7SIGNAL®
THE WI-FI PERFORMANCE COMPANY

7signal Sapphire

Deployment 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 people familiarizing themselves with the 7signal Sapphire system before deployment and to aid with the actual deployment. After completion of this document, 7signal Sapphire is 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 Sapphire 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 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) Contains FCC ID: YLFSE2200WL.

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) Contains IC: 11766A-2200WL.

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.

7SIGNAL®
THE WI-FI PERFORMANCE COMPANY

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 2200
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 email:	info@7signal.com
● by phone:	216-777-2900
● support:	support@7signal.com

TABLE OF CONTENTS

1

7SIGNAL SAPPHIRE SOLUTION

7signal Sapphire provides 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 Sapphire solution, companies can integrate the quality management of wireless networks with their existing IT and communications technology services.

7signal Sapphire uses monitoring sensors called Eyes 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, Eyes 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 access through Sapphire EyeQ which is a central console for 7signal Sapphire.

The Eye 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 then 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.

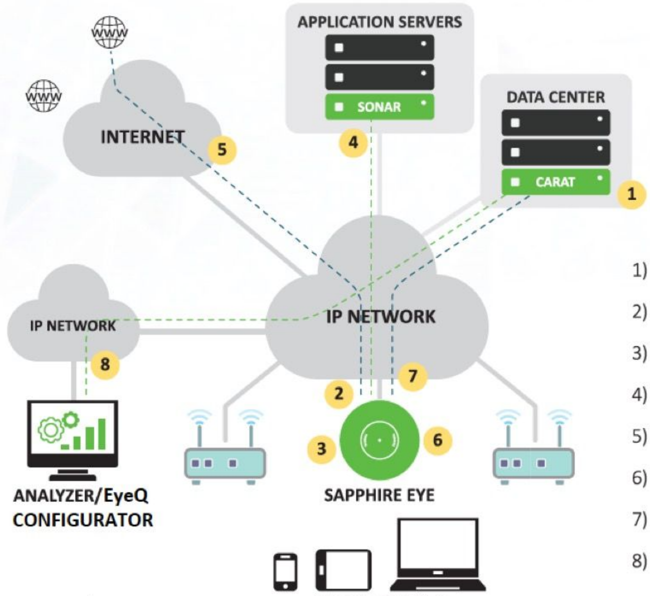
In user emulation tests, also known as active tests, the Eye connects to the Sonar over the wireless network and uses it like an ordinary production service. The usage may include TCP file transfers, browser downloads, wireless VoIP calls, or connections to another production server. Sapphire tests the 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 to locate of the problem area in the network topology, which often includes WLAN, LAN, and WAN elements.

The key differentiators of 7signal Sapphire 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. Sapphire, by contrast, produces 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 Sapphire quality monitoring solution consists of the Sapphire Eye monitoring 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 Sapphire Eye is a wireless probe or a monitoring station that is installed in a central position within the WLAN network. Currently there are five different hardware variants: the Standard Eye supporting 802.11a/b/g standards, Standard Eye supporting 802.11a/b/g/n standards, Indoor Eye supporting 802.11a/b/g/n standards and Gigabit Indoor Eyes supporting 802.11a/b/g/n/ac standards.

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)

2

Requirements

2.1 Carat server requirements

A cloud-based deployment is preferable because it ensures your software is always kept up to date. However, if you need to install a servers inside your network for security reasons, then you must follow the requirements specified in the table below.

Basic server dimensioning guidelines:

# of Sapphire Eyes	CPU Cores	CPU Type	RAM	DB Disc Space / IOPS	Logfile Disc Space / IOPS	Backup Disc Space / IOPS
1-25	2	Intel Xeon E5-2640 @ 2.50GHz (Sandy Bridge) or newer	32GB	75GB / 500	75GB / 125	150GB / 150
26-50	2	Intel Xeon E5-2640 @ 2.50GHz (Sandy Bridge) or newer	48GB	150GB / 2500	150GB / 250	300GB / 150

51-100	4	Intel Xeon E5-2640 @ 2.50GHz (Sandy Bridge) or newer	64GB	300GB / 5000	300GB / 300	600GB / 150
101-150	6	Intel Xeon E5-2697 v2 @ 2.70GHz (Ivy Bridge) or newer	96GB	450GB / 7500	450GB / 500	900GB / 150
151-200	6	Intel Xeon E5-2697A v4 @ 2.60GHz (Broadwell) or newer	128GB	600GB / 10000	450GB / 750	1.2TB / 150
201-250	6	Intel Xeon Gold 6144 @ 3.50GHz (Skylake SP) or newer	176GB	750GB / 12500	750GB / 850	1.5TB / 150
>250	Please Contact Support					

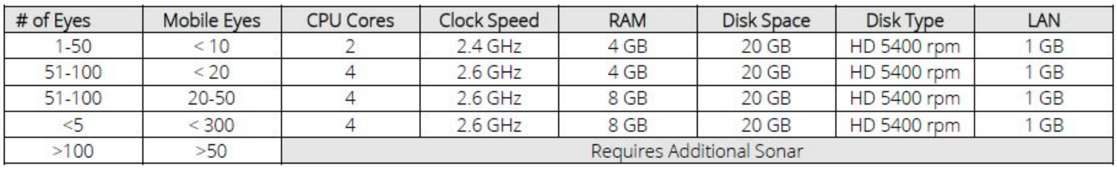
These requirements are only guidelines. Utilization may increase or decrease with RF topology and test profile configuration. We require that the VM have dedicated resources. There should not be any memory over-commitment or shared CPUs. Storage space requirements are based on 3 months data retention and will increase 33.3% each revolving month.

Consult 7signal sales or customer service for additional information.

2.2 Sonar server requirements

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

Basic server dimensioning guidelines:



# of Eyes	Mobile Eyes	CPU Cores	Clock Speed	RAM	Disk Space	Disk Type	LAN
1-50	< 10	2	2.4 GHz	4 GB	20 GB	HD 5400 rpm	1 GB
51-100	< 20	4	2.6 GHz	4 GB	20 GB	HD 5400 rpm	1 GB
51-100	20-50	4	2.6 GHz	8 GB	20 GB	HD 5400 rpm	1 GB
<5	< 300	4	2.6 GHz	8 GB	20 GB	HD 5400 rpm	1 GB
>100	>50	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 are 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.

2.3 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]
Carat IP Addr/32	Eye Ethernet IP Addr/32	TCP/22	SSH connection[3]
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

[3] On-premise 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

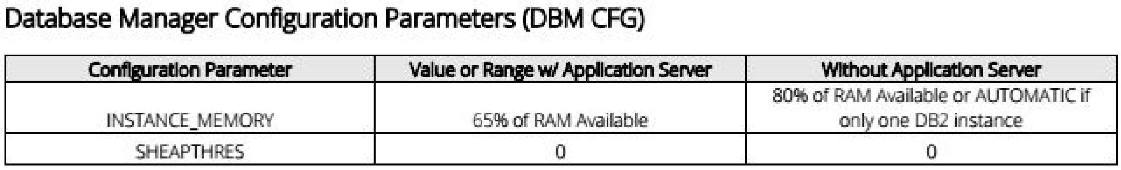
Source IP/Mask	**Destination IP/Mask**	**Protocol/Port**	**Comments**
Sonar server IP Addr/32	NTP server IP Addr/32	UDP/123	NTP

Carat IP Addr/32	NTP server IP Addr/32	UDP/123	NTP
Sonar server IP Addr/32	DNS server IP Addr/32	TCP/UDP/53	DNS
Carat IP Addr/32	DNS server IP Addr/32	TCP/UDP/53	DNS
Carat IP Addr/32	SNMP server IP Addr/32	UDP/162	SNMP Trap
Carat IP Addr/32	SYSLOG server IP Addr/32	UDP/514	SYSLOG
Carat IP Addr/32	Webhook receiver IP Addr/32	TCP/XXX	Webhook alarm (e.g. Slack)

2.4 Database configuration

For optimal performance, 7signal suggests the following DB2 database configuration settings:

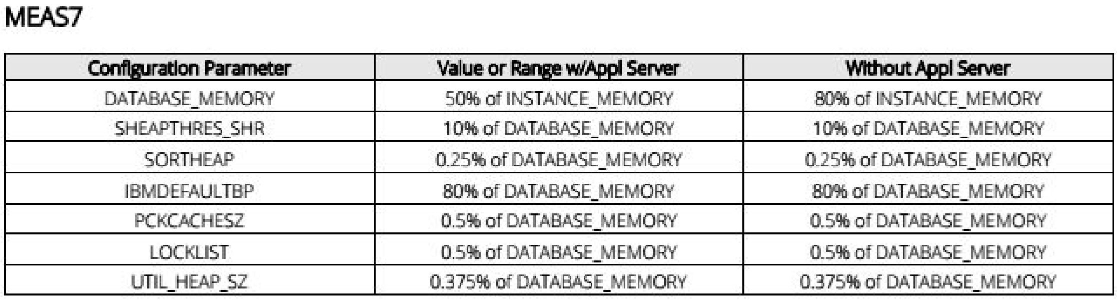
2.4.1 Database manager configuration



Database Manager Configuration Parameters (DBM CFG)

Configuration Parameter	Value or Range w/ Application Server	Without Application Server
INSTANCE_MEMORY	65% of RAM Available	80% of RAM Available or AUTOMATIC if only one DB2 instance
SHEAPTHRES	0	0

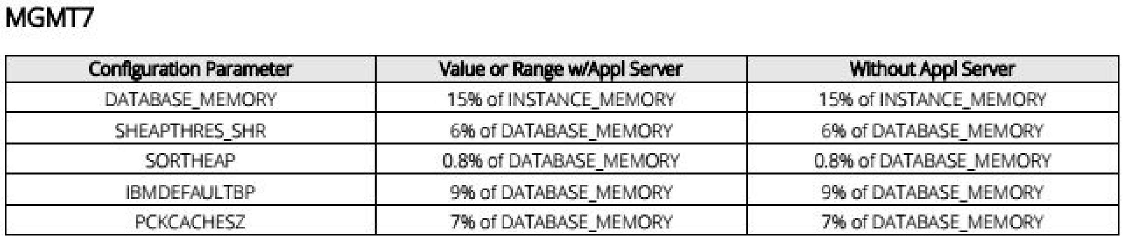
2.4.2 Database configuration for MEAS7



MEAS7

Configuration Parameter	Value or Range w/Appl Server	Without Appl Server
DATABASE_MEMORY	50% of INSTANCE_MEMORY	80% of INSTANCE_MEMORY
SHEAPTHRES_SHR	10% of DATABASE_MEMORY	10% of DATABASE_MEMORY
SORTHEAP	0.25% of DATABASE_MEMORY	0.25% of DATABASE_MEMORY
IBMDEFAULTBP	80% of DATABASE_MEMORY	80% of DATABASE_MEMORY
PCKCACHESZ	0.5% of DATABASE_MEMORY	0.5% of DATABASE_MEMORY
LOCKLIST	0.5% of DATABASE_MEMORY	0.5% of DATABASE_MEMORY
UTIL_HEAP_SZ	0.375% of DATABASE_MEMORY	0.375% of DATABASE_MEMORY

2.4.3 Database configuration for MGMT7



MGMT7

Configuration Parameter	Value or Range w/Appl Server	Without Appl Server
DATABASE_MEMORY	15% of INSTANCE_MEMORY	15% of INSTANCE_MEMORY
SHEAPTHRES_SHR	6% of DATABASE_MEMORY	6% of DATABASE_MEMORY
SORTHEAP	0.8% of DATABASE_MEMORY	0.8% of DATABASE_MEMORY
IBMDEFAULTBP	9% of DATABASE_MEMORY	9% of DATABASE_MEMORY
PCKCACHESZ	7% of DATABASE_MEMORY	7% of DATABASE_MEMORY

2.5 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.

Set the correct GDPR mode after Carat installation. Open the file `/opt/7signal/Carat/7signal/conf/server_conf.prop` in an editor and locate `carat.gdpr.mode` configuration parameter.

Set the value according to deployment plan:

- GDPR off:
  - `carat.gdpr.mode=`**`false`**
- GDPR on:
  - `carat.gdpr.mode=`**`true`**

If the server is located in an EU country, but you wish to control client data on an enterprise level, GDPR mode in configuration file should be set “off” (false). GDPR mode can later on turned in Configurator by editing Organizations.

Examples:

- Carat server is in US, all Eyes in US
  - GDPR mode should be “off”
- Carat server is in US, some Eyes are in US, some Eyes are in EU
  - GDPR mode should be “off”. Client data won’t be collected from Eyes located in EU.

- Carat server is in US, Privacy Shield compliant organization, some Eyes are in US, some Eyes are in EU
    - GDPR mode can be “on”. Client data will be collected from Eyes located in EU.
- Carat server in EU, all Eyes are in EU
    - GDPR mode should be “on”
- Carat server in EU, some Eyes are in US, some Eyes are in EU
    - GDPR mode should be “on”

3

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.
Every customer has a unique set of certificates, delivered within containers called *certificate packages*. It is not possible to use the delivered certificates to decrypt traffic on other 7signal Sapphire systems.

Q: Where can I find my certificates? All the customer certificates and certificate packages are located in the *7signal Share File*.

It is neither necessary nor encouraged to handle the certificate container files. Installation and upgrade processes of 7signal Sapphire software take care of all the typical cases. In untypical cases the 7signal staff shall be involved with all the help necessary.

3.2 Supportive connections

3.2.1 SSH for Eye

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

4

INSTALLING 7SIGNAL SAPPHIRE

4.1 Operating System installation tips

4.1.1 Required packages

A minimal Linux installation is recommended – just installing the packages that are required by the Sapphire software. For example, the CentOS Minimal CD distribution is suitable: http://wiki.centos.org/Manuals/ReleaseNotes/CentOSMinimalCD6.5 or the near equivalent "Minimal" installation set radio button.
A few additional packages need to be installed on top of a "Minimal" installation, and it is strongly recommended to regularly update both installations by typing:

```
# yum upgrade
```

CentOS installations:

Enable EPEL repository:

```
# yum install epel-release
```

Install the following packages by using yum:

```
# yum install pam.i686 numactl unzip system-config-firewall-tui xorg-x11-server-Xvfb libXtst libXrender
nginx policycoreutils-python
```

RHEL installations:

Enable repositories:

RHEL 6:

```
# subscription-manager repos --enable rhel-6-server-optional-rpms
# subscription-manager repos --enable rhel-server-rhscl-6-rpms
```

RHEL 7:

```
# subscription-manager repos --enable rhel-7-server-optional-rpms
# subscription-manager repos --enable rhel-server-rhscl-6-rpms
```

Install “rh-nginx” web server:

Figure out the most recent rh-nginx version:

```
# yum search nginx
```

The command lists available nginx versions.

Install the most recent rh-nginx version, for example:

```
# yum install rh-nginx112
```

Install the following packages by using yum:

```
# yum install pam.i686 numactl unzip system-config-firewall-tui xorg-x11-server-Xvfb libXtst libXrender policycoreutils-python
```

Sonar installations:

Install the following packages by using yum:

```
# yum install system-config-firewall-tui
```

4.1.2 Hard disk partitioning

This chapter gives some guidelines for hard disk partitioning. It is assumed that readers have comprehensive knowledge about Linux file systems, RAID, LVM and disk partitioning. This chapter does not cover basic partitioning requirements, e.g. configuring boot and swap partitions are not covered.

Swap is required by the DB2 database. Size of the swap must be 2 x RAM size.

Laptop installations

Default partitioning suggested by the OS installer is suitable for most cases. As laptops are rarely equipped with multiple hard drives, RAID configurations are not possible.

Server installations

At least one RAID array is recommended: 7signal databases and database log files should reside on a file system on top of RAIDed disks (RAID level 1 or higher, LVM on top of RAID). Multiple RAIDed file systems are also suitable, for example, OS installation could be on file system on RAID1, and databases on file system on top of RAID5.

It is suggested that LVM is used on top of RAIDs: this makes it possible to easily add a new RAID array as a LVM physical volume, if the existing one runs out of disk space. On large server installations (having tens of monitoring stations producing a large amount of measurement data), it is also suggested that database log files should be placed on different physical disk than the actual databases. This will improve database performance by reducing serialized disk access.

Example #1

- Two physical disks
- Boot and swap partitions
- RAID1 on top of disks, formatted as LVM physical volume
- Physical volume split into three logical volumes
  - 10% of space for OS installation, mount point “/” (LV1)
  - 70% of space for databases and database log files, mount point /opt/7signal/databases (LV2)
  - 20% of space for database backups, mount point /opt/7signal/backups (LV3)
- Sapphire installation
  - Sapphire components are installed to /opt/7signal (on LV1)

  - Sapphire databases are installed to /opt/7signal/databases (on LV2) (7signal DBMS installer asks for location of databases and database log files)
  - Sapphire database backups will be placed on /opt/7signal/backups (on LV3)

Example #2

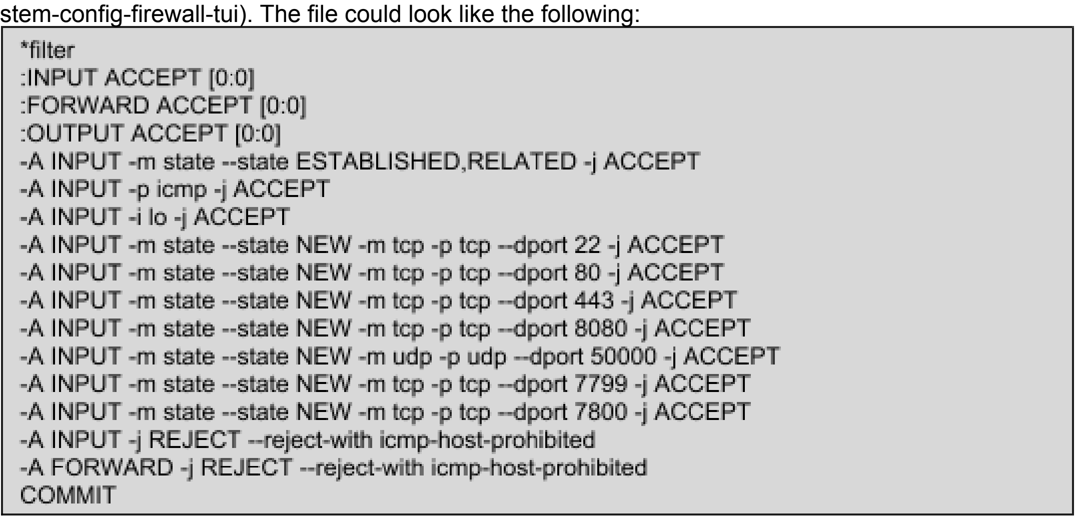
- Five physical disks
- Boot and swap partitions
- RAID1 on top of two disks, RAID5 on top of three disks, all formatted as LVM physical volumes
- Physical volume on RAID1 has two logical volumes
  - 50% of space for OS installation, mount point "/" (LV1)
  - 50% of space for database logs, mount point "/opt/7signal/database-logs" (LV2)
- Physical volume on RAID5 has two logical volumes
  - 70% of space for databases, mount point /opt/7signal/databases (LV3)
  - 30% of space for database backups, mount point /opt/7signal/backups (LV4)
- Sapphire installation
  - Sapphire components are installed to /opt/7signal (on LV1)
  - Sapphire databases are installed to /opt/7signal/databases (on LV3) and database logs are directed to /opt/7signal/database-logs (on LV2) (7signal DBMS installer asks for location of databases and database log files).
  - Sapphire database backups will be placed on /opt/7signal/backups (on LV4)

4.1.3 Server security

Firewall

Carat and Sonar server firewalls should be configured are described in section 2.3. Additionally, especially if the servers are located on the Internet, additional firewall rules should be configured:

In CentOS/Red Hat Enterprise Linux, the firewall configuration is /etc/sysconfig/iptables (configured via system-config-firewall-tui). The file could look like the following:



```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 50000 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 7799 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 7800 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Restricting Analyzer/EyeQ/Configurator access:

It might make sense to restrict Analyzer/EyeQ/Configurator access to certain IP addresses or IP networks. Edit the rules of TCP ports 80 and 443 by adding a source address filter (-s option).

