



Micro Focus Security ArcSight Connectors

SmartConnector for Sun ONE Directory Server File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Sun ONE Directory Server File

June, 2018

Copyright © 2005 – 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.
05/15/2012	Added new installation procedure.
09/24/2010	Updated supported versions; added support for Sun ONE Directory Server versions 6.0, 6.3, and 7.0.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure.
09/25/2008	Added CSV import/export feature to installation parameter section; updated versions supported.

SmartConnector for Sun ONE Directory Server File

This guide provides information for installing the SmartConnector for Sun ONE Directory Server Multiple Server File and the SmartConnector for Sun ONE Directory Server File and configuring the device for event collection. Sun ONE Directory Server versions 5.0, 5.2, 6.0, 6.3, and 7.0 are supported.

Product Overview

Sun ONE Directory Server provides organizations with a single deployment platform for Web services, JavaServer Pages (JSP) and Java Servlet technologies, Microsoft Active Server Pages, PHP, and CGI.

This ArcSight SmartConnector lets you import events generated by the SmartConnector for Sun ONE Directory Server File device into the ArcSight System. See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

Configuring Sun ONE Directory Server to Send Events

The Sun ONE Directory Server provides three types of logs: Access, Errors, and Audit. The ArcSight SmartConnector processes the Access and Errors Logs (the Audit Log is not processed).

Configure the Access Log

To configure the access log for your directory:

- 1 On the top-level **Configuration** tab of the Server console, select the **Logs** icon, then select the **Access Log** tab.
- 2 If not already selected, check the **Enable Logging** checkbox to enable Access logging. (Access logging is enabled by default.)
- 3 In the **Log File** field, enter the full path and filename you want the directory to use for the Access log. This information will be needed when you install the SmartConnector. The default file is:

ServerRootslapd-serverID/logs/access

- 4 Set the maximum number of logs, log size and frequency, and Deletion Policy parameters.
- 5 When you finish making changes, click **Save**.

Configure the Errors Log

To configure the Errors log:

- 1 On the top-level **Configuration** tab of the Server console, select the **Logs** icon, then select the **Errors Log** tab.
- 2 If not already selected, check the **Enable Logging** checkbox to enable access logging. (Error logging is enabled by default.)
- 3 In the **Log File** field, enter the full path and filename you want the directory to use for the Errors log. This information will be needed when you install the SmartConnector. The default file is:

ServerRootslapd-serverID/logs/error

- 4 Set the maximum number of logs, log size and frequency, and Deletion Policy parameters.
- 5 When you finish making changes, click **Save**.

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

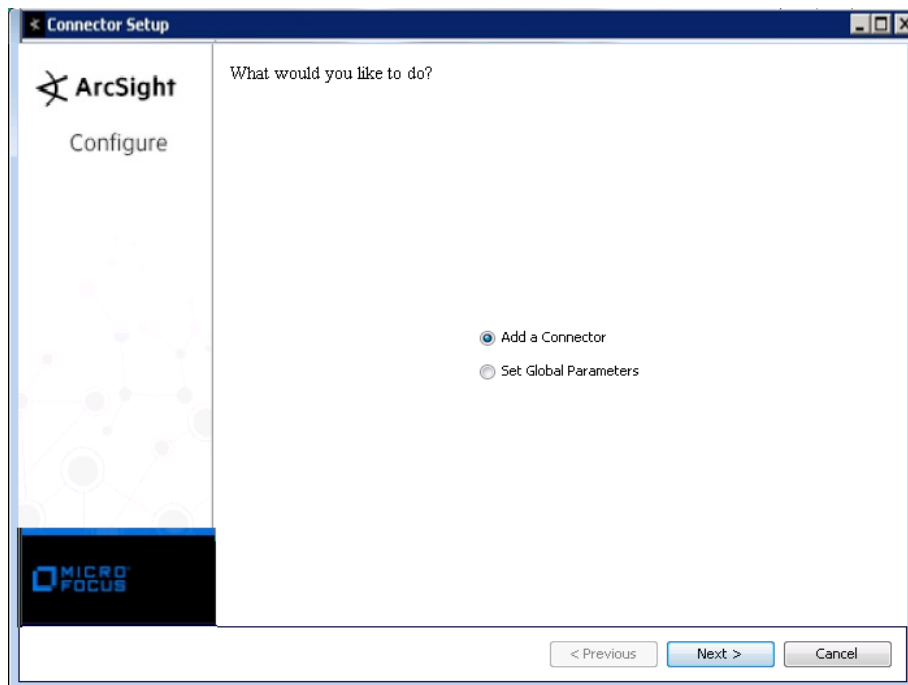
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 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.

