

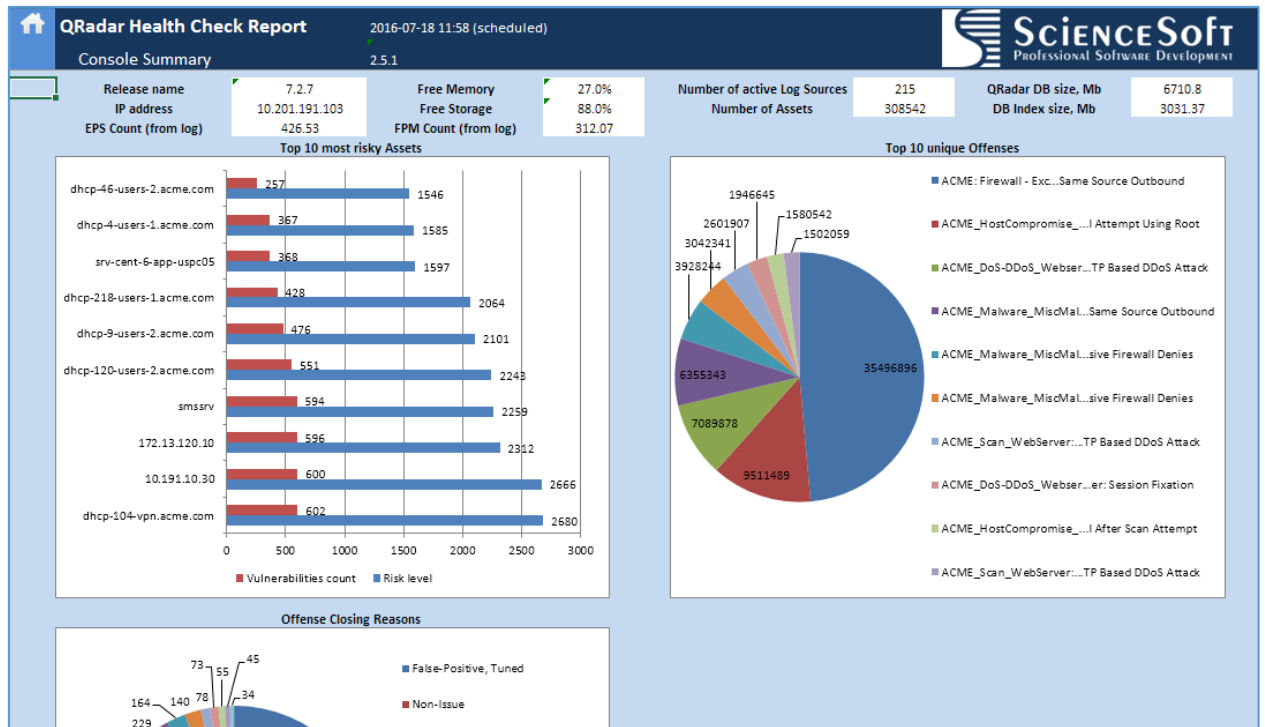
# Health Check Framework for IBM Security QRadar SIEM

## Contents

Overview .....	2
Installation.....	3
Download HCF Manager .....	3
Install HCF Manager .....	3
Download HCF.....	4
Prepare HCF server.....	4
Install HCF.....	5
Connect HCF Manager to HCF.....	5
Request license key .....	6
Install license key without HCF Manager .....	6
Install license key with HCF Manager.....	6
Execution parameters .....	7
Manual execution.....	7
Using HCF Manager .....	7
Using command line.....	7
Scheduling for periodical monitoring.....	8
Using HCF Manager .....	8
Using command line.....	9
Email reporting.....	9
Using HCF Manager .....	9
Without HCF Manager .....	10
Health markers.....	11
Custom logo .....	13
Adding Custom logo with HCF Manager .....	13
Adding Custom logo without HCF Manager.....	13
Disabling HCF Listener.....	14
Troubleshooting .....	14
Appendix A: Monitoring metrics .....	15
Appendix B: Release notes.....	18
Appendix C: Installing HCF on QRadar Console .....	22

## Overview

Health Check Framework (HCF) for IBM Security QRadar SIEM is a tool that allows QRadar users, administrators and security officers to perform periodical and on-demand monitoring of a range of statistical, performance and behavioral parameters of QRadar deployment including All-in-One and distributed environments.



Supported QRadar versions:

- 7.2.4
- 7.2.5
- 7.2.6
- 7.2.7
- 7.2.8

HCF gathers and analyzes more than 60 different parameters (metrics) and produces an Excel report that can be delivered to one or more recipients via email. This report reflects system health statistics in a tabular and graphical representation. For complete list of supported metrics please refer to [Appendix A: Monitoring metrics](#) section.

**NOTE:** HCF is a commercial software and requires a license key to run. Free demo mode with limited functionality is also available. No license key required for running HCF in this mode.

**NOTE:** HCF is developed by ScienceSoft Inc. and not supported by IBM.

**NOTE:** HCF does not change any settings of QRadar deployment.

## Installation

Fully functional HCF deployment includes the following components:

<b>Health Check Framework</b>	Main executable, libraries and configuration files
<b>HCF Manager</b>	App Exchange extension (HCF application tab in QRadar UI)
<b>HCF Listener</b>	Resident tool providing interaction between HCF and HCF Manager

In order to prepare HCF deployment the following steps should be taken:

1. Download HCF Manager
2. Install HCF Manager
3. Download HCF
4. Prepare HCF server
5. Install HCF
6. Connect HCF Manager to HCF
7. Install License key

Refer to corresponding sections in this document to complete all steps.

**NOTE:** HCF Manager and HCF Listener are optional components. If you are not planning to use them, skip steps **#1**, **#2**, **#6** from the list above and refer to [Disabling HCF Listener](#) section.

**NOTE:** Optionally HCF can be installed directly on QRadar Console. Refer to [Appendix C: Installing HCF on QRadar Console](#) for details.

