Micro Focus Security
ArcSight Malware Information Sharing Platform Solution

Software Version: 7.14.0.8248.0

Model Import Connector

Document Release Date: December 9, 2019

Software Release Date: December 9, 2019

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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:

ArcSight Product Documentation on the Micro Focus Security Community

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

Contents

Product Overview

The Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution) uses Threat Intelligence to detect Advance Persistent Threats, Ransomware, Phishing, Botnets and Cryptojacking. as well as provide context to security events. The Model Import Connector for MISP (Malware Information Sharing Platform Solution) is a component which retrieves Threat Intelligence from the MISP (Open Source Threat Intelligence and Sharing Platform) instance, processes this data, and forwards it to ArcSight ESM.

Model Import Connector for MISP (Malware Information Sharing Platform Solution)

This guide describes installing the Model Import Connector for MISP (Malware Information Sharing Platform Solution) and configuring the device for data collection.

The Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution) uses Threat Intelligence to provide known bad of harmful domains, IP addresses, emails, hash values, and URLs to provide context to security events. The Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution) is a component which retrieves Threat Intelligence from the MISP (Open Source Threat Intelligence and Sharing Platform) instance, processes this data, and forwards it to ArcSight 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 connector as a Linux daemon, run the following command as root. and ensure the -u parameter is a non-root user:
>
> ```
> $ARCSIGHT_HOME/current/bin/arcsight agentsvc -i -u user -sn <service_name>
> ```

- The Threat Intelligence Platform package, in /All Packages/ArcSight Foundation/Threat Intelligence Platform is installed.

Model Import Connector Installation

This section provides instructions on how to install the Model Import Connector for MISP (Malware Information Sharing Platform Solution).

> **Note:** Use a non-root account to install the Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution).

To install the Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution)

1. Download the Model Import Connector for MISP (Malware Information Sharing Platform Solution) installation executable using the link provided in the e-mail sent to you by Micro Focus.
2. Start the connector installer by running the executable.

   > **Note:** The **Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution)** 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. **Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution)** is already selected. Click **Next**.
5. Enter the required parameters to configure the connector, then click **Next**.

Parameter Name	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. Proceed with the proxy configuration: Enter the proxy host IP address.
Proxy Port	Enter the proxy port.
Proxy User Name	Enter the proxy user name. This value is populated when the proxy requires an authentication. **Note**: If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password of the proxy user. This value is populated when the proxy requires an authentication and if you have specified a proxy user name.
MISP URL	Enter the Model Import Connector for MISP (Malware Information Sharing Platform Solution) instance url.
Authorization Key	Enter the authorization key. To obtain the authorization key: a. Log in to the GUI of the Model Import Connector for MISP (Malware Information Sharing Platform Solution) instance. b. Go to Event Actions/Automation. c. Get the authorization key.

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.

If you are installing the MISP connector in FIPS mode:

a. Run the connector install up to the connector framework step and cancel the installation.

   The connector install may be resumed using the `runagentsetup` script.

b. Export the MISP Instance certificate from the browser as a DER encoded binary x.509 (.CER) file.

c. Import the MISP Instance exported certificate into the connector framework FIPS keystore, using a command similar to the example below (run the command from the connector current directory):

```
jre/bin/keytool -importcert -file /opt/arcsight/misp.cer -keystore
"user/agent/fips/bcfips_ks" -storepass changeit -storetype BCFKS -
providername BCFIPS -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"lib/agent/fips/bc-fips-1.0.0.jar" -J-
Djava.security.egd=file:/dev/urandom -alias MispConn
```

d. Complete the connector install by running `../current/bin/runagentsetup`.

   The file extensions are:

   For Linux —.sh

   For Windows —.bat

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

    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**.

11. 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.

    If the connector is run in standalone mode, the default heap size is 256MB. For proper operation of the connector, Micro Focus 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.

12. Increase the java heap memory for the connector by doing the following (ARCSIGHT_HOME represents the name of the directory where the connector is installed):

    a. If you running the connector as a Windows service or Linux daemon , set the heap size in the following file:`~../current/user/agent.wrapper.conf`

       Set the following parameters:

```
#Initial Java Heap Size (in MB)
wrapper.java.initmemory=2048
#Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=2048
```

    b. If you are going to run the connector as Standalone mode:

   i. 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 "
```

   ii. For Windows - create the following batch file:

```
$ARCSIGHT_HOME\current\user\agent\setmem.bat
```

   with the following content:

```
SET ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx2048m
```

   Use regular double quote characters in the file content in either the shell script or the batch file.

13. 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.
14. Set up the Model Import user in ESM. See Setting up the Model Import User in ESM.
15. Start the data import. See Starting and Stopping Data Import.

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 **Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution)**.
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.

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 as standalone mode, to run the connector 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 the connector, enter `Ctrl+C` in the command window.

> **Note**: By default, the connector collects events starting one month prior to the installation day. This parameter can be changed by modifying the `start.date` field in the `../current/user/agent/agent.properties` file. The format of the field is `YYYY-MM-DD`. The connector can only collect up to 6 months from the installation date. If the `start.date` set, is a period longer than 6 months, the default time of one month will be used. The MISP Instance timezone is defined in the PHP.ini file on the MISP Instance host.

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 MISP (Malware Information Sharing Platform Solution):

1. Select the **Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution)** and right-click.
2. Select **Send Command > Model Import Connector > Start** or **Stop**.

Administrative Tasks - Malware Information Sharing Platform Solution Using the ArcSight Console

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

Features and Functional Summary

The Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution) retrieves Threat Intelligence and forwards it to ESM. This connector supports one ESM destination.

This connector supports one ESM destination.

These entries are:

- IP addresses
- Domains name
- Emails
- Hash values
- URLs

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
```

Optional - Reloading Model Import Connector for MISP (Malware Information Sharing Platform Solution) Data

To reload Model Import Connector for MISP (Malware Information Sharing Platform Solution)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. At the ArcSight Console, clear all entries in the Suspicious Domain List, Suspicious Email List, Suspicious Hash List and Suspicious URL List. For each Active List:
   a. Under **Threat Intelligence Platform**, select the, **Suspicious Domain List**, **Suspicious Addresses List**, **Suspicious Email List**, **Suspicious Hash List** and/ or the **Suspicious URL List** and right-click.
   b. Select **Clear Entries**.
4. Restart the connector.

Connector Upgrade

To upgrade the Micro Focus Model Import Connector for MISP (Malware Information Sharing Platform Solution), 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.

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 Model Import Connector (Malware Information Sharing Platform Solution 7.14.0.8248.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!