FMC Rapid 7 Host Input Connector

Operations Guide

July 8, 2020

Version 1.0

Cisco Systems, Inc.
Corporate Headquarters
170 West Tasman Drive
San Jose, CA 95134-1706 USA
http://www.cisco.com
Tel: 408 526-4000 Toll Free: 800 553-NETS (6387)
Fax: 408 526-4100

Contents

About This FMC Rapid 7 Host Input Connector Operations Guide

Change Authority	Cisco Customer Experience
Project ID	928887

Document Conventions

Alerts readers to take note. Notes contain helpful suggestions or references to material not covered in the document.

Alerts readers to be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Alerts readers of a situation that could cause bodily injury. They need to be aware of the hazards involved with electrical circuitry and familiarize themselves with standard practices for preventing accidents.

Alerts the reader that they can save time by performing the action described in the paragraph affixed to this icon.

Alerts the reader that the information affixed to this icon will help them solve a problem. The information might not be troubleshooting or even an action, but it could be useful information similar to a Timesaver.

1 Overview

This document provides installation, configuration and execution instructions for the FMC Rapid 7 Host Input Connector application (the “Application”).

2 Background

Rapid 7 is a third-party vendor providing security intelligence and vulnerability management data. Certain Cisco customers leverage Rapid 7's vulnerability data and insights to manage the risks facing assets on their networks. Such customers desire a tool to import Rapid 7 vulnerability data directly into their Firepower Management Center (FMC) dashboards to enhance their network visibility and risk management postures. The Application provides such a solution.

3 Application Summary

The Application is a Python and Perl command-line tool. There is no graphical user interface.

3.1 Pre-requisites

Components	Version
Linux or MacOS host	Post-2016 Release
Python	3.6+
Perl	5.16+ Note: Depending on the Application host's Perl installation, the Perl modules: `YAML::XS` and `IO::Socket::SSL` may additionally need to be installed.
Rapid 7 API	Cloud API (Version 4)
Firepower Management Center (FMC)	6.6+

Table 1 - Application Pre-Requisites

The application will require:

1. Access to the Rapid 7 Cloud API (Version 4);
2. Access to the FMC instance; and
3. A FMC-generated certificate as described in Section 3.3 below.

3.2 Installation

The Application package contains one file: `fmcRapid7HostInputConnector.zip` (the "Application files"). The `fmcRapid7HostInputConnector.zip` file may of course be moved to the directory of your choice. In this example, we are using a directory called `fmcConnectorLinuxTest` which is referred to as the "root" directory.

Now, unzip the Application files (in the same directory) using `unzip fmcRapid7HostInputConnector.zip`. The following directory structure should be visible via the `ls -l` command as shown in Figure 1 below:

```
unzip fmcRapid7HostInputConnector.zip
ls -l
```

```
[root@localhost fmcConnectorLinuxTest]# ls -l
total 40
drwxr-xr-x. 2 root root  4096 Jul  8 11:34 connector
-rw-r--r--. 1 root root 21257 Jul  7 14:38 fmcRapid7HostInputConnector.zip
drwxr-xr-x. 2 root root   145 Jul  8 11:34 HostInputApi
-rwxr-xr-x. 1 root root    26 Jul  7 11:10 HostInputConnector
drwxr-xr-x. 2 root root    53 Jul  8 11:34 InputPlugins
-rw-r--r--. 1 root root    17 Jul  7 14:28 requirements.txt
-rw-r--r--. 1 root root   565 Jul  7 11:10 settings.ini.default
[root@localhost fmcConnectorLinuxTest]#
```

Figure 1 - Contents of the zip file

Please also note the `requirements.txt` file provided for Python dependencies that are not part of the Python standard library. To install the needed dependencies, please execute the following:

```
pip3 install -r requirements.txt
```

Note that the Python `pip` module may be aliased to `pip` or some other alias on the host system instead of `pip3`. Please ensure you are using the pip module associated with the Python 3 distribution installed on the host machine. Please consider using the `--user` flag to install Python dependencies or the use of a virtual environment as is appropriate for the host environment.

