

7signal Sapphire Carat

User Guide

Release 5.0

PREFACE

Document scope

This document is aimed at people that shall manage and configure 7signal Sapphire quality tests on WLAN networks. The test pattern configuration and 7signal Sapphire system administration are explained in this document.

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

FCC Compliance

Human RF Exposure

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

Antennas

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 violation of FCC requirements which would void the user's authority to operate the equipment.

This device is restricted to indoor-only use in 5180.0 - 5250.0 MHz and 5470.0 - 5725.0 MHz bands.

- 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.

Industry Canada Compliance

- The Industry Canada ID for 7signal Sapphire Eye, Model 2001 (802.11a/b/g/n) is 11766A-INEY2001

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) operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall comply with the e.i.r.p. limit; and
- (iii) the maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

- (i) *les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;*
- (ii) *le gain maximal d'antenne permis pour les dispositifs utilisant les bandes 5 250-5 350 MHz et 5 470-5 725 MHz doit se conformer à la limite de p.i.r.e.;*
- (iii) *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.

Contact information

Contact us at 7signal

- by mail: 526 S. Main Street, Suite 601G, Akron, Ohio 44311, USA
- by email: info@7signal.com
- by phone: 855-763-9526 (855-QOE-WLAN)
- support: support@7signal.com

TABLE OF CONTENTS

1 7signal solution	1
1.1 System overview	1
2 Monitoring stations	3
2.1 Sapphire Eye.....	3
2.2 Soft Eye	4
2.3 Micro Eye	4
3 Sapphire Carat	5
4 Sonar	6
5 Sapphire Analyzer	7
6 Carat user Interface	8
6.1 Menus	8
6.1.1 Navigation.....	8
6.2 Network Topology.....	9
7 Starting the Carat configuration	11
7.1 How to create the minimum set of users	11
7.2 Automated Tests	12
7.3 Access Control	12
8 User Management	13
8.1 User Groups and object permissions.....	13
8.2 User Group hierarchy	13
8.3 User access levels	14
8.4 User Group and User management.....	14
8.5 User Groups	14
8.5.1 Related icons.....	14
8.5.2 User Group parameters	14
8.5.3 Adding User Groups	15
8.5.4 Editing User Groups	15
8.5.5 Removing User Groups	15
8.5.6 User Group status	16
8.6 Users	16

8.6.1 Related icons.....	16
Parameters	16
8.6.2 Adding Users (New)	17
8.6.3 Adding Users by copying.....	17
8.6.4 Editing User information.....	17
8.6.5 Removing Users	18
8.6.6 Changing password for Users.....	18
9 Network topology configuration.....	19
9.1 Choosing networks to be monitored.....	19
9.1.1 Organization.....	19
9.1.2 Adding Network Locations	20
9.1.3 Hidden Networks	21
9.1.4 Meru networks	22
9.1.5 Avoiding band selection/steering	25
9.1.6 Removing Networks.....	26
9.1.7 Channel configuration.....	26
10 Eye configuration	28
10.1 States of Monitoring Stations.....	28
10.1.1 Monitoring station LED statuses	28
10.2 Adding Monitoring Stations	28
10.2.1 Detecting and adding monitoring station	28
10.2.2 Adding monitoring station manually.....	30
10.2.3 Install monitoring station software.....	30
10.3 Monitoring station settings	32
10.4 Activating Monitoring Stations.....	33
10.5 Managing monitoring station IP configuration.....	33
10.5.1 Changing static IP configuration.....	35
10.5.2 Configuring DHCP for monitoring station.....	35
10.6 Managing Monitoring Station Software	36
10.6.1 Importing monitoring station software (Solution Administrator only)	36
10.6.2 Update monitoring station software (configurator/organization admin users)	37
10.6.3 Uninstalling and changing monitoring station software versions	39
10.7 Initial network scan	40
11 Encryption key management	42

11.1 Supported encryption types	43
11.2 Adding encryption keys (PSK)	43
11.2.1 Passphrase and pre-shared key	43
11.2.2 Adding WPA-PSK key	44
11.3 Certificate-based encryption	44
11.4 HTTP (captive portal) authentication	45
11.4.1 Prerequisites	45
11.4.2 Creating Open HTTP Key	46
11.5 Multiple network keys per Eye	47
11.5.1 Microsoft PKI Infrastructure	48
12 Test end-points	50
12.1 Sonar	50
12.2 Generic test counterparts	50
13 Access Point Information	52
13.1 Replacing access points	52
14 Links And Link Groups	54
14.1 Forming Links	54
14.2 Removing Links	54
14.3 Creating Link Groups	55
14.4 Removing Link Groups	55
14.5 Adding Link to Group	55
14.6 Removing Links from Group	55
15 Alarms	56
15.1 Network Alarms	56
15.1.1 Creating Alarm Groups	56
15.1.2 Binding Alarm Groups to access points	58
15.1.3 Viewing Network Alarms	59
15.1.4 Network Alarm forwarding	59
15.2 System Alarms	61
15.2.1 Viewing System Alarms	62
15.3 Acknowledge alarms	62
15.4 Purge old alarms	62
16 Traffic Classes	63

17 Automated test configuration	64
17.1 Test Profiles.....	64
17.2 Contents of a Test Profile	65
17.2.1 Passive	66
17.2.2 Warehouse.....	66
17.2.3 Office	66
17.2.4 Lightweight	66
17.2.5 VoIP.....	67
17.2.6 Hospital.....	67
17.2.7 Spectrum and Noise.....	67
17.2.8 Surveillance.....	67
17.2.9 TripleSSID.....	67
17.3 Testing multiple WLAN networks in one test profile.....	67
17.4 Test Profile execution modes	67
17.4.1 Test centric test profiles.....	68
17.4.2 Access point centric Test Profiles.....	69
17.5 Operations on templates.....	70
17.5.1 Duplicate.....	70
17.5.2 Copy as essid.....	71
17.6 Operation on Test Element	71
17.6.1 Copy element.....	71
17.6.2 Configure Ethernet test.....	71
17.7 Operations on Test Profile Node	71
17.8 Operations on Test Profile.....	72
17.9 Operations on essid inside a test profile	73
17.10 On test elements.....	73
17.10.1 Modifying test parameter and test name	73
17.10.2 Disabling and enabling test elements	74
17.10.3 Use case: Multiple SSID testing	74
17.11 Running Test Profiles.....	75
17.12 Automated tests and KPIs	76
18 Manual tests.....	78
18.1 Session events.....	78
18.2 Network scan test	79
18.3 Client scan test.....	80
18.3.1 Adding a new client.....	83

18.4 Spectrum Analyzer	83
18.5 Noise monitor test	84
18.6 Air utilization test	85
18.7 Optimal antenna selection test	87
18.8 Download tests	88
18.9 Upload tests	89
18.10 Ping test	91
18.11 Trace route test	92
18.12 Access point traffic test	93
18.13 MOS test	95
18.13.1 MOS test parameters	95
18.13.2 MOS test result	96
18.14 Web page download test	98
18.15 Internet Availability test	99
18.16 SIP Register test.....	100
18.17 Packet capture test	102
19 Service Level Agreement	104
19.1 Defining a Service Level Agreement into the system	104
19.2 Defining SLA Key Performance Indicators (KPI)	104
19.3 Creating an SLA group	105
19.3.1 Creating an SLA group from a template	105
19.3.2 Creating an SLA group from scratch	106
19.3.3 Setting default SLA group.....	106
19.4 SLA propagation	107
19.5 Binding SLA Groups	109
19.5.1 Binding an SLA group to a Link	109
19.5.2 Binding an SLA group to a link group	110
19.5.3 Binding an SLA Group to other Entities	110
20 Continuous and automated reporting.....	111
20.1 Subscription for a new report	111
20.2 Adding Report Items	112
20.2.1 Adding SLA compliance report item	113
20.2.2 Adding KPI report item.....	114
20.2.3 Adding SLA report item	114
20.2.4 Adding alarm report item	115

20.2.5 Adding map report item.....	115
20.2.6 Report item general options	115
21 Import	122
21.1 Importing access point names.....	122
21.1.1 Example access point name import	123
21.2 Importing access point names (“last digit zero” mode).....	124
21.2.1 Overview	124
21.2.2 Running import	124
21.3 Import and replace APs	125
22 Exports	127
22.1 Configuring Carat system logging properties	127
22.2 Configuring system logger daemon.....	127
22.3 Exporting test results to system log	128
22.4 Exporting alarms results to system log.....	129
23 Change events	130
23.1 Reporting change events.....	131
23.2 Viewing change events.....	132
23.3 Removing change events.....	132
24 Viewer Software	134
25 Email Servers	135
26 Database maintenance.....	136
26.1 Measurement data purge	136
26.2 Database backup	137
26.2.1 Backup options	137
26.2.2 Database logging.....	138
26.2.3 Backup method options	139
26.2.4 Restoring backups.....	142
26.3 Management database integrity check	143
26.4 Reorganizing measurement database	144
27 Nagios Support	145
27.1 Adding Sapphire host information to Nagios server.....	145
27.2 Adding Nagios Plug-ins To Sapphire Software.....	146

27.2.1 Install NRPE daemon.....	146
27.2.2 Install toolset 'Nagios plugins'	146
27.3 Verifying Nagios Installation.....	146
27.4 Removing Nagios plugins	146

1 7SIGNAL 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 management tool called the Sapphire Carat. The measurement results are reported via a reporting application called the Sapphire Analyzer.

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 mass 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 to 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 help locate a 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 the commonly measured parameters.

1.1 System overview

The 7signal Sapphire Quality Monitoring Solution consists of Sapphire Eye monitoring sensors, Sonar test servers, the Sapphire Carat management software, and Sapphire Analyzer for viewing and reporting on results.

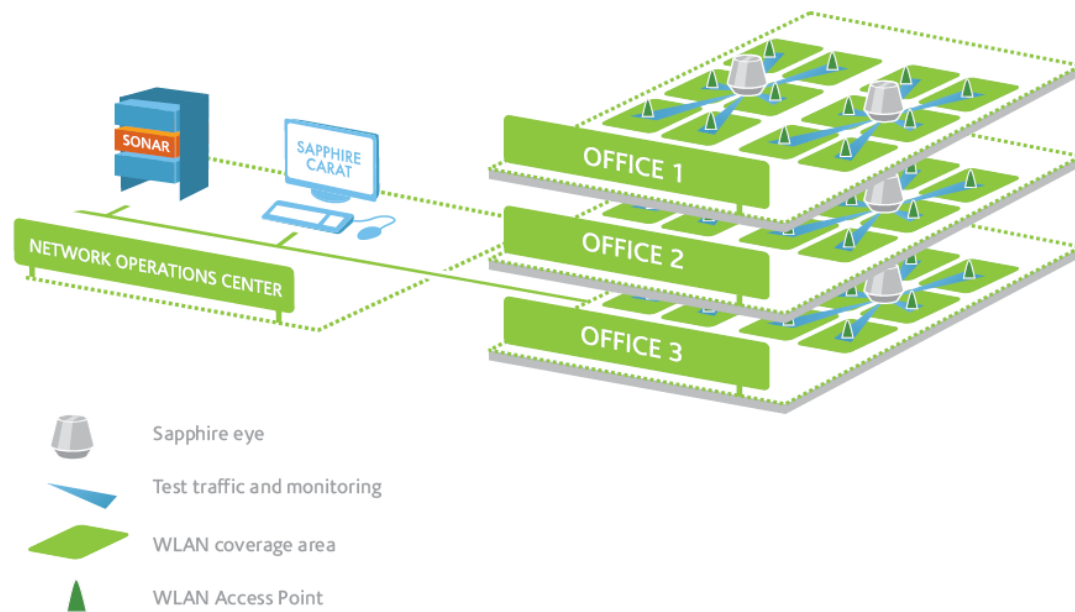


Figure 1: 7signal Sapphire installation

The system components are described in chapters 2–6. The remaining chapters describe the management software. The result viewing and reporting tool (Analyzer) is described in its own user guide.

2 MONITORING STATIONS

2.1 Sapphire Eye

Sapphire Eye is a monitoring station for WLAN environments. Unlike a common access point or client, the Eye monitoring station uses advanced broadband antenna technology, which creates an exceptionally large coverage area. Consequently, one Eye can monitor several access points, or WLAN cells. The typical number of monitored cells is 5–8.

There are two monitoring station variants: the Standard Eye and the Indoor Eye. The Standard Eye is protected against dust and water (conformant to IP55 or IP65 specifications, depending on the model), so it can be installed outdoors and in challenging environments.

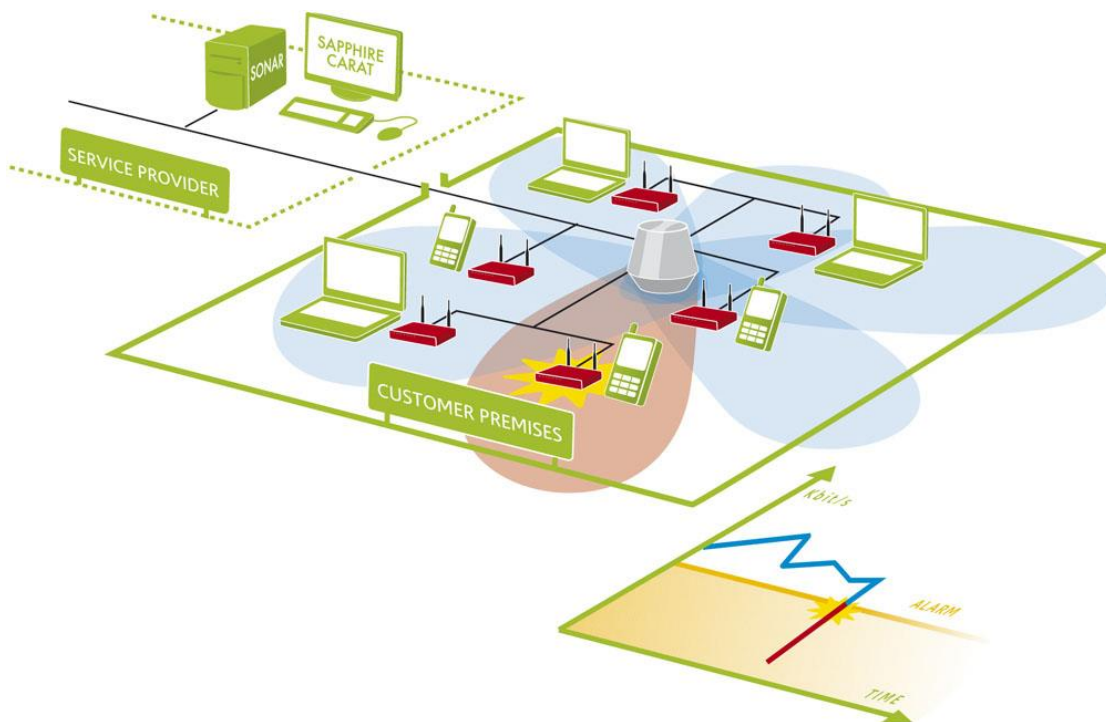


Figure 2: Monitoring station on customer's premises

In the picture above:

- The monitoring station (Eye) is the grey cone-like object in the center;
- the Carat management interface is on the service provider's premises (top left corner);
- the customer's premises have a wireless network with six access points (center part of the picture, access points in red);
- there is one monitoring station on the customer's premises (the colored lobes depict the station's directional antennas and their range);
- a problem has occurred in an access point in the red lobe;
- the problem can be seen in the monitoring interface or in a report as a falling performance indicator value (lower right corner).

In Sapphire, the management tool Carat and monitoring station Eye work as a client and server, with Eye being the server for Carat. The traffic between the client and server is strongly encrypted and uses 7signal's proprietary management protocol. This makes it possible to manage the monitoring stations from geographically distant locations and over insecure networks.

A monitoring station conducts both passive and active measurements in a WLAN environment. The passive measurements consist of listening to data traffic that uses the IEEE 802.11 protocol and of general analysis of the radio frequency spectrum in the coverage area. Passive measurements have no effect on the functionality or utilization rate of the target network, or the effect is very small (probe request transmissions). During active measurements, Sapphire Eye contacts each monitored access point in turn and uses the network services via the WLAN; i.e., it acts as a client in the network. Using both active and passive measurements, the 7signal solution can monitor the experienced network performance along the entire length of the service chain and locate problems in both WLAN and LAN environments.

The monitoring station is also able to execute active measurements over its Ethernet interface. Results of Ethernet tests can be distinguished from WLAN test results by applying Ethernet specific Area Aggregations in Sapphire Analyzer tool.

2.2 Soft Eye

The monitoring station software can be installed to a laptop PC running Linux distributions supported by 7signal. The laptop must be equipped with a suitable WLAN card. Supported WLAN cards are listed in the Release Notes document. Soft Eye supports smaller set of measurements than Sapphire Eye.

2.3 Micro Eye

Micro Eye is a Raspberry PI (rev B) computer board, equipped with suitable WLAN network interface card (supported WLAN cards are listed in Release Notes document). Micro Eye is shipped with pre-installed SDHC memory card, which contains operating system and Sapphire Eye software.

Micro Eye supports smaller set of measurements than Sapphire Eye, and it is not suitable for measuring e.g. maximum throughputs.

3 SAPPHIRE CARAT

With the Sapphire Carat management tool, you can manage the Sapphire Eye and Micro Eye monitoring stations, run interactive and real-time measurements, configure and manage automatic measurements, and generate reports of the measurement results. The reports shows measurement results in tables and charts.

Sapphire Carat stores the profiles used in the automatic testing of the monitored network, and the network's access rights information. Sapphire Carat can be used interactively to test various areas of the network, or it can be left running in the background for continuous collection of test results.

Key features:

- Status information on the radio network's availability and usability;
- Availability of a production service;
- Overview of data traffic from the client to the production server;
- Packet-level load measurement and traffic analysis in a radio network ;
- Tests at application level;
- Properties, signal levels, and noise levels of the radio frequency environment;
- Statistical analyses, averages, deviations, and distributions;
- Monitoring of data security settings;
- Location of interference;
- Alarms.

4 SONAR

The role of the Sonar test server in 7signal Sapphire is to emulate one of the customer's production servers. Sapphire Eye or Micro Eye connects to Sonar to measure QoS provided by the network. Measurements are performed in both directions (uplink and downlink). Uplink means traffic from end-user device (e.g. Eye) towards network (e.g. Sonar). Downlink means traffic from network towards the end-user device.

Single Sonar can serve several monitoring stations which has access through IP networks to Sonar. One Sonar server can therefore be used as the test point for several networks.

The 7signal Sapphire solution supports the concurrent use of several Sonar test servers, which means that Sonar can be installed on several servers within a company. Using several Sonars enables the company to detect and locate problems in its network. Sonar can be located in the same network as the access points, in a server room in the same building, or anywhere on the Internet – such as in the centralized identification and authorization center of an international organization.

5 SAPPHIRE ANALYZER

Sapphire Analyzer is the performance and QoS analysis tool in the 7signal solution. Analyzer cannot be used to control Sapphire's functions and measurements themselves.

Analyzer makes the network's key performance indicators (KPIs) available at a glance, or in more detailed form for a given time period. Starting from release 5.0, Analyzer also provides new features called "Automatic Analysis" and "Automatic Optimization".

Analyzer is browser-based, so authorized persons can use any of the most common browsers to view the results as long as they have an Internet connection. The result summaries can be saved as plain text to comma separated value files (CSV files), or as PDF files, preserving the formatting. The plain-text material can be used in many ways, including import into a spreadsheet.

There is a separate user document for the Sapphire Analyzer.

