FIREEYE HEALTH CHECK TOOL

USER GUIDE

Version 3.2

FireEye assumes no responsibility for any inaccuracies in this document. FireEye reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Endpoint Security Policy API Tool

Software Release 0.9

FireEye Contact Information:

Website: www.fireeye.com

Technical Support: https://csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

CONTENTS

Overview 5

Supported Platforms 5

New in Version 3.2 6

PX Reporting 6

IA Reporting 6

Changes 6

Reporting 6

Breaking Changes 6

Usage 7

Options Descriptions 8

Help..8

Target..8

Username 8

File 8

Encrypt..8

Configuration File..9

Create Configuration..9

Statistics..9

Timeout 10

Mode 10

API Key..10

SSL Check Override 10

PDF Reports 10

Quiet Mode 10

Execution 11

Appliance Example 11

Cloud Appliance Example Using a Longer Timeout 11

Appliance Example Specifying Multiple Targets 11

Appliance example Using Hosts Specified in a File 11

Helix Example 11

Create Config Example 11

Using a Config Example 12

Using a Proxy Example 12

Using a SOCKS5 Proxy Example 12

Using a Proxy With Authentication Example 12

Using a Proxy For External Connections Only Example 12

Using A Proxy For Internal Connections Only Example 12

Quiet Example 13

PDF Reports Example 13

Behaviors 13

Password Encryption 13

Usernames, Passwords And API Keys 13

Targets and Files 13

Reports 13

External Ports & Protocols 14

Issues and Troubleshooting 14

Known Issues 14

Crash Reports 14

Support 14

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, PX, IA
- Email Security – EX
- Management – CMS
- Content – FX
- Analysis - AX

Executable Checksums

MAC OS

Size: 25 MB

Date: Tue Apr 28 11:10:06 2020

MD5 : f3fa793d6068230222eb13890a03cee2

SHA1: 82c0a721f914e805f93e425d8998c312d59df040

Linux

Size: 27 MB

Date: Tue Apr 28 10:51:20 2020

MD5 : 2d386709908cb08f4121cf559a15328b

SHA1: 9efac00910076be3b02f06857069bdbc4d820209

Windows

Size: 29 MB

Date: Tue Apr 28 10:54:40 2020

MD5 : be08ef923fec87a82f7c5cef68a79273

SHA1: 968e0add58ccbb05ae978b06baf68dff3111f058

NEW IN VERSION 3.2

PX REPORTING

PX reporting is now supported through the `--mode px` argument. This requires a user that has the API role.

IA REPORTING

IA reporting is now supported through the `--mode ia` argument. This requires a user that has the API role.

CHANGES

REPORTING

Checks and reports have been improved based on feedback.

BREAKING CHANGES

None

USAGE

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

                                  /+///////++.
                                 -s`+'''''o-:o
                    ,............:s-y.....++/s.............,
                    y:--o+-------------:--------------+o--:y
                    y`  +/       `./+osssso+:`        /+  `y
                    y`  +/     `:syyys++++yyyy+.      /+  `y
                    y`  +/    `oyyyyy#####yyyyyy:     /+  `y
                    y`  +/    oyyoooo#####ooooyyy.    /+  `y
                    y`  +/   `yyy#############oyy/    /+  `y
                    y`  +/   `yyy#############oyy:    /+  `y
                    y`  +/    :yyyyyy#####yyyyyyo`    /+  `y
                    y`  +/     -syyyy#####yyyyy+`     /+  `y
                    y`  +/      `:oyyyyyyyyys/.       /+  `y
                    y`  +/         `.-:::-.`          /+  `y
                    s+//so////////////////////////////os//+s

