7SIGNAL 7S6300

Wi-Fi 6/6E Sensor

Deployment Guide

Draft Prerelease 0.94

PREFACE

Document scope

This document is aimed at people familiarizing themselves with the 7Signal Sensor system before deployment and to aid with the deployment. After completion of the steps in this document, the 7Signal Sensor should be installed, up and running and ready for Wi-Fi performance management.
This document does not describe how the software operates, how to configure testing or how to read the measurements. The actual use of 7Signal Sensor applications is explained in documents *7signal Sapphire Carat User Guide*, *7signal Sapphire Analyzer User Guide and 7signal Sapphire EyeQ and REST API User Guide.*

FCC:

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/ TV technician for help.

CAUTION:
Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

This equipment is a slave device, the device does not detect radar and does not support ad-hoc operation in the DFS band.
FCC regulations restrict the operation of this device to indoor use only.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.
Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

RF Exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

ISED :

Industry Canada Equipment Standard for Digital Equipment (ICES) – Canada Compliance Statement

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

ICES-003
CAN ICES-003(B) / NMB-003(B)

Innovation, Science and Economic Development Canada (ISED) Compliance Statement

This device complies with ISED's license-exempt RSS standard(s).
Cet appareil est conforme aux normes RSS exemptes de licence d'ISED.

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' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution:
User should also be advised that:
(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
(ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and
(iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate. High-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Les utilisateurs devraient aussi être avisés que
(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
(ii) le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5250-5350 MHz et 5470-5725MHz doit se conformer à la limite de p.i.r.e.;
(iii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande 5725-5825 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.
De plus, les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

The operation of this device is for indoor use only.
The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

Utilisation limitée à l'intérieur seulement
bUtilisation interdite à bord de plateformes de forage pétrolier, de voitures, de trains, de bateaux et d'aéronefs, sauf à bord d'un gros aéronef volant à plus de 10 000 pieds

d’altitude.

Radio Frequency (RF) Exposure Information

The radiated output power of the Wireless Device is below the Innovation, Science and Economic Development Canada (ISED) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.
This device has also been evaluated and shown compliant with the ISED RF Exposure limits under mobile exposure conditions. (antennas are greater than 20 cm from a person's body).

informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l’appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'ISED Canada (ISED). Utilisez l’appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.

Ce périphérique a également été évalué et démontré conforme aux limites d'exposition aux RF d'ISED dans des conditions d'exposition à des appareils mobiles (antennes sont supérieures à 20 cm à partir du corps d'une personne).

CE/UK:

CE RED Compliance Statement

EU Declaration of Conformity
Hereby, ***7SIGNAL, Inc.*** declares that the radio equipment type **7S6300** is in compliance with Directive 2014/53/EU.
The full text of the EU declaration of conformity is available at the following internet address: www.7signal.com/countries

UK Declaration of Conformity
Hereby, ***7SIGNAL, Inc.*** declares that the radio equipment type **7S6300** is in compliance with the essential requirements and other relevant provisions of the Radio Equipment Regulations 2017.
The full text of the UK Declaration of Conformity may be found at h at the following internet address: www.7signal.com/countries

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

CE WiFi 6E
This device is intended for indoor use only when operating in the frequency range 5945 to 6425 MHz which is applicable in countries that support WiFi 6E.

UKCA WiFi 6E
The device is restricted to indoor use only when operating in the 5925 to 6425 MHz frequency range.

RF Exposure warning

This device meets the EU requirements (2014/53/EU) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

RED:

AT	BE	BG	CH	CY	CZ	DK	DE
EE	EL	ES	FI	FR	HR	HU	IE
IS	IT	LT	LU	LV	MT	NL	PL
PT	RO	SI	SE	SK	NI		

UKCA:

All operational modes:
CE:

Technologies	Frequency range (MHz)	Max. Transmit Power
WLAN 2.4 GHz	2412-2472 MHz	19.92 dBm
WLAN 5 GHz	5180-5240 MHz	22.68 dBm
WLAN 5 GHz	5260-5320 MHz	22.79 dBm
WLAN 5 GHz	5500-5700 MHz	22.52 dBm
WLAN 5 GHz	5745-5825 MHz	13.55 dBm
WLAN 6 GHz	5945~6425 MHz	22.61 dBm

UK:

Technologies	Frequency range (MHz)	Max. Transmit Power
WLAN 2.4 GHz	2412-2472 MHz	19.92 dBm
WLAN 5 GHz	5180-5240 MHz	22.68 dBm
WLAN 5 GHz	5260-5320 MHz	22.79 dBm
WLAN 5 GHz	5500-5700 MHz	22.52 dBm
WLAN 5 GHz	5745-5825 MHz	22.71 dBm
WLAN 6 GHz	5945~6425 MHz	22.61 dBm

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 Model 7S6300 (Wi-Fi 6E) Sensor is YLF7S6300
- RoHS and REACH Compliant

Contact information

Contact us at 7SIGNAL

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

TABLE OF CONTENTS

(hold Ctrl+Left Click on text to jump to page)

1 7SIGNAL SENSOR SOLUTION

7Signal Sensors (formerly called Sapphire Eyes) provide you a new way to continuously and automatically measure the health and quality of a wireless network from the user's perspective. Companies and their business processes are becoming increasingly dependent on the performance and service quality of their wireless networks. Thanks to the Sensor, previously called “Sapphire” solution, companies can integrate the quality management of wireless networks with their existing IT and communications technology services.

7Signal systems use Wi-Fi radio sensors to monitor performance and quality in WLAN networks. It also monitors the surrounding radio frequency environment. The performance of the customer’s network is tested against the 7Signal Sonar, a test server that helps simulate client activity on the network. Interactive tests, Sensors and parameters for automatic measurement are managed with a centralized application called the Sapphire Carat. The measurement results are reported by Sapphire EyeQ Dashboard and detailed analysis can be performed with Sapphire Analyzer. All functionalities can be accessed through Sapphire EyeQ which is a central console for 7Signal Sensors.

The 7S6300 Sensor continuously monitors the selected WLAN channels via passive listening, which does not have an impact on network performance. It can also emulate a client device in the target network and use the network and the services provided through it. By analyzing the measurement results, the solution can detect network performance and quality-of-service (QoS) issues. The solution can also produce proactive statistics on the predicted user experience of network performance, which enables the company to increase network capacity before the users notice a loss of performance.

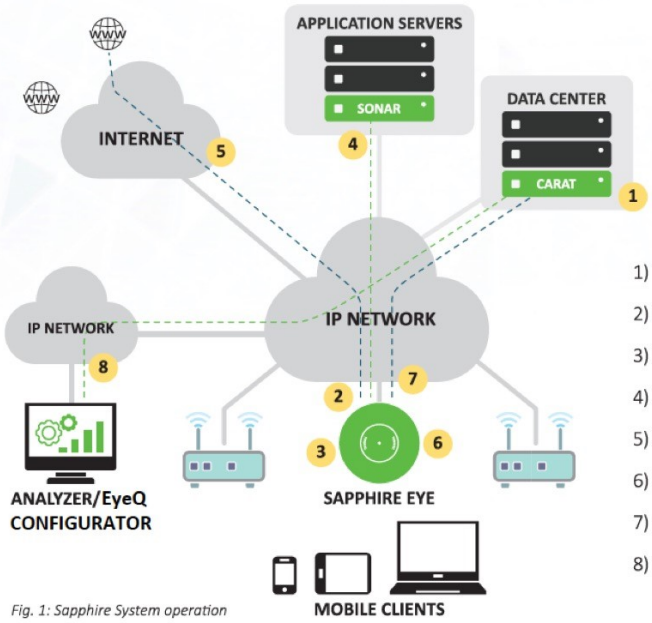
In user emulation tests, also known as active tests, the Sensor connects to the Sonar over the wireless network and uses it like an ordinary production service. The usage may include TCP file transfers, browser downloads, wireless VoIP calls, or connections to another production server. Sensors test the end-user experience by examining the entire data chain from the client to the production service. Active tests can monitor the network even when there are no users in the network. This makes it possible to forecast performance problems and take corrective actions before the service level suffers. Active tests show the availability and quality of services offered over the network and they help administrators see why some applications with their various demands for network performance do not work as expected in the network or some of its areas. When problems occur, active tests can also aid in locating the problem area in the network topology, which often includes WLAN, LAN, and WAN elements.

The key differentiators of 7signal Sensors are user emulation, superb coverage, continuous monitoring, and visibility of network health. Other solutions are often based on monitoring the access point settings. As a result, they do not give any indication of the service quality experienced by the end user. In such limited solutions, the service quality parameters measured are the same as in wired networks. Sensors, by contrast, produce a comprehensive picture of the radio connection quality, where delay, number of retransmissions, and packet loss are taken into account, in addition to other commonly measured parameters.

1.1 Solution Overview

The 7signal quality monitoring solution consists of the 7S6300 (& Eye) sensors, Sonar test servers, the Sapphire Carat management software, and Sapphire web applications for viewing and reporting on the results.