6 CARAT USER INTERFACE

The Carat user interface (GUI) is a stand-alone java client. The purpose of the Carat user interface is to configure and manage the Sapphire solution. Several users can access and configure single Carat simultaneously.

6.1 Menus

6.1.1 Navigation

The menu contents are dynamic based on context, user access rights and the current license.

Table 1: Management GUI menus

Menu	Description	Submenus/actions
File	Log in / log out, lock the session, and close the application.	<ul style="list-style-type: none"> • Lock session • Log in • Log off • Exit
Edit	Enter settings for applications used for viewing the exported result files and packet capture files. Specify the server for outgoing mail.	<ul style="list-style-type: none"> • Configure tools • SMTP server
View	View network topology, alarms and change events.	<ul style="list-style-type: none"> • Network topology • Network alarms • System alarms • View change events
Manage	Manage Sapphire's general settings: <ul style="list-style-type: none"> - alarms - user management - access keys to radio networks - test end point settings - administration of target network client information - settings for automatic reporting - remote management of monitoring station software - database maintenance 	<ul style="list-style-type: none"> • Alarm configuration • Users and groups • Access Control • Network Keys • Test end points • Alarms <ul style="list-style-type: none"> ○ Email ○ SNMP • Network clients • SLA Definitions • Automated report configuration • Eye software management <ul style="list-style-type: none"> ○ SW repository management ○ Eye software update ○ Eye software management • Change password • Test Profiles




		<ul style="list-style-type: none"> • Database maintenance
Tools	Start and stop the automatic test profile, import data from external source to Carat. Export test results and alarms in XML format to Carat server system log.	<ul style="list-style-type: none"> • Start automated testing • Stop automated testing • Automated tests management • Import... • Export...
Window	Refresh the main window of the user interface.	<ul style="list-style-type: none"> • Refresh
Help	Read user documentation and general information about the system installation.	<ul style="list-style-type: none"> • Release notes • Carat User guide • Analyzer User guide • About






6.2 Network Topology

The Network topology is a hierarchical tree displaying hierarchy from the Organization to Eyes and Access Points. The user can select from multiple ways to access the network: either via monitoring stations or via the network's service areas. Both methods support network testing, but monitoring stations can only be managed by using their respective icons.

The network hierarchy is displayed as a tree, with an icon representing each item at each node. If the item has functionality, you can bring it into view by right-clicking the icon.

Table 2: Network topology components

Topology Node	Icon	Description	Submenus
Organization		In the Organization menu, you can add organizations, locations and service areas to the organization that is being created.	<ul style="list-style-type: none"> • Edit • Wireless networks • Add location • Add organization • Remove organization • Bind SLA
Location		From the Location menu, you can set the network's physical location (e.g., country, city, or building). A location is always attached to a higher-level location or organization.	<ul style="list-style-type: none"> • Edit • Add Location • Add service area • Remove • Add Link Group • Bind SLA
Service area		A service area is a location where you can install a monitoring station. A service area is determined by the coverage area of the monitoring station, not by the coverage area of the target network. A service area can have a map on which the access	<ul style="list-style-type: none"> • Edit • Add Eye • Bind wireless networks • Remove • Allowed channels • Bind SLA • Bind Alarms • Bind to Test Profile • Unbind from Test Profile • Map

		points and Eyes can be placed.	
Eye		A Sapphire Eye or Micro Eye monitoring station always belongs to a service area. In this menu, you can perform Eye level tests, bind and unbind test profile to/from the Eye, report change events for this Eye and modify Eye connectivity properties (change IP configuration, SSH password etc.)	<ul style="list-style-type: none"> • Edit • Remove • (De)Activate • Network key bindings • Change events • Network scan • Client scan • Spectrum analysis • Noise Monitor • Packet capture • Air Utilization test • Manual tests • Bind to test profile • Unbind from test profile • Automated test status • Bind SLA • Connection management
Wireless network		This menu describes the target network, which can be located in one or more service areas. A service area can contain several target networks. This menu is used to configure the encryption method used in the network, configure allowed channels of the network, and report change events for the network.	<ul style="list-style-type: none"> • Add key • Edit • Unbind wireless network • Allowed channels • Bind SLA • Change events • Change events on this Service Area
Access Point		In this menu, you can perform tests, set alarm groups for an access point, report change events for the access point, and deactivate and activate the access point (meaning that the access point is monitored or not).	<ul style="list-style-type: none"> • Properties • Manual tests • Bind to Alarm group • Unbind from Alarm group • Bind SLA • Remove access point • Allowed Channels • Change Relation to Eye • Change events • Change events on this Eye • (De)Activate
Link		In this menu, you can bind an SLA group for the link.	<ul style="list-style-type: none"> • Edit • Remove link • Bind SLA • Change events
Link group		In this menu, you can bind an SLA group for the link group.	<ul style="list-style-type: none"> • Edit • Bind SLA • Remove

7 STARTING THE CARAT CONFIGURATION

The access rights and user management heavily relies a group-based model. The group is the starting point: every user belongs to one of the groups and the group determines the access rights of any given user. The technical details and management instructions are in the next section.

Any objects in the system – Eyes, Sonars, topology elements such as Organizations and Locations – belong to some administrative group. Objects that do not belong to a certain group are also invisible to the group. This isolation is very low-level in 7signal Sapphire in order to enable safe and secure operations in large setups with numerous and heterogeneous organizations. 7signal Sapphire supports multiple organizations that are under completely different administration and must remain unaware of each other.

NOTE: To fully utilize this feature it is strongly advised that a role called **Solution Administrator** (see the next section on user and group management) is **used only to create other Administrators** (Organization Administrators).

The recommended minimum setup for an operational 7signal Sapphire is to have default admin user for general handling of users and groups and admins of one or more organizations. Any organization needs two users: one for administration and one for configuration network tests etc.

7.1 How to create the minimum set of users

The system default user is the ‘Solution Administrator’ belonging to Solution Administrator Group. *Default user name of ‘Solution Administrator’ is ‘admin’, and the password is ‘admin’.* This requires no other action than the initial login and changing the default password to a non-default password.

As ‘Solution Administrator’

1. Choose ‘Manage | Users and Groups’ for user account management from the top-menu.
2. Create a new group for the administrators of the organization.
Use a descriptive name, f ex *NewAdminGroupForOrganizationX*
3. Create a new admin user for the organization.
Use a descriptive name, f ex *LocalAdministrator1*.
4. Logout

As ‘LocalAdministrator1’ created in the previous step

1. Choose ‘Manage | Users and Groups’ for user account management from the top-menu.
2. Create a new group for the configurators of the organization under previously created administrator group.

- Use a descriptive name, f ex *NewConfigGroupForOrganizationX*
3. Create a new configurator user to the Configurator group.
Use a descriptive name, f ex *LocalConfigurator1*.
 4. Continue using Sapphire.

All other configurations related to network topology, test profiles, WLAN network keys etc. should be made by the user *LocalConfigurator1* to enable proper operation of the automated object access rights management system.

Some top-level operations for *Solution Administrator* are explained right below

7.2 Automated Tests

Top-menu selection “Tools | Start automated testing” affects only those objects that are accessible to the user issuing the command. Stopping works similarly.

Solution Administrator level user starts and stops testing system-wide i.e. all the monitoring stations. Local Administrator may affect the monitoring stations only inside their own administrative boundary i.e. only part of the monitoring stations start/stop. However it is advised to use Configurator level users to manage automated testing.

7.3 Access Control

The “Access control” is an accessible pane in the “Manage” menu. When one follows the intended way of user and group definition, the contents and actions in the “Access control” pane are redundant. The feature remains activated but the use of it is discouraged and thus not instructed in detail.

For sandbox testing and non-warranted try-outs: the left panel contains actual users and groups and related access rights. The right panel contains all objects in 7signal Sapphire. With combinations of right-clicks and drags&drops fine-level adjustment and changes to access rights are possible.

8 USER MANAGEMENT

User management in 7signal Sapphire is based on user groups. A user's access rights in the system derive from the user group that the user belongs to. A user may belong to one or more user groups.

In addition to normal user management the Sapphire system supports user group specific view virtualization. The system can be configured so that different user groups have access to different objects that have been created into the system. For instance, one user group may have access to all objects and two subgroups of that group may only have access to a portion of all objects. It is also not necessary for the subgroups to have access to any of the same objects.

User management is also restricted in the same manner as object management. An administrator user only has access to the users created to subgroups in addition to any users belonging to the same administrator group he/she belongs to.

Users belonging to the Sapphire admin group have access to the entire system.

8.1 User Groups and object permissions

Almost every object created in the Sapphire system includes an access control list (ACL). An object's ACL is mainly determined by the user group of the user that creates the object in question.

Note that objects are also created through automatic testing. For example access points, wireless clients and alarms created this way. Objects created as a result of automatic testing inherit their ACL from the Eye that conducted the test.

The Sapphire system also includes the functionality to transfer access rights of objects from one user group to another.

8.2 User Group hierarchy

The Sapphire system supports two types of user groups: normal user groups and referencing user groups.




A normal user group can be created either as a new root group or as a subgroup to an already existing user group. When new groups are created as subgroups under an existing user group, the existing group inherits access rights to all objects that its subgroups have access rights to. This inheritance rule applies to the whole user group hierarchy meaning that the root user group in a hierarchy gets access rights recursively from all subgroups. Access rights of referencing user groups are not inherited in this way.

A referencing user group can be created for any group except the Solution Administrator group. A referencing user group always has the same access rights as the user group it references. The only difference is that a referencing user group cannot be granted the same access level as the group it references. A common use for a referencing user group is to have it reference for example an organization's configuration group. This way the referencing group's users can view the configuration group's objects, but cannot configure the system.

8.3 User access levels

The Sapphire system supports three elementary access levels for user groups: Reporter, Configurator and Administrator. Access rights are inherited from lower to higher levels: Reporter users only have their own level's access rights, Configurator users have reporter level rights plus additional rights granted by their configurator level, and Administrator users have all rights.

There are four levels of access rights:

- **Solution Administrator** – system-wide super-user that may be the only user in small set-ups and should be used only for other administrator definitions in large-scale environments
- **Administrator** – full access and management rights 
- **Configurator** – full access rights, no user management rights 
- **Reporter** – access rights to alarms and reports 

8.4 User Group and User management

The Sapphire Carat user management dialog can be accessed from the main menu by selecting "Manage | Users and groups". Only administrator level users can access user group and user management in the Sapphire system.

When the user management dialog is opened, a tree view showing the users and user groups currently existing in the system opens to the left of the dialog.

8.5 User Groups

8.5.1 Related icons

Reporter group



active group



referencing group



inactive group

Configurator group



active group



referencing group



inactive group

Administrator group



active group



referencing group



inactive group

8.5.2 User Group parameters

- **Name** - The name of the user group
- **Description** - A description of the group
- **Service Role** - Defines access rights for the group's users in the Sapphire system
- **Type** - The group type (normal/referencing)
- **Status** - The group status (active/inactive)

8.5.3 Adding User Groups

A new user group can be added into the system in three different ways:

1. As a new root group under which to start creating a new user group hierarchy.
2. As a subgroup to an already existing user group.
3. As a symbolic (referencing) group for an already existing group.

Adding a group can be done by right-clicking on either the "Groups and users" node in case n:o 1 or an existing user group in cases 2 and 3 and selecting "Add instance group" in case n:o 1 and n:o2 or "Add symbolic group" in cases n:o 3 from the pop-up menu.

Steps to create a new group:

1. From the top menu bar select "Manage | Users and Groups" to open a pane on left
2. Right-click the root object named "Users and Groups" or an existing group to get a submenu
3. Select "Add group" to open a pane on right
4. Enter the relevant group information
 - a. user name: login name for the user
 - b. (optional) Description: free-text field for the group description
 - c. Role: group access right level. The field is dynamic; the super-group dictates the default level and available range of valid access level.
 - d. Status: Active or inactive. Only users in an active group may login.
5. Save the group by clicking "Save"

8.5.4 Editing User Groups

The user group editing dialog can be accessed by right-clicking the desired user group and selecting "Edit" from the pop-up menu.

An example of editing a user group:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Select the desired user group for editing by right-clicking on it and choosing "Edit" from the pop-up menu
4. Make the desired changes to the user group's settings
5. Save the changes by clicking on the "Save" button

8.5.5 Removing User Groups

A user group can be removed by selecting the group to be removed by right-clicking on it and selecting "Remove Group" from the pop-up menu. The following criteria must be satisfied before a user group can be removed:

1. The group must be empty of users
2. The group must not have any subgroups
3. The group must not own any objects

An example of removing a user group:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Right-click on a group that satisfies the removal criteria and select "Remove" from the pop-up menu

8.5.6 User Group status

In certain situations it may be desired to inactivate some user group. An inactive user group has no access rights in the system. A user group can be inactivated by right-clicking on the desired group and selecting "Inactivate" from the pop-up menu. An inactive group can be re-activated by right-clicking on the group and selecting "Activate" from the pop-up menu.

An example of changing a group's status:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar

Right-click on the desired group and select "Inactivate" from the pop-up menu

8.6 Users

8.6.1 Related icons

Administrator user



Configurator user



Reporter user



Parameters

- User name - User name
- Alias - An alias for the user name, for example the user's real name
- Email Address - User's email address
- Phone - User's phone number
- Organization - The Organization that the user belongs to. Useful for example when a service provider wants to give access rights to clients it manages.
- Status - User's status
- Password/Confirm password: Password/Confirm password

When creating a new user the user name, status and password fields are required, the rest of the parameters are optional.

8.6.2 Adding Users (New)

A new user can be added by right-clicking on the user group that the user is to be added into and selecting "Add user" from the pop-up menu.

Steps to create a new user:

1. From the top menu bar select "Manage | Users and Groups" to open a pane on left
2. Right-click the relevant group to get a submenu
3. Select "Add user" to open a pane on right
4. Enter the relevant user information
 - a. Username: login name for the user
 - b. (optional) Alias: alternative name for the user
 - c. (optional) Email address: contact information for the user
 - d. (optional) Organization: user's organization
 - e. Status: Active or inactive. Only active users may login.
 - f. Password and confirmation: login password
5. Save the user by clicking "Save"

8.6.3 Adding Users by copying

An existing user can be copied to several groups. This enables one single account to be used on numerous organizations while preserving the strict access policy.

Steps to copy a user:

1. Create one more group
2. Select a user from a previously existing group and right-click for the menu
3. Select "Copy user"
4. Select the icon of the new group and right-click for the menu
5. Select "Paste user"

The copied account may now access numerous groups. The login of a user belonging to several groups starts in the typical manner. After successful login a pop-up is shown in order to make selection of the group used for the login. The possible other groups are invisible after the chosen group (context) has been chosen.

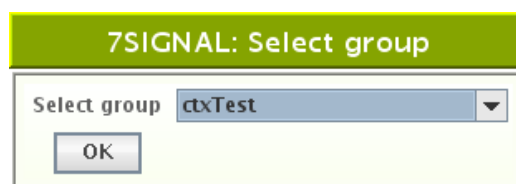


Figure 3: User group selection dialog

8.6.4 Editing User information

A user's information can be edited by right-clicking on the desired user and choosing "Edit" from the pop-up menu. User name and password cannot be changed from here.

An example of editing a user's information:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Right-click on the desired user and pick "Edit" from the pop-up menu
4. Change the desired parameters
5. Save changes by clicking "Save"

8.6.5 Removing Users

A user can be removed by right-clicking on him/her and selecting "Remove" from the pop-up menu.

An example of removing a user:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Right-click on the desired user and pick "Remove" from the pop-up menu

User's status

If for some reason it is desired to deny a certain user from accessing the system, that user can be inactivated by right-clicking on the user and selecting "Inactivate" from the pop-up menu. An inactivated user may be re-activated by right-clicking on him/her and selecting "Activate" from the pop-up menu.

An example of changing a user's status:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Right-click on the desired user and select "Passivate" or "Activate" from the pop-up menu

8.6.6 Changing password for Users

A user's password can be changed by right-clicking on the user and selecting "Change Password" from the pop-up menu. This will open a new dialog into which the user's new password can be entered.

An example of changing a user's password:

1. Log in as an administrator group user
2. Open the user group and user management dialog by clicking "Manage | Users and Groups" from the top menu bar
3. Right-click on the desired user and select "Change Password" from the pop-up menu
4. Input new password
5. Save new password by clicking the "Save" button

9 NETWORK TOPOLOGY CONFIGURATION

Network topology is defined in Carat to reflect geography and organization and help with reporting necessary entities separately. Network topology consists of organizations, locations, service areas, Eyes and managed access points.

9.1 Choosing networks to be monitored

9.1.1 Organization

Sapphire can simultaneously manage networks in several independent organizations. A company or other organization can have many separate locations. The networks are displayed in a hierarchical tree starting from the Organization.

A company can have several networks, for different purposes. For example:

- Office network
- Warehouse network
- Guest network

To meet this need, Sapphire can monitor several networks at the same time.

To handle a hierarchy that might grow utterly complex, 7signal uses a tree-structure. Organization is a starting point to create tree structure. User can add one or more organizations depending what is an appropriate structure.

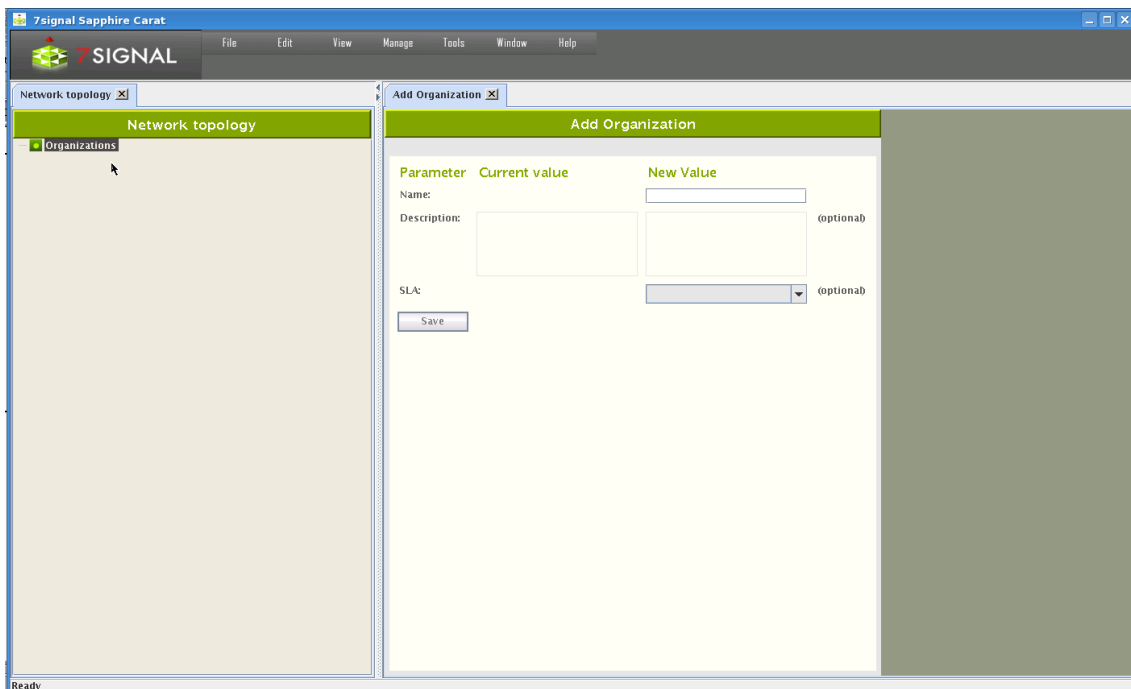


Figure 4: Adding new organization

1. Right click Organizations node in tree and select “Add Organization”
2. Enter the organization’s name
3. Save by clicking “Save”

9.1.2 Adding Network Locations

Location is used to define the network's location in a precise or descriptive way. A location might be a city, a part of the city, a building, or a single floor in a building, depending on the coverage area of the organization's network. A small organization might have only a single location, an office. On the other hand, a large organization might have several locations, in different cities, or a single overall location, such as "Europe," under which countries and cities etc. are defined.

