Micro Focus Security ArcSight Connectors

SmartConnector for ArcSight Asset Import

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for ArcSight Asset Import

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.
05/15/2012	Added new installation procedure.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
08/01/2008	Update to installation procedure.
08/15/2007	General content update.
06/26/2007	Updated configuration information.
09/30/2006	Updated headers available table.
06/30/2006	Added Notes section.
03/17/2006	First edition of this configuration guide.

SmartConnector for ArcSight Asset Import

The SmartConnector for ArcSight Asset Import is a tool for configuring the definitions that represent your network assets in ArcSight's network model. This configuration can be done manually on an asset-by-asset basis using the ArcSight ESM Console. However, if you have many assets that you want to model with the same distinctions, this tool lets you do so in a single batch rather than repeating the process for multiple assets.

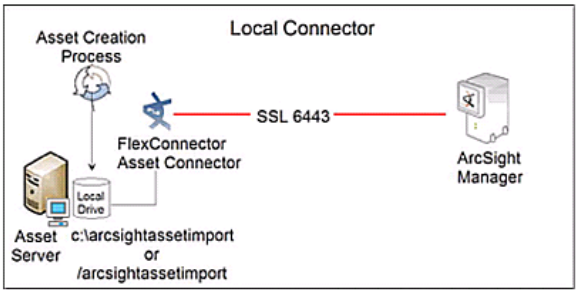
> This tool is not intended to address any asset scalability issues in currently released products (ArcSight ESM 3.5 and prior ESM versions).

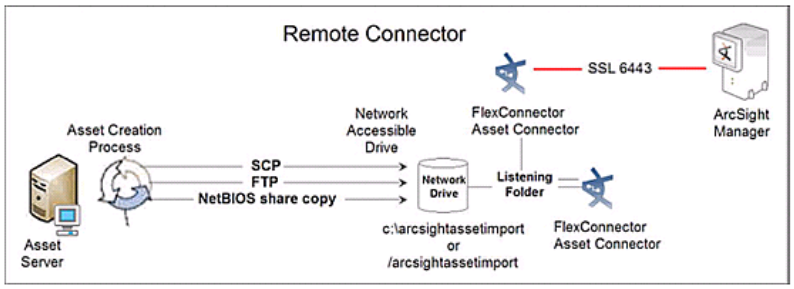
Product Overview

The SmartConnector for Asset Import lets you define a comma-separated (.csv) file that imports asset modeling details in a batch. You can use this tool to assign asset categories to any of your network assets, as well as to those regulated by Sarbanes-Oxley compliance. The tool assigns existing asset categories, and also can be used to create and assign new categories.

If your asset inventory changes regularly, you can set up a process to update and export this list at regular intervals to update the assets in ArcSight ESM.

Depending upon your connector configuration, you can install the SmartConnector for Asset Import on a local asset host or on a dedicated connector server.





