Hewlett Packard
Enterprise

HPE Security ArcSight Model Import Connector for RepSM Plus

Software Version: 7.3.0.7954.0

Configuration Guide

November 7, 2016

Legal Notices

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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Model Import Connector for RepSM Plus

This guide describes installing the Model Import Connector for HPE Security ArcSight Reputation Security Monitor Plus (RepSM Plus) and configuring the device for data collection.

The HPE RepSM Plus solution uses internet reputation data to provide a list of known bad or harmful domains of IP addresses to provide context to security events. The Model Import Connector for RepSM Plus is a component of RepSM Plus which retrieves reputation data from the RepSM Plus threat intelligence service , 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 Plus 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 HPE Reputation Security Monitor Solution Guide.

Features and Functional Summary

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

The connector only sends the delta information from the last retrieved data to the ESM.

These entries are:

- IPv4 addresses
- Host and domain names

For each entry these reputation attributes are retrieved:

- Reputation Score
- Exploit Type

The initial import happens when the connector is started for the first time and the initial import command is issued from the ESM console. Following the initial load of the entries, the connector checks for updates, by default, every two hours. With the data from this query, the connector will process the deltas to add or delete the entries or update the threat scores as required and sends this information to the ESM.

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.
- 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.

  Note: When installing the model import connector as a service (and as a non-root user), run this command:

  ```
  $ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u user -sn <service_name>
  ```

Model Import Connector Installation

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

Note: Use a non-root account to install the Model Import Connector for RepSM Plus.

To install the Model Import Connector for RepSM Plus:

1. Download the Model Import Connector for RepSM Plus installation executable using the link provided in the e-mail sent to you by HPE.
2. Start the connector installer by running the executable.

   Note: The Model Import Connector for RepSM Plus 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...

3. Select **Add a Connector**.
4. **Model Import Connector for RepSM Plus** is already selected. Click **Next**.
5. Enter the required parameters to configure the connector, then click **Next**.

Parameter	Description
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.

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

8. 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.
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" below.
15. Set up the Model Import user in ESM. See "Setting up the Model Import User in ESM" on the next page.
16. Start the data import. See "Starting and Stopping Data Import" on page 9.

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 Plus, 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 Plus Configuration Using the ArcSight Console

There are mandatory and optional administrative tasks. "Setting up the Model Import User in ESM" below and "Starting and Stopping Data Import" on the next page are mandatory steps for connector installation, and are mentioned as part of the installation procedure. See "Installing the Connector" on page 5 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 Plus Data" on the next page and "Optional - Optimization of Data Transfer Using a Timer" on the next page 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 Plus**.
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**.

   Note: 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.

Note: 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 Plus:

1. Select the Model Import Connector for RepSM Plus and right-click.
2. Select **Send Command > Model Import Connector > Start** or **Stop.**

Optional - Reloading RepSM Plus Data

To reload RepSM Plus data:

1. If active, stop the connector.
2. Remove all files at:
   Linux - `~/ARCSIGHT_HOME/current/user/agent/agentdata`
   Windows - `$\ARCSIGHT_HOME\current\user\agent\agentdata`
3. Remove all folders and XML files (if any) at:
   Linux - `~/ARCSIGHT_HOME/current/user/agent/mic/repsm`
   Windows - `$\ARCSIGHT_HOME\current\user\agent\mic\repsm`
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
```

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide (Model Import Connector for RepSM Plus 7.3.0.7954.0)

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 arc-doc@hpe.com.

We appreciate your feedback!