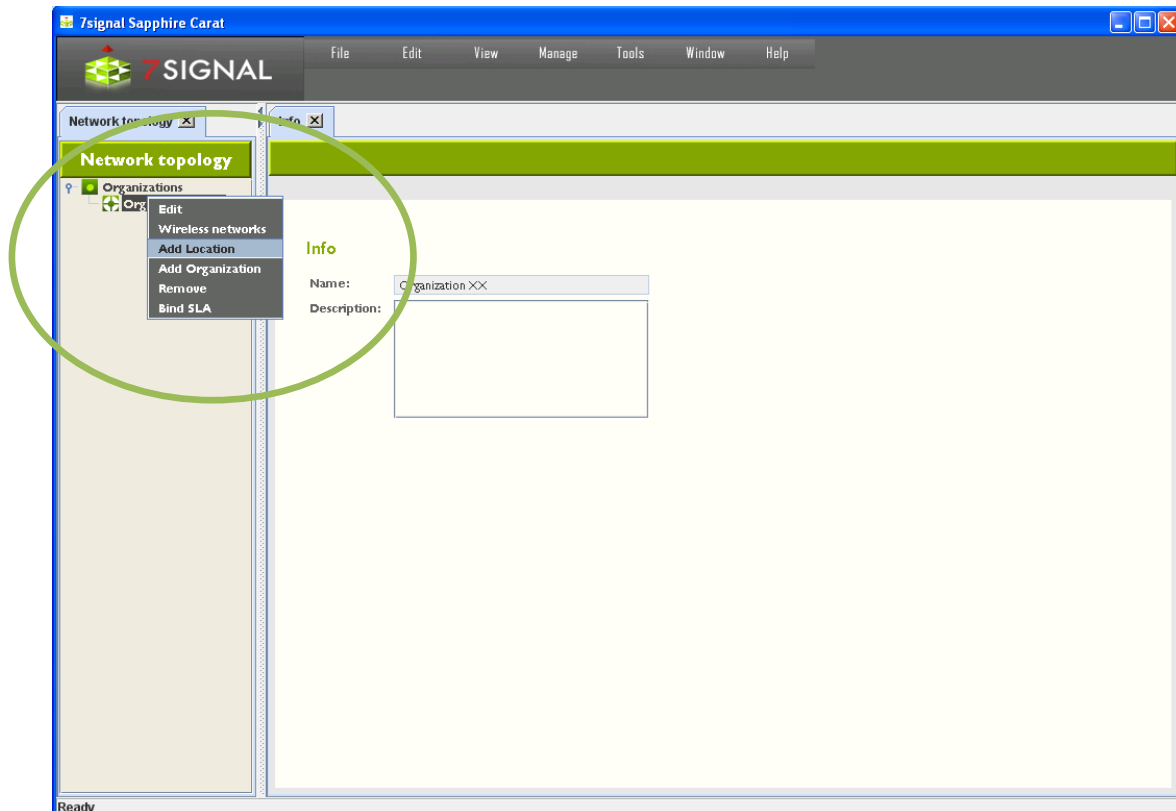


Figure 5: Adding new location

1. From the top menu bar, select "View | Network topology"
2. Right-click the organization
3. Select "Add location"
4. Enter the location's name
5. Select the location type from the pull-down menu
6. Enter an optional description for the location
7. Click "Save"

You can add as many locations as needed to describe the organization's structure.

After you have added a location, you can add a service area.

1. Right-click a location
2. Select "Add service area"
3. Enter a name for the service area
4. Enter an optional description for the service area
5. Click "Save"

9.1.3 Hidden Networks

7signal Sapphire considers a hidden network to be a property of certain Organization. The network scans are based on listening and actively requesting beacon information on the Service Areas. The hidden networks shall not actively transmit beacons nor respond to requests with partial information only. Due to this the various scans - including the initial scan - in 7signal Sapphire do not capture hidden networks. Tests related to traffic analysis shall contain also information on hidden networks but the capture is not used as a technique in scans.

NOTE: Hiding the network SSID should not be used as a security as it does not limit sending the beacons or SSID names in payload frames but leaves only network SSID field blank in beacon signal. Any attacker or publicly available analysis tool can find hidden network as soon as there are any payload packets in the network. Even popular operating systems may present hidden network after a certain period of time. If SSID name is not transmitted, client devices are forced to start probing their access points continuously. This increase significantly radio interface traffic overhead and lowers overall network performance.

In order to add a hidden network to 7signal Sapphire:

1. Locate the Organization with a hidden network from the Topology tree
2. Right-click menu on the Organization and select "Wireless networks"
3. Enter the relevant data on the hidden network on the pane that opened on the right
 - a. Name type (optional): currently only text strings are supported SSIDs
 - b. Name: the name of the network - not friendly name but SSID
 - c. Description (optional): description on the hidden network
 - d. Contact person (optional): the administrator for the hidden network
 - e. Key: the name of the WLAN network access key that has been stored earlier to the system
4. Select "Save" to store the data to the system
5. Locate the Service Area on which the hidden network will be monitored
6. Right-click menu on the Service Area and select "Bind Wireless Networks"
7. Choose the hidden network from the list

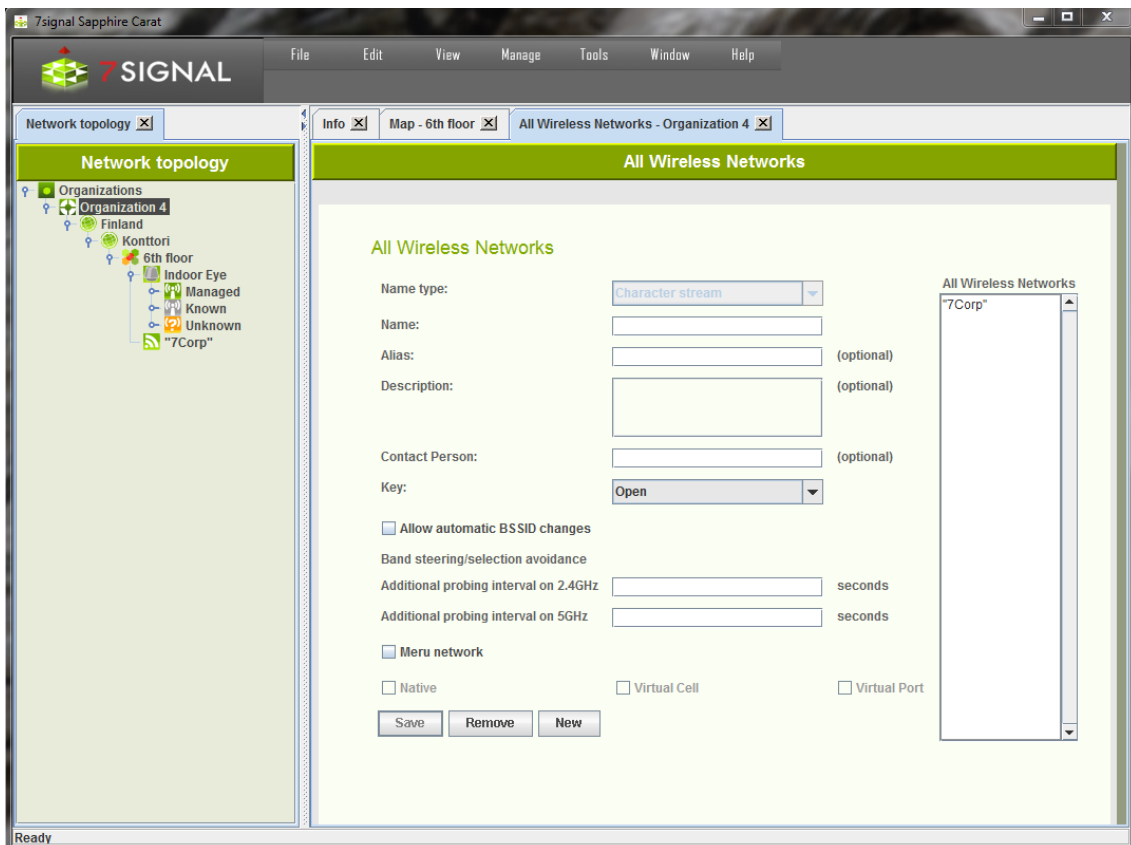


Figure 6: All Wireless Networks view

The pane "All Wireless Networks" shows all defined networks. By choosing the network it is possible to change the current data. Button "Remove" deletes the network and the related information from the system.

9.1.4 Meru networks

Virtual Cell and Virtual Port technologies used in Meru networks requires additional configuration steps. In addition to that, certain passive measurement KPIs with certain area aggregations are not available for Meru networks, since for example, access points cannot be distinguished in Virtual Cell environments.

Setting correct Meru mode

Meru networks can operate in three different modes:

- Native: Standard operation
- Virtual Cell
- Virtual Port

The screenshot shows the 'Edit Wireless Network' window for '7SIGNAL SOL (MU)'. The 'Wireless Network' title bar is at the top. The main content area has a light green background and contains the following fields and options:

- Name type:** Character stream (dropdown)
- Name:** "7SIGNAL SOL (MU)" (text field)
- Alias:** (empty text field) (optional)
- Description:** dd (text field) (optional)
- Contact Person:** (empty text field) (optional)
- Key:** Meru (dropdown)
- Allow automatic BSSID changes
- Band steering/selection avoidance:**
 - Additional probing interval on 2.4GHz: 0 seconds
 - Additional probing interval on 5GHz: 0 seconds
- Meru network
- Native
- Virtual Cell
- Virtual Port
-

Figure 7: Selecting Meru mode

In order to set correct mode:

1. Locate Meru network in Topology tree
2. Right-click and select "Edit"
3. Select the correct Meru operation mode by selecting a checkbox.
4. Click "Save" button.

Access point naming

As the access points cannot be distinguished by their BSSID in Meru networks, *serial MAC address*, *Meru access point ID*, and *radio index* of the access point are used. From the user perspective, an access point name is composed from network name, serial MAC and supported standards, instead of network name, BSSID and supported standards. Radio MAC (BSSID) can be seen on Info tab of the Management GUI when a Meru access point is selected in the Topology tree:

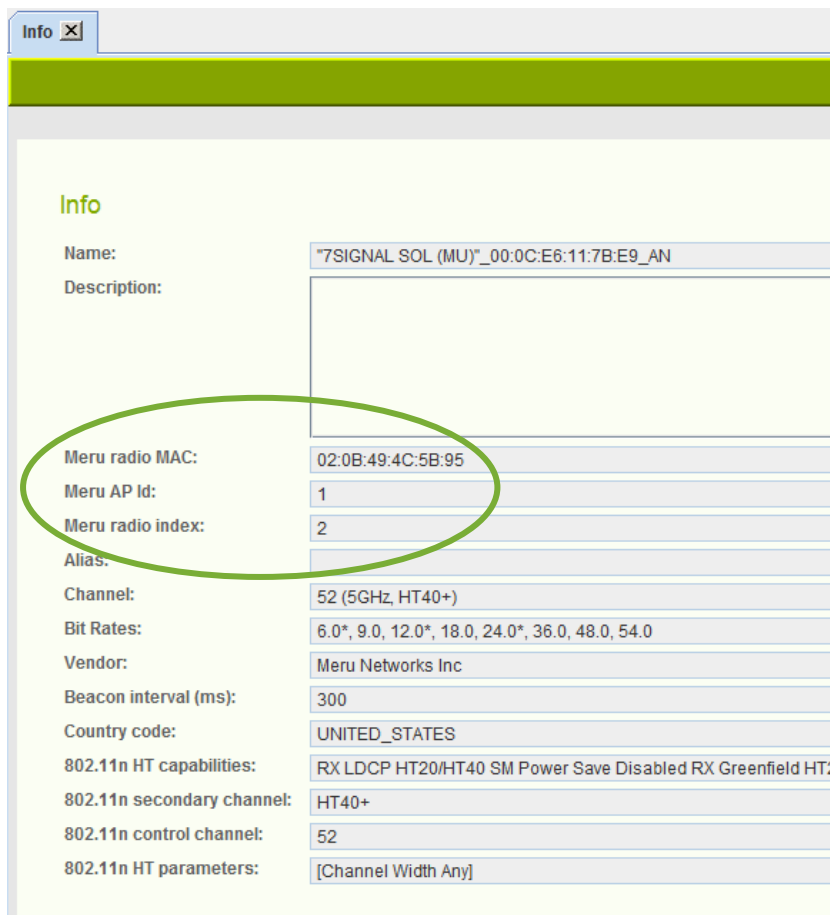


Figure 8: Meru specific properties

In Sapphire Analyzer, the same information can be seen in Info pop-up window.

Active and passive measurements

All active measurements of Meru networks work similarly to measurements executed for standard networks.

Passive measurements are more problematic. In order to collect passive measurement data, you need to add NetworkTraffic to the test profile, and because of nature of Meru networks, only certain area aggregations will work for passive measurement KPIs.

Supported area aggregations for passive measurements are:

- NW
- Eye
- NWEye
- NWEyeAnt
- NWServ
- NWBandServ
- NWBand
- NWBandEye
- NWBandEyeAnt

- NWBandEyeClient
- NWBandEyeAntClient

9.1.5 Avoiding band selection/steering

Some WLAN vendors have implemented different kinds of methods to guide (or force) clients on a certain WLAN band, typically from 2.4 GHz to 5 GHz, which is less crowded. As monitoring stations run measurements on both bands, these band steering/selections will affect negatively to test results, usually resulting attach failures.

In order to avoid these problems, monitoring stations can be configured to send additional probe request while it is attaching to a band-steering-enabled network. WLAN controllers typically allow connections from clients that probe more aggressively.

The screenshot shows the configuration interface for a wireless network. The title bar indicates the window is titled "Edit Wireless Network - '7SIGNAL SOL (MU)'". The main content area is titled "Wireless Network" and contains the following fields and options:

- Name type:** Character stream (dropdown)
- Name:** "7SIGNAL SOL (MU)" (text input)
- Alias:** (empty text input, optional)
- Description:** dd (text input, optional)
- Contact Person:** (empty text input, optional)
- Key:** Meru (dropdown)
- Allow automatic BSSID changes
- Band steering/selection avoidance:**
 - Additional probing interval on 2.4GHz:** 1 seconds
 - Additional probing interval on 5GHz:** 1 seconds
- Meru network
- Native
- Virtual Cell
- Virtual Port
-

Figure 9: Configuring band steering avoidance

In order to enable band steering avoidance:

1. Select wireless network in Topology tree.
2. Right-click and select "Edit"
3. Enter non-zero values in "Additional probing interval" fields.
 - a. Additional probing if configurable per band basis
 - b. Value 1 means one additional probe per second, value 2 means one additional probe per each two seconds, etc.
4. Click "Save" button

9.1.6 Removing Networks

All networks managed by Sapphire are displayed in the Network topology. Networks can be deleted on the organization level. To delete a network from the Network topology:

1. From the Network topology, select the organization containing the wireless network you wish to remove
2. Right-click the organization and select “View wireless network” – then the “All Wireless Networks” view is displayed in the right-hand pane
3. Select from the list the network you want to remove
4. Click “Remove”

9.1.7 Channel configuration

In addition to access points, a wireless network can include a controller, which remotely sets RF parameters for a network. In such a case, the transmitting power and channels may change over time, due to operator actions or the controller’s own actions.

Sapphire supports controllers via channel configuration so that each managed wireless network or access point can have its own set of allowed channel changes. Changes that stay within the preconfigured channel set do not cause an alarm. A change in a channel outside the preconfigured channel set causes an alarm if that alarm has been activated.

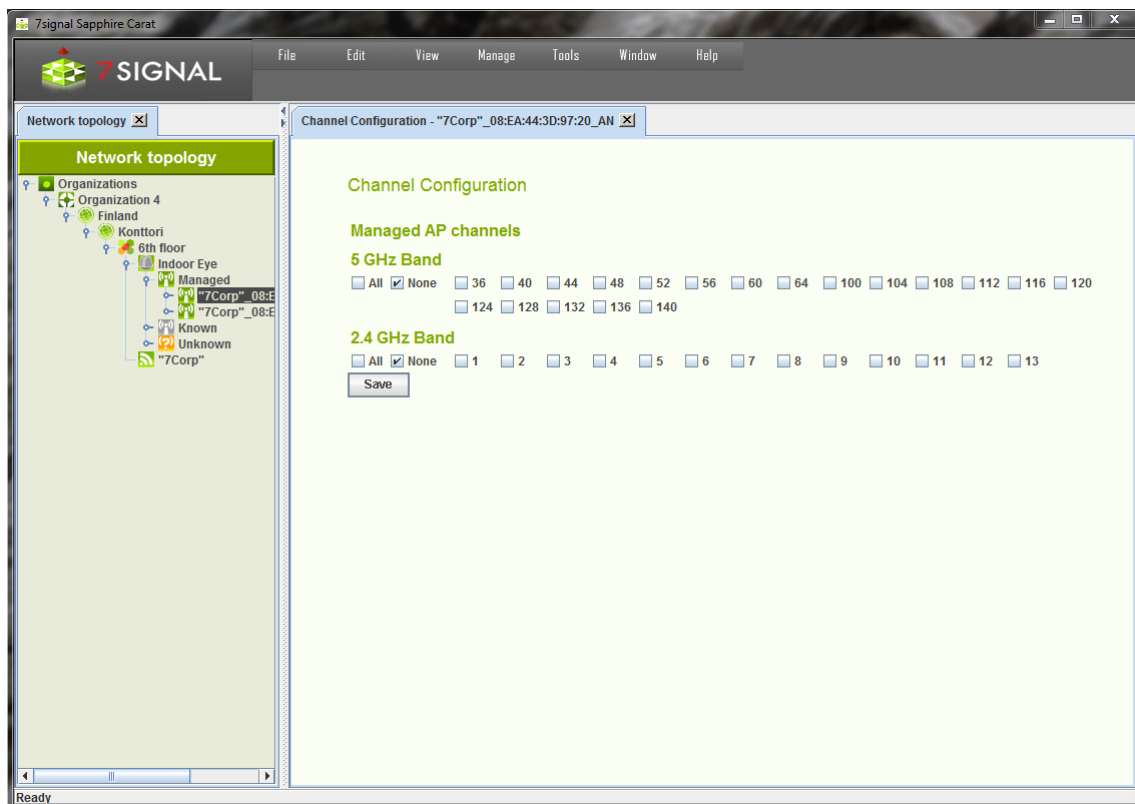


Figure 10: Channel configuration of a Wireless Network

To set up channel configuration, proceed as follows:

1. From the top menu bar, select “View | Network topology”
2. Right-click the item (access point, service area or network) for which you want to set up a channel configuration and select “Channels”
3. Select the allowed channels
4. Select “Save”

7signal Sapphire Enterprise extends this functionality such that all access points or networks within the service area can have their own allowed and forbidden channels. This allows Sapphire to monitor the channel configuration in several networks, and to obtain information on other networks that use channels in unexpected ways. One obvious area of application for channel configuration is office hotels, which have several small wireless networks that can interfere with each other.



