approximately twice a week, and the connector downloads the file from the appliance and saves it in the local ASPL XML folder.

If, in the future, Tripwire is not reachable for some reason, the connector can get the ASPL XML file from the local folder. That occurs only when the appliance cannot be reached; otherwise, the connector looks for new versions in the appliance. It only downloads the ASPL XML file when the file has changed in the appliance.

Prior to Tripwire version 6.8, the connector picked up ASPL XML files from the local folder only if they were named ASPL-*.<lang>.xml (where <lang> is `en` for English or `jp` for Japanese). With the Tripwire Device Profiler version 6.8 support, the connector picks up compressed files as well as files starting with ontology. The following types of files will be picked up:

ASPL-*.<lang>.xml
ASPL-*.<lang>.xml.gz
ASPL-*.<lang>.xml.zip
ontology-*.<lang>.xml
ontology-*.<lang>.xml.gz
ontology-*.<lang>.xml.zip

Configure the Device for Event Collection

The VnE Manager is the central management tool for IP360. It automatically and manually exports scan data (both .xml and .md5 files) to user-specified destinations. In Version 6.3.0, IP360 uses XML as a format for automatically exported Device Profiler scan results. This SmartConnector reads XML3 exported data.

Under **Administer: System -> VnE Manager -> Automated Export**, click **Modify** to view (and change, if needed) the following fields, which are required during SmartConnector installation:

- **User** - The user account on the machine to which the data is exported (the user password also will be required during SmartConnector installation).

- **Host** - Host name or IP address of the machine (the port to which VnE Manager is listening is also required during SmartConnector installation).
- **Directory** (Scan Report Folder) - The path to the directory in which the data is stored.
- **Format** - The format for the exported data (ensure XML3 is selected).
- **Status** - Ensure that **Active** is selected. This turns automated export on. If **Inactive** is selected, automated export is off.

Click **Submit** to save any changes you made.

Modes of Operation

The SmartConnector for Tripwire IP360 File SmartConnector, as with other vulnerability scanners, supports two operation modes:

- **Interactive** – This mode is designed to be used by an operator who requires only certain reports to be sent to the connector. In this mode, the SmartConnector reads the contents of the configured folder and presents it in a UI window. You can select which scan reports are to be sent to the ESM Manager. After completing the selections, click on **Send** to send all the selected scanner reports to ESM. Close (exit) the window when all the desired scans have been sent to ESM and the connector will terminate. In this mode, the SmartConnector should not be run as a service, only as a stand-alone application.
- **Automatic** – This mode is designed to be used in conjunction with an automated procedure to periodically run scans with the Tripwire scanner. At the end of the scan, Tripwire creates another file with the same name but with the 'md5' extension. When the VnE Manager is configured to export the XML report, it also exports the .md5 file into the same folder. The appearance of this file triggers the SmartConnector to import the report. The reports processed are renamed to {original report file} + "xml_processed".

In both modes, the SmartConnector records the file names of the reports that have been sent to the ESM Manager; therefore, if you use the interactive mode, the list of files available displays only the files that have not yet been sent to the ESM Manager. The same applies for the automatic mode; only files that are present in the configured folder that have not been sent already are processed.

To run a scanner connector in interactive mode, the connector must be run in standalone mode and not as a service. Automatic mode, however, can be run either standalone or as a service,

Increase Memory Size for XML Reports

The connector cannot process reports that are too lengthy. With the default 256M memory setting, the connector can safely process reports up to 250K in length. If memory is increased to the maximum limit of 1024M, the connector can process reports up to a million lines in length. Longer reports cannot be processed. ArcSight's recommendation for long reports is to split the scan into multiple smaller reports and import them individually.

To increase the memory size for stand-alone connectors from the command line, change the following line in `$ARCSIGHT_HOME\current\bin\scripts\connectors.bat` (Windows) or `$ARCSIGHT_HOME/current/bin/scripts/connectors.sh` (Unix)

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms256m -Xmx256m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS="  -Xms1024m -Xmx1024m "
```

To increase the memory size for connectors being run as a service, change the following lines in `user/agent/agent.wrapper.conf` from:

```
wrapper.java.initmemory=256
wrapper.java.maxmemory=256
```

to:

