Developer's Guide

Asset Model Import FlexConnector

July 7, 2015

ArcSight
An HP Company

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	http://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Contents

Chapter 1: Overview 5

Assumptions 5

Chapter 2: Asset Model Import FlexConnector Attributes 7

CSV File Attributes 7

Chapter 3: Installing and Configuring the Asset Model Import FlexConnector 9

Prerequisites 9
Installing the Asset Model Import FlexConnector 10
Configuring the Asset Model Import FlexConnector 10
Running SmartConnectors 11
Set the Model Import User 12
CSV Format and Parser Example 12
Default CSV Format 12
Parser Example and Template 13
CSV File Attributes 16
Reloading Asset Model Data 16

Chapter 1
Overview

The Asset Model Import FlexConnector allows you to develop a model import connector to import the asset model data from a file. This enables you to create and maintain ESM Network Model data, and keep this data in sync with the data in your Asset Management system. Based on configuration, files are read by the connector, and converted to XML based on parser attributes. Upon generation, the XML files are automatically transferred by the connector to the ESM server.

CSV is the only file format supported.

You configure the connector using the SmartConnector Configuration Wizard. Also, you must create parser files from the provided template that match the format of the CSV files.

The connector supports two modes of operation:

- Initial read and import
- Ongoing detection and import of updates

During the initial read and import for attributes specified in the CSV files, the connector can import a full set or subset of attributes for each asset based on CSV file content and corresponding matching parser configuration.

Once the information is imported into ESM, the list of attributes the connector sends to ESM for existing assets is not updated. If you add or remove attributes to be sent to ESM from the connector after you import the asset data, you will not get a history of the new attributes. Updates will only be from the point of time the attributes were added. If you want a history of the added attributes, re-import the asset data.

Assumptions

You should be familiar with writing a Log File FlexConnector. Refer to the *FlexConnector Developer's Guide* for more information about writing a parser.

Chapter 2
Asset Model Import FlexConnector Attributes

CSV File Attributes

The following table lists the CSV file attributes for the Asset Model in ESM. In order to work with these attributes, you should be familiar with the ESM Asset Model. See the ArcSight Console User's Guide, topics "Modeling the Network" and "Asset Model".

Attribute	Description
Inactive Asset	Use to disable an asset.
Inactive Reason	The reason the asset was inactivated (disabled).
Name	The asset's friendly name. This field can default to the asset's host name or IP address. This name is listed in the Asset tree in ESM.
IP Address	The asset's IP address, in dotted-decimal notation.
MAC Address	The unique hardware ID for the network device.
Host Name	The asset's DNS name.
External ID	The asset's user-defined identifier.
Alias	The asset's display name. If an alias is not specified, the asset name is used. Typically used in a localized environment to display the asset name in the local language.
Parent Group	The URI of the asset's immediate parent group in the hierarchy, based on ESM's Asset tree. For example, "/All Assets/Customer A/".
Old Parent Group	Used only to move one asset from one group to another. Is the URI of the source group for the asset.
Description	The asset's text description.
Zone	As described in Assets and Changing Assets. Specify the Zone URI of the Asset, as shown in the in ESM Zones tree.
Location	The asset's specified location.
Category	The URI of the category to which the asset belongs. An asset can belong to more than one category. Assets can be categorized based on business use, criticality, applications, hardware, operating system, or other criteria. If a category does not exist, it is automatically created for the asset. For example, for the category Criticality, and asset can belong to the category High (with the Criticality categories of High, Medium, and Low).

Chapter 3
Installing and Configuring the Asset Model Import FlexConnector

This chapter provides information about the prerequisites, installation and configuration of the Asset Model Import FlexConnector.

The following topics are covered:

"Prerequisites" on page 9
"Installing the Asset Model Import FlexConnector" on page 10
"Configuring the Asset Model Import FlexConnector" on page 10
"Running SmartConnectors" on page 11
"Set the Model Import User" on page 12
"CSV Format and Parser Example" on page 12
"Reloading Asset Model Data" on page 16

Prerequisites

Before installing the Asset Model Import FlexConnector, the following prerequisites must be met:

- Ensure that ESM and the Console are installed. For more information, see the ArcSight ESM Installation and Configuration Guide.
- Local access to the machine where the Asset Model Import FlexConnector is to be installed and administrator privileges to that machine.
- A minimum of 256 MB of memory and 3 GB of available hard disk space on the host machine.
- Start the Manager. The command prompt window or terminal box displays a **Ready** message when the Manager starts successfully. Monitor the `server.std.log` file located in `$ARCSIGHT_HOME\logs\default`. Although not required, it is helpful to have the Console running when installing the Asset Model Import FlexConnector to verify a successful installation.
- Zones must have been created in ESM to use with the assets, using the Network Modeling Wizard in the ArcSight Console. If the zones are not created, assets are not assigned to zones, and the zone information for the asset is ignored.
- ArcSight ESM and database components must be up and running to configure the Asset Model Import FlexConnector.

