Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for VMware Web Services

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for VMware Web Services

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
08/15/2017	Updated guide to show added support for ESXi server and vCenter 6.5. Replaced 'connectorsetup' command with 'runagentsetup'. Support ended for vCenter versions 2.5, 3.5, 4.0, and 5.0 and ESX/ESXi servers 3.0, 4.0, and 5.0 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
06/30/2016	Updated guide to show added support for ESXi and vCenter 6.0, which was added with the 7.1.6 connector release.
11/14/2014	Added permission access note.
06/30/2014	Added support for ESX/ESXi Server v5.5.
02/14/2014	Updated parameter screen image.
06/28/2013	Added mappings for Device Custom String 6 and Source Address.
03/29/2013	Added import certificate information to installation procedure.

SmartConnector for VMware Web Services

This guide provides information for installing the SmartConnector for VMware Web Services and configuring the device for event collection. VMware Web Services vCenter versions 5.5, 6.0, and 6.5 are supported on ESXi servers 5.5, 6.0, and 6.5 respectively.

Product Overview

The VMware vSphere API provides an infrastructure for managing and monitoring VMware vSphere components (such as virtual machines and host systems) and subsystems (such as performance managers). The API has been implemented as industry-standard Web services, hosted on VMware vSphere systems, including ESXi and vCenter systems.

In vSphere there are Event Managed Objects, Task Managed Objects, and other types. Currently, the SmartConnector can access only Event Managed Objects. (An Event is a data object that conveys information about changes in the state of managed entities such as login, logout, VM power on/off, start/stopping, rename').

The ArcSight SmartConnector acts as a Web Service Client using VMware vSphere Web Services SDK to connect and access managed objects on VMware ESXi and vCenter Servers, importing events generated by the VMware Web Services device into the ArcSight System.

Obtain Server Certificates

The information in this section has been derived from the VMware vSphere Web Services SDK information in VMware's *Developer's Setup Guide*. See the relevant guide for your version for complete information about obtaining server certificates.

The server certificates are created automatically during the process of installing VMware products, including ESXi and vCenter Server systems. Because these certificates are not signed by an official root CA, you must obtain the server certificate from each server that you plan to target by the SmartConnector and store it locally.

For example, if you are creating a client application to run against the vCenter Server and an ESXi system directly (in standalone mode), obtain both the vCenter Server certificate and the ESXi certificate. If your application is aimed solely at the vCenter Server that might manage any number of ESXi systems, obtain the certificate only from the vCenter Server.

You can obtain the certificates in one of two general ways:

- Users working on the Microsoft Windows platform can use the certificate-handling capabilities of the vSphere Client from the development workstation to connect to each vCenter Server, accept the certificate into the local cache, and export the certificate. See "Obtaining Certificates using the vSphere Client."

Users with access privileges on the target server systems can use a secure shell client utility (SCP, WinSCP, or SSH) to connect directly to the vCenter Server and copy the certificates directly from the server to the client (connector) machine. See "Obtaining Certificates by Connecting Directly to Server Systems" for details.

Obtain Certificates using the vSphere Client

This approach requires you to install the vSphere Client on your development machine. The vSphere Client leverages the native Microsoft credential-handling mechanisms to allow you to accept the certificate and export it as a local file.

To obtain server certificates using vSphere Client:

1. Create a directory named `VMware-Certs` (at the root level) for the certificates. Several of the vSphere Web Services SDK batch files assume this path as the location of the keystore and fail if you do not use this path.

   ```
   C:\VMware-Certs
   ```

2. Install the vSphere Client on the development workstation if necessary.

3. Launch the vSphere Client and then navigate to the ESXi or vCenter Server web server. A security warning message box displays regarding the certifying authority for the certificate.

4. Click **View Certificate** to display the Certificate properties page.

5. Click the **Details** tab.

6. Click **Copy to File...** to launch the Certificate Export wizard.

7. Select **DER encoded binary X.509** (the default) and click **Next**.

8. Click **Browse...** and navigate to the `C:\VMware-Certs` subdirectory.

9. Enter a name for the certificate that identifies the server to which it belongs.

   ```
   C:\VMware-Certs\<servername>.cer
   ```

You will import this certificate during the SmartConnector installation and configuration process.

Obtain Certificates by Connecting Directly to Server Systems

This approach is for users who have appropriate privileges to directly connect to the target server. These instructions require administrative privileges on the ESXi or vCenter Server, and assume that you can access the necessary subdirectory.

To obtain server certificates using secure shell client application:

1. From the development workstation, create a directory in which to store certificates of servers from which the connector will pull events.

