FIREEYE HEALTH CHECK TOOL

VERSION 2.0

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

TABLE OF 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: 12.0 MB

Date: Thu Jan 31 16:40:02 2019

MD5: 47967cd9350731fbae30e7c21a26b851

SHA1: 37820d0b1e36af9920d5b3e6c146d211938d7859

Linux

Size: 22.0 MB

Date: Thu Jan 31 16:33:01 2019

MD5: c4d0db515a3645d1a664d606ac1da38e

SHA1: 8d313234212fa8ce404268c7bea7309e02c45b9e

Windows

Size: 19.0 MB

Date: Thu Jan 31 16:19:19 2019

MD5: 55db296c9a58cae123d8e3ddec2987b2

SHA1: 912cf7e269b65f95faf49b5a1f25578900507b77

USAGE

```
c:\FEHCA>fe_hca.exe -h
default

                                /+///////++.
                               -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 - v2.0

usage: fe_hca.exe [-h] [-e] [-c CONFIG] [-m MODE] [-s] [-T TIMEOUT] [-S]
                  [-u USERNAME] [-t TARGET] [-f FILE] [-hi HELIXINSTANCE]
                  [-hk HELIXKEY]

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. 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 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 5.
  -S, --statistics      Display execution statistics.
  -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. 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 specified per line.
  -hi HELIXINSTANCE, --helixinstance HELIXINSTANCE
                        Helix instance identifier. Only used with --mode
                        helix. If not provided, you will be prompted.
  -hk HELIXKEY, --helixkey HELIXKEY
                        Helix 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`

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.

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 tool 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 reiencrypted.

CONFIGURATION FILE

An encrypted file that contains a list of target hosts with accompanying authentication credentials that can be stored for reuse. This can be used to run against Helix and on premesis appliances in a single execution. 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
helixkey:<encrypted api key generated with '-e'>
helixinstance:hexabc123
```

STATISTICS

Provides statistics on the execution of the agent.

REPORTS

Report generation. This flag should be used on execution to enable the report generation feature of this tool. Report generation is automated when this option is enabled.

TIMEOUT

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

MODE

Operation mode. Supported options are appliance (default), HELIX & FSO. Note: Appliance mode is used for both physical and virtual 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. This option can be avoided using the Configuration File option described above.

HELIX INSTANCE

Specifies the customer Helix instance ID to query for reporting pull.

HELIX KEY

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

SSL CHECK OVERRIDE

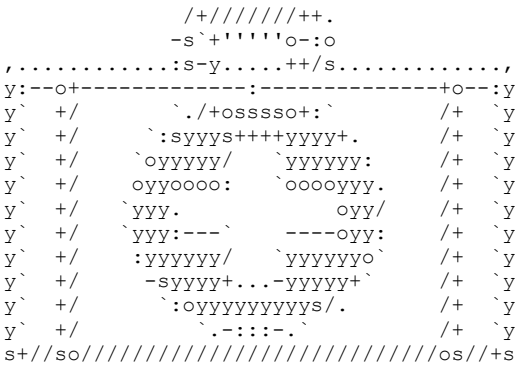
Override the SSL check if an SSL Intercept solution is in use and having SSL certificate verification to fail. Note: Only use this if you are certain on why certificate checks are failing.