### Download HCF Manager

- Go to <https://exchange.xforce.ibmcloud.com/hub>
- Login using your IBMid
- Filter by Type: Application
- Select **HCF Manager** extension
- Click **Download** button at the top right corner
- Save the extension zip file

### Install HCF Manager

- Login to QRadar UI
- Go to **Admin** tab
- Open **Extensions Management**
- Click **Add** button
- Click **Browse** button, locate the extension file downloaded from IBM App Exchange and click **Add** button
- Confirm on all steps and wait for installation to finish
- Close **Extensions Management** window, press **Ctrl+F5** to fully reload QRadar UI. New **HCF** tab will be added

**NOTE:** it takes several minutes for HCF Manager to become active after installation is completed.

**NOTE:** For more details on using IBM App Exchange and Extension Management tool, please refer to official IBM documentation:

[http://www.ibm.com/support/knowledgecenter/en/SS42VS\\_7.2.7/com.ibm.apps.doc/c\\_Qapps\\_MngExt.s.html](http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.apps.doc/c_Qapps_MngExt.s.html)

## Download HCF

- In QRadar UI, navigate to **HCF** tab and click **download** link. Fill out the form and click **Get download link** button

The screenshot shows the 'Health Check Framework Manager' interface within the IBM QRadar Security Intelligence console. At the top, there's a navigation bar with tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, User Analytics, and HCF. Below the navigation bar, the title 'Health Check Framework Manager' is displayed. A section titled 'Execution status:' is present. The main section is 'HCF deployment', which includes input fields for 'HCF Server IP addr' and 'HCF Server key', followed by a 'Connect' button. Below this, a message states: 'If you don't have HCF installed yet, please [download](#) the installation package.' A form titled 'Please provide a valid email address so that we can send you a download link' contains several input fields: 'First Name: \*', 'Last Name: \*', 'E-mail: \*', 'Phone:', 'Company: \*', 'Title:', and 'Country:'. A 'GET DOWNLOAD LINK' button is located at the bottom right of the form.

**NOTE:** Internet connection is required on your QRadar Console in order to send the form. If communication to external network is denied, fill out the form at <https://www.scnsoft.com/services/security-intelligence-services/health-check-framework-for-ibm-qradar-siem> instead and click **Start your free trial** button

- Download link will be sent to your email address defined in the form. Follow the link and save the zip file

## Prepare HCF server

HCF requires a physical or virtual server with the following minimum specifications:

- RAM: **1 Gb**
- HDD: **5 Gb**
- CPU: **2 cores**
- Network adapter: **1**
- OS: **CentOS 6.8**

Below are the steps to prepare HCF server:

- Allocate resources for virtual server or prepare a physical server according to system requirements listed above
- Download **CentOS-6.8-x86\_64-minimal.iso** from official CentOS mirror
- Install CentOS
- Set up default network interface (eth0):
  - Assign IP address from the same subnet/VLAN as your QRadar Console/AiO (this IP address is referred below as **HCF Server IP**)
  - Make sure the interface is enabled on boot
  - Verify SSH connection to QRadar Console/AiO
- Install additional packages using the following command:
  - ***yum install perl fuse-libs dmidecode zip***
- Allow HTTPS communication to HCF server:
  - ***iptables -I INPUT 1 -p tcp -m tcp --dport 443 -j ACCEPT***
  - ***service iptables save***

**NOTE:** Refer to CentOS official documentation to complete all OS installation and configuration steps.

## Install HCF

- Extract **HCF-<version>.el6.x86\_64.rpm** file from the archive obtained in [Download HCF](#) section
- Upload the RPM file to HCF server using your preferred SCP client
- Login as root user to HCF server and change directory to the one containing the RPM package
- Install using the following command:

```
rpm -Uvh <RPM_file_name>
```

HCF will be installed to **/opt/scnsoft/hcf** folder.

Linux man page is available for HCF: **man healthcheck**

Also, HCF Listener will be installed to **/opt/scnsoft/hcflistener** folder.

## Connect HCF Manager to HCF

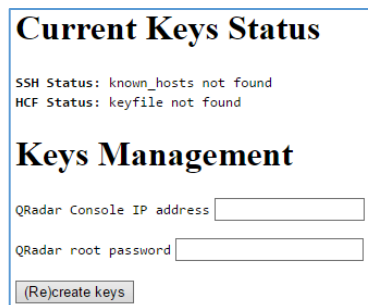
In order for HCF Manager to interact with HCF server the following steps should be taken:

- Make sure QRadar Console/AiO appliance is accessible via SSH (port 22):

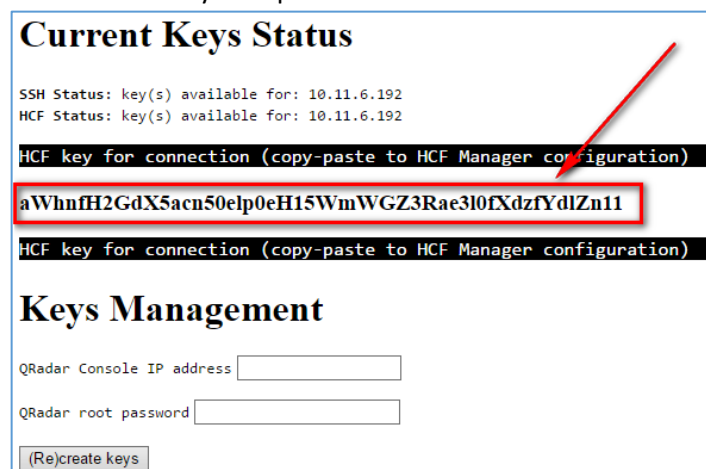
```
ssh <QRadar_Console_IP>
```

The **authenticity of host ... can't be established** message should appear. Enter **no** to the question **Are you sure you want to continue connecting (yes/no)?**

