Micro Focus Security ArcSight Connectors

SmartConnector for Tripwire Manager File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for Tripwire Manager File

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

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.
09/30/2014	Removed Windows 2000 support.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
06/30/2009	Global update to installation procedure.
02/11/2009	Added notation that Tripwire for Servers is required to use twprint.
03/01/2008	Updated installation procedure.

SmartConnector for Tripwire Manager File

This guide provides information for installing the SmartConnector for Tripwire Manager File and configuring the device for log event collection. This SmartConnector is supported on Windows 2003 Standard platforms and on UNIX platforms. Tripwire Manager versions 3.0, 4.5, and 5.0 are supported.

Product Overview

Tripwire software assures the integrity of critical data and network infrastructure by detecting and reporting change. You configure Tripwire software to monitor the data that is important to you. Based upon your configuration, the software creates a baseline snapshot of your data in a known good state. After you establish the baseline, you run regular integrity checks to monitor your data. During an integrity check, Tripwire software compares the current state of data to the baseline and reports a violation for any change it detects.

The Tripwire Manager system consists of two main components:

- **Tripwire for Servers**, a self-contained integrity assessment system that you install on each machine you want to monitor. Tripwire for Servers reports additions, deletions, or modifications to monitored objects.
- **Tripwire Manager**, a Java application with a graphical user interface (GUI) that allows you to manage multiple installations of Tripwire for Servers software from a central location.

The most basic configuration is a single Manager that controls all Tripwire for Servers machines.

Configuration

Configuring Tripwire Manager to Convert Log Files

This configuration task is to create a command on the Tripwire Manager that, upon execution, accesses the Manager's log files and converts them to XML format for retrieval by the Tripwire Manager SmartConnector. The log files from the individual Tripwire for Servers machines should be written to the Tripwire Manager `c:\arcsight\twrreports` folder you create in this section. The files in XML format are written to `c:\arcsight\xmlreports`; this is the path and file name you should specify during SmartConnector installation.

On the Tripwire Manager machine:

1. Create `c:\arcsight\twrreports` and `c:\arcsight\xmlreports`.
2. Using the following command, create a batch file (`c:\arcsight\arcsight.bat`):

'twprint' is not part of the Tripwire Manager. Tripwire for Servers is required to use 'twprint.'

```
for %%i in (C:\arcsight\twrreports\*.twr) do "C:\Program
Files\Tripwire\TFS\Bin\twprint" -m r -r %%i -F xml -o
C:\arcsight\xmlreports\%%~ni.xml & move %%i %%i.processed
```

3 In the Tripwire Manager GUI, create a new scheduled task, specifying a time interval of your choice.

4 In the Launch menu, create a new command using the `arcsight.bat` file created earlier. Name it **ArcSight**.

5 In the **Preferences-Notification** tab, select the **Archive Report** option and **Notify on every Integrity Check**. Check the execute command and select the ArcSight command you just created.

Setting Up Tripwire for Servers Log File Reporting

For each Tripwire for Servers machine that is to send its logging information to the Tripwire Manager, perform the following steps:

1 Select a machine from the Machine List and select **Machine -> Edit Config File**.

2 Select the **Logging** tab, then check the **Syslog Reporting** check box.

3 If you are using the Windows operating system, specify a **Syslog Host**.

4 Set the **Syslog Report Level** to set the detail level for log reports.

5 Set the **Syslog Facility** to specify the destination facility for log entries made by Tripwire. Set this to send log reports to the Tripwire Manager. The path should point to the `c:\arcsight\twrreports` folder you created in the previous section.

6 Set the **Syslog Priority** to access the numeric range of syslog priorities.

7 Specify whether Tripwire for Servers is to write audit log entries.

Creating a Machine List

In order for Tripwire Manager to monitor a machine (or machine group), you must include that machine in the Machine list. You can connect machines individually or import a list. If you are connecting more than ten machines, it is faster to import a list.

To import a list of Tripwire for Servers machines:

1 Create a comma-delimited.txt file listing each Tripwire for Servers machine on a separate line, using this format:

`machine_name,group,address,port#,memo,site,local`

where:

`group` is this machine's Tripwire Manager group (if you do not want to group machines, leave this field empty).

`address` can be specified using an IP address or DNS hostname.

`site` and `local` are the site and local passphrases for each machine.

If you omit any of the fields in the import file, leave that field's comma as a placeholder.

2 Select `Manager -> Add Machines` in the Tripwire Manager menu, then click **Import** and navigate to the import file.

3 Click **OK** to register the machines.

To add Tripwire for Servers machines individually:

1 Select `Manager -> Add Machines` from the menu.

2 Enter information for the machine you want to add.

- Use default port number 1169, unless a different port is specified in a machine's agent.cfg file
- If you use DHCP to assign IP addresses in your network dynamically, put the DNS-resolvable hostname for the machine in the **Address** field AND the **Machine Name** field.

3 Click **Add** to add more than one machine, and enter information for the next machine.

4 Click **OK** to register the machines, then provide the console passphrase for the Manager, and the site and local passphrases for each Tripwire for Servers machine.