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

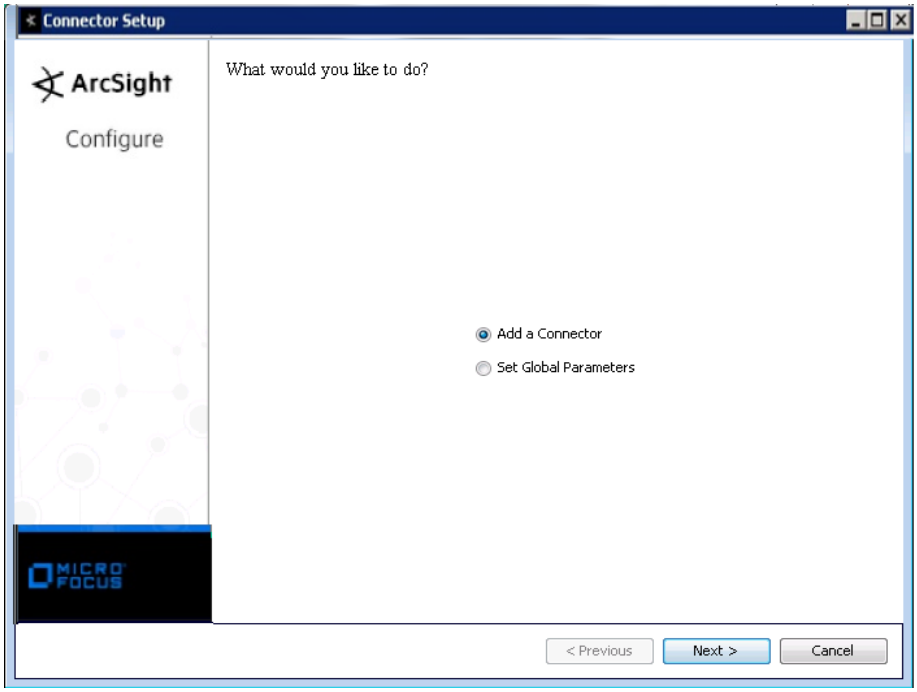
Install Core Software

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.

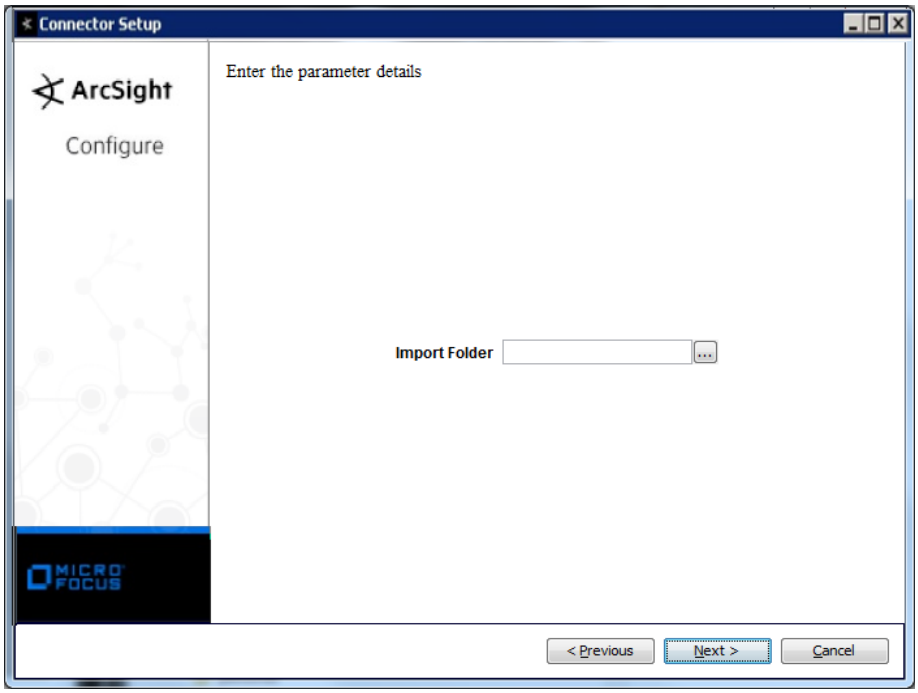
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of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

Parameter	Setting
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 **ArcSight Asset Import** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Enter the file path to the folder where the CSV files to be imported are stored (or browse to the directory in which the files to be imported are stored) for the connector to automatically import the assets into ArcSight ESM. Verify that the directory specified as the connector destination directory is dedicated as a repository for the Asset Import connector only. Any files placed in this directory are processed by the connector and removed from the system.

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**.

   If your environment is going to build a process to automatically update the assets on a recurring basis, ArcSight recommends running the connector as a service. You can then simply drop an updated file into the defined Asset Input directory, and the connector automatically imports the contents.

   If you intend to use this connector once only to configure your Sarbanes-Oxley assets, select **No**. This deactivates the polling feature that detects updated files and sends them to the Manager. Any subsequent updates to your assets list must be implemented manually.

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*.