EXECUTION

EXAMPLE

A typical execution of this agent for reporting on appliance health should resemble the following output. Device addresses and credentials will vary:

```
C:\>fe_hca.exe -r -f Appliances.txt -u user.name@company.com
```



```
   FireEye Health Check Agent - v2.0

FIREEYE HEALTH CHECK AGENT END USER LICENSE AGREEMENT
--------------------------------------------------------------------------------
Your use of this FireEye Health Check Agent tool is subject to the applicable terms found at:

    http://www.fireeye.com/company/legal

By running this tool, you confirm and acknowledge that you have read and agree to those terms
presented in the link above. If you do not agree to these terms, please exit and discontinue the
use of this tool.

All Intellectual Property Rights in FireEye Materials, Products, Deliverables, Documentation, and
Subscriptions belong exclusively to FireEye and its licensors. Customer will not (and will not
allow any third party to):

(i) disassemble, decompile, reverse compile, reverse engineer or attempt to discover any source
code or underlying ideas or algorithms of any FireEye Materials (except to the limited extent
that applicable law prohibits reverse engineering restrictions);
(ii) sell, resell, distribute, sublicense or otherwise transfer, the FireEye Materials, or make
the functionality of the FireEye Materials available to any other party through any means (unless
otherwise FireEye has provided prior written consent)

Have you read and agree to all the terms? (Yes/No): yes

Okta User: user.name@company.com
Okta Password:
Appliance(s) Password:
>>> Gathering Configurations
```

```
Hosts                                                                                :
100%|#################################################################################| 38/38
[01:10<00:00,  1.66hosts/s]
[ 192.168.1.250                                          ][ Completed.   ]:
100%|#################################################################################|
112/112 [00:55<00:00,  3.33cmd/s]
[ 10.1.1.120                                             ][ Completed.   ]:
100%|#################################################################################|
112/112 [00:53<00:00,  2.57cmd/s]
[ hexabc123-hxprim.helix.apps.fireeye.com                ][ Completed.   ]:
100%|#################################################################################|
112/112 [00:53<00:00,  2.40cmd/s]
[ hexabc123-hxdmz.helix.apps.fireeye.com                 ][ Completed.   ]:
100%|#################################################################################|
112/112 [00:53<00:00,  2.33cmd/s]

>>> Processing Configurations
Configs                          : 100%|##########| 35/35 [00:01<00:00, 19.21files/s]
>>> Generating Reports
Reports                          : 100%|##########| 33/33 [00:08<00:00,  4.09files/s]
    reports\192.168.1.250_141218T103332.docx
    reports\10.1.1.120_141218T103332.docx
    reports\hexabc123-hxprim.helix.apps.fireeye.com_141218T103332.docx
    reports\hexabc123-hxdmz.helix.apps.fireeye.com_141218T103332.docx
```

BEHAVIORS

USERNAMES AND PASSWORDS

In the event that `--username` or `--password` is not specified on the command line, the tool will prompt for those at execution time.

TARGETS AND FILES

In the event that neither `--target` nor `--file` is specified, the tool 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 tool is located.

ISSUES AND TROUBLESHOOTING

KNOWN ISSUES

- None

SUPPORT

This tool is not supported by FireEye Technical Support; however, bugs can reported to FireEye Technical Support.

Phone:

1-877-FIREEYE

Email:

Support@fireeye.com

Web:

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

LICENSING

To assist you, an index of each license referenced is provided. Full text copies of the open source licenses may be found by following the links set out below. Some of the open source licenses require FireEye to make the corresponding source code available. For those, you may obtain the corresponding source code from FireEye by contacting: FireEye-OpenSource@fireeye.com.

This offer ends three years after delivery by FireEye of the corresponding FireEye Software Release to you or, where the license so requires, at the expiration of a longer period of time as expressly set out in the license. To defray the costs associated with fulfilling your request a nominal charge of $15 may apply.

The FireEye Health Check Tool contains the open source software (OSS) packages listed below:

- jmespath is licensed under the MIT license and is Copyright (c) 2013 Amazon.com, Inc. or its affiliates. All Rights Reserved.
- python_docx is licensed under the MIT license and is Copyright (c) 2013 Steve Canny, https://github.com/scanny.

- json2html is licensed under the MIT license and is Copyright (c) 2013 Varun Malhotra.
- jsonmerge is licensed under the MIT license and is Copyright 2018, Tomaz Solc <tomaz.solc@tablix.org>.
- docxtpl is licensed under the GNU LGPL, Version 2.1.
- tqdm is licensed under the MIT license in part and the Mozilla Public License, 2.0 in part. (For additional details refer to: https://github.com/tqdm/tqdm/blob/v4.25.0/LICENCE)
- paramiko is licensed under the GNU LGPL, Version 2.1.
- colorama is licensed under the BSD 3-Clause license and is Copyright (c) 2010 Jonathan Hartley. All rights reserved.
- requests is licensed under the Apache License, Version 2.0. Copyright (c) 2018 Kenneth Reitz.
- HMAC.py & setup.py are licensed under the Python 2.2 license and is Copyright (c) 2001, 2002, 2003 Python Software Foundation. All Rights Reserved.
- docx is licensed under the MIT license and is Copyright (c) 2013 Steve Canny, https://github.com/scanny.
- beautifulsoup4 is licensed under the MIT license and is Copyright (c) 2009-2010 Mike MacCana.

