FIREEYE HEALTH CHECK TOOL

VERSION 3.0

FireEye, Inc. | 601 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

CONTENTS

OVERVIEW

FireEye Health Check Tool is a standalone agent that allows customers to collect health-related information from their cloud and on-premises FireEye appliances. The agent will run configuration and metric collections against FireEye appliances and provide an automated report detailing the health findings of the appliances based on predefined conditions of Hardware, System, Configuration, Detection and Best Practices health. The intent is to provide the status of the assessed systems and self-help recommendations for any issues identified by the FireEye Health Check Tool.

SUPPORTED PLATFORMS

The Health Check Agent is supported to be executed from Windows, Mac OSX and Linux CentOS 7 and Ubuntu 16.4.

Supported FireEye platforms to perform Health Check against includes the following:

- Helix – Cloud Threat Analytics
- Endpoint Security – HX, HX DMZ
- Network Security – NX, VX
- Email Security – EX
- Management – CMS
- Content – FX
- Analysis - AX

EXECUTABLE CHECKSUMS

MAC OS

Size: 12 MB

Date: Fri Oct 11 09:16:56 2019

MD5 : 747241c4b3df16e40a87d1399e40135f

SHA1: 4a990d1be89bb7f9c5be35b0b8503238fd781c0c

Linux

Size: 19 MB

Date: Fri Oct 11 08:55:40 2019

MD5 : cbffaab169cec841a2aab6acaa97be9d

SHA1: 3acb0bc621a65e0a7cc49c0c37a28e60dffd037b

Windows

Size: 16 MB

Date: Fri Oct 11 09:01:28 2019

MD5 : a423727ea5e4e9f6b05ac33b87015a1f

SHA1: 096194a4d3eda9558ceb174e7eafcff983a9655c

NEW IN VERSION 3.0

UNIFIED HTML REPORTING

Based feedback from customers, the reporting has been completely overhauled. The Docx reporting has been replaced by HTML reporting and now features a much-improved look and feel. Additionally, execution runs that are made against multiple appliances specified manually or by using config mode are now unified in the single consolidated HTML report.

SPEED IMPROVEMENTS

Windows execution averages a ~163% performance gain, and Linux and OSX an average of ~133%. Full execution against any size mixed mode fleet now take under a minute to complete.

CREDENTIAL & EULA CASHING

After the initial EULA acceptance and successful Okta authentication the credential state is cached removing the need to reauthenticate during each subsequent run.

CREATE CONFIG OPTION

Manually executed runs can now be saved to a config file that saves the username, encrypted password, targets, execution mode and any other parameters stored in the `config` folder. The config file can then be recalled by passing the path to the config file using the `-c/--config` parameter to the tool.

The tool will parse the config, run collection and generate reports without any additional user input being required.

Multiple configs can be manually merged into a single config for consolidated reports against an entire fleet of appliances including mixed modes.

EXIT CODES

The now tool returns standard system exit codes after execution:

- 0 - Program successfully completed
- 1 - Program encountered an issue during execution

UNATTENDED EXECUTION

The combination of credential and EULA caching, use of config files and exit codes facilitate the execution of the tool in an unattended fashion with your preferred scheduler.

IMPROVED FEEDBACK DURING EXECUTION

A new feedback cue system provides status information during the initial execution stages of the tool.

CRASH REPORTS

If a non-recoverable issue is encountered during execution, a crash report file is generated in the `crash` folder. These crash files can be used by the D&I Tech Team to identify and troubleshoot the cause and implement a fix in a future release.

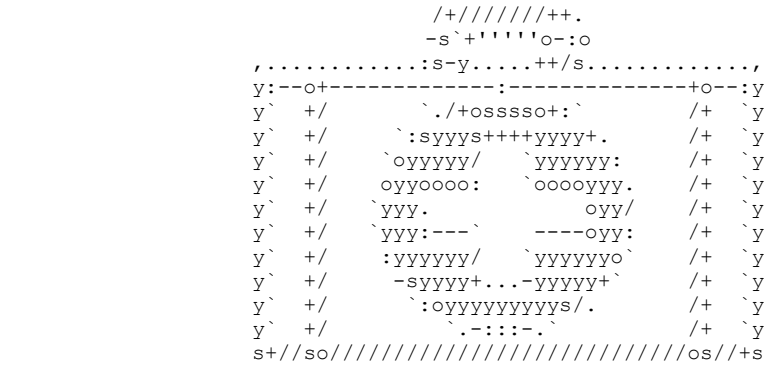
BREAKING CHANGES

ENCRYPTED PASSWORDS IN CONFIGURATION FILES

Version 3.0 uses a complexly new encryption backend. The new implementation is not backwards compatible with previously encrypted passwords used in config files, and will require being regenerated using the `-e` argument.