3.3 FMC Configuration

Before running the Application, a certificate must be generated from the FMC for the Application host. This will enable the Application to interface with the FMC's Host Input API and import data into the FMC instance. Please complete the following steps:

- Login to the Firepower Management Center
- Navigate to "System" and "Integration"
- Click the tab for "Host Input Client"
- Select "Create Client" in the top right corner as shown in Figure 2 below:

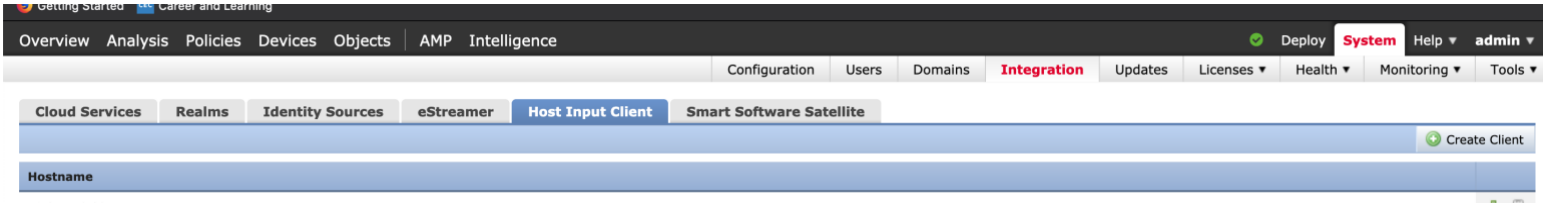

Figure 2 – FMC Host Input Client tab

- In the “Create Client” dialogue box, enter the Application’s host’s IP address and click “Save”.

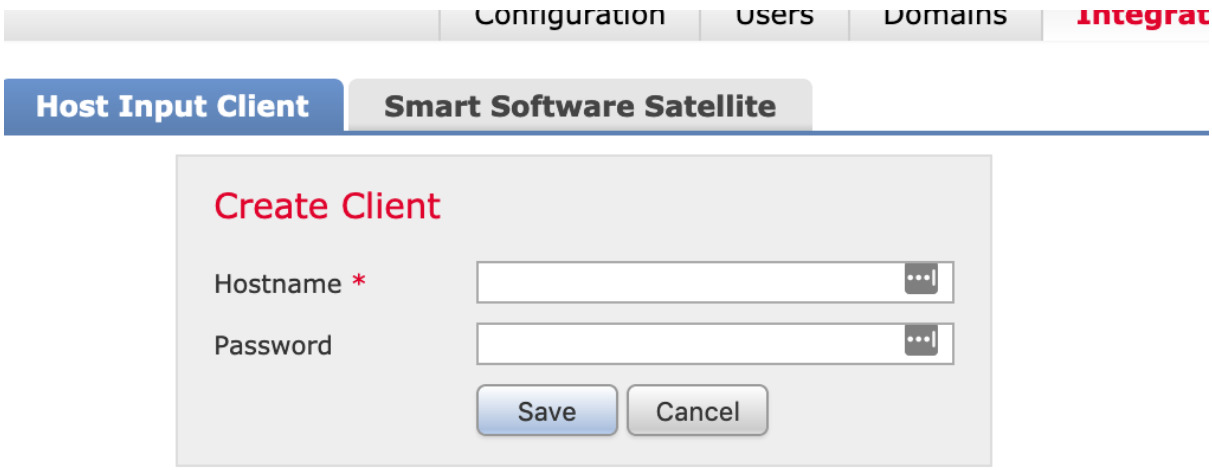

Figure 3 – Host Input Client Create Client dialogue

- Back on the main menu the Application host should now be listed. Select the green Download button for your Application host to download the certificate.

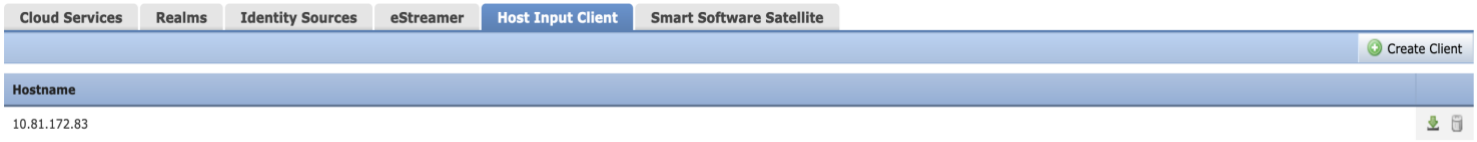

Figure 4 – Application host certificate download

- Place the downloaded certificate (a `pkcs12` file) into the root directory as described in Section 4.1 below.

