Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Symantec AntiVirus Corporate Edition File and Multiple File

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Symantec AntiVirus Corporate Edition File and Multiple File

October 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
05/15/2011	Corrected copyright dates.
03/30/2011	Corrected path for default log location.
09/24/2010	Updated versions supported.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure.
02/11/2009	Updated field mappings.

SmartConnector for Symantec AntiVirus Corporate Edition File and Multiple File

This guide provides information for installing the SmartConnectors for Symantec AntiVirus Corporate Edition File and Symantec AntiVirus Corporate Edition Multiple File and configuring the device for log file event collection. Symantec AntiVirus Corporate Edition versions 8.0, 9.0, and 10.0 are supported.

Product Overview

Symantec AntiVirus Corporate Edition combines real-time malware protection for enterprise workstations and network servers with graphical Web-based reporting and centralized management and administration capabilities.

Configuration

For complete information about configuring Symantec AntiVirus Corporate Edition for event logging, see "Working with Histories and Event Logs" in the *Symantec AntiVirus Administrator's Guide* and "Configuring Alerts" in the *Symantec Reporting User's Guide*.

By default, the Symantec AntiVirus log files are located at `x:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs` .

Configure Log Events to Forward

You can configure the events that are forwarded from a client to its parent management server, or from a secondary management server to its primary management server.

If you change primary management servers, the log from the former primary management server is not forwarded to the new primary management server.

To configure events to forward from clients to their parent management servers:

1. In the **Symantec System Center** console, right-click a server, server group, or client, and then click **All Tasks -> Symantec AntiVirus -> Logs -> Client Log Forwarding**.
2. In the **Log Event Forwarding** dialog box, for quicker configuration, you can display only certain items in the list by selecting one of the following preconfigured options from the drop-down list:
   - All events (default)
   - Scanning and infection events
   - Virus definition events
   - Management and configuration events
   - Startup and shutdown events

- Licensing events
- Security related events

3 Check the events that you want the clients to forward to their parent management servers.

4 Click **OK**.

To configure events to forward from secondary management servers to their primary management servers:

1 In the Symantec System Center console, right-click a server or server group, and then click **All Tasks -> Symantec AntiVirus -> Logs -> Server Log Forwarding**.

2 In the **Log Event Forwarding** dialog box, for quicker configuration, you can display only certain items in the list by selecting one of the following preconfigured options from the drop-down list:

- All events (default)
- Scanning and infection events
- Virus definition events
- Management and configuration events
- Startup and shutdown events
- Licensing events
- Security related events

3 Check the events that you want the secondary management servers to forward to their primary management server.

4 Click **OK**.

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.

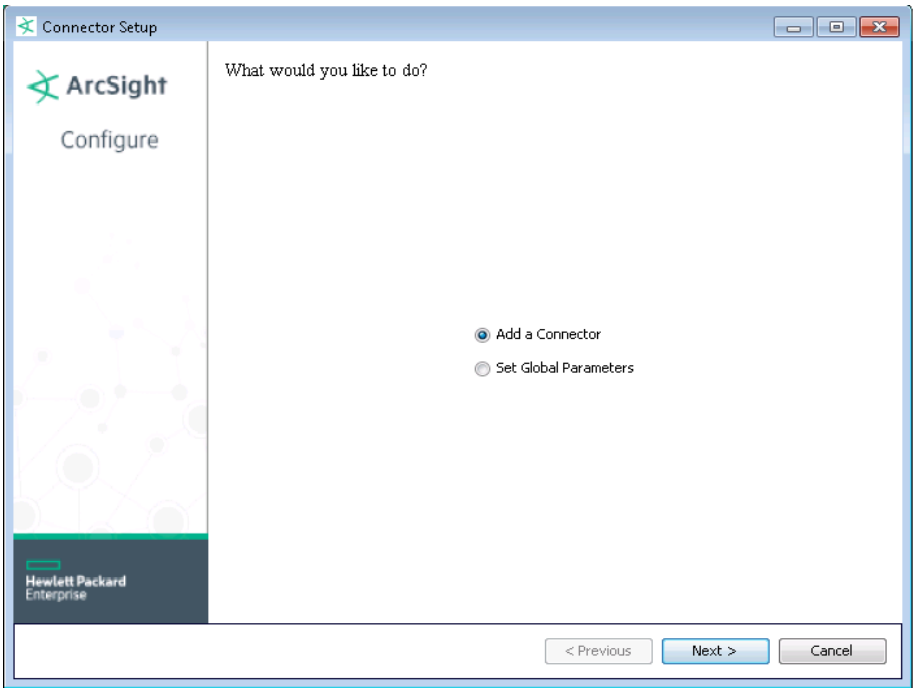
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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'.
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.

Parameter	Setting
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.