```
wrapper.java.initmemory=1024
wrapper.java.maxmemory=1024
```

To increase the memory size for connectors managed by the Connector Appliance/ArcSight Management Center, the heap size can be set using a container level command.

Install the SmartConnector

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

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

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.

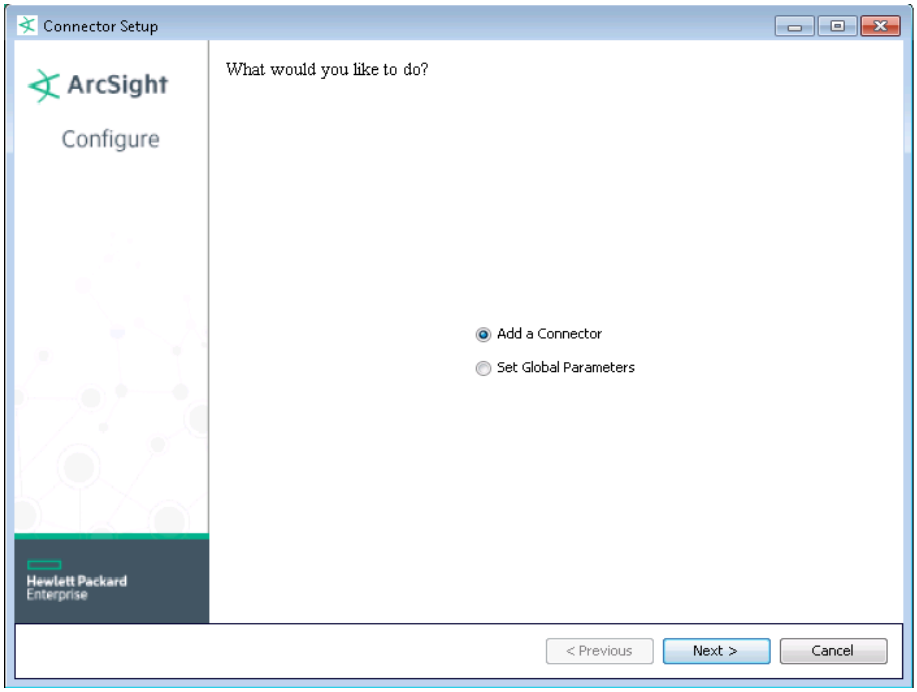
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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:



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'.

Parameter	Setting
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'.
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.

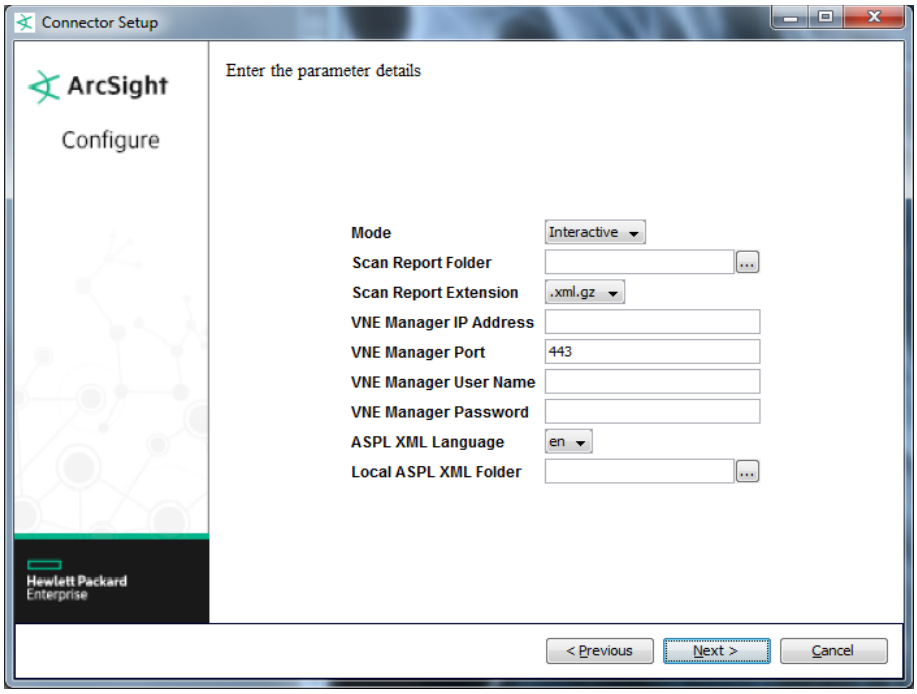
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

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 HPE 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 HPE 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 HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE 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 **Tripwire IP360 File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Mode	Select whether to send event logs to the connector using Interactive (manual) or Automatic mode.
Scan Report Folder	Enter the name of the folder in which scan reports are stored.
Scan Report Extension	Select the file extension format for output files to the SmartConnector: xml.gz, xml.zip, or .xml.
VNE Manager IP Address	Enter the IP address of the Tripwire VNE Manager Appliance.
VNE Manager Port	Enter the number of the port to which Tripwire VNE Manager is listening. The default value is port 443.
VNE Manager User Name	Enter the User name to login to Tripwire VNE Manager.
VNE Manager Password	Enter the password for the Tripwire VNE Manager user.
ASPL XML Language	Select the language for ASPL XML (en=English, jp=Japanese). See "The ASPL XML Folder" earlier in this document.
Local ASPL XML Folder	Enter the name of the folder in which the downloaded ASPL XML files are deposited.
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 Host Validation	Specify whether the SmartConnector is to enable the validation of the sensor's hostname. Hostname validation is enabled (true) by default.

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.

Open Ports Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	medium = Medium
Bytes Out	bytesOut
Category Technique	Vulnerability Category (1)
Destination Address	ip
Destination Host Name	One of (dnsName, serverHostName, serverName, 'Port')
Destination Mac Address	One of(macAddress,macAddressItem)
Destination Port	One of(port,portItem)
Device Custom Date 2	detectedTime
Device Custom String 4	hostScore
Device Custom String 5	Nmapstatus
Device Event Class ID	Open Port
Device Product	'IP360'
Device Receipt Time	StartDate
Device Severity	Medium
Device Vendor	'Tripwire'
End Time	EndDate
File Path	path
File Permission	permissionInfo
Message	One of (certificateError, serverStatus)
Name	'Open Port'
Request Client Application	One of (clientApplication, clientApplicationItem, clientApplicationVersion)
Source Host Name	sourceHostName
Source User Name	One of (lastLoggedInUser, userCredentialInfo, 'Username: Password', sourceUser, clientUserName)
Transport Protocol	One of(protocol,portInfo)

Scanner Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	ip
Destination Host Name	dnsName
Destination Mac Address	MacAddress
Device Custom Date 2	detectedTime