The Sapphire Enterprise setup consists of Sapphire Eye sensors, Carat Analytics Engine software and Sonar Test Server software. The basic principles of operation are described below:



1) The Carat server sends an execute command to the Eye
2) Eye monitors the radio environment and collects stats
3) Eye authenticates and associates to the Wi-Fi network
4) Eye starts upstream and downstream tests against Sonar
5) Eye performs additional throughput tests against websites
6) Eye disconnects from the Wi-Fi network
7) Eye uploads results to the Carat server
8) Performance results are available via Sapphire Analyzer

Fig. 1: Sapphire System operation

1.2 Hardware

The 7signal Sensors are wireless probes that are installed in a central position within the WLAN network. Currently there have been/are seven different hardware variants:

1.2.1 802.11a/b/g/n Indoor Eye (Sapphire Eye 2000)

802.11a/b/g/n version of the Eye has the following main features (partly optional):

- Mechanical parts injection molded polycarbonate plastic
- Linux computer, 1GB Flash memory
- WLAN radio module, 802.11 a/b/g/n support (2.4 GHz, 5.180 GHz - 5.825 GHz)
- Expansion card slots inside the unit: One PCI Express for future use
- Micro SD card slot inside the unit
- Spectrum Analyzer component
- 6 sectored high gain antennas covering 360 degrees in horizontal directions
- RF board with antenna beam selection and low noise amplifiers in the receiver chain
- Electronic compass
- Reset button
- LED indicating status

1.2.2 802.11a/b/g/n/ac wave-1 Gigabit Indoor Eye (Sapphire Eye 2100)

802.11a/b/g/n/ac version of the Eye has the following main features (partly optional):

- Mechanical parts injection molded polycarbonate plastic
- Linux computer, 1GB (2GB Optional) Flash memory, 512MB (1GB Optional) DDR3 SDRAM
- Gigabit Ethernet port (RJ-45)
- Power Over Ethernet (PoE+)
- Gigabit WLAN radio module, 802.11 a/b/g/n/ac support (2.4 GHz, 5.180 GHz - 5.825 GHz)

- Expansion card slot inside the unit: One PCI Express for future use
- Spectrum Analyzer operational over 2.4GHz and 5GHz Wi-Fi bands
- 6 sectored 3x3 high gain antennas covering 360 degrees in horizontal directions
- Electronic compass
- Reset button
- LED status Indicator (blue)

1.2.3 802.11a/b/g/n/ac wave-1 Gigabit Indoor Eye (Sapphire Eye 500)

802.11a/b/g/n/ac version of the Eye has the following main features (partly optional):

- Mechanical parts injection molded ABS based plastic
- Linux computer, 1GB (2GB Optional) Flash memory, 512MB (1GB Optional) DDR3 SDRAM
- Gigabit Ethernet port (RJ-45)
- Power Over Ethernet (PoE+)
- Gigabit WLAN radio module, 802.11 a/b/g/n/ac support (2.4 GHz, 5.180 GHz - 5.825 GHz)
- Expansion card slot inside the unit: One PCI Express for future use
- Spectrum Analyzer operational over 2.4GHz and 5GHz Wi-Fi bands
- Reset button

1.2.4 802.11a/b/g/n/ac wave-2 Gigabit Indoor Eye (Sapphire Eye 2200)

802.11a/b/g/n/ac wave-2 version of the Eye has the following main features (partly optional):

- Mechanical parts injection molded polycarbonate plastic
- Linux computer, 1GB (2GB Optional) Flash memory, 512MB (1GB Optional) DDR3 SDRAM
- Gigabit Ethernet port (RJ-45)
- Power Over Ethernet (PoE+)
- 1.733 Gigabit WLAN radio module, 802.11 a/b/g/n/ac wave2 support (2.4 GHz, 5.180-5.825 GHz)
- VHT bandwidth up to 80MHz with 4 spatial streams
- VHT bandwidth up to 160MHz (where available) with 2 spatial streams
- Spectrum Analyzer operational over 2.4GHz and 5GHz Wi-Fi bands
- 4x4:4 Omni-directional antenna, configurable as directional 1x1:1 in 4 sectors, 2x2:2 in 3 sectors, or 3x3:3 in 2 sectors
- Separately tuned yagi antennae for 2.4GHz (with 6dBi gain and over 30 dB isolation) and 5GHz (with 7dBi gain and over 35 dB isolation)
- Reset button
- LED status indicator (blue)
- LED power indicator (green)
- LED ethernet link/activity status indicator (amber)
- Common 5.5mm by 2.1mm barrel connector for 12v, 2A AC power supply (AC Adapter Optional, US only)

1.2.5 802.11a/b/g/n/ac wave-1 Gigabit Indoor Eye (Sapphire Eye 250)

802.11a/b/g/n/ac version of the Eye has the following main features (partly optional):

- Linux computer, 4GB EMMC Flash memory, 1GB DDR4 RAM
- Gigabit Ethernet WAN port (RJ-45)
- Gigabit WLAN radio module, 802.11 a/b/g/n/ac support (2.4 GHz, 5.180 GHz - 5.825 GHz)
- Spectrum Analyzer operational over 2.4GHz and 5GHz Wi-Fi bands
- USB: 1 x USB 3.0, 1 x USB 2.0
- Reset button
- Power supply: 12V DC jack, AC to DC 12V Power Adapter included

1.2.6 802.11ax (Wi-Fi 6) Gigabit Indoor Eye (Sapphire Eye 6200)

802.11ax version of the Eye has the following main features (partly optional):

- Mechanical parts injection molded polycarbonate plastic
- 1.8GHz NXP i.MX8M computer, 16GB eMMC Flash memory, 4GB DDR4 SDRAM
- Gigabit Ethernet port (RJ-45)

- Power Over Ethernet (PoE+)
- Gigabit WLAN radio module, 802.11 ax support (2.4 GHz, 5.180 GHz - 5.825 GHz)
- Expansion card slots inside the unit: Two PCI Express slots plus one M.2 slot for future use
- Spectrum Analyzer operational over 2.4GHz and 5GHz Wi-Fi bands
- 4x4 broadband (2.4GHz to 7.125GHz omni directional antennas 360° in horizontal directions
- Reset button
- Multicolor (RGB) LED status Indicator
- Operating Temperature Range: 0°C (32°F) to 45°C (113°F)

1.2.7 802.11ax (Wi-Fi 6E) Gigabit Indoor Sensor Model 7S6300

802.11ax Wi-Fi 6E version sensor has the following main features (partly optional):

- Mechanical parts injection molded polycarbonate plastic top and cast Aluminum base
- 2.2GHz Quad-Core IPQ8072A computer, 1GB eMMC Flash memory, 1GB DDR4 SDRAM
- Gigabit Ethernet 1x 10/100/1000/2500/5000Mbps RJ45 Port
- Power Over Ethernet (PoE+)
- Gigabit WLAN radios, 802.11 ax support (2.4 GHz, 5GHz, 6GHz Bands)
- Spectrum Analyzer operational over 2.4GHz, 5GHz and 6GHz Wi-Fi 6E bands
- 4x4 broadband (2.4GHz to 7.125GHz omni antennas 360° in horizontal directions
- Reset button
- LED status Indicators
- Operating Temperature Range: 0°C (32°F) to 40°C (104°F)

2 REQUIREMENTS

2.1 Sonar server requirements

Sonar is the end-point software for Sensor active tests. The Sonar server software runs on the Linux operating system and can be installed on dedicated server or virtual environment.

Table 1: Sizing Requirements Matrix for Sonar VM

# of Sensor Eyes	# of Mobile Eyes	CPU Cores	Clock Speed	RAM	Disk Space	Disk Type	LAN
1-50	< 100	2	2.4 GHz	4 GB	20 GB	HD 5400 rpm	1 GB
51-100	< 1,000	4	2.6 GHz	4 GB	20 GB	HD 5400 rpm	1 GB
100-300	<3,000	4	2.6 GHz	8 GB	20 GB	HD 5400 rpm	1 GB
>300	>3,000	Requires Additional Sonar					

Other generic requirements are:

- Intel and AMD processors
- 1Gpbs Ethernet
- CentOS 6/7 or Red Hat Enterprise Linux 6/7
- When the same Sonar is used also by significant amount of Mobile Eye traffic, resource requirements are higher.

Both onsite and remote Sonars can be used. Onsite Sonar is considered highly preferable. Onsite is within the LAN and allows measuring solely the internal network. Remote Sonar may be in Cloud or central data center running enterprise applications.

2.2 Firewall settings

The following ports should be opened in firewalls:

Source IP/Mask	Destination IP/Mask	Protocol/Port	Comments
Eye Ethernet IP Addr/32	redirector.7signal.com	TCP/UDP 53	Eye DNS Authentication[1]
Eye Ethernet IP Addr/32	Carat IP Addr/32	TCP/7799	Management
Eye Ethernet IP Addr/32	Carat IP Addr/32	TCP/7800	Eye Authentication[2]
Browser (host) IP Addr/32	Carat IP Addr/32	TCP/80	Configurator/Analyzer/EyeQ (HTTP)

[1] If 7signal redirector is used for Sapphire Eye connection
[2] Cloud only

Browser (host) IP Addr/32	Carat IP Addr/32	TCP/443	Configurator/Analyzer/EyeQ (HTTPS)
Eye Wi-Fi IP Addr/32	Sonar server IP Addr/32	TCP/80	Sonar tests
Eye Ethernet IP Addr/32	Sonar server IP Addr/32	TCP/80	Sonar Ethernet tests
Eye Wi-Fi IP Addr/32	Sonar server IP Addr/32	UDP/50000-50300	Sonar VoIP (UL)
Eye Ethernet IP Addr/32	Sonar server IP Addr/32	UDP/50000-50300	Sonar Ethernet VoIP (UL)
Eye Wi-Fi IP Addr/32	Sonar server IP Addr/32	ICMP	Sonar RTT
Eye Ethernet IP Addr/32	Sonar server IP Addr/32	ICMP	Sonar Ethernet RTT
Sonar server IP Addr/32	Eye Wi-Fi IP Addr/32	UDP/9999	Sonar VoIP (DL)
Sonar server IP Addr/32	Eye Ethernet IP Addr/32	UDP/9999	Sonar Ethernet VoIP (DL)

Optional ports

Source IP/Mask	Destination IP/Mask	Protocol/Port	Comments
Sonar server IP Addr/32	NTP server IP Addr/32	UDP/123	NTP

2.3 GDPR compliance

> Important: If GDPR mode is set on, the Sapphire server must be located in an EU country, or be otherwise certified compliant, e.g. Privacy Shield in US. Important compliance GDPR information can be found in Carat User Guide.