Installing the Asset Model Import FlexConnector

This section provides instructions on how to install the Asset Model Import FlexConnector.

1 Using the log-in credentials supplied to you by ArcSight, download the Asset Model Import FlexConnector installation executable file from the HP software support site to the machine where the connector will run.

2 Place the executable file in a directory.

3 Double-click the executable file to start the installer.

4 Follow the installation 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...

Configuring the Asset Model Import FlexConnector

This section provides information about configuring the Asset Model Import FlexConnector. After installation completes, the SmartConnector Configuration Wizard displays.

1 Select **Add a Connector**. Click **Next**.

2 **Asset Model Import FlexConnector for File** is already selected. Click **Next**.

3 Enter devices details, which are the folder locations and parser names. Click **Add** to add folder locations for folders containing the CSV log files and the associated parsers.

Field	Description
Folder Location	Enter the complete path to the folder containing the CSV log files. Each folder must contain CSV files of the same format, and associated with the same parser.
Parser File Name	Enter the name of the parser associated with the specific CSV folder. The parser must match for the format of the CSV file. You can create a different parser format for each folder configured.

Use **Import** and **Export** to copy the list of folders and parsers to or from a spreadsheet if needed. Click **Next**.

4 In the destination type window, verify that **ArcSight Manager (encrypted)** is selected and click **Next**.

When selecting destinations for the Asset Model Import FlexConnector, select **ArcSight Manager (encrypted)** only. No other destinations are supported.

5 Enter destination parameters, including the host and port information, and click **Next**.

Parameter	Description
Manager Host Name	Enter the name of the host on which the Manager is installed.
Manager Port	Enter the network port from which the Manager is accepting requests. The default port is 8443.
User Name	Enter a valid ArcSight user name to log in to configure the SmartConnector. This is the same user name you created during the Manager installation.
Password	Enter a valid ArcSight password to log in to configure the SmartConnector. This is the same password you created during the Manager installation.
AUP Master Destination	Select true or false.
Filter Out All Events	Select true or false.
Enable Demo CA	Select true or false.

6 Enter connector details. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**.

7 Select whether to import a certificate. Click **Next**.

8 Read the SmartConnector summary and click **Next**. If the summary is incorrect, click **Previous** and make changes.

9 The Wizard now prompts you to choose whether you want to run the SmartConnector as a process or as a service. If you choose to run the SmartConnector as a service, the Wizard prompts you to define service parameters for the SmartConnector. Click **Next**. The Wizard displays a dialog confirming the SmartConnector's configuration.

10 Choose **Exit** and click **Next**.

11 Click **Done**.

A parser example that you can use as is or use as a template is created during the configuration process is located at:
`$ARCSIGHT_HOME\user\agent\flexagent\mic\asset_flexfile\`.

Running SmartConnectors

SmartConnectors can be installed and run in standalone 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 installed standalone, the SmartConnector must be started manually, and is not automatically active when a host is re-started. If installed as a service or daemon, the SmartConnector runs automatically when the host is re-started. For information about connectors running as services or daemons, see the ArcSight SmartConnector User's Guide.

For connectors installed standalone, to run all installed SmartConnectors 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.

Set the Model Import User

After installing, configuring, and starting the connector, from the ArcSight Console set the Model Import User for the connector (this must be a user with Console administrative privileges). Setting the user links the user to the assets, and that user is then treated as the "creator" of the assets. The connector is then run on that user's behalf.

1. From the ArcSight Console, go to the **Navigator** panel and choose the **Resources** tab.
2. Under **Resources**, choose the **Connectors** resource.
3. Under **All Connectors**, navigate to your **Asset Model Import FlexConnector**.
4. Right click on the connector and select **Configure**.
5. On the **Inspect/Edit** panel and choose the **Connector** tab.
6. Under the **Connector** tab, go to **Model Import User** and select a user from the **Administrators** group.
7. Click **OK**.

CSV Format and Parser Example

The following is an example of the CSV format. Each line of the CSV file represents one asset.

If you want categories to be created automatically on the ESM server side, the property `archive.import.asset.category.auto.create` must be set to true in the server.properties property file. See the ArcSight Console User's Guide, "Asset Model", for details on working with assets. See the ESM Administrator's Guide, "Editing Properties Files", for details on how to edit a properties file.