URIs Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	medium = Medium

ArcSight ESM Field	Device-Specific Field
Bytes Out	bytesOut
Category Technique	Vulnerabililty Category (4)
Destination Address	ip
Destination Host Name	One of (dnsName, serverHostName, serverName, 'Port')
Destination Mac Address	One of(macAddress,macAddressItem)
Destination Port	One of(portItem,portInfo)
Device Custom Date 2	detectedTime
Device Custom String 4	hostScore
Device Custom String 5	Nmapstatus
Device Event Class ID	One of (Application Detected","Operating System Detected")
Device Product	'IP360'
Device Receipt Time	StartDate
Device Severity	Medium
Device Vendor	'Tripwire'
End Time	EndDate
File Path	One of(Both("/Site Asset Categories/Application/",appname),path)
File Permission	permissionInfo
Message	One of (certificateError, serverStatus)
Name	Application Detected or Operating System Detected
Request Client Application	One of (clientApplication, clientApplicationItem, clientApplicationVersion)
Source Host Name	sourceHostName
Source User Name	One of (lastLoggedInUser, userCredentialInfo, 'Username: Password', sourceUser, clientUserName)
Transport Protocol	portInfo

Vulnerabilities Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Bytes Out	bytesOut
Category Technique	Vulnerability Category (0)
Connector (Agent) Severity	Very High = 60000..89999; High = 40000..59999; Medium = 20000..39999; Low = 0..19999
Destination Address	ip
Destination Host Name	One of (dnsName, serverHostName, serverName, 'Port')
Destination Mac Address	One of(macAddress,macAddressItem)
Destination Port	One of(portItem,portInfo)
Device Custom Date 1	date
Device Custom Date 2	detectedTime
Device Custom Number 1	ruleId
Device Custom String 1	solution
Device Custom String 2	category
Device Custom String 3	netbiosName
Device Custom String 4	hostScore
Device Custom String 5	Nmapstatus
Device Custom String 6	ontology_module_name

ArcSight ESM Field	Device-Specific Field
Device Event Category	risk
Device Event Class Id	Tripwire id
Device Product	'IP360'
Device Receipt Time	StartDate
Device Severity	score
Device Vendor	'Tripwire'
End Time	EndDate
File Path	path
File Permission	permissionInfo
Message	One of (certificateError, serverStatus)
Name	vulnName
Request Client Application	One of (clientApplication, clientApplicationItem, clientApplicationVersion)
Source Host Name	sourceHostName
Source User Name	One of (lastLoggedInUser, userCredentialInfo, 'Username: Password', sourceUser, clientUserName)
Transport Protocol	portInfo

SmartConnector Verification

The SmartConnector, when run in interactive mode, displays all the available scan jobs that are yet to be sent to the ESM Manager. You can select one or more jobs and click **Send**. In less than a minute, the ESM Console displays several events coming from this connector reporting the assets discovered, open ports and vulnerabilities, vulnerability details, and operating system information. In addition, you should see the created or updated asset resources under /All Assets/Site AssetCategories/Zone where Zone is the ESM default or configured zone for the address range where asset's ip address falls. Also displayed are open ports, applications, and operating system information represented as asset categories added to this asset. Vulnerabilities for the asset are found under the Vulnerabilities tab.

Troubleshooting

The Connector GUI in interactive mode does not display some reports.

Click on **Options** and select **Refresh Job List**. This should display any new scan jobs that may have completed while the connector is running.