Due to EU General Data Protection Regulation (GDPR), it is extremely important that, in addition to other measures you take to comply with the GDPR, you configure Sapphire so that your compliance with GDPR is not adversely affected. Sapphire provides two modes for GDPR operation: on or off:

- When GDPR is off, Sapphire does not collect any client data from Eyes located in EU countries. This is the default mode.
- When GDPR is on, Sapphire collects client data from all countries, including EU.
- If GDPR mode is set to off, it is still possible to enable it on at Organization level.

3 7SIGNAL SENSOR CONNECTIVITY

3.1 Communication security

All connections containing meaningful traffic are encrypted. The cryptographic protocols used are TLS and SSL. The PKI infrastructure (certificates) are used throughout the solution.

3.1.1 SSH for Sensors (Eyes)

Static IP address configuration can be done with the Eye CLI 7config utility. Sensor (Eye) firmware can also be managed with SSH (not recommended normally).

4 INSTALLING 7SIGNAL SENSORS

4.1 Setting up Sensors

4.1.1 Change default SSH password

The Sensor (Eye) root default password is '7signal'. It is strongly advised to change this password as it is a factory default for every sensor unit. The default password is "7signal".

Step 1: Connect to the Sensor (Eye) unit

 # ssh root@<Eye IP address>

Step 2: Change the password by using passwd command

 # passwd

Enter new password

4.1.2 Static IP address configuration

By default, The Sensors have DHCP enabled on their Ethernet interface. In order to configure a static IP address to an Eye:

Step 1: Connect to the Sensor (Eye) unit

 # ssh root@<Eye IP address>

Step 2: Configure IP settings

Set the IP address of the Eye management interface. **DO NOT REBOOT** between configuration steps below.

Type N to "IP configuration changed. Do you want to activate new configuration by restarting Eye services (otherwise, the new configuration will be activated after next boot) [Y/**n**]?"

 # 7config ip set addr <IP address>

Set the network mask of the Eye management interface:

 # 7config ip set mask <dot-format-mask>

Set the port of the Eye management interface (optional – default is TCP/7999):

 # 7config ip set port <port>

Verify all the entered settings with the 'show' command:

 # 7config ip show

Disable DHCP

#7config ip set dhcp off

Step 3: Reboot Eye unit

Reboot the Eye unit to make the changes effective:

 # reboot

4.2 Configuring Sensors to connect a Carat server

The Sensors can be configured to connect to Carat by several ways:

1. Manual configuration. The Carat server IP address, port numbers and organization name are configured for each Eye by using 7config utility
2. DHCP based configuration. The Sensors obtain the Carat IP address, port numbers and organization name by utilizing DHCP options 60 and 43 as described below.
3. DNS redirector based configuration. The Sensors obtain Carat IP address, port numbers and organization name by utilizing specially configured DNS server as described below.

If the Eye is not already provisioned in the Carat server configuration, the Carat server will add the Eye automatically to its network topology configuration. The following rules are applied:

1. Sensors must have been registered to Carat[3].
2. The Eye will be added to the Default Service Area.
3. If a Default Service Area has not been defined, it will be created to first Location of the Organization.
4. If there are no Locations configured yet, a Location named “Default” will be created.
5. If there are no Organizations configured yet, an Organization named “Default” will be created.

4.2.1 Manual configuration

1. Login to the Eye unit using SSH
2. Configure Carat IP address (manual configuration does not support DNS names) and port numbers by issuing “7config conn carat set” command:

   # 7config conn carat set <*Carat server IP address*>:<*Carat server port, typically 7799*>:<*Carat server default port, typically 7800*[4]>[:<*Organization name to which the Eye belongs to*[5]>]
3. Reboot Eye unit:

   # reboot

An example:

 # 7config conn carat set 192.168.10.10:7799:7800:7SignalSolutionsInc

After reboot, the Eye establishes a connection to the Carat server on IP address 192.168.10.10 in the example above. If the Eye is not already in the Carat server configuration, it will be added to the organization 7signalSolutionsInc.

4.2.2 DHCP based configuration

Sensors can obtain Carat server connection information by utilizing DHCP options 60 and 43. A company DHCP server needs to be configured to respond to DHCP option 60. The Sensors send DHCP option 60 with vendor-class-identifier “SevenSignal-Eye” when they request an IP address for their Ethernet interface.
The DHCP server must respond with DHCP option 43, vendor option space must be “SevenSignal”.
Options for Carat connection information are:

Option name	Description	Value type
SevenSignal.carat-address	Carat server IP address	ip-address
SevenSignal.carat-port	Carat server port, typically 7799	unsigned integer 16
SevenSignal.carat-default-port	Carat server default port (Eyes connect to this port initially), typically 7800	unsigned integer 16
SevenSignal.carat-organization	Organization name (optional)	string

For ISC DHCP server, the content of the DHCP server configuration file would be like the following:

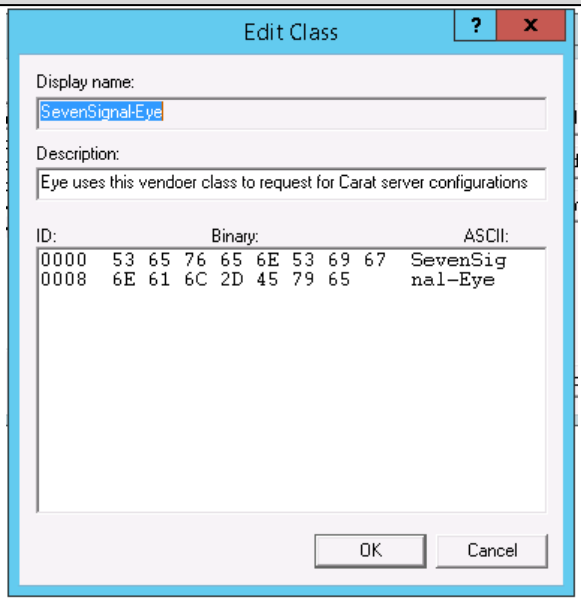
[3] See Carat User Guide
[4] The default port is the TCP port to which new Eyes connect initially. When Eye setup phase is complete, Eye will connect to port 7799.
[5] If the organization name has space characters, escape them by using “\” character. I.e. “My Company” would be “My\ Company”

For DHCP server in Windows Server 2012 R2 Standard, below are the steps to configure the DHCP server. The premise is that DHCP is already installed on Windows server and DHCP scope is setup.

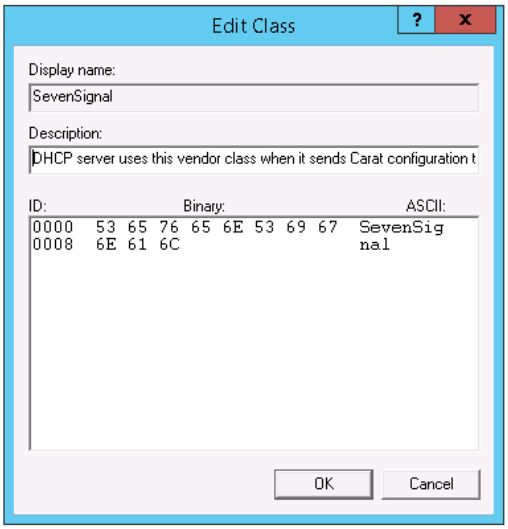
1. Define Vendor Classes

- In Server Manager, navigate to “Tools -> DHCP” to launch DHCP server window.
- From left-side navigation bar, select the windows server. Right-click “IPv4” and select “Define Vendor Classes”.
- Click “Add” to add vendor class “SevenSignal-Eye”, which was used by Sensors to request for Carat server configurations.

```
set vendor-string = option vendor-class-identifier;
option space SevenSignal code width 1 length width 1 hash size 3;
option SevenSignal.carat-address code 1 = ip-address;
option SevenSignal.carat-port code 2 = unsigned integer 16;
option SevenSignal.carat-default-port code 3 = unsigned integer 16;
option SevenSignal.carat-organization code 4 = string;
subnet 192.168.0.0 netmask 255.255.255.0 {
      default-lease-time 200;
      max-lease-time 200;
      option subnet-mask 255.255.25.0;
      option routers 192.168.0.1;
      option domain-name-servers 8.8.8.8;
      class "SevenSignal-Eye" {
            match if option vendor-class-identifier = "SevenSignal-Eye";
            vendor-option-space SevenSignal;
            option SevenSignal.carat-address 10.10.10.8;
            option SevenSignal.carat-port 7799;
            option SevenSignal.carat-default-port 7800;
            option SevenSignal.carat-organization "Huuhaa";
      }
      range 192.168.0.10 192.168.0.100;
}
```



- Add another vendor class “SevenSignal”, which was used by DHCP server to send Carat server configurations to Sensors.