```
-A INPUT -m state --state NEW -m tcp -p tcp -s 199.95.207.10 --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp -s 199.95.207.10 --dport 443 -j ACCEPT
```

Example 2: Allow access from address 199.95.207.0/24 network only:

```
-A INPUT -m state --state NEW -m tcp -p tcp -s 199.95.207.0/24 --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp -s 199.95.207.0/24 --dport 443 -j ACCEPT
```

If any changes were made to iptables configuration rules, the added/modified rules need to be reloaded:

```
# service iptables reload
```

SSH connectivity

Disable SSH root logins

Super user (root) SSH logins are enabled by default in CentOS and RHEL. This is not a recommended configuration. If root permissions are needed, a user should first log in as an ordinary user and then switch user to root or better yet, use sudo to execute a root level command, which provide more granular auditing capabilities.

Open the file /etc/ssh/sshd_config in an editor. Locate the following line:

```
#PermitRootLogin yes
```

Change it to following:

```
PermitRootLogin no
```

Save the file and restart SSH daemon:

# service sshd restart

Consider using SSH keys instead of password login
Generally, an SSH public key login is more secure than password logins.

4.1.4 Operating system limits

The default number of allowed OS threads may not be sufficient for larger Sapphire installations. It is suggested to double the allowed “carat7” process threads from 1024 to 2048.
Open the file /etc/security/limits.d/90-nproc.conf in an editor. Add the line in red to the file and save the file.

```
# Default limit for number of user's processes to prevent
# accidental fork bombs.
# See rhbz #432903 for reasoning.

*           soft    nproc     1024
carat7      soft    nproc     4096
root        soft    nproc     unlimited
```

If you are modifying the file after installing the Carat server, restart the server in order to get the new limits into use:

# 7carat restart

4.1.5 SELinux and nginx HTTP server

If SELinux is in enforcing mode, you may see ”502 Bad Gateway” error when trying to access web apps. In order to avoid this error, execute the following commands:

```
# sudo cat /var/log/audit/audit.log | grep nginx | grep denied | audit2allow -M mynginx
# sudo semodule -i mynginx.pp
```

4.2 Setting up Eyes

4.2.1 Change default SSH password

The Eye root default password is ‘7signal’. It is strongly advised to change this password as it is a factory default for every Eye unit. The default password is “7signal”.

Step 1: Connect to the Eye unit

```
# ssh root@<Eye IP address>
```

Step 2: Change the password by using passwd command

```
# passwd
```

Enter new password

4.2.2 Static IP address configuration

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

Step 1: Connect to the 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
```

4.3 Configuring Eyes to connect a Carat server

Starting with Sapphire release 5.2, it is now possible to configure the Eyes to connect to the Carat server (before release 5.2, Carat server always initiated the connection to the Eyes). The Eyes 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 Eyes 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 Eyes 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. The Eye will be added to a Service Area named “Default”.
2. If a Service Area named “Default” does not exist, it will be created to first Location of the Organization.
3. If there are no Locations configured yet, a Location named “Default” will be created.
4. If there are no Organizations configured yet, an Organization named “Default” will be created.

4.3.1 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]*>*]

[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”

3. Reboot Eye unit:

   # reboot

An example:

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

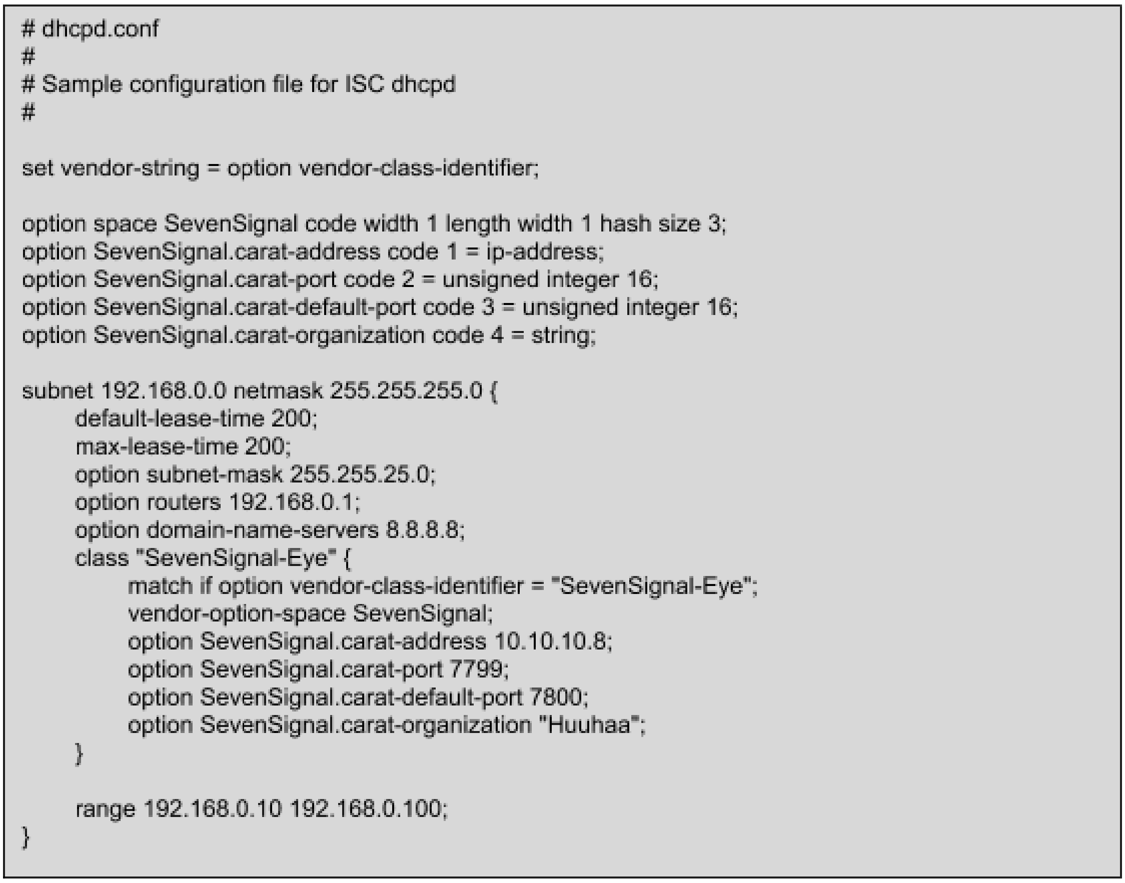
After reboot, the Eye establishes a connection to the Carat server on IP address 192.168.10.10 in the example above. If the Eye is not already in the Carat server configuration, it will be added to the organization 7signalSolutionsInc.

4.3.2 DHCP based configuration

Eyes 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 Eyes 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

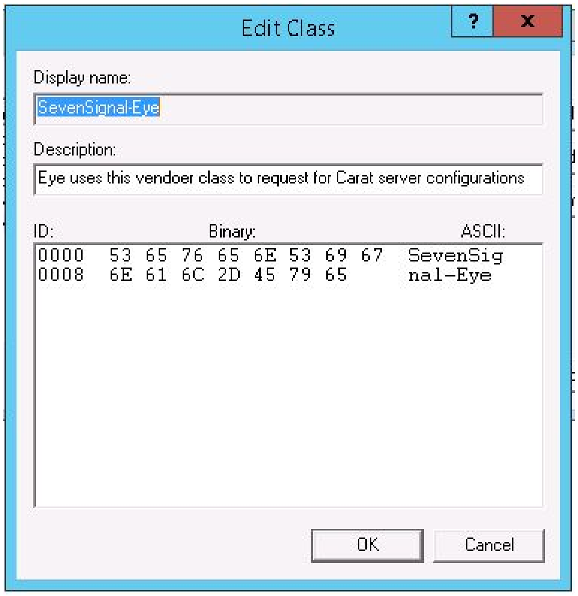
For ISC DHCP server, the content of the DHCP server configuration file would be like the following:



```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

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;
}
```

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 Eyes to request for Carat server configurations.

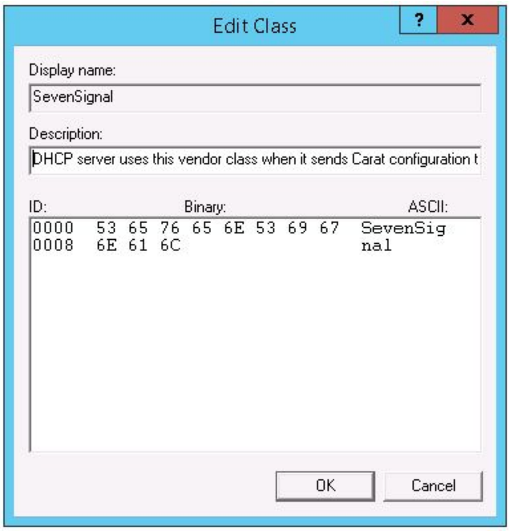


Display name:
SevenSignal-Eye

Description:
Eye uses this vendoer class to request for Carat server configurations

```
ID:              Binary:                    ASCII:
0000   53 65 76 65 6E 53 69 67   SevenSig
0008   6E 61 6C 2D 45 79 65      nal-Eye
```

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



Edit Class

Display name: SevenSignal

Description: DHCP server uses this vendor class when it sends Carat configuration t

```
ID:             Binary:                 ASCII:
0000   53 65 76 65 6E 53 69 67   SevenSig
0008   6E 61 6C                  nal
```

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:

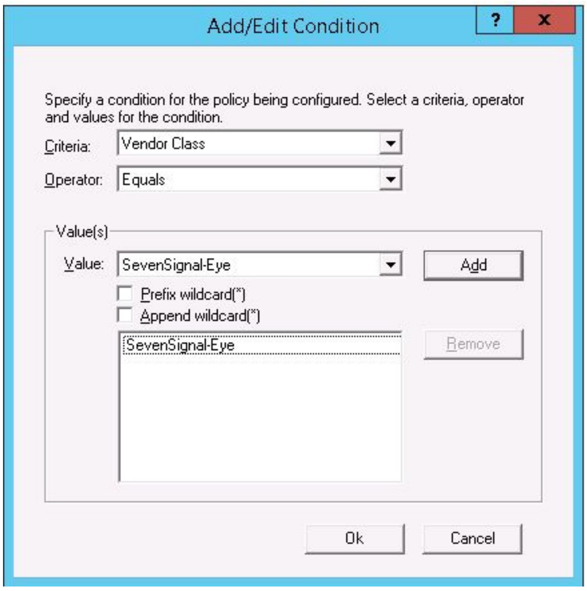
Name	Data type	Code	Value
ldress	ess		server_IP_address>
rt			
efault-port			

ganization			ization_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”



Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Equals

Value(s)

Value: SevenSignal-Eye

□ Prefix wildcard(*)

□ Append wildcard(*)

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.

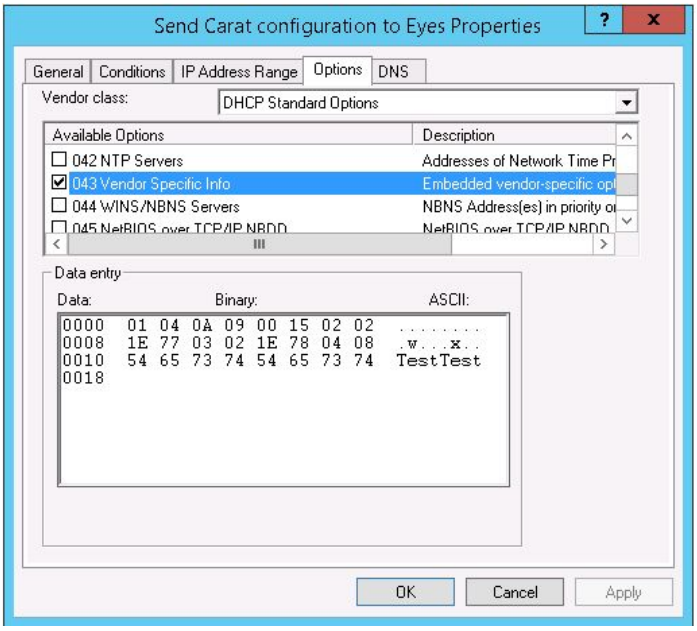
2) Select “043 Vendor Specific Info” under “DHCP standard Options”. Option 43 is in TLV format: <tag id> (byte) <tag length> (byte) <data vector>. For example, is options set in Step 2 are:

Code	Data type	value
	ess	1
		t

In TLV format, they are:

Tag ID	Tag length	data vector
		0 15
		3 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”.



Vendor class: DHCP Standard Options

Available Options	Description
☐ 042 NTP Servers	Addresses of Network Time Pr
☑ 043 Vendor Specific Info	Embedded vendor-specific opt
☐ 044 WINS/NBNS Servers	NBNS Address(es) in priority or
☐ 045 NetBIOS over TCP/IP NBDD	NetBIOS over TCP/IP NBDD

Data entry

```
Data:           Binary:                   ASCII:
0000  01 04 0A 09 00 15 02 02   ........
0008  1E 77 03 02 1E 78 04 08   .w...x..
0010  54 65 73 74 54 65 73 74   TestTest
0018
```

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.

4.3.3 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 Eye monitoring stations.
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:

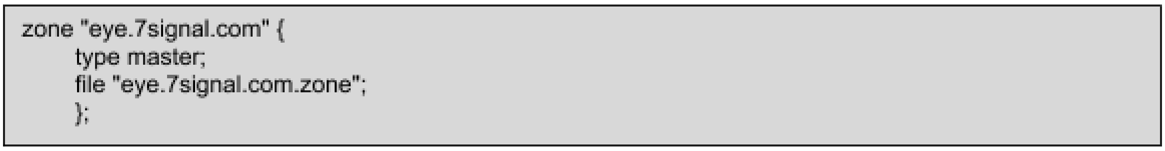
- A record contains the IP address of the Carat server
- Three TXT records contain port number, default port number and organization information.

DNS redirector server configuration

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

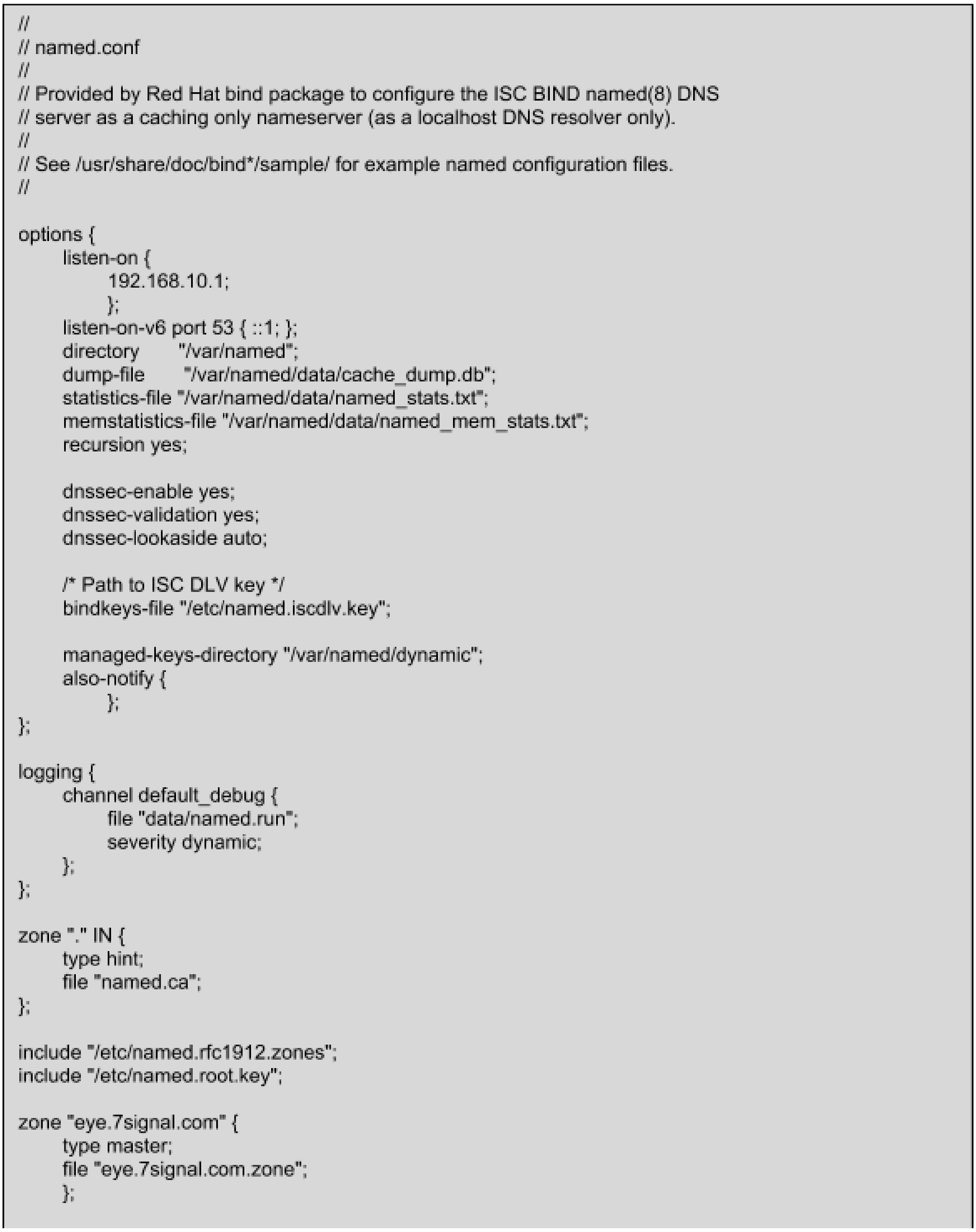
1. Install **bind** package by using yum in a Linux system which will be hosting DNS redirector service.
2. Edit configuration file /etc/named.conf. The most important parts are:
    a. DNS server listen address
    b. Zone information block

