7SIGNAL®
THE WI-FI PERFORMANCE COMPANY

7signal Sapphire

EyeQ and REST API User Guide

Release 8.2

7signal Solutions Inc. 6155 Rockside Road, Suite 110, Independence, Ohio 44131, USA, 216-777-2900,
info@7signal.com, www.7signal.com

PREFACE

Document scope

This document is aimed at users who use EyeQ Dashboard to review and define status of the Wi-Fi network.

This document does not describe how the software is installed and how to handle the monitoring station. This is found in 7signal Sapphire Deployment Guide. To get guidance on how to interpret the measurements, please turn to the *7signal Sapphire Analyzer User Guide*.

FCC Compliance

Human RF Exposure

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimetres between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be located or operating in conjunction with any other antenna or transmitter.

Part 15

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Antenna

This device has been designed to operate on internal antennas or with an external patch type antenna having a maximum gain of 6dBi. Antennas having a gain greater than 6dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

Notes to the user

Any unauthorized modification of 7signal products may result in a violation of FCC requirements which would void the user’s authority to operate the equipment.

- The FCC ID for the 7signal Sapphire Eye IEEE802.11a/b/g Eye Unit is YLF-2010-08-APU2.
- The FCC ID for the 7signal Sapphire Eye, Model 1001 (802.11a/b/g/n), is YLF-EYE-ABGN-APU3
- The FCC ID for the 7signal Sapphire Eye, Model 2001 (802.11a/b/g/n) is YLF-INEY2001.
- The 7signal Sapphire Eye Model 2100 (802.11a/b/g/n/ac) Contains FCC ID: YLFSE2100WL.
- The 7signal Sapphire Eye Model 500 (802.11a/b/g/n/ac) Contains FCC ID: YLFSE2100WL.
- The 7signal Sapphire Eye Model 2200 (802.11a/b/g/n/ac-wave2) FCC ID: YLFSE2200.

Industry Canada Compliance

- The Industry Canada ID for 7signal Sapphire Eye, Model 2001 (802.11a/b/g/n) is 11766A-INEY2001
- The 7signal Sapphire Eye Model 2100 (802.11a/b/g/n/ac) Contains IC: 11766A-2100WL.
- The 7signal Sapphire Eye Model 500 (802.11a/b/g/n/ac) Contains IC: 11766A-2100WL.
- The 7signal Sapphire Eye Model 2200 (802.11a/b/g/n/ac) IC: 11766A-2200.

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Limitations in 5GHz Radar and Mobile Satellite Bands:

(i) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the EIRP limit; and
(ii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the EIRP limits specified for point-to-point and non point-to-point operation as appropriate.

(i) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;
(ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5 725-5 825 MHz) doit se conformer à la limite de p.i.r.e. spécifiée pour l'exploitation point à point et non point à point, selon le cas.

Note: High-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

EU DECLARATION OF CONFORMITY

With regard to the Radio Equipment Directive 2014/53/EC

We:

7signal Solutions, Inc.
6155 Rockside Rd, Suite 110
Independence, OH 44131

Declare under our sole responsibility that the products,

Sapphire Eye 2100
Sapphire Eye 500

Fulfill the essential requirements of the Radio Equipment Directive/53/EC.

The following standards were applied:

Radio **EN 300.328-2 V2.1.1 (2016); EN 301 893 V2.1.0 (2017-03);**
EN 302 502 V1.2.1 (2008-07)

EMC **EN 301 489-17 v3.1.1 (2017); EN 301.489-1 v2.1.1 (2016)**
EN 61000-3-2:2014; EN 61000-3-3:2013

Safety EN60950-1:2013, A2; LVD 2006/95/EC

The conformity assessment procedure referred to in Article 3 and Annex II of the Radio Equipment Directive 2014/53/EC has been followed.

The product carries the CE Mark:

CE

Date & Place of Issue: 7 August 2017, Independence, Ohio

Mexico

Radio: IFT #: RCP7S2117-1621
Safety: NOM-001

Non-interference:
La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

Compliance statements for India, Singapore, China for the manual

INDIA: Model 2100 operating at 2400-2483.5MHz: ETA #: 2923/17-RLO(WR)
Model 2100 operating at 5180-5320MHz & 5745-5825MHz: ETA #: 2935/17-RLO(WR)

Singapore: Model 2100: Complies with IMDA Standards DA103787

China: Model 2100: CMIIT ID: 2018AJ1640

Contact information

Contact us at 7signal

- by mail: 6155 Rockside Road, Suite 110, Independence, Ohio 44131, USA
- by phone: 216-777-2900
- support: support@7signal.com

TABLE OF CONTENTS

1 EYEQ and REST API 1

1.1 EyeQ at a glance 1

1.2 REST API at a glance 1

2 USING EYEQ 2

2.1 Accessing EyeQ 2

2.2 Accessing Analyzer from EyeQ 2

2.3 Accessing Configurator from EyeQ 2

2.4 Dashboard level 1 3

2.4.1 Level 1 SLA compliance 3

2.4.2 Topology tree and selectors 3

2.4.3 Navigator 4

2.4.4 Breadcrumb 4

2.4.5 Status tiles 4

2.4.6 Drill into Level 2 graphs 5

2.5 Connectivity KPIs (level 2) 6

2.6 Authentication KPIs (level 2) 7

2.7 IP and DNS Services (level 2) 8

2.8 Quality KPIs (level 2) 9

3 USING REST API 11

3.1 High Level capabilities 11

3.2 Authenticating to the API 11

3.2.1 To Obtain an Access Token 11

3.3 Using the API 11

3.3.1 Time Selection and Aggregations 12

4 Supported KPIS 14

1 EYEQ AND REST API

Sapphire EyeQ is the central user interface for all Sapphire functions. EyeQ Dashboard is a browser application for viewing network performance at a glance. EyeQ also offers access to Analyzer and Configurator functionalities. EyeQ uses an open REST API towards 7signal Carat engine and database.

REST API enables make queries to 7signal database and receive information to be displayed in other systems.

1.1 EyeQ at a glance

EyeQ provides users a quick view to most essential aspects of Wi-Fi network service and performance. These include compliance against targeted performance with Authentication, IP and DNS services, Connectivity and Quality. User may also drill into each four metrics and review next level metrics, which contribute to the value. Login and authentication is similar to the Configurator and Analyzer and uses the same credentials and access rights. EyeQ also provides access to Analyzer and Configurator.

1.2 REST API at a glance

REST API allows other systems making queries and receiving the same Key Performance Indicator (KPI) information as displayed in EyeQ Dashboard. API allows user defining the time of interest, averaging period, aggregation and the KPI itself.

2 USING EYEQ

2.1 Accessing EyeQ

EyeQ can be accessed with web browser from Carat server IP address.

Example:

Analyzer URL:

https://148.251.233.34/7signal/portal/SapphireLoupe

EyeQ URL:

https://148.251.233.34/eyeq/

Note: *eyeq* must be written in lower case.

2.2 Accessing Analyzer from EyeQ

Analyzer is web application, which is launched from Analyzer link. Analyzer uses the same credentials as the EyeQ.

Analyzer provider detailed analytics capabilities on all KPIs.

For instruction on using Analyzer, please refer to Analyzer User Guide.

2.3 Accessing Configurator from EyeQ

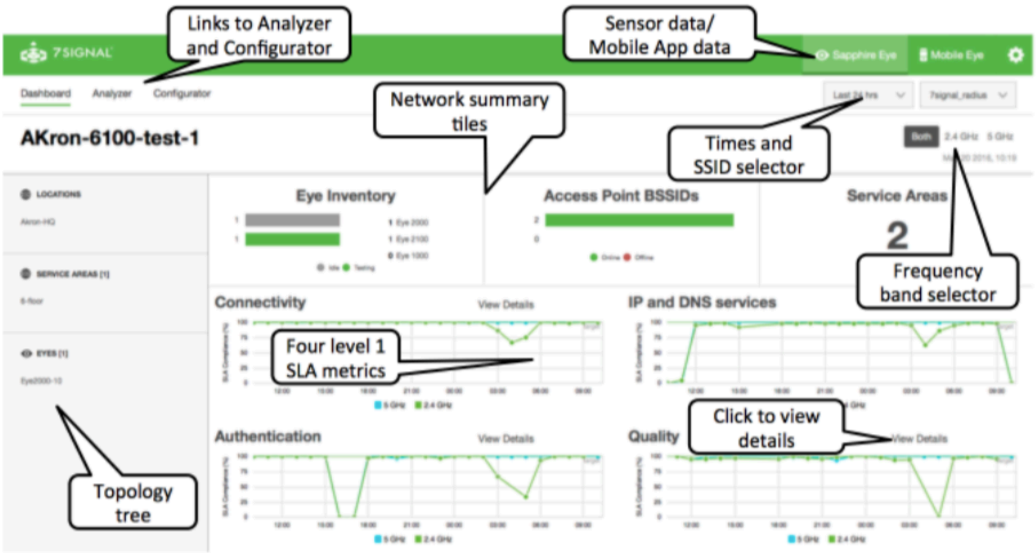
Configurator is a Java application, which is launched through a WebSwing session and can be fully operated though a browser window. Clicking configurator opens in a new browser tab like Analyzer. Configurator uses the same credentials as the EyeQ.

Only one active Configurator session/user account is allowed at a given time. Closing Configurator can be done by logging out and closing the tab. Alternatively Configurator can be also closed directly by closing the tab. Configurator session will be automatically terminated in 15 seconds after the tab has been closed. Note: Opening another Configurator session will automatically terminate the previous session and maintains only one active session at a time.

Number of parallel and simultaneous configurator sessions in enterprise setups is limited by default to 10.

For instructions on using Configurator, please refer to Carat User Guide.