USAGE

```
C:\>fe_hca.exe -h
```



```
                      FireEye Health Check Agent - v3.0

usage: fe_hca.exe [-h] [-e] [-c CONFIG] [-cc] [-m MODE] [-s] [-T TIMEOUT] [-S]
                  [-v] [-u USERNAME] [-t TARGET] [-f FILE] [-ak APIKEY]

Automated health check reports for FireEye solutions.

optional arguments:
  -h, --help            show this help message and exit
  -e, --encrypt         Encrypt a password for use in storing in config files.
                        Prompts for password interactively.
  -c CONFIG, --config CONFIG
                        Configuration file containing hosts. Used for
                        conducting single runs against multiple hosts that
                        have different passwords or scheduled executions.
  -cc, --createconfig   Create a configuration file based on the current run
                        paramaters. Experimental.
  -m MODE, --mode MODE  Operation mode. Supported options are appliance
                        (default), helix & fso. Note: Appliance mode is used
                        for both physical and virtual appliances.
  -s, --sslcheckoverride
                        Override the SSL check if an SSL Intercept solution
                        isin use and having SSL certificate verification to
                        fail. Note: Only use this if you are certain on why
                        certificate checks are failing
  -T TIMEOUT, --timeout TIMEOUT
                        Connection timeout in seconds. Default is 5.
  -S, --statistics      Display execution statistics.
  -v, --version         Display full version and exit.
  -u USERNAME, --username USERNAME
                        Username to use for target appliance. Admin level user
                        required. If not provided, you will be prompted.
  -t TARGET, --target TARGET
                        IP or hostname of target appliance. Multiple hosts can
                        be specified separated by , between targets. If not
                        provided and --file not specified, you will be
                        prompted.
  -f FILE, --file FILE  File to read target hostnames or IPs from. One
                        hostname/IP specified per line.
  -ak APIKEY, --apikey APIKEY
                        API key. Only used with --mode helix. If not provided,
                        you will be prompted.
```

HELP

When FE_HCA is executed without any arguments, or `-h` or `--help` is specified, the default usage is displayed

TARGET

Target hosts for data collection can be specified directly. A single host can be provided, or optionally, multiple hosts separated by a comma, e.g.; `192.168.1.150,10.1.1.39`

Helix instances are also addressed using target by specifying the instance name, e.g.: `hexabc123`

USERNAME

Username for the appliance. This should be a user with admin credentials on the appliance to facilitate complete configuration collection. Collection from the use of a non-admin account is not supported.

Note: Helix reporting uses an API key instead of usernames.

FILE

A file that contains a list of target hosts to be assessed, each specified on its own line, can be provided. This is useful for large deployments.

ENCRYPT

Encrypt password / API key to be saved in a configuration file. Only encrypted passwords are supported in configuration files. Encrypted passwords can only be used on the same host that the agent is being run from. If the configuration file and moved to another system and used with a configuration file, the passwords / API keys need to be re-encrypted.

CONFIGURATION FILE

An INI style file that contains a list of target hosts with accompanying authentication credentials that can be stored for simple reuse. This can be used to run against Helix, cloud, virtual and on-premise appliances in a single execution. The two primary modes of operation are “appliance” for on-premises and cloud hosted appliances (such as CMS, HX, NX, FX and AX), and “helix” for Cloud Threat Analytics Platform. This option may also assist with conducting a single execution against multiple hosts that have different accounts and passwords. This is useful for large deployments. Example config:

```
[appliance_set_1]
mode:appliance
username:account1
```

```
password:<encrypted password generated with '-e'>
target: 10.11.3.8,172.168.2.155,192.168.1.98,axhost.localdomain

[appliance_set_2]
mode:appliance
username:account2
password:<encrypted password generated with '-e'>
target:10.11.1.5,172.168.1.150,192.168.1.96,hxprimary.otherdomain


[helix_set_1]
mode:helix
apikey:<encrypted api key generated with '-e'>
target:hexabc123
```

CREATE CONFIGURATION

Using create configuration will automatically create a config file in the `config` folder in the same folder in which the agent is located dynamically named based on the mode and date. This file can then be referenced with the config argument execute the agent without having to manually specify any parameters.