Extended channel configuration is a feature in the enterprise edition and requires a license. Each version of Sapphire supports channel configuration in managed networks. To monitor external networks, you need the enterprise license or some other license model that supports channel configuration. Without a suitable license, accessing channel configuration in the user interface does nothing.

10 EYE CONFIGURATION

10.1 States of Monitoring Stations

The Eye unit may be in an inactive state. This happens if there is no network connectivity to the monitoring station when a monitoring station is being added to the system. Also, an active monitoring station may be turned inactive. This allows exceeding the number of monitoring stations limited by the license. Only active monitoring stations may run the tests but the topology may contain unlimited number of inactive monitoring stations.

Related icons

-  active monitoring station
-  inactive monitoring station

10.1.1 Monitoring station LED statuses

LED on the bottom side of an Eye monitoring station indicates its current status:

Table 3: Monitoring station LED states

LED status	Description
Off	Power off
0.5 seconds on 4 seconds off	Monitoring station power on, no connection to Carat server
2 seconds on 2 seconds off	Monitoring station connected to Carat server, idle state
On	Monitoring station connected to Carat server and executing a measurement

10.2 Adding Monitoring Stations

Monitoring stations can be added in the service areas in the Network topology.

There are two ways to add a monitoring station: Automatically detect monitoring station in the network, or adding monitoring station manually.

10.2.1 Detecting and adding monitoring station

1. In the Network topology, select the service area where you want to set up a monitoring station (Eye)
2. Right-click the service area and select "Find and add Eye"

Carat server detects any non-configured monitoring stations in the local area network, and shows a list of IP addresses of these stations.

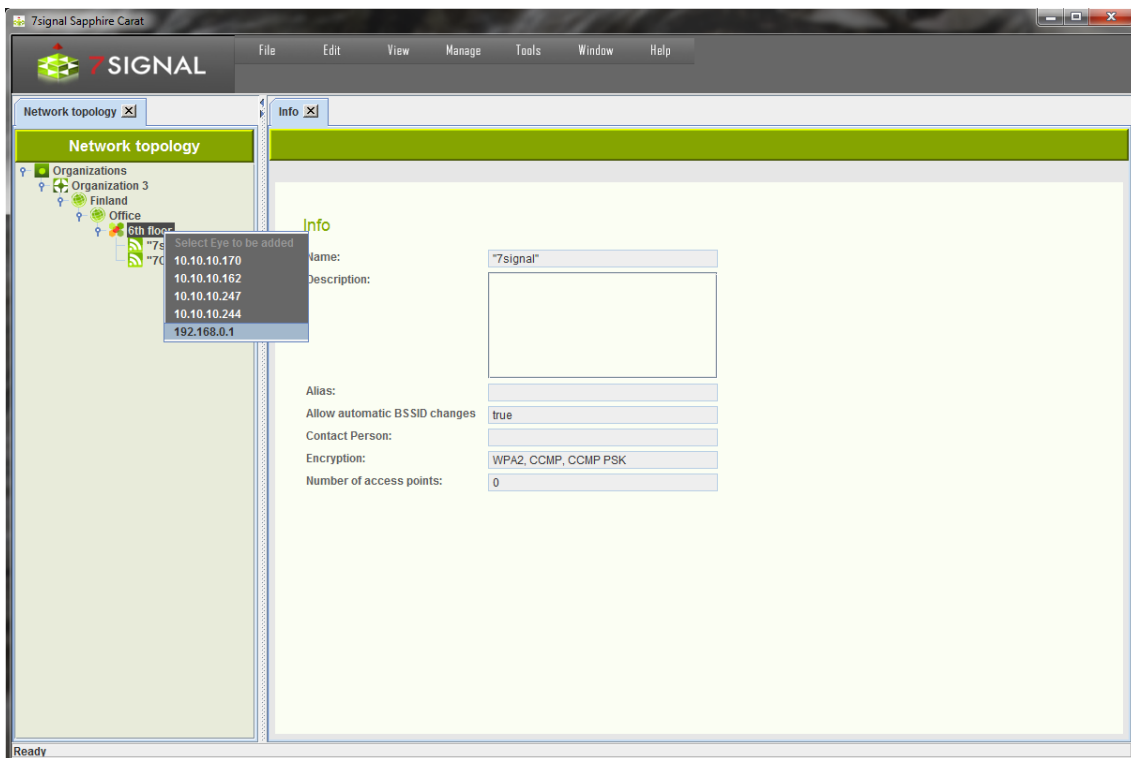


Figure 11: Selecting detected monitoring station in the list

3. Select a monitoring station by left-clicking it. “Add Eye” dialog will be opened:

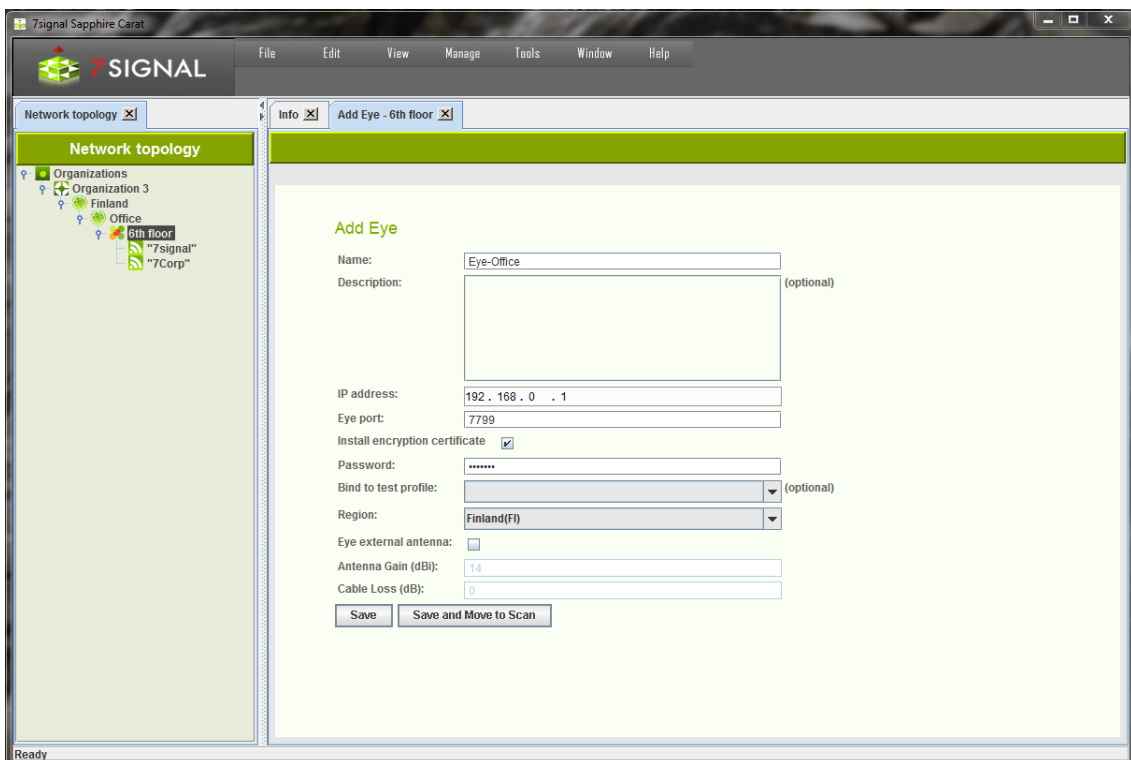


Figure 12: Adding a new monitoring station

4. Enter a name for the Eye
5. Enter a description for the Eye (optional)
 - a. for example, its location and mount information

6. Enter Eye SSH password to password field. This enables automatic installation of encryption certificate in the monitoring station¹.
7. If you already know the test profile you want to use, you can select it now (for more information on test profiles, see the section on test profiles in this user guide)
8. Enter the regional domain. The WLAN channels and possibly power options are dependent on this setting so one should always choose the right setting².
9. If an external antenna is attached to the monitoring station, it is possible to use the 8th beam or diversity antenna with the check-box. When selected, one must also provide
 - a. Antenna gain
 - b. Cable loss (measured or estimate)
10. Save the monitoring station settings by clicking “Save” or “Save and move to scan”

10.2.2 Adding monitoring station manually

1. In the Network topology, select the service area where you want to set up a monitoring station (Eye)
2. Right-click the service area and select “Add Eye”
3. Enter a name for the Eye
4. Enter the Eye’s IP address³
5. Enter a description for the Eye (optional)
6. Enter Eye SSH password to password field. This enables automatic installation of encryption certificate in the monitoring station⁴.
7. If you already know the test profile you want to use, you can select it now (for more information on test profiles, see the section on test profiles in this user guide)
8. Enter the regional domain. The WLAN channels and possibly power options are dependent on this setting so one should always choose the right setting⁵.
9. If an external antenna is attached to the monitoring station, it is possible to use the 8th beam or diversity antenna with the check-box.
10. Save the monitoring station settings by clicking “Save” or “Save and move to scan”

10.2.3 Install monitoring station software

After clicking “Save” button, Carat checks if the monitoring station software is needed to be updated. When installing a new Eye unit, this is usually the case. A popup-window is opened:

¹ If you have already installed encryption certificate manually in the monitoring station, uncheck “Install encryption certificate checkbox and leave the password field empty)

² Regulatory domain cannot be changed in some countries, including United States.

³ In case of a Soft Eye installed to the same host as the Carat server, loopback address 127.0.0.1 **MUST BE USED!**

⁴ If you have already installed encryption certificate manually in the monitoring station, uncheck “Install encryption certificate checkbox and leave the password field empty)

⁵ Regulatory domain cannot be changed in some countries, including United States.

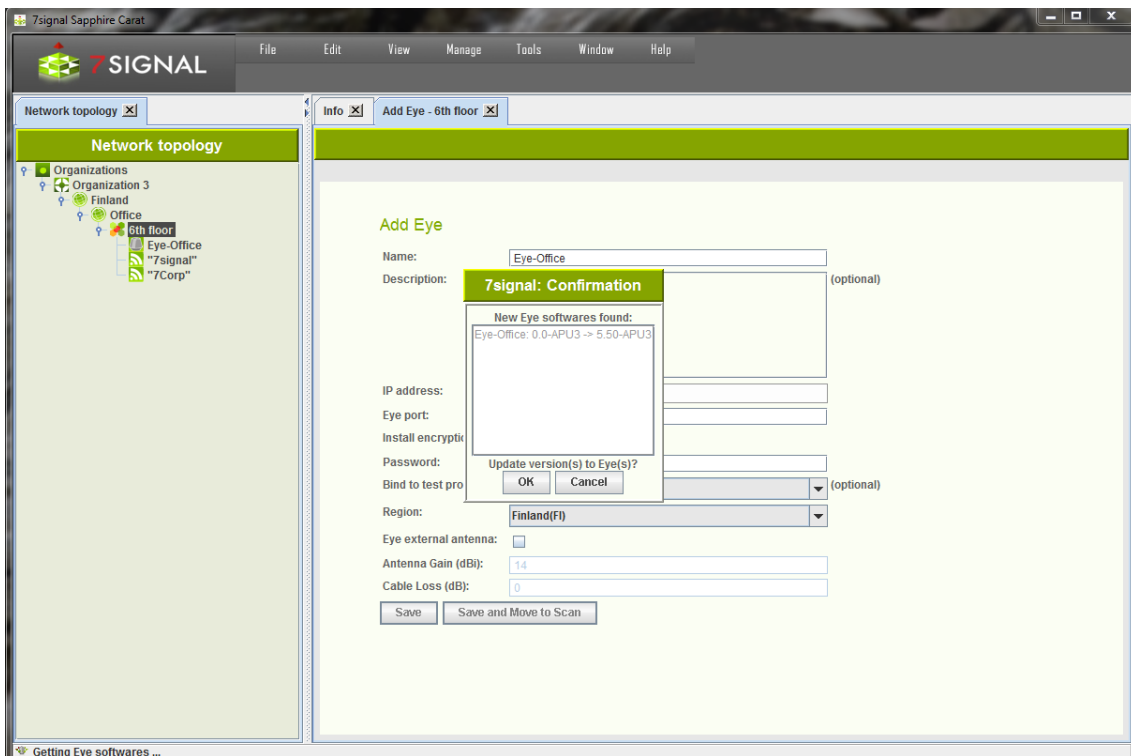


Figure 13: Update monitoring station software

Click "OK" in order to install the software to the monitoring station. Progress bar shows the status of uploading and installation process:

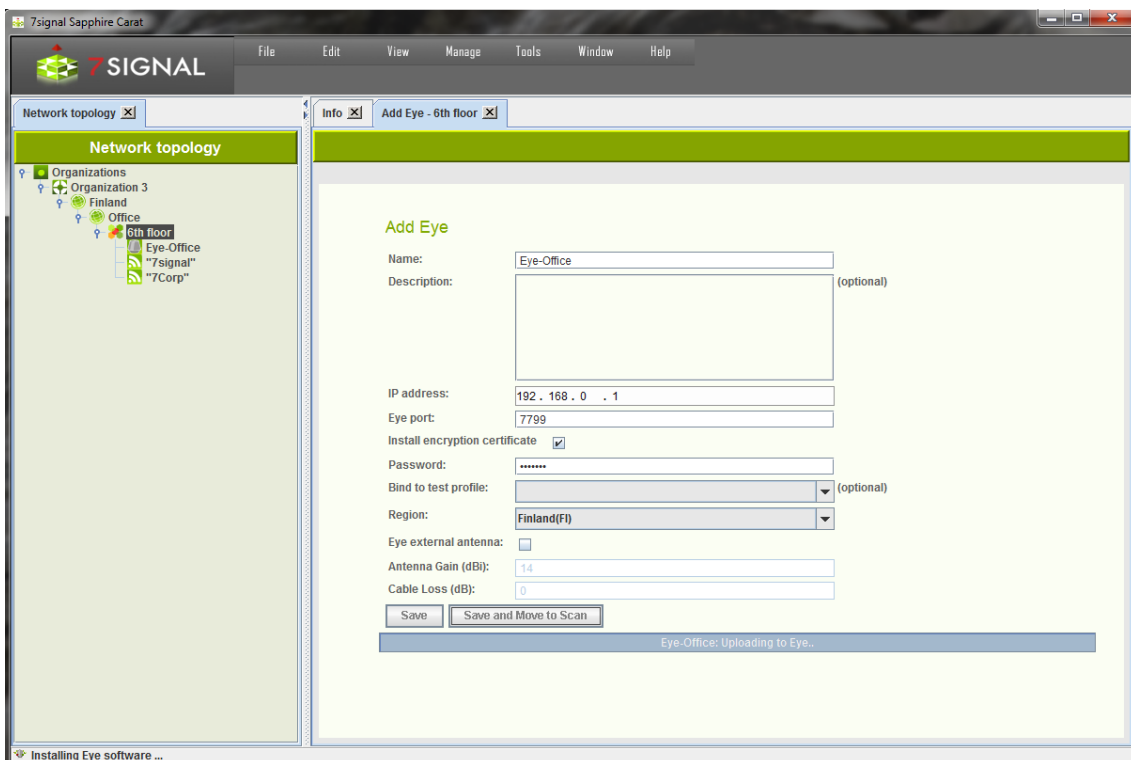


Figure 14: Installing monitoring station software

After software is uploaded and installed, the dialog is closed.

10.3 Monitoring station settings

1. Activate the monitoring station by right-clicking on it in the Network topology
2. Select “Edit”
 - a. This opens the settings window in the right pane
3. The settings window allows you to view and edit the following information about the monitoring station:
 - a. Name
 - b. Description
 - c. Test profile
 - d. Regulatory domain⁶
 - e. Settings for the Eye’s heating resistor⁷
 - f. Monitoring station’s uptime
 - g. Monitoring station’s current time
 - h. External antenna enabled or disabled^{7,8}
 - i. gain of the external antenna
 - ii. cable loss
 - i. Software versions and temperature⁷ of the monitoring station (in a table)
 - j. Ethernet and wireless MAC addresses
 - k. Antenna compass headings⁷
 - l. Information about the access points within the monitoring station’s range
4. You can check the information about the access points monitored by the monitoring station:
 - a. Access point name (AP name)
 - b. Access point alias name (AP alias)
 - c. The role of the access point with relation to this Eye (Relation to Eye)
 - d. Selected antenna
 - e. Current channel
5. You can also modify the information about the access points monitored by the monitoring station:
 - a. The role of the access point with relation to this Eye (Relation to Eye)
 - b. Selected antenna
6. Click
 - a. “Save” to save any changes you have made
 - b. “Save and Move to Scan” to save any changes you made and move to wireless network scan test.
 - c. “Reset Eye” to reset the monitoring station
 - d. “Update antenna headings” to update antenna headings from the monitoring station (may be needed if the location of the monitoring station has changed)

⁶ Regulatory domain cannot be changed in some countries, including United States.

⁷ Not available in Micro and Soft Eye

⁸ External antenna cannot be configured in some countries, including United States.

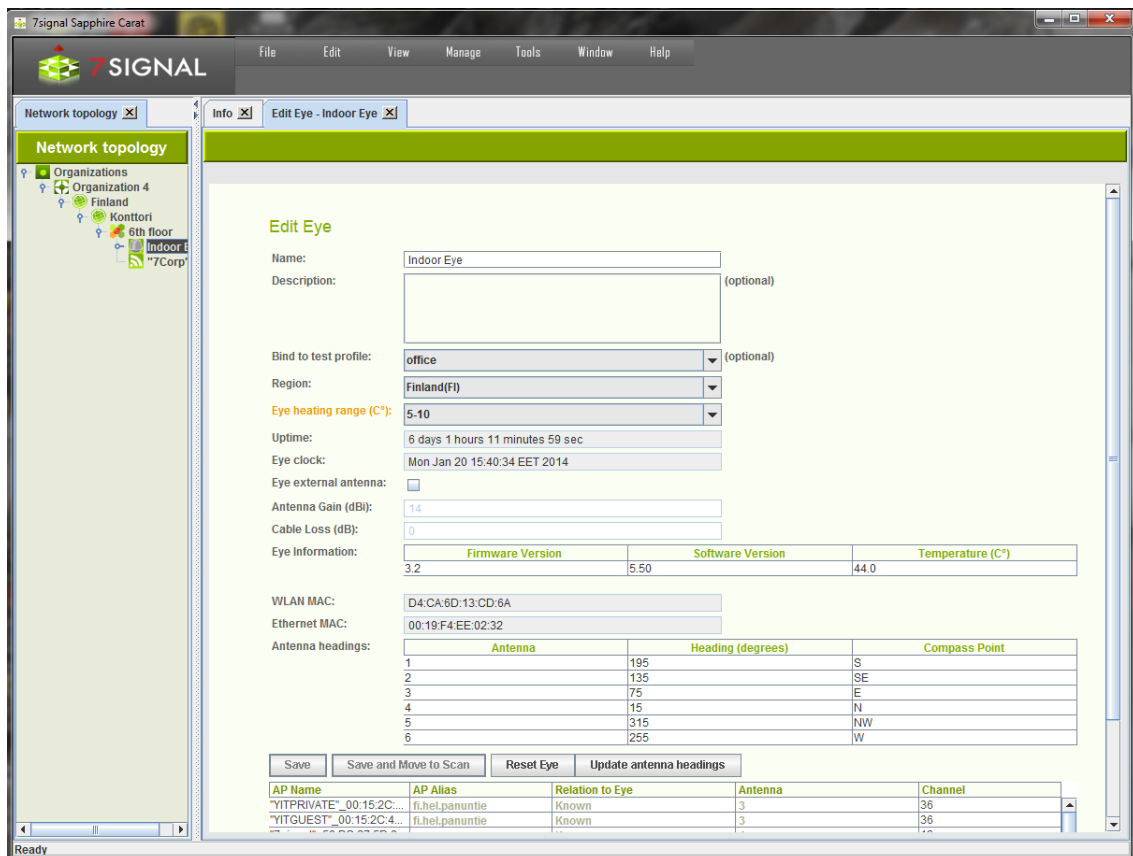


Figure 15: Viewing and editing monitoring station properties

10.4 Activating Monitoring Stations

By default, the monitoring station is in active state. This is flagged with the green background color in the Network topology. An inactive monitoring station would have orange background color.

