Hewlett Packard
Enterprise

Configuration Guide

HPE ArcSight Actor Model Import Connector
7.1.2.7394.0

for ArcSight RepSM

July 7, 2015

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from HPE 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.

Copyright Notice

Contact Information

Phone	A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page: www.hpe.com/software/support/contact_list
Support Web Site	www.hpe.com/software/support
Protect 724 Community	https://www.protect724.hpe.com

Configuration Guide Contents

Model Import Connector for RepSM

This guide describes installing the Model Import Connector for RepSM and configuring the device for data collection.

Product Overview

The HPE Reputation Security Monitor (RepSM) solution uses internet reputation data to detect Advance Persistent Threats and zero day attacks as well as provide context to security events. The Model Import Connector for RepSM is a component of RepSM which retrieves reputation data from the RepSM threat intelligence service (powered by DVLabs), processes this data, and forwards it to ArcSight ESM.

The threat intelligence includes reputation information about internet nodes which are known to exhibit bad behavior. The ill reputed nodes are identified by their network address or Domain Name System (DNS) name. This data is used by the accompanying RepSM content package to detect malware infected machines, zero day attacks, and dangerous browsing. The user can also use the data to implement custom ESM solutions. For further details on this solution, see the Reputation Security Monitor Solution Guide.

Features and Functional Summary

The Model Import Connector for RepSM retrieves the reputation data and forwards it to ESM. This connector supports one ESM destination.

Between restarts, the connector retrieves from the reputation service only the delta from the last retrieved version. If the connector requests only delta information from the threat intelligence service, and the service cannot provide such a delta, then a full update of data will be sent to the connector. In this case, the existing entries in the ESM active list will be dropped, and the list repopulated with new entries from the latest full update.

These entries are:

- IPv4 addresses
- Host and domain names

For each entry these reputation attributes are retrieved:

- Reputation Score
- Exploit Type

The initial load and any manually initiated full update will see a delay of about 5 minutes from the time the update is initiated. In the subsequent updates following the initial load of the entries, the connector will process deltas to add, delete, and update the entries which the RepSM service releases at intervals of every several hours. The connector checks for updates, by default, every two hours. The connector will read any warning codes or messages sent by the RepSM service and will send these to ESM as an ArcSight event.

Due to storage requirements, the RepSM service might not provide accumulated delta updates if the connector has been down for more than a week. In this case, a full import will be automatically performed.

Installing the Connector

Before installing the connector, verify that ESM (the product with which the connector will communicate) and Console have already been installed correctly. It is recommended that the connector not be installed on the same machine as ESM. Also, be sure the following are available:

- Additional 2GB memory if the connector is run in standalone mode
- Subscription to the Reputation Security Monitor Service (RepSM)
- Local administrator access to the machine on which the connector will be installed.
- The machine, on which the connector will be installed, has external access over the Internet to any system over port 443 and connectivity to the ESM machine over port 8443 (default) or the configured port if the default was not used.
- ESM IP address, port, administrator user name, and password

Model Import Connector Installation

This section provides instructions on how to install the Model Import Connector for RepSM.

To install the Model Import Connector for RepSM:

1. Obtain the license activation key. You will have received an e-mail containing a link to the license activation page and an order number. Click the link or copy and paste the order number, and follow the instructions that you receive from there on.
2. Download the Model Import Connector for RepSM installation executable using the link provided in the e-mail sent to you by HPE.
3. Start the connector installer by running the executable.

The Model Import Connector for RepSM installation requires additional steps after the installation wizard has finished. See step 16 of this procedure and subsequent steps for details.

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...

4 Select **Add a Connector**.

5 **Model Import Connector for RepSM** is already selected. Click **Next**.

6 Enter the required parameters to configure the connector, then click **Next**.

Parameter	Description
Service Activation Key	When you request an activation key, HPE will send you a .dat file. Open the .dat file in a pure ASCII text editor (such as Notepad++) and copy the entire second line of the file (the activation key). Paste the activation key into the Service Activation Key field. This field is required.
Update Frequency (hours)	Interval at which the connector checks for updates. The default is **2** (two hours). The value must be 1 or larger, and in whole numbers. Zero (0) is invalid. The default is recommended for performance reasons. This field is required.
Proxy Host (https)	Use this field and the following three fields only if you need the connector to use a proxy to access the Internet. Enter the proxy host IP address. This value is required for proxy configuration.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
Proxy User Name	Enter the proxy user name. This value is needed if the proxy requires authentication. If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password for the proxy user specified. This value is needed if the proxy requires authentication. This field is required only if you have specified a proxy user name.

7 **ArcSight Manager (encrypted)** is selected. Click **Next**.

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

Parameter	Description
Manager Host Name	Enter the name or IP address 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.

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

9 Select whether to import a certificate.

10 Review the **Add connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

Some folders, files, and logs are named `RepDV` or `repdv`. This naming does not affect the functioning of the connector and can be ignored.