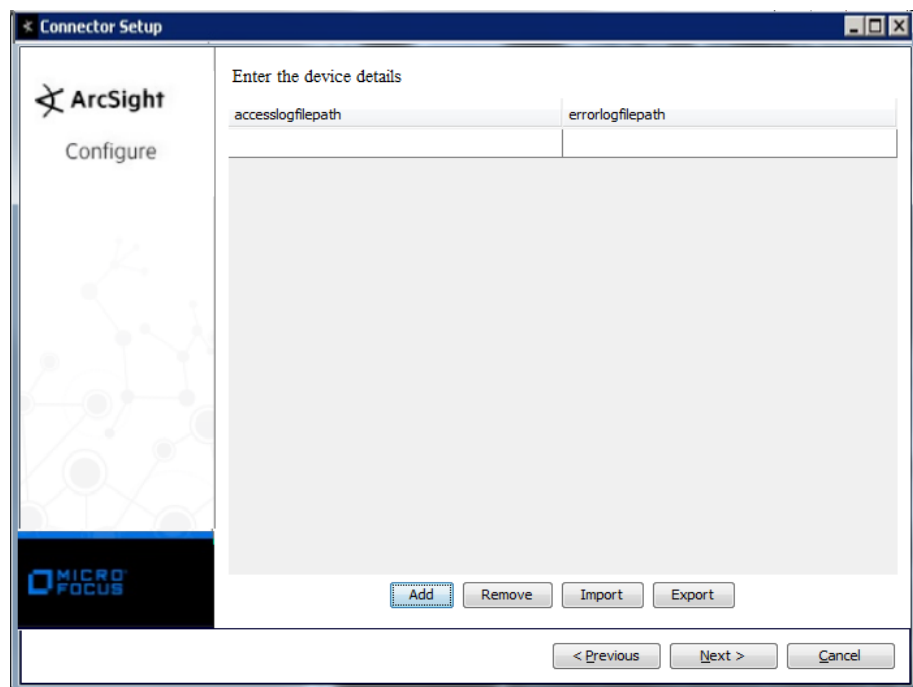
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
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 **Sun ONE Directory Server File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

The screenshot shows the 'Connector Setup' window for ArcSight. The window has a title bar with '< Connector Setup' and standard window controls. On the left is a sidebar with the ArcSight logo and the word 'Configure'. The main area is titled 'Enter the parameter details' and contains two text input fields: 'Access Log File Path' and 'Error Log File Path', each followed by a browse button (three dots). At the bottom of the window are three buttons: '< Previous', 'Next >' (highlighted with a dashed border), and 'Cancel'.



Parameter	Description
	For the Multiple Folder connector, enter parameter information in the table for each directory you will be monitoring.
Access Log File Path	Complete path and name of the directory containing the Access log files. See "Configuring the Access Log" for more information.
Errors Log File Path	Complete path and name of the directory containing the Errors log files. See "Configuring the Errors Log" for more information.

You can click the 'Export' button to export the host name data you have entered into the table 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.