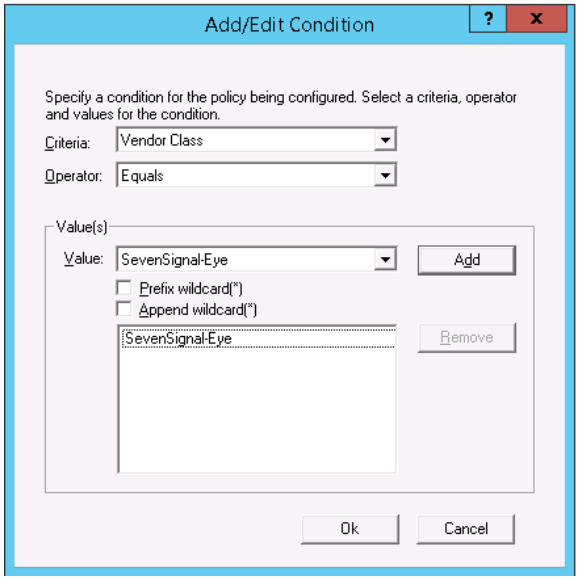
2. Set Predefined Options

- Right-click “IPv4” and select “Set Predefined Options”.
- Choose “SevenSignal” from Option Class pull-down menu. Add the following four policies under this class:

Name	Data type	Code	Value
carat-address	IP Address	1	<Carat_server_IP_address>
carat-port	Word	2	7799
carat-default-port	Word	3	7800
carat-organization	String	4	<Organization_name>

3. Add policy

- From left-side navigation bar, select “Policies” under “Scope”. Right-click it and select “New Policies”.
- Type in a Policy name, for example, “Send Carat configuration to Eyes”. Click Next.
- Add the following condition:
  Criteria: Vendor Class
  Operator: Equals
  Value: “SevenSignal-Eye”



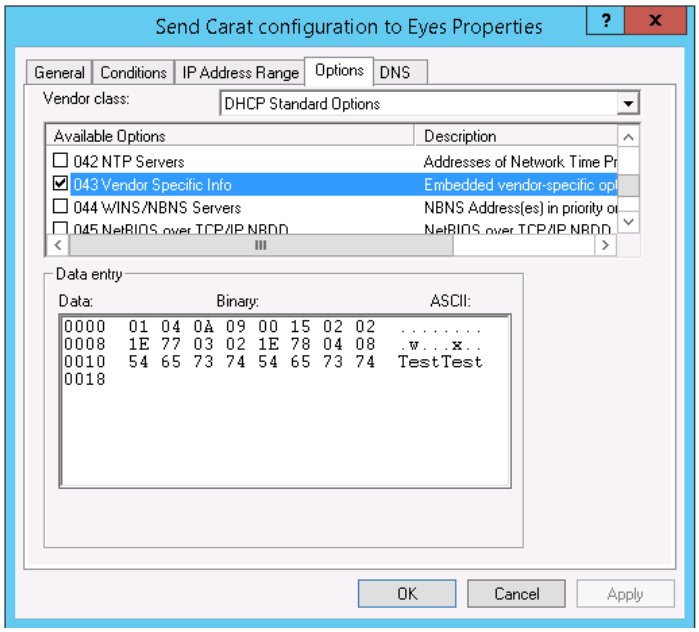
  Click Ok and then Next.
- Configure an IP address range for the Policy.
- Configure Settings for the policy.
  1) Select “006 DNS servers” under “DHCP Standard Options”. Add DNS servers according to your network configurations.
  2) Select “043 Vendor Specific Info” under “DHCP standard Options”. Option 43 is in TLV format: <tag id> (byte) <tag length> (byte) <data vector>. For example, is options set in Step 2 are:

Code	Data type	value
1	IP Address	10.9.0.21
2	Word	7799
3	Word	7800
4	String	TestTest

In TLV format, they are:

Tag ID	Tag length	data vector
01	08	0a 09 00 15
02	02	1e 77
03	03	1e 78
04	08	54 65 73 74 54 65 73 74

Binary value to input in 043 is “01 08 01 09 00 15 02 02 1e 77 03 02 1e 78 04 08 54 65 73 74 54 65 73 74”.



3) Choose “SevenSignal” from Vendor class pull-down menu, select options 001, 002, 003, and 004 under this class. Click Next, and then click Finish. The policy is added.

4.2.3 DNS redirector based configuration

The Eyes can obtain their Carat server connection information from a specially configured DNS server, called a DNS redirector service.
DNS redirector service can be hosted by the Carat server itself, or any other (Linux) host accessible for Eyes.
The DNS redirector service has a record for each Eye. The record contains the IP address of the Carat server as an A record, and port numbers and organization name as TXT records.
If an Eye has been configured to get Carat connection information from DNS redirector service, it will send a DNS query targeted to the DNS redirector service. The queried is formed as follows:
Eye-<*MAC address separated by dashes*>.eye.7signal.com
The DNS redirector server configuration has an entry for Eye:

- A record contains the IP address of the Carat server
- Three TXT records contain port number, default port number and organization information.

DNS redirector server configuration

The following instructions apply to ISC **bind** DNS server

1. Install **bind** package by using yum in a Linux system which will be hosting DNS redirector service.
2. Edit configuration file /etc/named.conf. The most important parts are:
    a. DNS server listen address
    b. Zone information block

Zone information defines e.g. the DNS suffix from which the Eyes will search the Carat connection information:

```
zone "eye.7signal.com" {
      type master;
      file "eye.7signal.com.zone";
      };
```

Example named configuration file /etc/named.conf:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on {
                192.168.10.1;
                };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
        also-notify {
                };
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

zone "eye.7signal.com" {
        type master;
        file "eye.7signal.com.zone";
        };
```

3. Create zone configuration file. Zone information files are located in directory /var/named. In this example, the name of the zone information file must be eye.7signal.com.zone.

Example eye.7signal.com zone file /var/named/eye.7signal.com.zone