                       FireEye Health Check Agent - v3.2

usage: fe_hca [-h] [-e] [-c CONFIG] [-cc] [-m {appliance,helix,fso}] [-s]
              [-T TIMEOUT] [-S] [-v] [-q] [-P PROXY] [-PA]
              [-PM {all,internal,external}] [-rp] [-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   Experimental: Create a configuration file based on the
                        current run parameters.
  -m {appliance,helix,fso}, --mode {appliance,helix,fso,px,ia}
                        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
                        is in 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 10.
  -S, --statistics      Display execution statistics.
  -v, --version         Display full version and exit.
  -q, --quiet           Disable execution mode. Used for scheduled runs.
  -P PROXY, --proxy PROXY
                        Experimental: Proxy server: http://host:port. Socks5:
                        socks5://host:port.
  -PA, --proxyauth      Experimental: Prompt for proxy username and password
                        at runtime. Optionally cache encrypted proxy
                        credentials.
  -PM {all,internal,external}, --proxymode {all,internal,external}
                        Experimental: Use proxy settings for all, internal or
                        external connections. Default is all.
  -rp, --reportpdf      Experimental: Outputs report in PDF format.
  -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.

Detailed execution examples can be found in the documentation.
```

OPTIONS DESCRIPTIONS

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 and is dynamically named based on the mode and date. This file can then be referenced with the config argument to 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 or slow links. Default timeout window is 10 seconds.

MODE

Operation mode. Supported options are `appliance` (default), `helix`, `fso`, `px` & `ia`. 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.

PDF REPORTS

Experimental support for generating PDF reports is now available on Windows 10 64-bit systems with the `-rp/--reportpdf` argument.

PDF reporting depends on several libraries to be available OSX and Linux systems. To verify if your OSX or Linux system is capable of generating PDF reports, confirm with `fe_hca --help`. If the `-rp/--reportpdf` argument is displayed, then PDF report generation is available.

QUIET MODE

For unattended or timed executions through a scheduler, output can now be suppressed with the `-q/--quiet` argument.

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 -username username --target 10.10.11.4
```

CLOUD APPLIANCE EXAMPLE USING A LONGER TIMEOUT

Execution:

```
fe_hca.exe -username username -target hexabc123-hx-ssh-
1.hex01.helix.apps.fireeye.com --timeout 20
```

APPLIANCE EXAMPLE SPECIFYING MULTIPLE TARGETS

Execution:

```
fe_hca.exe -username username --target 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 --username username --file Appliances.txt
```

HELIX EXAMPLE

Execution:

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

CREATE CONFIG EXAMPLE

Execution:

```
fe_hca.exe --mode helix -target hexabc123 --createcconfig
```

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 --conig config\helix_290919T164917.cfg
```

USING A PROXY EXAMPLE

Execution:

```
fe_hca.exe --mode helix --target hexabc123 --proxy http://10.11.24.10:8080
```

USING A SOCKS5 PROXY EXAMPLE

Execution:

```
fe_hca.exe --mode helix --target hexabc123 --proxy socks5://10.11.24.10:8080
```

USING A PROXY WITH AUTHENTICATION EXAMPLE

Execution:

```
fe_hca.exe --mode helix --target hexabc123 --proxy http://10.11.24.10:8080 --
proxyauth
```

USING A PROXY FOR EXTERNAL CONNECTIONS ONLY EXAMPLE

Execution:

```
fe_hca.exe --mode helix --target hexabc123 --proxy http://10.11.24.10:8080 –
proxymode external
```

USING A PROXY FOR INTERNAL CONNECTIONS ONLY EXAMPLE

Execution:

```
fe_hca.exe --mode helix --target hexabc123 --proxy http://10.11.24.10:8080 --
proxymode internal
```

QUIET EXAMPLE

Execution:

```
fe_hca.exe –-mode helix --target hexabc123 --quiet
```

PDF REPORTS EXAMPLE

Execution:

```
fe_hca.exe –-mode helix --target hexabc123 –reportspdf
```

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 parameters.

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.

EXTERNAL PORTS & PROTOCOLS

Service	Description	Port	Protocol
healthcheck.fireeye.com	Update checks	443	TCP
fireeye.okta.com	Authentication	443	TCP
apps.fireeye.com	Helix API	443	TCP
***.hex01.helix.apps.fireeye.com**	Cloud appliances API	443	TCP
***.hex01.helix.apps.fireeye.com**	Cloud appliances SSH	22	TCP

ISSUES AND TROUBLESHOOTING

KNOWN ISSUES

- None at this time

CRASH REPORTS

Crash reports are generated and stored in the `crash` folder. 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