Sun ONE Directory Server Access Log Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	attrs
Additional data	base
Additional data	encryptionMethod
Additional data	errorID
Additional data	etime
Additional data	filter
Additional data	mech
Additional data	oid
Additional data	op
Additional data	remlog
Additional data	scope
Agent (Connector) Severity	ERROR = High; WARNING = Medium; INFO, DEBUG = Low
Application Protocol	LDAP or HTTP (dependent upon event)
Bytes Out	Bytes transferred
Destination Address	dependent upon event
Destination Port	port to which event was sent
Destination User Name	dependent upon event
Device Action	Server action, dependent upon event
Device Custom Number 1	conn (Connection Number)
Device Custom Number 2	fd (File Descriptor)
Device Custom Number 3	Error Code
Device Custom String 1	DN
Device Custom String 2	Bind Method
Device Custom String 3	Request ID
Device Custom String 4	Tag
Device Custom String 5	Connection Code
Device Custom String 6	number of entries in directory
Device Event Category	recordType
Device Event Class ID	Status code
Device Product	'Sun ONE Directory Server'
Device Receipt Time	timestamp
Device Severity	'INFO'
Device Time Zone	zone indicated by the timestamp offset
Device Vendor	'Sun'
Message	LDAP error or status code
Name	dependent upon event

ArcSight ESM Field	Device-Specific Field
Request Method	HTTP request type
Request URL	URL
Source Address	Host IP address
Source Host Name	Host Name or IP address
Source Port	port from which event received

Sun ONE Directory Server Error Log Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	access_allow
Additional data	account_dn
Additional data	aci_index
Additional data	aciIndex
Additional data	acl_elevel
Additional data	acl_index
Additional data	acl_version
Additional data	allow_handles
Additional data	attrs
Additional data	backend
Additional data	base
Additional data	block_type
Additional data	calledAt
Additional data	code
Additional data	conns
Additional data	context
Additional data	container
Additional data	csn
Additional data	current_entry
Additional data	current_state
Additional data	deciding_aci
Additional data	deny_handles
Additional data	deref
Additional data	deviceCustomString1
Additional data	event-id
Additional data	filter
Additional data	index
Additional data	indexmask
Additional data	indextype
Additional data	ldap_attr
Additional data	line
Additional data	lpd
Additional data	matched_value
Additional data	maxconns

ArcSight ESM Field	Device-Specific Field
Additional data	module
Additional data	nattr
Additional data	next_state
Additional data	nsslapd-dbcachesize-value
Additional data	nthandles
Additional data	number
Additional data	old_dn
Additional data	old_ldap_attr
Additional data	operation
Additional data	percentage
Additional data	ptald
Additional data	read
Additional data	resource_type
Additional data	response
Additional data	right
Additional data	rule_type
Additional data	search
Additional data	scheduled
Additional data	scope
Additional data	sizelimit
Additional data	slapd_poll
Additional data	string
Additional data	threadcount
Additional data	time
Additional data	timelimit
Additional data	uniqueid
Additional data	val
Agent (Connector) Severity	ERROR = High; WARNING = Medium; INFORMATION, INFO, DEBUG = Low
Destination Host Name	host to which event was sent
Destination Port	port to which event was sent
Destination Process Name	dependent upon event
Destination User Name	user to whom event was sent
Device Action	action taken by the device
Device Custom Number 1	conn (Connection Number)
Device Custom Number 2	FD (File Descriptor)
Device Custom Number 3	errorcode (Error Code)
Device Custom String 1	DN
Device Custom String 2	Bind Method
Device Custom String 3	Request ID
Device Custom String 4	Tag
Device Custom String 5	Connection Code
Device Custom String 6	number of entries in the directory

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	Status code
Device External ID	dependent upon event
Device Process Name	process
Device Product	'Sun ONE Directory Server'
Device Receipt Time	timestamp
Device Severity	'INFO'
Device Time Zone	zone indicated by the timestamp offset
Device Vendor	'Sun'
Device Version	dependent upon event
External ID	dependent upon event
File ID	file ID
File Name	file name
File Type	file type
Name	dependent upon event
Old File Name	previous file name
Source Host Name	Host Name or IP address
Source Port	port from which event received