```
$ORIGIN eye.7signal.com.
$TTL 86400
;
@       IN      SOA     dns.eye.7signal.com. hostmaster.7signal.com (
                        2001062304
                        21600
                        3600
                        604800
                        86400 )
;
;
                        IN  NS      dns.eye.7signal.com.
dns.eye.7signal.com.    IN      A       192.168.10.1
;
Eye-00-19-F4-EE-00-33.eye.7signal.com.  IN      A       10.10.10.8      ; Carat IP address
                        IN  TXT     "carat-port=7799"           ; Carat TCP port
                        IN  TXT     "carat-default-port=7800"   ; Carat TCP port for default connections
                        IN  TXT     "carat-organization=7signal" ; Organization in Carat configuration
```

When configuring an Eye that should receive Carat connection information from the DNS redirector, add a new record to the end of the file:

Eye-<*Eye Ethernet MAC Address*>.eye.7signal.com. IN A <*Carat IP address*>
IN TXT "carat-port=7799"
IN TXT "carat-default-port=7800"
IN TXT "carat-organization=<*Carat organization to which the Eye is added*>"

After adding a new record to zone file, the named server needs to be restarted:

 # service named restart

Configuring Eyes to obtain Carat connection information from DNS redirector service

By default, the Eyes try to obtain Carat connection information from the DNS redirector service dns.7signal.com. The default DNS redirector service can be changed by using 7config utility.

1. Login to Eye by using SSH.
2. Issue command:

   # 7config conn dns set *<IP address/DNS name of the DNS redirector service>*
3. If a DNS director service is the only source for Carat connection information, use of a DNS redirector service is mandatory:

   # 7config conn dns force on
4. Reboot the Eye:

   # reboot

Removing Eye from DNS redirector configuration

1. Remove Eye records from zone file
2. Restart named server

   # service named restart
3. Login to Eye by using SSH
4. Remove DNS redirector configuration by issuing a command:

   # 7config conn dns remove
5. Remove Carat connection configuration by using a command:

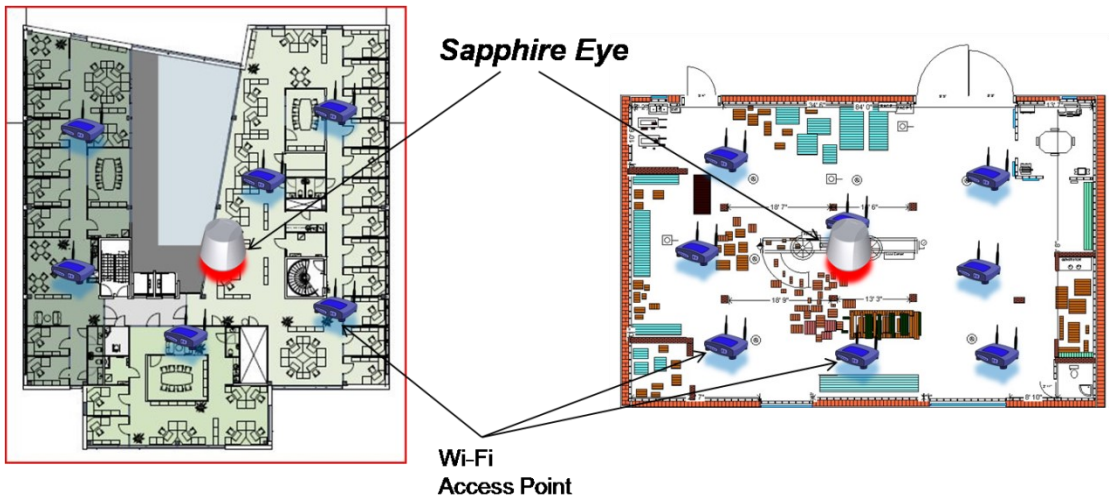
   # 7config conn carat remove

6. Reboot the Eye:

   # reboot

4.3 Mounting Sensors

Mount 7Signal Sensors (previously Eyes) in the most centralized location of the WLAN area. The Sensor can be installed on the ceiling, wall (in a horizontal orientation) or mast.



Sapphire Eyes have extremely sensitive radio technology inside

- The receiving signal is 10-20dB stronger than the basic WLAN end-user
- The transmitted signal is 5-6dB stronger at the access point side than with the basic WLAN end-user

For best accuracy of the WLAN performance, the Sapphire Eye location should be selected so that:

- The average signal level for the managed WLAN access points are between -65dBm and -30dBm. The distance from any access point should be > 10ft/3m.

NOTE: Eyes must not be located too close (> 3ft/1m) to any metal objects and places surrounded by concrete walls.

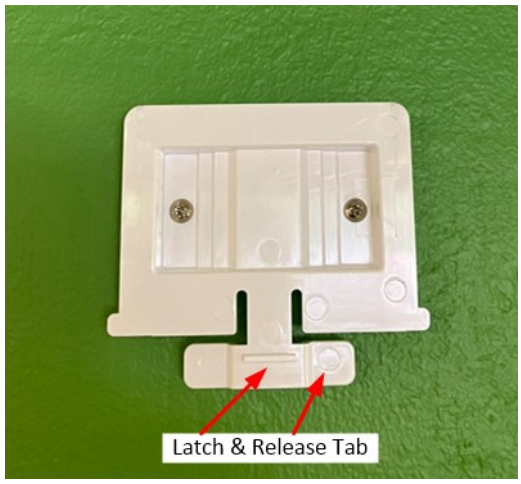
The best installation location is easily verified with:

- Site Survey signal level results

4.3.1 Wall Mounting the 7S6300 Sensor

The 7S6300 may be mounted on a wall or ceiling using the screw mounted wall bracket shown below with two Philips screws holding it in place.

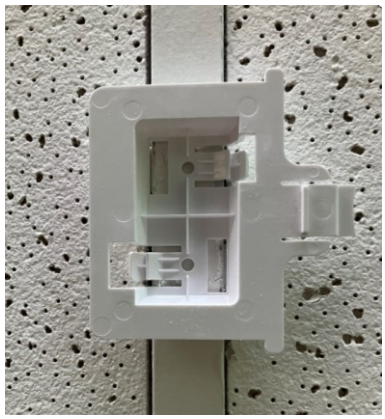
The wall bracket can also be used as a pole mount bracket using the included tie straps through slots in the side of the bracket.



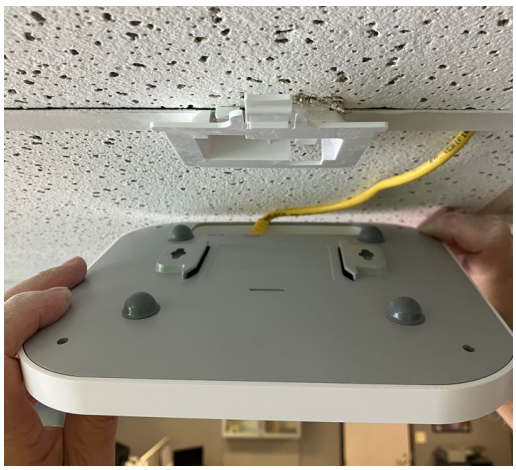
Connect the Ethernet cable or other port wires to the port(s) and slide the unit downward onto the wall bracket until it latches in place.

4.3.2 Ceiling T-Bar Mounting the 6300 Sensor

Two different sizes of T-Bar mounts are included, for 15/16-inch T-Bar, or 9/16-inch T-Bar. Install the T-Bar twist bracket onto a ceiling T-Bar at the desired location.



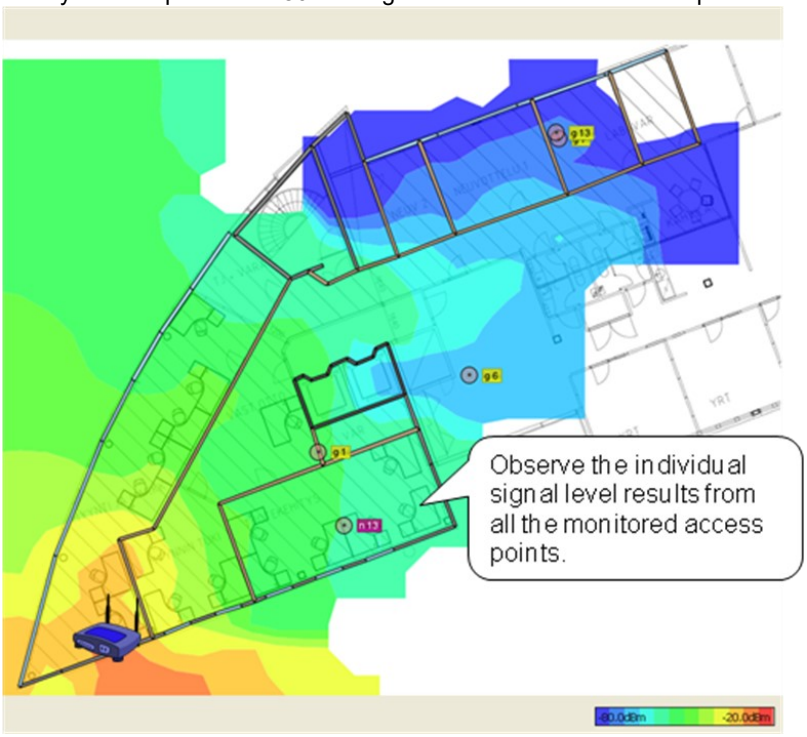
Plug in the network cable or other port cables and slide the unit onto the ceiling bracket until the latch clicks in place.



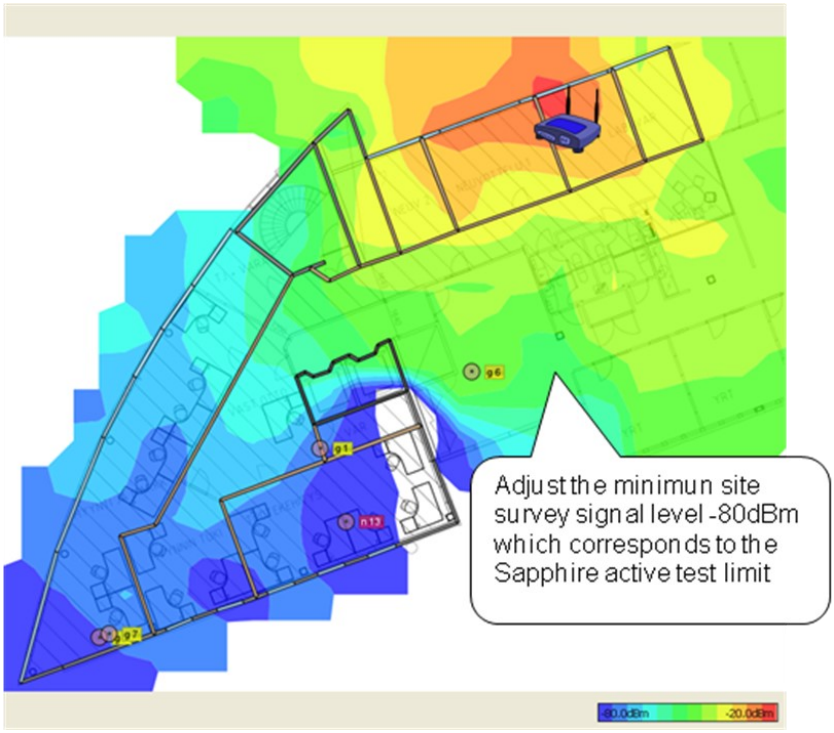
Ensure the Sensor is securily latched in place. The mounting is complete.

4.3.3 Eye installation examples

The Site Survey results are valuable for Eye location estimation. The Eye location is good if the Site Survey heat map shows >-80dBm signal level from all the access points.



The Site Survey results are valuable for Eye location selection



Verify the signal levels from the far end access points

4.4 Installing 7signal Sensor software

4.4.1 Installation from VM templates

Supported VM platforms

VM templates can be downloaded from here: https://dl.cloudsmith.io/public/7signal-solutions-inc/sonar-vm-templates/raw/

This folder contains virtual images of:

- CentOS 7 with Sonar SWs ready installed. The 7signal Sensor Software is located in the /opt/7signal/ directory.
- CentOS 7 base image for Carat installation. This image has preconfigured system layout.

The virtual images have been created for VMware ESXi 5.5-6.7. It should also work with older versions if the hash is converted to SHA1.

Please refer to the below KB article if you are running under ESXi 6.5 or encounter the following error message: "The OVF package is invalid and cannot be deployed" error when deploying the OVA"

https://kb.vmware.com/s/article/2151537

Note if you have received an OVF it may be a multi-part file, however it deploys in the same manner as an OVA file.

https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html

Credentials

The username and password for both the Carat Server and Sonar Server VM's are shown below:

Username: root
Password: 7Signal7

Hardware Recommendations

See https://info.7signal.com/sapphire-eye/server-requirements/

Configuration Instructions

Sonar VM configuration

Step 1: Login to Sonar VM as root user.

Step 2: Configure IP address

Open file /etc/sysconfig/network-scripts/ifcfg-<*ethernet interface name*> in an editor. Edit

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=<*ethernet interface name*>
DEVICE=<*ethernet interface name*>
ONBOOT=yes

IPADDR=<*IP address*>
NETMASK=<*netmask*>
GATEWAY=<*default GW*>

Save the file and reboot the VM.

4.4.2 Installation from sapphire-distribution yum repository

> Root privileges are needed for installation of Sapphire components.

Configure and enable sapphire-distribution yum repository

Note : configuring the yum repository is not needed if running from the 7signal VM template.
Configure and enable sapphire-distribution yum repository by issuing command:

 # curl -1sLf 'https://dl.cloudsmith.io/public/7signal-solutions-inc/sapphire-distribution/cfg/setup/bash.rpm.sh' | sudo codename=7 bash

```
Executing the setup script for the '7signal-solutions-inc/sapphire-distribution'
repository ...