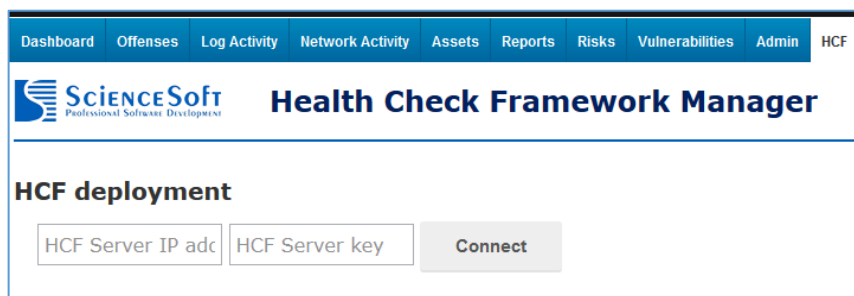
- In your web browser go to **https://<HCF Server IP>** where **HCF Server IP** is an IP address defined in [Prepare HCF server](#) section



- Enter QRadar Console IP address and QRadar Console root password
- Click **(Re)create keys** button
- Copy the generated connection key to clipboard



- Login to QRadar UI as Admin user
- Go to **HCF** tab



The screenshot shows the 'HCF deployment' section of the ScienceSoft Health Check Framework Manager. At the top, there is a navigation bar with tabs: Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Vulnerabilities, Admin, and HCF. Below the navigation bar, the ScienceSoft logo and the title 'Health Check Framework Manager' are displayed. The main content area is titled 'HCF deployment' and contains two input fields: 'HCF Server IP address' and 'HCF Server key', followed by a 'Connect' button.

- Enter **HCF Server IP** address and paste the connection key into corresponding fields
- Click **Connect** button

If everything was done correctly, HCF Manager interface will be shown in HCF tab, containing three sections: *HCF deployment*, *Execution parameters* and *Reports*.

### Request license key

In order to generate full reports, HCF requires a license key. You can request a commercial license by sending request to [contact@scnsoft.com](mailto:contact@scnsoft.com).

The following information required for the license key to be created:

- Company name
- Contact person
- Contact person position
- Contact email
- Contact phone
- QRadar version
- **UUID code** of QRadar Console/AiO

In order to obtain UUID code of your QRadar Console/AiO follow the steps below:

- Login as root user to QRadar Console/AiO via SSH
- Execute command: ***dmidecode -s system-uuid***
- Copy the generated alpha-numeric code to use it in your license request.

You will be sent an email with a license key once you complete your purchase.

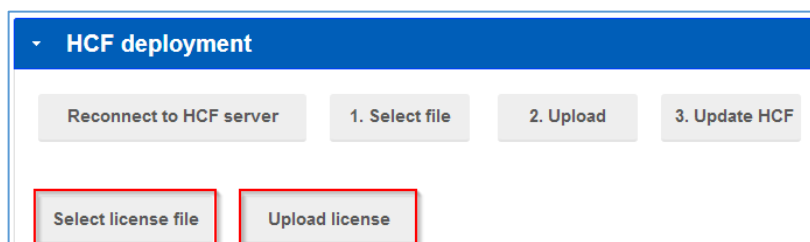
### Install license key without HCF Manager

Extract **hcf\_license.key** file from the received archive and upload it to the following folder on HCF server:

**`/opt/scnsoft/hcf`**

### Install license key with HCF Manager

- In QRadar UI, navigate to **HCF** tab
- Open **HCF deployment** section
- Click **Select license file** button, locate the ZIP file received from ScienceSoft and click Upload license button



The screenshot shows the 'HCF deployment' section of the HCF Manager interface. It features a blue header with a dropdown arrow and the text 'HCF deployment'. Below the header, there are four buttons: 'Reconnect to HCF server', '1. Select file', '2. Upload', and '3. Update HCF'. At the bottom, there are two buttons: 'Select license file' and 'Upload license', both of which are highlighted with red rectangular boxes.

## Execution parameters

Command line	HCF Manager	Description
<b>-d</b>	Enable debug	Debug mode. Enhanced execution log will be created. Commands output will be written to /opt/scnsoft/hcf/reports/HCF-YYYY-mm-DD-HH-MM-DebugInfo.zip file for further review. Some information about your deployment and connected Log Sources will be extracted from configuration database.
<b>-ndq</b>	Disable Data Quality analysis	Disables Data Quality analysis in order to reduce HCF execution time.
<b>-nam</b>	Disable Advanced JMX metrics	Disables Advanced Metrics in order to reduce HCF execution time.
<b>-ntr</b>	Precise EPS/FPM timelines	Disables rounding and omitting of values in EPS/FPM timelines
<b>-r [RULESPERFINTERVAL]</b>	Rules performance interval	Rules performance check duration (in seconds). If not defined, will run with default 600 seconds interval.
<b>-a [ARIELDELTA]</b>	Time range for Ariel queries	Time range for Ariel queries (in hours). If not defined, will run with default 24 hours range.
<b>-v</b>	N/A	Display HCF version and exit.

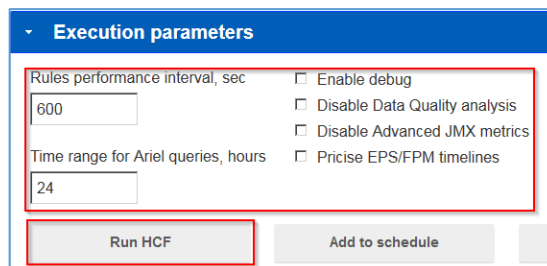
For example: executing `/opt/scnsoft/hcf/healthcheck -d -ndq -r 60` will run HCF in debug mode, skipping Data Quality metrics, and rules performance monitoring will last for 1 minute.

## Manual execution

### Using HCF Manager

- Login to QRadar UI
- Go to **HCF** tab, **Execution parameters** section
- Define execution parameters as described in the previous section
- Click **Run HCF** button

Execution status will be displayed at the top of the window. Once finished, reports list will be updated.



### Using command line

- Login as root via SSH to your HCF Server
- Execute `/opt/scnsoft/hcf/healthcheck [-d] [-ndq] [-nam] [-ntr] [-r number] [-a number]`

with parameters defined according to the previous section

Execution log will be displayed in the console.