   ```
   ~\vmware-certs\
   ```

2. Connect to the ESXi system using an SSL client from the development workstation. Remote connections to the ESXi server console as root are effectively disabled, so you must connect as another user with privileges on the server to obtain the certificate. The server certificate filename and location of the vCenter Server is:

```
C:\Documents and Settings\All Users\Application Data\VMware\VMware
VirtualCenter\SSL\rui.crt
```

For Windows Server 2008:

```
C:\Users\All Users\Application Data\VMware Virtual Center\SSL\rui.crt
```

In newer Windows versions, select `Run...` to open a Command window and enter `%appdata%\VMware Virtual Center\SSL\rui.crt`.

For ESXi Server:

```
/etc/vmware/ssl/rui.cert
```

3 Copy the certificate or certificates from the server to the certificate subdirectory of the development workstation, using a unique filename for each certificate.

You will import the certificate or certificates during the SmartConnector installation and configuration process.

The account you use to install the connector must have the appropriate permissions to access VMware Web Services. See the VMware documentation for more information.

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.

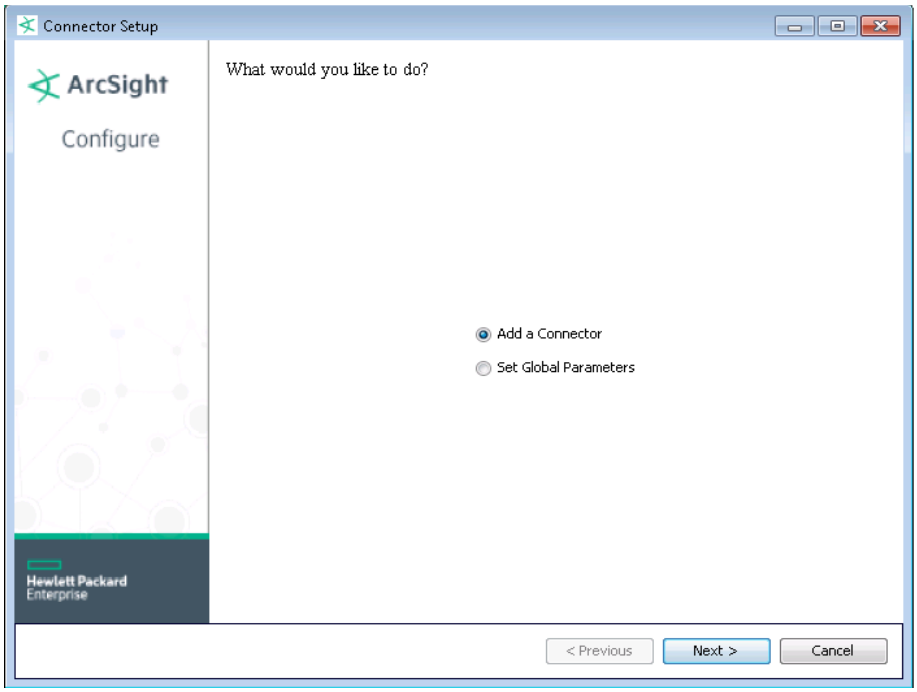
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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:



The following steps are for importing the device certificate to the connector's local Java Runtime Environment. If you are not using certificate verification, you can skip this step and continue with step 4.

This example is for Windows systems; if you are using Linux or Solaris, change the command to reflect your $ARCSIGHT_HOME and change backslash (\) to forward slash (/).

A Click **Cancel** to exit the wizard at this point.

B Contact VMware for instructions on exporting the authentication certificate. Copy this certificate file to `$ARCSIGHT_HOME\current\jre\lib\security\`.

For vCenter 5.x for example, the certificate file could be located at:

```
C:\Documents and Settings\All Users\Application Data\VMware Virtual
Center\SSL\rui.crt
```

For Windows Server 2008:

```
C:\Users\All Users\Application Data\VMware Virtual Center\ssl\rui.crt
```

In newer Windows versions, select `Run...` to open a Command window and enter `%appdata%\VMware Virtual Center\SSL\rui.crt`.

For ESXi Server:

```
/etc/vmware/ssl/rui.crt
```

C From `$ARCSIGHT_HOME\current\bin\` for Windows or from `$ARCSIGHT_HOME/current/bin` for Linux, execute the **keytool** application to import the certificate. Enter this command on a single line.

```
arcsight agent keytool -import -file rui.crt -alias vmware -keystore
cacerts -store clientcerts
```

where `<rui.crt>` is the actual name of the certificate file. This parameter can be a pathname such as `C:\vmware_certs\my_vcenter.cert`. When queried for the keystore password, enter `changeit`.

D Following the prompts, answer **yes** for the prompt **Do you still want to add it?**

E Be sure to import certificates for each VMware server instance.

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

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

The new certificate is displayed in the list.

G 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:

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'.
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.