11 The wizard now prompts you to choose whether you want to run the connector as a stand-alone process or as a service. Choose either **Install as a service** or **Leave as a standalone application**. Click **Next**.

12 To close the installation wizard, choose **Exit** and click **Next**. There are further installation steps after you close the wizard. Be sure to continue with the subsequent installation steps.

13 If the connector is run in standalone mode, the default heap size is 256MB. For proper operation of the connector, HPE recommends that you modify the heap size setting to 2GB. There is no need to modify memory if the connector is run as a service; if the connector is configured to run as a service, the heap size is set to 2GB by default.
Increase the memory for the connector by doing the following (in the following example commands, ARCSIGHT_HOME represents the name of the directory where the connector is installed):

- For Linux - create the following shell script and be sure it is executable:
  `~/ARCSIGHT_HOME/current/user/agent/setmem.sh`
  with the following content:
  `ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx2048m "`
- For Windows - create the following batch file:
  `$ARCSIGHT_HOME\current\user\agent\setmem.bat`
  with the following content:
  `SET ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx2048m "`

Be sure to use regular double quote characters in the file content in either the shell script or the batch file.

14 Verify that the connector is running. You can check the ArcSight Console Navigator in the Resources tab, under Connectors. If the connector is running, you will see ***<connector_name>*** **(running)** listed. See "Running Connectors" on page 9.

15 Set up the Model Import user in ESM. See "Setting up the Model Import User in ESM" on page 9.

16 Start the data import. See "Starting and Stopping Data Import" on page 10.

Running Connectors

Connectors 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, connectors also can be run using shortcuts and optional Start menu entries.

If installed standalone, the connector 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's Guide, Chapter 3, Installing SmartConnectors, in the section "Running SmartConnectors".

For connectors installed standalone, to run all installed connectors on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `./arcsight agents`

To view the connector log, read the file:
For Windows - `$ARCSIGHT_HOME\current\logs\agent.log`
For Linux - `~/ARCSIGHT_HOME/current/logs/agent.log`

To stop all connectors, enter `Ctrl+C` in the command window.

Connector Upgrade

To upgrade the Model Import Connector for RepSM, you must uninstall the current version of the connector and then install the latest version. For information about uninstalling connectors, see the ArcSight SmartConnector User's Guide.

Administrative Tasks - RepSM Configuration Using the ArcSight Console

There are mandatory and optional administrative tasks. "Setting up the Model Import User in ESM" on page 9 and "Starting and Stopping Data Import" on page 10 are mandatory steps for connector installation, and are mentioned as part of the installation procedure. See "Installing the Connector" on page 6 for details. You might also find that you need to perform these tasks outside of the context of the installation procedure.

The tasks "Optional - Reloading RepSM Data" on page 10 and "Optional - Optimization of Data Transfer Using a Timer" on page 11 can be performed as needed.

Setting up the Model Import User in ESM

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 **Model Import Connector for RepSM**.

4 Right click on the connector and select **Configure**.

5 On the **Inspect/Edit** panel, 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**.

If a user that does not have administrator privileges is used, the import will fail.

Starting and Stopping Data Import

By default the connector’s data import capability is not started. You must start the import manually in the ArcSight Console.

Data import needs to be started only once from the ArcSight Console. Unless it is stopped from the ArcSight Console, there is no need to restart the data import.

To start and stop import for the Model Import Connector for RepSM:

1 Select the Model Import Connector for RepSM and right-click.

2 Select **Send Command > Model Import Connector > Start** or **Stop.**

Optional - Reloading RepSM Data

To reload RepSM data:

1 If active, stop the connector.

2 Remove all files at:
Linux - `~/ARCSIGHT_HOME/current/user/agent/agentdata`
Windows - `$\ARCSIGHT_HOME\current\user\agent\agentdata`

3 Remove all folders and XML files (if any) at:
Linux - `~/ARCSIGHT_HOME/current/user/agent/mic/repdv`
Windows - `$\ARCSIGHT_HOME\current\user\agent\mic\repdv`

4 At the ArcSight Console, clear all entries in the Malicious Domains and Malicious IP Addresses Active Lists. For each Active List:

a Under **Reputation Security Monitor**, select the **Malicious Domains** and/or the **Malicious IP Addresses Active List** and right-click.

b Select **Clear Entries**.

5 Restart the connector.

Optional - Optimization of Data Transfer Using a Timer

The time interval between archives sent by the connector to ESM can be controlled by the `buildmodeldelay` property. The default value is 1 minute.

To increase or decrease this time interval, you can add the `buildmodeldelay` property to the file `agent.properties` (located at `$ARCSIGHT_HOME\current\user\agent`). The property `buildmodeldelay` is expressed in milliseconds.

For example, the following property sets the time interval to 10 seconds:

```
agent.component[35].buildmodeldelay=10000
```