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";
      };
```

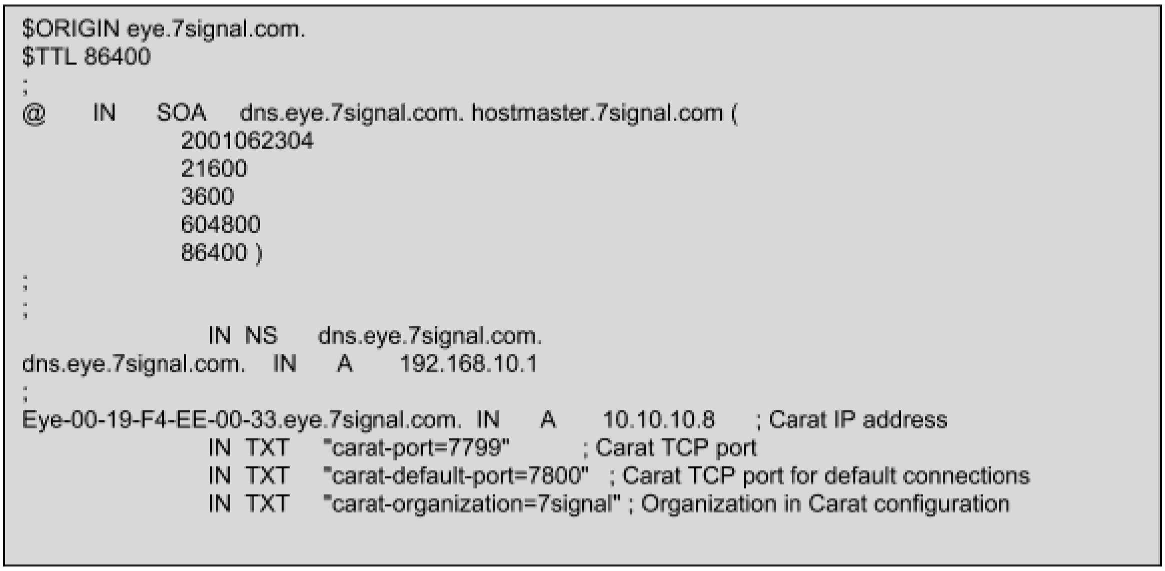
Example named configuration file /etc/named.conf:



```
//
// 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:

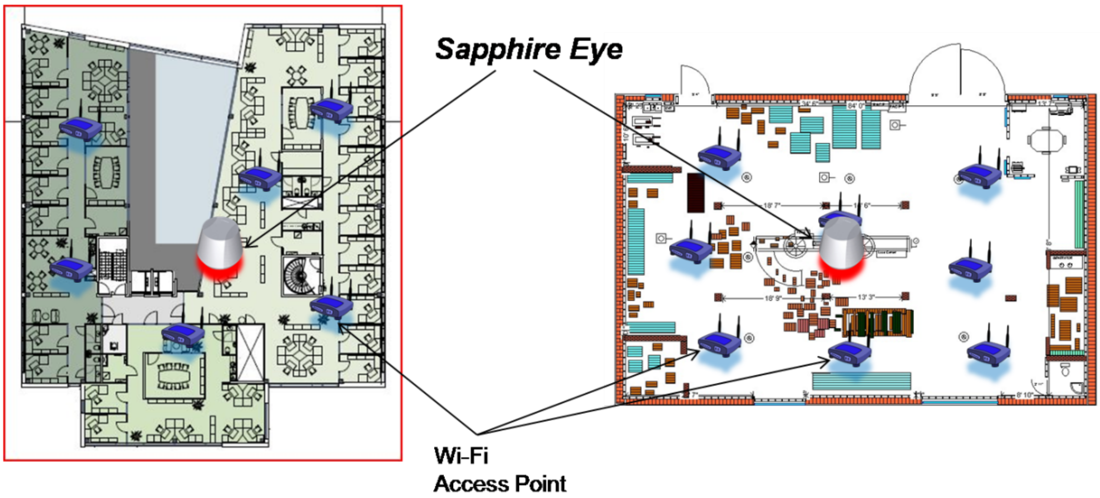
   ```
   # 7config conn dns remove
   ```
5. Remove Carat connection configuration by using a command:

   ```
   # 7config conn carat remove
   ```
6. Reboot the Eye:

   ```
   # reboot
   ```

4.4 Mounting Eyes

Mount Sapphire Eyes in the most centralized location of the WLAN area. The Eye 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

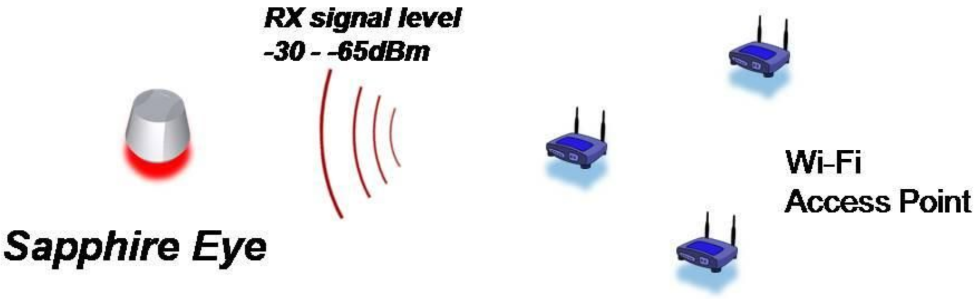
For best accuracy of the WLAN performance, the Sapphire Eye location should be selected so that:

- 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.

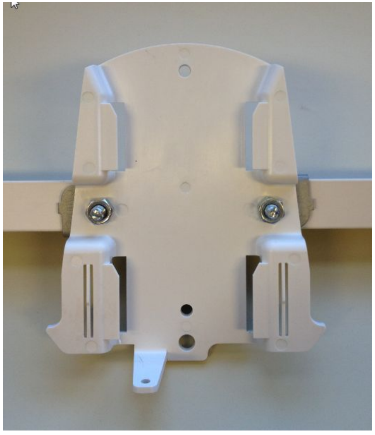
The best installation location is easily verified with:

- Site Survey signal level results

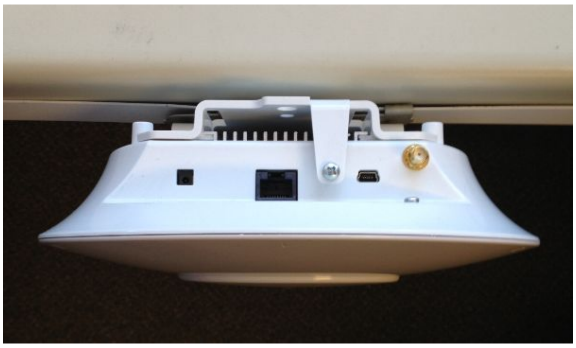

RX signal level
-30 - -65dBm
Sapphire Eye
Wi-Fi
Access Point

4.4.1 Indoor Eye (Eye 2000/Eye 2100/Eye 2200) Ceiling Installation

Attach the Indoor Eye sliding bracket onto a suspended ceiling T-rail using the two Twist Clips included with the Eye, and two ¼-inch nuts. Or, secure the bracket with screws to any solid ceiling structure.

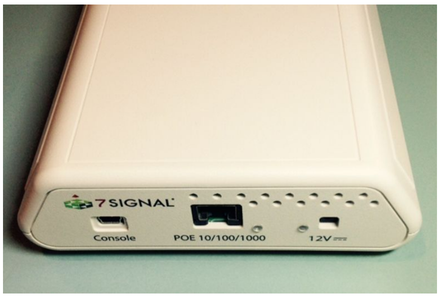


Slide the Indoor Eye onto the bracket and secure it with the #6-32 x 5/16” Phillips head screw.

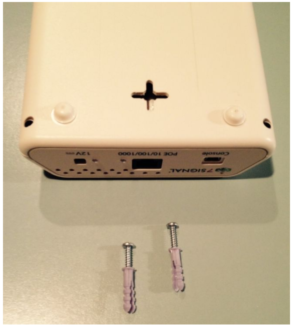


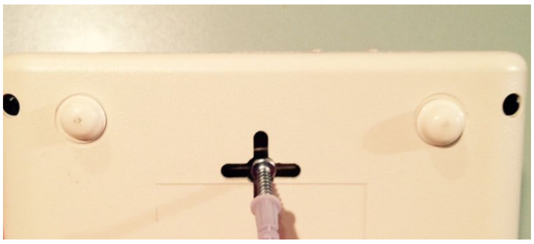
4.4.2 Eye Model 500 Table Top or Wall Mount Installation

The Model 500 sits on 4 rubber feet on a table top



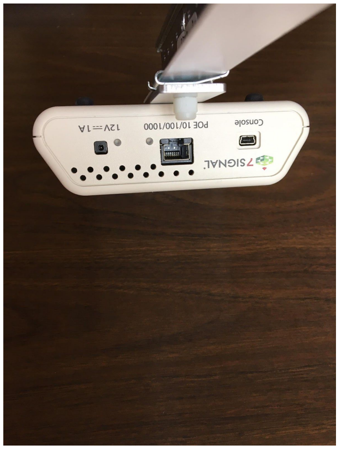
Or, mounts on a wall in any one of 4 orientations using two wall anchors with two #6 screw heads inserted in the two 4-way keyhole slots on the bottom of the unit.





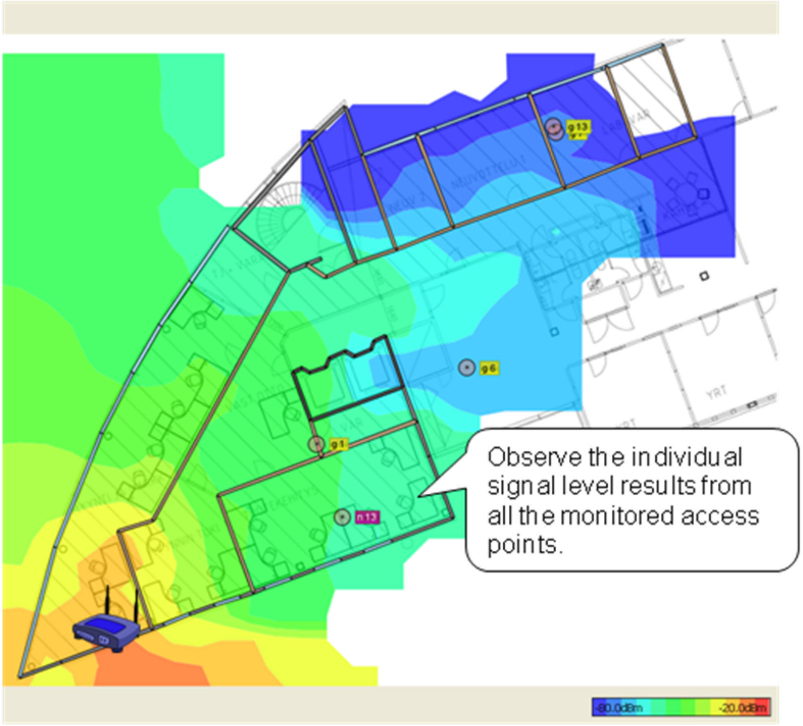
4.4.3 Eye Model 500 Ceiling Mount Option

The Model 500 may also be mounted on suspended ceiling. The standard clips are for 1” T-rail.



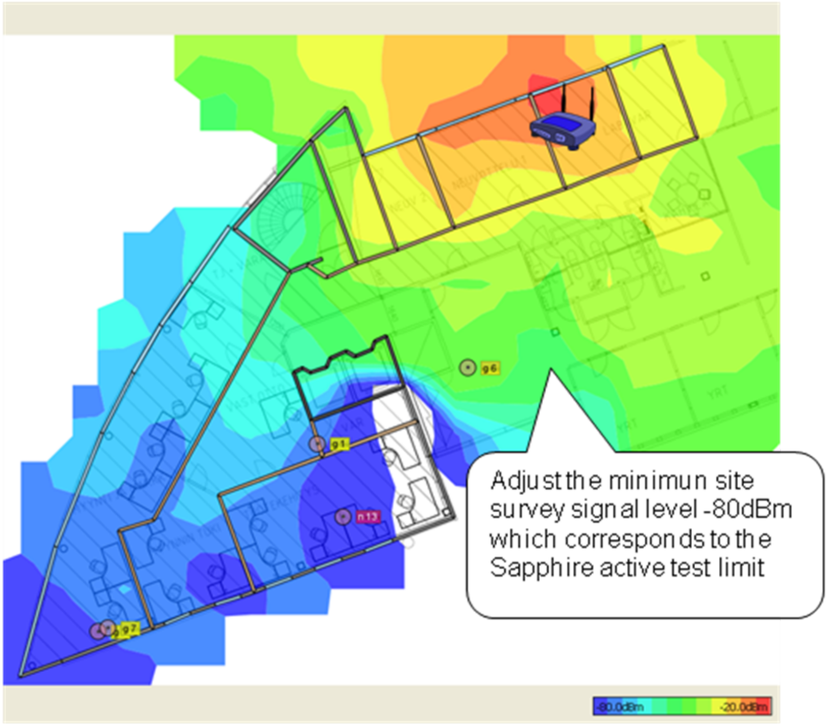
4.4.4 Eye installation examples

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.



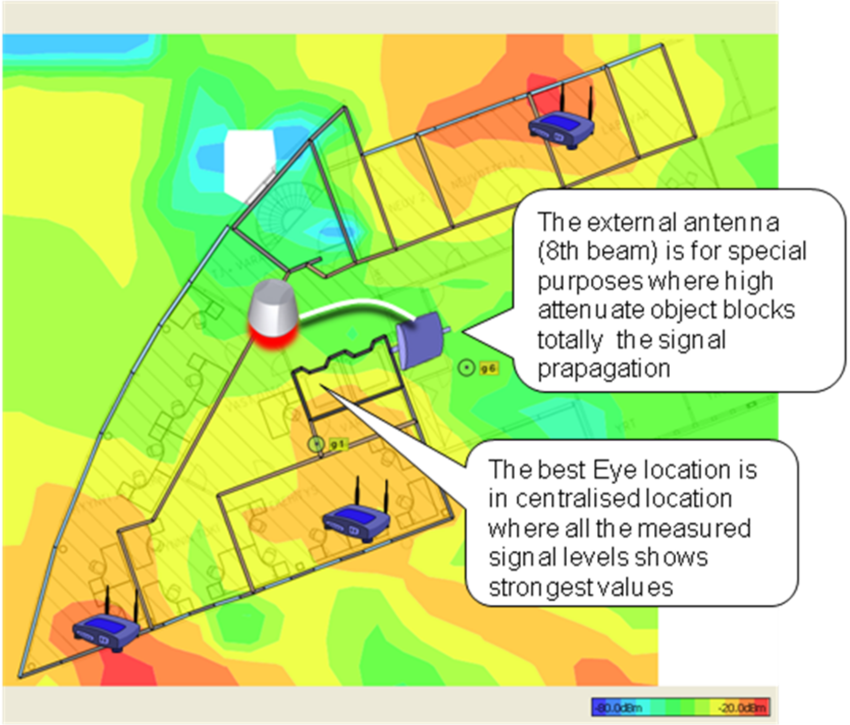
Observe the individual signal level results from all the monitored access points.

The Site Survey results are valuable for Eye location selection



Adjust the minimun site survey signal level -80dBm which corresponds to the Sapphire active test limit

Verify the signal levels from the far end access points


The external antenna (8th beam) is for special purposes where high attenuate object blocks totally the signal prapagation
The best Eye location is in centralised location where all the measured signal levels shows strongest values
96
91
-80.0dBm
-20.0dBm

The external antenna is useful in the environment where shafts or thick walls are attenuating radio too much.

4.5 Installing 7signal Sapphire software

The 7signal Sapphire software can be downloaded from 7signal Share File.

Root privileges are needed for installation of Sapphire components.

Installation steps:

1. Install DB2 and Sapphire DBMS
2. Install Carat server software
3. Install Application Server and web applications

4.5.1 Installation from VM templates

The 7signal Sapphire software can be installed from pre-installed VM templates. The templates have all the Sapphire components ready installed which will make the installation process fast.

