



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for SAINT Vulnerability Scanner**

### **Configuration Guide**

**June, 2018**

## Configuration Guide

### SmartConnector for SAINT Vulnerability Scanner

June, 2018

Copyright © 2007 – 2017; 2018 Micro Focus and its affiliates and licensors.

### Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated. Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

## 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.
06/30/2016	Added Device Event Class ID and severity mappings for Open Ports; added Device Event Class ID mapping for URIs.
05/15/2012	Added new installation procedure.
09/24/2010	Updated supported versions.
02/11/2010	Added support for FIPS Suite B and CEF File transport.

---

## SmartConnector for SAINT Vulnerability Scanner

---

This guide provides information for installing the SmartConnector for SAINT Vulnerability Scanner and configuring the device for scan report event collection. SAINT Vulnerability Scanner versions 6.1 and 6.4 are supported.



The SAINT Vulnerability Scanner product is not supported for installation on Windows platforms.

---

### Product Overview

SAINT is the Security Administrator's Integrated Network Tool, which is used to non-intrusively detect security vulnerabilities on any remote target, including servers, workstations, networking devices, and other types of nodes. It also gathers information such as operating system types and open ports. Reports on complete scan results can be generated and saved through the SAINT graphical user interface.

### Configuration

This section provides instructions for configuring the SAINT Vulnerability Scanner to send reports to the ArcSight SmartConnector. The SAINT SmartConnector supports importing scan reports in XML format (not other files) for single or multiple host scans in an UNIX environment. The SAINT Vulnerability Scanner currently is not installable in the Windows environment.

### Mode for Sending Events

The SAINT Vulnerability Scanner SmartConnector, as other vulnerability scanners, supports two modes of operation:

- **Interactive:** This mode is designed to be used by an operator who requires that only certain reports be sent to ArcSight. In this mode, the SmartConnector first retrieves a list of the scan reports contained in the scanner's database and presents it in a UI window for you to select which scan reports are to be sent to the ArcSight Manager. After your selection, you can click **Send** for all the selected scanner reports to be sent to ArcSight. You can simply close the window when all the desired scans have been sent to ArcSight and the SmartConnector terminates. *In Interactive mode, the SmartConnector should not be run as a service, only as a stand-alone application.*
- **Automatic:** This mode is designed to automatically import the reports from SAINT to the ArcSight Manager whenever a new scan is performed using the SAINT Scanner application. In this mode, the SmartConnector queries the database constantly to check for new completed scans. When the it detects that a new scan has been successfully completed, it sends the scan report to the ArcSight Manager. *The SmartConnector can run as a service in this mode since this mode is designed to run unattended.*

The configuration of the SmartConnector for SmartConnector for SAINT Vulnerability Scanner in automatic mode lets you send SAINT scan reports automatically to ArcSight. To do this, create a shell script that executes a SAINT scan periodically and saves a report in XML format. Once the report is created, create a "triggering" file (can be any file) to indicate that the report can be sent to

ArcSight. This is an empty file with the same name as the original file, but with an extension `xml_done`; for example, for the file `xyz.xml`, you would create `xyz.xml_done`.

In both modes, the SmartConnector records the IDs of the reports that have been sent to the ArcSight Manager; therefore, if you use interactive mode, the list of reports available displays only the reports that are in the database and have not yet been sent to the ArcSight Manager. The same applies for automatic mode; only reports in the database and not yet sent are processed.



To run a scanner connector in interactive mode, the connector must be run in standalone mode and not as a service. Automatic mode, however, can be run either standalone or as a service, although the general preference is to run automatic mode as a service.

---

## 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

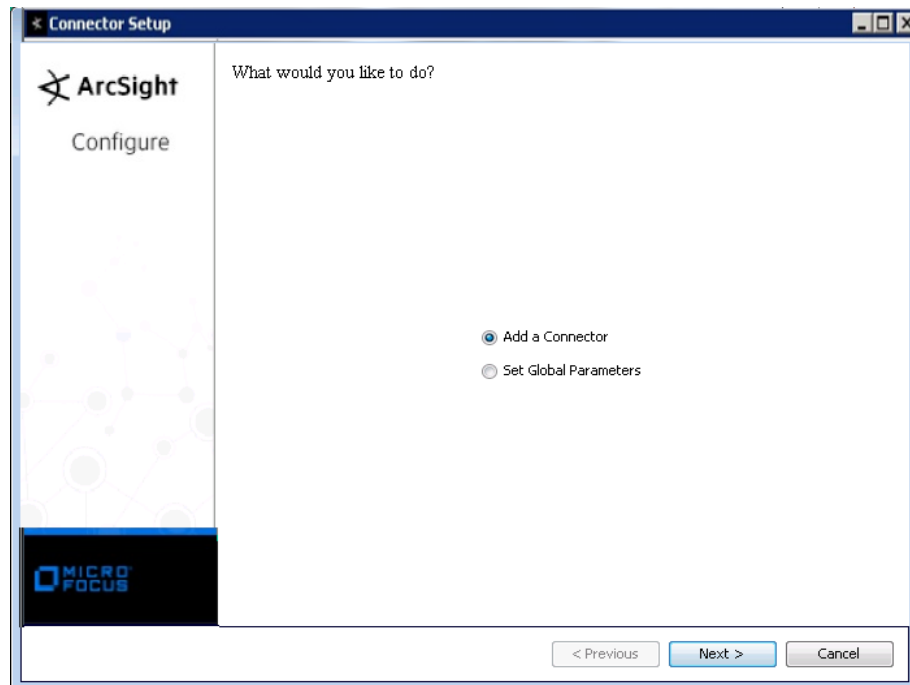
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus 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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