Assign the SmartConnector to an ArcSight Network

Whether you have existing assets or are creating assets for the first time, assign your Asset Import connector to the ArcSight Network or Networks represented by the assets modeled in your CSV file. This process ensures that each asset is correctly associated with the proper zone.

For a list of networks and zones and an overview of ArcSight's network modeling framework, see *ArcSight 101*.

> If you do not assign the connector to an ArcSight network, any newly created assets are assigned to the ArcSight default zone definition, which may not match your environment.

To assign the connector:

1 Launch the ArcSight ESM Console.

2 In the Navigator panel, go to Connectors and navigate to the Asset Import connector you configured (*Asset Importer*). Right-click on your Import connector name and select **Configure**.

3 In the Connector Inspector in the Inspect/Edit panel, select the **Networks** tab.

4 Click the add (**+**) icon in the Network Selector. Browse to and select the networks you have defined for your environment. Select as many networks as required to cover the assets described in your CSV file.

5 Click **OK** in the Networks Selector and again in the Connector editor.

Import Assets

Now that the CSV file has been created and the Asset Import connector is installed and configured, you can import the CSV file into the connector.

> Assets should not be imported into a system folder; you will not be able to delete any assets you import into system folders.

Before you import the file, consider creating simplified asset names as documented n the following section.

Create Simplified, Host-Based Asset Names in Console Display

By default, assets created by the Asset Import Connector (or a vulnerability scanner) appear in the Console display with a long, multi-element name that uses the following naming convention:

```
Device (Address: $destinationAddress Hostname:
$destinationHostName Zone: $!destinationZone.Resource.Name)
```

This results in long names that are hard to view in the Console Navigator panel. Once the assets are imported, the only way to change these long names is to change them manually, one by one, in the Console UI. To avoid this, you can change this default naming convention for a convention that is easier to view by appending an override naming convention in the server.properties file.

1 At a command line, stop the Manager service:

UNIX: Enter `/etc/init.d/arcsight_manager stop`.

Windows: Stop the ArcSight Manager service from **Control Panel -> Administrative Tools -> Services**.

2 In a text editor, first backup then edit `$ARCSIGHT_HOME/config/server.properties`. To modify the multi-element template to one that displays only the host name, copy the following line and paste it at the bottom of the server.properties file:

```
scanner-event.auto-
create.asset.name.template=$destinationHostName
```

This modifies the format permanently, so when you subsequently batch imports from the Asset Import connector or a vulnerability scanner, the Console displays the host name only.

3 Save and close `server.properties`.

4 Restart the Manager service:

UNIX: `/etc/init.d/arcsight_manager start`

Windows: Start the ArcSight Manager service from `Control Panel -> Administrative Tools -> Services`.

When you import the CSV file, the assets are displayed in the Console, identified by their easier-to-read host names.

Copy CSV File into Target Directory

Now that the SmartConnector has been installed and the correct network has been assigned to the SmartConnector, you can copy the CSV file containing your asset configurations into the monitored directory on the connector system. Importing assets consists of copying the CSV file you created into the directory you specified as the target directory during connector installation.

Verify that the directory specified as the connector destination directory is dedicated only as a repository for the Asset Import SmartConnector. Any files placed in this directory will be processed by the connector and removed from the system. Always **copy** your CSV file to the destination folder on the connector system. **Do not move it there**; the connector deletes the file when it has finished processing it.

The connector need not be on the same system as your asset creation process. As long as you can place the file into the monitored folder, you can copy the source file to the directory, as long as the source file is accessible by the network.

For example, on Windows systems, you can share directories and copy the file over the network to the monitored directory. In a UNIX environment, you can ftp or "secure copy" (scp) the file to the appropriate location.

1. Copy your CSV file into the directory the connector is monitoring, which you set up during connector installation.

2. As part of the connector heartbeat with the Manager, the connector detects the new file and immediately processes it, and imports the new or updated asset configuration information into the Manager. When the connector and Manager have finished processing the file, the connector removes the CSV file from the connector system.