1. Supported VM platforms
   The virtual images have been created for Oracle Virtual Box 4.3.12 (or greater), VMware Workstation 10.0.1 (or greater), VMWare Player 6.0.2 (or greater), and VMware vSphere ESXi 4.x and greater.
   The virtual images is using CentOS 6.7 for both Carat and Sonar VMs. The 7signal Sapphire Software is located in the /opt/7signal/ directory.
2. Credentials

The username and password for both the Carat Server and Sonar Server VM's are shown below:
Username: 7admin (with sudo access)
Password: 7admin

NOTE! It is recommended to change VM's default passwords. Root password can be found from the VM template Readme document

3. Specifications
   Settings of the virtual images are listed below.
   Carat Server VM (1-25 Eyes):
   CPU 4
   RAM 6114MB
   HD 450GB (thin provisioned)

   Sonar Server VM:
   CPU 4
   RAM 6114MB
   HD 40GB (thin provisioned)
   This is default configuration. Server configuration depends on the number of sensors. Configuration should be adjusted according to 7signal server requirements.
4. Configuration Instructions
   Step 1: Login to Carat server VM using "root" or "7admin" user:
   If "7admin" user is used to login to Carat server VM, please type in "sudo su -" for root access.
   Step 2: Assign a static IP address to Carat server VM:
   The IP address of Carat server is obtained by DHCP in default**.** Use system-config-network-tui to uncheck "Use DHCP" for eth0 and assign a static IP address (with root access) according to your network settings:

# system-config-network
Fill in the Static IP, Netmask, Default gateway IP, Primary DNS Server and/or Sedondary DNS Server according to your network settings:
If VM is logged in via SSH, please execute a reboot after network configuration is saved. After a reboot, eth0 IP address is changed to the Static IP.
IF VM is logged in via Console, execute the following two commands to activate the VM's network card with the updated configuration:
# ifdown eth0
# ifup eth0
Assume **SERVER_IP** is the static IP address of the Carat Server.
Step 3: Transfer certificate and license from local computer to /home/7admin folder on the Carat Server VM:
The certificate and license files are not pre-installed in the Carat server template. These two files should be transferred to the Carat server VM manually.
If you are using a Linux computer, please use "scp" command to transfer files:
# scp certificate_file.tar.gz license_file.lic 7admin@SERVER_IP:/home/7admin
If you are using a Windows computer, please use "WinSCP" tool to transfer files.
Step 4: Update DB2 password:
If "7admin" user is used to login to Carat server VM, please type "sudo su -" for root access to execute "7setup" commands.
# 7setup dbpass
Step 5: Set certificate and license for Carat server and Application server server:
The "7setup certlic" command is used to set or update certificate and license for each locally installed component: Carat and Application server.
# 7setup certlic /home/7admin/certificate_file.tar.gz /home/7admin/license_file.lic
Carat server and Application server server are automatically shut down and then restarted when the "7setup certlic" command is executed.

Step 6: To this point, configurations on Carat server VM is done. Please launch and login to Carat Configurator using the default username and password “admin”.

Step 8: Sonar VM configuration:
Please follow steps 1 and 2 to login to Sonar VM and assign a static IP address to Sonar VM. After this, please use command “7sonar status” to check if Sonar service is running:

```
# 7sonar status
7signal Sonar is running
Done!
```

4.5.2 Java installation

7signal Sapphire requires Orace Java Runtime Environment. Download the Java 8 Runtime from Oracle website https://www.oracle.com/technetwork/java/javase/downloads/index.html . Install the JRE by issuing the command:

```
# yum install jre-8u<version>-linux-x64.rpm
```

4.5.3 DB2 and Sapphire DBMS installation

Prerequisites

Please verify the following items:

- The IP address of the server must be resolvable to its DNS name. This can be achieved by the following procedures:
    - Server has been added to DNS
    - Hosts file contains the DNS name.
        - cat /etc/hosts
        - edit the hosts file if needed

Installation

The DB2 database and Sapphire DBMS are available in two RPM files.

Copy 7signal-DB2 and 7signal-DBMS RPMs from delivery medium to for example /root directory.

Step 1: Install DB2 and DBMS

Issue command:

```
# yum install 7signal-DB2-x.x.x-y.el7.x86_64.rpm 7signal-DBMS-x.x.x.x-y.el7.noarch.rpm
```

Step 2: Create and configurate databases

Issue command:

```
# 7db install
```

The command asks location for the databases:

```
Enter location for databases [/home/db7sign]: (See NOTE below)
```

The database location defaults to the /home file system just like the database logs that are configured below.

NOTE! This default database location is not recommended, if the /home file system is not backed up or otherwise replicated, or does not have enough disk space. The logs and the actual database should always reside in separate file systems, preferably on RAIDed, separate physical devices.

Database must be always on local disk, for example, not on NFS mount!

Creating and configuring databases takes several minutes. After completed, it is possible to change DB2 transaction logging method from circular logging to archival logging:

```
Do you want to change the default database logging method (circular logging) to
infinite archival logging [y/N]? <enter>
```

It is encouraged to make the install with circular logging. The infinite archival logging requires design and practically endless storage device. The instructions for moving to infinite archival logging are in the Carat User Manual among other detailed backup process design issues.

The next step is to specify location for database log files. Log file location defaults to the /home file system just like the actual database.

```
Enter location for Management DB log files
[/home/db7sign/db7sign/NODE0000/SQL00001/SQLOGDIR/]: <enter>

OK. Using default.

Enter location for Measurement DB log files
[/home/db7sign/db7sign/NODE0000/SQL00002/SQLOGDIR/]: <enter>

OK. Using default.

Enter location for Security DB log files
[/home/db7sign/db7sign/NODE0000/SQL00003/SQLOGDIR/]: <enter>

OK. Using default.
```

The install is now complete. The DB2 is now installed, up and running.

4.5.4 Carat server installation

Copy the RPM files from the delivery medium to for example /root directory.

Step 1: Change to the directory where installer was copied and execute the installer.

Install the Carat server by issuing the command:

```
# yum install 7signal-Carat-x.x.x.x-y.el7.x86_64.rpm
```

If you wish to install sensor softwares to SW repository of the Carat server, issue the command:

```
# yum install 7signal-Eye-x.x-y.el7.centos.noarch.rpm
```

Step 2: Install the certificate bundle and license file:

The certificate package can be downloaded from 7signal Share File. Install the certificates by issuing the command:

```
# 7carat certificate set <certificate package>
```

The license file is created for each customer individually. It is in the same delivery medium with the certificate packages. Install license by issuing the command:

```
# 7carat license set <license file>
```

Step 3: Setup maximum memory

Configure maximum memory (RAM) that Carat server can use by issuing command:

```
# 7carat memoryconf
```

Step 4: Start Carat server software

Start the Carat server software by issuing the command:

# 7carat start

4.5.5 Application server and web app installation

Copy 7signal-Application-Server, 7signal-nginx-conf, 7signal-AnalyzerApp, 7signal-ConfiguratorApp, 7signal-EmeraldApp and 7signal-EyeQApp RPMs from the delivery medium to e.g. /root directory.

Step 1: Install Application Server

Issue command:

```
# yum install 7signal-Application-Server-x.x.x.x-y.el7.noarch.rpm
```

Step 2: Install web apps:

Issue command:

```
# yum install 7signal-ConfiguratorApp-x.x.x.x-y.el7.noarch.rpm
7signal-AnalyzerApp-x.x.x.x-y.el7.noarch.rpm 7signal-EmeraldApp-x.x.x.x-y.el7.noarch.rpm
7signal-EyeQApp-x.x.x.x-y.el7.noarch.rpm
```

Step 3: Install certificate package:

The certificate package can be downloaded from 7signal Share File.

# 7analyzer certificate set <*certificate package*>

Step 4: Setup maximum memory

Configure maximum memory (RAM) that Carat server can use by issuing command:

```
# 7analyzer memoryconf
```

Step 5: Restart Application Server

Issue command:

```
# 7analyzer restart
```

Notice: If you see "502 Bad Gateway" error when trying to access web apps, see chapter 4.1.5.

Step 6: Install nginx configuration

Sapphire uses nginx web server as a proxy. The Sapphire nginx configation can be installed by issuing command:

```
# yum install 7signal-nginx-conf-x.x.x.x-y.el7.noarch.rpm
```

This installs nginx configuration to /etc/nginx/conf.d.

On RHEL, the nginx server configuration directory is not necessarily /etc/nginx. You may need to find out the correct configuration directory and copy the /etc/nginx/conf.d/tomcat-proxy.conf to conf.d directory of the RHEL ngihx configuration directory.

4.5.6 Sonar Installation

Copy 7signal-Sonar RPM from the delivery medium e.g. to /home directory.

Step 1: Install Sonar

Issue command:

```
# yum install 7signal-Sonar-x.x.x.x-y.el7.centos.x86_64.rpm
```

Step 2: 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*>

Step 3: Start the Sonar server:

Issue the command:

# 7sonar start

Upgrading Sapphire

5.1 Copy the latest Sapphire release to the hard disk

Step 1: Download new Sapphire version from 7signal Share File

Step 2: Copy Sapphire software to the Carat server

IMPORTANT: When upgrading between major versions a new Sapphire Software license file will be required.

5.2 Stop Sapphire solution (Linux)

Step 1: Stop the Carat server:

Stop the Carat server by issuing the command:

```
# 7carat stop
```

Step 2: Stop the Application Server server:

Stop the Analyzer server by issuing the command:

```
# 7analyzer stop
```

5.3 Upgrade from 8.1 to 8.2

Sapphire installers have been changed from proprietary binary installers to standard RPM installers in release 8.2. All components except DBMS must be re-installed.

5.3.1 Java installation

7signal Sapphire requires Orace Java Runtime Environment. Download the Java 8 Runtime from Oracle website https://www.oracle.com/technetwork/java/javase/downloads/index.html . Install the JRE by issuing the command:

```
# yum install jre-8u<version>-linux-x64.rpm
```

5.3.2 DBMS upgrade

Important: Backup the databases prior to upgrade, either by using “7db backup” command or 7BUtool.sh utility script.

When upgrading to 8.2, you must install 7signal-DB2 and 7signal-DBMS RPMs:

- Installing DB2 by using 7signal-DB2 RPM does not actually install the DB2, but it updates RPM database, and all future dependencies will be handled correctly by RPM.
- Installing DBMS by using 7signal-DBMS will upgrade the existing installation (made by using proprietary binary installer)

Step 1: Install DB2

Issue command:

```
# yum install 7signal-DB2-10.5.5-1.el7.x86_64.rpm
```

The command outputs:

```
DB2 is already installed
```

Step 2: Install DBMS

Issue command:

```
# yum install 7signal-DBMS-8.2.0.0-1.el7.noarch.rpm
```

Step 3: Upgrade DBMS from 8.1 to 8.2 level

Issue command:

# 7db upgrade

5.3.3 Carat server upgrade

Step 1: Uninstall Carat

Uninstall Carat as described in the chapter 6.1.2

Step 2: Install Carat

Install Carat as described in the chapter 4.5.4

5.3.4 Analyzer server upgrade

Step 1: Uninstall Analyzer

Uninstall Analyzer as described in the chapter 6.1.1

Step 2: Install Application server and web appps

Install Application server and web apps as described in the chapter 4.5.5

5.3.5 Sonar upgrade

Step 1: Uninstall Sonar

Uninstall Sonar as described in the chapter 6.1.4

Step 2: Install Sonar

Install Sonar as described in the chapter 4.5.6

5.4 Start Sapphire solution (Linux)

After all components have been upgraded, start the Carat and Application servers.

Step 1: Start the Carat server:

Start the Carat server by issuing the command:

```
# 7carat start
```

Step 2: Start the Application server:

Start the Application server by issuing the command:

# 7analyzer start

5.5 Eye upgrade

5.5.1 Eye upgrade (Configurator)

Note: The Eye SW version number in these instructions may not be the one that is going to be installed. However, the instructions are applicable to all SW versions.

Step 1: Start the Configurator:

Step 2: If necessary, install new software version:

This step needs to be executed only if Carat was updated without in-bundled Eye software packages (i.e. “full” version was not used).

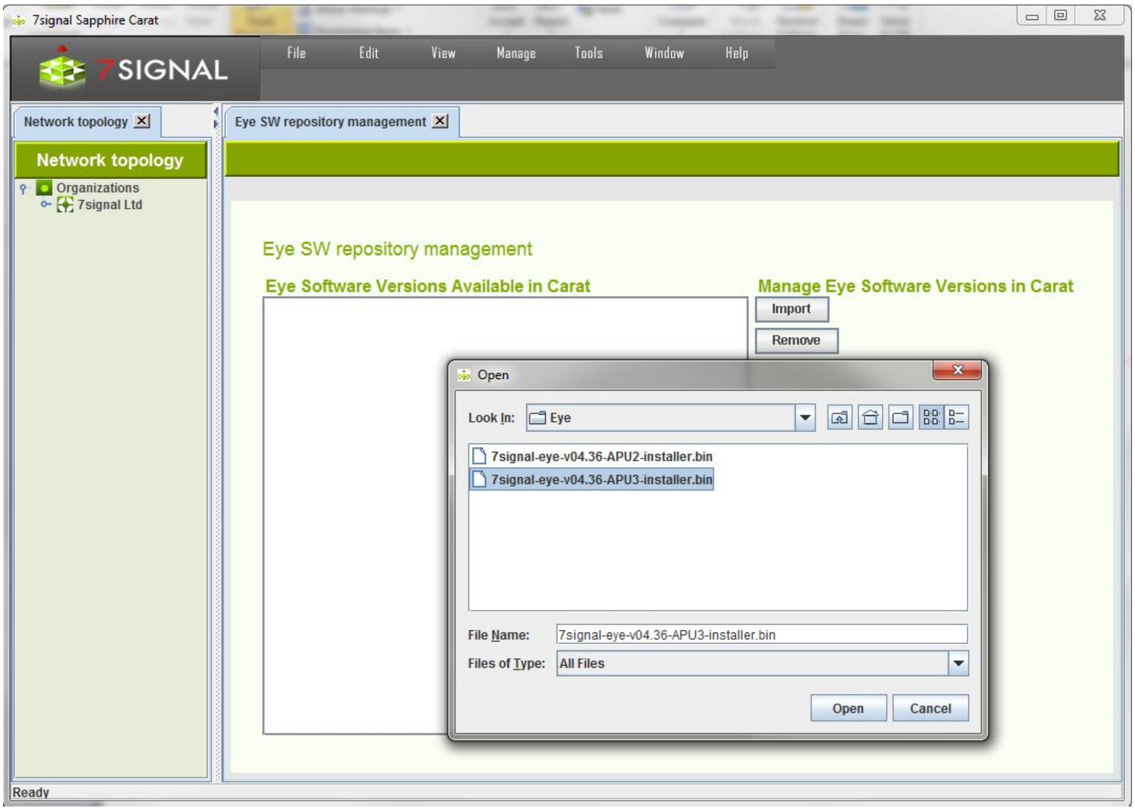
Login as solution admin user.

Open the “Manage | Eye Software Management | SW repository management” view

- Select “Import”
- Browse the Eye software installer
  - APU3 installers are for 802.11a/b/g/n Eyes

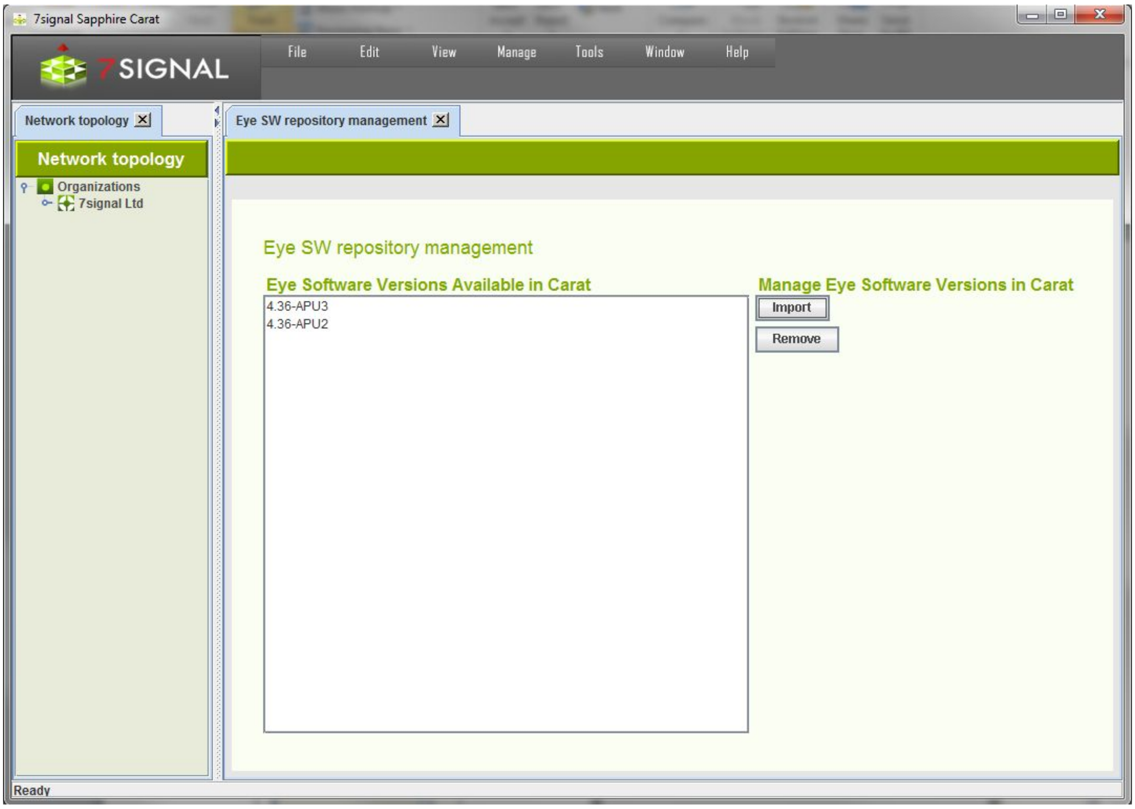
  - MPU1 installers are for 802.11a/b/g/n/ac Eyes

- Select the desired installer, select “Open”



7signal Sapphire Carat
7SIGNAL
File
Edit
View
Manage
Tools
Window
Help
Network topology
Eye SW repository management
Network topology
Organizations
7signal Ltd
Eye SW repository management
Eye Software Versions Available in Carat
Manage Eye Software Versions in Carat
Import
Remove
Open
Look In: Eye
7signal-eye-v04.36-APU2-installer.bin
7signal-eye-v04.36-APU3-installer.bin
File Name: 7signal-eye-v04.36-APU3-installer.bin
Files of Type: All Files
Open
Cancel
Ready

- Eye software versions available is Carat are populated on the list:



Eye SW repository management

Eye Software Versions Available in Carat

4.36-APU3
4.36-APU2

Manage Eye Software Versions in Carat

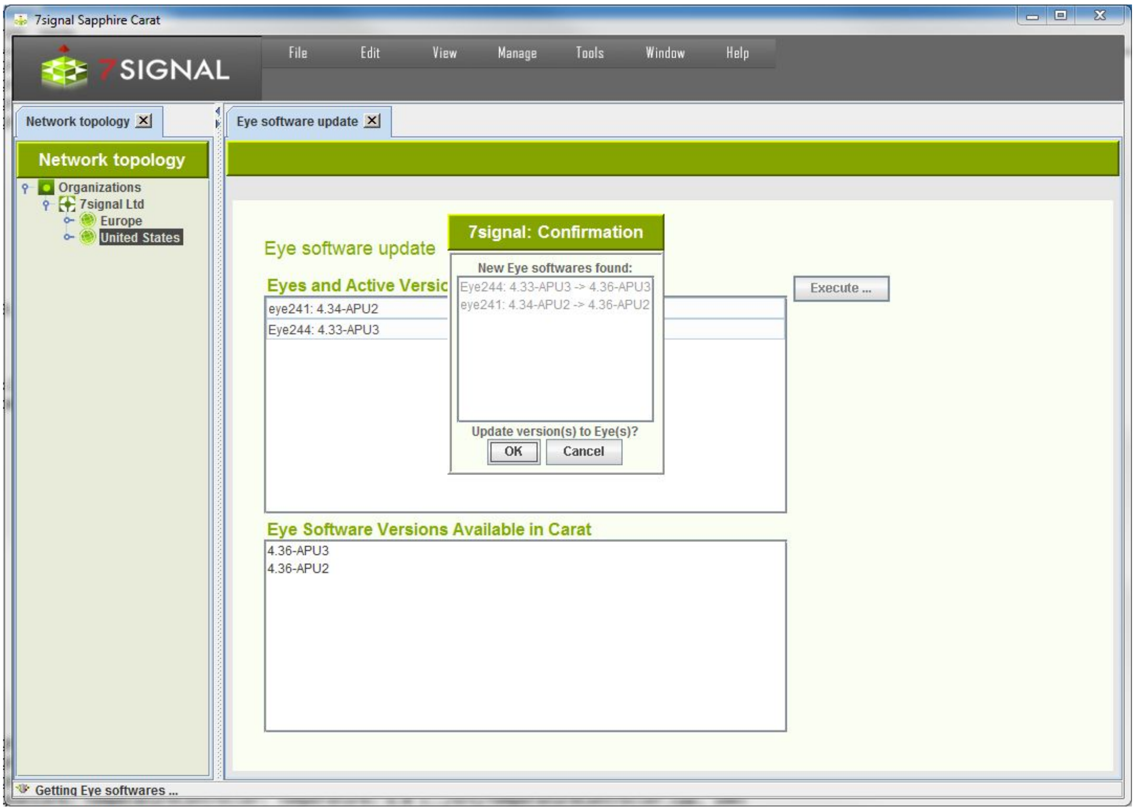
- Import installers for all needed platforms
- Close the “Eye SW repository management” view.