2.4 Dashboard level 1



Links to Analyzer and Configurator

Sensor data/ Mobile App data

Network summary tiles

Times and SSID selector

Frequency band selector

Four level 1 SLA metrics

Click to view details

Topology tree

2.4.1 Level 1 SLA compliance

Four top level graphs indicate SLA compliance against set target values in each KPI category. Goal is to keep SLA compliance at 100%.

Each four Level 1 SLA metric is calculated based on several Level 2 SLA metrics. The ones included in the level 1 SLA are defined in the Level 2 view.

Compliance is calculated against target levels, which can be adjusted based on network baseline performance. Default values are used, if no custom values have been defined. SLA settings are defined with Carat management GUI.

2.4.2 Topology tree and selectors

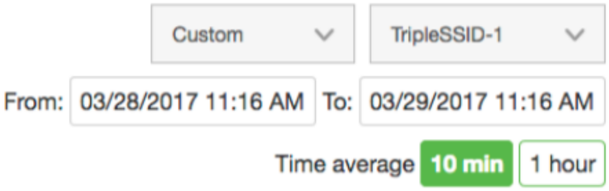
Selecting one item in topology tree with narrow down data selection accordingly. Graphs will be updated to reflect the performance in the selected area/element.

Time selector allows choosing views between last 1 hour, 12 hours, 24 hours, 7 days, 30 days, 90 days and custom. Time average selector can be used to vary granularity of the presented graphs. Longer averages yield cleaner graphs but may miss important events during the used minimum time period.

SSID selector is used to choose which network/SSID data is presented.

Frequency band selector allows presenting 2.4 GHz network data, 5 GHz network data or both simultaneously.

“View details” link takes user to the Level 2 view for the selected KPI.



Custom

TripleSSID-1

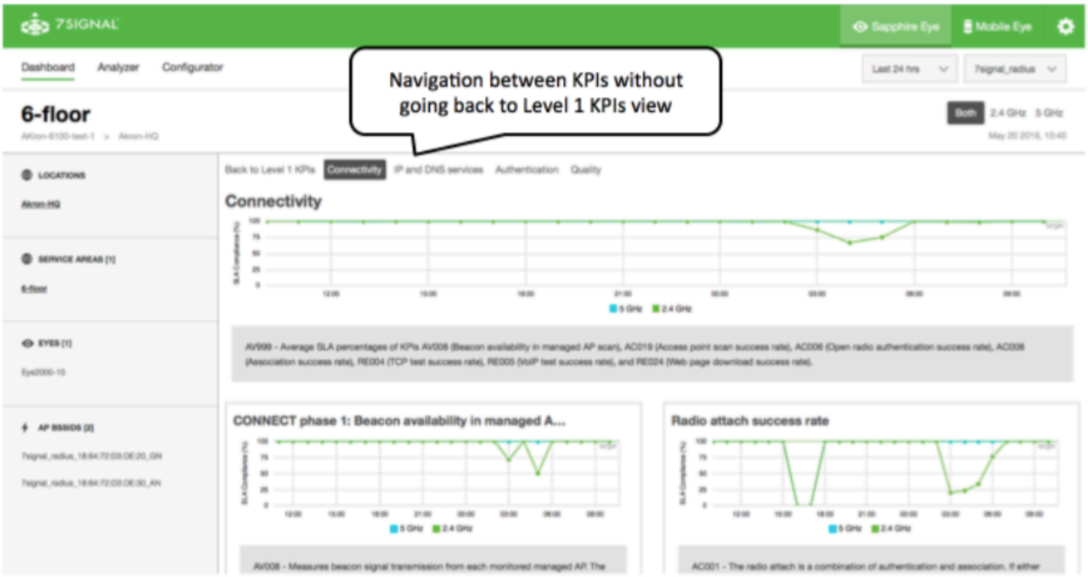
From: 03/28/2017 11:16 AM To: 03/29/2017 11:16 AM

Time average [✓ 10 min] 1 hour

Time, time average and SSID selector allow narrowing down the graphed data

EyeQ refreshes graphs automatically every 5 minutes.

2.4.3 Navigator

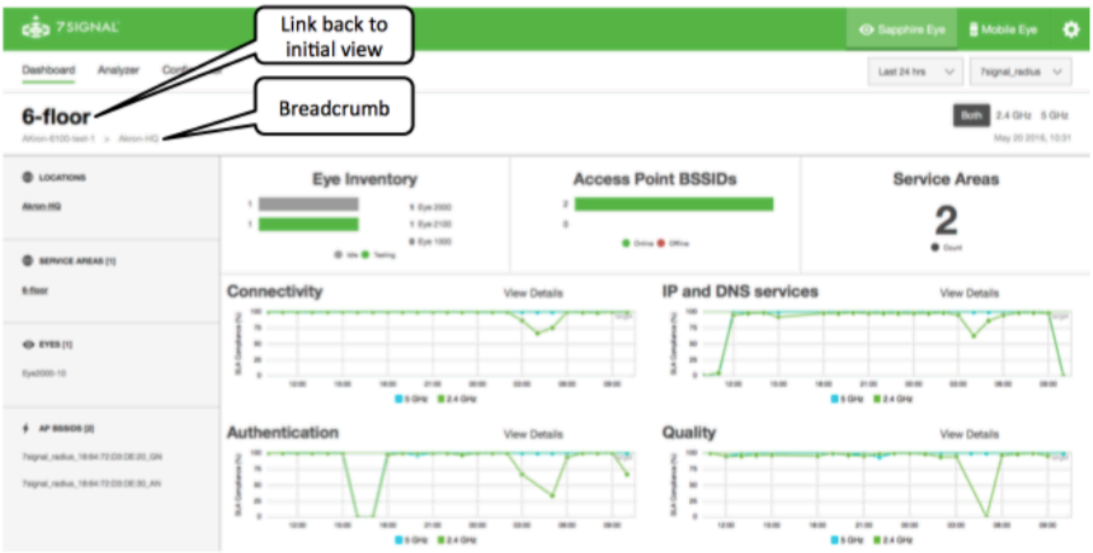


Navigation between KPIs without going back to Level 1 KPIs view

AV999 - Average SLA percentages of KPIs AV008 (Beacon availability in managed AP scan), AC019 (Access point scan success rate), AC006 (Open radio authentication success rate), AC008 (Association success rate), RE004 (TCP test success rate), RE005 (VoIP test success rate), and RE024 (Web page download success rate).

Navigator comes visible on the second level of KPIs. It allows moving “sideways” between KPIs.

2.4.4 Breadcrumb



Link back to initial view

Breadcrumb

Breadcrumb is an active link and allows user to move quickly back to higher level in topology.

User may go back to initial view by clicking the organization name.

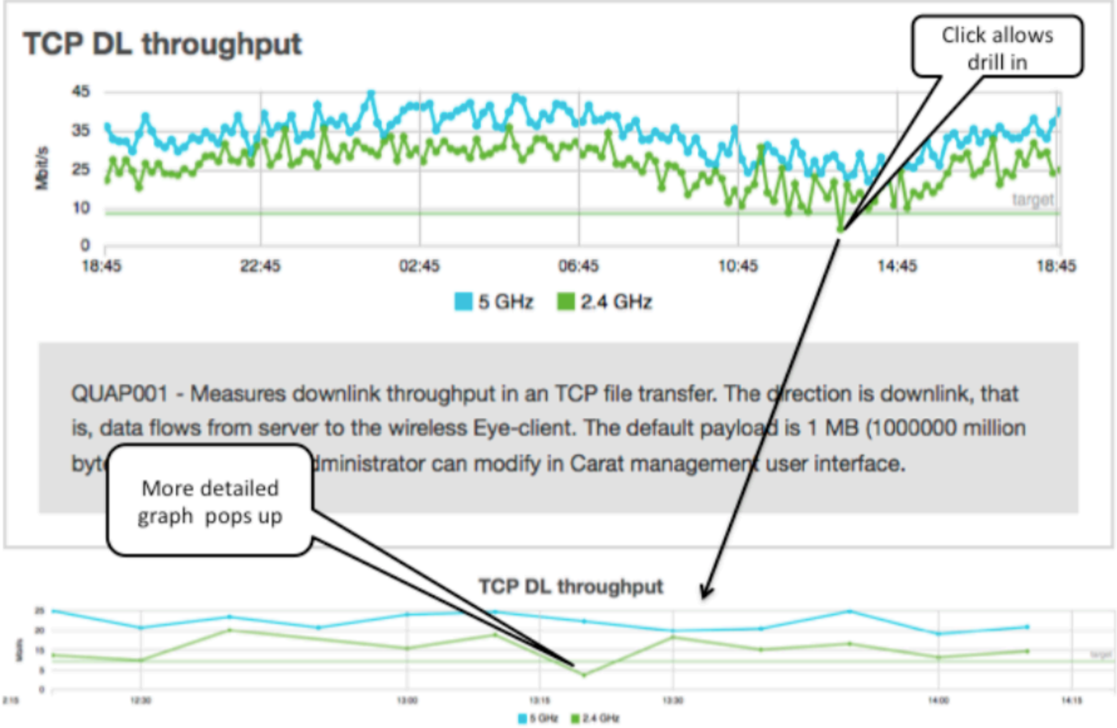
2.4.5 Status tiles

Status tiles present overview of the whole monitored network. Data is based on collected information during the last one hour.

- “Eye inventory” shows active and idle sensors as well as type of sensors in the network. “Active” means that sensor has been configured and is actively measuring according to a test profile. “Idle” means that sensor is not measuring but has been registered to Carat.

- “Access Point BSSIDs” indicates how many BSSIDs offer network connectivity. Data is calculated based on successful associations and authentications during the previous two hours times period. BSSID is included in the tile if there have been at least two association and authentication attempts during the last two hours. BSSID is reported to be online if at least one of the attempts was successful. If there have been at least two attempts but no success during the two hour period, BSSID is considered to be offline.
- “Service areas” indicates the quantity of monitored service areas.