Passwords provided at run time are securely encrypted and stored in the config file.

STATISTICS

Provides statistics on the execution of the agent.

TIMEOUT

Enables a custom timeout window in seconds. Typically used to accommodate connections with latency such as cloud appliances. Default timeout window is five seconds.

MODE

Operation mode. Supported options are `appliance` (default), `helix` & `fso`. Note: Appliance mode is used for both physical, virtual and cloud appliances. Only one Mode can be executed at a time. Ex. Helix mode must be run separately from FSO mode, and Appliance mode must be run separately when the agent is being executed without the use of a config file.

API KEY

Provides the parameter to enter in the API key required to query the Helix API when running the Helix mode reporting.

Note: When using the api key argument, the api key will be visible in the command / shell history. The argument can be omitted and you will be prompted to enter the api key at run time which is recommended.

SSL CHECK OVERRIDE

Override the SSL check if an SSL Intercept solution is in use and having SSL certificate verification to fail. Note: Only use this if you are certain on why certificate checks are failing.

EXECUTION

The following examples demonstrate executing the agent in different scenarios.

Note: Device addresses, credentials and file names need to be substituted with your own.

APPLIANCE EXAMPLE

Execution:

```
fe_hca.exe -u username -t 10.10.11.4
```

CLOUD APPLIANCE EXAMPLE USING A LONGER TIMEOUT

Execution:

```
fe_hca.exe -u username -t hexabc123-hx-ssh-1.hex01.helix.apps.fireeye.com -T
10
```

APPLIANCE EXAMPLE SPECIFYING MULTIPLE TARGETS

Execution:

```
fe_hca.exe -u username -t 10.10.11.4,10.10.11.5
```

APPLIANCE EXAMPLE USING HOSTS SPECIFIED IN A FILE

Appliances.txt contents:

```
10.10.11.4
```

```
10.10.11.5
```

Execution:

```
fe_hca.exe -u username -f Appliances.txt
```

HELIX EXAMPLE

Execution:

```
fe_hca.exe --mode helix -t hexabc123
```

CREATE CONFIG EXAMPLE

Execution:

```
fe_hca.exe --mode helix -t hexabc123 -cc
```

Contents of `config\helix_290919T164917.cfg` file created in config folder:

```
[helix_290919T164917]
mode:helix
target:,hexabc123,
apikey:<encrypted_api_key>
```

USING A CONFIG EXAMPLE

Execution:

```
fe_hca.exe -c config\helix_290919T164917.cfg
```

BEHAVIORS

PASSWORD ENCRYPTION

Passwords and are encrypted using attributes that are unique to the machine that the they were generated on. If a config file containing passwords is moved to a new machine, decryption will fail and need to be regenerated on the system that the agent will be run on.

USERNAMES, PASSWORDS AND API KEYS

In the event that `-username`, `--password` or `-apikey` is not specified on the command line, the agent will prompt for those at execution time. If there is a concern about having any of these credentials exposed on the shell / command history is a concern, please do not specify these paramaters.

TARGETS AND FILES

In the event that neither `--target` nor `--file` is specified, the agent starts in an interactive mode where target hosts can be specified.

REPORTS

Reports are generated automatically and output customized based on the appliance that was detected at run time. Reports can be found in the `reports` folder in the same location where the agent is located.

ISSUES AND TROUBLESHOOTING

KNOWN ISSUES

- None at this time

CRASH REPORTS

Crash reports are generated and stored in the `crash` folder in the same location where the agent is located. These files are used for troubleshooting and debugging if an issue is encountered.

SUPPORT

This agent is not supported by FireEye Technical Support; however, bugs can be reported to FireEye Technical Support. A JIRA will need to be filed to address any bugs that require correction, or feature enhancement.

Phone:

1-877-FIREEYE

Email:

Support@fireeye.com

Web:

https://www.fireeye.com/support/contacts.html