Step 3: Upgrade Eye software to Eye units:

Login as configurator user.

Open the “Manage | Eye Software Management | Eye software update” view

- If a software update is available for some Eyes, the software version and the name of the Eye unit appear on a pop-up window:



Network topology

- Organizations
  - 7signal Ltd
    - Europe
    - United States

Eye software update

Eyes and Active Versic

eye241: 4.34-APU2
Eye244: 4.33-APU3

7signal: Confirmation

New Eye softwares found:

Eye244: 4.33-APU3 -> 4.36-APU3
eye241: 4.34-APU2 -> 4.36-APU2

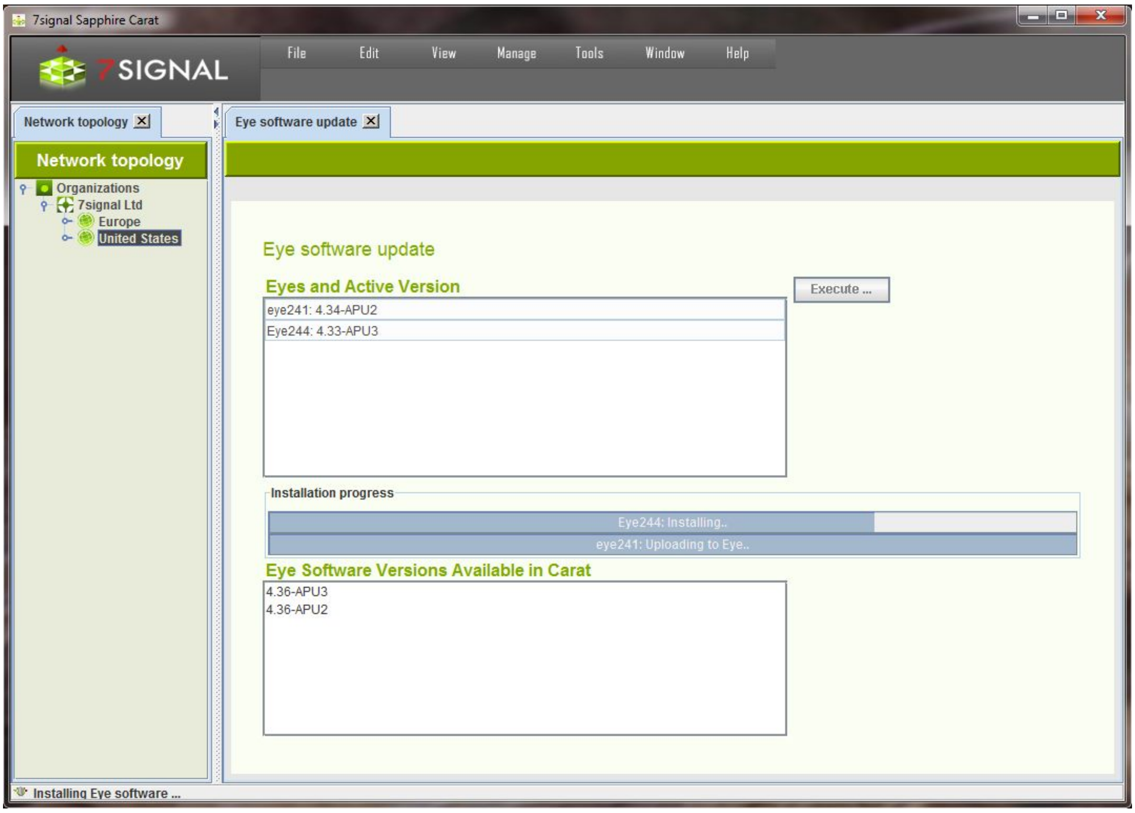
Update version(s) to Eye(s)?

Eye Software Versions Available in Carat

4.36-APU3
4.36-APU2

Getting Eye softwares ...

- To update the software version to Eye, select “OK”
- Software is uploaded and installed to Eye units



Network topology

Organizations
7signal Ltd
Europe
United States

Eye software update

Eyes and Active Version

eye241: 4.34-APU2
Eye244: 4.33-APU3

Installation progress

Eye244: Installing..
eye241: Uploading to Eye..

Eye Software Versions Available in Carat

4.36-APU3
4.36-APU2

Installing Eye software ...

- After the installation is complete, close the “Eye software update view”

5.5.2 Eye upgrade (command line)

Step 1: Change to the Eye installer directory:

```
# cd /root/SapphireXXYY/Carat_CD/Eye
```

Step 2: Copy the SW to Eye unit:

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

```
# scp 7signal-eye-v0X.YY-APU3–installer.bin root@<IP_address>:/nand
```

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

```
# scp 7signal-eye-v0X.YY-MPU1–installer.bin root@<IP_address>:
```

Step 3: Login to Eye:

```
# ssh root@<eye_ip_address>
```

Step 4: Install the Eye new SW package:

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

```
[root@Eye]# cd /nand
```

802.11a/b/g/n unit:

```
[root@Eye]# ./7signal-eye-v0X.YY-APU3–installer.bin
```

802.11a/b/g/n/ac unit:

```
[root@Eye]# ./7signal-eye-v0X.YY-MPU1–installer.bin
```

Step 5: Restart:

802.11a/b/g unit and 802.11a/b/g/n units (E1000 / E2000):

```
[root@Eye]# reboot
```

5.6 Start Automated Testing

Automated testing is in a stopped state after the Sapphire has been upgraded.

Step 1: Start Configurator:

Step 2: Start Automated Testing:

Select “Tools | Start Automated Testing”.

6

UNINSTALLING SAPPHIRE

6.1 Pre 8.2 releases

6.1.1 Uninstall Analyzer server

Step 1: Stop Analyzer server:

Login to Carat host and stop the Analyzer server by issuing the command:

```
# 7analyzer stop
```

Step 2: Uninstall Analyzer server:

Change to Analyzer installation directory:

# cd <*Analyzer installation directory*>

Uninstall the Analyzer server by issuing the command:

```
# ./analyzer_server_uninstall.sh
```

The uninstaller script starts. Confirm uninstall by entering “y”:

```
7signal Sapphire Analyzer server will be removed (/opt/7signal/Analyzer). Are you
sure [y/N]? y
```

The uninstallation is finished when the script is ready.

6.1.2 Uninstall Carat server

Step 1: Stop Carat server:

Login to Carat host and stop the Carat server by issuing the command:

```
# 7carat stop
```

Step 2: Uninstall Carat server:

Change to Carat installation directory:

```
# cd /<Carat installation directory>/vX.X-Y.Y/
```

Uninstall the Carat server by issuing the command:

```
# ./carat_uninstall.sh
```

The uninstaller script starts. Confirm uninstall by entering “y”:

```
7signal Sapphire Carat, related user account and home directory will be removed. Are you sure
        [y/N]? y
```

The uninstallation is finished when the script is ready.

6.1.3 Uninstall DBMS

The Carat and Application servers must be uninstalled before DBMS can be uninstalled. See sections 6.1.1 and 6.1.2.

Login to Carat host and change to DBMS installation directory. It is the parent directory of the former Carat installation[6]:

# cd /<*DBMS installation directory*>

Uninstall the DBMS by issuing the command:

# ./uninstall-dbms.sh

[6] For example, if Carat server was installed to `/opt/7signal/Carat`, the DBMS installation directory is `/opt/7signal/dbms`.

The uninstaller script starts. Confirm uninstall by entering “y”:

The uninstallation is finished when the script is ready.

6.1.4 Uninstall Sonar

Step 1: Stop Sonar server:

Login to Sonar host and stop the Sonar server by issuing the command:

```
# service 7signalSonar stop
```

Step 2: Uninstall Sonar server:

Change to Sonar installation directory (e.g. /opt/7signal/Sonar):

```
# cd /<Sonar installation directory>
```

Uninstall Sonar by issuing the command:

```
# ./sonar_uninstall.sh
```

The uninstaller script starts. Confirm uninstall by entering “y”:

```
7signal Sonar will be removed. Are you sure [y/N]? y
```

The uninstallation is finished when the script is ready.

7

Log Settings

All 7signal Sapphire elements have logging capability.

7.1 Carat server log

The log file - server.log - is located in /opt/7signal/Carat/7signal. The directory contains older log files as well, named server.log.* where by default the asterisk (*) is in range of 1..5. Altogether, there is one active log file named server.log and five files for circulating the files. The oldest log gets overwritten.

To check the latest logs one should issue the following command:

```
# 7carat log
```

For continuous real-time logging:

```
# 7carat log -f
```

The Carat log level can be checked or changed by using loglevel command of 7carat tool (for example, from INFO to DEBUG which produces much more detailed information):

```
# 7carat loglevel show

# 7carat loglevel set DEBUG
```

Notice that Carat server has to be restarted in order to bring the changed log level into use.

7.2 Eye 1000/2000 log

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.

The Eye unit has an in-memory circular log that can be followed in real-time with the following command:

```
# logread -f
```

Without any arguments the command shows the complete log file immediately:

```
# logread
```

The logging can be directed to rotating log files instead of the ring buffer with 7config log – command. The log file is /var/log/messages

In order to change logging to log files, issue the following command:

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

To change logging back to ring buffer, use the following command:

```
# 7config log set target buffer
```

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

```
# 7config log show
```

7.3 Eye 2100/500/2200 log

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.

7.3.1 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.

In order 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
```

7.3.2 System logs

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

7.4 Application server log

Application server is based on Tomcat so the log file is named *catalina.out* and is by default in directory /<*Analyzer installation directory*>/apache-tomcat-<*version*>/logs.

Tool to follow the most recent logging is

```
# 7analyzer log
```

and for continuous log monitoring:

```
# 7analyzer log -f
```

7.5 Sonar log (Linux)

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

7.6 Eye 2100/500/2200 remote syslog configuration

Eye 2100/500/2200 support remote syslogging. The following instructions show how to configure it.

Step 1: Install rsyslog 7 to the logging server

Uninstall rsyslog 5:

```
$ sudo yum remove rsyslog
```

Install rsyslog 7:

```
$ sudo yum install rsyslog7
```

Install rsyslog TLS plugin:

```
$ sudo yum install rsyslog7-gnutls
```

Restart rsyslog and verify it starts without problems:

```
$ sudo service rsyslog restart
```

```
$ sudo tail -f /var/log/messages
Sep 18 10:55:37 localhost rsyslogd: [origin software="rsyslogd" swVersion="5.8.10"
x-pid="2275" x-info="http://www.rsyslog.com"] exiting on signal 15.
```

```
Sep 18 10:58:33 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.10"
x-pid="5860" x-info="http://www.rsyslog.com"] start
```

Step 2: Create TLS certificates

Create TLS certificates for remote syslogging. Use 7signalSyslogCertTool.sh, the tool will create server and client certificates. It also creates a CA if necessary. You cand find the 7signalSyslogCertTool.sh on the distribution media “Utilities/Script/Syslog” directory.

Install gnutls.utils first, 7signalSyslogCertTool.sh requres it:

```
$ sudo yum install gnutls-utils

$ ./7signalSyslogCertTool.sh
7signalSyslogCertTool.sh [-avsch] <Certificate directory>

CA is generated only if it has not been generated yet.

Options:

-a <CA valid days>             Default 3650 days.
-v <Certificate valid days>     Default 365 days.
-s <Server address>            Generate server certificate, server address.
-c                             Generate client certificate.
-h                             Show help.
```

For example, the command below creates a CA (if it is not already created in directory /root/newcerts), CA will be valid about 10 years, certificates will be valid about 5 years, and both client and the server certificates will be created. Syslog server IP address will be 10.10.10.147.

```
$ ./7signalSyslogCertTool.sh -a 3650 -v 1800 -s 10.10.10.147 -c \
/<dir>/newcerts
```

The following directory structure will be created in /<*dir*>/newcerts:

```
|---- CA
|     |---- 7signal-syslog-ca-key.pem
|     |---- 7signal-syslog-ca.pem
|
|---- syslog-client
|     |---- 2017-09-18_130448
|           |---- 7signal-syslog-client-cert.pem
|           |---- 7signal-syslog-client-key.pem
|           |---- 7signal-syslog-client-request.pem
|
|---- syslog-server
    |---- 017-09-18_130448
            |---- 7signal-syslog-server-cert.pem
            |---- 7signal-syslog-server-key.pem
            |---- 7signal-syslog-server-request.pem
```

Remember to secure the CA private key!

Step 3: Install server certificates on the logging server

Copy the server certificate, private key and CA certificate to the logging server, in this example 10.10.10.147:

```
$ scp /<dir>/newcerts/CA/7signal-syslog-ca.pem
/<dir>/newcerts/syslog-server/2017-09-18_130448/7signal-syslog-server-cert.pem
/<dir>/newcerts/syslog-server/2017-09-18_130448/7signal-syslog-server-key.pem
10.10.10.147:/<remotedir>/
```

On the logging server, create directory structure under /etc/ssl and move the certificate files to correct directories:

```
$ sudo mkdir -p /etc/ssl/7signal/private
$ sudo mv /<remotedir>/7signal-syslog-ca.pem /etc/ssl/7signal/
$ sudo mv /<remotedir>/7signal-syslog-server-cert.pem /etc/ssl/7signal/
$ sudo mv /<remotedir>/7signal-syslog-server-key.pem /etc/ssl/7signal/private/
```

Change file permissions of the CA and server certificates:

```
# sudo chmod 755 /etc/ssl/7signal/7signal-syslog-ca.pem
/etc/ssl/7signal/7signal-syslog-server-cert.pem
```

Step 4: Configure rsyslog:

Create configuration file for Eye remote syslogs:

```
$ sudo vi /etc/rsyslog.d/7signalEyeLogs.conf
```

Set the configuration parameters:

```
$ModLoad imtcp
```

```
$DefaultNetstreamDriver gtls
$DefaultNetstreamDriverCAFile /etc/ssl/7signal/7signal-syslog-ca.pem
$DefaultNetstreamDriverCertFile /etc/ssl/7signal/7signal-syslog-server-cert.pem
$DefaultNetstreamDriverKeyFile /etc/ssl/7signal/private/7signal-syslog-server-key.pem
$InputTCPServerStreamDriverAuthMode x509/name
$InputTCPServerStreamDriverPermittedPeer Eye
$InputTCPServerStreamDriverMode 1
$InputTCPServerRun 10514

$template EyeMessages,"/var/log/EyeLogs"

if $source != 'localhost' then ?EyeMessages
& stop
```

The configuration above:

- Enables remote TLS syslogs for “Eye” peers
- Uses custom TCP port 10514
- Configures authentication
- Redirects log entries from Eyes to /var/log/EyeLogs

If SELinux is enabled and a custom port (not 6514 or 601) is wanted to be used:

Install policycoreutils:

```
$ sudo yum install policycoreutils-python
```

Configure the custom port:

```
$ sudo semanage port -a -t syslogd_port_t -p tcp 10514
```

Restart rsyslog and verify that there are no errors reported in /var/log/messages:

```
$ sudo service rsyslog restart
$ sudo tail -f /var/log/messages

Sep 18 11:46:31 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.10"
x-pid="5860" x-info="http://www.rsyslog.com"] exiting on signal 15.
Sep 18 11:46:31 localhost rsyslogd: [origin software="rsyslogd" swVersion="7.4.10"
x-pid="9838" x-info="http://www.rsyslog.com"] start
```

Step 5: Configure firewall

Add a rule for syslog TCP port to /etc/sysconfig/iptables, in this example the port is 10514

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 10514 -j ACCEPT
```

Reload iptables:

```
$ sudo service iptables reload
```

Step 6: Configure logrotate on the logging server

Create logrotate configuration for Eye logs:

```
$ sudo vi /etc/logrotate.d/Eyelogs
```

A configuration file example:

```
/var/log/EyeLogs
{
    missingok
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

Step 7: Configure Eyes to start logging to the logging server

Copy the client certificates to the Carat server. In this example, Carat and syslog server are running on the same host.