2.4.6 Drill into Level 2 graphs



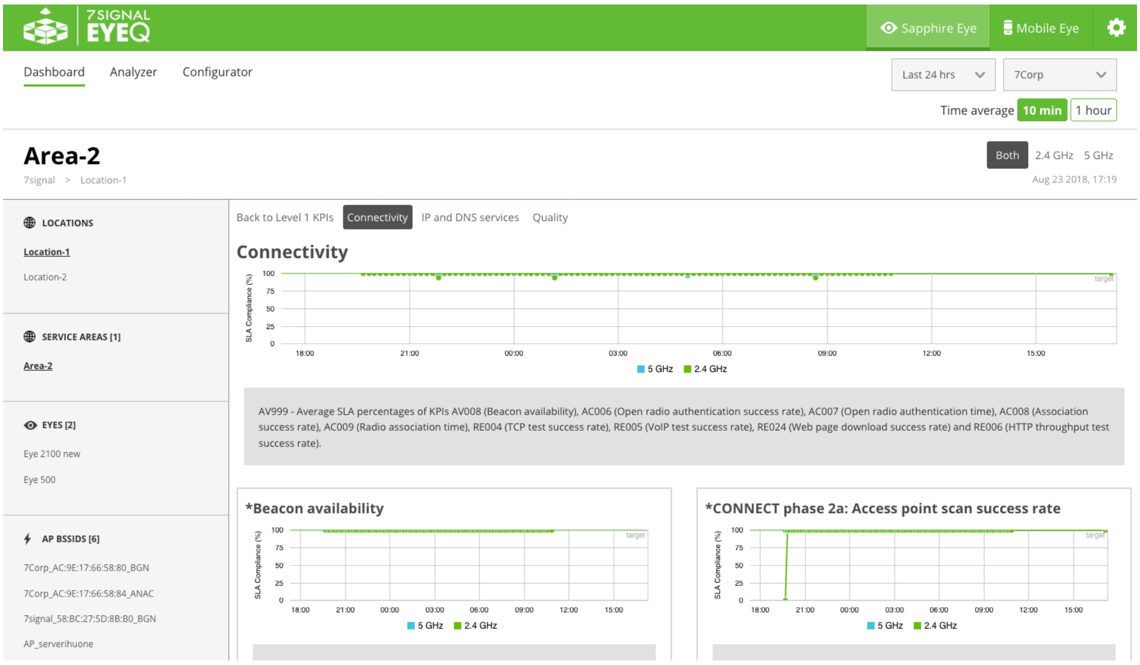
QUAP001 - Measures downlink throughput in an TCP file transfer. The direction is downlink, that is, data flows from server to the wireless Eye-client. The default payload is 1 MB (1000000 million byt dministrator can modify in Carat management user interface.

Click allows drill in

More detailed graph pops up

User may drill in to certain interesting data point. A more detailed graph is presented in a new window.

2.5 Connectivity KPIs (level 2)



AV999 - Average SLA percentages of KPIs AV008 (Beacon availability), AC006 (Open radio authentication success rate), AC007 (Open radio authentication time), AC008 (Association success rate), AC009 (Radio association time), RE004 (TCP test success rate), RE005 (VoIP test success rate), RE024 (Web page download success rate) and RE006 (HTTP throughput test success rate).

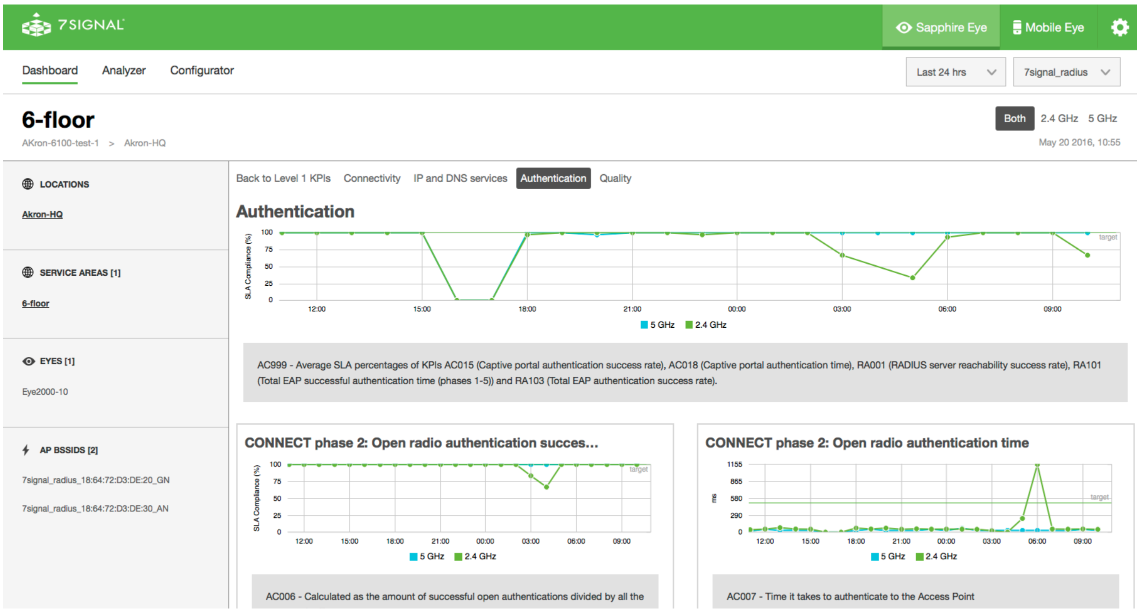
Each level 2 view provides the overall SLA compliance % metric as the top line graph. This graph is the same as can be seen in the Level 1 summary view. This is called here “Connectivity” and scale is %. Connectivity KPI is calculated as an average of several Level 2 KPIs.

Connectivity includes the following Level 2 KPIs

1. *Beacon availability
2. CONNECT phase 2a: Access point scan success rate
3. *CONNECT phase 2b: Open radio authentication success rate
4. *CONNECT phase 2b: Open radio authentication time
5. *CONNECT phase 2c: Radio association success rate
6. *CONNECT phase 2c: Radio association time
7. *HTTP throughput test success rate
8. *VOIP test success rate
9. *Web page download success rate

Symbol * is used to indicate which level 2 KPIs are included in the Connectivity Level 1 SLA compliance %.

2.6 Authentication KPIs (level 2)



AC999 - Average SLA percentages of KPIs AC015 (Captive portal authentication success rate), AC018 (Captive portal authentication time), RA001 (RADIUS server reachability success rate), RA101 (Total EAP successful authentication time (phases 1-5)) and RA103 (Total EAP authentication success rate).

AC006 - Calculated as the amount of successful open authentications divided by all the

AC007 - Time it takes to authenticate to the Access Point

Authentication Level 2 metrics present mode details of authentication process. Authentication process is split to multiple phases. For each phase, success rate and required time are presented.

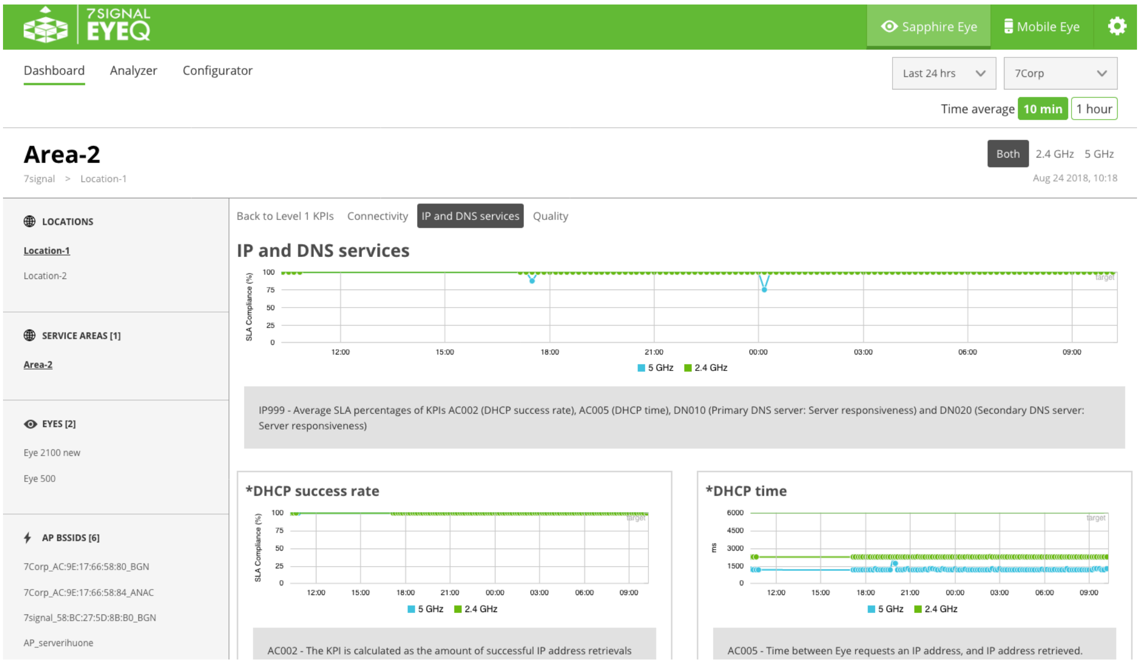
Authentication includes the following Level 2 metrics:

1. *Captive portal authentication success rate
2. *Captive portal authentication time
3. *RADIUS server reachability success rate
4. Number of EAP authentication attempts
5. *Total EAP authentication success rate
6. *Total EAP successful authentication time
7. RADIUS phase 1: Association completed to EAP authentication started success rate
8. RADIUS phase 1: Time from association completed to EAP authentication started
9. RADIUS phase 2: EAP method proposed by the server success rate
10. RADIUS phase 2: Time to EAP proposed method received from the server
11. RADIUS phase 3: EAP selected method success rate
12. RADIUS phase 3: Time to EAP method selected
13. RADIUS phase 4a: EAP peer certificate validation success rate
14. RADIUS phase 4a: Time to EAP peer certificate validation
15. RADIUS phase 5: EAP authentication completed success rate
16. RADIUS phase 5: Time to EAP authentication completed

If certain services are not used, like captive portal, graph will not be visible at all. Graphs are presented when there is data.