It is possible to deactivate the monitoring station. This feature is mainly targeted for temporary installations. An inactive monitoring station exists in the system and its measurements are accessible as usual. In inactive state, monitoring station IP address can be changed.

Only an active monitoring station may produce measurements and run manual tests. The state management enables consistent user view on Network topology and measurements.

The use case is to have temporary measurements in numerous locations and to have the possibility to return to one location and continue with identical monitoring station setup to keep the measurements comparable. After activating monitoring station, it is recommended that it would be treated as new if it will be used for monitoring.

10.5 Managing monitoring station IP configuration

In order to change monitoring station IP configuration settings:

1. Activate the monitoring station by right-clicking on it in the Network topology
2. Select "Connection management"

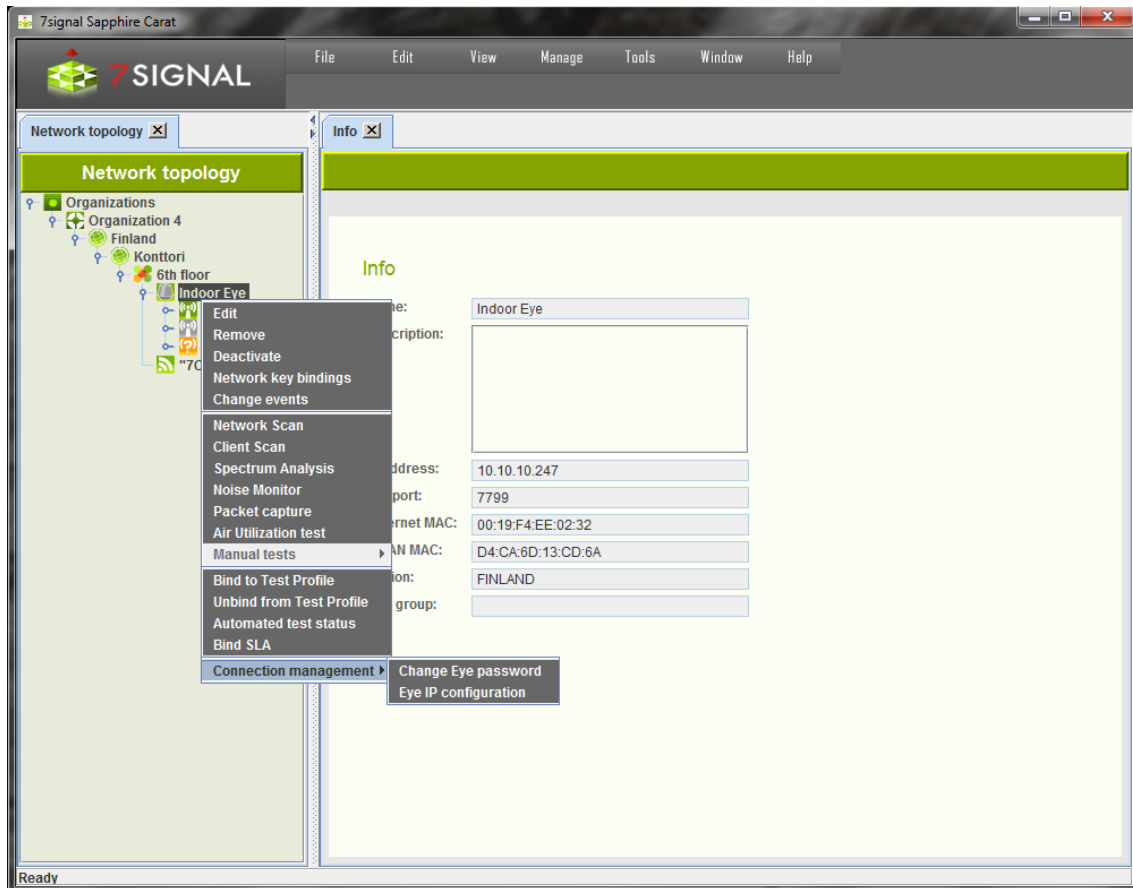


Figure 16: Eye IP configuration submenu

3. Select "Eye IP configuration"

Eye IP configuration dialog is opened:

Eye IP configuration

Name:

Use DHCP:

Discover new address:

IP address:

Eye port:

Network mask:

Default gateway:

10.5.1 Changing static IP configuration

1. Edit IP address/network mask/default gateway properties
2. Click “Save and restart Eye” button

New IP properties are updated to the monitoring station and the monitoring station restarts

10.5.2 Configuring DHCP for monitoring station

1. Select “Use DHCP” checkbox. Leave “Discover new address” checkbox selected.
2. Click “Save and restart Eye” button

New IP properties are updated to the monitoring station and the monitoring station restarts. After restart, the monitoring station obtains its IP configuration from DHCP server and Carat will discover the new IP address automatically by applying mDNS/DNS-SD protocol.

10.6 Managing Monitoring Station Software

The software versions of the monitoring stations are managed via Carat. Actions related to monitoring station software management can be found in the “Eye software management” submenu of “Manage” menu.

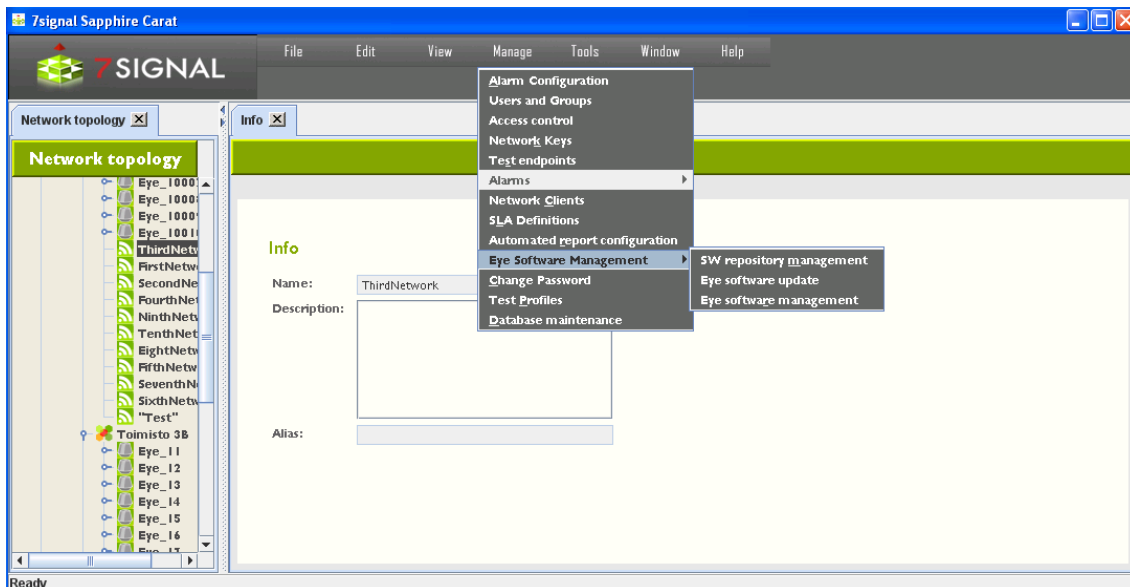


Figure 17: Eye Software Management submenu

Update of monitoring station software can be divided in two steps:

- Import latest monitoring station software to Carat
- Update monitoring station software to monitoring stations

10.6.1 Importing monitoring station software (Solution Administrator only)

Only a Solution Administrator can import new monitoring station software packages. Select “SW repository management” in “Eye software management” menu. “Eye SW repository management” view is opened.

On this view, you can manage monitoring station software versions in the Carat server. All software versions imported into Carat are visible in a list.

Notice that starting to release 5.0, new monitoring station software versions, specific to the current release, are automatically imported to the system, if Carat server was installed/upgraded by using “full” installers. If the upgrade was done by using a full installer, this step is unnecessary.

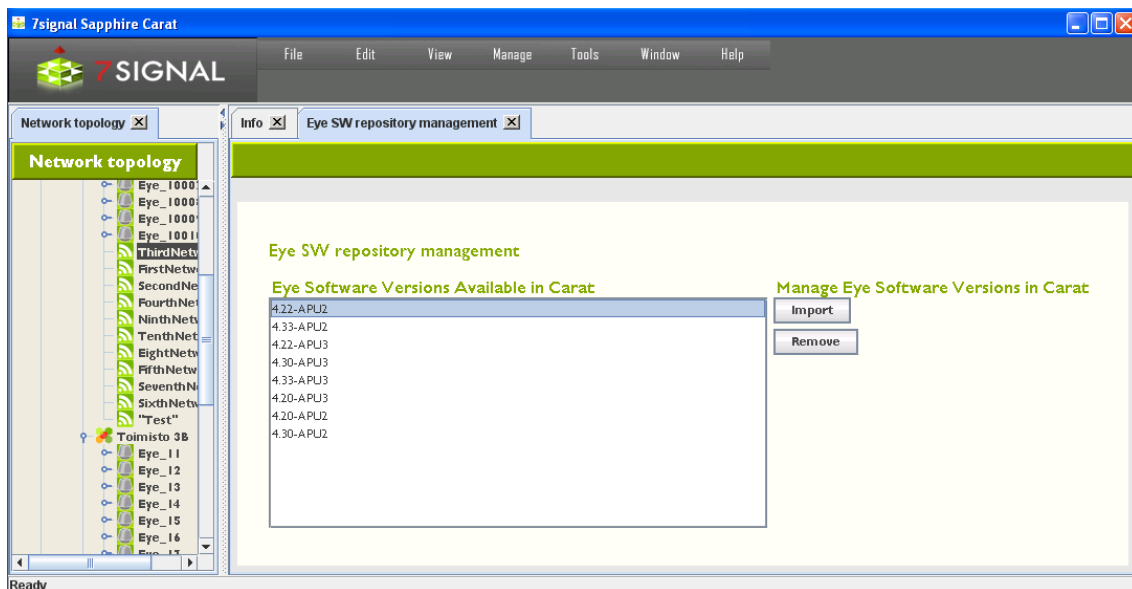


Figure 18: SW repository management view

Import monitoring station software as follows:

1. Make sure that you have monitoring station software available in your computer (7signal-eye-x.y-APU2/APU3/x86)
2. Click “Import” button
3. Browse and select the monitoring station software from the file list

The imported software appears to the software version list.

In order to remove old software versions from Carat:

1. Select unwanted software versions from the list.
2. Click “Remove” button.

10.6.2 Update monitoring station software (configurator/organization admin users)

Select “Eye software update” in “Eye Software Management” menu. “Eye software update” view is opened. If Carat detects monitoring stations that do not have the latest software installed, Carat proposes the update:

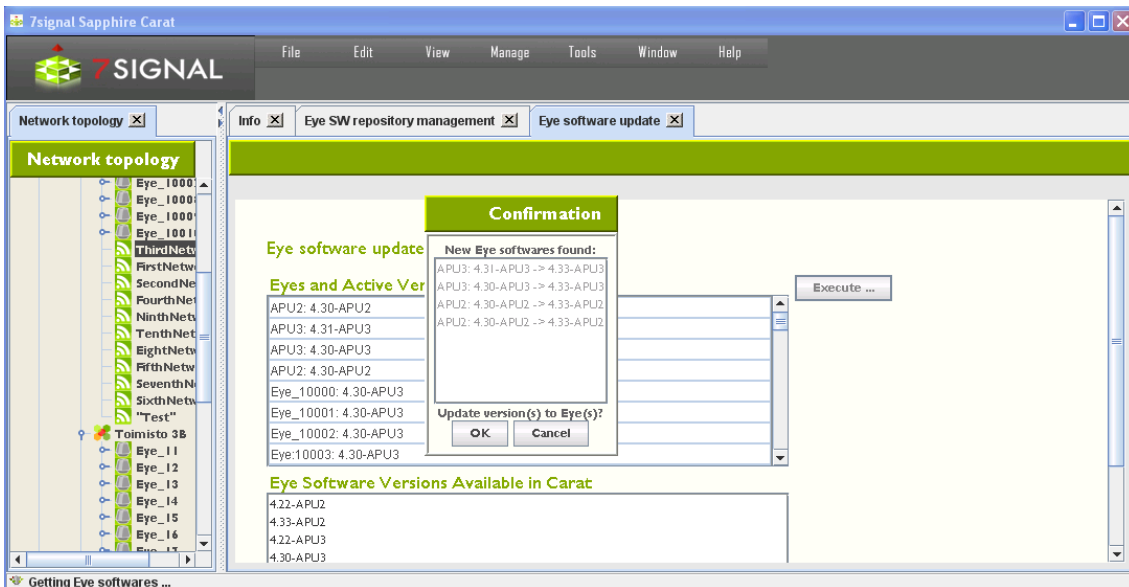


Figure 19: Start Eye software update

Accept the software update by clicking “OK” button on confirmation dialog.

Installation progress can be inspected by following the progress bars that appear for each monitoring station. First, the software is uploaded to the monitoring stations:

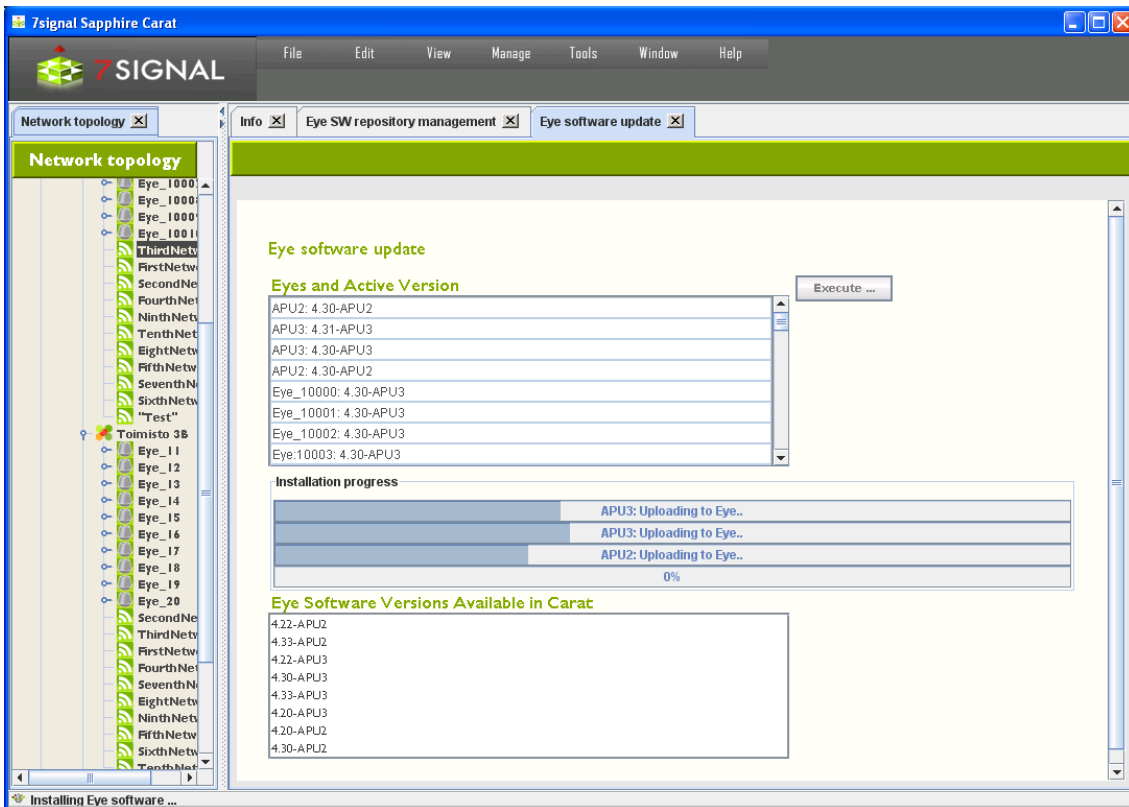


Figure 20: Software upload to monitoring stations ongoing

After the upload phase is completed, the monitoring station installs the software update and restarts itself:

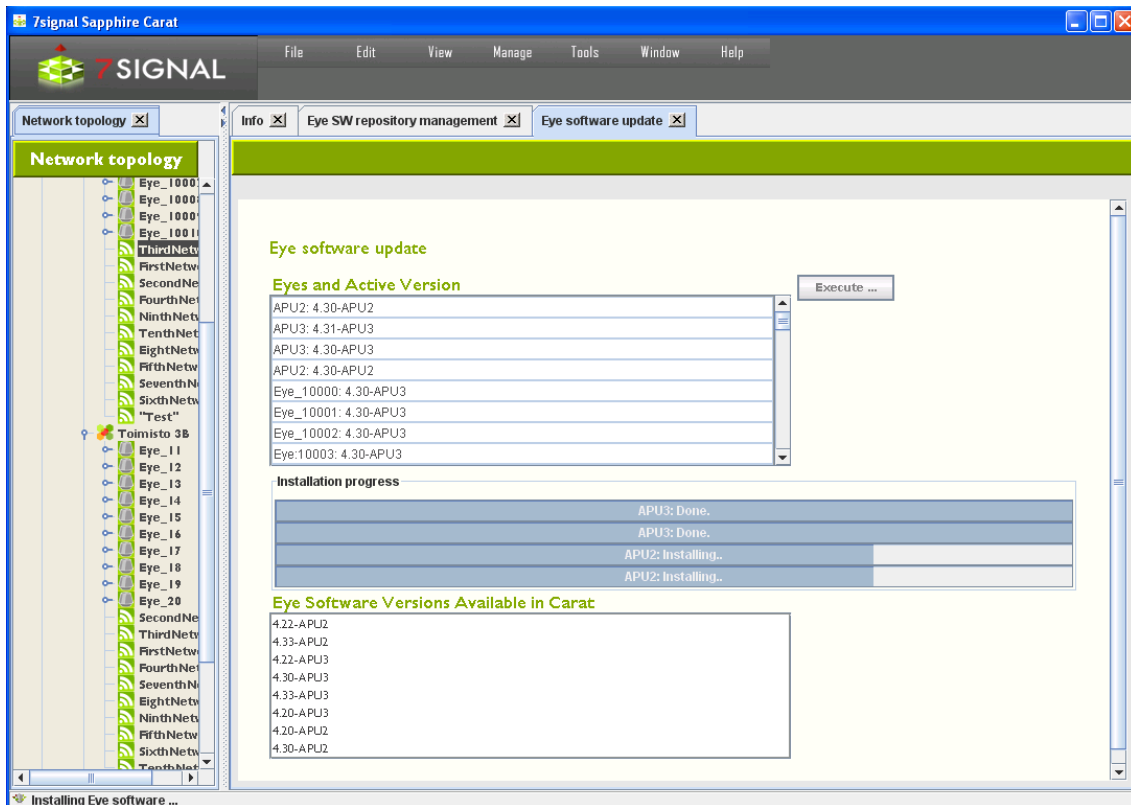


Figure 21: Software installation ongoing

10.6.3 Uninstalling and changing monitoring station software versions

Sometimes it is necessary to uninstall old software versions from monitoring stations. On rare occasions, a rollback to an older version (already installed in monitoring station) is necessary. These actions can be done by using the “Eye software management” view.