```
$ scp /<dir>/newcerts/CA/7signal-syslog-ca.pem
/<dir>/newcerts/syslog-client/2017-09-18_130448/7signal-syslog-client-cert.pem
/<dir>/newcerts/syslog-client/2017-09-18_130448/7signal-syslog-client-key.pem
10.10.10.147:/<remotedir>/
```

Log in to the Carat server, and copy the certificate files e.g. to /home/carat7/certificates:

```
$ sudo mkdir /home/carat7/certificates
$ sudo mv /<remotedir>/7signal-syslog-ca.pem /home/carat7/certificates/
$ sudo mv /<remotedir>/7signal-syslog-client-cert.pem /home/carat7/certificates/
$ sudo mv /<remotedir>/7signal-syslog-client-key.pem /home/carat7/certificates/
$ sudo chown -R carat7:carat7 /home/carat7/certificates/
```

Edit Carat configuration file /opt/7signal/Carat/7signal/conf/server_conf.prop. Set up certificates, remote server and syslog mode:

```
# Eye syslog mode: "local", “udp”, "tcp" or "tls"
eye.syslog.method=tls

# Eye remote syslog server address (if syslog mode is "tcp" or "tls")
eye.syslog.remote.server.address=10.10.10.147

# Eye remote syslog server port  (if syslog mode is "tcp" or "tls")
eye.syslog.remote.server.port=10514

# The certificate (PEM format) that Eyes will use to verify identity of a remote syslog server
(if syslog mode is "tls")
eye.syslog.remote.ca.certificate=/home/carat7/certificates/7signal-syslog-ca.pem

# The client certificate (PEM format) that Eyes will use when connecting to a remote syslog
server (if syslog mode is "tls")
eye.syslog.remote.client.certificate=/home/carat7/certificates/7signal-syslog-client-cert.pem

# The private key (PEM format) that Eyes will use when connecting to a remote syslog server (if
syslog mode is "tls")
eye.syslog.remote.ca.private.key=/home/carat7/certificates/7signal-syslog-client-key.pem
```

Restart the Carat server:

```
$ sudo service 7signalCarat restart
```

8

SAPPHIRE PROCESS MANAGEMENT

8.1 Carat

Carat is a service on Linux systems. However, the Carat process is supposed to be used by 7signal tool called *7carat*:

```
# 7carat <parameter-from-the-bullet-list>
```

- start
- stop
- restart
- status

8.2 Application server

Application server is a service on Linux systems. However, the Application server process is supposed to be used by 7signal tool called *7analyzer*:

```
# 7analyzer <parameter-from-the-bullet-list>
```

- start
- stop
- restart

- status

8.3 Sonar

Sonar is a service on Linux systems:

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

- start
- stop
- restart
- status

8.4 Eye

NOTE: The following command requires an SSH session into the Eye (monitoring station).

The utility 7config controls the Eye configuration. See more details for the tool in chapter 10. The process is controlled with command group *run*.

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

- start
- stop
- restart
- status

9

TROUBLESHOOT

9.1 Cannot add Eye unit

1. Check that license.xml file is located in the Carat server
    a. Check the Carat server log for possible license errors
    b. Check the existence of the file
        i. The default location for the license file is /opt/7signal/Carat/7signal/conf
    c. The file permission should be 744.
    d. Check the contents of the file to look for any anomalies
2. Run 7config verify command in Eye unit
3. Check that maximum number of Eye's (license defines) is not exceeded.
4. Check that carat.keystore is located in the Carat server
    a. the default folder location is /opt/7signal/Carat/7signal/conf

9.2 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

9.3 Web app cannot connect to Carat server

Application server and Carat are both run on the Carat host machine.

1. Check that username and password are correct
2. Check Application server log for error messages
   a. 7analyzer log
3. Check that Application server server is running
   a. 7analyzer status
4. Check Carat log for error messages
   a. 7carat log
5. Check that Carat server is running
   a. Run command 7carat status

9.4 Eye IP address forgotten

9.4.1 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

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

9.5 Collecting information for further analysis

Sometimes it might be necessary to collect Sapphire log files and Linux system information and send them to 7signal support team. To make this easier, “7carat collect logs” will gather all required information into one file.
On the Carat server, as root, issue the command:

# 7carat collect logs

The command collects Sapphire log files and other information (see chapter 12.4) and stores all data to one file, Sapphire_logs-<*timestamp*>.tar.gz.

10

Command-line utility for Eye

10.1 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
```

10.2 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
```

10.3 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
```

10.4 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
```

10.5 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>
```

10.6 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
```

10.7 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
```

10.8 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) (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) 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
```

COMMAND-LINE TOOL FOR DATABASE MANAGEMENT

7db command is a tool for the Carat database. It supports limited data retrieval, general management and database backup administrator for both immediate and automatic backups.

It is recommended that database backups should be taken regularly.

7db command groups:

dump	Dump export and import
show	Show status and configurations
reinit	Re-initialize databases
backup	Automatic backup management
logsetup	To change the current logging method
reorg	Reorganize the database
db2	Access to database management system command-line tool

11.1 Logsetup command

Changes the way the underlying DBMS handles logging.

NOTE: the command is trivial to issue but its consequences are highly resource consuming.
Observe awareness when using this command.

There are two different logging modes in 7signal Sapphire. This command switches between the modes. There is lots of informative output as this command should not be used carelessly or without proper planning and understanding of the consequences.

The command examines the current state of all three different underlying databases. In case they differ from each other, the processing shall stop as it is expected that all the databases are handled similarly. In case the logging method differs, there has been some significant error in DB administration and system otherwise.

The *logsetup* command may result in numerous backups for the safety reasons so the overall process duration is rather long.

11.2 Backup command group

Creates instant and automatic database backups. It is possible to schedule one offline and/or one online backup point.

NOTE: the backup policy should be well-planned. Please see the 7signal Sapphire User Guide for further discussion on backup and the options available.

Backup commands:

- show Show automatic backup configuration
- remove Remove automatic backup configuration
- set Configure automatic backup
    - daily <HH:mm> <backup directory>
    - weekly <DDD> <HH:mm> <backup directory>
      <DDD> = Mon, Tue, Wed, etc.
    - monthly <day> <HH:mm> <backup directory>
    - directory <backup directory>
      Backup directory is optional if a backup configuration already exists.
- now Immediate backup.
    - online
    - offline
- restore Recovery command
- workdir Configure working directory used in backup and restore operations.

Examples:

Remove configuration

```
# 7db backup remove
```

Backup offline every Wednesday at 00:30 to /mnt/backups

```
# 7db backup set weekly Wed 00:30 /mnt/backups offline
```

Backup online every day at 03:00 to /mnt/backups

```
# 7db backup set daily 03:00 /mnt/backups online
```

Change backup directory to /mnt/newbackups, do not change time settings

```
# 7db backup set directory /mnt/newbackups
```

Backup every Sunday at 00:30, do not change backup directory

```
# 7db backup set weekly Sun 01:30
```

Back the system up immediately offline

```
# 7db backup now /mnt/backups offline
```

Back the system up immediately online (requires archival database logging)

```
# 7db backup now /mnt/backups online
```

Set working directory for backup and restore (highly recommended for larger databases)

```
# 7db backup workdir set /opt/largefilesystem
```

Restore a known-to-be-good system state

```
# 7db backup restore <backup-file>
```

11.3 Show command group

Shows the status and configuration of the database

Show commands:

- tabstatus   Show the status of the tables.
    - all
    - <database_name>
- conf   Show configuration of the database.

Examples

Show status of the tables in the MEAS7 and MGMT7 databases

```
# 7db show tabstatus all
```

Show status of the tables in the SECUR7 database

```
# 7db show tabstatus secur7
```

Show status of the CARAT7.ap_ftp_qos_test table in the MEAS7 database

```
# 7db show tabstatus meas7 ap_ftp_qos_test
```

Show configuration of the database

```
# 7db show conf
```

11.4 Reinit command group

Empty the database and resume initial state of the system.

```
# 7db reinit
```

Examples:

Re-initialize the MEAS7 and MGMT7 databases

```
# 7db reinit all
```

Re-initialize the MEAS7 database

```
# 7db reinit meas7
```

Re-initialize CARAT7.ap_ftp_qos_test table in the MEAS7 database

```
# 7db reinit meas7 ap_ftp_qos_test
```

11.5 Reorg command group

Reorganize the database.

```
# 7db reorg
```

Examples:

Re-organize the MEAS7 and MGMT7 databases

```
# 7db reorg all
```

Re-organize the MEAS7 database

```
# 7db reorg meas7
```

Re-organize the MGMT7 database

```
# 7db reorg mgmt7
```

12

COMMAND-LINE TOOL FOR CARAT SERVER

7carat command is a tool for Carat server management. 7carat command groups are:

start/stop/status/restart	Manage the carat process
log	Show the log of the server
conf	Show the configuration of the server
verify	Verify the configuration
loglevel	Manage the carat log levels
license	Manage the carat license
integritycheck	Verify database integrity
certificate	Update encryption certificates
ip configuration	Update server IP address to
collect for analysis	Collect Sapphire log files and configuration
memoryconf	Reconfigure Carat Java memory heap

12.1 License command group

Manage the carat license.

Examples:

Show the license information

```
# 7carat license
```

Install new carat license

```
# 7carat license set <full path and name of the license file>
```

12.2 Integritycheck command group

Verify the database integrity.

Examples:

Execute the integritycheck

```
# 7carat integritycheck
```

IMPORTANT: Sapphire Carat must not be running when issuing this command!

12.3 Ip command group

If the IP address of the Linux host is changed, the changed IP address needs to be configured to the Carat server as well.
Examples:
IP address of the Linux server is changed to 192.168.10.10. Configure new address to Carat server.

```
# 7carat ip set 192.168.10.10
# 7carat restart
```

12.4 Collect command group

Collect information about Sapphire installation and status of the Linux host for analysis. This collected information includes:

- Application server (Analyzer)
  - Certificate files
  - Configuration files
  - Log files
- Carat
  - Certificate files
  - Configuration files

  - Log files
- DB2
  - DB2 diagnostics log
  - DB2 instance log file
- Linux host
  - CPU information
  - Kernel log
  - Memory information
  - System log files
  - List of running processes
  - Linux distribution information
  - Top memory consumers
  - System information (uname)
  - vmstat output

The information is collected to a file named Sapphire_logs-<*timestamp*>.tar.gz.

12.5 Memoryconf command group

The Carat installer sets appropriate size for the Carat server Java heap memory automatically. However, if the available RAM of the server changes, it can be necessary to reconfigure the Java heap. memoryconf command analyzes the available RAM and reconfigures the Carat Java heap memory automatically.
Examples:

```
# 7carat memoryconf
```

13

Updating encryption certificates

Sometimes it is necessary to update encryption certificates used throughout the Sapphire solution. Certificates can be updated from the certificate package file in Linux, a separate truststore file and truststore password are needed in Windows. Certificate packages can be downloaded from 7signal Share File.
It is also possible to install a custom HTTPS certificate for the Analyzer/EyeQ/Configurator. By using this feature, organizations can use their own HTTPS certificates in the Analyzer.

13.1 Updating Carat server certificates

Step 1: Login to Carat server host as root user

Step 2: Use 7carat tool to update certificate

```
# 7carat certificate set /path_to_package/mycerts-7signal-all.tar.gz
```

```
Validating archive file..........................................OK
Updating Carat server certificates.................................
Found Carat configuration from /opt/7signal/Carat/7signal/conf...OK
Extracting carat keystore files..................................OK
Extracting 7signal keystore......................................OK
Extracting Eye certificate......................................OK
Extracting Eye certificate password.............................OK
Extracting carat keystore password..............................OK
Extracting 7signal keystore password.............................OK
Updating server configuration file...............................OK
Updating setup configuration file................................OK
```

13.2 Updating web app certificates

Step 1: Login to Application server host as root user

Step 2: Use 7analyzer tool to update certificates

```
# 7analyzer certificate set /path_to_package/mycerts-7signal-all.tar.gz
```

```
Validating archive file.........................................OK
Updating Analyzer certificates....................................
Found /opt/7signal/Analyzer/webapps/WEB-INF/web.xml.............OK
Found /opt/7signal/Analyzer/apache-tomcat-5.5.26/conf/server.xml.OK
Found /opt/7signal/Analyzer/start_loupe_server.sh................OK
Found current truststore file....................................OK
Extracting 7signal truststore....................................OK
Installing 7signal truststore....................................OK
Extracting Analyzer keystore.....................................OK
Extracting truststore password...................................OK
Extracting keystore password.....................................OK
Modifying configuration files....................................OK
```

13.3 Updating Eye certificates

Step 1: Transfer certificate package to Eye /tmp directory by using SCP

For example, in Carat server host:

```
# scp /path_to_package/mycerts-7signal-all.tar.gz root@<Eye IP address>:/tmp
```

Step 2: Login to Eye by using SSH

```
# ssh root@<Eye IP address>
```

Step 3: Install certificate from certificate package

```
# 7config conn encryption install /tmp/mycerts-7signal-all.tar.gz
```

13.4 Installing custom HTTPS certificate to Application server

It is possible to install organization's own HTTPS certificates to the Application server.

Step 1: Concatenate all certificate files to one file

Importing custom certificates require that all certificates must be in PEM format. In order to avoid browser warnings, the whole certificate chain must be included (root certificate and all intermediate certificates). Certificates must be in a right order. The root certificate must be on bottom, and the server certificate on the top. The server certificate private key must be also available in PEM format.
Example:
There are four certificates:

- AddTrustExternalCARoot.crt: Root certificate
- UserAddTrustCA.crt: 1st level intermediate certificate
- MySSLProvider.crt: 2nd level intermediate certificate
- MyServerCertificate.crt: The server certificate to be installed

Concatenate the certificates (Unix example)

```
# cp AddTrustExternalCARoot.crt all_certificates.pem
# cat UserAddTrustCA.crt >> all_certificates.pem
# cat MySSLProvider.crt >> all_certificates.pem
# cat MyServerCertificate.crt >> all_certificates.pem
```

All certificates are now in the file all_certificates.pem, in the right order.

Step 2: Install the certificates to the Application server

Once all certificates are in one file and the private key is available, issue a command:

```
# 7analyzer certificate install <certificate file> <private key file>
```

Example:

If the certificates are in all_certificates.pem and the private key is in file mykey.pem:

```
# 7analyzer certificate install all_certificates.pem mykey.pem

Certificate and private key are in PEM format, ok
Removing current TLS certificate..
Creating temporary keystore..
Importing temporary keystore to Analyzer keystore..
Entry for alias tomcat successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
Successfully installed a custom TLS certificate.
```

14

DATABASE MAINTENANCE

In order to keep the database working optimally, it is suggested that the following database maintenance tasks are scheduled to be done automatically:

1. Online data purges. Data purges prevent database file systems to not get full.
2. Database backups. Recent backups are mandatory in order to recover from fatal file system errors, broken disks, etc.
3. Table / index reorganizations. By doing regular reorganizations the database structure stays in optimal shape.
4. Collecting statistics. This keeps database query access paths optimized.
5. Watching DB / log filesystem usage. This prevents database corruption if filesystems are getting full.

Because any of tasks can take a considerably long time to execute, it is important to be able to execute the tasks in the background:

Install tmux:

```
# yum install tmux
```

tmux commands:

- Start a new session: **tmux**
- Detach from the session without closing it: **CTRL b+d**
- Joining to the created session: **tmux a**
- Exiting from the session and closing it: **exit**

Alternatively, **screen** utility can be used.

Please wait for one task to complete before starting the next one.

14.1 Online data purge

The measurement data collected by 7signal Sapphire can take lots of disk space. Sapphire provides a tool for online removal of old measurement data.

> Configuring the data purge requires knowledge about DB2 database, so a Database Administrator should always be involved when setting up measurement data purge process.

Online data purge requires a set of additional database indexes, which can take reasonable amount of disk space. Make sure that there is at least 30% free disk space on the database partition before upgrading to Sapphire 7.3 or 8.1.

It is preferred to execute the purge daily basis, in conjunction with the backup. See chapter 14.3 for more information about the backup process.

Database with archival logging

If the DB2 archival logging is enabled, online data purge can be configured without any further steps. Notice that data purge produces lots of database transactions, and transaction logs will be archived, so a proper backup plan must be in place (backup process deletes old archived transaction logs automatically).

Database with circular logging

If the DB2 circular logging is enabled (the default), some additional steps are needed. The database indexes required by the online data purge are not created automatically, because the database can run out of transaction logs while creating the indexes. How to create the indexes is described in the next chapter.

If creating indexes does not succeed due to insufficient amount of transaction log space, you can change database configuration parameters in order to get more space of the transactions. Before changing any parameters, save the current values:

```
$ db2 get db cfg for meas7 > /tmp/meas7_db_config.txt
```

Change either maximum number of log files or log file size parameters, or both:

1. Increase number of transaction logs. The maximum number of files is 256

   ```
   $ db2 connect to meas7
   $ db2 update db cfg using logprimary 256
   ```

2. Increase size of the log files

   ```
   $ db2 connect to meas7
   $ db2 update db cfg using logfilsiz 32768
   ```

After changing the database configuration, you must restart the database instance:

```
$ db2stop force
$ db2start
```

After changing the configuration parameters, try to re-create the indexes (as described chapter 14.1.1).

- If the indexes are generated successfully, restore the original database configuration parameters and restart the instance.
- If the index creation fails again due to insufficient transaction log space, increase the database configuration parameters and try to recreate the indexes.

If you have any problems or questions, please contact 7signal Customer Service (support@7signal.com).

14.1.1Required database indexes

Online data purge requires a set of database indexes. The index set is created automatically on Sapphire installations that have archival database logging enabled. On installations that have circular database logging enabled, the index set must be created manually.

Step 1: Login to Carat server host as root

Step 2: Switch to db7sign user

```
# su – db7sign
```

Step 3: Execute SQL script that creates the indexes

NOTE: If the database partition does not have much free disk space, it is suggested that current index set is dropped before the new ones are created. Issue the command:

```
$ /opt/7signal/dbms/v<version number>/db2/drop_meas_indexes.sh
```

Update the index set by issuing the command:

```
$ /opt/7signal/dbms/scripts/update_meas7_indexes.sh
```

Step 4: Rebind purge stored procedure

```
$ db2 "CALL SYSPROC.REBIND_ROUTINE_PACKAGE ('P','CARAT7','','PRUNE_DATA','')"
```

14.1.2Executing data purge

The utility used for online data removal is “`7PurgeTool.sh`” and it can be found on the Carat server in directory “`/opt/7signal/dbms/scripts`”. The utility removes data one day at once. In catch-up mode, the utility removes data one day at once until the desired amount of data (days) is left in the database.

Step 1: Login to Carat server host as root

Step 2: Switch to db7sign user