## Scheduling for periodical monitoring

### Using HCF Manager

- Login to QRadar UI
- Go to **HCF** tab, **Execution parameters** section
- Click **Add to schedule** button
- Define the schedule using drop-down lists or enter manually in the text field
- Click **Schedule** button

The screenshot shows the 'Health Check Framework Manager' interface. The 'Execution parameters' section is expanded, showing fields for 'Rules performance interval, sec' (600) and 'Time range for Ariel queries, hours' (24). There are checkboxes for 'Enable debug', 'Disable Data Quality analysis' (checked), 'Disable Advanced JMX metrics' (checked), and 'Pricise EPS/FPM timelines'. The 'Add to schedule' button is highlighted with a red box and a '2' label. Below it, the 'Schedule' dialog is open, showing 'Every week on Saturday at 01:00' and a cron expression '0 1 \* \* 6'. The 'Schedule' button in the dialog is highlighted with a red box and a '4' label. The 'Run HCF' button is highlighted with a red box and a '1' label. The 'Edit HCF tasks' button is highlighted with a red box and a '3' label. The 'Close' button is highlighted with a red box and a '4' label. The 'HCF started' status shows 'Tue Sep 27 14:41:19 2016'.

Click **Edit HCF tasks** button to review and/or change existing crontab entries

The screenshot shows the 'Health Check Framework Manager' interface. The 'Execution parameters' section is expanded, showing fields for 'Rules performance interval, sec' (600) and 'Time range for Ariel queries, hours' (24). There are checkboxes for 'Enable debug', 'Disable Data Quality analysis' (checked), 'Disable Advanced JMX metrics' (checked), and 'Pricise EPS/FPM timelines'. The 'Add to schedule' button is highlighted with a red box and a '2' label. Below it, the 'Edit HCF tasks' dialog is open, showing a list of crontab entries. The 'Save' button is highlighted with a red box and a '4' label. The 'Cancel' button is highlighted with a red box and a '4' label. The 'HCF started' status shows 'Schedule added'.



## Using command line

In order to configure periodical HCF execution perform the following actions on HCF Server:

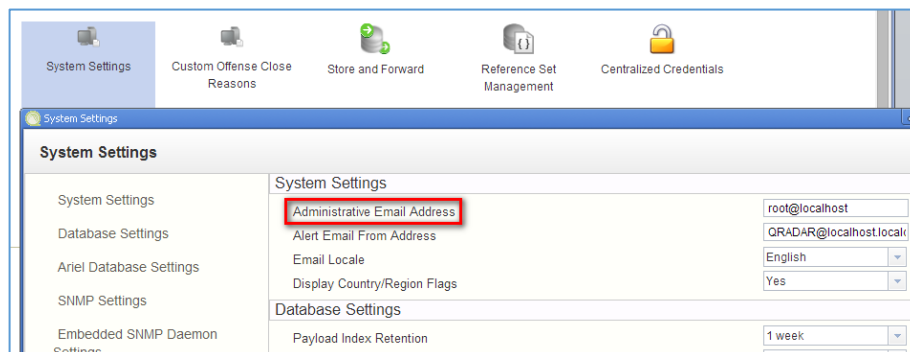
- Type ***crontab -e***
- Press **i** key to enter Insert Mode
- Scroll down to the end of file using cursor buttons
- Type ***0 17 \* \* \* /opt/scnsoft/hcf/healthcheck*** (specify execution parameters when required)
- Press **Esc** key to exit from Insert Mode
- Type ***ZZ*** (capital Z twice) to save changes and exit the editor

**NOTE:** refer to crontab scheduling format below to create desired HCF tasks

```
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan, feb, mar, apr ...
# | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR
sun, mon, tue, wed, thu, fri, sat
# | | | | |
# * * * * * command to be executed
```

## Email reporting

After each run HCF can send reports via email. By default the report will be sent to the email address specified under **System Settings – Administrative Email Address** in QRadar Admin tab:



If you want to send HCF reports via email to other addresses, refer to steps below.

## Using HCF Manager

- Login to QRadar UI
- Navigate to **HCF** tab
- Open **HCF deployment** section
- Click **Create report recipients list** button. QRadar Reference Set will be created and the button will change to **Report recipients** which is intended to manage email addresses via QRadar standard Reference Set editor.

### Without HCF Manager

- Create new Reference Set
  - Login to QRadar UI
  - Navigate to **Admin** tab
  - Press **Reference Set Management** button
  - Press **Add** button
  - Type **HCF Report Emails** as Name
  - Enable **Lives Forever** checkbox
  - Press **Create** button

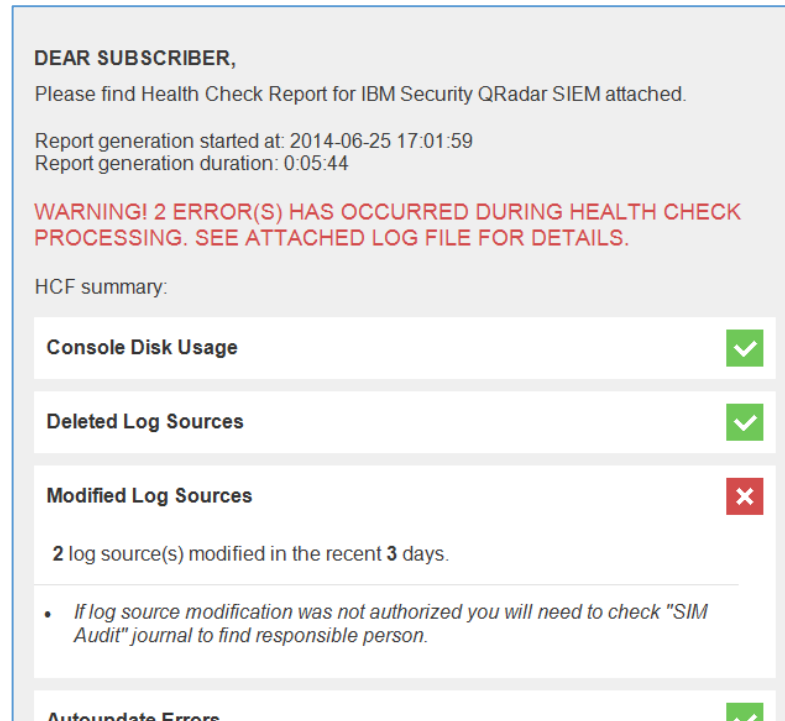
- Update Reference Set content
  - Double click on **HCF Report Emails** reference set
  - Press **Add** button
  - Add one or several email addresses to the list

Value	Origin
psayenka@scnsoft.com	admin
nikolaenya@scnsoft.com	admin

**NOTE:** In order to temporary disable email reports without removing the existing recipients, add **nomail** item to the Reference Set. Delete this item once you need email reports again.

