



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for the F-Secure Anti-Virus File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2022-2023 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 the F-Secure Anti-Virus File SmartConnector 4
- Product Overview 5
- Configuration 6
- Installing the SmartConnector 7
 - Preparing to Install the SmartConnector 7
 - Installing the SmartConnector 7
- Device Event Mapping to ArcSight Fields 9
 - F-Secure Mappings to ArcSight ESM Fields 9
- Send Documentation Feedback 10

Configuration Guide for the F-Secure Anti-Virus File SmartConnector

This guide provides information for installing the SmartConnector for F-Secure Anti-Virus File and configuring the device for event collection.

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 8.4](#).

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

F-Secure Policy Manager offers an easy and scalable way to deploy security applications, define and deploy security policies, and monitor security to ensure compliance with corporate security policies. Policy Manager provides a centralized management console for the security of the managed hosts in the network.

Configuration

F-Secure Policy Manager Console logs messages in the **Message** pane about different events in Information, Warnings, and Error categories. Each **Message** pane tab can contain messages of all three severity.

You can delete a category in the displayed context menu. Right-click an individual message to cut, copy, and delete operations.

By default, messages are logged into UTF-8 files in the message subdirectory of the local F-Secure Policy Manager Console installation directory.

A separate log file is created for each message category. You can use the **Preferences-Locations** page to specify the directory for the log file and to switch logging on and off.

Installing 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.

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 the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Select **F-Secure Anti-Virus File** from the Type drop-down, then click **Next**.

5. For **Trap Files Base Folder**, specify the absolute path to the directory in which the log files are located, then click **Next**.



Note: Mapped network drives must not be used in a Windows environment. When Windows executes a process as a service, an entirely new "virtual" environment is created. As a result, any drives you have mapped as a user must be re-mapped to be recognized by the SmartConnector.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (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.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [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.

F-Secure Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Action	Action taken by the device
Device Custom Number 1	Checked by Admin
Device Custom Number 2	Trap Count
Device Custom String 1	Param1
Device Custom String 2	Param0
Device Custom String 3	Param2
Device Custom String 4	Message
Device Event Class Id	Trap Number
Device Product	F-Secure Anti-Virus
Device Receipt Time	Time Stamp
Device Severity	Severity (5 = High, 4 and 3 = Medium, 1 and 2 = Low)
Device Vendor	F-Secure
Message	Trap description
Name	Trap name
Target Host Name	Host Name
Target User Name	User ID

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 the F-Secure Anti-Virus File SmartConnector (SmartConnectors 8.4.3)

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!