4 Operations

4.1 Properties Configuration

The Application is configured through the `settings.ini.default` file in the root directory. The file must be renamed `settings.ini`. Additionally, the `*.pkcs12` file described in Section 3.3 should be placed in the root directory as shown in Figure 5 below:

```
[root@localhost fmcConnectorLinuxTest]# ls -l
total 44
-rw-r--r--. 1 root root  3521 Jul  7 20:28 10.122.109.212_10.pkcs12
drwxr-xr-x. 2 root root  4096 Jul  8 11:34 connector
-rw-r--r--. 1 root root 21257 Jul  7 14:38 fmcRapid7HostInputConnector.zip
drwxr-xr-x. 2 root root   145 Jul  8 11:34 HostInputApi
-rwxr-xr-x. 1 root root    26 Jul  7 11:10 HostInputConnector
drwxr-xr-x. 2 root root    53 Jul  8 11:34 InputPlugins
-rw-r--r--. 1 root root    17 Jul  7 14:28 requirements.txt
-rw-r--r--. 1 root root   643 Jul  7 20:55 settings.ini
[root@localhost fmcConnectorLinuxTest]#
```

Figure 5 - Directory structure with renamed settings.ini and *.pkcs12 file

The `settings.ini` parameters are set forth below:

Section		
[RAPID7_SETTINGS]		
Key		Description
1	api_key	Rapid 7 API-Key.
2	rapid7_url	Rapid 7 URL.
3	health_check_endpoint	Rapid 7 API endpoint used to check whether the Rapid 7 API is up and available. This should not need to be changed from the default setting.
4	asset_endpoint	Rapid 7 API endpoint used to retrieve assets (hosts) scanned by Rapid 7. This should not need to be changed from the default setting.
5	vuln_endpoint	Rapid 7 API endpoint used to retrieve vulnerability details for a given vulnerability affecting a network asset (host). This should not need to be changed from the default setting.
6	vuln_types	Specifies the types of vulnerabilities to be checked and processed from the Rapid 7 asset API endpoint response. Please take precaution before altering.

7	last_scan_read	This is the last time the Rapid 7 asset API was successfully queried. Please see the notes section below for usage details.
[FMC_SETTINGS]		
Key		Description
8	fmc_ipaddress	IP address of the user's FMC instance into which Rapid 7 API vulnerability information will be imported.
9	debug	If set to `true`, will produce more verbose output when Rapid 7 data is imported into the FMC instance.
[CSV_FILE_SETTINGS]		
Key		Description
10	csv_directory	Path to the directory into which the Application will write Host Input CSV files. If this directory does not already exist, the Application will create it. Recommend using a directory under the root directory, e.g., `csv_directory = ./csv_files`
[LOG_SETTINGS]		
Key		Description
11	log_file	Log file name. The log file will be available in the "connector" subdirectory. This may be customized as desired.
12	log_format	Python LogRecord attributes. These may be customized as desired.
13	log_level	DEBUG, INFO, WARNING, ERROR, CRITICAL. This may be customized as desired.
14	file_handler_level	DEBUG, INFO, WARNING, ERROR, CRITICAL. Should match the value for the log_level attribute.
15	mode	"w" for write to overwrite the existing log_file on each run of the Application or "a" to append log output to the existing log_file.

Table 2 - Key configuration parameters

The `api_key` and `fmc_ipaddress` are the only two keys that *require* customization for Application operation. A Rapid 7 API-Key may be procured via logging into a Rapid 7 account, navigating to `Settings` → `API-Keys` and selecting an API-Key with appropriate permissions (i.e., Read-only). For more details (including screenshots) of the API-Key procurement process, please consult the following resource: https://insightops.help.rapid7.com/docs/api-keys.

Additionally, the `last_scan_read` key determines whether the Application will request *all* assets and associated vulnerability data corresponding to the configured `api_key` value from the Rapid 7 asset API endpoint or only those assets scanned after a configured date (in UTC format). The `last_scan_read` key is initially configured to 0 and, accordingly, on the first run of the Application all assets and related data associated with the configured `api_key` will be queried from the Rapid 7 API. The Application will also write the time the API query started to the `last_scan_read` field so that, unless manually re-set to 0, the next time the Application runs only those assets that were scanned after the `last_time_read` timestamp will be queried.