Default CSV Format

By default, the parser supports the following CSV format:

```
Action,InactiveAsset*,InactiveReason,AssetName,Ip,Mac,HostName,Ext
ernalId,Alias,ParentGroupUri,OldParentGroupUri,AssetDescription,Zo
neUri,LocationUri,AssetCategory
```

*the asset can be inactive or active based on the value passed (true or false) to enable or disable the asset

An example of a CSV file:

```
addAsset,,,asset_1,199.199.0.1,00:11:22:33:44:51,myhostname_1,myex
ternalid_1,myalias_1,myparentgroupuri_1,,myassetdesc,myzoneuri,myl
ocationuri,myassetcategory
```

Where **AssetCategory** can be multiple categories separated by ";" and **Action** can be one of the following:

- **addAsset:** Creates an asset
- **updateAsset:** Update an existing asset on the server. The server will update asset attributes and merge categories.
- **removeAsset:** Removes the asset
- **addCategory:** Assigns one or more categories, separated by a semi-colon (;)
- **removeCategory:** Removes one or more categories, separated by a semi-colon (;)
- **addZone:** Assigns a zone. An asset can belong to one zone only. If an asset belongs to a zone, the newly-added zone will replace the existing zone. Do not add assets from more than one zone in a CSV file. Generate separate CSV files to contain assets from different zones.
- **removeZone:** Removes the asset from a zone.
- **moveAsset:** Removes the asset from the existing parent group and associates it with the new parent group.

The connector does not validate the data in the CSV file or in the XML archive. The archive can fail processing based on existing edit checks in ESM.

Parser Example and Template

You create parser files to match the format of your CSV files. This example is provided to help you create your own parser files.

```
comments.start.with=#

delimiter=,

token.count=15

token[0].name=Action

token[0].type=String

token[1].name=Inactive

token[1].type=String

token[2].name=InactiveReason

token[2].type=String

token[3].name=AssetName

token[3].type=String

token[4].name=Ip

token[4].type=String
```

```
token[5].name=Mac

token[5].type=String

token[6].name=HostName

token[6].type=String

token[7].name=ExternalId

token[7].type=String

token[8].name=Alias

token[8].type=String

token[9].name=ParentGroupUri

token[9].type=String

token[10].name=OldParentGroupUri

token[10].type=String

token[11].name=AssetDescription

token[11].type=String

token[12].name=ZoneUri

token[12].type=String

token[13].name=LocationUri

token[13].type=String

token[14].name=AssetCategory

token[14].type=String


###keep these 7 fields unchanged###


additionaldata.enabled=true

additionaldata.duplicate.keys.allowed=false

event.deviceEventCategory=__stringConstant(Asset)

event.deviceCustomString1Label=__stringConstant(model.sender)

event.deviceCustomString1=__stringConstant(flexcsv)

event.deviceCustomString2Label=__stringConstant(model.template)

event.deviceCustomString2=__stringConstant(mic/asset_flexcsv/asset
.vm)


###field mappings###
```

```
event.deviceVendor=__getVendor(CSV File)
event.deviceProduct=__stringConstant(Assets)
event.deviceAction=Action
additionaldata.Action=Action
event.externalId=ExternalId
event.flexString1=AssetName
#following mappings maybe removed in future but required for now
additionaldata.UniqueUserId=AssetName
event.destinationUserId=AssetName
```

CSV File Attributes

Attribute	Description
Action	Defines the action you can take. See "Default CSV Format" on page 12 for details on possible actions.
InactiveAsset	Use to disable an asset.
InactiveReason	The reason the asset was inactivated (disabled).
AssetName	The asset's friendly name. This field can default to the asset's host name or IP address. This name is listed in the Asset tree in ESM.
IP	The asset's IP address, in dotted-decimal notation.
MAC	The unique hardware ID for the network device.
HostName	The asset's DNS name.
ExternalID	The asset's user-defined identifier.
Alias	The asset's display name. If an alias is not specified, the asset name is used. Typically used in a localized environment to display the asset name in the local language.
ParentGroupUri	The URI of the asset's immediate parent group in the hierarchy, based on the Console's Asset tree. For example, "/All Assets/Customer A/".
OldParentGroupUri	Used only to move one asset from one group to another. Is the URI of the source group for the asset.
AssetDescription	The asset's text description.
ZoneUri	As described in Assets and Changing Assets. Specify the Zone URI of the Asset, as shown in the in ESM Zones tree.
LocationUri	The asset's specified location.
AssetCategory	The URI of the category to which the asset belongs. An asset can belong to more than one category. Assets can be categorized based on business use, criticality, applications, hardware, operating system, or other criteria. If a category does not exist, it is automatically created for the asset. For example, for the category Criticality, and asset can belong to the category High (with the Criticality categories of High, Medium, and Low).

Reloading Asset Model Data

A redeployment, reconfiguration, or mistaken deletion of attributes of your ESM structure may require reloading all asset data. Use the following procedure to reload asset data:

1. Stop the connector if running.
2. From the ArcSight Console, go to the **Navigator** panel and choose the **Resources** tab.
3. Under **Resources**, choose the **Asset** tab.

4 Under **All Assets**, go to the top level directory. Highlight the **asset data**, right-click and choose **Delete Group** from the menu.

Be sure not to delete all assets. Delete only the asset data managed by this connector.

5 On the connector side, reconstitute the asset data by recopying it from its original source, or renaming the backup files to their original file names.