Symbol * is used to indicate which level 2 KPIs are included in the Authentication Level 1 SLA compliance %.

2.7 IP and DNS Services (level 2)



IP999 - Average SLA percentages of KPIs AC002 (DHCP success rate), AC005 (DHCP time), DN010 (Primary DNS server: Server responsiveness) and DN020 (Secondary DNS server: Server responsiveness)

AC002 - The KPI is calculated as the amount of successful IP address retrievals

AC005 - Time between Eye requests an IP address, and IP address retrieved.

IP and DNS services SLA % is calculated based on success and duration of IP and DNS services.

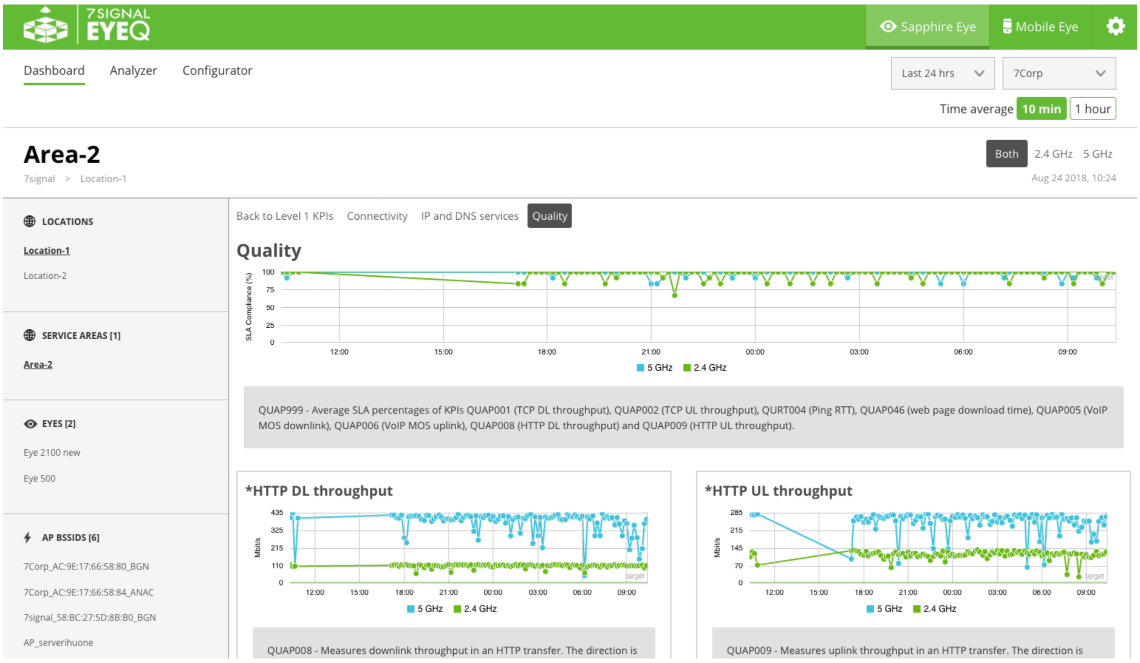
IP and DNS services process includes as well several phases. Success rate and duration is presented for each phase.

IP and DNS services includes the following Level 2 metrics:

1. *DHCP success rate
2. *DHCP time
3. *Primary DNS server: Server responsiveness
4. *Secondary DNS server: Server responsiveness
5. DHCP: Host reachability success rate
6. DHCP phase 1: DHCP discovery made success rate
7. DHCP phase 2: DHCP offer received success rate
8. DHCP phase 2: Time to DHCP offer received
9. DHCP phase 3: DHCP request made success rate
10. DHCP phase 3: Time to DHCP request made
11. DHCP phase 4: DHCP ACK received success rate
12. DHCP phase 4: Time to DHCP ACK received
13. Primary DNS server: Query success rate (Authoritative)
14. Primary DNS server: Successful query time (Authoritative)
15. Secondary DNS server: Query success rate (Authoritative)
16. Secondary DNS server: Successful query time (Authoritative)

Symbol * is used to indicate which level 2 KPIs are included in the IP and DNS services Level 1 SLA compliance %.

2.8 Quality KPIs (level 2)



QUAP999 - Average SLA percentages of KPIs QUAP001 (TCP DL throughput), QUAP002 (TCP UL throughput), QURT004 (Ping RTT), QUAP046 (web page download time), QUAP005 (VoIP MOS downlink), QUAP006 (VoIP MOS uplink), QUAP008 (HTTP DL throughput) and QUAP009 (HTTP UL throughput).

QUAP008 - Measures downlink throughput in an HTTP transfer. The direction is

QUAP009 - Measures uplink throughput in an HTTP transfer. The direction is

Quality SLA % includes several quality metrics for Wi-Fi connection. SLA % is calculated as an average of several KPIs.

1. *TCP DL throughput
2. *TCP UL throughput
3. *HTTP DL throughput
4. *HTTP UL throughput
5. *Ping RTT
6. *Web page download time
7. *VoIP MOS downlink (listening)
8. *VoIP MOS uplink (talking)
9. Packet loss in VoIP test
10. Jitter in VoIP test
11. Signal strength
12. AP signal to noise level at Eye
13. AP retries
14. Client retries
15. Channel utilization
16. Number of clients per AP
17. QBSS channel utilization
18. QBSS station count

Symbol * is used to indicate which level 2 KPIs are included in the Quality Level 1 SLA compliance %.

For more detailed analysis, user may choose to log in to Analyzer for deeper analysis capabilities.

3 USING REST API

3.1 High Level capabilities

In 7.1-0.0, the API implementation provides the following capabilities

- Organization information
- Reports for KPIs

3.2 Authenticating to the API

Before you get started, you need to first authenticate to the API. All APIs are protected using the OAuth 2.0 protocol. Accessing the API begins by providing both a Client name and Client secret, as well as a username and password—the same username and password your account uses on the Analyzer and/or Carat GUI. Once authenticated, you will receive an “access token”. Including this bearer “access token” in your API calls going forward will keep your access to the API.

Client name: `api–access`

Client password: `cdbff430–8353–45d2–a9f5–d19969dda406`

3.2.1 To Obtain an Access Token

1. HTTP POST to https://[analyzer hostname or IP]/carat-api/oauth/token
   -Include the client name and secret as HTTP Basic Auth parameters
   -Include the "Content-Type : application/x-www-form-urlencoded" Header
2. -Include the following as data:
   ```
   grant_type=password&
   username=[carat username]&
   password=[carat password]
   ```
3. If authentication is successful, a token in JSON format is returned:
   ```
   {“access_token”: “e1037d24-18b0-42b1-a05b-59cb53262910”,
   “token_type”: “bearer”,
   “refresh_token”: “5e57e32b-b0ca-4793-a558-0d4718ed3ae2”,
   “expires_in”: 43199,
   “scope”: “api”}
   ```
4. Include this token in all of the http request headers like so to enable access to the requested resources:
   ```
   “Authorization: Bearer e1037d24-18b0-42b1-a05b-59cb53262910”
   ```

3.3 Using the API

Once you are authenticated to the API, you can make various requests to the API. To start off, it could be helpful to get the full listing of organizations, locations, or service areas, access points, or wireless networks available to your user on your Carat, with the following calls:

```
GET https://[IP]/carat-api/organization
GET https://[IP]/carat-api/location
```

```
GET https://[IP]/carat-api/service-area
GET https://[IP]/carat-api/wireless-network
GET https://[IP]/carat-api/access-point
```

These responses will include arrays of the topology elements available in your user account. Every object has associated links embedded in the response, which allows you to learn more about different requests that can be made to the API, following the HATEOAS REST navigation standards. Additionally, extra related objects get embedded within the response for convenience. As an example, if your organization ID is 5, you can get a response with detailed information about the organization, some top-level KPIs and their results, and other related topology elements by making the following call:

GET https://[IP]/carat-api/organization/5

Another very useful endpoint is the KPI endpoint, which allows you to run a single or multiple KPI reports for a topology element. For example:

GET https://[IP]/carat-api/kpi/orgnanization/5/AV999,AC999,RA001

This request will return reports for KPI codes AV999, AC999, and RA001, if such reports are available.

3.3.1 Time Selection and Aggregations

Each reporting endpoint (topology endpoints and the KPI endpoint) has the ability to select a certain time range of data collection, as well as aggregations for specific time resolutions in the data returned.

The optional parameters for this are `start-time`, `end-time`, or `timelimit` for time selection, and `averaging` for aggregation. The averaging will combine all results within that time window and average them, spacing the results evenly, for example, every 10 minutes. Time is formatted in standard ISO-8601 format. The `timelimit` parameter is useful for obtaining data from the last specified time-period—such as for the last day or the last week, without formatting your own time parameter.