License Index:

- BSD 3-Clause license: https://opensource.org/licenses/BSD-3-Clause
- GNU LGPL, Version 2.1: https://www.gnu.org/licenses/old-licenses/lgpl-2.1.en.html
- MIT license: https://opensource.org/licenses/MIT
- Mozilla Public License, 2.0: https://www.mozilla.org/en-US/MPL/2.0/
- Python 2.2 license: https://www.python.org/download/releases/2.2/license/

FREEWARE END USER LICENSE AGREEMENT
(FOR OBJECT CODE VERSIONS OF FIREEYE SOFTWARE)

BY DOWNLOADING, INSTALLING OR USING (WHICHEVER COMES FIRST) THIS SOFTWARE AND RELATED DOCUMENTATION (THE “SOFTWARE”) YOU AND THE ENTITY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY THIS END USER LICENSE AGREEMENT WITH FIREEYE, INC. (“FIREEYE”). IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO THE TERMS OF THIS AGREEMENT, YOU MUST NOT DOWNLOAD INSTALL OR USE THE SOFTWARE.

Grant of License and Restrictions. Subject to the terms hereof, FireEye grants Licensee a personal, non-sublicensable, non-transferable and nonexclusive, right to use the Software, but only in object code form. FireEye retains ownership of the Software and Licensee shall maintain the copyright and other notices that appear on the Software.

No Obligation to Deliver Updates and Support Services. In no event shall FireEye be liable for any support, maintenance or updates of the Software. In the event FireEye provides, in its sole discretion, any such updates, they shall be deemed “Software” subject to this Agreement unless otherwise stated in writing by FireEye.
Restrictions. Licensee shall not, and shall not authorize or assist any third party to, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of the Software (except to the limited extent that applicable law prohibits reverse engineering restrictions). Prior to disposing of any media or apparatus containing any part of the Software, Licensee shall completely destroy all copies of the Software contained therein. Licensee acknowledges that the Software may contain or use certain open source or other third party components (“Third Party Software”). Licensee agrees to be bound to any and all license provisions applicable to the Third Party Software. No rights or licenses are granted other than as expressly and unambiguously set forth herein.

Confidentiality. The Software in source code form remains a confidential trade secret of FireEye. The Software is protected by the copyright and other intellectual property laws of the United States and international treaties.

Termination. This Agreement is effective until terminated. This Agreement shall terminate automatically if Licensee fails to comply with any term or condition of this Agreement. Upon termination, Licensee shall destroy all copies of the Software. Paragraphs 3, 4, 6, 7, 8, and 9 of this Agreement shall survive any termination.

Limited Warranty and Disclaimer. LICENSEE ACCEPTS THE SOFTWARE "AS IS," AND FIREEEYE MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, AND NONINFRINGEMENT. FIREEYE DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE’S REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE. THE ENTIRE RISK ARISING OUT OF SELECTION, USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

Limitation of Liability. LICENSEE'S EXCLUSIVE REMEDY AND THE ENTIRE LIABILITY OF FIREEYE RELATED TO THE SOFTWARE SHALL BE EXPRESSLY LIMITED TO REPLACEMENT OF THE SOFTWARE. IN NO EVENT WILL FIREEYE OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR OTHER LIABILITY.
Export Control. Licensee represents and warrants that it shall comply with all laws and regulations applicable to Licensee with respect to the Software and its license and use, including without limitation those with respect to export.

Miscellaneous. This Agreement shall be deemed to have been made in, and shall be governed by the laws of the State of California and the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods or the Uniform Computer Information Transactions Act. This is the complete and exclusive statement of the mutual understanding of the parties with respect to the license granted herein and supersedes and cancels all agreements and communications relating to such license.