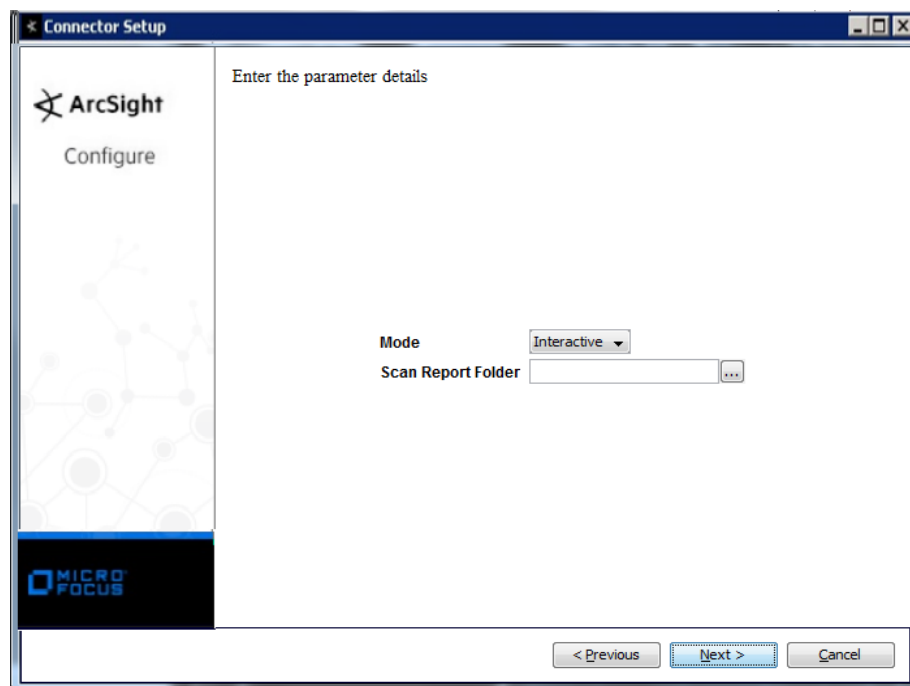
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.

Parameter	Setting
Format Preserving Policy URL	Enter the URL where the Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 **SAINT Vulnerability Scanner File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Mode	Select whether to manually (interactive) or automatically (automatic) send reports to ArcSight. (See details in "Configuration.")
SAINT Report Folder	The folder in which the SAINT scanner reports are located.

## 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.

### SAINT Open Ports Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Service = Low
Application Protocol	Application protocol part of the description field.
Category Technique	VulnerabilityCategory
Destination Address	ipaddr
Destination Host Name	hostname
Destination Port	Port information from the description field.
Destination Service Name	service
Device Event Class ID	Both ('Saint', description)
Device Product	'SAINT Vulnerability Scanner'
Device Receipt Time	scan_time
Device Severity	severity
Device Vendor	'SAINT'
Device Version	scanner_version
Name	'Service' plus description
Transport Protocol	Transport protocol part of the description field.

### SAINT Scanner Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Address	ipaddr
Destination Host Name	hostname

### SAINT URIs Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Category Technique	VulnerabilityCategory
Destination Address	ipaddr
Destination Host Name	hostname



ArcSight ESM Field	Device-Specific Field
Device Event Class ID	Both ('Saint', hosttype)
Device Product	'SAINT Vulnerability Scanner'
Device Receipt Time	scan_time
Device Vendor	'SAINT'
Device Version	scanner_version
File Path	hosttype
Name	'OS:' plus hosttype

## SAINT Vulnerabilities Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
ArcSight (Connector) Severity	critical or Critical Problem = Very High; concern or Area of Concern = High; potential or Potential Problem = Medium; info, service, or Service = Low
Category Technique	VulnerabilityCategory
Destination Address	ipaddr
Destination Host Name	hostname
Device Event Class ID	SAINT ID
Device Product	'SAINT Vulnerability Scanner'
Device Receipt Time	scan_time
Device Severity	severity
Device Vendor	'SAINT'
Device Version	scanner_version
Name	description

## Troubleshooting

When a user kills the SmartConnector in the middle of processing a vulnerability scan XML file, asset population cannot be completed. Restarting the SmartConnector does not resolve this problem. The workaround is to rename the XML file to its original file name, and then restart the SmartConnector.