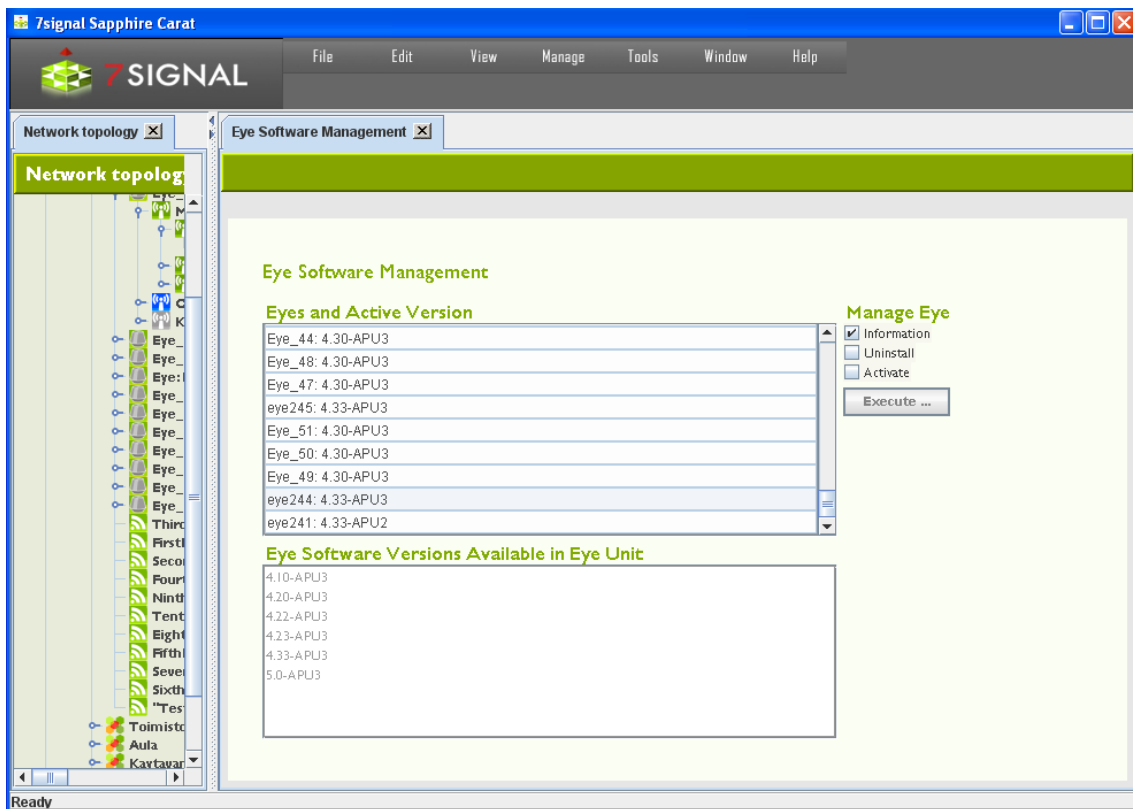


Figure 22: Eye software management view

The top portion of the view lists the software versions of an individual monitoring station when the monitoring station is activated. At the same time, you can also perform operations that are available in the top part of the pane.

Operations:

- **Information** displays the software versions in the activated Eye
- **Uninstall** uninstalls the software version
- **Activate** activates the software uploaded to the monitoring station⁹

10.7 Initial network scan

When the Eye has been installed or needs to be reconfigured, you must run a network scan. There are various preconfigured scanning durations. The purpose of the initial scan is to scan the monitoring station's radio frequency environment very thoroughly and to detect the access points suitable for monitoring.

Network scan type	Description	Estimated duration (all antennas and channels) for channels 1-11 excl. 5 GHz
Slow	First deployment	21–27 min
Regular	Normal	9–12 min
Fast	Quick	less than 3 min

⁹ Usually, it is not necessary to activate software version manually. New software version is activated automatically after software update.

The scan results are presented in a table. An initial scan should be run whenever substantial physical changes have been made in the environment being monitored (for example, new or removed walls), or if the Eye's location has been changed.

The table contains the following information about the WLAN access points detected:

- Network name (ESSID)
- Encryption methods supported by the access point
- MAC address of the access point¹⁰
- Alias (access point name in Cisco and Aruba¹¹ access points)
- Channel
- Management status (if not known, denoted as "Unknown")
- Managing Eye (if managed by other Eye)
- Currently selected antenna
- Antenna that hears the access point best
- Access point signal strength
- Noise level¹²

The access points in the service area must have a management status. Setting a management status means that the access point's existence is acknowledged. Unacknowledged access points prompt issuing of an alarm if such an alarm has been configured. The management statuses are as follows:

- **Managed:** Monitored by this monitoring station
 - The recommendation for signal strength is >-65 dBm
- **Own:** Own access point managed by another monitoring station
- **Known:** An access point that is an accepted part of the radio frequency environment (for example, a neighboring network)
 - If possible, ensure the access point operates properly and can be accepted
- **Unknown:** An access point without a monitoring status
 - In practice, this status should exist only during network scans in new service areas; it should not exist in normal use

The changes are saved in Sapphire Carat's database and the installed monitoring station. The test is described in more detail below, under the "Network Scan" description.

¹⁰ In case of a Meru access point, serial MAC of the access point.

¹¹ Availability depends of Aruba software level.

¹² No available with Micro Eyes. Might not be available in Soft Eyes.

11 ENCRYPTION KEY MANAGEMENT

Related icons

-  WPA 2 encryption
-  WPA 1 encryption
-  IEEE 802.11X authentication with dynamic WEP keys
-  HTTP authentication
-  WPA EAP encryption
-  WEP encryption

Before accessing secured WLAN, an encryption key for that network should be created.

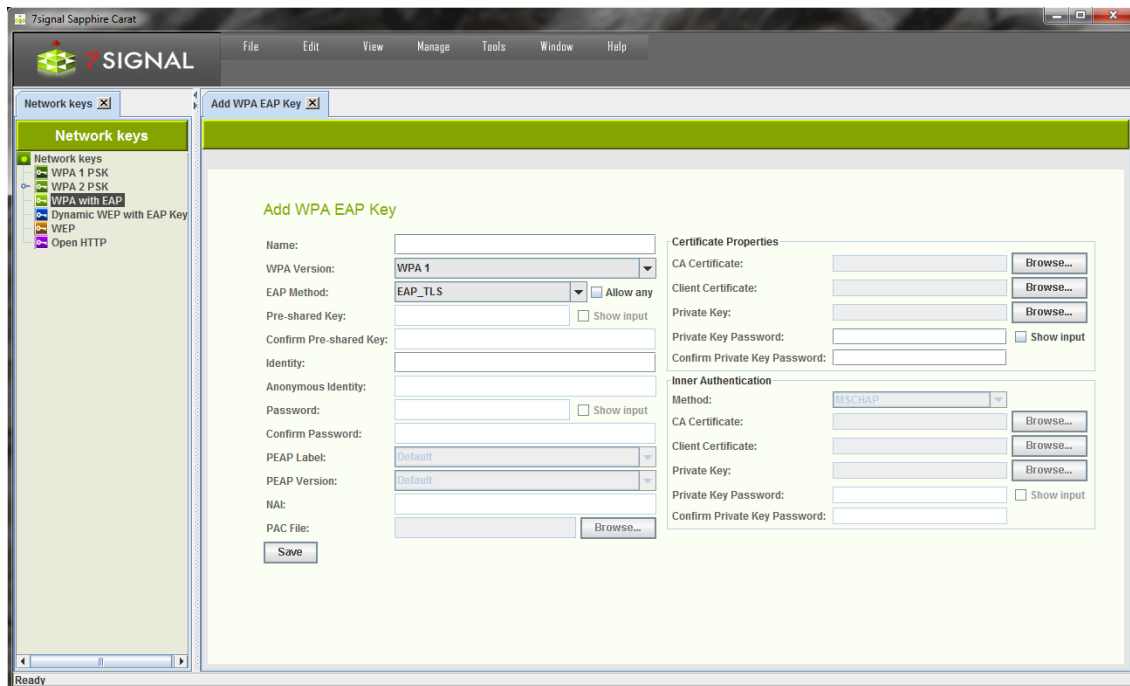


Figure 23: Network key configuration dialog

11.1 Supported encryption types

Table 4: Supported encryption types

Key type	Authentication method	Inner authentication
WPA 1 PSK		
WPA 2 PSK		
WPA with EAP	EAP_TLS	
	EAP_PEAP	GTC MD5 MSCHAPV2 OTP TLS
	EAP_TTLS	MSCHAP MSCHAPV2 PAP CHAP EAP-MSCHAPV2 EAP-TLS EAP-GTC EAP-OTP EAP-MD5
	EAP_PSK	
	EAP_FAST	
	LEAP	
	EAP_MSCHAP_V2	
	Dynamic WEP with EAP	EAP_TLS
EAP_PEAP		GTC MD5 MSCHAPV2 OTP TLS
EAP_TTLS		MSCHAP MSCHAPV2 PAP CHAP EAP-MSCHAPV2 EAP-TLS EAP-GTC EAP-OTP EAP-MD5
LEAP		
EAP_MSCHAP_V2		
WEP	WEP 104 Hex	
	WEP 104 Asc	
	WEP 40 Hex	
	WEP 40 Asc	
Open HTTP		

11.2 Adding encryption keys (PSK)

11.2.1 Passphrase and pre-shared key

Pre-shared key authentication is sometimes called passphrase authentication. Standard configuration interfaces allow user to type passphrase (that is converted to PSK) and proprietary interfaces can allow direct entry of PSK.

WPA and WPA2 are both vulnerable to brute force attacks if you use weak PSK.

The user may enter either a PSK or a passphrase when creating WPA1/2 PSK.

11.2.2 Adding WPA-PSK key

Add a key by following the instructions below:

1. From the top menu bar, select “Manage | Network Keys” – the available key types and existing keys are displayed in a hierarchical structure in the left pane
2. Right-click the key type you want to create and select “Add key”
3. Enter a name for the key
4. Enter the data required by the key type
 - a. There are significant differences in the data required for different key types
 - b. When “Show input” is checked, the user interface displays the passwords in plain-text.
5. Save the key by clicking “Save”

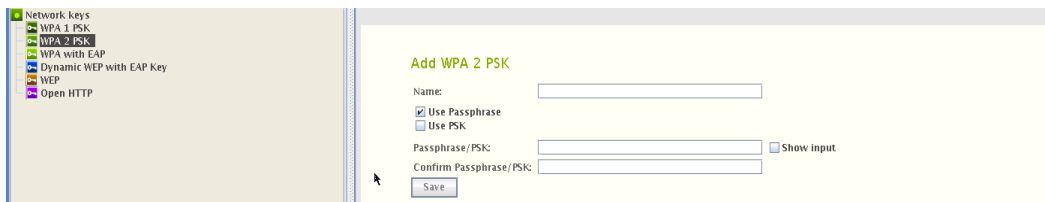


Figure 24: Adding WPA-PSK key

After a key has been created, it should be attached to a wireless network.

1. From the top menu bar, select “View | Network topology”
2. In the Network topology, select the network to which you want to add the encryption key and right-click
3. Select “Add Key”
4. Select a suitable encryption key for the network from the pull-down menu
5. Click “Save”

11.3 Certificate-based encryption

There are input fields for the “CA certificate” and “Client certificate”. It is recommended that both certificates are added. If one certificate file contains all the information, it should be used in both of the input fields.

The certificate container is expected to be accessible by the Carat GUI client in the local or shared file system of the host machine. Accepted formats are the following:

- CA certificate – PEM, DER, PKCS12 (aka PFX)
- Private key – PKCS12 (aka PFX)

As a corollary, a single PKCS12 formatted file that contains the CA certificate as well as the private key, can be used in both of the cases.

If conversions are required to achieve these formats, please consult Your Certificate Authority. In Linux and UNIX environments OpenSSL is commonplace tool and can handle the conversions required:

To export client certificate from p12 container:

```
openssl pkcs12 -in <yours>.p12 -clcerts -nokeys -out <yours>client_cert.pem
```

To export private key from p12 container:

```
openssl pkcs12 -in <yours>.p12 -nocerts -out <yours>private_key.pem
```

To export CA certificate from p12 container:

```
openssl pkcs12 -in <yours>.p12 -cacerts -nokeys -out <yours>cacert.pem
```

TIP: Microsoft environments may have certificate files with file extension CER. The file content format typically is DER. To turn DER files into PEM, please use the command below:

```
openssl x509 -informat DER -in <yours>.cer -outformat PEM -out <target>.pem
```

Windows environments have extension “PFX” to mark a typical certificate container file type. This format is exactly PKCS12 format that typically has “p12” extension in Linux/Unix world. 7signal Sapphire does not care about the extension but the internal format of the file.

11.4 HTTP (captive portal) authentication

7signal Sapphire has a limited support for HTTP captive portal authentication. There are two basic requirements that must be fulfilled in order to get authentication work:

1. Login form on a login web page must not contain any dynamic fields. As dynamic fields will usually change for each separate login, for monitoring station it is difficult to adapt changing content of the login form.
2. There must not be any mandatory HTTP redirect request during login process.

Upcoming Sapphire versions will have support for dynamic fields and HTTP redirects.

Captive portal authentication is done simply by issuing HTTP GET or POST request, containing the user credentials, directly to captive portal/authentication server, i.e. not loading the login page first.

11.4.1 Prerequisites

Resolve login information

A login page typically consists of a HTML form that contains fields for login information. Open the login page in a web browser, and select “view source”. The login form is an HTML block enclosed within `<form>` tag. For example:

```
...
<form method="post" action="http://login.mycompany.com/login">
  <input type="hidden" name="SiteId" value="123"/>
  <input type="hidden" name="Target" value="www.othercompany.com"/>
  <input type="hidden" name="PaymentMethod" value="Passthrough"/>
  <input type="hidden" name="ProxyHost" value=""/>
  <input name="Confirmed" value="1" type="hidden">
  <input type="text" name="Username" value="JohnDoe"/>
  <input type="password" name="Password" value="VerySecret"/>
  <div id="do_submit">
    <div id="free_submit_btn">
      <input type="submit" tabindex="5" name="connect" value="" />
    </div>
  </div>
  <div id="do_agree" >
    <input name="DoAgree" value="1" type="checkbox" checked>
  </div>
</form>
```

Based on this HTML code, the browser would generate a following HTTP POST data targeted to <http://login.mycompany.com/login>:

```
SiteId=123&Target=www.othercompany.com&PaymentMethod=Passthrough&ProxyHost=&Confirmed=1&
Username=JohnDoe&Password=VerySecret&connect=&DoAgree=1
```

For more information how different HTML elements will be encoded, see

http://en.wikipedia.org/wiki/POST_%28HTTP%29

11.4.2 Creating Open HTTP Key

1. From the top menu bar, select “Manage | Network Keys” – the available key types and existing keys are displayed in a hierarchical structure in the left pane
2. Right-click “Open HTTP” and select “Add key”
3. Fill in a name for the key
4. Enter authentication URL
5. Select “Use HTTP POST”, if needed (this is the usual case)
6. Enter POST data
7. Save the key by clicking “Save”.

Based on the HTTP POST example above, the Open HTTP key would look like the following:

Figure 25: Adding Open HTTP Key

11.5 Multiple network keys per Eye

There is no limitation to number of keys per Eye or per Wireless Network. If there is only one key bound to Wireless Network, that key shall be used every time this particular SSID is associated with. On top of that, each Eye unit may be bound with Eye specific key.

The rationale is to support environments where the actual key dictates both access to the access point in general and also the access level to the network services beyond the access point.

In order to bind an Eye specific network key to Eye

1. Right-click Eye in the Network Topology
2. Select "Network key binding"
3. "Eye network keys" view is opened

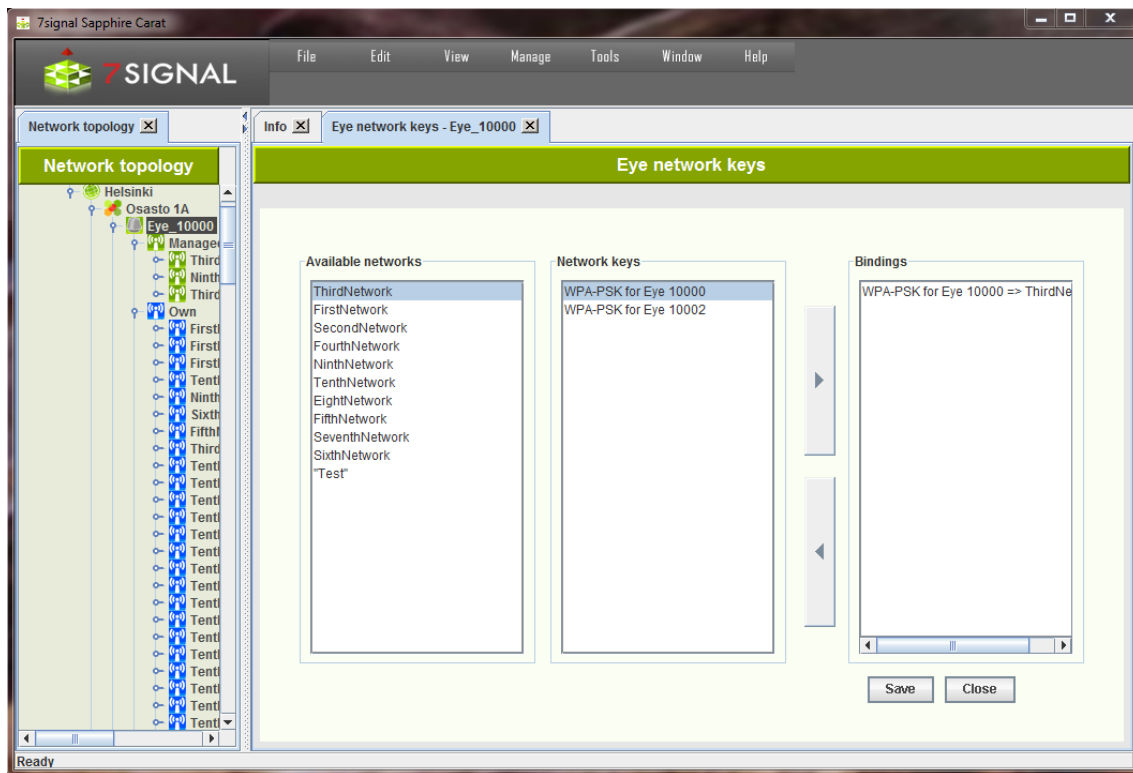


Figure 26: Binding network key to an Eye

4. Select the network in “Available networks” list
5. Select the network key in “Network keys” list
6. Click the right-arrow button
7. Select “Save”

In order to remove network key binding

1. Select the binding in “Bindings” list
2. Click the left-arrow button
3. Select “Save”

11.5.1 Microsoft PKI Infrastructure

One commonplace certificate-based environment is implemented by Microsoft. Typically any appliance shall have its own account (“machine-account”). It would very challenging to make the Linux-based Eye to serve Windows infrastructure with the proper certificate. An applicable option is to create one user-account to be used by all Eye units, or separate user accounts for each Eye.