```
# su – db7sign
```

Step 3: Execute initial data purge

Usually, users want to keep certain amount of historical data in the database. When configuring the data removal first time, there can be more data in the database than desired amount of days. The first

Check the options:

```
$ /opt/7signal/dbms/scripts/7PurgeTool.sh -h
Usage: 7PurgeTool.sh OPTIONS

OPTIONS -d <days> Number of days of data left to the database.
                  All tables except SCAN_RADIO and SPECTRUM_PARAM,
                  SPECTRUM_RESULT and SPECTRUM_RESULT_5GHZ
                  Default value is 180.
        -s <days> Number of days of data left to the database.
                  Tables SCAN_RADIO and SPECTRUM_PARAM,
                  SPECTRUM_RESULT and SPECTRUM_RESULT_5GHZ
                  Default value is 30.
        -c        Catch up mode. Purges data one day at once until
                  desired number of days have been reached.
        -w <secs> In catch-up mode, wait <sec> number of seconds
                  before running the next purge.
```

Execute the utility in catch-up mode. For example, if 30 days of spectrum and scan data is fine, but amount of other data should be 90 days:

```
$ /opt/7signal/dbms/scripts/7PurgeTool.sh -c -d 90 -w 0
```

-w 0 means that the utility does not wait before it proceeds to delete the next day.

The utility starts to delete data one day at once:

```

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.5
 SQL authorization ID   = DB7SIGN
 Local database alias   = MEAS7

Current date is 2017-12-19
Spectrum data: oldest date: 2017-10-19
Scan data: oldest date    : 2017-12-08
Other data: oldest date   : 2017-06-23
Spectrum data: catch-up days: 61
Scan data: catch-up days    : 11
Other data: catch-up days   : 179
Executing purge: Number of days: Other data 179, Spectrum and Scan 61

  Value of output parameters
  --------------------------
  Parameter Name  : P_SQLCODE_OUT
  Parameter Value : 0

  Parameter Name  : P_SQLSTATE_OUT
  Parameter Value : 00000

  Parameter Name  : P_ERROR_MSG
  Parameter Value :

  Parameter Name  : P_START_TIME
  Parameter Value : 2017-12-19-13.28.41.665326

  Parameter Name  : P_END_TIME
  Parameter Value : 2017-12-19-13.29.04.810131

  Return Status = 0

Purge executed successfully.
Waiting 0 seconds ...
Executing purge: Number of days: Other data 178, Spectrum and Scan 60

  Value of output parameters
  --------------------------
  Parameter Name  : P_SQLCODE_OUT
  Parameter Value : 0

  Parameter Name  : P_SQLSTATE_OUT
  Parameter Value : 00000

  Parameter Name  : P_ERROR_MSG
  Parameter Value :
```

```
  Parameter Name  : P_START_TIME
  Parameter Value : 2017-12-19-13.29.04.880104
```

Depending on how many days it needs to delete, the execution can take from few hours to few days.

Step 4: Configure daily purge

Once the initial purge is complete, a daily purge can be configured as a cron task.

As db7sign user:

$ crontab –e

Add a line for a scheduled purge. In an example below, purge is executed daily at 3am

```
0 3 * * 0      /opt/7signal/dbms/scripts/7PurgeTool.sh -d 90 >> /var/log/purge.log 
2>&1
```

Save the crontab and the configuration is ready.

14.2 Table / index reorganization

The `7Reorg.sh` tool, located in directory `/opt/7signal/dbms/scripts`, checks if tables or indexes need a reorganization, and executes the online reorganization if necessary. Depending on DB2 license, the tool can either reorganize tables and indexes, or indexes only:

- DB2 Express-C (default license): Reorganizes indexes only. The tool outputs a warning if it detects a table that would need reorganization. Offline reorganization is needed for the tables.
- DB2 Express/Workgroup etc.: Reorganizes tables and indexes

14.2.1Executing online reorganization

Step 1: Switch to “db7sign” user

Step 2: Execute the utility.

```
$ /opt/7signal/dbms/scripts/7Reorg.sh
```

Example output on a system with DB2 Express-C database

```
Reorg start time Sun Aug 19 10:00:01 EDT 2018

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.5
 SQL authorization ID   = DB7SIGN
 Local database alias   = MEAS7

WARNING: CARAT7.SCAN_RADIO needs OFFLINE REORG
WARNING: CARAT7.SPECTRUM_PARAM needs OFFLINE REORG
WARNING: CARAT7.SPECTRUM_RESULT needs OFFLINE REORG
WARNING: CARAT7.SPECTRUM_RESULT_5GHZ needs OFFLINE REORG
Checking index CARAT7.GTS1_X1_AIR_UTILIZATION_TEST
Reorganizing all indexes of table AIR_UTILIZATION_TEST
DB20000I  The REORG command completed successfully.
Checking index CARAT7.GTS1_X2_AIR_UTILIZATION_TEST
Checking index CARAT7.GTS1_X11_AP_ACCESS_TEST
Reorganizing all indexes of table AP_ACCESS_TEST
DB20000I  The REORG command completed successfully.
...
Checking index CARAT7.GTS2_SCAN_RADIO
DB20000I  The SQL command completed successfully.
Reorg end time Sun Aug 19 14:00:50 EDT 2018
```

The output indicates that four tables would benefit from an offline reorganization. All indexes that required a reorganization were reorganized successfully.

Example output on a system with DB2 Express license

```
Reorg start time Sun Jul 29 10:00:01 CDT 2018

   Database Connection Information
```

```
 Database server        = DB2/LINUXX8664 10.5.5
 SQL authorization ID   = DB7SIGN
 Local database alias   = MEAS7

Reorganizing table CARAT7.SPECTRUM_RESULT_5GHZ
DB20000I  The REORG command completed successfully.
DB21024I  This command is asynchronous and may not be effective immediately.

Reorg done. Reorganizing all indexes of table CARAT7.SPECTRUM_RESULT_5GHZ
DB20000I  The REORG command completed successfully.
Checking index CARAT7.GTS1_X1_AIR_UTILIZATION_TEST
Reorganizing all indexes of table AIR_UTILIZATION_TEST
DB20000I  The REORG command completed successfully.
Checking index CARAT7.GTS1_X2_AIR_UTILIZATION_TEST
Checking index CARAT7.GTS1_X11_AP_ACCESS_TEST
...
Checking index CARAT7.GTS2_SCAN_RADIO
DB20000I  The SQL command completed successfully.
Reorg end time Sun Jul  29 11:13:21 CDT 2018
```

The output shows that one table required a reorganization. The table and all indexes that required a reorganization were reorganized successfully.

14.2.2Executing offline table reorganization

`7Reorg.sh` output may indicate that reorganizing some of the tables offline would be beneficial. For example:

"**`WARNING: CARAT7.SCAN_RADIO needs OFFLINE REORG`**"

In order to execute offline reorganization of tables:

Step 1: Stop Carat and Application servers

```
# 7carat stop
# 7analyzer stop
```

Step 2: Switch to "db7sign" user

Step 3: Connect to measurement database

```
$ db2 connect to meas7
```

Step 4: Execute reorganization command for each table that required offline reorganization

```
$ db2 reorg table CARAT7.SCAN_RADIO
```

Step 5: Switch back to root user and start Carat and Application servers

```
$ exit
# 7carat start
# 7analyzer start
```

Notice: Offline reorganization of a table can take several hours. However, table level reorganizations are not needed very often.

14.2.3Scheduling reorganizations

Reorganizations should be done regularly. Probably the easiest way to schedule reorganizations is to use cron.

Important: Use crontab of “db7sign” user.

Example reorganizations schedule

Use “crontab -e” to edit the crontab of the “db7sign”user.

```
# Reorganization every Sunday at 3 am. Redirect output to /var/log/reorg.log
0 3 * * 0     /opt/7signal/dbms/scripts/7Reorg.sh >> /var/log/reorg.log 2>&1
```

14.3 Database backups

Database backup utility 7BUtool.sh can be found in directory `/<DBMS install directory>/scripts`. The utility can be used to take offline, online and incremental online delta backups. Online backups are possible only if archival logging has been enabled on DB2. The utility is also able to transfer backup images to a remote storage server.

Multiple backup directories can be provided. By using multiple backup directories backup process is faster, due to DB2 I/O parallelism. If DB2 archival logging is configured, the utility deletes old archived transaction logs automatically (by default, the utility retains 7 days of old log files). The utility also keeps latest offline/online backup images locally, and incremental online delta backups for 7 days by default.

When creating offline backups, the utility must be executed as a root user. When creating online backups, the utility must be executed as “db7sign” user.

14.3.1Backup planning

Backups can require lots of disk space. That’s why it is important to have a proper backup plan, and in most of the cases a Database Administrator (DBA) should be involved in backup planning/implementation.

The following things should be considered:

- Depending on how many backups are wanted to be kept locally, the combined size of the backup file systems should be at least *2 x number of backups x current database size*. Backups images are not compressed by the backup utility.

- If DB2 archival logging (which enables online backups) is in use, archived transaction log files can take lots of disk space. When taking a backup, archived log files will be included in the backup images, and they can be deleted afterwards. 7BUtool.sh deletes the old archived log file automatically, but by default it keeps log files of last 7 days. You can control how many days will be kept by using `-l` option of the 7BUtool.sh utility.
- If the backup plan includes incremental online delta backups, by default the backup utility keeps delta backups of last 7 days locally. You can control how many days will be kept by using `-k` option of the 7BUtool.sh utility.
- If a remote storage server is in use, it must be verified that the server does not run out of disk space. This means that older backup images must be deleted periodically on the server. In order to automate deletion of old backup images you can use the `cleanupOldBackups.sh` script.

14.3.2Command arguments and options

Use `-h` option to show command help:

```
$ ./7BUtool.sh -h

Usage: 7BUtool.sh <backup directory1> [backup directory2] [backup directory3]
Options: -s <server>          Name of this server (on which 7BUtool.sh is run).
         -b <backup server>   Address of the remote backup server. The server to
                              which the backup images are copied.
         -u <username>        User name on the remote backup server.
         -d <directory>       Backup directory on the remote backup server.
                              The directory to which the DB backup images
                              are copied over the network.
         -o                   Do an online backup.
         -i                   Do an online incremental delta backup.
         -f <email address>   Email sender address. The email address
                              that will appear in "From:" field of
                              email notifications.
         -t <email address>   Email recipient address. The email address
                              to which the email notification will be sent.
         -k <days>            Keep delta backups for number of days.
         -l <days>            Keep archived transaction logs for number of days.

Arguments: Backup directories on this server where DB2 will put
           the backup images. If -b, -u and -d options are
           provided, the BU images will be transferred to
           the remote backup server.
```

Arguments: <backup directory1>, [backup directory2], ...

At least one backup directory must be given. The tool creates the following directory structure unser <backup directory>:

```
<backup directory> |- backup-work
                   |- latest
                   |- latest-delta
```

- `backup-work`: Work directory of the utility
- `latest`: Directory to which full offline/online backup images are copied
- `latest-delta`: Directory to which incremental online delta backups are copied

Common options

- `-s <server>`: Name of this server. The name of the directory to which the backup images will be will be copied on a remote storage server.
- `-o`: Do a full online backup. By default, a full offline backup will be created. NOTE: Archival logging is required for online backups.
- `-i`: Do an incremental online delta backup. NOTE: Archival logging is required for online backups.
- `-f <email address>`: Sender email address in email notifications send by the utility.
- `-t <email address>`: Email recipient of the email notifications send by the utility.
- `-k <days>`: If incremental online delta backups have been taken, retain the backup images locally for number of days. The default is 7 days.
- `-l <days>`: If online backups have been taken, retain the archived transaction logs for number of days. The default is 7 days.

Options related to copying backup images to a remote storage server

Before executing the utility with remote copy enabled, copy the SSH public key of the “db7sign” user to `.ssh/authorized_keys` file on the remote storage server.

- `-b <backup server address>`: Address of the remote storage server.
- `-u <user name>`: User name on the remote storage server.
- `-d <directory>`: Directory to which the backup images will be copied

14.3.3Examples

Offline backups

<u>Local full offline backup</u>

<u>Step 1: Switch to root user (or use sudo)</u>

<u>Step 2: Execute the backup command</u>

Full offline backup by using two backup directories, backup images are not transferred to a remote storage server:

```
# /opt/7signal/dbms/scripts/7BUtool.sh -s my-carat-server -f
my-carat-server@example.com -t admin@example.com /home/db7sign/dir1
/home/db7sign/dir2
```

<u>Full offline backup, backup images are transferred to a remote server</u>

<u>Step 1: Switch to root user (or use sudo)</u>

<u>Step 2: Execute the backup command</u>

Full offline backup by using two backup directories, backup images are transferred to a remote storage server:

```
# /opt/7signal/dbms/scripts/7BUtool.sh -s my-carat-server -f
my-carat-server@example.com -t admin@example.com -b remote-backup.example.com -u
backup -d /home/backup/my-carat-server /home/db7sign/dir1 /home/db7sign/dir2
```

The backup images will be copied to directory `/home/backup/my-carat-server/my-carat-server-offline/<date>` on the remote storage server `remote-backup.example.com`. The username on the remote server is “`backup`”.

Online backups

<u>Local full online backup</u>

<u>Step 1: Switch to “db7sign” user</u>

<u>Step 2: Execute the backup command</u>

Full online backup by using two backup directories, backup images are not transferred to a remote storage server:

```
$ /opt/7signal/dbms/scripts/7BUtool.sh -o -s my-carat-server -f
my-carat-server@example.com -t admin@example.com /home/db7sign/dir1
/home/db7sign/dir2
```

Full online backup, backup images are transferred to a remote server

Step 1: Switch to "db7sign" user

Step 2: Execute the backup command

Full online backup by using two backup directories, backup images are transferred to a remote storage server, keep 2 days of archived transaction logs locally:

```
$ /opt/7signal/dbms/scripts/7BUtool.sh -o -l 2 -s my-carat-server -f
my-carat-server@example.com -t admin@example.com -b remote-backup.example.com -u
backup -d /home/backup/my-carat-server /home/db7sign/dir1 /home/db7sign/dir2
```

The backup images will be copied to directory `/home/backup/my-carat-server/my-carat-server-online/<date>` on the remote storage server `remote-backup.example.com`. The username on the remote server is "`backup`".

Local incremental online delta backup

Step 1: Switch to "db7sign" user

Step 2: Execute the backup command

Incremental online delta backup by using two backup directories, backup images are not transferred to a remote storage server. Keep online delta backup images locally for 5 days:

```
$ /opt/7signal/dbms/scripts/7BUtool.sh -i -k 5 -s my-carat-server -f
my-carat-server@example.com -t admin@example.com /home/db7sign/dir1
/home/db7sign/dir2
```

Incremental online delta backup, backup images are transferred to a remote server

Step 1: Switch to "db7sign" user

Step 2: Execute the backup command

Incremental online delta backup by using two backup directories, backup images are transferred to a remote storage server, keep 2 days of archived transaction logs locally, keep online delta backups locally for 2 days:

```
$ /opt/7signal/dbms/scripts/7BUtool.sh -i -l 2 -k 2 -s my-carat-server -f
my-carat-server@example.com -t admin@example.com -b remote-backup.example.com -u
backup -d /home/backup/my-carat-server /home/db7sign/dir1 /home/db7sign/dir2
```

The backup images will be copied to directory `/home/backup/my-carat-server/my-carat-server-online-inc-delta/<date>` on the remote storage server `remote-backup.example.com`. The username on the remote server is "`backup`".

14.3.4Scheduling backups

Probably the easiest way to schedule backups is to use cron. For online backups, use crontab of “db7sign” user. For offline backups, use crontab of the root user.

Example backup schedule

Use “crontab -e” to edit the crontab of the “db7sign”user.

```
# Full online backup every Sunday at 3 am
0 3 * * 0     /opt/7signal/dbms/scripts/7BUtool.sh -o -s my-carat-server -f
my-carat-server@example.com -t admin@example.com -b remote-backup.example.com -u
backup -d /home/backup/my-carat-server /home/db7sign/dir1 /home/db7sign/dir2 >>
/var/log/BU.log 2>&1
# Incremental online delta backup every Monday to Saturday at 3 am
0 3 * * 1-6   /opt/7signal/dbms/scripts/7BUtool.sh -i -s my-carat-server -f
my-carat-server@example.com -t admin@example.com -b remote-backup.example.com -u
backup -d /home/backup/my-carat-server /home/db7sign/dir1 /home/db7sign/dir2 >>
/var/log/BU.log 2>&1
```

14.3.5Deleting old backups on the remote storage server

It can be necessary to delete old backups periodically on a remote storage server. The utility script `cleanupOldBackups.sh` can be found in directory `/`*`<DBMS install directory>`*`/scripts`.

Copy the script to the remote storage server. The should be executed as the backup user. In this example, the username is “backup”.

The command syntax is the following:

```
Usage: cleanupOldBackups.sh <backup directory> <OFFLINE> <ONLINE> <ONLINEINCDELTA>

    Where:
       OFFLINE          - Number of offline backups left to the backup directory
       ONLINE           - Number of online backups left to the backup directory
       ONLINEINCDELTA   - Number of online incremental delta backups left to the
                          backup directory
```

- <backup directory> is the same directory which is provided to 7BUtool.sh with -d option.
- OFFLINE defines how many full offline backups will be kept on the backup server.
- ONLINE defines how many full online backups will be kept on the backup server.
- ONLINEINCDELTA defines how many incremental online delta backups will be kept on the backup server.

Use for instance cron to execute the clean-up script periodically.

Example

Backup directory on the remote server is /home/backup/my-carat-server. Keep 2 full online and 2 full offline backups and 7 incremental online delta backups.

```
$ ./cleanupOldBackups.sh /home/backup/my-carat-server 2 2 7
```

14.4 Collecting statistics

Collecting statistics ("RUNSTATS") about the data in regular basis is important in order to keep database query optimizer up to date, and it makes possible for the optimizer to always select the best access path for the data. The `7Runstats.sh` tool, located in directory `/opt/7signal/dbms/scripts`, collects statistics on all measurement data tables.

14.4.1Executing statistics collection

Step 1: Switch to "db7sign" user

Step 2: Execute the utility.