Below are some sample requests you could make:

Request	Result Description
GET https://[IP]/carat-api/organization/5	Default: returns the last day, with 1 hour averaging
GET https://[IP]/carat-api/organization/5?averaging=tenmin	Returns the last day, with 10 minute averaging

GET https://[IP]/carat-api/organization/5?averaging=raw	Returns the last day, with raw results (all data points collected)
GET https://[IP]/carat-api/organization/5?timelimit=onemonth	Returns results for the last month (averaging 1 hour by default)
GET https://[IP]/carat-api/organization/5?start-time=2015-10-15T12:00:00.000&end-time=2015-10-16T12:00:00.000	Returns results between 2015-10-15 12:00:00.00 and 2015-10-16 12:00:00.00 (UTC timezone), averaged hourly
GET https://[IP]/carat-api/organization/5?start-time=2015-10-15T12:00:00.000&end-time=2015-10-16T12:00:00.000&averaging=tenmin	Returns results between 2015-10-15 12:00:00.00 and 2015-10-16 12:00:00.00 (UTC timezone), averaged every 10 minutes

For a more complete documentation of the available calls in the API, please visit the documentation at https://east1.cloud.7signal.com/carat-api/swagger-ui.html

4 SUPPORTED KPIS

Sapphire Carat gathers and stores data obtained from automated test to the database. 7signal API offer the following KPIs.

KPI ID	Name	Description	Unit
Availability			
AV999	Connectivity	Average SLA percentages of KPIs AV008 (Beacon availability), AC006 (Open radio authentication success rate), AC007 (Open radio authentication time), AC008 (Association success rate), AC009 (Radio association time), RE004 (TCP test success rate), RE005 (VoIP test success rate), RE024 (Web page download success rate) and RE006 (HTTP throughput test success rate).	%
AV008	Beacon availability	Measures beacon signal transmission from each monitored managed AP. The KPI is the relative amount of received and expected beacons. The test is called SCAN_MANAGED. Results from SCAN_RADIO-tests are ignored.	%
AV009	Access point beacon availability in global AP scan	Measures beacon signal transmission from all heard APs. The KPI is the relative amount of received and expected beacons. The scan is called SCAN_RADIO. Results from SCAN_MANAGED are ignored.	
AV001	AP beacon availability	Measures beacon signal transmission from each monitored AP. The KPI is the relative amount of received and expected beacons.	%
AV002	Radio IP connection availability	Radio IP connection availability between Eye and AP. The radio IP connection has failed, if the connection establishment fails either in the radio-attach-phase or in the IP-address-retriaval-phase.	%
Accessibility			
AC001	Radio attach success rate	The radio attach is a combination of authentication and association. If either one fails, the attach procedure fails. During the test, Eye attempts to attach to the monitored AP. KPI is calculated as the number of successful attachments, divided by the number of all the attachment attempts.	%

AC004	Radio attach time	Time between Eye starts radio attach to an AP, and attach complete. Time between Eye starts radio attach to an AP, and attach complete.	ms
AC019	CONNECT phase 2a: Access point scan success rate	Measures access point scan success rate.	%
AC008	CONNECT phase 2a: Radio association success rate	The KPI is calculated as the amount of successful associations divided by all the requests by Eye.	%
AC009	CONNECT phase 2a: Radio association time	Time it takes to associate to the Access Point	ms
IP999	IP Services	Average SLA percentages of KPIs AC002 (DHCP success rate), AC005 (DHCP time), DN010 (Primary DNS server: Server responsiveness) and DN020 (Secondary DNS server: Server responsiveness)	%
RE004	TCP test success rate	Measures the successful completion rate of all TCP tests. Combines download and upload tests	%
RE001	TCP download success rate	Measures TCP download completion rate.	%
RE002	TCP upload success rate	Measures TCP upload completion rate.	%
RE006	HTTP throughput test success rate	Measures the successful completion rate of all HTTP throughput tests. Combines downlink and uplink tests.	%
RE007	HTTP DL throughput test success rate	Measures downlink HTTP throughput test completion rate.	%
RE008	HTTP UL throughput test success rate	Measures uplink HTTP throughput test completion rate.	%
RE005	VoIP test success rate	Measures the successful completion rate of VoIP tests. Combines download and upload tests	%
RE011	VoIP download test success rate	Measures VoIP (MOS) download completion rate.	%
RE012	VoIP upload test success rate	Measures VoIP (MOS) upload completion rate	%
RE013	VoIP download test success rate (G.711)	Measures VoIP (MOS) download completion rate (G.711).	%
RE014	VoIP upload test success rate (G.711)	Measures VoIP (MOS) upload completion rate (G.711).	%
QUAP046	Web page download time	Measures web page download time	ms
AC011	Radio association status code	Status code resulted by association	Code
AC013	Radio disassociation reason code	Reason code resulted by disassociation	Code

AC014	Time before starting Access point scan	Time from supplicant authentication started to supplicant has started to scan (probe) the Access point.	ms
AC017	Captive portal login page loading time	Time it takes to load HTTP captive portal login page	ms
QUAP032	TCP connection time	Time in which TCP connection between Eye and Sonar has been established	us
QUAP037	TCP retry count	Number of TCP retransmissions during active test	#
QUAP040	SIP registration time	Time in which SIP registration is complete between Eye and SIP server	ms
QUAP042	SIP unregistration time	Time in which SIP unregistration is complete between Eye and SIP server	ms
QUAP043	SIP registration status code	Status code resulted by SIP registration.	Code
QUAP045	SIP unregistration status code	Status code resulted by SIP unregistration.	Code
QUAP050	Redirections before captive portal login page	Measures number of HTTP redirects before captive portal login page is reached	#
QUAP051	Redirections after captive portal login	Measures number of HTTP redirects after captive portal login	#
QUAP052	Target web page loading time	Measures target web page (defined by HTTP authentication key) loading time when captive portal login is not needed	ms
QUAP053	Target web page loading time with login	Measures target web page (defined by HTTP authentication key) loading time when captive portal login is done prior to load of actual target web page	ms
RE015	VoIP download test success rate (G.719)	Measures VoIP (MOS) download completion rate (G.719).	%
RE016	VoIP upload test success rate (G.719)	Measures VoIP (MOS) upload completion rate (G.719).	%
RE020	SIP registration success rate	Measures SIP registration completion rate	%
RE022	SIP unregistration success rate	Measures SIP unregistration completion rate	%
RE024	Web page download success rate	Measures web page download completion rate	%
Authentication			
AC006	CONNECT phase 2b: Open authentication success rate	The KPI is calculated as the amount of successful open authentications divided by all the requests by Eye	%
AC007	CONNECT phase 2b: Open radio authentication time	Time it takes to authenticate to the Access Point	ms

AC999	Authentication	Average SLA percentages of KPIs AC015 (Captive portal authentication success rate), AC018 (Captive portal authentication time), RA001 (RADIUS server reachability success rate), RA101 (Total EAP successful authentication time) and RA103 (Total EAP authentication success rate).	%
AC015	Captive portal authentication success rate	Measures HTTP captive portal authentication success rate. Only successful and unsuccessful authentications are measured by this metric: direct pass-throughs are not measured	%
AC018	Captive portal authentication time	Captive portal authentication time	ms
RA103	Total EAP authentication success rate	Measures total EAP authentication success rate.	ms
RA101	Total EAP successful authentication time	Total time taken by successful EAP authentication.	ms
RA004	RADIUS phase 1: Association completed to EAP authentication started success rate	Measures success rate of starting EAP authentication (EAP-Identity request received from a RADIUS server).	%
RA005	RADIUS phase 1: Time from association completed to EAP authentication started	Measures elapsed time between completed Association and start of EAP authentication (EAP-Identity request received from a RADIUS server).	ms
RA006	RADIUS phase 2: EAP method proposed by the server success rate	Measures success rate of receiving proposed EAP method from the RADIUS server.	%
RA007	RADIUS phase 2: Time to EAP proposed method received from the server	Measures elapsed time between start of an EAP authentication and the time when the RADIUS server proposes an EAP Method.	ms
RA008	RADIUS phase 3: EAP selected method success rate	Measures success rate of selecting EAP Method proposed by the RADIUS server.	%
RA009	RADIUS phase 3: Time to EAP method selected	Measures elapsed time between receiving a proposed EAP Method to selecting an EAP Method.	ms
RA010	RADIUS phase 4a: EAP peer certificate validation success rate	Measures success rate of receiving and validating TLS peer certificate.	%
RA011	RADIUS phase 4a: Time to EAP peer certificate validation	Measures elapsed time between selecting an EAP Method and validating a peer certificate sent over TLS.	ms
RA014	RADIUS phase 5: EAP authentication completed	Measures success rate completion of successful EAP authentications.	%

7signal Sapphire EyeQ and REST API User Guide Release 8.2

	success rate		
RA015	RADIUS phase 5: Time to EAP authentication completed	Measures elapsed time between successful validation of a peer certificate and a successful completion of an EAP authentication.	ms
AC010	Radio authentication status code	Status code resulted by authentication	Code
AC012	Radio deauthentication reason code	Reason code resulted by deauthentication	Code
AC016	Captive portal pass-through success rate	Measures success rate of loading a web page defined in the HTTP authentication network key. Loading of the page takes place if HTTP authentication is not needed (session is still active)	%
QUAP041	SIP authentication time	Time in which SIP authentication is complete between Eye and SIP server	ms
QUAP044	SIP authentication status code	Status code resulted by SIP authentication.	Code
RA001	RADIUS server reachability success rate	Measures RADIUS server reachability, i.e. is the RADIUS server responding at all.	%
RA012	RADIUS phase 4b: EAP TLS peer certificate validation error rate	Measures error rate of receiving and validating TLS peer certificate.	%
RA013	RADIUS phase 4b: Time to EAP peer certificate validation error	Measures elapsed time between selecting an EAP Method and a unsuccessful validation of a peer certificate.	ms
RA016	EAP authentication failure error rate	Measures error rate completion of unsuccessful EAP authentications (EAP-Failure received).	%
RA017	Time to EAP authentication failure	Measures elapsed time between unsuccessful validation of a peer certificate and a unsuccessful completion of an EAP authentication (EAP-Failure received).	ms
RA018	Number of EAP authentication retries detected in one session	Measures number of EAP authentication retries during one active test.	#
RA019	Number of EAP authentication attempts	Measures number of EAP authentication attempts within given time.	#
RA020	EAP proposed method	EAP method proposed by the server.	#
RA021	EAP selected method	EAP method selected.	#
RA022	EAP TLS certificate validation reason code	EAP TLS certificate validation reason code.	#