When a user-account is in place, the authentication may be defined as follows:

Add WPA EAP Key

Name:

WPA Version: **WPA 1 PSK**

EAP Method: **EAP_MSCHAP_V2** Allow any

Pre-shared Key: Show input

Confirm Pre-shared Key:

Identity: **local_ID**

Anonymous Identity:

Password: **secret123** Show input

Confirm Password: **secret123**

PEAP Label: **Default**

PEAP Version: **Default**

NAI:

PAC File:

Certificate Properties

CA Certificate:

Client Certificate:

Private Key:

Private Key Password: Show input

Confirm Private Key Password:

Inner Authentication

Method: **MSCHAP**

CA Certificate:

Client Certificate:

Private Key:

Private Key Password: Show input

Confirm Private Key Password:

Figure 27: Adding network key for Microsoft PKI infrastructure


1. Select “Dynamic WEP with EAP key” to get the dialog above
2. Select WPA key type, either 1 or 2, according the local environment
3. EAP method must be set to “EAP_MSCHAP_V2”
4. Fill in the account user name to the field “Identity”
5. Enter and confirm the account password.
6. Enter Windows infrastructure CA certificate.
7. One may enter the same certificate as “Client Certificate” as well.

The Eye is now properly authenticated in Windows PKI environment.

12 TEST END-POINTS

12.1 Sonar

Sonar is 7signal specific server that handles typical network requests i.e. it emulates numerous servers in the network.

Sonar (icon ) is the server needed for executing elementary tests. There can be several Sonar servers configured. Each test can be configured to use any of the configured Sonars. Configuring Sonar servers makes it easy to define the parameters for the automatic measurements.

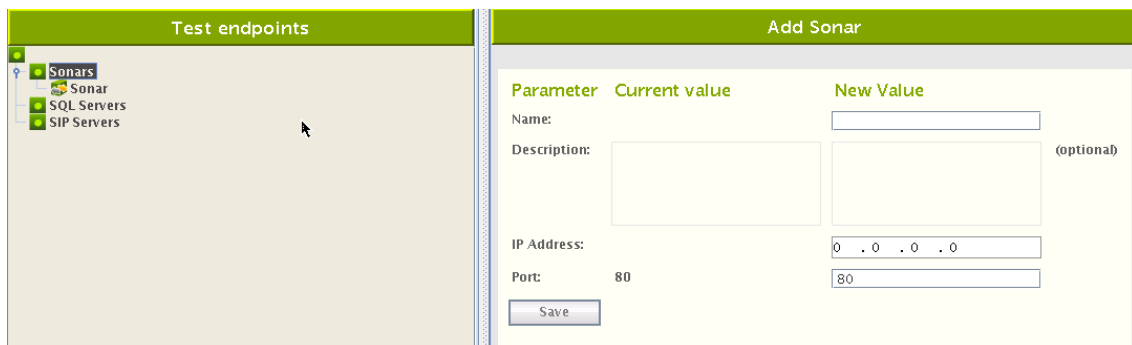


Figure 28: Adding new Sonar server

1. From the top menu bar, select “Manage | Test endpoints”
2. Select “Add Sonar” from Sonars tree node after right clicking it.
3. Enter a name for the Sonar instance (*Note: The name should be descriptive, especially when one is using several Sonars*)
4. Enter a description for the Sonar (optional)
5. Enter the IP address and TCP port (*Note: At this stage, Carat does not verify that the Sonar actually exists, so ensure that the Sonar exists before you begin testing*)
6. Click “Save”

12.2 Generic test counterparts

It is possible to run tests towards actual network servers such as SIP servers or database hosts.

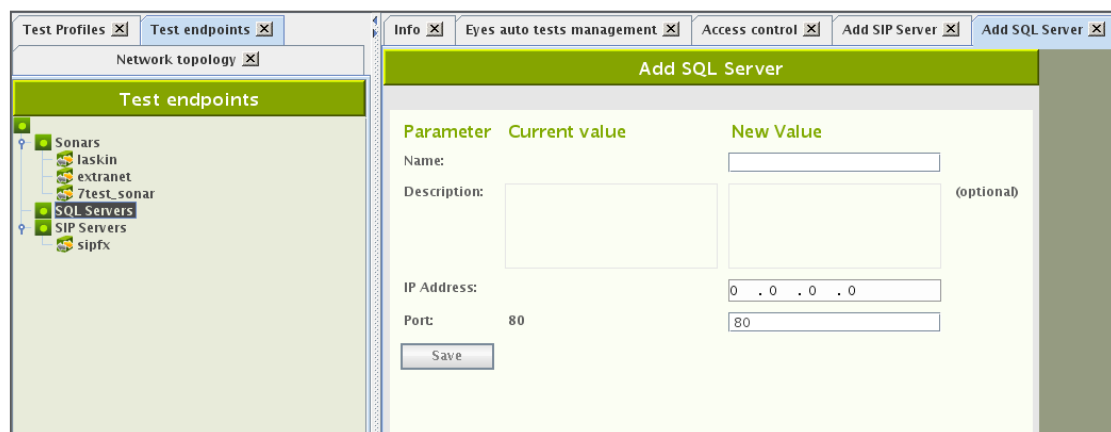







Figure 29: Adding generic test counterpart

Test endpoint definition requires information on networking level but does not require anything application specific. For example, an SQL server is considered only from connectivity point of view while the actual access credentials and test queries are defined per test. Therefore the endpoint definition is a simple procedure and is similar to all supported test endpoints.

13 ACCESS POINT INFORMATION

Related icons

-  unknown access point (unwanted state)
-  known access point (in the coverage area but outside administrative domain)
-  own access point (in administrative domain)
-  managed access point (target to a monitoring station, in administrative domain)
-  deactivated managed access point

The access point information can be displayed by right-clicking the access point in the Network topology and selecting “Properties”. The information includes the following:

- Access point name
- Alias
- Vendor
- Meru access points only:
 - Meru radio MAC
 - Meru access point ID
 - Meru radio index
- Description
- The managing Eye (i.e., the Eye that performs the tests)
- Related Eyes
- ESSID
- The antenna used by the Eye to monitor the access point
- Network
- MAC address (in case of Meru access point, serial MAC address)
- Alarm group
- SLA Group
- Encryption
- Beacon Interval
- Country Code
- Environment
- Capabilities
- Channel and channel change history
- legacy bitrates and changes in those
- 802.11n MCS Indexes
- 802.11n HT Capabilities
- 802.11n secondary Channel
- 802.11n Control Channel
- 802.11n HT Parameters
- WMM Category: Best Effort
- WMM Category: Background
- WMM Category: Video
- WMM Category: Voice

13.1 Replacing access points

7signal Sapphire saves all access points it has noticed. The changes in the hardware may be due removal of existing hardware or because of extensions of the current network. These cases are handled by inactivation of the removed access points or scanning and saving the new ones.

The hardware replacements require a different approach. The new equipment shall have new MAC addresses and this causes a discontinuity in the measurements as it is considered a new access point in the target network. If this is not the intention and the new equipment should totally replace an access point that was previously in Managed more, 7signal Sapphire must be informed.

To retain the measurement history with a new hardware:

1. Scan the network to get hold of the new access point hardware
2. Right-click on the access point that has been replaced to summon the “properties” dialog
3. Locate the replace panel and choose from the drop-down list the new access point that shall assume the role of the replaced access point.

Alternatively, it is possible to do replacing-by-import by using import utility. For more information, see chapter 21.

The intended use of this feature is to help with replacing identical hardware. If the hardware is not identical, the results may be many-fold. SLAs and alarm thresholds should be checked, for example.

There is also possibility to enable automatic access point change logic in Carat server. This can be done configuring Wireless Network to allow automatic changes¹³.

1. Open Edit Wireless Network by right clicking network in tree and selecting “Edit”
2. Enable “Allow automatic BSSID changes”
3. Save Wireless Network Configuration.

¹³ This feature works only with current Cisco hardware, on which how the MAC addresses are allocated is known.

14 LINKS AND LINK GROUPS

In 7signal Sapphire a link denotes an end to end connection between an Eye monitoring station and a Sonar server. Link consists of a monitoring station, an access point and a Sonar server. In the Network topology links are positioned below the managed access points. 7signal Sapphire forms the links automatically when it detects an established end to end connection.

Related icons



link



link group

A link group is a grouping of links defined by a user. A user can create a link in a Location in the Network topology. The main purpose of a link group is to give users the ability to easily bind one SLA group to multiple links with similar expected level of service.

Links and link groups enable the versatile binding of SLA groups formed from service level agreements to end to end connections. For example an SLA group bound to an organization is applied to all topology elements within that organization. However, this can be overridden by binding different SLA groups to specific links or link groups, in which case their compliance with the service level agreement is determined by measuring against the KPIs defined in their own SLA group, instead of the SLA group bound to the organization.

14.1 Forming Links

7signal Sapphire Carat forms a link automatically once a test profile with a Sonar definition is bound to a monitoring station.

For example when a test profile containing active tests to two Sonars ("Sonar1" and "Sonar2") is bound to a monitoring station ("Eye1") with two managed access points ("AP1" and "AP2") 7signal Sapphire carat forms the following links:

1. Eye1 - AP1 - Sonar1
2. Eye1 - AP1 - Sonar2
3. Eye1 - AP2 - Sonar1
4. Eye1 - AP2 - Sonar2

14.2 Removing Links

7signal Sapphire Carat automatically removes a link if one of its components (the monitoring station, access point or Sonar) is removed. Because links are formed automatically it may be in certain rare situations necessary for the user to remove links one deems unnecessary.

Remove a link as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link to be removed from the tree hierarchy
3. Choose "Remove link" from the pop-up menu
4. Confirm link removal

14.3 Creating Link Groups

Create a link group as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the desired Location into which the link group is to be added
3. Choose "Add Link Group" from the pop-up menu. A dialog for adding a link group is opened to the right.
4. Name the link group
5. Define the SLA group to be bound to the link group (optional)
6. Click "Save"

14.4 Removing Link Groups

Remove a link group as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link group to be removed from the tree hierarchy
3. Choose "Remove" from the pop-up menu
4. Confirm link group removal

14.5 Adding Link to Group

Add a link to a link group as follows:

1. Click on "View | Network topology" from the top menu bar
2. Drag the link to the desired link group

14.6 Removing Links from Group

Remove a link from a link group as follows:

1. Click on "View | Network topology" from the top menu bar
2. Right-click on the link (under a link group) to be removed from the tree hierarchy
3. Choose "Remove link" from the pop-up menu
4. Confirm link removal

15 ALARMS

7signal Sapphire has two types of alarms: Network Alarms and System Alarms:

- The network alarms are triggered by changes in the monitored network's status or topology. Network alarms are configurable; alarms can be switched on and off, alarm thresholds can be configured.
- System alarms are triggered by serious issues in 7signal Sapphire solution itself. For example, losing connectivity to monitoring station causes a system alarm.

15.1 Network Alarms

Related icons



alarm configuration



alarm configuration group



critical alarm



network error



informational message



warning message

The network alarms are initiated by significant changes in the monitored network's status or topology. It is possible to send the alarms to an SNMP system. Please see the instructions later in this document.

Alarms are used through alarm groups to which the desired alarms can be assigned. There is a preconfigured alarm group, Global Alarms, which is active by default. The alarms will then be issued by any access point in the network. The Global Alarms group includes the following alarms:

- Managed Access Point Down
- Offending Channel Changes of Managed Domain
- Offending Channel Changes of External Domain

15.1.1 Creating Alarm Groups

You can extend the Global Alarms group or create new alarm groups. It is recommended that you create new groups. To create a group, proceed as follows:

1. From the top menu bar, select "Manage | Alarm configuration"
2. Select "Alarm Groups" and right-click it
3. Select "Add Alarm Group"
4. Enter a name for the alarm group
5. Select the alarms by dragging them from "Alarm Templates" to the alarm group pane
6. When you have added all the alarms you want, select "Save"

Modification of alarms in a group

The table below lists the alarms. Some of them have parameters that can be modified. To modify the parameters of an alarm, proceed as follows:

1. Select the alarm to be modified in the alarm group
2. Right-click and select "Edit"
3. Modify the parameter value
4. Select "Update"

Table 5: Alarms

Menu	Severity	Description	Modifiable
Managed Access Point Not Responding	Critical	The alarm is activated when a managed access point does not respond.	No
Channel Interference	Warning	The alarm is activated when a new access point with a strong signal is detected on a managed channel.	Yes
Managed Access Point Security Settings Changed	Critical	The alarm is activated when the security settings of a managed access point are changed.	No
Managed Access Point Channel Violation	Warning	The alarm is activated when a managed access point starts to use a restricted channel.	No
Non-Managed Access Point Channel Violation	Warning	The alarm is activated when an external access point starts to use a restricted channel.	No
Unknown Access Point Detected	Warning	The alarm is activated when an unknown access point is detected.	Yes
End to end latency time exceeded.	Warning	The alarm is activated when the average round-trip time in a ping test exceeds the set limit.	Yes
End-to-End Connection Loss	Critical	The alarm is activated when ping tests fail.	Yes
Retransmission Rate Exceeded	Critical	The alarm is activated when the retransmission rate exceeds the set limit.	Yes
DCHP Server Unreachable	Critical	The alarm is activated on DHCP timeout.	Yes
Access Point MAC Change.	Warning	Alarm is activate when BSSID's MAC changes.	No
Attach Success Rate	Warning	Alarm is activated when Attach Success Rate falls under configured value.	Yes
DHCP Server Success Rate	Warning	Alarm is activated when DHCP success Rate falls under configured value.	Yes
Beacon Availability	Critical	Alarm is activated when beacons are not detected under configured value.	yes
TCP Download Throughput	Warning	Alarm is activated when throughput is lower than configured value.	Yes
TCP Upload Throughput	Warning	Alarm is activated when throughput is lower than configured value.	Yes

VoIP MOS, listen quality	Warning	Alarm is activated when listening quality drops under configured value.	Yes
VoIP MOS, Talk quality	Warning	Alarm is activated when Talk quality drops under configured value.	Yes
Ping Success Rate	Warning	Alarm is activated when Ping success rate drops under configured value.	Yes
TCP Success Rate	Warning	Alarm is activated when TCP success rate drops under configured value.	Yes
VoIP Success Rate	Warning	Alarm is activated when VoIP test success rate drops under configured value.	Yes
Internet Availability	Warning	Alarm is activated when Internet availability is lost.	No
Attach availability	Critical	Alarm is activated by consecutive attach failures	Yes
VoIP MOS, listening performance	Critical	Alarm is activated when average MOS download value consecutively drops under a configured threshold value.	Yes
VoIP MOS, talking performance	Critical	Alarm is activated when average MOS upload value consecutively drops under a configured threshold value.	Yes
TCP Download performance	Critical	Alarm is activated when average TCP download throughput consecutively drops under a configured threshold value.	Yes
TCP Upload performance	Critical	Alarm is activated when average TCP upload throughput consecutively drops under a configured threshold value.	Yes
Beacon success rate	Warning	Alarm is activated when beacons/probe responses are not heard from the access point	Yes
Noise level exceeded	Warning	Noise level on channel has exceeded configured threshold values	Yes

15.1.2 Binding Alarm Groups to access points

Network alarms can be configured on a per-access-point basis by binding an alarm group to an access point. Only an existing group can be bound to an access point.

1. In the Network topology, right-click the access point to which you want to bind the alarms
2. Select "Bind to alarm group"
3. From the pull-down menu, select the alarm group you want to use for this access point

Or

1. Open Service Alarm Binder Dialog by right clicking Service Area Node and selecting “Bind Alarms”
2. Select Alarm Limit Group from the drop-down list
3. Select Access Points for the binding
4. Save

15.1.3 Viewing Network Alarms

To view the network alarms issued, select “View | Network alarms” from the top menu bar. You can indicate whether you want to see all alarms or only alarms that are currently active. You can also select how the alarms are listed.

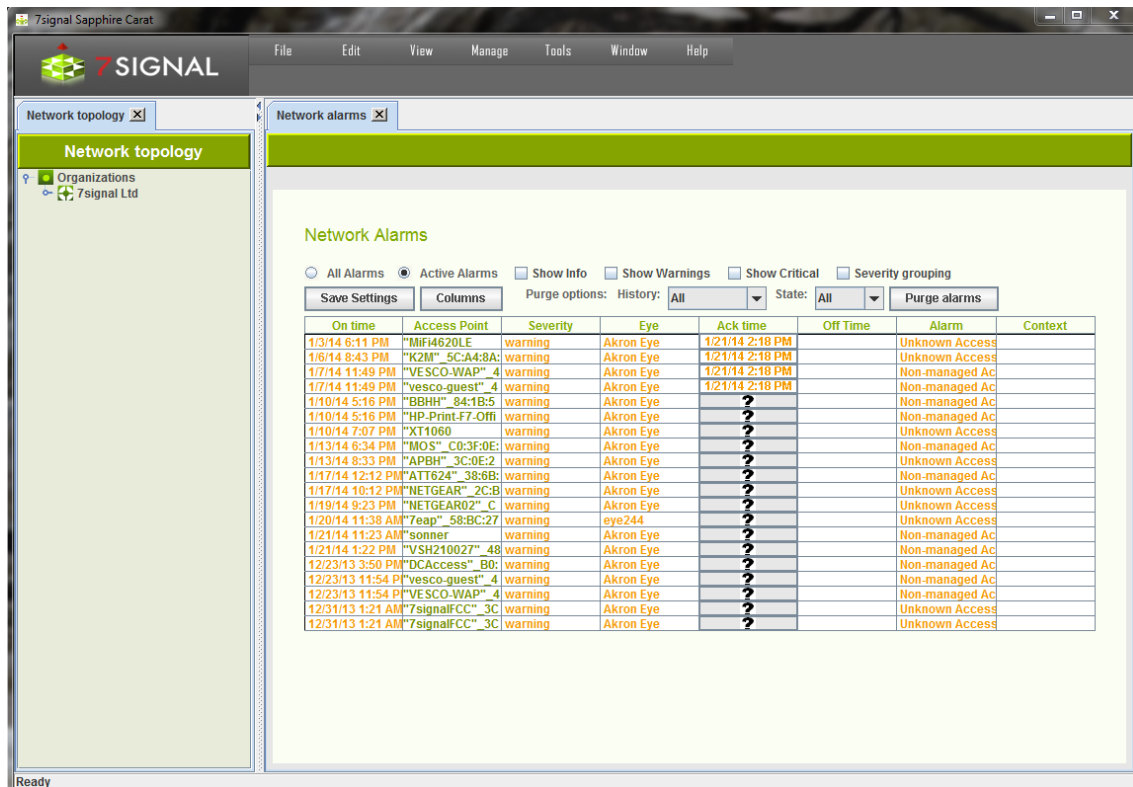


Figure 30: Network alarm view

15.1.4 Network Alarm forwarding

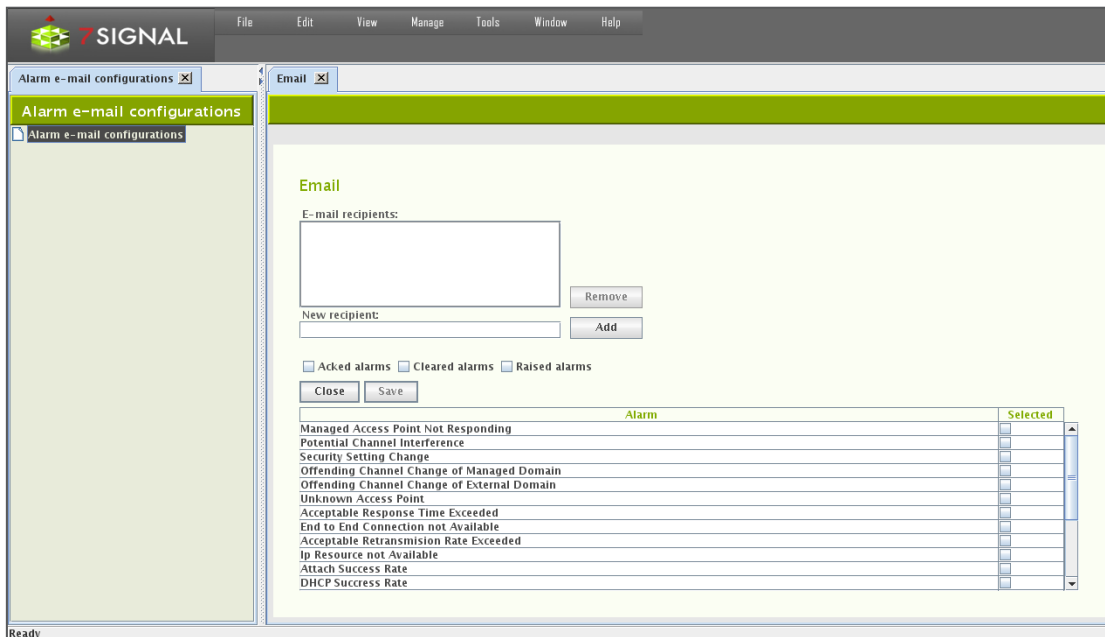
There are two methods that network alarms may be brought to attention of external systems: email forwarding and SNMP.