## Health markers

HCF provides user with extended email reports which contain 25 “OK/Failed” Health Markers in order to indicate important metrics changes in your QRadar deployment. In case of marker fire you’ll receive a warning with description and some basic recommendations.



Health Markers fire on the following metrics:

- **Console Disk Usage:** if used disk space on the Console/AiO appliance exceeds the given threshold (95% by default).
- **Deleted Log Sources:** if at least one Log Source was deleted during the last days (3 days by default).
- **Modified Log Sources:** if at least one Log Source was modified during the last days (3 days by default).
- **Autoupdate Errors:** if at least one Autoupdate failed during the last days (3 days by default).
- **Asset Risk Level:** if at least one Asset reached Risk level, which exceeds the top-10 average level on more than given threshold (70% by default).
- **Offense Types:** if at least one Offence type occurs more often (80% by default) than the top-10 average periodicity.
- **Nightly Backups:** if at least this many (0 by default) failures occurred among last 5 backups.
- **System Notifications:** if at least one error/warning was detected in System Notifications journal during the last days (3 days by default).
- **Inactive Log Sources:** if at least one Log Source became inactive during the last days (3 days by default).
- **Disabled Log Sources:** if at least one Log Source was disabled during the last days (3 days by default).
- **Protocol Errors:** if at least one Log Source has a Protocol configuration errors.
- **Modified Searches:** if at least one Search was modified during the last days (3 days by default).
- **Data Integrity:** if at least one event/flow data file corrupted or integrity check failed.

- **Rules Execution Time:** if at least one correlation rule executes longer than the top-10 average rules execution time on more than given threshold (70% by default).
- **Rules Response Time:** if at least one correlation rule responses longer than the top-10 average rules response time on more than given threshold (70% by default).
- **Reports Execution Time:** if at least one report executes longer than the average execution time among top-10 most heavy reports on more than given threshold (70% by default).
- **Distributed EPS:** if at least one managed host reached EPS utilization more than the given threshold (95% by default).
- **Distributed FPI:** if at least one managed host reached FPI utilization more than the given threshold (95% by default).
- **Managed hosts RAM:** if at least one managed host runs below the given amount (10% by default) of free RAM.
- **Managed hosts CPU:** if at least one managed host has CPU load over the given threshold (95% by default) in the last 15 minutes.
- **Managed hosts /store partition:** if at least one managed host has used /store partition space over the given threshold (90% by default).
- **Managed Hosts Status:** if at least one managed host is in state different than Active or Standby (normal operation of HA appliances).
- **Generic DSM:** if at least one SIM Generic DSM Log Source generates more than given number of events (50 by default).
- **Unknown Events:** if at least one Log Source generates more than given threshold of unknown events (90% by default).

Default thresholds can be modified either by editing the **markers.ini** file stored in **/opt/scnsoft/hcf/** folder or through HCF Manager by defining required values per marker:

Execution status: Not running

- HCF deployment
- Execution parameters
- Reports
- ▾ **Health Markers**

Reports execution time ▾ 70

Level of deviation from average execution time for top-10 most heavy reports, %

**NOTE:** **markers.ini** file will be overwritten during update via command line. If you have made any changes in markers configuration, please backup this file before updating. Updating via HCF Manager extension backs up and restores it automatically.

## Custom logo

HCF allows to use a custom logo picture in report headers.

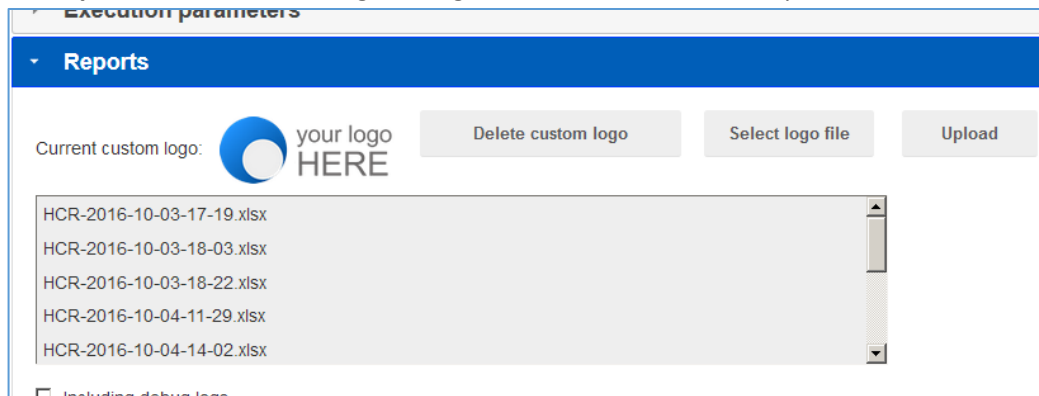
The following requirements must be met:

- File name: **logo.png** (not necessary when uploading via HCF Manager)
- Image format: **PNG**
- Color depth: **24 bit**
- Image size: **296x59 or less**
- Image resolution: **72 dpi**

Report header background color is RGB **22, 54, 92** (HEX **#16365C**). For better logo readability use transparent image background or contrast colors.