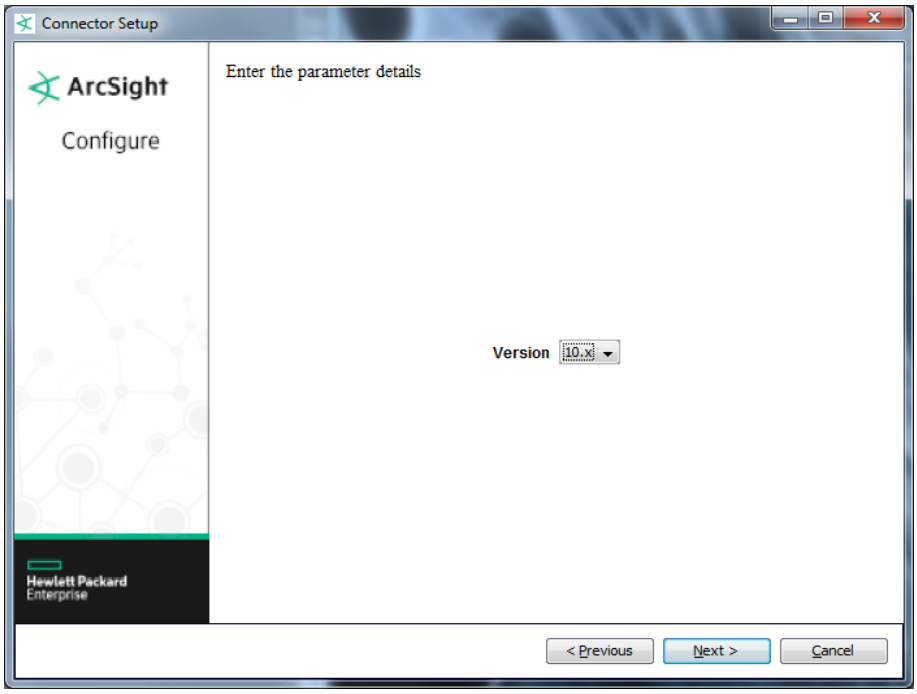
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

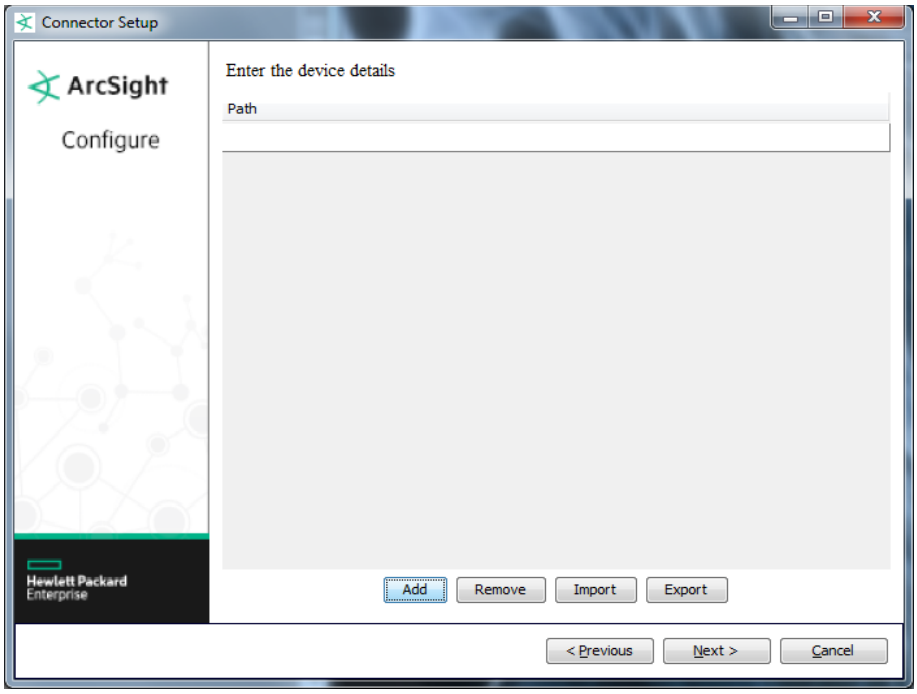
Select Connector and Add Parameter Information

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 **Symantec AntiVirus Corporate Edition File | Symantec AntiVirus Corporate Edition Multiple File** and click **Next**.

3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.





Parameter	Description
Version	Select the appropriate version number for the Symantec Corporate Edition server: 8.0, 9.0, or 10.0. The default value is 8.0. Be aware that this connector is designed to process log files of only one version. To process logs from different versions requires deploying different connectors for the different versions.
Log File or Path	The absolute path (drive and directory) of Symantec AntiVirus log files in daily rotation mode (by default) or the absolute file name in non-rotation mode. The SmartConnector automatically selects the current log file based upon the date included in the filename. By default, Symantec AntiVirus log files are located at: 'x:Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs'

For the Multiple File connector, select the product version, click 'Next', and then enter the path for each log file to be monitored. For the single file connector, select the version and enter the absolute path on one screen. The images are from the installation of the multiple file connector. You can click the 'Export' button to export the host name data you have entered into the able 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.

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.