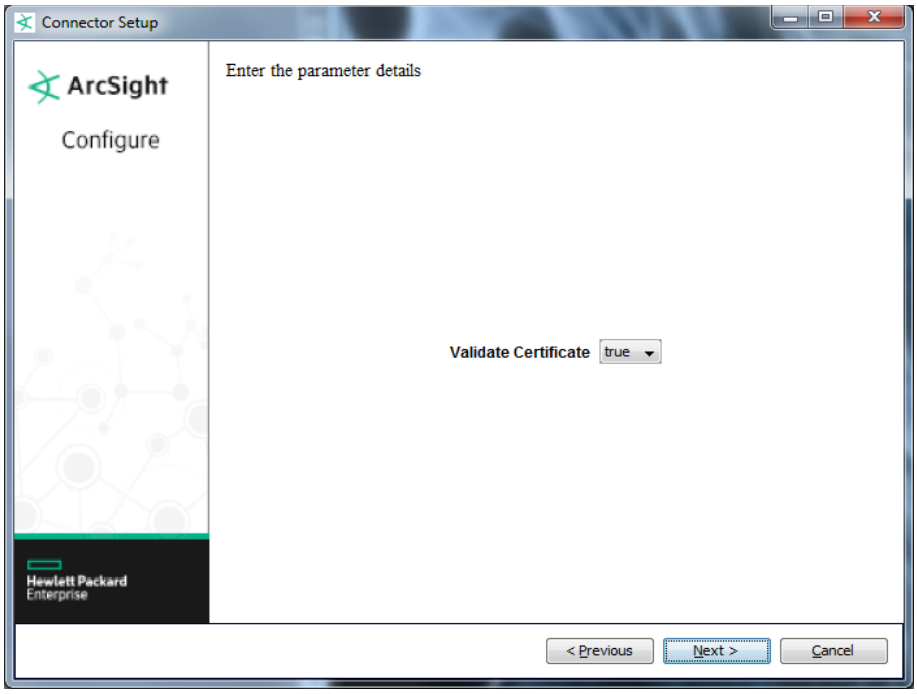
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

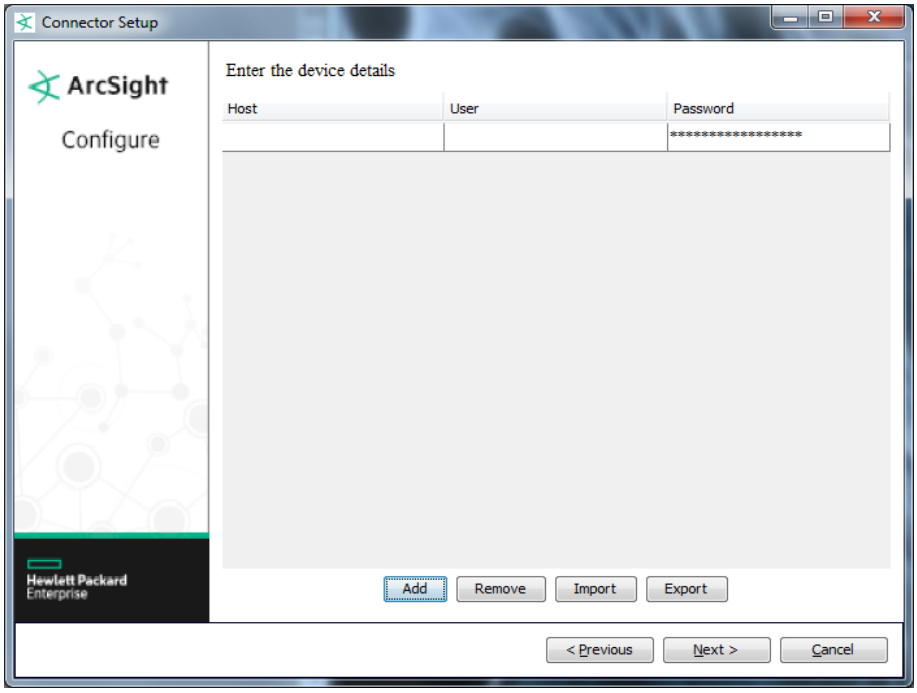
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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 **VMware Web Services** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.





Parameter	Description
Validate Certificate	Select 'true' for certificate validation to take place; select 'false' if the certificate is not to be validated.
Host	Host name or IP address of the VMware Web Services device.

Parameter	Description
User	User name for accessing VMware Web Services.
Password	Password for the VMware Web Services user.

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.

VMware Web Services Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Destination Host Name	One of (Host, Server)
Destination User Name	UserName
Device Custom String 2	Ds (Datastore)
Device Custom String 3	ComputeResource (Compute Resource)
Device Custom String 4	Datacenter
Device Custom String 5	VmName (VM Name)
Device Event Class ID	Name
Device Host Name	Server
Device Product	Product
Device Receipt Time	CreateTime
Device Vendor	'VMware'
Device Version	Product
Message	Message
Name	Name
Source Address	User logged in