### Adding Custom logo with HCF Manager

- Prepare your logo file according to the requirements above
- Login to QRadar UI
- Navigate to **HCF** tab
- Open **Reports** section
- Click **Select logo file** button and locate your logo file
- Click **Upload** button. A warning message will be shown if some requirements are not met.



Click **Delete custom logo** button to remove your custom logo when necessary.

**NOTE:** only one logo file can be stored at one time. Any existing logo file will be overwritten after pressing Upload button.

### Adding Custom logo without HCF Manager

Prepare a Custom logo file according to the requirements above and upload it via SCP to **/opt/scnsoft/hcf/** folder on your HCF Server.

## Disabling HCF Listener

During HCF installation **/opt/scnsoft/hcflistener** folder will be created and the following cron task will be added:

```
*/5 * * * * /opt/scnsoft/hcflistener/hcflistener
```

If you don't use HCF Manager application, change the schedule and stop already running instance as follows:

- Login as root to HCF Server via SSH
- Execute **crontab -e** command
- Navigate to the line stated above with cursor keys
- Comment out...
  - Press **i** key to enter Edit Mode
  - Insert **#** in the beginning of the line
  - Press **Esc** key to exit Edit Mode
- Or delete...
  - press **d** key **twice** to delete entire line
- Press **Shift+z** keys **twice** to save changes and exit from cron editor
- Execute **pskill hcflistener** command.

## Troubleshooting

If you have problems with HCF execution or reports generation, run it with debug mode enabled:

```
/opt/scnsoft/hcf/healthcheck -d
```

Or execute via HCF Manager with **Enable debug** checkbox selected.

**HCF-YYYY-mm-DD-HH-MM-DebugInfo.zip** file will be generated, stored at **/opt/scnsoft/hcf/reports** folder and attached to the report email. Forward this file and your Excel report to the following address for investigation:

[hcf.support@scnsoft.com](mailto:hcf.support@scnsoft.com)

## Appendix A: Monitoring metrics

The following metrics are monitored with HCF:

	7.2.4	7.2.5	7.2.6	7.2.7	7.2.8
<b>Console Summary</b>					
Release name	+	+	+	+	+
IP address	+	+	+	+	+
EPS Count (from log)	+	+	+	+	+
FPI Count (from log)	+	+	+	+	+
Free Memory	+	+	+	+	+
Free Storage	+	+	+	+	+
Number of active Log Sources	+	+	+	+	+
Number of Assets	+	+	+	+	+
QRadar DB size, Mb	+	+	+	+	+
DB Index size, Mb	+	+	+	+	+
Top 10 most risky Assets	+	+	+	+	+
Top 10 unique Offenses	+	+	+	+	+
Offense closing reasons	+	+	+	+	+
<b>Console Generic</b>					
Product name	+	+	+	+	+
Release Name	+	+	+	+	+
Product version	+	+	+	+	+
Appliance type	+	+	+	+	+
Is Console	+	+	+	+	+
IP Address	+	+	+	+	+
Hardware class	+	+	+	+	+
OS	+	+	+	+	+
Kernel architecture	+	+	+	+	+
Hardware Unique ID	+	+	+	+	+
Disk usage (all partitions)	+	+	+	+	+
Last 5 backups	+	+	+	+	+
Last 24h System Statistics	+	+	+	+	+
List of QRadar users and roles	+	+	+	+	+
<b>Attention</b>					
Top 10 Offenses	+	+	+	+	+
Top 10 most risky assets	+	+	+	+	+
Last warnings and errors from System Notification	+	+	+	+	+
Top autoupdate errors	+	+	+	+	+
Last 10 Installations	+	+	+	+	+
<b>Log Sources</b>					
Number of active Log Sources	+	+	+	+	+
Number of active Log Source Groups	+	+	+	+	+
Number of Assets	+	+	+	+	+
Last inactive Log Sources (720 min)	+	+	+	+	+
Disabled Log Sources	+	+	+	+	+
Protocol Configuration Errors	+	+	+	+	+
Last 10 added Log Sources	+	+	+	+	+

Last 10 deleted Log Sources	+	+	+	+	+
Last 10 modified Log Sources	+	+	+	+	+
<b>Events and Rules</b>					
Number of enabled rules	+	+	+	+	+
Number of disabled rules	+	+	+	+	+
Number of Building Blocks	+	+	+	+	+
Number of custom rules	+	+	+	+	+
Number of modified rules	+	+	+	+	+
Integrity of events for recent 24h	+	+	+	+	+
Integrity of flows for recent 24h	+	+	+	+	+
EPS and FPI	+	+	+	+	+
EPS/FPI Statistics per Log Source	+	+	+	+	+
Rules performance: Fired count	+	+	+	+	+
Rules performance: Top Average Execution Time	+	+	+	+	+
Rules performance: Top Average Actions Time	+	+	+	+	+
Rules performance: Top Average Response Time	+	+	+	+	+
<b>Services and DB</b>					
Hostcontext Mem Usage, %	+	+	+	+	+
ECS Mem Usage, %	+	+	+	+	+
Tomcat Mem Usage, %	+	+	+	+	+
JVM Mem allocation	+	+	+	+	+
DB Index size, Mb	+	+	+	+	+
All DB's sizes	+	+	+	+	+
Top 10 active DB index hits	+	+	+	+	+
Top size DB tables	+	+	+	+	+
<b>Distributed EPS</b>					
EPS/FPI statistics per host	+	+	+	+	+
Event processor IP address	+	+	+	+	+
Average EPS for last 1 day	+	+	+	+	+
Average FPI for last 1 day	+	+	+	+	+
EPS License limit	+	+	+	+	+
FPI License limit	+	+	+	+	+
Percentage of EPS utilization	+	+	+	+	+
Percentage of FPI utilization	+	+	+	+	+
<b>Heavy Reports</b>					
Top 10 most heavy active reports	+	+	+	+	+
10 Recently Modified Searches	+	+	+	+	+
<b>Managed Hosts</b>					
IP Address	+	+	+	+	+
HA IP Address	+	+	+	+	+
HA Host role	+	+	+	+	+
Hostname	+	+	+	+	+
Host status	+	+	+	+	+
Uptime in days	+	+	+	+	+
Avg CPU load	+	+	+	+	+
Total RAM, Mb	+	+	+	+	+
Free RAM, %	+	+	+	+	+