Email forwarding

Alarms are sent as plain-text emails with standard formatting easy to be parsed with typical text-processing tools.

NOTE: Email may be used only for relaying the alarms to the other messaging system that convert emails to f ex SMS and messenger formats. 7signal products do not directly provide such integration.

Email forwarding requires an SMTP server to be defined. There may be numerous recipients that shall receive the alarms.



1. From the top menu bar, select “Manage | Alarms | Email”
2. Enter target email address to “New recipient” field
3. Select “Add” to register the email address as a recipient. It shall appear in the box named “Email recipients”
 - a. Incorrectly added or not any more relevant recipients may be removed by activating the recipient in the box and then selecting “Remove”
4. Choose the types of alarm event that shall be forwarded by ticking the check-boxes.
 - a. Types are: raised, aked, offed.
5. Choose the set of alarms to be forwarded by ticking the check-boxes on the alarm table.
6. Select “Save” the make the selection permanent and stored.
7. Select “Close” to close the pane.

SNMP

Some alarms in Sapphire Carat can be forwarded as SNMP notifications to a receiving server.

1. From the top menu bar, select “Manage | Alarms | SNMP”
2. Enter the IP address of the receiving server
3. Enter the UDP port to use
4. Select the SNMP version (v2c/v3) to be used for the message format
5. If you select v3, you must also:
 - a. Enter a security name
 - b. Select the security level (authentication / no authentication)
 - c. If you select authentication, configure its settings:
 - i. Select an encryption method (MD5/SHA)
 - ii. Enter a password
 - iii. Re-enter the password
6. Select the alarms you want to forward
7. Select the events you want to forward:
 - a. Alarms issued

- b. Acknowledged alarms
- c. Alarms that have been turned off
- 8. Select "Update"
- 9. Click Save all Changes.

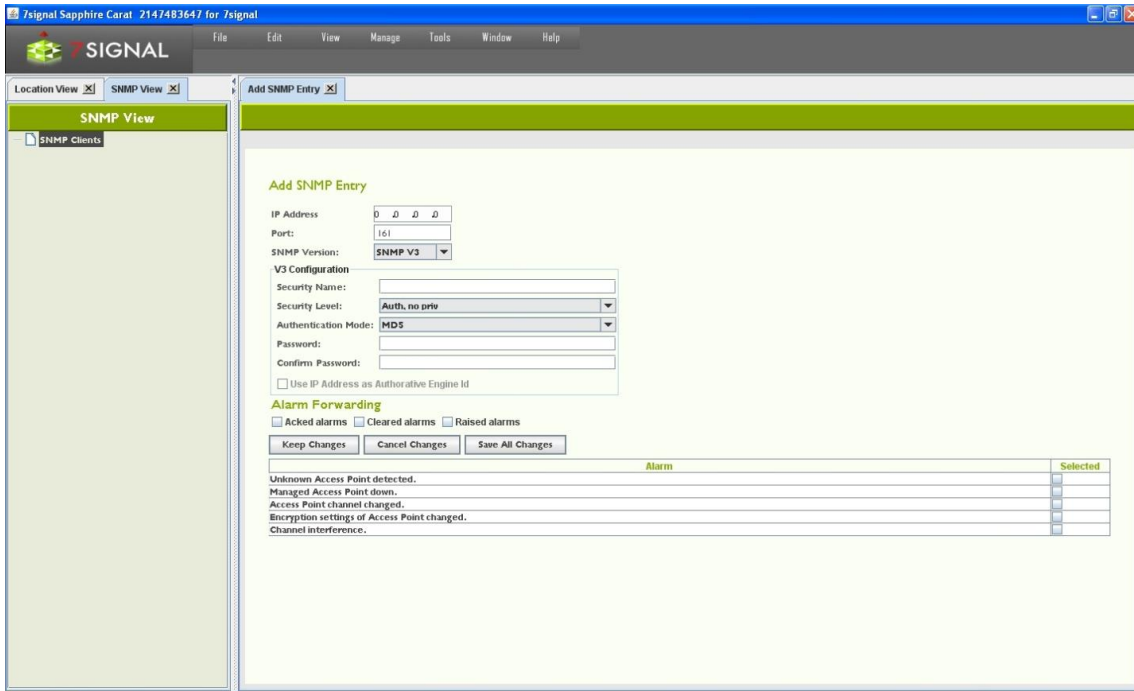


Figure 31: SNMP alarm forwarding

15.2 System Alarms

System alarms cannot be adjusted, since situations causing a system alarm are always serious. The alarm types are listed in following table:

Table 6: System Alarm types

Alarm name	Severity	Description	Info
Connection lost to Eye unit	Warning	Connection lost to Eye unit	Eye ID and its IP address
Database write failed	Critical	Test result write to database failed.	Table name and SQL error code.

15.2.1 Viewing System Alarms

To view the network alarms issued, select “View | System alarms” from the top menu bar. You can indicate whether you want to see all alarms or only alarms that are currently active. You can also select how the alarms are listed.

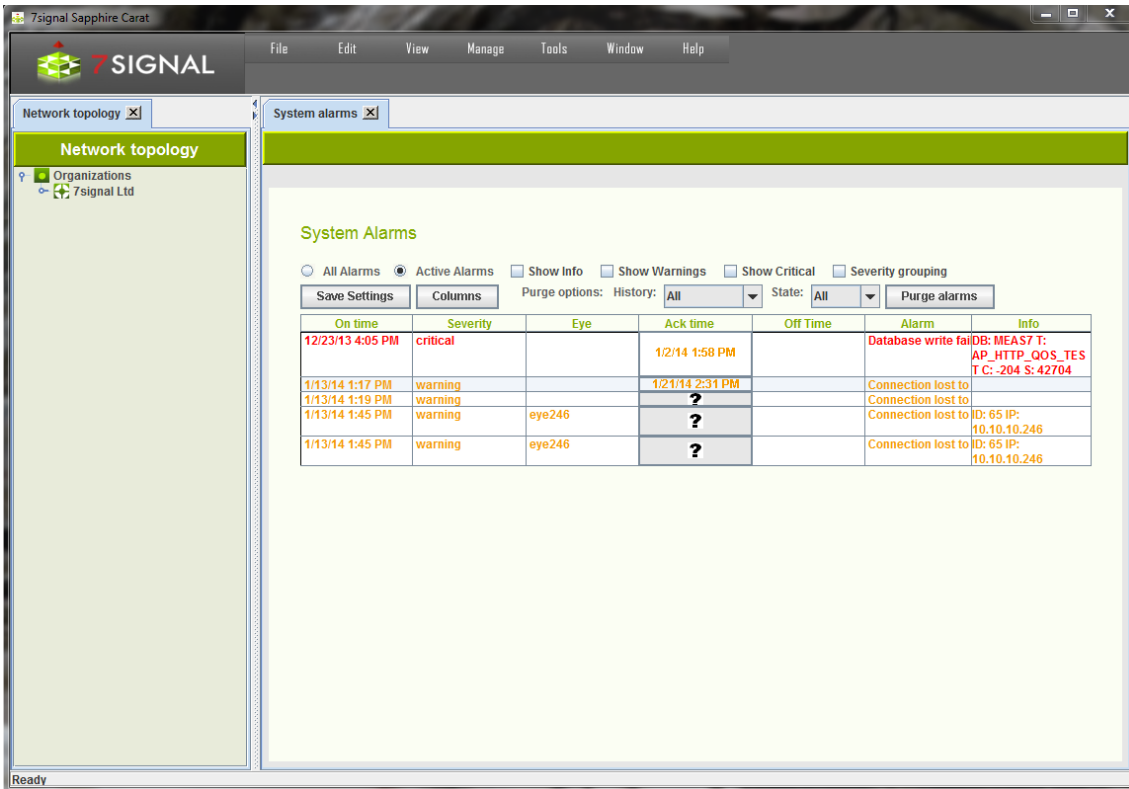


Figure 32: System Alarms

15.3 Acknowledge alarms

You can acknowledge a network or system alarm by clicking the symbol under “Ack time”. The symbol will be replaced by the current time of the Carat server, and the alarm is acknowledged. The alarms are turned off when the cause of the alarm is no longer present.

15.4 Purge old alarms

You can purge old alarms clicking “Purge alarms” button. In order to choose the criteria which alarms will be purged, select appropriate alarm state and time from drop-down lists.

16 TRAFFIC CLASSES

The IEEE 802.11e standard defines eight traffic classes. Most mission-critical access points support this standard. Traffic classes are becoming more and more important, especially on account of wireless VoIP.

7signal Sapphire Enterprise supports the 802.11e standard. Active tests can be configured to have a traffic class. All Sapphire versions support assignment of traffic classes, but if the Sapphire license does not include traffic classes, Sapphire will treat the traffic as ordinary traffic (Non-QoS, best-effort). Traffic classes are taken into account in only those networks whose access points support this feature. A request for a traffic class does not guarantee that it is granted. When viewing measurement reports, you might see that several traffic classes have been used. The class granted will never exceed that requested.

The following figure describes the traffic classes for the parameters of active tests:

802.11e category	
BestEffort(0)	<input checked="" type="checkbox"/>
Background(1)	<input type="checkbox"/>
Video(5)	<input type="checkbox"/>
Voice(6)	<input type="checkbox"/>

Figure 33: 802.11e traffic category selection

17 AUTOMATED TEST CONFIGURATION

The tests are grouped into passive listening tests and active tests in the radio network. There are two ways to run tests in Sapphire Carat: user-initiated (manual) tests to locate a fault and automated tests for continuous monitoring and collecting of measurement results.

You can run the tests from a hierarchical tree. Test menus are accessible by right-clicking a monitoring station or an access point.

17.1 Test Profiles

Related icons



test profile element (passive test)



test profile element (active test)



test profile element (disabled)



test profile



test profile template

A test profile is a series of tests that can be run continuously either on a per-access-point basis or in monitor mode, thus listening all 802.11 traffic. Test profile (element) can also be configured to run tests through monitoring station Ethernet port. Sapphire contains preconfigured profiles intended for typical business environments.

To set up test profiles, select “Manage | Test Profiles” to display the Test Profiles view. The existing templates, test elements and actual profiles are displayed on the left in the management tree in descending order, respectively.

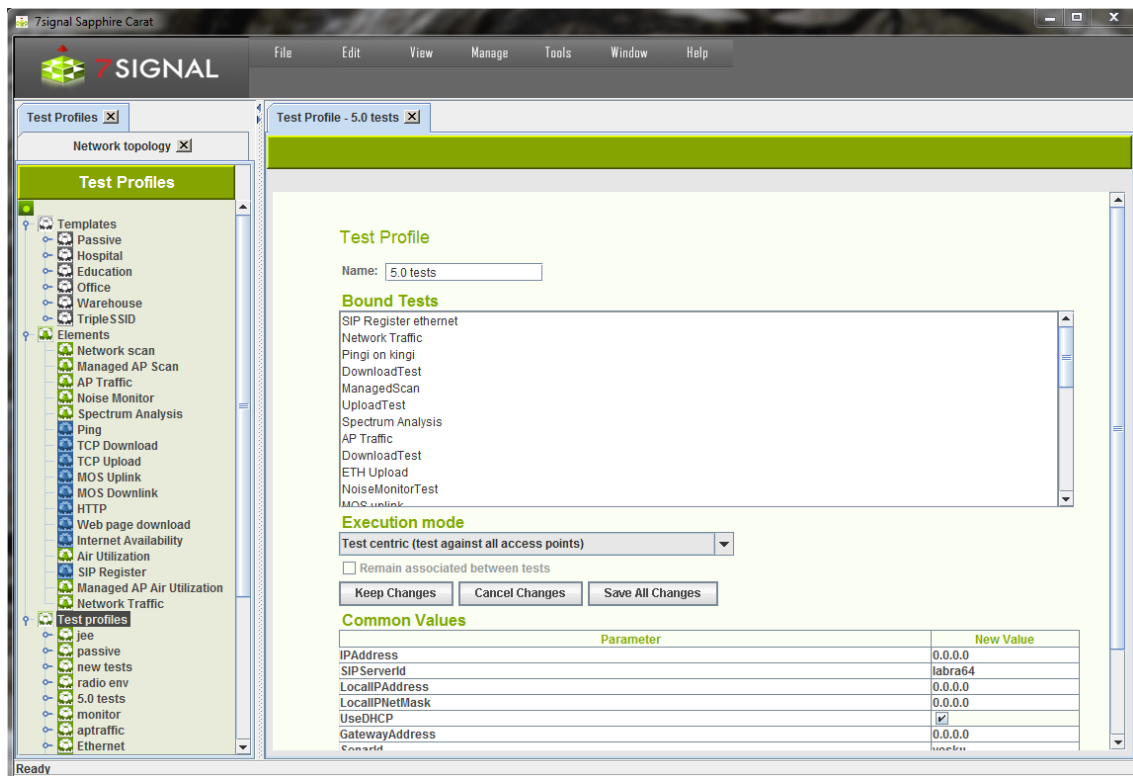


Figure 34: Test profile configuration

- **Templates** are a collection of pre-configured test profiles aimed at various business purposes. They are not to be used as runnable test profiles but as a source, reference and model for the user creating the runnable test profiles.
- **Elements** are individual tests that may be inserted to test profiles. Color of the test profile element icon indicates type of the test (passive or active).
- **Test profile** is a collection of test elements that may be executed. The user is supposed to copy either templates or elements to a test profile. There may be numerous profiles for different purposes. A test profile is always bound to a monitoring station.

Test profile can be either *test centric* or *access point centric*. *Test centric test profile* (default type) means that individual active tests are run against each access point before test profile proceeds to next test. *Access point centric test profile* means that all individual active tests are run against an access point at once¹⁴.

17.2 Contents of a Test Profile

The purpose of the network dictates which tests should be used to get the best picture of its functionality. As a result, there are several preconfigured test profiles, where the order and frequency of tests is different and so are test parameters, such as the number of megabytes downloaded and uploaded. The test profile names reflect the business environment in which they are thought to be most useful.

¹⁴ Test profile mode does not have any effect to Ethernet tests, because association to a network does not take place.

Below is a sample profile that could be used for a monitoring station.

Table 7: Test profile example

Test	Test parameters
RTT ping	32 B x 10
Download	2 MB x 2
Scan managed	350 ms/channel
Download	2 MB x 2
Access point traffic	60 s
Noise monitor	350 ms/channel
Scan	350 ms/channel
Http	500 kB
MOS	VoIP parameters

When the profile is running, each test is run in its turn, followed by the next test. After the last test is run, the test profile starts from the beginning. The table shows the most important test parameters, but the tests also have other configurable parameters.

Below are descriptions of the preconfigured profiles - Templates - in Sapphire. You can copy a template and save it under a different name. You can then freely modify the parameters in the original profile and the copy. By copying test profiles, you can easily create a customized profile for each monitoring station.

17.2.1 Passive

“Passive” template contains five passive tests and no active tests. In passive tests, the monitoring station does not attach to an access point; it just listens to radio traffic for the specified time. When using a passive profile, you do not need to configure encryption settings or authentication for the radio network.

Note: A passive profile has an extremely small effect on the monitored network. The only effect is that Sapphire sends probe requests to access points.

17.2.2 Warehouse

The “Warehouse” template serves the needs of logistics services where the amount of data transferred is not large but the data traffic is continuous. Network availability and uptime are vital. The network clients are mostly known or even preconfigured. This profile can be used in all environments that have similar circumstances.

17.2.3 Office

The “Office” template is intended for office use wherein the clients are mostly laptops running office applications. An office WLAN must have superb usability and a robust data transfer capacity. This profile can be used in all environments with similar circumstances.

17.2.4 Lightweight

The “Lightweight” profile is intended for environments that do not have several concurrent users and that have a narrowband link to a central server (<512 kbit/s). This profile emphasizes

WLAN availability. Another emphasis is on a fast testing cycle, where each test takes only a short time.

17.2.5 VoIP

The “VoIP” template is intended for environments where the wireless clients are mostly VoIP devices. A wireless VoIP network must have extremely high-quality radio connections. The MOS test indicates packet losses and jitter in the network, among other things.

17.2.6 Hospital

“Hospital” resembles the “Office” template. However, the “Hospital” template produces more results that describe the status of the wireless clients. The profile is a general purpose one that emphasizes wireless clients.

17.2.7 Spectrum and Noise

This template is limited in test elements: there are no active tests at all. It is targeted for environments that have severe interference conditions. This can be considered as a troubleshooting template that is activated if the normal course of testing does not provide enough information on the source of the interference.

17.2.8 Surveillance

The “Surveillance” is a limited template with one test only that specializes in surveillance. The point is to capture traffic in any channel in any direction. The rationale is environments where there should be no radio traffic at all or only for white-listed devices.

17.2.9 TripleSSID

Mainly example how to configure test profiles that access numerous WLAN networks in a single profile. This is the case one Eye unit is supposed to monitor multiple WLANs concurrently. The next chapter has more details on this.

17.3 Testing multiple WLAN networks in one test profile

One monitoring station may test multiple access points that provide multiple WLAN networks. In the context of test profiles WLAN networks are referred as ESSIDs.

Testing on multiple ESSIDs is achieved by either copying and editing individual test element in a profile or copying a complete template to an existing profile.

Whenever it is possible to define an essid to a test element there may be exactly one ESSID per element or no ESSID at all. The latter means that the test in question shall be executed against all access points managed by the monitoring station. The former limits the access points to ones that have the ESSID and are managed by the monitoring station.

17.4 Test Profile execution modes

The test profile execution mode controls how the tests are run within the test profile. The execution mode can be set while the test profile is created (or duplicated), or later by editing the test profile.

The execution modes are the following:

- Test centric (default execution mode)
- Access point centric

The execution modes are described in the following subchapters.

17.4.1 Test centric test profiles

Test centric test profile means that individual active tests are run against each access point before test profile proceeds to next test. This is the default execution mode.

Consider a test profile consisting of the following elements:

- Ping (active test)
- TCP download (active test)
- TCP upload (active test)
- Managed AP scan (passive test)
- Ping (active test)
- MOS uplink (active test)
- MOS downlink (active test)
- Noise monitor (passive test)

For example, if the monitoring station is monitoring access points AP1, AP2 and AP3, the execution order of the test would be the following:

Table 8: Test execution order on test centric test profile

