



ArcSight SmartConnector

Software Version: CE 24.3

Configuration Guide for VMware Web Services SmartConnector

Document Release Date: July 2024

Software Release Date: July 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
- Obtain Server Certificates 6
 - Obtain Certificates using the vSphere Client 6
 - Obtain Certificates by Connecting Directly to Server Systems 7
- Installing the SmartConnector 9
 - Preparing to Install the SmartConnector 9
 - Installing and Configuring the SmartConnector 9
- Device Event Mapping to ArcSight Fields12
 - VMware Web Services Mappings to ArcSight ESM Events12
- Send Documentation Feedback 13

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 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.

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

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 using certificate verification, you can skip this certificate import step and continue with step 4.

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

The following table shows the location of the certificate file for different servers:

Server	Certificate location
vCenter 5.x	C:\Documents and Settings\All Users\Application Data\VMware Virtual Center\SSL\rui.crt
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.
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 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 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. Make 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.
4. Specify the relevant [Global Parameters](#), when prompted.
5. In the **Type** drop-down, 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	<p>Validates the VMware server certificate.</p> <p>Select True or False:</p> <p>where</p> <p>True: The connector will validate the VMware server certificate.</p> <p>False: The connector will not validate the VMware server certificate.</p> <p>The default value is True.</p>

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

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.



Note: 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 instructions 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. 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

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 VMware Web Services SmartConnector
(SmartConnector CE 24.3)**

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!