Total /store space	+	+	+	+	+
Free /store space, %	+	+	+	+	+

**Log Source List**

ID	+	+	+	+	+
Hostname	+	+	+	+	+
Source Name	+	+	+	+	+
Source Type	+	+	+	+	+
Activity	+	+	+	+	+
Addition Type	+	+	+	+	+
Status	+	+	+	+	+
Event Collector Name	+	+	+	+	+
Last event seen	+	+	+	+	+
Groups	+	+	+	+	+
Average EPS for last 1 minute	-	-	-	+	+

**Advanced JMX Metrics**

Event Statistics	+	+	+	+	+
Flow Statistics	+	+	+	+	+
Offense Statistics	+	+	+	+	+
Active Sessions	+	+	+	+	+

**Data Quality Framework**

By Device Type	+	+	+	+	+
By Log Source	+	+	+	+	+
Unknown and Stored	+	+	+	+	+

**Ariel Usage**

Event and Flows	+	+	+	+	+
-----------------	---	---	---	---	---

**EPS Timeline**

Average and Peak	+	+	+	+	+
------------------	---	---	---	---	---

**FPI Timeline**

Average and Peak	+	+	+	+	+
------------------	---	---	---	---	---

**Offense Analysis**

Offenses and rules	+	+	+	+	+
--------------------	---	---	---	---	---

**DSM info**

DSM info	+	+	+	+	+
----------	---	---	---	---	---

**\* - Not available in free demo mode**

## Appendix B: Release notes

### HCF 2.5.5 (08 Dec 2016):

- **Fixed:** NaN check in *DSMinfo* metrics
- **Fixed:** GZ log reading during remote run for *EPS per Log Source Type* stats
- **Fixed:** *Ariel usage* failures on remote hosts with SSH banners
- **Fixed:** false *SSH connect failed* errors removed
- **Improved:** labels overlapping on *EPS per Log Source Type* chart
- **Improved:** labels overlapping on *Offense Analysis* chart
- **Improved:** *Top Risky Assets* chart disabled when no vulnerability data exists

### HCF 2.5.4 (27 Oct 2016):

- **New:** *DSMinfo* metrics
- **Improved:** JMX metrics timeout
- **Fixed:** DQ interruption when running with disabled debug
- **Fixed:** minor UI issues.

### HCF 2.5.3 (17 Oct 2016):

- **New:** License uploading via HCF Manager.
- **New:** Health markers editing via HCF Manager.
- **Improved:** temporary files storing and cleanup.
- **Improved:** HCF Listener disabled when installed on QRadar Console.

### HCF 2.5.1 (05 Oct 2016):

- **New:** execution status messaging for HCF Manager.
- **New:** QRadar v. 7.2.8 support.
- **Fixed:** EPS/FPI per Log Source statistics failures.
- **Fixed:** Heavy Reports failures.

### HCF 2.5.0 (24 Aug 2016):

- **New:** installation and remote execution on a separate server.
- **Fixed:** multiline messages in Top autoupdate Errors.
- **Fixed:** Ariel Usage data collection failures.
- **Fixed:** minor UI issues.

### HCF 2.4.4 (12 Jul 2016):

- **New:** QRadar v. 7.2.7 support.
- **Removed:** support for QRadar versions < 7.2.4.
- **Improved:** Average EPS column in Log source list for QRadar 7.2.7.
- **Improved:** updated query for Offense Closing Reasons.
- **Fixed:** minor UI issues.

### HCF 2.4.3 (07 Jun 2016):

- **New:** HCF Listener added for IBM Security App Exchange HCF Management application.
- **New:** custom logo function added.
- **Improved:** Log Source List: "Groups" column added, columns order changed.
- **Improved:** JMX metrics collection method redesigned.
- **Fixed:** minor UI issues.
- **Fixed:** Top risky assets display hostname or MAC address when combined name is unavailable.

### HCF 2.3.5 (07 Dec 2015):

- **Improved:** CLI parameter added for disabling values rounding and omitting in EPS and FPI timelines.
- **Fixed:** FPM timelines data source changed.

HCF 2.3.4 (25 Nov 2015):

- **New:** raw inbound flows timeline.
- **New:** Offense Analysis worksheet.
- **Improved:** Log Source List: Event Collector name instead of ID, “Last seen” column added.
- **Improved:** license limits on EPS/FPI timeline charts.
- **Fixed:** cleanup in Ariel Usage.
- **Fixed:** signal handlers.
- **Fixed:** minor issues.

HCF 2.2.9 (15 Oct 2015):

- **Fixed:** EPS statistics on HA deployments.
- **Fixed:** Distributed Memory metrics for Event Collector management hosts.
- **Improved:** detailed execution time information in email report.
- **Improved:** separated CLI arguments for Data Quality and Advanced JMX Metrics.
- **Improved:** failover categories updated for Juniper MX, F5 BIG-IP AFM, Infoblox NIOS in Data Quality metrics.

HCF 2.2.6 (01 Oct 2015):

- **Fixed:** parseDiffSysStat execution warning.
- **Fixed:** Data Quality calculations on QRadar 7.2.5 Patch 3 and higher.
- **Fixed:** minor UI issues.
- **Improved:** offense closing reason chart limited to top 20 entries.

HCF 2.2.5 (17 Jul 2015):

- **Improved:** logging, pid check and signal handling updated.
- **Improved:** demo data removed.
- **Fixed:** offense closing reason failure on Unicode strings.
- **Fixed:** rules performance processing when running with nohup.

HCF 2.2.1 (16 Jul 2015):

- **Improved:** logging.
- **Improved:** the HCF binary moved to /opt/scnsoft/hcf folder.
- **Fixed:** heavy reports health marker failure on empty values.