   OK: Checking for required executable 'curl' ...
   OK: Checking for required executable 'rpm' ...
   OK: Detecting your OS distribution and release using system methods ...
 ^^^^: OS detected as: centos 7 (Core)
   OK: Importing '7signal-solutions-inc/sapphire-distribution' repository GPG key
into rpm ...
   OK: Checking for available package manager (DNF/YUM/Zypper) ...
 ^^^^: Detected package manager as 'yum'
   OK: Checking for yum dependency 'yum-utils' ...
   OK: Checking for yum dependency 'pygpgme' ...
   OK: Checking if upstream install config is OK ...
   OK: Fetching '7signal-solutions-inc/sapphire-distribution' repository
configuration ...
   OK: Installing '7signal-solutions-inc/sapphire-distribution' repository via yum
...
   OK: Updating the yum cache to fetch the new repository metadata ...
 ^^^^: The repository has been installed successfully - You're ready to rock!
```

Sonar server

Install Sonar

Install Sonar by issuing command:

 # yum install 7signal-Sonar

Configure Sonar

Configure Sonar by using 7sonar utility. Show the default configuration:

 # 7sonar config

```
Server name           : Sonar
Server port(s)        : 80
Max. clients          : 300
First MOS port        : 50000
Number of MOS ports   : 100
```

 # 7sonar loglevel
```
Log level is INFO
```

Use “7sonar config set” to change the configuration parameters:

- **7sonar config set name <*name*>** : change the Sonar name
- **7sonar config set port <*TCP port number*>** : change the Sonar TCP port number
- **7sonar config set maxclients <*number of clients*>** : change the maximum number of concurrent clients
- **7sonar mosstart <*UDP port number*>** : change the first UDP port number in MOS UDP port pool
- **7sonar mossize <*number of ports*>** : change the MOS UDP port pool size

Use “7sonar loglevel set” command to change the log level (available levels are DEBUG, INFO, WARN and ERROR):

 # 7sonar loglevel set <*log level*>

Start the Sonar server:

Issue the command:

 # 7sonar start

5 UPGRADING SAPPHIRE

5.1 Upgrades from 8.2 onwards

5.1.1 Sonar upgrade

On Sonar server, execute:

yum upgrade

“yum” will download and install possible upgrades automatically.

5.2 Eye upgrade

5.2.1 Eye upgrade (Configurator)

Eye SW upgrade by using Configurator is covered in Carat User Guide.

5.2.2 Eye upgrade (command line)

Step 1: Copy the Eye SW installer to the Eye:

802.11a/b/g/n units (E2000):

 # scp 7signal-Eye_XX.YY.APU3.ipk root@<*IP_address*>:/nand

802.11a/b/g/n/ac units (E2100, E2200, E500):

 # scp 7signal-Eye_XX.YY.MPU1.ipk root@<*IP_address*>:/tmp

802.11a/b/g/n/ac units (E250):

 # scp 7signal-Eye_XX.YY.SCOUT.ipk root@<*IP_address*>:/tmp

802.11a/b/g/n/ac/ax units (E6200):

 # scp 7signal-Eye_XX.YY.MLAN.ipk root@<*IP_address*>:

Step 2: Login to Eye:

 # ssh root@<*eye_ip_address*>

Step 3: Install the Eye new SW package:

802.11a/b/g unit and 802.11a/b/g/n units:

[root@Eye]# cd /nand
[root@Eye]# opkg install 7signal-Eye_XX.YY.APU3.ipk

802.11a/b/g/n/ac unit (E2100, E2200, E500):

[root@Eye]# cd /tmp
[root@Eye]# opkg install 7signal-Eye_XX.YY.MPU1.ipk

802.11a/b/g/n/ac unit (E250):

[root@Eye]# cd /tmp
[root@Eye]# opkg install 7signal-Eye_XX.YY.SCOUT.ipk

802.11a/b/g/n/ac/ax unit (E6200):

[root@Eye]# opkg-cl install 7signal-Eye_XX.YY.MILAN.ipk

Step 4: Reboot:

[root@Eye]# reboot

6 LOG SETTINGS

6.1 Eye log files

NOTE: As this is for Eye logging, all the below commands are to be entered at the prompt of the Eye, not on the Carat or Sonar server.

6.1.1 Application logs

By default, application logs are stored to rotating log files in RAM file system /tmp directory. The name of the log file is /tmp/7signal.log.

The logging can be directed to a persistent storage with 7config log – command. The name of the log file is then /var/log/7signal.log.

The log file can be followed in real-time with the following command:

 # 7config log f

To show the current log file, execute the command:

 # 7config log view

To change logging to persistent storage, issue the following command:

 # 7config log set target persistent

To change logging back to RAM file system, use the following command:

 # 7config log set target buffer

The following command shows the log level and log target information:

 # 7config log show

6.1.2 System logs

Eye 2100/500/2200/250/6200 store system logs always to persistent storage. The name of the log file is /var/log/syslog.

6.2 Sonar log (Linux)

The log file - sonar-server.log - is located by default in /<*Sonar installation directory*>/Sonar/log.

7 SAPPHIRE PROCESS MANAGEMENT

7.1 Sonar

Sonar is a service on Linux systems:

7sonar <parameter-from-the-bullet-list>

- start
- stop
- restart
- status

7.2 Eye

NOTE: The following command requires an SSH session into the Eye.

The utility 7config controls the Eye configuration. See more details for the tool in chapter 9. The process is controlled with command group *run*.

7config run <parameter-from-the-bullet-list>

- start
- stop
- restart
- status

8 TROUBLESHOOT

8.1 No access to Sonar server, active test failed

1. Check that Sonar server is configured correctly to Carat (Manage | Test endpoints)
    a. IP address and Sonar port
2. Check the process at the Sonar host with the command
    a. service 7signalSonar status
    b. One can remotely telnet or http <sonar-ip-addr> <port-default-80>
        i. Sonar opens the connection and closes it after 1 second of idle time or displays XML Error.
3. Check Sonar log for error messages
4. Check that Sonar ports are open on the firewall(s)
5. Check that the WLAN encryption key has correct definition (or run a Manual test selecting the Eye Ethernet Interface to narrow down the problem).
6. Check that the key is bound to the managed network
7. Check connectivity options and requirements for Eye and Sonar

8.2 Eye IP address forgotten

8.2.1 Reset Eye IP configuration

From Sapphire release 5.2 onwards, Eye restarts and obtains its IP address from a DHCP server. In earlier Sapphire releases, Eye IP will be reset back to static 192.168.0.1.

Indoor Eye 2000

1. Locate Reset button of the Indoor Eye unit.
2. Push and hold the Reset button ~ 30 seconds
3. Eye LED light blinks 5 times
4. Release the Reset button

Indoor Eye Eye 2100/500/2200/250

1. Locate Reset button of the Indoor Eye unit.
2. Push and hold the Reset button ~ 30 seconds
3. Release the Reset button
4. Wait until LED light blinks 5 times

9 COMMAND-LINE UTILITY FOR EYE

9.1 Overview

7config is a command line utility for configuring various things on the Eye unit. Commands are divided into command groups so that each group contains one or more commands. A command may also have an argument and a value.

Currently supported command groups are the following:

- ip: IP address management.
- keys: Key storage management.
- ap: Access point configuration storage management.
- conn: Connection management.
- run: Software run-state management.
- txp: External antenna configuration.
- log: Log configuration
- iface: Global interface management.
- verify: System verification.

Command group specific help can be shown with command:

```
7config <group> help
```

General help can be shown with command:

```
7config help
```

9.2 7config ip command group

This command group contains commands for configuring IP configuration of the Eye Ethernet interface. Currently, it is possible to show the current IP configuration, set IP address, network mask and default gateway address (or alternatively, use DHCP configuration) of the management interface. It is also possible to take a backup from the current IP configuration, and restore the configuration from the backup.

```
7config ip <CMD> <ARG> [VALUE]
'set' command arguments:
   addr      Set IP address of management interface (eth0)
             VALUE = Valid IPv4 address
   mask      Set netmask of IP address of management address
             VALUE = Valid IPv4 netmask in dotted format
                 (x.x.x.x)
   port      Set management port
             VALUE = TCP port number
   gateway   Set IP address of default gateway (optional)
             VALUE = Valid IPv4 address
                 or 'remove' to remove configured gateway
   dhcp      Set DHCP on/off
             VALUE = on|off
'show' command arguments: none
'backup' command arguments:
   create    Create backup from existing IP configuration.
   restore   Restore IP configuration from backup.
```

Examples:

Setting IP address of the management interface:

```
# 7config ip set addr <IP_address>
```

Setting network mask of the management interface:

```
# 7config ip set mask <mask_in_dotted_format>
```

Setting port of the management interface:

```
# 7config ip set port <IP_address>
```

Create backup from current IP configuration:

```
# 7config ip backup create
```

Restore IP configuration from a backup:

```
# 7config ip backup restore
```

Show current IP configuration:

```
# 7config ip show
```

9.3 Keys command group

This command group contains command for managing WLAN network keys stored on the Eye unit. Currently, the only supported operation is to destroy all WLAN keys from the Eye.

