



ArcSight SmartConnector

Software Version: CE 24.4

Configuration Guide for VMware Web Services SmartConnector

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2024 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 VMware Web Services SmartConnector 4
- Product overview 5
- Configuration 6
 - Obtaining the server certificates 6
 - Downloading the server certificates using the vSphere Client 7
 - Copying the certificates directly from the server to the development platform 7
- Installing the SmartConnector 9
 - Preparing to install the SmartConnector 9
 - Installing and configuring the SmartConnector 9
- Device event mapping to ArcSight fields13
 - VMware Web Services mappings to ArcSight ESM events13
- Send Documentation Feedback 14

Configuration Guide for VMware Web Services SmartConnector

This guide provides information for installing the SmartConnector for VMware Web Services and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

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](#).

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

The VMware vSphere API provides an infrastructure to manage and monitor VMware vSphere components, including virtual machines and host systems, and subsystems such as performance managers. The API is 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.

The VMware Web Services 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. It imports events generated by the VMware Web Services device into the ArcSight.

Configuration

OpenText recommends that you validate the VMware server certificate while installing the VMware Web Services SmartConnector to make sure that your application uses HTTPS connection. For more information about when to bypass certificate validation and the associated risks, see *VMware vSphere Web Services SDK Developer's Setup Guide*.

To encrypt session information sent over SSL connections, VMware products use the standard X.509 version 3 (X.509v3) certificates.

vSphere components, including ESXi and vCenter Server systems, create server certificates automatically during their installation process. However, these certificates are not signed by an official root certificate authority (CA). You must get the server certificate from each server that your client application targets and store it on your local machine.

For instance, if your client application runs against the vCenter Server and an ESX system in standalone mode, you must get the server certificate from both vCenter Server and ESX system. If your application is aimed only at the vCenter Server that manages multiple ESX systems, then you need to get the server certificate only from the vCenter Server.

Obtaining the server certificates

You can obtain the server certificates through one of the following ways:

- **If you are working on the Microsoft Windows platform:** Connect to each vCenter Server using the certificate-handling capabilities of the vSphere Client from the development workstation and accept the certificate into the local cache and export the certificate.
- **If you are having access privileges on the target server systems:** Connect directly to the vCenter Server using a secure shell client utility (SCP, WinSCP, or SSH) and copy the certificates directly from the server to the development platform.

For more information, see *VMware vSphere Web Services SDK Developer's Setup Guide*.

Downloading the server certificates using the vSphere Client

If you are using vSphere Client to get the certificates, you do not have to install another client on your development workstation.

To download the server certificates using vSphere Client:

1. Open a web browser and go to the URL of the vCenter Server instance.
`https://my-vc-name.example.com`
2. Click the **Download trusted root CA certificates** link to download a ZIP file of all the root certificates and all the CRLs in the VMware Endpoint Certificate Store (VECS).
3. Extract the ZIP file.

The .certs folder contains two types of files.

- Files with a number as the extension are root certificates. For example, .0, .1, and so on.
 - Files with an extension that starts with an r are CRL files associated with a certificate. For example, .r0, .r1, and so on.
4. Install the certificate files as trusted certificates by following the process that is appropriate for your operating system.

For more information, see *VMware vSphere Web Services SDK Developer's Setup Guide*.

You will import the required server certificates during the SmartConnector installation and configuration process.

Copying the certificates directly from the server to the development platform

Use this method if you have the privileges to directly connect to the target server system.

Prerequisite:

Administrative privileges on the ESXi or VCenter Server and must be able to access the necessary subdirectories.

To copy the server certificates directly from the server:

1. Create a directory in the development workstation to store the server certificates, 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 get the certificate.

3. The following table shows the path of the server certificate for different vSphere components such as vCenter Server and ESXi:

vSphere components	Server certificate path
vCenter Server	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 type %appdata%\VMware Virtual Center\SSL\rui.crt.
ESXi	/etc/vmware/ssl/rui.cert

4. 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 required server certificates during the SmartConnector installation and configuration process.

Installing the SmartConnector

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

Preparing to install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

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



The account that you use to install the connector must have the appropriate permissions to access VMware Web Services. For more information, see the VMware documentation.

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. If you are not going to validate the certificate, you can skip the following certificate import procedure and continue with step 4. However, bypassing certificate validation is not recommended in a production environment.

To import the device certificate to the connector's local Java Runtime Environment:



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. Copy the server certificate file to \$ARCSIGHT_HOME\current\jre\lib\security\.

For more information about obtaining the server certificate, see the [Obtaining the server certificate](#) section.

- c. From \$ARCSIGHT_HOME\current\bin\ on Windows or from \$ARCSIGHT_HOME/current/bin on Linux, execute the **keytool** application to import the certificate. Enter the following command on a single line:

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

where <rui.crt> is the 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. Make sure to import the 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.
4. Specify the relevant [Global Parameters](#), when prompted.
 5. In the **Type** list, select **VMware Web Services**, then click **Next**.
 6. In the **Enter the parameter details** page, select the required value for the following parameter, and then click **Next**:

Parameter	Description
Validate Certificate	Validates the VMware server certificate. Select True or False : where True : The connector will validate the VMware server certificate. False : The connector will not validate the VMware server certificate. The default value is True .

7. In the **Enter the device details** page, add the following details, and then click **Next**:



This step is optional if you are using certificate verification. However, it is mandatory if you are connecting to a VMware server with no certificate.

Device detail	Description
Host	Host name or the IP address of the vCenter Server or the ESXi host to which you want to connect. For example: <ul style="list-style-type: none">• Host name: vcenter.example.com• IP Address: 192.168.1.100
User	User name of an account with sufficient permissions to automate the required operations. This account is typically of an administrative user in the vSphere environment. For example: <ul style="list-style-type: none">• User name: administrator@vsphere.local• User name: root (if connecting directly to an ESXi host)
Password	Password for the user account specified in the User box.

8. Select a [destination and configure parameters](#).
9. Specify a name for the connector.
10. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



If you select **Do not import the certificate to connector from destination**, the connector installation will end.

11. Select whether you want to install the connector as a service or in the standalone mode.

12. Complete the installation.

13. [Run the SmartConnector.](#)

For more information about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector.](#)

Device event mapping to ArcSight fields

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

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

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 VMware Web Services SmartConnector
(SmartConnector CE 24.4)**

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!