HCF 2.2.0 (26 Jun 2015):

- **New:** global configurable Ariel timeframe.
- **Improved:** CLI arguments parsing.
- **Fixed:** JMX stats failure on scheduled run.

HCF 2.1.7 (23 Jun 2015):

- **New:** health markers added for Data Quality metrics.
- **Fixed:** minor bugs.

HCF 2.1.6 (22 Jun 2015):

- **New:** Data Quality Unknown and Stored events.
- **Improved:** error message removed for top risky assets when no VA scanner connected.

HCF 2.1.5 (18 Jun 2015):

- **Improved:** exception handling.
- **Improved:** Storage usage by Ariel data for all Event Processors in distributed deployment.
- **Fixed:** /store usage on Risk Manager hosts.
- **Fixed:** Unicode names in Log Source List.

HCF 2.1.4 (17 Jun 2015):

- **Fixed:** support for QRadar V7.2.5 API changed permissions.
- **New:** integrity check for flows.

HCF 2.1.3 (12 Jun 2015):

- **Improved:** raw inbound EPS timeline for all Event Processors in distributed deployment.
- **Fixed:** failover categories updated for certain Device Types in Data Quality metrics.

HCF 2.1.2 (10 Jun 2015):

- **Fixed:** Data Quality crash on *Device Type* = 0.
- **New:** creating dumps of significant configuration tables in debug mode.
- **Improved:** Flow Processors and Collectors added to Managed Hosts table.
- **Improved:** added debug information attachment to report email.
- **Improved:** Data Quality metrics design updated.
- **Fixed:** EPS statistics error with recently disabled Log Sources.
- **Fixed:** raw inbound EPS timeline sorting.
- **New:** Top offense closing reason chart added.

HCF 2.1.1 (16 Apr 2015):

- **Fixed:** *can't find value for 'Disk Read'* error.
- **Fixed:** minor UI issues.
- **Improved:** --no-data-quality parameter disables JMX metrics too.
- **Improved:** failover categories updated for certain Device Types in Data Quality metrics.

HCF 2.1.0 (12 Mar 2015):

- **New:** raw inbound EPS timeline added (Console/AiO only).
- **Improved:** a CLI parameter added for disabling Data Quality metrics.

HCF 2.0.5 (27 Feb 2015):

- **New:** Storage usage by Ariel data added (Console/AiO only).

HCF 2.0.4 (19 Feb 2015):

- **New:** Log Sources information available in free demo mode.

HCF 2.0.3 (10 Feb 2015):

- **New:** Managed Hosts Status marker added.
- **Improved:** clear representation of HA devices (Cluster IP, HA Role columns added to managed Hosts list).
- **Fixed:** Data Quality calculation for Cisco ASA devices.
- **Fixed:** EPS calculation for heavy loaded deployments.
- **Fixed:** minor UI issues.
- **Fixed:** updated test data.

HCF 2.0.2 (4 Feb 2015):

- **Improved:** Protocol error status added in Log Source list.
- **Fixed:** Protocol Configuration Errors table now displays only initial warnings and errors.
- **Fixed:** EPS from log file calculation: internal sources excluded.

HCF 2.0.1 (16 Jan 2015):

- **New:** Table of contents and navigation buttons added.

HCF 2.0.0 (22 Dec 2014):

- **New:** free demo mode. A limited report can be generated without license.
- **New:** additional tab with advanced data collection statistics.
- **New:** “Fired rules count” and “Rules average execution time” charts added.
- **New:** Data Quality statistics by device type and Log Source added.
- **Improved:** Log Source list updated with Event Collector names.
- **Improved:** Managed Hosts updated with Hostname and Host Status.
- **Improved:** Health Markers reports are saved to reports folder.
- **Fixed:** minor bugs.

HCF 1.2.6 (28 Aug 2014):

- **Fixed:** support of Flow Processor and QFlow Collector appliances.
- **Fixed:** representation of disk storage in terabytes.
- **Fixed:** calculation of Console’s disk and memory usage separated from managed hosts.
- **Improved:** minor changes in Health Markers reports.

HCF 1.2.5 (28 Jul 2014):

- **Fixed:** display Log Source List entries with pipe symbol in Log Source Name (e.g. DB views).
- **Fixed:** some cosmetic issues.

HCF 1.2.0 (12 Jul 2014):

- **Improved:** Y axis set to 100% maximum value in distributed EPS chart.
- **Fixed:** /store space usage on Managed Hosts tab.
- **Fixed:** some cosmetic issues.
- **Fixed:** sample data updated corresponding to changes submitted in HCF 1.1.0.

HCF 1.1.0 (24 June 2014):

- **New:** Health Markers extended email reporting with configurable *markers.ini* file.
- **New:** Show HCF version in log, on Console Summary sheet and with `-v` CLI parameter.
- **Improved:** added to Log Source List: activity (active/inactive/error with highlight), addition type (manual/autodiscover) and status (enabled/disabled with highlight).
- **Fixed:** CPU utilization for multicore processors.
- **Fixed:** minor bugs.

HCF 1.0.0 (4 June 2014):

- Initial version.

## Appendix C: Installing HCF on QRadar Console

Optionally HCF can be installed directly on QRadar Console/AiO appliance.

In this case HCF Manager extension is not functional, and HCF Listener application should be disabled after installation.

Follow the steps below to install HCF on QRadar Console/AiO:

- Download HCF package as described in [Getting HCF for IBM QRadar SIEM](#) section
- Extract and upload **HCF-<version>.el6.x86\_64.rpm** file to QRadar Console via your preferred SCP tool
- Login as **root** to QRadar Console via SSH
- Change directory to the one containing the RPM package
- Install using the following command:

***rpm -Uvh <RPM\_file\_name>***

HCF will be installed to **/opt/scnsoft/hcf** folder. Also, HCF Listener will be installed to **/opt/scnsoft/hcflistener** folder.

**NOTE:** As IBM Security QRadar does not support the installation of any third-party packages, when installing HCF on QRadar appliance you assume all risks, including any process interruption, damaged data or termination of support services provided by IBM.