3. To verify that the asset configuration values were imported correctly, check the following points in the Console Navigator panel:

   - For newly created assets, expand the Assets in the Navigator panel to verify that any new assets you defined are present at the location you defined in the CSV file.

   - For asset category assignments, navigate to **Assets** and click the **Assets** tab. Go to **ArcSight System Administration/Connectors**, where you will find the connectors installed for your environment. Double-click the asset you categorized in the CSV file to open its configuration definitions in the **Inspect/Edit** panel. Verify that the asset categories you specified in the CSV file appear on the list of asset categories associated with this asset.

As soon as the file is deposited in the destination directory, its content is monitored.

Define the Asset Input CSV File

The section describes how to define the asset input CSV file. This task can be performed either before or after the Asset Import SmartConnector is installed. See "Installation" for steps to install the SmartConnector.

> In addition to describing how to install the SmartConnector, the Installation section is followed by sections describing assigning the connector to a network and importing assets.

Define Assets

To define assets, first create a comma-separated value (CSV) file in a spreadsheet or database, then save the file as a CSV file.

Notes:

- Use the full URI to the location being defined in the CSV file
- List each field to be defined as its own column in the asset CSV file
- Be sure to enter existing values exactly as they are on your system

The SmartConnector is configured to recognize specific header names. The order of the headers is not significant and not all possible header names need be used. Whatever headers you do use are case sensitive and must appear as shown in the following table. This table presents the headers available and an example of the data that can be used.

Header Name	Data Description
address	IP address of the asset.
macAddress	MAC address of the asset with colons between the hexadecimals. For example: `00:10:V6:VC0:CA:35`
hostname	Hostname of the asset (if blank, use `IPAddress`).
location	The entire URI to the location of the asset exactly as it appears in your system. This full URI must be included in the CSV file.
category	Replace **M** with the name of the category you want to associate with the asset. For each new category, add a new column and enter **'category:CategoryName'** where the **CategoryName** describes its function. Examples could be: category:NetowrkDomain, category:SOX, category:location, category:Temp. Note that 'category' is required for processing.

You can define as many asset categories as you want, as long as you prefix the header with `category:`. Asset categories defined for each asset are assigned either upon import (if the category already exists) or are created automatically (if the category does not already exist).

Sample category definitions follow.

To define Sarbanes-Oxley assets:

```
hostHame, address,category:Sarbanes
server1,10.0.0.1, /All Asset Categories/ArcSight
Solutions/Compliance Insight Package/Regulation/Sarbanes-
Oxley
```

To define NIST 800-53 Email assets:

```
hostName,address,category:NetworkDomain1
server2,10.0.0.2, /All Asset Categories/ArcSight
Solutions/Compliance Insight Package/Control Framework/NIST
800-53/Network Domains/Email
```

To define multiple categories to one asset: Sarbanes-Oxley and E-mail:

```
hostName,address,category:NetworkDomain1,category:Sarbanes
server1,10.0.0.1, /All Asset Categories/ArcSight
Solutions/Compliance Insight Package/Control Framework/NIST
800-53/Network Domains/Email, /All Asset
Categories/ArcSight
Solutions/Compliance Insight Package/Regulation/Sarbanes-
Oxley
```

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.

Issues

Possible Overwritten Assets

When you have an asset or assets categorized using site asset categories, the categories are overwritten. This occurs because any URI reported by a scanner connector is marked as reported by the manager internal connector, causing any previously existing categorization to be dropped. This will be corrected in a future SmartConnector release.

Asset Creation under ArcSight System Administrator

In the ArcSight ESM Console, a user cannot create or delete assets in the ArcSight System Administrator folder. However, because anything coming from a connector is considered to have root privileges, asset creation is possible under ArcSight System Administrator as a result of processing events coming from the Asset Import SmartConnector. Be aware that assets should not be created under this folder; once they are created, they cannot be deleted.