```
# 7config keys destroy
```

9.4 AP command group

This command group contains commands for managing the Access Point information stored to the Eye unit. Currently, the only supported operation is to destroy all Access Point information on the Eye.

```
# 7config ap destroy
```

9.5 Conn command group

This command group contains commands for managing encryption settings of management traffic between the Eye unit and Carat server, and command for configuring the Carat server connection information (how the Eye can connect to a Carat server).

```
7config conn <CMD> <ARG> [VALUE]
'cert' command arguments:
   set       Set management connection encryption certificate file.
             VALUE = Certificate file name. File must reside
                  in /nand/etc/certificates directory.
   show      Show current encryption certificate file name.
   install   Install certificate from certificate archive.
             VALUE = Archive name (<prefix>-7signal-certs.tar.gz)
'pwd' command arguments:
   set       Set encryption certificate password.
   install   Install password from password archive.
             VALUE = Archive name (<prefix>-7signal-pwds.tar.gz)
'encryption' command arguments:
   install   Install encryption certificate and password
```

```
            from combined certificate and password archive.
            VALUE = Archive name (<prefix>-7signal-all.tar.gz)
'ssh' command arguments:
   show       Show SSH public key or tunnel configuration.
            'show key': Show SSH public RSA key.
            'show tunnel': Show tunnel configuration.
   set tunnel Set SSH tunnel configuration.
            Set tunnel state:
              'set tunnel state <enabled|disabled>'
            Set Carat server address:
              'set tunnel carat <address/host name>'
            Set user name in Carat server:
              'set tunnel user <username>'
            Set local Eye management connection TCP port number:
              'set tunnel ltcpp <port>'
            Set local Eye SSH port number:
              'set tunnel lsshp <port>'
            Set remote Eye management connection port number
            in Carat server:
              'set tunnel rtcpp <port>'
            Set remote Eye SSH port number in Carat:
              'set tunnel rsshp <port>'
'carat' command arguments:
   show       Show Carat configuration.
   set        Set Carat configuration manually:
            VALUE=Carat connection information in following
                 format:
                 <IP address>:<port>:<default port>[:organization]
   remove     Remove Carat configuration.
'dns' command arguments:
   show       Show 7signal DNS server information.
   set        Set 7signal DNS server name/address
            VALUE=DNS name or IP address of 7signal DNS server.
   remove     Remove 7signal DNS configuration. Defaults to
            'dns.7signal.com'
   force      Force DNS. Eye will wait until it gets Carat configuration
            from DNS server.
            VALUE=<on>|<off>
```

Examples

Install certificate from certificate package:

```
# 7config conn cert install <certificate package file>
```

Install password from password package:

```
# 7config conn pwd install <password package file>
```

Configure Eye to connect a Carat server:

```
# 7config conn carat set 192.168.10.10:7799:7800:SomeCompany
```

Configure Eye to connect a Carat server by using DNS redirector service

```
# 7config conn dns set <IP address/DNS name of DNS redirector service>
```

9.6 Run command group

This command group contains commands for managing Eye software run-state. Currently supported operations are to ask current status of the software, to start, stop and restart the software, activate software version, show installed version, uninstall a software version, and to reconfigure Eye unit without restarting it.

```
7config run <CMD> [ARG]
   status    Show status of Eye software.
   start     Start Eye software.
   stop      Stop Eye software.
   restart   Restart Eye software.
   reconfig  Reconfigure unit and restart Eye software.
   show      Show active software version.
   list      List installed software versions.
   activate  Activate software version.
             Example: 7config run activate 02.80
                      Activates version 2.80
   remove    Uninstall Eye software version.
             Example: 7config run remove 02.61
                      Uninstalls SW version 2.61
```

Examples:

Query status of the Eye software:

```
# 7config run status
```

Start the Eye software:

```
# 7config run start
```

Stop the Eye software:

```
# 7config run stop
```

Restart the Eye software:

```
# 7config run restart
```

List installed Eye softwares:

```
# 7config run list
```

Reconfigure the Eye:

```
# 7config run reconfig
```

9.7 Txp command group

This command group contains commands for showing and setting of TX power related parameters. Currently supported operations are showing of TX power settings, setting default TX power, setting gain of an external antenna and setting cable loss of the external antenna.

```
7config txp  [ARG] [VALUE]
'show' command arguments:
  default   Show default TX power.
   ext      Show configured gain of external antenna.
   cable    Show configured cable loss of external antenna.
   If no arguments given, all information will be shown.
```

'set' command arguments:
default Set default TX power.
VALUE = TX power (dBm).
ext Set gain of external antenna.
VALUE = Gain of external antenna (dBi).
cable Set cable loss of external antenna.
VALUE = Cable loss of external antenna cable (dB).

Examples:

Show all information in TX power configuration:

```
# 7config txp show
```

Show configured cable loss:

```
# 7config txp show cable
```

Set external antenna gain to 10 dBi:

```
# 7config txp set ext 10
```

9.8 Log command group

This command group contains commands for configuring log production of the Eye. Logs can be produced either to a ring buffer on RAM (Eye 1000/2000) or to a RAM disk (Eye 2100/500/2200/250) (this is the default, can be read by logread command), or to persistent storage on NAND flash. In 802.11a/b/g, the persistent log resides in the folder /nand/ as files named syslog*, in 802.11a/b/g/n in folder /var/log as files named messages, and in 802.11a/b/g/n/ac (Eye 2100/500/2200/250) in folder /var/log as files named 7signal.log.

Reading of the log files is either from the chosen storage directly or with the command logread (Eye 1000/2000 only).

By default, only the critical messages are logged. Currently, the supported commands are:

- show which shows the current log configuration.
- set
  - level which sets the current level of logging
  - default which sets default level of logging at system start-up
  - target which sets logging target, ring buffer or NAND.

Log level set by 'set level' command remains active until restart of the system. Default log level after installation is "ERROR".

Log levels are the following:

- CRIT - Critical messages
- ERROR - Error messages
- WARN - Warning messages.
- INFO - Informational messages.
- DEBUG - Debug messages.

Log levels are cumulative, i.e. the level CRIT logs only critical messages, WARN logs all levels including CRITICAL, ERROR and WARN messages. DEBUG logs all possible messages.

Log command group arguments:

```
  'show'       Show log configuration.

  'set' command arguments:
     level     Set log level.
               VALUE = CRIT | ERROR | WARN | INFO | DEBUG
     default   Set default log level. This log level will be active
               when 7signal software starts.
               VALUE = CRIT | ERROR | WARN | INFO | DEBUG
     target    Set logging target.
               VALUE = buffer | persistent
```

Examples:

Set log level to DEBUG:

```
# 7config log set level DEBUG
```

Set log level to WARN:

```
# 7config log set level WARN
```

Set default log level to ERROR:

```
# 7config log set default ERROR
```

Show default log level:

```
# 7config log show
```

Set logging target to NAND flash:

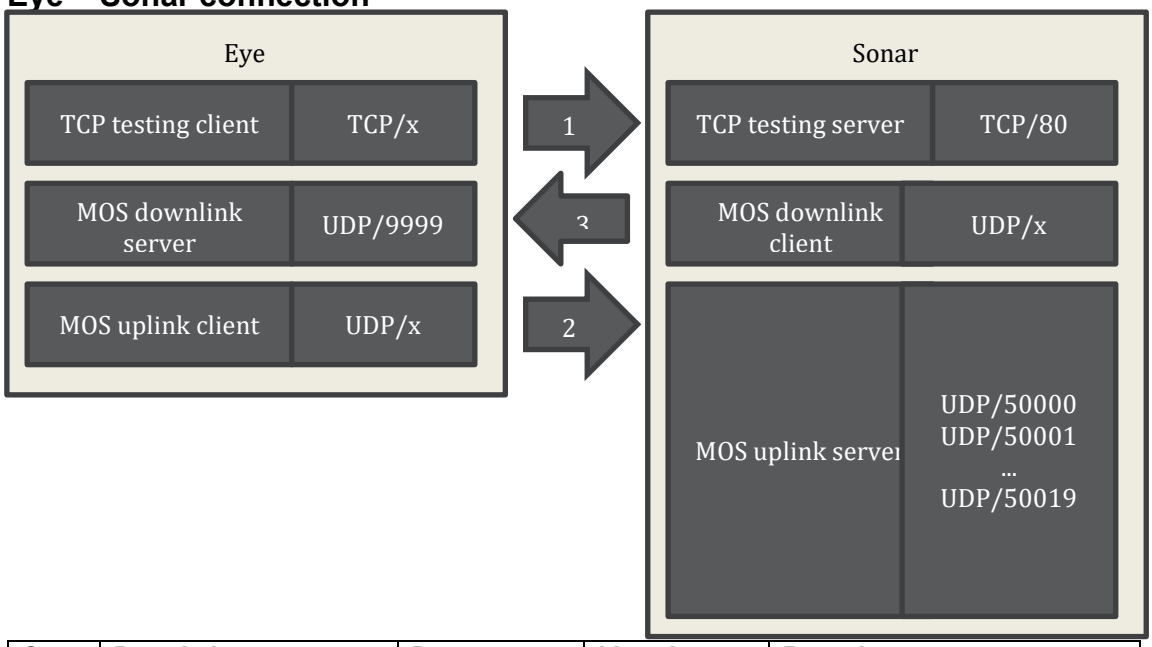
```
# 7config log set target persistent
```

APPENDIX A. LOGICAL CONNECTIONS

Sapphire elements and their logical connections are in the picture below:

- **Eye** – a WLAN probe with both WLAN interface (WLAN client and analysis functions) and Ethernet interface (management functions).
- **Sonar** – Server software emulating various business services for testing purposes. Deployment method is two-fold as follows: 7signal Solution: the application is running in hosts chosen by the customer. 7signal Site Miner: a dedicated mini-laptop is running the application.
- **Carat** – centralized management software, a stand-alone application. Deployment method is two-fold as follows: 7signal Solution: the application running in a host chosen by the customer. 7signal Site Miner: a dedicated normal laptop running the application.
- **Analyzer** – A web-application for measurement visualization that is deployed in conjunction of the Carat server software.
- **Internet browsers** – Thin-clients for Application server. Not provided by 7signal.

Eye – Sonar connection



Conn ID	Description	Data content	Listening port(s)	Remarks
1	Test management and typical test connection	Test control message and pseudo-data	TCP/80 Configurable during Sonar deployment	Traffic is properly encapsulated HTTP. Uses Eye WLAN interface.
2	MOS test, uplink direction	MOS test specific data	udp/50000 – 50019 Configurable during Sonar installer	Optional. Uses Eye WLAN interface. The number of port varies between 0 and 20. The port numbers are consecutive. By default 10 ports are opened.
3	MOS test, downlink direction	MOS test specific data	udp/9999 Configurable during Eye deployment	Optional. Uses Eye WLAN interface.

Main purpose: Eye connects through WLAN interface to the remote server that simulates or emulates business applications.

Important notice: The Sonar servers may be numerous and the network topology between Eye and Sonar may vary radically and could contain numerous firewalls. 7signal has no control over the network topology and cannot influence arbitrary devices and network elements between the endpoints. To ensure fluent deployment, the user/configurator has to have a thorough understanding of the network between the endpoints and the ability to affect all the network elements necessary.

To test and use the wireless connection the following variables must be known:

- ESSID – test parameter to connect to a particular wireless network.
- WLAN encryption

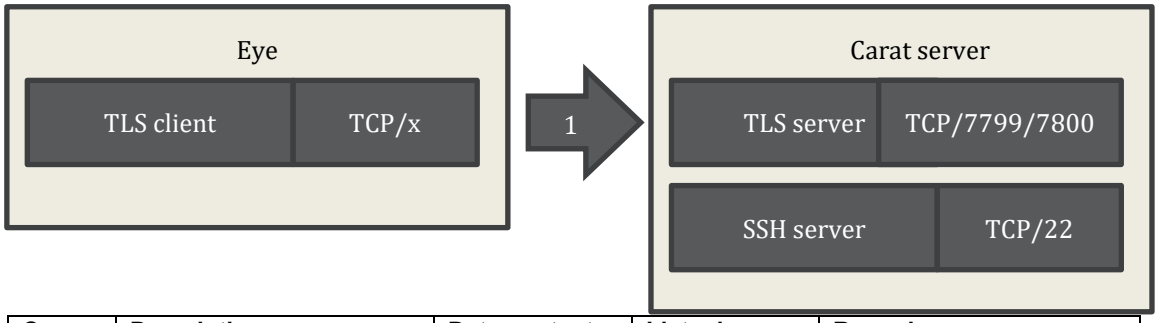
Network keys – pre-shared keys, certificates or similar - are stored in Eye file system by Carat application.
To be observed: the target wireless network may be configured with MAC address restrictions so the MAC address of WLAN interface of the Eye unit must be white-listed as a network client. The Eye does not act as an access point of the wireless network. The Eyes WLAN MAC address can be discovered using the Configurator or via SSH and executing a ifconfig –a.

MOS test connections

MOS test requires additional ports to be used. The MOS traffic test uses special-purpose traffic with an identical fingerprint to a VoWLAN call.
The Sonar may serve numerous Eyes concurrently and therefore it is able to listen to numerous UDP ports for incoming VoIP calls. Ports are listened on a per-need basis. One UDP port may serve one Eye at a time so the number of concurrent MOS tests on a single Sonar is dictated by the number of available ports that are configured during the Sonar deployment phase.
The Eye has only one UDP port open for VoIP calls as it communicates with a single Sonar at a time.

Carat – Eye connection

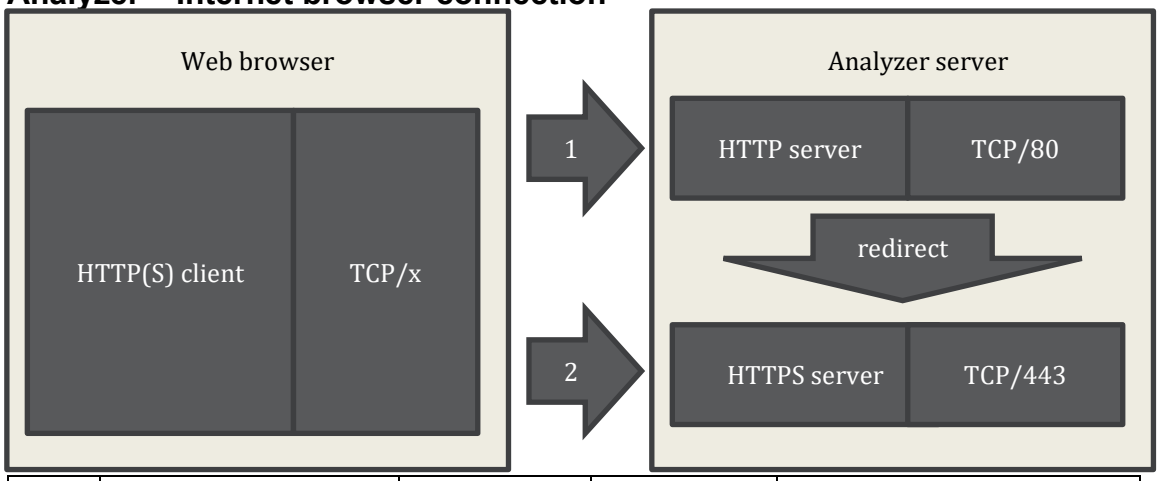
Eyes connect to Carat server (”Cloud setup”).



Conn ID	Description	Data content	Listening port(s)	Remarks
1	Carat server	TLS encrypted binary protocol for management and testing.	TCP/7799 TCP/7800 Configurable in Carat deployment	Uses Carat Ethernet interface.

In this case the Carat acts as a server and Eyes are clients.

Analyzer – Internet browser connection



Conn ID	Description	Data content	Listening port(s)	Remarks
1	Standard HTTP connection.	Standard HTTP traffic for creating a HTTPS connection.	TCP/80 Configurable during Analyzer deployment.	Redirects to HTTPS port of Application server.
2	Standard HTTPS connection for measurement requests and responses.	Secure HTTP. Report and chart requests and responses.	TCP/443 Configurable during Application server deployment.	Business connection for Application server.

APPENDIX B. BANDWIDTH REQUIREMENTS

NOTE: the volume estimates are estimates and vary based on the configuration.

9.8.1 Eye – Sonar

From	To	Medium	Traffic motivator	Volume estimate	Major factor
Eye	Sonar	WLAN	Automated test engine and interactive testing by users.	Low, each request is a few hundred bytes. Eye acts as one WLAN end-user would do, one operation per minute.	The test profile that the Eye is running. In case of MOS test VoFi traffic is transmitted as long as requested in the test parameters, constant traffic at the rate of 100 kBs/s.
Sonar	Eye	WLAN	Responses to client.	Typically pseudo-data that varies based on the test parameters.	MOS test most probably contain significant amount of data.

For example, the TCP download test transfers by default 2 megabytes of data that does not take long. The amount of data is exceptionally high for data transfer in a logistics environment but on the other hand in office environment transfer of this size is relatively low. The test parameter should be adjusted, either to simulate typical transfer or to save the bandwidth while keeping the transfer size high enough to give measurements out of the network.

9.8.2 Eye – Carat/Carat – Eye

From	To	Medium	Traffic motivator	Volume estimate	Major factor
Carat	Eye	Ethernet	Configuration actions and manual testing by users.	< 1 kB/minute. The binary protocol for requests is volume-efficient.	Duration of one test varies from a few seconds to almost minutes per request depending on the test type.
Eye	Carat	Ethernet	Responses to client.	100 kB /minute.	Spectrum Analysis and MOS test most probably contain significant amount of data.

The data transferred in most cases is results of analysis, sometimes raw measurements.
Naturally the number of Eyes is directionally proportional the traffic load as each Eye connection are independent and concurrent. One single Eye typically executes a test in one minute in the average. However, there are tests that finish in 10 seconds (practical minimum) and few tests run few minutes.
The communication protocol is both minimal and binary so the traffic from Carat to Eye is very economic. The measurement result minimum is around 100 bytes in one message and the top range is the spectrum measurement (not available in all configurations) that returns approximately 300 times a 50 byte result unit.
In data communications sense the traffic for single Eye is minimal.

9.8.3 Analyzer server – Analyzer client (browser)

From	To	Medium	Traffic motivator	Volume estimate	Major factor
Analyzer host	Clients in WWW	Ethernet, general networking	User actions	Volatile. Like one HTTP client.	User activity. Per any request the amount of requested KPIs is the driving factor.

There is no continuous machine-to-machine interaction, all activities are initiated by the user. The amount of traffic depends completely on user-decisions. Server output typically contains graphics. Medium duty cycle.