```
$ /opt/7signal/dbms/scripts/7Runstats.sh
```

Example output:

```
Start time: Wed Aug 22 11:41:17 EEST 2018

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.5
 SQL authorization ID   = DB7SIGN
 Local database alias   = MEAS7

Doing RUNSTATS for carat7.AIR_UTILIZATION_CODECS
DB20000I  The RUNSTATS command completed successfully.
Doing RUNSTATS for carat7.AIR_UTILIZATION_TEST
DB20000I  The RUNSTATS command completed successfully.
Doing RUNSTATS for carat7.AP_ACCESS_TEST
...
End time: Wed Aug 22 12:30:11 EEST 2018
```

14.4.2Scheduling statistics collection

Statistics collection should be done regularly. Probably the easiest way to schedule reorganizations is to use cron.

Important: Use crontab of “db7sign” user.

Example statistics collection schedule

Use “crontab -e” to edit the crontab of the “db7sign”user.

```
# Collect statistics every Sunday at 6 am. Redirect output to /var/log/runstats.log
0 6 * * 0     /opt/7signal/dbms/scripts/7Runstats.sh >> /var/log/runstats.log 2>&1
```

14.5 Watching DB and log filesystem usage

`db2_watchdog.sh` script, found in directory `/opt/7signal/dbms/scripts` can be used to monitor DB and archive log filesystem disk usage.

If the disk usage exceeds configured usage percentage, the script will shut down the Sapphire applications and DB2, preventing possible database corruption caused by a full filesystem. `db2_watchdog.sh` must be run as root user.

The utility has the following options:

```
# /opt/7signal/dbms/scripts/db2_watchdog.sh -h
Usage db2_watchdog.sh [OPTIONS]

Options:
-d    DB file system, default is '/DB'
-c    DB file system usage threshold percents, default '95'
-t    Check usage of log file systems. By default, only DB file
      system usage is checked.
-p    Primary archive log file system, default is '/NFS-logs'
-a    Primary archive log usage threshold percents, default is '95'
-s    Secondary archive log file system, default is '/DB-logs'
-f    Secondary archive log usage threshold percents, default is '95'
-l    Log directory, default is '/tmp/7signal'
-h     Show this help
```

14.5.1Example configurations

Example 1:

- Databases on /opt/7signal/database
- Circular logging in use

Check DB filesystem usage, shutdown DB and application if filesystem usage exceeds 70%

```
/opt/7signal/dbms/scripts/db2_watchdog -c 70 -d /opt/7signal/database
```

Example 2:

- Databases on /opt/7signal/database
- Archival logging in use
  - Archive log directory on /DB-archive/logs
  - Failure log directory on /DB-failure/logs

Check DB and log filesystem usages, shutdown DB and application if filesystem usage exceeds 95%

```
/opt/7signal/dbms/scripts/db2_watchdog -t -d /opt/7signal/database -p /DB-archive/logs -s /DB-archive/logs
```

14.5.2Scheduling DB2 watchdog

db2_watchdog.sh should be run at least once in 10 minutes. Probably the easiest way to schedule checks is to use cron.

Important: Use crontab of “root” user.

Example schedule

Use “crontab -e” to edit the crontab of the “root” user. Add line

```
*/10 * * * * /opt/7signal/dbms/scripts/db2_watchdog -t -d /opt/7signal/database -p
/DB-archive/logs -s /DB-archive/logs -l /var/log
```

14.6All together

The following example schedules all important database maintenance tasks on cron:

```
# Full online backup every Sunday at 3 am
0 3 * * 0   /opt/7signal/dbms/scripts/7BUtool.sh -s my-carat -f
notification@my-carat.example.com -t reports@example.com -o /backups >> /var/log/backup.log 2>&1
```

```
# Incremental delta backups from Monday to Saturday
0 3 * * 1-6 /opt/7signal/dbms/scripts/7BUtool.sh -s my-carat -f my-carat@example.com -t
reports@example.com -i /backups >> /var/log/backup.log 2>&1
# Data purge every day at 12:30 am
30 0 * * *  /opt/7signal/dbms/scripts/7PurgeTool.sh 2>&1 >> /var/log/purge.log
# Statistics collection every Saturday at 10 am
0 10 * * 1 /opt/7signal/dbms/scripts/7Runstats.sh 2>&1 >> /var/log/runstats.log
# Reorganization every Sunday at 10 am
0 10 * * 0 /opt/7signal/dbms/scripts/7Reorg.sh 2>&1 >> /var/log/reorg.log
# DB2 watchdog every 10th minute
*/10 * * * * /opt/7signal/dbms/scripts/db2_watchdog -t -d /opt/7signal/database -p
/DB-archive/logs -s /DB-archive/logs -l /var/log
```

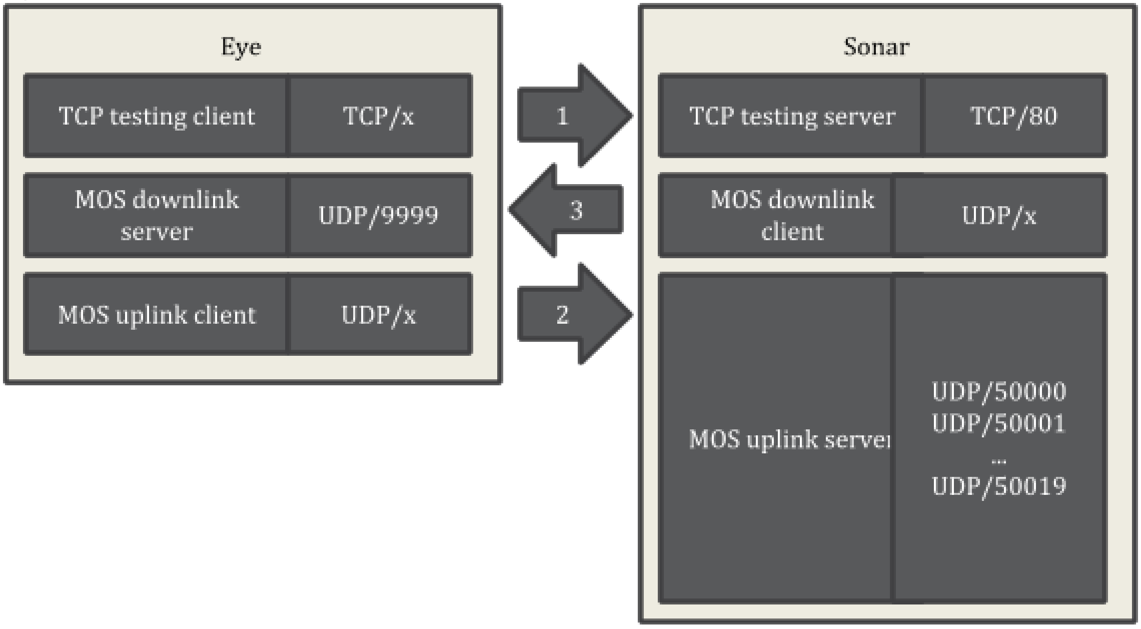
Appendix A.

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	Traffic is properly encapsulated HTTP. Uses Eye WLAN interface.
			Configurable during Sonar deployment	
2	MOS test, uplink direction	MOS test specific data	udp/50000 – 50019	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.
			Configurable during Sonar installer	
3	MOS test, downlink direction	MOS test specific data	udp/9999	Optional. Uses Eye WLAN interface.
			Configurable during Eye deployment	

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

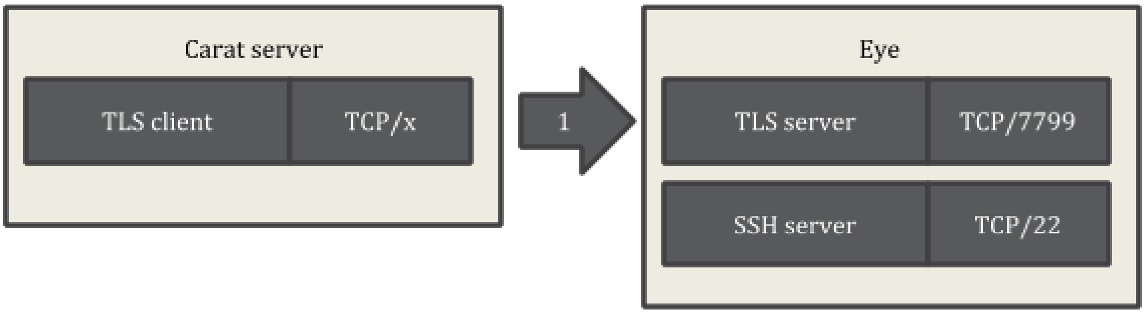
Network keys – pre-shared keys, certificates or similar - are stored in Eye file system by Carat application. To be observed: the target wireless network may be configured with MAC address restrictions so the MAC address of WLAN interface of the Eye unit must be white-listed as a network client. The 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.

Eye – Carat connection

Carat server connects to Eyes (”Enterprise setup”).

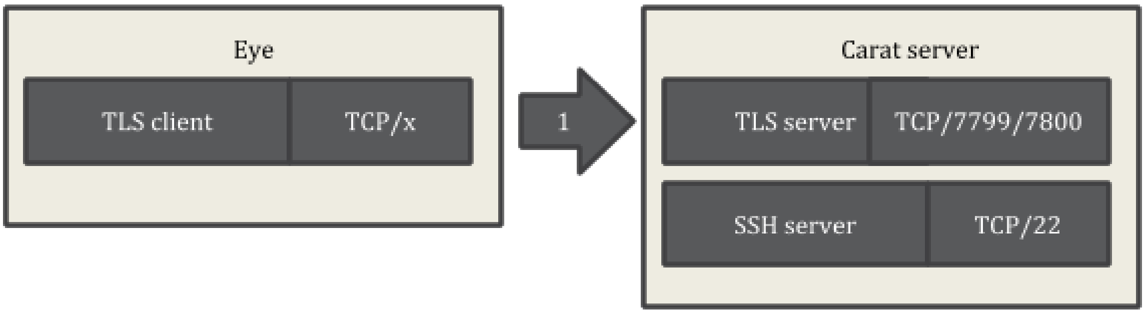


Conn ID	Description	Data content	Listening port(s)	Remarks
1	Eye server	TLS encrypted binary protocol for management and testing.	TCP/7799 Configurable in Eye deployment	Uses Eye Ethernet interface.

In this case the Eye acts as a server and Carat software is a client.

Carat – Eye connection

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

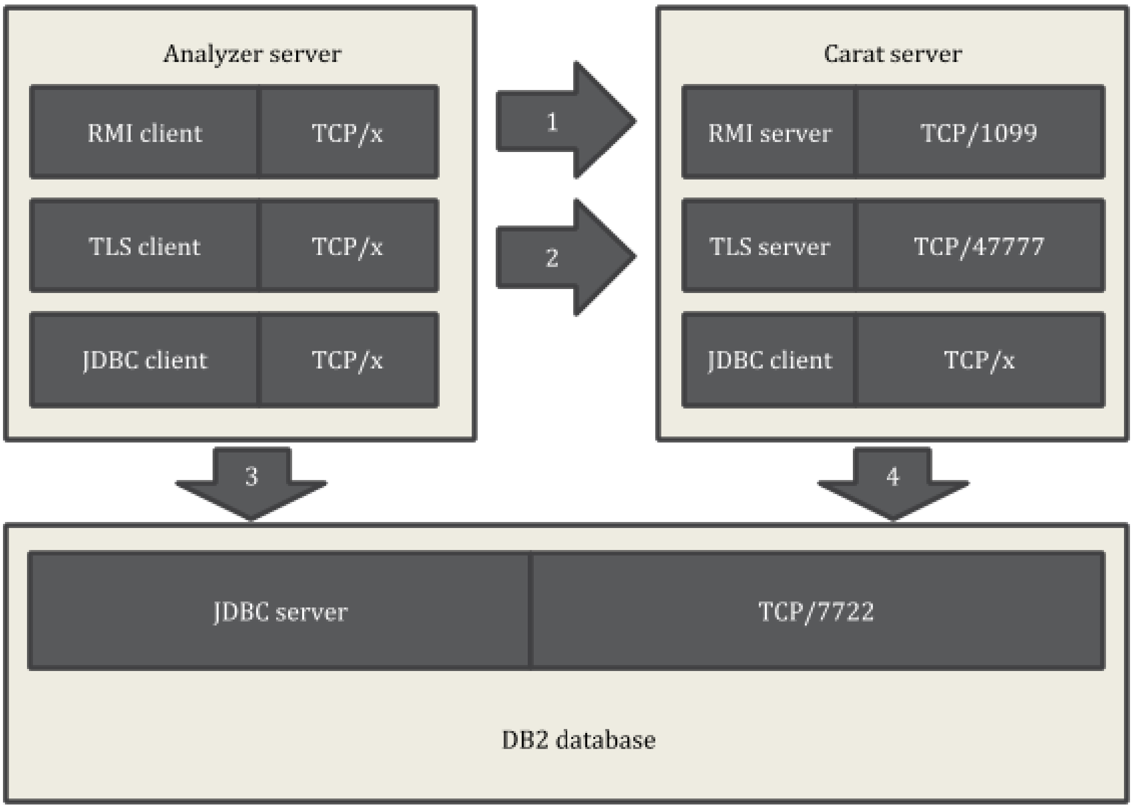


Conn ID	Description	Data content	Listening port(s)	Remarks
1	Carat server	TLS encrypted binary protocol for management and testing.	TCP/7799 TCP/7800 Configurable in Carat deployment	Uses Carat Ethernet interface.

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

Internal connections in Carat server

Note: as the following connections occur inside one host machine only, this part may be skipped regarding the firewall settings and other networking.

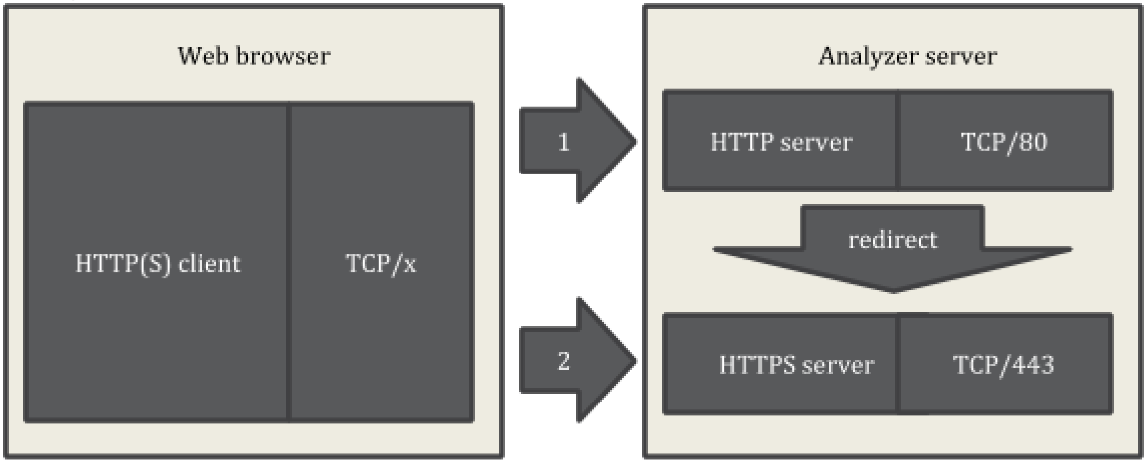

Analyzer server
RMI client
TCP/x
TLS client
TCP/x
JDBC client
TCP/x
1
2
Carat server
RMI server
TCP/1099
TLS server
TCP/47777
JDBC client
TCP/x
3
4
JDBC server
TCP/7722
DB2 database

Conn ID	Description	Data content	Listening port(s)	Remarks
1	RMI service.	RMI service protocol	TCP/1099 Typically not changed.	Discovery service for conn #2.
2	web-apps connecting as a client to a Carat server.	RMI calls	TCP/47777 Configurable during Application server deployment	
3	IBM DB2 database service for web apps.	JDBC traffic.	TCP/7722 Configurable during DBMS deployment	
4	IBM DB2 database service for Carat.	JDBC traffic.	TCP/7722	

			Configurable during DBMS deployment	

Analyzer is a web-application that visualizes the measurements and it has a dual-role in the sense of connectivity: Analyzer acts as a client to both the Carat server and DB2 and as a server to the browser clients. Currently, Carat, Analyzer and IBM DB2 applications are inseparable as they run in the same host in all supported setups.
7signal installers contain the installation medium for DB2 and the setup of DB2 is automated by 7signal DBMS installer. It is possible to change the defaults during installation time.

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	Redirects to HTTPS port of Application server.

			Configurable during Analyzer deployment.	
2	Standard HTTPS connection for measurement requests and responses.	Secure HTTP. Report and chart requests and responses.	TCP/443	Business connection for Application server.
			Configurable during Application server deployment.	

Appendix B.

BANDWIDTH REQUIREMENTS

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

14.6.1 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.

14.6.2 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.

14.6.3 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.

14.6.4 DB2 and Application server, DB2 and Carat server

In current implementation all three processes are running in the same host so there is no network burden whatsoever outside the host.

From	To	Medium	Traffic motivator	Volume estimate	Major factor
localhost	localhost	IP stack	Interoperable server processes.	N/A	The amount of Eyes in the network. Data is transferred in the core memory of the host.

APPENDIX C.

OFFLINE DATA PURGE

The utility used for offline data removal is “purge_old_data.sh” and it can be found on the Carat server in directory “/opt/7signal/dbms”. The suggested data purge method is online data purge, which is described in the chapter 14.1.

Step 1: Login to Carat server host as root

Step 2: Change to DBMS directory

For example:

```
# cd /opt/7signal/dbms
```

Step 3: Create work directory writable by database user

For example:

```
# su – db7sign
$ mkdir /home/db7sign/purge_work_dir
$ exit
```

Step 4: Check data removal options

Execute data removal tool without options:

```
# ./purge_old_data.sh
```

```
Usage: purge_old_data.sh <backup directory>
Options: -w <directory>   Use work directory <directory>
         -m <months>      Number of months left to DB (default 6)
         -s <months>      Number of months spectrum data left to DB (default 2)
         -r <months>      Number of months scan radio data left to DB (default 3)
```

Step 5: Execute data removal tool:

For example, if data older than one year should be removed from the measurement DB. Spectrum and Scan Radio data older than three months will be removed:

```
# ./purge_old_data.sh -m 12 -s 3 -r 3 –w /home/db7sign/purge_work_dir /mnt/backups
```

Wait until command finishes. Notice that with large databases, data removal may take several hours.