4.2 Execution

The Application is launched directly from the command line. Execute the following from the root directory:

```
./HostInputConnector
```

Please note that `./HostInputConnector` is a wrapper around the following (and underlying) Python 3 invocation `python3 ./connector/run.py` and that the host system may have the Python 3 installation aliased to just `python` or some other alias. It is only necessary that Python 3 is invoked. Upon execution the console will display that the Application has started and provide milestone updates as shown in Figure 6 below.

```
[root@localhost fmcConnectorLinuxTest]# ./HostInputConnector
./csv_files
Host Input Connector 0.1 started.
Application logfile is available at connector/application.log.
Retrieving Asset pages from Rapid 7 for assets scanned after 2020-06-23T21:06:24.713Z.
Asset pages received from Rapid 7 for assets scanned after 2020-06-23T21:06:24.713Z.
List of Hosts and associated vulnerabilities generated for assets scanned after 2020-06-23T21:06:24.713Z.
Host Input Connector finished.
[root@localhost fmcConnectorLinuxTest]#
```

Figure 6 – Application launch and progress updates

Further note that the Application created the configured csv_directory under the root directory at `./csv_files`. The Host Input CSV file created by the Application will be retained and available for inspection until the next run of the Application. Additionally, please further note the creation of the log files application.log and hostInput.log all as shown in Figure 7 below:

```
[root@localhost fmcConnectorLinuxTest]# ls -l csv_files/
total 88
-rw-r--r--. 1 root root 87346 Jul  8 14:52 host_input.csv
```

```
[root@localhost fmcConnectorLinuxTest]# ls -l
total 52
-rw-r--r--. 1 root root  3521 Jul  7 20:28 10.122.109.212_10.pkcs12
-rw-r--r--. 1 root root  2257 Jul  8 14:52 application.log
drwxr-xr-x. 3 root root  4096 Jul  8 14:44 connector
drwxr-xr-x. 2 root root    28 Jul  8 14:52 csv_files
-rw-r--r--. 1 root root 21257 Jul  7 14:38 fmcRapid7HostInputConnector.zip
drwxr-xr-x. 2 root root   145 Jul  8 11:34 HostInputApi
-rwxr-xr-x. 1 root root    26 Jul  7 11:10 HostInputConnector
-rw-r--r--. 1 root root  1832 Jul  8 14:52 hostInput.log
drwxr-xr-x. 2 root root    53 Jul  8 11:34 InputPlugins
-rw-r--r--. 1 root root    17 Jul  7 14:28 requirements.txt
-rw-r--r--. 1 root root   643 Jul  8 14:52 settings.ini
[root@localhost fmcConnectorLinuxTest]#
```

Figure 7 – Host Input CSV directory and log file creation

4.3 Logging

The application has a log file named `application.log` (or as otherwise configured via the `log_file` configuration key). Additionally, the application creates a log file named `hostInput.log` that captures output from the FMC's Host Input API when data is imported into the FMC. The log files may be consulted to help troubleshoot issues.

5 Troubleshooting

5.1 FMC Certificate Placement May Give an Error

Issue: The following error is output to console:

```
subprocess.CalledProcessError: Command
'['./HostInputApi/sf_host_input_agent.pl',
'server=172.26.48.86', '-level=3', '-
plugininfo=0/host_input.csv', 'csv', '-
logfile=hostInput.log']' returned non-zero exit status 2.
```

And in `hostInput.log` the following `DEBUG` message appears:

```
Tue Jul  7 12:49:32 2020 [DEBUG] Setting up auth certificate
[/<path_to>/fmcConnectorTest/HostInputApi/SFHostInputAgent.pm
350]
```

or

```
SFPkcs12: Unable to automatically locate pkcs12 file
```

Solution/Workaround: The issue may be that the `*.pkcs12` file generated from the FMC is not present in the root directory. Please ensure the file is located in the root directory.

5.2 Unable to Read Underlying FMC Certificate

Issue: The following error is output to console as in 5.1 above:

```
subprocess.CalledProcessError: Command
'['./HostInputApi/sf_host_input_agent.pl',
'server=172.26.48.86', '-level=3', '-
plugininfo=0/host_input.csv', 'csv', '-
logfile=hostInput.log']' returned non-zero exit status 2.
```

And the following appears in `hostInput.log`:

```
SFPkcs12: Unable to get certificate
```

Solution/Workaround: There may be an issue with the underlying `*.pkcs12` certificate itself. A possible workaround is to regenerate the certificate from the FMC and attempt to re-launch the Application using the new certificate.

6 Known Issues

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THIRD PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.