RA100	Total EAP authentication time	Total time taken by EAP authentication, including successful and unsuccessful cases.	ms
RA102	Total EAP unsuccessful authentication time	Total time taken by unsuccessful EAP authentication.	ms
RE021	SIP authentication success rate	Measures SIP authentication completion rate	%
DHCP			
AC002	DHCP success rate	Measures DHCP success rate. The KPI is calculated as the amount of successful IP address retrievals divided by all the requests by Eye.	%
AC005	DHCP time	Time between Eye requests an IP address, and IP address retrieved.	ms
IP001	DHCP: Host reachability success rate	Measures DHCP server reachability, i.e. is the DHCP server responding at all.	%
IP003	DHCP phase 1: DHCP discovery made success rate	Measures DHCP discovery success rate, i.e. DHCP client on Eye sensor has successfully sent DHCP discovery messages to DHCP servers.	%
IP004	DHCP phase 2: DHCP offer received success rate	Measures DHCP offer received success rate, i.e. DHCP client on Eye sensor has received DHCP offer from the DHCP server.	%
IP005	DHCP phase 2: Time to DHCP offer received	Time from DHCP discovery request made to DHCP offer received.	ms
IP006	DHCP phase 3: DHCP request made success rate	Measures DHCP request made success rate, i.e. DHCP client on Eye sensor has sent DHCP request to the DHCP server.	%
IP007	DHCP phase 3: Time to DHCP request made	Time from DHCP offer received to DHCP request made.	ms
IP008	DHCP phase 4: DHCP ACK received success rate	Measures DHCP ACK received success rate, i.e. DHCP client on Eye sensor has received DHCP ACK from the DHCP server.	%
IP009	DHCP phase 4: Time to DHCP ACK received	Time from DHCP request made to DHCP ACK received.	Ms

IP002	DHCP: Host response time	Measures delay to first response received from the DHCP server.	ms
IP011	DHCP: Number of DHCP tests	Measures number of DHCP tests made in the selected time period.	#
IP012	DHCP: DHCP address renewal success rate	Measures DHCP address renewal success rate, if attempted.	%
IP013	DHCP: Time to DHCP renewal	Time from DHCP request sent to DHCP ack received.	Ms
DNS			
DN001	Regular DNS query: Service responsiveness	Does the DNS service respond to a query in any manner.	%
DN002	Regular DNS query: Query success rate	Success rate for regular host resolving query. Does not separate primary, secondary, tertiary responses	%
DN003	Regular DNS query: Successful query time	Response time for regular successfull host resolving query. Does not separate primary, secondary, tertiary responses.	ms
DN010	Primary DNS server: Server responsiveness	Does the DNS server respond to a query in any manner	%
DN011	Primary DNS server: Query success rate (Authoritative)	Success rate for authorative, recursive UDP query. Return code = 0	%
DN012	Primary DNS server: Successful query time (Authoritative)	Response time for authorative, recursive UDP query	ms
DN014	Primary DNS server: Query success rate (Non-Authoritative)	Success rate for non-authorative, recursive UDP query. Return code = 0	%
DN015	Primary DNS server: Successfull query time (Non-Authoritative)	Response time for non-authorative, recursive UDP query	ms
DN020	Secondary DNS server: Server responsiveness	Does the DNS server respond to a query in any manner	%

DN021	Secondary DNS server: Query success rate (Authoritative)	Success rate for authorative, recursive UDP query. Return code = 0	%
DN022	Secondary DNS server: Successful query time (Authoritative)	Response time for authorative, recursive UDP query	ms
DN024	Secondary DNS server: Query success rate (Non-Authoritative)	Success rate for non-authorative, recursive UDP query. Return code = 0	%
DN025	Secondary DNS server: Successfull query time (Non-Authoritative)	Response time for non-authorative, recursive UDP query	ms
DN030	Tertiary DNS server: Server responsiveness	Does the DNS server respond to a query in any manner	%
DN031	Tertiary DNS server: Query success rate (Authoritative)	Success rate for authorative, recursive UDP query. Return code = 0.	%
DN032	Tertiary DNS server: Successfull query time (Authoritative)	Response time for authorative, recursive UDP query	ms
DN034	Tertiary DNS server: Query success rate (Non-Authoritative)	Success rate for non-authorative, recursive UDP query. Return code = 0.	%
DN035	Tertiary DNS server: Successfull query time (Non-Authoritative)	Response time for non-authorative, recursive UDP query	ms
DN004	Regular DNS query: Error rate for "Host Not Found"	Operating system error rate for "Host Not Found" for a regular host resolving query. Does not separate primary, secondary, tertiary responses	%
DN005	Regular DNS query: Error rate for "Name Valid But No Address"	Operating system error rate for "Name Valid But No Address" for a regular host resolving query. Does not separate primary, secondary, tertiary responses	%
DN006	Regular DNS query: Error rate for "Non-recoverable name server error"	Operating system error rate for "Non-recoverable name server error" for a regular host resolving query. Does not separate primary, secondary, tertiary responses	%
DN007	Regular DNS query: Error rate for DNS query "Try again	Operating system error rate for "Try again" for a regular host resolving query. Does not separate primary, secondary, tertiary responses	%

DN008	Regular DNS query: Error rate for "Top level error"	Operating system error rate for "Top level error" for a regular host resolving query. Does not separate primary, secondary, tertiary responses	%
DN013	Primary DNS server: Query return code (Authoritative)	Return code for authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code
DN016	Primary DNS server: Query return code (Non-Authoritative)	Return code for non-authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code
DN023	Secondary DNS server: Query return code (Authoritative)	Return code for authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code
DN026	Secondary DNS server: Query return code (Non-Authoritative)	Return code for non-authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code
DN033	Tertiary DNS server: Query return code (Authoritative)	Return code for authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code
DN036	Tertiary DNS server: Query return code (Non-Authoritative)	Return code for non-authorative, recursive UDP query. Codes: 0 = No Error, 1 = Format Error, 2 = Server Failure, 3 = Name Error, 4 = Not Implemented, 5 = Refused, 6 = YXDomain, 7 = YXRRSet, 8 = NXRRSet, 9 = NotAuth, 10 = NotZone, -1 = timeout, -2 = communication error	Code

Data Quality			
QURT007	Ping success rate	Number of successful pings divided by the total amount of ping attempts.	%
QUAP999	Quality	Average SLA percentages of KPIs QUAP001, QUAP002, QURT004, QUAP046, QUAP005 and QUAP006.	%
QUAP008	HTTP DL throughput	Measures downlink throughput in an HTTP transfer. The direction is downlink, that is, data flows from server to the wireless Eye-client. The default transfer time is 5 seconds, which value an administrator can modify in Carat management user interface.	Mbit/s
QUAP009	HTTP UL throughput	Measures uplink throughput in an HTTP transfer. The direction is uplink, that is, the wireless Eye-client sends data to a test-server. The default transfer time is 5 seconds, which value an administrator can modify in Carat management user interface.	Mbit/s
QURT004	Ping RTT	Measures the round trip time between Eye and Sonar server. The test uses a serie of pings to ping server 20 times with zero wait time between the pings. The calculation is done internally in Eye and the output of the test is average, 95% percentile, max and min values of RTT. The objective is to measure the ping quality, not ping availability.	ms
QUAP005	VoIP MOS downlink (listening)	MOS (Mean Opinion Score) value of a VoIP downlink test.	MOS
QUAP006	VoIP MOS uplink (talking)	MOS (Mean Opinion Score) value of a VoIP uplink test.	MOS
QUAP015	Packet loss in VoIP test	Packet loss during a VoIP test.	%
QUAP013	Jitter in VoIP test	The variation of delay (jitter) during a VoIP test.	ms
QUAP033	Jitter in VoIP uplink (talking) test	The variation of delay (jitter) during a VoIP uplink test	ms
QUAP034	Jitter in VoIP downlink (listening) test	The variation of delay (jitter) during a VoIP downlink test	ms
QUAP035	Packet loss in VoIP uplink (talking) test	Packet loss during a VoIP uplink test	%

QUAP036	Packet loss in VoIP downlink (listening) test	Packet loss during a VoIP downlink test.	%
QURS032	Retransmissions in TCP test	Measures IEEE802.11 frame retransmission rate as (retrans_ul_count+retrans_dl_count)/(frame_ul_count+frame_dl_count) during TCP file transfer tests. This KPI combines DL and UL tests, and DL and UL retransmissions to give an overall metric of the retransmission in radio link	%
QURS033	Eye retransmissions in TCP test	Measures IEEE802.11 Eye frame retransmission rate during TCP file transfer tests. This KPI combines DL and UL tests to give an overall metric of Eye retransmissions in radio link	%
QURS034	Access point retransmissions in TCP test	Measures IEEE802.11 access point frame retransmission rate during TCP file transfer tests. This KPI combines DL and UL tests to give an overall metric of access point retransmissions in radio link	%
QURS035	Eye retransmissions in TCP DL test	Measures IEEE802.11 Eye frame retransmission rate during downlink TCP file transfer tests	%
QURS036	Eye retransmissions in TCP UL test	Measures IEEE802.11 Eye frame retransmission rate during uplink TCP file transfer tests	%
QURS037	Access point retransmissions in TCP DL test	Measures IEEE802.11 access point frame retransmission rate during downlink TCP file transfer tests	%
QURS038	Access point retransmissions in TCP UL test	Measures IEEE802.11 access point frame retransmission rate during uplink TCP file transfer tests	%
QURS046	Retransmissions in HTTP throughput test	Measures IEEE802.11 frame retransmission rate as (retrans_ul_count+retrans_dl_count)/(frame_ul_count+frame_dl_count) during HTTP throughput tests. This KPI combines DL and UL tests, and DL and UL retransmissions to give an overall metric of the retransmission in radio link.	%
QURS047	Eye retransmissions in HTTP throughput test	Measures IEEE802.11 Eye frame retransmission rate during HTTP throughput tests. This KPI combines DL and UL tests to give an overall metric of Eye retransmissions in radio link.	%