Symantec AntiVirus Corporate Edition Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	FileDeletable (4 = VEDELETABLE, 5 = VENOTDELETABLE)
Additional data	FileCleanable (0 = VECLEANABLE, 1 = VENOCLEANPATTERN, 2 = VENOTCLEANABLE)
Additional data	ServerGroup
ArcSight Severity	High when Device Severity = GL_CAT_INFECTION; Medium when Device Severity = GL_CAT_SECURITY; Low when Device Severity = GL_CAT_SUMMARY or GL_CAT_PATTERN
Destination Address	IpAddress
Destination Host Name	Computer
Destination Mac Address	HardwareAddress
Destination NT Domain	WindowsDomainOrWorkgroup
Destination User ID	UserName
Destination User Name	UserName
Device Action	Taken Action (One of 0=Intrusion detected and blocked, 1=Quarantined, 2=Renamed, 3=Deleted, 4=Left alone, 5=Cleaned, 6=Cleaned or macros deleted, 7=Saved file as, 8=Sent to Intel, 9=Moved to backup location, 10=Renamed backup file, 11=Undo action in Quarantine View, 12=Write protected or lack of permissions - Unable to act on file, 13=Backed up file, 14=Pending analysis, 15=First action- partially successful second action- Leave Alone, 16=A process needs to be terminated to remove a risk, 17=Prevent logging of a risk or display of an user interface, 18=Performing a request to restart the computer, 19=The only way to clean the file is to delete it, 20=Auto-Protect prevented a file creation; reported Access denied)
Device Custom Number 1	PrimaryAction
Device Custom Number 2	SecondaryAction
Device Custom Number 3	FileStillInfected
Device Custom String 1	VirusName
Device Custom String 2	VirusType
Device Custom String 3	ClientGroup
Device Custom String 4	ScanResults or ResultOfScan
Device Custom String 5	QuarantineStatus (0 = QF_NONE, 1 = QF_FAILED, 2 = QF_OK)
Device Custom String 6	VirusDefVersion
Device Event Class ID	EventNumber
Device Facility	TakenAction
Device Host Name	ClientParentName
Device Product	'AntiVirus Corporate Edition'
Device Receipt Time	HexEncodedTime
Device Receipt Time	HexEncodedTime
Device Severity	Category (1 = GL_CAT_INFECTION, 2 = GL_CAT_SUMMARY, 3 = GL_CAT_PATTERN, 4 = GL_CAT_SECURITY)
Device Vendor	'Symantec'
Device Version	SoftwareVersion
Event Category	Category (1=GL_CAT_INFECTION, 2=GL_CAT_SUMMARY, 3=GL_CAT_PATTERN, 4=GL_CAT_SECURITY)

ArcSight ESM Field	Device-Specific Field
Event Name	EventNumber (1=Alert, 2=Scan Stopped, 3=Scan Started, 4=PATTERN UPDATE, 5=INFECTION, 6=Scan Omission, 7=LOAD PATTERN, 10=Checksum, 11=TRAP, 12=Configuration Changed, 13=Symantec AntiVirus Shutdown, 14=Symantec AntiVirus Startup, 16=Definition File Download, 17=TOO MANY VIRUSES, 18=Sent To Quarantine Server, 19=Delivered To Symantec Security Response, 20=Backup Restore Error, 21=Scan Aborted, 22=Symantec AntiVirus Auto-Protect Load Error, 23=Symantec AntiVirus Auto-Protect Loaded, 24=Symantec AntiVirus Auto-Protect Unloaded, 25=Removed Client, 26=Scan Delayed, 27=Scan Re-started, 28=Roaming Client added to Server, 29=Roaming Client deleted from Server, 30=License Warning, 31=License Error, 32=LICENSE GRACE, 33=Access Denied Warning, 34=Log Forwarding Error, 35=License Installed, 36=License Allocated, 37=License Ok, 38=License Deallocated, 39=Bad Definitions Rollback, 40=Bad Definitions Unprotected, 41=SAV Provider Parsing Error, 42=RTS Error, 43=Compliancy Fail, 44=Compliancy Success, 45=Symantec Security Policy Violation, 46=Anomaly Start, 47=Detection Action Taken, 48=Remediation Action Pending, 49=Remediation Action Failed, 50=Remediation Action Success, 51=Anomaly Finish, 52=Login Failed, 53=Login Succeeded, 54=Unauthorized Communications, 55=Antivirus Client Installation, 56=Firewall Client Installation, 57=Client Software Uninstalled, 58=Client Software Uninstall Rollback, 59=Server Group Root Certificate Issued, 60=Server Certificate Issued, 61=Trusted Root Change, 62=Server Certificate Startup Failed, 63=Client Checkin, 64=No Client Checkin, 65=Scan Suspended, 66=Scan Resumed, 67=Scan Duration insufficient, 68=Client Move, 69=Scan Failed Enhanced, 70=Max Event Number, 472000=Implicit block rule blocked, 472001=Configuration - change / startup /shutdown, 472003=Policy update event, 472004=Intrusion detection is monitoring, 492000=Firewall Violation, 492001=Intrusion attempted, 8=8, 9=9, 15=15, 32=32, 35=35, 492002=492002
External ID	ScanIDNumber
File Name	VirusLocation
Source Address	RemoteComputerIP
Source Host Name	Computer or RemoteComputerName