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 Micro Focus SSO and Protect 724 sites.

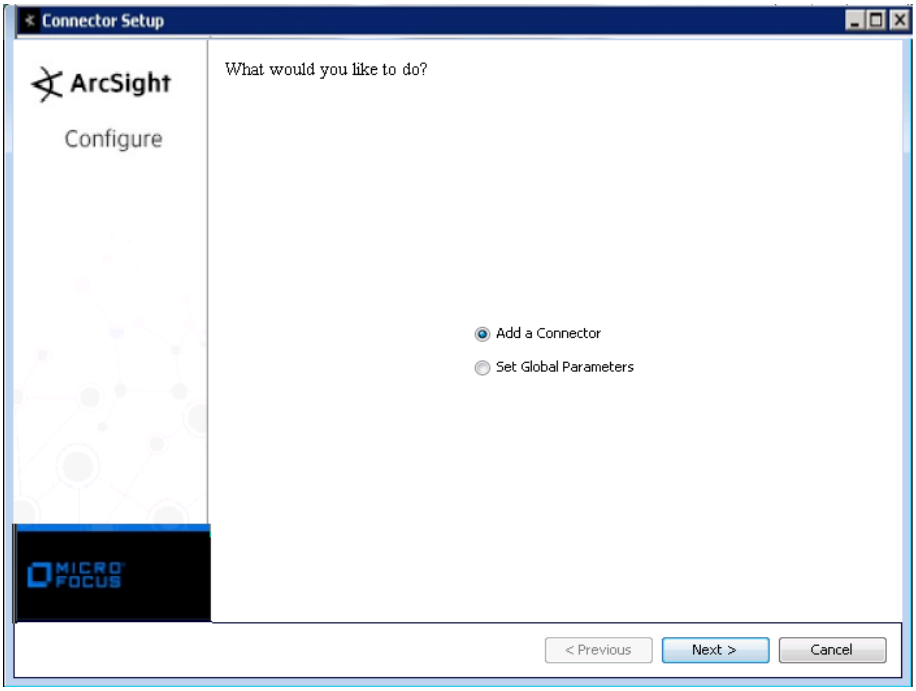
1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.

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

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.

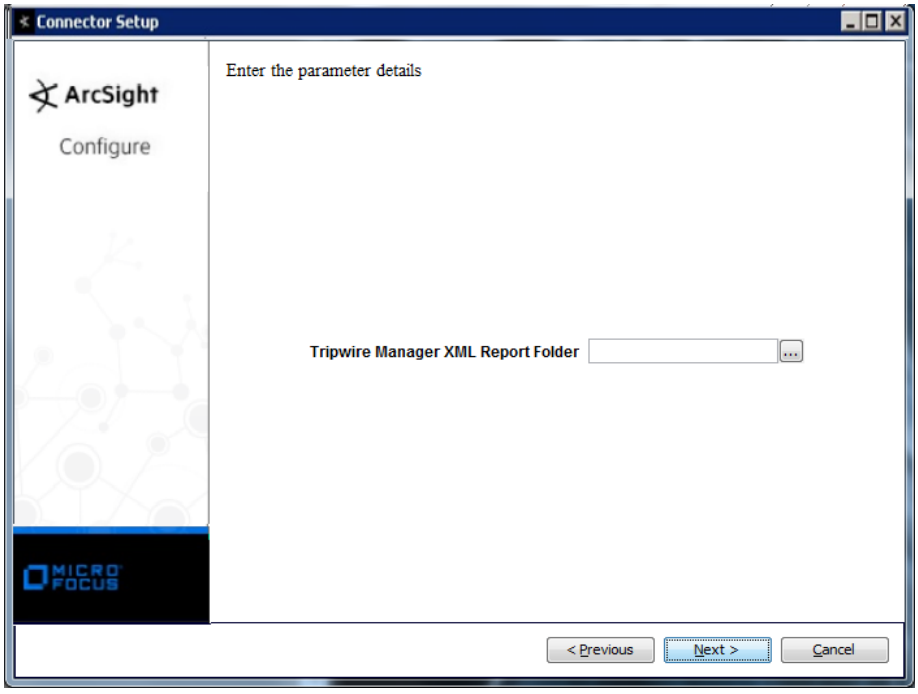
The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

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



Parameter	Description
Tripwire Manager XML Report Folder	Absolute path to the folder containing the log files. Per the configuration steps you followed prior to installing this SmartConnector, specify the path to the \arcsight\xmlreports folder.

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.

Tripwire Manager Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	Owner
Detect Time	Creation Time
Device Action	`Added´, `Changed´, or `Removed´
Device Address	IP Address
Device Custom String 1	Rule Name
Device Event Category	Section Type
Device Event Class Id	`File Added´, `File Changed´, or `File Removed´
Device Host Name	System Name
Device Product	`Tripwire for Servers´

ArcSight ESM Field	Device-Specific Field
Device Severity	Severity
Device Vendor	`Tripwire´
File Name	Object Name
File Path	Start Point
Name	`File Added´, `File Changed´, or `File Removed´
Source User Name	Creator