QURS048	Access point retransmissions in HTTP throughput test	Measures IEEE802.11 access point frame retransmission rate during HTTP throughput tests. This KPI combines DL and UL tests to give an overall metric of access point retransmissions in radio link.	%
QURS049	Eye retransmissions in HTTP DL throughput test	Measures IEEE802.11 Eye frame retransmission rate during downlink HTTP throughput tests.	%
QURS050	Eye retransmissions in HTTP UL throughput test	Measures IEEE802.11 Eye frame retransmission rate during uplink HTTP throughput tests.	%
QURS051	Access point retransmissions in HTTP DL throughput test	Measures IEEE802.11 access point frame retransmission rate during downlink HTTP throughput tests.	%
QURS052	Access point retransmissions in HTTP UL throughput test	Measures IEEE802.11 access point frame retransmission rate during uplink HTTP throughput tests.	%
QUAP001	TCP downlink throughput	Measures downlink throughput in an TCP file transfer. Measures downlink throughput in an TCP file transfer.	Mbit/s
QUAP002	TCP uplink throughput	Measures uplink throughput in an TCP file transfer. Measures uplink throughput in an TCP file transfer.	Mbit/s
QUAP007	DL throughput of basic HTTP test	Measures downlink throughput in an HTTP document transfer. The test measures both the time of the transfer and the size of the document, from which the throughput in Mbit/s is calculated.Measures downlink throughput in an HTTP document transfer. The test measures both the time of the transfer and the size of the document, from which the throughput in Mbit/s is calculated.	Mbit/s
QUAP011	TCP downlink throughput of E2E maximum	Measured throughput divided by the theoretical maximum throughput that is a function of measured SNR.	
QUAP012	TCP uplink throughput of E2E maximum	Measured throughput divided by the theoretical maximum throughput that is a function of measured SNR.	%
QUAP060	Jitter in VoIP test (G.711)	The variation of delay (jitter) during a VoIP test (G.711).	ms
QUAP061	Jitter in VoIP test (G.719)	The variation of delay (jitter) during a VoIP test (G.719).	ms

QUAP063	Packet loss in VoIP test (G.711)	Packet loss during a VoIP test (G.711).	%
QUAP064	Packet loss in VoIP test (G.719)	Packet loss during a VoIP test (G.719).	%
QUAP072	Jitter in VoIP uplink (talking) test (G.711)	The variation of delay (jitter) during a VoIP uplink test (G.711).	ms
QUAP073	Jitter in VoIP uplink (talking) test (G.719)	The variation of delay (jitter) during a VoIP uplink test (G.719).	ms
QUAP075	Jitter in VoIP downlink (listening) test (G.711)	The variation of delay (jitter) during a VoIP downlink test (G.711).	ms
QUAP076	Jitter in VoIP downlink (listening) test (G.719)	The variation of delay (jitter) during a VoIP downlink test (G.719).	ms
QUAP078	Packet loss in VoIP uplink (talking) test (G.711)	Packet loss during a VoIP uplink test (G.711).	%
QUAP079	Packet loss in VoIP uplink (talking) test (G.719)	Packet loss during a VoIP uplink test (G.719).	%
QUAP081	Packet loss in VoIP downlink (listening) test (G.711)	Packet loss during a VoIP downlink test (G.711).	%
QUAP082	Packet loss in VoIP downlink (listening) test (G.719)	Packet loss during a VoIP downlink test (G.719).	%
QUIP005	WLAN radio frame size, TCP downlink	RF frame size distribution in TCP downlink transfer test. If possible, WLAN devices try to use the maximum transmission unit. Due to radio interference, WLAN devices might reduce the frame size, which leads to relatively larger frame overhead, and eventually to lower data throughput. Note that this indicator measures the size of the data link layer frame, which is defined by IEEE 802.11, thus, this indicator doesn't measure the size of TCP/IP packets.	byte(s)

QUIP006	WLAN radio frame size, TCP uplink	RF frame size distribution in TCP uplink transfer test. If possible, WLAN devices try to use the maximum transmission unit. Due to radio interference, WLAN devices might reduce the frame size, which leads to relatively larger frame overhead, and eventually to lower data throughput. Note that this value is the size of the data link layer frame, which is defined by IEEE 802.11, thus, this indicator doesn't indicate the size of TCP/IP packets.	byte(s)
QUIP013	WLAN radio frame size, basic downlink HTTP test	RF frame size distribution in basic HTTP download test. If possible, WLAN devices try to use the maximum transmission unit. Due to radio interference, WLAN devices might reduce the frame size, which leads to relatively larger frame overhead, and eventually to lower data throughput. Note that this value is the size of the data link layer frame, which is defined by IEEE 802.11, thus, this indicator doesn't indicate the size of TCP/IP packets.	byte(s)
QUIP020	WLAN radio frame size, HTTP DL throughput test	RF frame size distribution in downlink HTTP throughput test. If possible, WLAN devices try to use the maximum transmission unit. Due to radio interference, WLAN devices might reduce the frame size, which leads to relatively larger frame overhead, and eventually to lower data throughput. Note that this indicator measures the size of the data link layer frame, which is defined by IEEE 802.11, thus, this indicator doesn't measure the size of TCP/IP packets.	byte(s)
QUIP021	WLAN radio frame size, HTTP UL throughput test	RF frame size distribution in uplink HTTP throughput test. If possible, WLAN devices try to use the maximum transmission unit. Due to radio interference, WLAN devices might reduce the frame size, which leads to relatively larger frame overhead, and eventually to lower data throughput. Note that this value is the size of the data link layer frame, which is defined by IEEE 802.11, thus, this indicator doesn't indicate the size of TCP/IP packets.	byte(s)

QoS Category			
QUAP016	Requested QoS category in TCP test	Requested QoS category in an TCP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP019	Used QoS category in TCP test	Used QoS category in TCP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP022	Requested QoS category in VoIP test	Requested QoS category in VoIP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP025	Used QoS category in VoIP test	Used QoS category in VoIP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP028	Requested QoS category in HTTP test	Requested QoS category in HTTP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP031	Used QoS category in HTTP test	Used QoS category in HTTP test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP066	Requested QoS category in VoIP test (G.711)	Requested QoS category in VoIP test (G.711). The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP067	Requested QoS category in VoIP test (GSM 06.10)	Requested QoS category in VoIP test (GSM 06.10). The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP069	Used QoS category in VoIP test (G.711)	Used QoS category in VoIP test (G.711). The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP070	Used QoS category in VoIP test (GSM 06.10)	Used QoS category in VoIP test (GSM 06.10). The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP090	Requested QoS category in HTTP throughput test	Requested QoS category in an HTTP throughput test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP091	Used QoS category in HTTP throughput test	Used QoS category in HTTP throughput test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP092	Requested QoS category in HTTP DL throughput test	Requested QoS category in a downlink HTTP throughput test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP093	Used QoS category in HTTP DL throughput test	Used QoS category in downlink HTTP throughput test. The QoS categories are defined by the IEEE 802.11e amendment.	#
QUAP094	Requested QoS category in HTTP UL throughput test	Requested QoS category in an uplink HTTP throughput test. The QoS	#

		categories are defined by the IEEE 802.11e amendment.	
QUAP095	Used QoS category in HTTP UL throughput test	Used QoS category in uplink HTTP throughput test. The QoS categories are defined by the IEEE 802.11e amendment.	#
Signal			
QURS002	Signal strength	Measures the AP transmitted power level of radio signal from the Eye point of view	dBm
QURS001	Channel noise level at Eye	RF noise level in dBm, measured by Eye	dBm
QURS003	AP signal to noise ratio at Eye	Measures the AP transmitted power level of radio signal relative to the power level of noise. Note that this measurement is from the Eye point of view, so the location of the measuring Eye influences greatly to the measurement results of this KPI	dB
AV004	Number of available SSID-AP-pairs	Number of available WLAN connections. A WLAN connection is a combination of SSID-APs that have sent a beacon in the selected area	#
AV010	AP channel	Channel number of an AP as a function of time: "channel(AP_ID, timestamp)"	#
QURS009	Global AP signal level at Eye	Measures the AP transmitted power level of radio signal from the Eye point of view	dBm
QURS010	Global AP signal to noise ratio at Eye	Measures the AP transmitted power level of radio signal relative to the power level of noise. Note that this measurement is from the Eye point of view, so the location of the measuring Eye influences greatly to the measurement results of this KPI	dB
QURS026	Eye-AP signal level in TCP DL	Signal power level between AP and Eye, during an TCP download test	dBm
QURS027	Eye-AP signal level in TCP UL	Signal power level between AP and Eye, during an TCP upload test	dBm
QURS028	Eye-AP SNR in TCP DL	Signal to noise ratio between AP and Eye, during an TCP download test	dB
QURS029	Eye-AP SNR in TCP UL	Signal to noise ratio between AP and Eye, during an TCP upload test	dB
QURS030	Channel noise during TCP DL	Measures the average channel noise on the channel where the TCP download test is done. Calculated as Signal level minus SNR	dBm

