Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for ArcSight Asset Import

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for SmartConnector for ArcSight Asset Import

The SmartConnector for ArcSight Asset Import is a tool to configure the definitions that represent your network assets in ArcSight's network model. Although you can configure it manually on an asset-by-asset basis by using the ArcSight ESM Console, it can be a cumbersome process if you have multiple assets that you want to model with same distinctions. The SmartConnector for ArcSight Asset Import allows you to configure definitions in a batch rather than having to repeat 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).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight 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.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

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 Documentation-Feedback@microfocus.com.

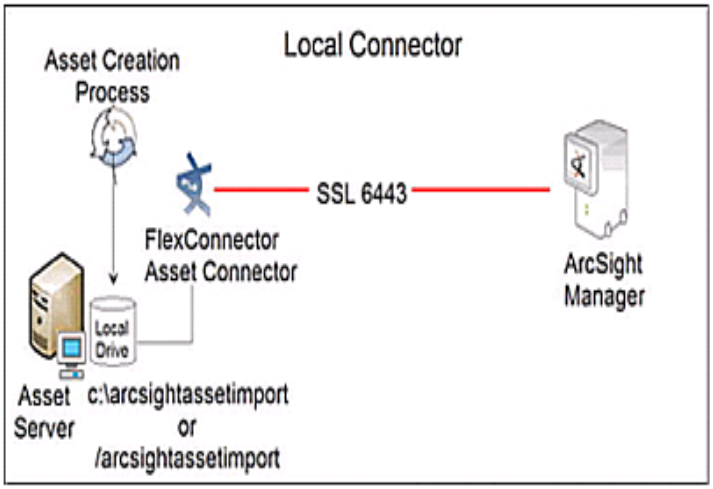
For specific product issues, contact Micro Focus Customer Care.

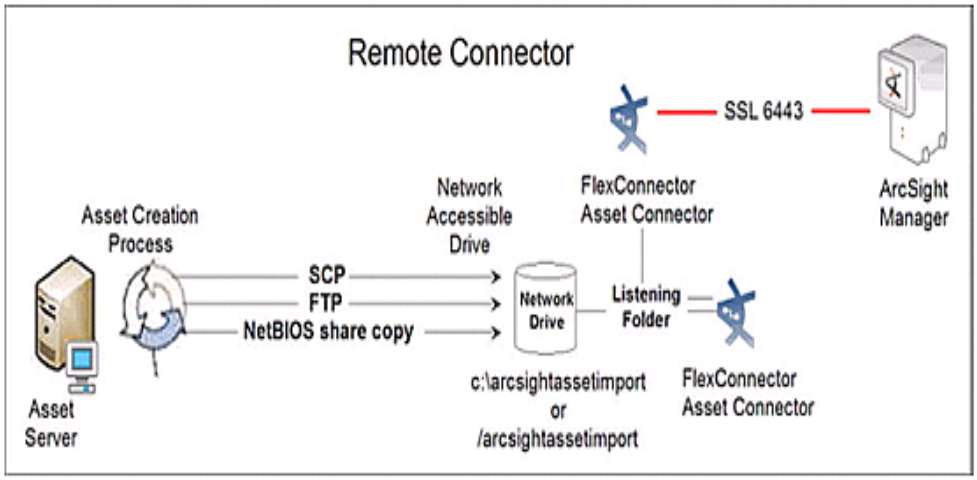
Product Overview

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





Installing the SmartConnector

The following sections provide instructions to install and configure your the SmartConnector.

Preparing to Install the SmartConnector

Start the installation wizard.

Follow the instructions in the wizard to install the core software.

Specify the relevant Global Parameters, when prompted.

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 and Configuring 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. From the **Type** drop-down, select **ArcSight Asset Import** , then click **Next**.
5. For the **Import Folder** field, specify the path to directory that contains the CSV file, which has the asset configurations, then click **Next**.
6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
9. Select whether you want to run 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 SmartConnector Installation and User Guide.

Assigning 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 *ESM 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. Go to Connectors, navigate to the Asset Import connector you configured, then right-click 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 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. **5** Click **OK** in the Networks Selector and again in the Connector editor.

Defining the Asset Input CSV File

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
- 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
```

Importing Assets

After the CSV file is created and the Asset Import SmartConnector is installed and configured, you can import the CSV file into the SmartConnector.

Note: Make sure that you do not import Assets into a system folder any assets that you import into system folders cannot be deleted.

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

Creating 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. After 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 the default naming convention for a convention that is easier to view by appending an override naming convention in the server.properties file.

1. Open command prompt, then stop the Manager service:

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

   Windows: Stop the ArcSight Manager service from **Control Panel > Administrative Tools > Service**.
2. Make a backup of `$ARCSIGHT_HOME/config/server.properties` file.
3. 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
   ```
4. Save and close `server.properties`.

   This modifies the format permanently. When you subsequently import batches from the Asset Import connector or a vulnerability scanner, the Console displays only the host name.

5. 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 easy-to-read host names.

Copying CSV File into Target Directory

Importing assets consists of copying the CSV file you created into the directory you specified as the import directory during the smartconnector installation.

Verify that the specified directory is dedicated only as a repository for the Asset Import SmartConnector. Any files placed in this directory will be processed by the SmartConnector and removed from the system.

Note: Always copy and not move your CSV file to the destination folder on the connector system. The connector deletes the file when it finishes processing it.

The SmartConnector 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 the CSV file to the directory that you specified during SmartConnector configuration.
2. The content of the file is monitored as soon as the file is deposited in the destination directory. content is monitored. As part of the SmartConnector heartbeat with the Manager, the connector detects the new file, immediately processes it, and imports the new or updated asset configuration information into the Manager.
3. When the SmartConnector and Manager have finished processing the file, the SmartConnector removes the CSV file from the SmartConnector system.
4. To verify that the asset configuration values were imported correctly, check the following points in the Console Navigator panel:
    a. 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.
    b. 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.

Known 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. Make sure that assets are not created under this folder because they cannot be deleted.

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 SmartConnector for ArcSight Asset Import (SmartConnectors 8.3.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!