QURS031	Channel noise during TCP UL	Measures the average channel noise on the channel where the TCP upload test is done. Calculated as Signal level minus SNR	dBm
QURS040	Eye-AP signal level in HTTP DL throughput test	Signal power level between AP and Eye, during a downlink HTTP throughput test.	dBm
QURS041	Eye-AP signal level in HTTP UL throughput test	Signal power level between AP and Eye, during an uplink HTTP throughput test.	dBm
QURS042	Eye-AP SNR in HTTP DL throughput test	Signal to noise ratio between AP and Eye, during a downlink HTTP throughput test.	dB
QURS043	Eye-AP SNR in HTTP UL throughput test	Signal to noise ratio between AP and Eye, during an uplink HTTP throughput test.	dB
QURS044	Channel noise during HTTP DL throughput test	Measures the average channel noise on the channel where the downlink HTTP throughput test is done. Calculated as Signal level minus SNR.	dBm
QURS045	Channel noise during HTTP UL throughput test	Measures the average channel noise on the channel where the uplink HTTP throughput test is done. Calculated as Signal level minus SNR.	dBm
Action			
TR128	Number of action frames from a managed access point	Measures number of action frames sent by a managed access point	frames/ min
TR129	Number of action frames from a client	Measures number of action frames sent by a client	frames/ min
TR140	Action frame density: Measurement Request	Measures Measurement Request action frame density from a managed access point	frames/ min
TR141	Action frame density: Measurement Report	Measures Measurement Report action frame density from a client	frames/ min
TR142	Action frame density: TPC Request	Measures TPC Request action frame density from a managed access point	frames/ min
TR143	Action frame density: TPC Report	Measures TPC Report action frame density from a client	frames/ min
TR144	Action frame density: Channel Switch	Measures Channel Switch action frame density from a managed access point	frames/ min
Association			
TR116	Number of association requests towards a managed access point	Measures number of association requests sent to a managed access point by clients	frames/ min
TR117	Number of association requests sent by client	Measures number of association requests sent by client	frames/ min

TR118	Number of association responses from a managed access point	Measures number of association responses sent to clients by a managed access point	frames/ min
TR119	Number of association responses sent to a client	Measures number of association responses to a client sent by a managed access point	frames/ min
TR700	Managed access point association response status code	Measures association response status codes of association response frames sent by a managed access point	Code
TR701	Client association response status code	Measures association response status codes of association response frames received by a client	Code
Authentication			
TR112/	Number of authentication requests towards a managed access point	Measures number of authentication requests sent to a managed access points by clients	frames/ min
TR113	Number of authentication requests sent by client	Measures number of authentication requests sent by client	frames/ min
TR114	Number of authentication responses from a managed access point	Measures number of authentication responses sent to clients by a managed access point	frames/ min
TR115	Number of authentication responses sent to a client	Measures number of authentication responses to a client sent by a managed access point	frames/ min
TR704	Managed access point authentication response status code	Measures authentication response status codes of authentication response frames sent by a managed access point	Code
TR705	Client authentication response status code	Measures authentication response status codes of authentication response frames received by a client	Code
Beacons			
TR033	Gross beacon density	Number of beacon management frames per minute on channel	frames/m in
TR037	Beacon traffic air time utilization	Measures beacon air time percentage of total air time	%
TR053	Gross beacon density on channel of access point	Number of beacon management frames per minute on the same channel as the access point	frames/m in
TR057	Beacon channel utilization	Measures beacon air time percentage of total air time on the same channel as the access point	%
Clients			
CL001	Signal level of WLAN devices	Device (clients and APs) information from the Client surveillance (sentinel) test	#
QURS005	Client signal level at Eye	Measures the signal power level of clients, which are connected to APs, from the Eye point of view	dBm

QURS006	Client signal to noise ratio (SNR) at Eye	Measures the signal to noise ratio of clients, which are connected to APs, from the Eye point of view	dB
QURS008	Client data uplink rate	Traffic balance between Client-transmitter (uplink) and AP-transmitter (downlink). If value is 100%, then all traffic has been uplink (from Client to AP). If value is 0%, then all traffic has been downlink. If value is null, then there has been no traffic in either direction	%
TR012/ TR013	Client uplink/downlink data	Measures the amount of uplink/downlink data transmitted by a client	Kbyte
TR019	QoS category in client traffic monitor	The average of all the used QoS-categories during client monitoring. The QoS categories are defined by the IEEE 802.11e amendment	#
TR800	Total number of 5 GHz supporting clients	Absolute number of identified 5GHz supporting clients	#
TR801	Client 5G Hz support ratio	Measures share of clients supporting 5 GHz vs. all clients	%
TR802	Number of 5 GHz capable clients on 2.4 GHz band	Measures number of 5 GHz capable clients not using 5 GHz band	#
Deauthentication			
TR126/ TR127	Number of deauthentication frames from a managed access point / Client	Measures number of deauthentication frames sent by a managed access point / Client	frames/ min
TR706/ TR707	Managed access point / Client deauthentication reason code	Measures deauthentication reason codes of deauthentication frames sent by a managed access point / Client	Code
Disassociation			
TR124/ TR125	Number of disassocation frames from a managed access point / Client	Measures number of disassocation frames sent by a managed access point / Client	frames/ min
TR708/ TR709	Managed access point / Client disassociation reason code	Measures disassociation reason codes of disassociation frames sent by a managed access point / Client	Code
Frame Delivery			
QURS004	AP retries	Number of retransmitted WLAN RF frames divided by the number of all the frames sent to uplink by an AP	%
QURS007	Client retries	Number of retransmitted frames divided by the number of all the frames sent to an AP uplink by a client	%
TR014	Client frame size	Measures the IEEE802.11 frame sizes per client during a client monitoring	byte
TR015	AP radio frame size	Measures the IEEE802.11 frame sizes during a monitoring per AP	byte

TR020	Client DL frame size	Measures the IEEE802.11 downlink frame sizes per client during a client monitoring	byte
TR021	Client UL frame size	Measures the IEEE802.11 uplink frame sizes per client during a client monitoring	byte
TR022	AP DL frame size	Measures the IEEE802.11 downlink frame sizes during a monitoring per AP	byte
TR023	AP UL frame size	Measures the IEEE802.11 uplink frame sizes during a monitoring per AP	byte
Legacy Mode			
TR036	802.11b legacy mode utilization	Measures how many percent of beacon management frames contains "Non-ERP Present" information element	%
TR056	802.11b legacy mode utilization on channel of access point	Measures how many percent of beacon management frames contains "Non-ERP Present" information element on the same channel as the access point	%
Probing			
TR034/ TR035	Gross probe request/response density	Number of probe request/response management frames per minute on channel	frames/ min
TR038/ TR039	Probe request/response traffic air time utilization	Measures probe request/response air time percentage of total air time	%
TR054/ TR055	Gross probe request/response density on channel of access point	Number of probe request/response management frames per minute on the same channel as the access point	frames/ min
TR058/ TR059	Probe request/response channel utilization	Measures probe request/response air time percentage of total air time on the same channel as the access point	%
Reassociation			
TR120	Number of reassocation requests from clients	Measures number of reassociation requests sent to a managed access points by clients	frames/ min
TR121	Number of reassociation requests sent by client	Measures number of reassociation requests sent by client	frames/ min
TR122	Number of reassociation responses from a managed access point	Measures number of reassociation responses sent to clients by a managed access point	frames/ min
TR123	Number of reassociation responses sent to a client	Measures number of reassociation responses to a client sent by a managed access point	frames/ min
TR145	Reassociation success rate	Measures reassociation success rate	%
TR702	Managed access point reassociation response status code	Measures reassociation response status codes of reassociation response frames sent by a managed access	Code

		point	
TR703	Client reassociation response status code	Measures reassociation response status codes of reassociation response frames received by a client	Code
Utilization			
TR030-TR032	Management, Data and Control traffic channel utilization	Percentage of each traffic from total traffic on channel	%
TR040	WLAN traffic air time utilization	Measures total air time percentage	%
TR041	Raw capture CRC error rate	Measures percentage of bad CRC frames of all frames.	%
TR050-TR052	Management, Data and Control traffic channel utilization on channel of access point	Percentage of each traffic from total traffic on the same channel as the access point	%
TR060	Air time utilization	Measures total air time percentage on the same channel as the access point	%
TR061	Raw capture CRC error rate on channel of access point	Measures percentage of bad CRC frames of all frames captured on the same channel as the access point	%
TR100/ TR101	Cisco Compatible Extensions enabled in access point/client	Measures whether Cisco Compatible Extensions are enabled in an access point/client or not	%
TR102	Cisco Compatible Extensions utilization	Measures how many percent of management frames sent to a managed access points have CCX enabled.	%
TR103	Probe request density towards a managed access point	Measures probe request density towards a managed access point.	%
TR104-TR110	Client device 802.11 data rate support	Measures 802.11 data rate support of a client device	%
TR111	Probe response density from managed access point	Measures probe response density from managed access point	frames/ min
TR130/ TR131	Management traffic density from/towards a managed access point	Measures management traffic density from/towards a managed access point	frames/ min
TR132/ TR133	Control traffic density from/towards a managed access point	Measures control traffic density from a managed access point	frames/ min
TR134	Data traffic density from AP	Measures data traffic density from a managed access point	frames/ min
TR135/ TR136	Total traffic density towards/from AP	Measures traffic density of all frames towards/from a managed access point	frames/ min
TR138	Gross frame density per channel	Measures gross frame density per channel	%

TR150	QBSS channel utilization	Measures channel utilization reported by a managed access point.	%
TR151	QBSS station count	Measures station count reported by a managed access point.	#
Volume			
TR001/ TR002	UL/DL data volume	Measures the amount of uplink/downlink data transmitted from an AP during the measurement periods. During the test, Eye listens traffic for T seconds per each access point. The default value for the listening time T is 90 seconds	Kbit/s
TR003	Number of clients per AP	Measures the number of concurrent clients that are using the specified AP during the monitoring. This KPI is measured concurrently with the TR001 AP uplink throughput and TR002 AP downlink throughput	#
TR018	QoS category in AP traffic monitor	The average of all the used QoS-categories during AP traffic monitoring. The QoS categories are defined by the IEEE 802.11e amendment	#